2011

Improving Intrusion Prevention, Detection and Response

Ibrahim, Tarik Mohamed Abdel-Kader

IMPROVING INTRUSION PREVENTION, DETECTION AND RESPONSE

TARIK MOHAMED ABDEL-KADER IBRAHIM

PhD 2011

Improving Intrusion Prevention, Detection and Response

By

TARIK MOHAMED ABDEL-KADER IBRAHIM

A thesis submitted to the University of Plymouth
in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Computing & Mathematics
Faculty of Science & Technology

November 2010

Abstract

Improving Intrusion Prevention, Detection and Response

Tarik Mohamed Abdel-Kader Ibrahim
BMath (Hons)

In the face of a wide range of attacks, Intrusion Detection Systems (IDS) and other Internet security tools represent potentially valuable safeguards to identify and combat the problems facing online systems. However, despite the fact that a variety of commercial and open source solutions are available across a range of operating systems and network platforms, it is notable that the deployment of IDS is often markedly less than other well-known network security countermeasures and other tools may often be used in an ineffective manner.

This thesis considers the challenges that users may face while using IDS, by conducting a web-based questionnaire to assess these challenges. The challenges that are used in the questionnaire were gathered from the well-established literature. The participants responses varies between being with or against selecting them as challenges but all the listed challenges approved that they are consider problems in the IDS field.

The aim of the research is to propose a novel set of Human Computer Interaction-Security (HCI-S) usability criteria based on the findings of the web-based questionnaire. Moreover, these criteria were inspired from previous literature in the field of HCI. The novelty of the criteria is that they focus on the security aspects. The new criteria were promising when they were applied to Norton 360, a well known Internet security suite. Testing the alerts issued by security software was the initial step before testing other security software. Hence, a set of security software were selected and some alerts were triggered as a result of performing a penetration test conducted within a test-bed environment using the network scanner Nmap. The findings reveal that four of the HCI-S usability criteria were not fully addressed by all of these security software.

Another aim of this thesis is to consider the development of a prototype to address the HCI-S usability criteria that seem to be overlooked in the existing security solutions. The thesis conducts a practical user trial and the findings are promising and attempt to find a proper solution to solve this problem. For instance, to take advantage of previous security decisions, it would be desirable for a system to consider the user's previous decisions on similar alerts, and modify alerts accordingly to account for the user's previous behaviour. Moreover, in order to give users a level of flexibility, it is important to enable them to make informed decisions, and to be able to recover from them if needed. It is important to address the proposed criteria that enable users to confirm / recover the impact of their decision, maintain an awareness of system status all the time, and to offer responses that match users' expectations.

The outcome of the current study is a set of a proposed 16 HCI-S usability criteria that can be used to design and to assess security alerts issued by any Internet security suite. These criteria are not equally important and they vary between high, medium and low.

Contents

List of Figures

Lists of Tables

Acknowledgements

The work, and indeed this PhD, would not have been possible without the help and support of my Director of Studies, Prof. Steven Furnell. Thanks go to him for his tireless effort in steering me through the PhD process, from publishing papers to presenting at international conferences. His professionalism and experience has been invaluable, and I owe much of my success to his guidance.

Thanks must also go to my other supervisors, Dr Maria Papadaki and Dr Nathan Clarke, who have spent a lot time proof reading papers and my thesis, in addition to providing helpful experience and guidance throughout my studies.

Thanks must also go to my sponsors, the embassy of the arab republic of Egypt (cultural centre & educational bureau) in London as the opportunity to obtain my PhD degree would not have been possible without their funding support.

Finally, I wish to thank my friends and family for their support.

Authors Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award.

Signed Tarik Ibrahim

Date 01/06/2011

Chapter 1

Introduction and Overview

1 Introduction and Overview

Network technology takes place in many major activities. For instance, it is used in Internet banking, telecommunications, electronic commerce and transportation. Hence, the need for secure information, computers and networks is increased in the network world because of the importance of this technology, specially, in the civilized societies. It is common in the network security field to encounter the term intrusion. Unfortunately, the concept of intrusion can have various meanings among the specialists who work in the technology field (Amoroso 1999). Moreover, some of them use the terms intrusion, incident, threat, malicious activity and attack interchangeably, which is not always true. However, there is no doubt that intrusions can cause damages; the amount of damages which varies according to many criteria, such as the vulnerability level of the attacked system, the skills level of the attacker and what is the purpose of the attack.

Evidence of the scale of this problem is that Symantec created 1,656,227 new malicious code signatures in 2008 (Symantec, 2009).The report mentioned that that number of intrusions is increasing every year and at the same time the nature of them became more sophisticated. Further evidence comes from the recent CSI/FBI survey (Peters, 2009), the Verizon report states that, of the breaches they investigated that involved malware in some fashion, 59% involved highly customized malware. The fact that such incidents occurred, in spite of that fact that an Intrusion Detection System (IDS) was used by 72.6% of the organizations while Intrusion Prevention System (IPS) was used by 59.1%, suggests that improvements in the technologies (or their deployment) are required to increase protection.

1.1 Intrusion Prevention

One of the major aims of most of the organizations is to have a secure system (i.e. information, computers and networks). Usually, these organizations achieve this goal by checking their systems frequently to reduce the flaws in them and by reconfiguring the system periodically. Moreover, these organizations search and inspect to discover if there is any vulnerability in the system and work hard to patch them as soon as possible. In other words, the intrusion prevention process focuses on the pre-attack period and works towards protecting the system from the known and the anticipated intrusions (Schultz and Ray 2007). Unfortunately, this process is not enough because the infrastructure of the network becomes more complicated and intruders become more intelligent and skilled. In addition to that, the aims of the intruders vary in a way that they know exactly what they want to do and how to do it. Therefore, highly skilled intruders can manage to avoid the traditional security tools. At this point, the importance of IDS appears.

1.2 Intrusion Detection

Intrusion detection can be defined as the process of monitoring and identifying the computer and network events, to determine the appearance of any unusual incident, as consequence, this unusual event is considered to be an intrusion. In other words, intrusion detection is defined as the "the process of identifying and responding to malicious activity targeted at computing and networking resources" (Amoroso 1999).

The intrusion detection research began in 1980s, with seminal work from (Denning, 1986) proposing a model of intrusion detection.. Denning later extended this work with the development of the real time Intrusion Detection Expert System (IDES) (Denning, 1987). Furthermore, a lot of research has been done for studying intrusion detection; as a result, some

experiments have been undertaken by practitioners to improve the performance of the existing IDS.

The problem of attacks and the need for defensive technologies to protect, detect and respond to them such as IDSs, firewalls and antiviruses is a requirement. Each of them has its own advantages and disadvantages. Chapter 3 and chapter 4 will focus on the IDS challenges in the real world.

1.3 Aims and Objectives of the Research

This research investigates methods of protecting network systems, with a specific reference to prevention, detection, and response against intrusions. The focus of the research is on IDS technologies. The work investigates previous and current IDS, their structure, their methodology, the place of deployment, their cost-effectiveness, their advantages, and their limitations.

The research can be divided into five phases

- The focus of the research during the first phase is to identify and analyze problems associated with the deployment of these technologies. The investigation establishes an awareness of existing published research in the area and then investigates problems that organizations actually face, by actively making contact with them. The aim is to have a good analysis of the problems that impede the use of IDS technologies.

- It is anticipated that the previous phase will reveal a significant problem of false positives (Yurcik 2002) as well as other challenges such as handling heavy network traffic in real-time. On this basis the challenges that encounter by the organizations in reality will be investigated to evaluate the severity of false positives and the other

challenges. According to the findings recommendations will be provided to alleviate these problems.

- To develop a set of HCI-S usability criteria based on the established literature and a walk-through method using the Norton 360 product.

- The previous HCI-S criteria will lead the current phase of the research by examining a selected set of integrated security products to assess whether they meet the HCI-S usability criteria requirement or not.

- Finally, the research proposed a solution to implement the criteria that were not fully addressed by the security products in the previous phase.

A prototype will be designed in the final phase to assess how would end users manipulate with the HCI-S usability criteria especially those criteria that were not addressed by the security products within phase 4.

1.4 Thesis Structure

The main discussion starts with Chapter 2, which introduces the main concepts of intrusion detection. In particular, the history, the models and the methods of intrusion detection will be clarified.

Chapter 3 presents the shortcomings and the challenges that are encountered with IDS. Hence, the main purpose of this chapter is to verify and demonstrate the existence of these challenges from the theoretical and academic point of view. Moreover, a list of these challenges is generated; this list is the base of the research that follows in the next chapter.

Chapter 4 utilises the list of challenges as the basis for a questionnaire and sent it to significant number of participants, most of them are practitioners in order to explore IDS challenges that are faced in practice. The results of the questionnaire are analyzed and the conclusions are provided.

Chapter 5 presents a new set of Human Computer Interaction and Security HCI-S usability criteria based on the established guidelines in the field of research. The criteria are tested by an alert issued by a well known security product namely Norton 360 version one.

Chapter 6 builds upon the findings of Chapter 5 by evaluating a selected set of security products to design, develop and evaluate IDS alerts that support end-users in protecting their network system and to improve the efficiency of responding to intrusions. Therefore, the outcome of the research should provide the end-users with a significant interface, informing them of the current state of the system and appropriate solutions to handle the situation.

The analysis in Chapter 6 reveals that several of the HCI-S criteria remain unaddressed by current packages, and Chapter 7 therefore proposes and implements a prototype solution that demonstrates approaches for handling these points. The prototype is then used as the basis for an end-user trial, enabling an assessment of its effectiveness in practice. An analysis of the resulting findings is presented, leading towards the final conclusions of the research in Chapter 8, which reviews the contributions and considers potential future work.

Chapter 2

A Review of Intrusion Detection Technologies

2 A Review of Intrusion Detection Technologies

The previous chapter focused on the terms of prevention, detection and response to intrusions. Hence, it is useful to mention that the term "system" can be used for a workstation, a network element, a server, a mainframe, a firewall, a web server, an enterprise network, etc.; and the term "audit" is used to indicate the information provided by the system including the inner work and the behavior of the system.

Computer system intrusion is an attempt to violate the integrity, confidentiality or availability of resources (Abimbola et al. 2006). There are many ways to protect systems against intrusions, some of which are called preventative techniques. Three of these preventative techniques are access control (Caelli 1994), authentication (Russel and Gangemi 1992) and encryption (Holz 2004).They are security techniques which are used to prevent intruders (specially unauthorized intruders) but they are not always successful. These types of security techniques can be the first line of defense against intrusions but because they sometimes fail there is a need for a second line of defense (Wu et al. 2006). Researchers suggest Intrusion Detection Systems (IDS) to be the second line of defense, which can detect intrusions when they happen and then have a response (the type of response depend on the kind of IDS).

This chapter will cover the efficiency of IDS, and their types and methods. In order to understand the behavior of IDS, the responses of these systems will be considered. Actually, the security administrator is responsible of the system security issue and what techniques will be used, but there is usually the problem of what type of IDS is suitable to use with the system that he/she is responsible of. There are two main detection methods and they are constructed with respect to information, if the intrusion-detection system uses information of the behavior

of the system it monitors, it is called anomaly detection system. If the intrusion-detection system uses information about the attacks, it is called misuse detection system.

2.2 Efficiency of Intrusion Detection Systems

There are many researches in the area of intrusion detection systems and researches construct many prototypes, attempting to determine the best among them. Actually, it is difficult to determine an efficient IDS without identifying some criteria to compare between them. Researchers state the criteria from their point of view; some of these proposed criteria are (Porras and Valdes 1998, Debar et al. 1999):

- **Accuracy:** The less the intrusion-detection system indicates a normal action as an intrusion the more accurate it will be.
- **Performance:** The more auditing the intrusion-detection system does the better performance it will have (more auditing means here the speed of auditing); good performance means that the real-time detection for the intrusion is more possible.
- **Effectiveness:** An intrusion-detection system should be designed in a way that makes it safe from any kind of attack, because if an attacker successes in his attack all the systems that IDS is used as a line defense for will be under attack as well.
- **Completeness:** Completeness means that the intrusion-detection system can detect all the types of attacks. This criterion if very hard to be measured because every day there is a new kind of attacks so no IDS will be complete 100% at least now. Constructing complete IDS is a hard research aim.

2.3 Misuse versus Anomaly Intrusion-Detection

There are two types of intrusion detection. The following sections describe each of them.

2.3.1 Misuse Detection

Misuse detection sometimes called knowledge-based intrusion detection or detection by appearance (Spirakis et al. 1994), is based on the intrusions which happened and detected in the past and then analyzed in a way that the researchers gain information from it and save these information in a knowledge base. In some organizations the security administrators only deploy the knowledge-based intrusion detection system, and they encounter the intruder's attempts to attack their systems. Therefore, if the type of the intrusion is found in the knowledge base that implies that the IDS will detect the attack (Sundaram1996). In other words, any action that the knowledge base does not classify as an attack will be classified as a normal activity. Hence, the accuracy of the knowledge-based intrusion detection systems is certainly good but the completeness of this method of detection needs an effort to update the knowledge base regularly.

Most of network intrusion detection systems (NIDS) use misuse detection methods to detect attacks, where the packets in the network traffic are compared against the signatures of a signature set that defines characteristics of an intrusion. If there is a match between a packet and a signature in the signature set then the intrusion detection system sends an alert to the security administrator or make any other response that depend on the way where the intrusion detection system is programmed to act (Kreibich and Crowcroft 2003).

It was mentioned that most of network intrusion detection systems (NIDS) depends on signatures so it is worth explaining what signatures are and how to generate them. Attack signatures describe the characteristic components of attacks. There is no common standard definition for these signatures, so different systems use different signature languages. The generation of these signatures is mostly a manual process that needs detailed knowledge of

each intrusion or attack that might be captured. Too simple (general, loose) signatures tend to generate large numbers of false positives, while too specific (tight) signatures cause false negatives.

Advantages of the misuse approach are that they have low false alarm rates (i.e. false alarm is one of the biggest problems in network security) and the knowledge base of the intrusion detection system is obvious so the security administrator of intrusion-detection system can have a fast response to an attack (Green et al. 2007).

Disadvantages of the misuse approach are that it is not easy to construct the knowledge base, because that needs to record in it all the types of attacks and a lot of information about them. This is the problem with previous attacks so for new attacks, the knowledge base needs to be updated regularly or this detection method will not be efficient enough.

The implementation of misuse intrusion-detection techniques can be done in several ways. The most widely used tools to misuse intrusion-detection are:

- Signature matching
- Signature languages

2.3.1.1 Signature-Matching

Signature matching is used to inspect user activity and identify, based on rules, what constitutes an attack. The attack signatures can be easily shared and provide a popular method of detecting known attacks.

Signature-matching also has disadvantages because when using tight signatures the signature matcher has no ability to detect attacks other than those for which it has exact signatures so the

signature matcher will not detect new types of attacks, loose signatures have the problem of false positives where alerts do not reflect an actual attack. It is important to know the difference between un-harmful network traffic causing an alert and successful attacks (Sommer and Paxson 2003).

2.3.1.2 Signature Languages

Any signature-based NIDS requires a language for defining signatures but most string-based NIDS use their own signature language, that way different NIDS are incompatible. For instance, Snort is an open-source lightweight network-based IDS which have a large collection of signatures (Roesch 1999, see www.snort.org). Moreover, Snort use a pattern matching model to detect network attack signatures using characteristic elements such as IP addresses, TCP/UDP port numbers, TCP fields, ICMP and strings contained in the packet payload (Patton et al. 2001). Each Snort rule has a rule header and rule options (Eckmann 2001).

NIDS Bro (Paxson 1999) is another known signature language which is constructed of two components: protocol analysis and policy script. The protocol analysis component provides the policy script component with a stream of events that categorize the activities detected by the protocol analysis (Sommer and Paxson 2003). One of the features of the Bro language is that, instead of using strings to detect an attack as many NIDSs do, it uses what is called regular expressions. These regular expressions have the ability of set-wise matching which make matching faster (Coit et al. 2001; Fisk and Varghese 2001).

Furthermore, there exist other signature languages such as N-code language used by Network Flight Recorder (NFR) (Ranum et al. 1997), the State Transition Analysis Technique (STAT) (Eckmann et al. 2002) and Production-Based Expert System Toolset (P-BEST) (Lindqvist and Porras 1999).

2.3.2 Anomaly Detection

Anomaly detection (sometimes called behavior-based intrusion detection or detection by behavior (Spirakis et al. 1994)) is based on monitoring and analyzing the system activities until generating what is called the normal system activity profile. As the security administrator uses the anomaly intrusion detection system, if the activity of the system is similar to the normal system activity that means that there are no intrusions but if the activity of the system is not similar to the normal system activity that means that there are intrusions (Sundaram 1996).

The completeness of the anomaly detection method vs. the accuracy of the anomaly intrusion detection shows that the completeness is good as the method has the ability to detect intrusions without the need for the signature database as the case of misuse detection method while the accuracy of the anomaly intrusion detection is not very good, because the high rate of false positives in comparison with the misuse detection method.

The advantage of anomaly intrusion detection is that it can detect new types of attacks that misuse intrusion detection cannot detect.

The disadvantage of anomaly intrusion detection is that, when the behavior of the system is not similar to the normal system activity the IDS classifies this as an intrusion, but sometimes there is no intrusion but there is just a deviation of the normal system activity, this case is called false positive error. Sometimes the intruder behaves like the normal system activity so the IDS do not refer this as an intruder and treat him as a normal user, this case is called false negative error.

Both false positive errors and false negative errors are significant problems. The first one requires a lot of effort to deal with what the security administrators considers as an attack and at ultimately they find that they spend a lot of effort on nothing. The problem, in practice, that there is not one error but many of them. Hence, a lot of effort, time and cost are wasted for nothing.

While in the case of false negative errors there is no effort but the problem is that the security team can not know anything about the intrusion until the damage has happened (of course that depends on the type of intrusions and the expertise of the security team).

The implementation of anomaly intrusion detection techniques can be done in several ways (Bierman et al. 2001). The following are an example of the most widely used analysis methods to build anomaly intrusion detection:

- Statistics
- Neural networks
- Computer Immunology

2.3.2.1 Statistics

Many researches worked in the field of the statistical anomaly detection such as (Helman et al. 1992, Helman and Liepins 1993) but the challenge that still encounters the statistical-based IDS is the requirement for gathering the sufficient amount of data to construct an efficient mathematical model. Unfortunately, the process of gathering the data is not practical, especially when the complexity of the network traffic is considered (Gordeev 2000). In addition, the Bayesian algorithm is used to improve the anomaly network intrusion detection method (Farid and Rahman, 2010).

2.3.2.2 Neural Networks

The science of neural networks (NN) gained a lot of interest in various researches. Therefore, intrusion detection researches also used NN, hence, some early researches such as (Debar et al. 1992, Sarle 1994) took advantage of the training process in the NN and employed them to develop their methods of the research (Giacinto et al. 2003; Cho 2002). The disadvantage of many of the IDS researches that employ the NN is that they use only a single neural network. Therefore, the neural network is unable to understand the environment, even if the NN is trained for a long time. Thus, to avoid this limitation, it is recommended to use more than one single layer (i.e. increase the number of the hidden layers). This strategy provides the advantage of better understanding of the environment by increase trading period for the NN because it will be more complex and sophisticated (Zhang et al., 2005, Seliya and Khoshgoftaar, 2010).

2.3.2.3 Computer Immunology

An Artificial Immune Systems (AIS) is a paradigm inspired by the immune system and is used for solving computational and information processing problems (Stibor et al. 2005). The AIS has the ability to adjust with their environments. They have the ability to differentiate between the existing pattern or normal, so-called "self" and the new patterns or abnormal, so-called "non-self" (Overill 2007). Moreover, (AIS) has been used in improving (IDS) from a long time, for instance, the work of (Debar et al. 1998 a, Debar et al. 1998 b) until now, for instance, the work of (Kotov and Vasilyev, 2009) and (Fang and Li, 2010).

The aim of AIS-based IDS is to perform a classification to the network traffic to decide whether it is self or non-self. The term detectors have a vital role is this process. Therefore, the process starts with creating a random set of immature detectors, these detectors will be

combined with the environment "self patterns" for a period of time. Thus, there are two main possibilities for this process:

(a) Some of the immature detectors will be similar to one of the "self patterns", hence these immature detectors will be taken out from the process (i.e. so-called negative selection).

(b) Some of the immature detectors will not be similar to any of the "self patterns", hence these immature detectors will be called mature detectors. Hence, these mature detectors will be representing the "non-self patterns". In addition, these mature detectors be examined by further learning process until the system be satisfied that they are an attack or just a suspicious activity.

The disadvantage of using AIS-based IDS is that there is no guarantee of the amount of false negatives. In other words, there is no complete control on the attacks categories that might bypass the system without being detected (Dozier et al. 2004).

2.4 Passive versus Active Intrusion Detection

This section is concerned with how an intrusion detection system can respond to an attack. When the intrusion detection system detects an attack, it will have a reaction to the attack; this reaction may be a corrective action such as solving a weakness in the system, or proactive actions such as logging of suspicious traffic or closing down the connecting port. In the case that the reaction of the IDS is corrective or proactive the intrusion detection system is called to be an active intrusion detection system. If the intrusion detection system only generates alarms to the security administrator, the intrusion detection system is called to be a passive intrusion detection system. Most intrusion detection systems are passive (Tian and Xueming, 2009), that means a large possibility of false positive alarms, having a negative impact on the system.

2.5 Summary

This chapter covers the two major methods of IDS: anomaly intrusion detection and misuse intrusion detection. In the real world, the use of anomaly intrusion detection is not enough; the case is the same for the use of misuse intrusion detection, because no one of them can detect all types of intrusions. It appears to be better to construct a hybrid IDS (i.e. an IDS which have the facilities of both anomaly intrusion detection and misuse intrusion detection). It will be easy for the security administrator to detect the intrusions for which patterns are recorded in the knowledge base by using the benefits of misuse intrusion detection while the anomaly intrusion detection give IDS the ability to detect unknown intrusions. Of course the accuracy of the misuse intrusion detection is better than the accuracy of the anomaly intrusion detection but it can not detect new attacks until its knowledge base is upgraded, which itself still an open area for research.

Even though there are many types of signature-based IDS and they are using different types of signatures languages, Snort and Bro are the most popular in the area of intrusion detection. There is still a need to improve them or to develop a new powerful signature language that has the advantages of both of them but at same time reduces the false rates and reduces the cost of detection as well and make the detection faster.

There are many open areas for researchers, such as it is not easy to define what the normal system activity, and to identify the IDS sensitivity problem to the environment. Moreover, studying the attempts of how to decrease the false alarms and how to make the IDS more active but at the same time the system does not lose its availability. Furthermore, how to deploy the IDS to be more effective. Therefore, it is recommended to the researchers who want to improve their IDS, firstly to understand their system and what kind of threat can affect it, secondly to

understand intrusion signatures. The next chapter will be the initial phase for studying some of these points. The aim of Chapter 3 is to provide a sufficient overview of the problems encountered by the users of IDS, as the first step in the overall process to develop a method to reduce the impact of at least one of the challenges that impede the IDS efficiency.

Chapter 3

IDS Challenges

3 IDS Challenges

Whilst a variety of IDSs exist within the marketplace, the level of deployment of such systems is far lower than other security countermeasures, such as anti-virus and firewalls. The CSI Computer Crime and Security Survey 2009 (Peters, 2009) shows adaption of IDSs at 72.6%. However, the deployments of anti-virus and firewall protection are used by 99.1% and 97.8% of respondents respectively. The adoption of IDSs can also be improved to reach a similar percentage.

Such findings raise questions about why IDS are less prominent than other well-known countermeasures, including many that have appeared in the marketplace more recently and had less time to establish themselves. One possible reason could, of course, be that the threats that IDS seek to combat are not as prominent or significant as those targeted by the other, more popular countermeasures. However, given that IDS can actually assist in dealing with many of the same threats as firewalls and anti-virus, this would not be a valid conclusion. Similarly, another possible argument is that they may not represent an effective solution, and therefore many organisations chose not to use them. However, if this was the case then one would instinctively expect the level of penetration to be even lower. As such, it appears likely that other factors are also coming into play, with potential users facing challenges that ultimately prevent IDS from being adopted.

With the above in mind, this chapter seeks to further explore the challenges posed by IDS technologies, drawing upon a literature-informed assessment of the potential problem areas. These will be used to establish a design of a survey amongst IDS users and others in a position to deploy the technology. More details about the survey can be found in chapter 4.

This chapter is organized as follows: deployment challenges, management challenges, technical challenges, detection challenges and finally, response challenges.

3.1 Deployment Challenges

This section focuses on the challenges that arise based on the way an IDS is configured, installed, and positioned in an organization. The following challenges have been identified:

- Scalability constraints,
- Switched Networks,
- Packet dropping and high speed network traffic,
- Encrypted traffic and IPv6,
- Initial deployment cost.

Each of the challenges are discussed and demonstrated in the following subsections.

3.1.1 Scalability Constraints

The size of the system affects the decision of what type of IDS should be used (Zhang et al. 2010). When the size of the protected network is small, the system administrator concentrates on the outsider attacks but when the size of the network is large, the insider attacks are considered as well. Moreover, when the size of the network is large the amount of data to be analyzed is large. Therefore, the efficiency of the IDS decreases when the size of the network increases. For instance, as the size of the network increases, the efficiency of signature-based IDS decreases.

Nowadays, the nature of the networks is large-scale distributed systems. These large-scale distributed systems require the deployment of distributed IDS (i.e set of IDS deployed in the

network and have the ability communicate with each other even directly or indirectly through an additional central server) to detect security events effectively (Fessi et al. 2007).

The deployment of the distributed IDS have various advantages, such as discovering attack scenarios, but it also has some limitations and challenges during the implementation process:

First, the increase in the network congestions, during the communicating processes between the distributed IDS. Definitely, the more complex the network topology is, the more increase in the network congestions will be.

Second, the selection of efficient methods for the decision making process must be considered. The decision making is based on the information transmitted from the various distributed IDS but this information should be evaluated carefully before making any decision.

Third, the selection of the sufficient number of IDS to support the decision making process must be considered. Therefore, the location where the IDSs are deployed should be selected carefully, at the same time, the number of the IDSs should be selected carefully as well, not too small; if the number is too small the awareness of the overall network will be not possible, not too large; if the number is too large even if the awareness of the overall network becomes possible there will be an overload with redundant information.

3.1.2 Switched Networks

Networks used to depend on hubs, which let the information available to all the ports. This ability is one of the hubs disadvantages, which help the attacker to sniff the network traffic (Tanase 2001). Later, switches were developed to increase the speed of the network. Switches have another important feature; they are capable of avoiding the sniffing process of the

attackers. Unfortunately, this feature reduces the effectiveness of the NIDS. This problem can be solved by increasing the number of NIDS in the network but this solution will not be cost-effective (O'Sullivan et al. 2005).

Some research has been conducted to measure the performance of IDS within the switched network environment (Iheagwara and Blyth 2002). The result of the research reveals two important points. Firstly, that the IDS performance becomes less effective when the bandwidth utilization is increased. Therefore, to avoid that impact more sensors can be used to increase the IDS performance but unfortunately this solution is expensive. Secondly, the IDS performance becomes more effective when the sensors are deployed at main entry points of the network. The final result does not neglect the importance of deploying sensors in other locations but that importance depends on the whole infrastructure of the network and other criteria according to the security policy of each organization. It is worth to mention that, the impact of routing and switching the packets has a great concern in this sort of research, especially, the amount of packets that might be lost because of the routing and switching process.

3.1.3 Packet Dropping and High Speed Network Traffic

The high speed of network traffic combined with the information overload can cause packet dropping. Therefore, the probability of missing attacks increases. Traditionally, IDS were off-line systems, logging and analyzing packets, hence, their performance was not that good because they did not have the ability of real-time response. Therefore, the research trend was to have real-time IDS which in theory is a perfect idea but in practice encountered the problem of dropping packets, leading to false negatives as well. Sometimes the system administrator is required to undertake the risky task of selecting the packets to be dropped (Salour and Su 2007).

Even though signature-based IDSs are widely used in the IDSs security world, they still suffer from the large volume of network traffic, which is transmitted through the network segments. These IDSs suffer because all the transmitted packets have to be checked by every signature in the database to identify if a match exists or not. Usually, these databases contain hundreds or thousands of signatures. Moreover, the signature-based IDSs are not only a resource consuming process but they are time consuming as well.

Existing signature-based IDSs cannot always handle all the network traffic, therefore, they start to drop packets as soon as they failed to compare all the coming packets with the signatures within the signature database. Hence, the possibility to bypass the IDS without being detected increases (i.e. false negative rates will increase) (Salour and Su 2007).

Most IDS have problems in detecting intrusions in low and medium network traffic speed but the problem is exaggerated when networks administrators or engineers start to use high speed networks to improve their performance from a communication point of view.

The high speed of the network traffic means that the IDS will receive a large amount of data that should be analyzed in real-time. Moreover, a drop of packets will occur if the processor speed in the IDS is not high enough to let the analysis process be done in real-time. Since most of the IDS are signature-based IDS and the rate of the increase of new intrusions is high, the developed signatures are increasing as well, therefore, the signature-based IDS suffer more than other IDS. In general, the problem is worse when the traffic in encrypted (Peddisetty 2005).

3.1.4 Encrypted Traffic and IPv6

IDS have the ability of monitoring normal network traffic; hence, it can analyze them and perform a suitable response. The problem of the normal traffic is that some attackers can

monitor them as well; therefore, the idea of encrypted traffic appears to have a more secure traffic. In other words, encrypted traffic supports the confidentially of the transmitted information. The drawback of the encrypted traffic from the IDS researchers and practitioner's point of view is that the encrypted traffic attacks can successfully reach the destination without being monitored by IDS (Fadlullah et al. 2010).

In the field of the network every computer connected to a network system must have an address, this address is called Internet Protocol Address (IP address). Most of the current IP addresses are IP version 4 (IPv4) which are 32-bit address space. Therefore, there was a need to increase the address space because of the increasing in the number of people using the network. To face this problem, IETF (Internet Engineering Task Force) started to develop a new version and called it (IPv6) which are 128-bit address space. The use of the new IPv6 encounters some problems when it was applied in the network environment.

The first problem is that (IPv6) is compatible with the old version (IPv4) but the reverse in not possible. The second problem is that since (IPv6) does not allow fragmentation at intermediate routers so it may be vulnerable to fragmentation attacks created to (IPv4) stacks (Durdag˘i and Buldu, 2010).

3.1.5 Initial Deployment Cost

The initial deployment costs may include the cost of purchasing the IDS and the initial training for those who will be responsible for managing it. Initially, the organizations should determine the components of their network system and evaluate the advantage of having each of them. (Wei et al. 2001) outlined some of the initial deployment costs as shown in Table 1.

COST CATEGORY	COST ELEMENTS
Equipment and Hardware	Computers (every kind), disks, tape drivers, printers, telecommunication, network systems, modems.
Software	Operating systems, utility programs, diagnostic programs, application programs.
Services	Commercially provided services, such as teleprocessing, local batch processing, on-line processing, internet access, e-mail, voice mail, telephone, fax and packet switch of data.
Supplies	Any consumable item designed specifically for use with equipment, software, service or support service.
Personnel	The salaries (compensation) and benefits for persons who perform functions, such as development, support, management, operation and analysis for running this system.
Other resources	Any not included in the above categories.

Table 1: Initial cost strategy (Wei et al. 2001)

Moreover, the cost categories; equipment and hardware, software, services, supplies and personnel; which were mentioned in Table 1, can be determined by a certain value of money. However, there are other types of components which cannot be quantified, such as data stored on disks (Wei et al. 2001). In addition, the evaluation process of the advantages of the deployment of the previous components can vary according to numerous criteria.

3.2 Management Challenges

This section focuses on the following challenges:

- Volume of information
- Ensuring effective configuration

- Managing a heterogeneous IDS environment
- Ongoing operational costs

Each of the above listed challenges will be discussed in the following subsections.

3.2.1 Volume of Information

Usually, the deployed network sensors and host-based agents generate a large volume of data. As consequence, the security administrators who monitor the system have to prioritise and filter this amount of information (Conti et al. 2006). Moreover, the amount information generated by the IDS increases the workload for the system/security administrator who has to consider it. Hence, the security performance is affected negatively by the time-consuming process that the administrators have in monitoring and manipulating unimportant information. In addition, the term "Information overload" is sometimes used in the field of security analysis as meaning a large volume of information (Conti et al. 2006).

The problem of the information overload is expressed by real numbers through a life example which is Georgia Institute of Technology's campus network. As (Conti et al. 2006) demonstrated in their paper that the number of the students, staff and employees who use the campus network is roughly 20,000 persons. The numbers of computers that are or can be connected to the network is approximately 35,000. The estimated amount of the transmitted data is 4 terabytes per day. This example raises the issue of dealing with this amount information of information without considering the type of information. The important question now is if this amount of data is 100% free of intrusions or not. To answer this question all of this amount data need to be examined. In the case that there are no intrusions, the administrators will be exhausted for nothing but if they detect any intrusions or any suspicious activity an alert will be launched which was the case in Georgia campus where roughly 50,000

alerts were generated every day from the IDS. The large number of alerts is another IDS challenge which will be discussed later in this chapter.

3.2.2 Ensuring Effective Configuration

It is difficult to tune the intrusion-detection system to minimize false alarms, without increasing the risk of missing attacks, and a balance needs to be struck between the two (Cavusoglu et al 2005). Hence, the aim of the IDS configuration is to reduce both of the false positives and false negatives rates while considering effective strategies to make the cost as minimum as possible. (Salour and Su 2007)

Some organizations do not completely trust the IDS when the organizations decide to deploy them. Therefore, the organizations try to identify the state of the organization before deploying the IDS and after the deployment. Usually, the organization uses the default configuration at the first period of the deployment until they start to be aware of how the system works. During the default period, the administrators in the organization become aware of the weakness and the strengths of the default configuration (Cavusoglu et al 2005). Hence, they work toward adjusting the configuration to make the IDS more powerful.

Moreover, knowing and understanding the environment where the IDS is deployed is important to avoid the occurrence of any problem that could raise if the previous experience of the current system administrator is related to another environment. Hence the configuration and the reconfiguration of the IDS are very important to make it more efficient (Goodall et al. 2004).

3.2.3 Managing a Heterogeneous IDS Environment

In the case of deploying multiple IDSs from different vendors, problems of interoperability might occur. Some of these differences might be in the way IDSs report alerts, their rule set, etc.

Practically, if the size of the network is large the deployment of more than one IDS is usually necessary and sufficient, to protect the system and to detect any sort of malicious event that might occur (Perdisci et al. 2006). Moreover, the deployment of one IDS might not cover the whole network that need to be protected, and it would not be able to detect distributed attacks such as DDoS. However, the alert formats in multiple generated IDS might be different. Therefore, the initial step to analyze these IDS alerts is to translate and unify their different formats to one understandable format if possible. Moreover, the process of having a standard format for the IDS alerts is called "format normalization" (Xiao, M. and Xiao, D. 2007).

Another side of the problem of the IDS heterogeneous environment is the analysis of the heterogeneous events it produces. These heterogeneous events require an effective method to correlate them to detect the intrusions, especially, in the case of multistage attacks. Therefore, the development of new strategies to correlate the variant heterogeneous network events enhances the performance of the existing IDS (Mathew et al. 2006).

It worth to mention that, because of the increase in the number of intrusions and the diversity of the methods that the attackers use, many heterogeneous IDS have to be deployed beside other security controls. Signature matching is one of the most effective methods in manipulating with the heterogeneous IDS alerts for discovering the multi-stage attacks.

As an example of how to deal with heterogeneous events (Carey et al. 2003) used Intrusion Detection Message Exchange Format (IDMEF) to manipulate with the received alerts from the heterogeneous IDS and other system controls such as firewalls. The reason of using IDMEF was because its ability to identify the alerts is greater than individuals IDS. Hence, the use of the IDMEF increases the possibly of detecting more attacks.

3.2.4 Ongoing Operational Costs

In the network security field, the increase in the capabilities of the IDS is associated with the increase of its cost. An IDS is useless if the cost of the deployment is more than the damage cost caused by the expected attacks. Researcher's investigations of the components that make the IDS cost-effective are very important in the process of improving the existing IDS. The cost of maintaining IDSs can be significant, as it requires skilled staff to manage it, analyze and respond to the security alerts that are generated.

There are many factors which contribute to the ongoing operational costs:
First, the detection cost (i.e. the sensors which are placed in selected locations are responsible of collecting data and then as a consequence these data are forwarded to an analyzer). Second, the analysis cost, (i.e. the analyzer receives that data from the sensors and then investigates the occurrence of the attack). Third, the reaction cost, which can be estimated by money expenses or human and tools consuming. Fourth, the attack impact (i.e. the caused damage if the attack successes to comprise the system, the side effects caused by the attack on the affected system if the IDS successes to detect the intrusion in an early stage).

Occasionally, the money cost of responding to the security event is much higher than the influence of the damage. Therefore, cost of reaction should be estimated before activating the reaction process to avoid the cost-loss. It is worth to mention that, the cost-loss is not always

money but in some circumstances it can be the impact on the organization reputation (Fessi et al. 2007). It is worth to mention that the previous components were called cost factors in (Lee et al. 2000), the factors were operational cost, response cost and damage cost.

3.3 Technical Challenges

This section focuses on the following challenges:

- Vulnerability to attacks
- Difficulty in customizing and updating the IDS ruleset
- Data collection and logging
- Understanding and interpreting IDS data

Each of the above challenges will be discussed in the following subsections.

3.3.1 Vulnerability to Attacks

Currently, many organizations use IDS as a defense for their systems. Attackers suffer from the existence of the IDS, so they start to launch attacks to exploit the IDS itself, which makes their main aim, to attack the organization systems, easier. One type of these attacks is backtracking, which exploits signature-based NIDS (Smith et al. 2006).

Some attackers target the IDS itself rather than other elements in the network, with the aim of bypassing intrusion detection. If attackers can take the IDS out service, further attacks can be launched against other targets within the network. Moreover, some IDS are built inside the system that they protect (Frincke et al. 2007), which means that, as the IDS is infected, the whole system is infected at the same time.

In the case of signature based IDS, the transmitted packets have to be checked by every signature in the database to identify if a match exists or not. Smart attackers are aware of the fact that this type of IDS is resource and time consuming. Therefore, some of them overload these systems with flood of packets (i.e. DoS attack). Moreover, signature based IDS are useless in the case of unknown attacks (i.e. attacks which has no signature in the database), this type of IDS can often fail to detect variations of known attacks (Salour and Su 2007).

3.3.2 Difficulty in Customizing and Updating the IDS Ruleset

One of the challenges is to keep the IDS ruleset regularly updated. In addition, it is important to customize the set of rules, in order to effectively detect attacks in the monitored network.

In the case of signature based IDS, to generate a signature for new attacks is not trivial. The signature generating process requires that the new attack had taken place and had been detected before. On one hand, after the detection of the new attack, an analysis process is provided to create a suitable signature which matches the new attack. On the other hand, the analysis procedure requires the analysis of many packets to generate an efficient signature (Salour and Su 2007). However, system administrators usually recommend that the databases to be constructed of small number of signatures because that implies that the packets will not be examined by large number of signatures.

Another part of the dilemma is the decision of selecting the appropriate signatures of the existing signature database and how to sort them to detect intrusions (i.e. the sort of intrusions that is most possible in the current network environment) by employing an efficient strategy. Unfortunately, the process is usually a manual one, human experts sort the signatures according to their experience, enable some of the signatures while ignoring others, train the IDS until finally they decide to use some kind of rule set that they are satisfied with. The danger of this

strategy is very obvious, especially if the disabled signatures were intrinsic in detecting the attacks, hence, avoiding the damage is unavoidable. Moreover, it is possible that the network be provided with a new protocol or service, hence, the administrators might not be able to modify there rule set in the immediately present time (Salour and Su 2007).

3.3.3 Data Collection and Logging

A secure network requires more than one layer of defense; each layer collects data in a special way. After collection, these data must be correlated to gain knowledge of what is really happening. Many sources can provide the IDS with data, which might have different formats. Therefore, there is a requirement to integrate these into an appropriate format for the IDS. Hence, data collection is the process of collecting information from different components of the network. The main data sources are system logs, packet headers, and packet contents. The data sources give us the information of the ports which are open and which are close, which IP address was probed, what is the objective of an attacker.

The IDS usually collect the required information by deploying numerous sensors in critical locations in the network. These sensors produce a large amount of information; this information has to be organized, accessible and readable. Hence, there is a need for an effective database which can manipulate with this large amount of information. In addition, the structure of the network (i.e. the network topology) is vital in planning the locations where the sensors are deployed.

It is worth to mention that even that the network topology is very important in deciding the suitable method to locate the sensors, there is another factor which is not less important, this factor is the how these information will be analyzed (Fessi et al. 2007). The major problems in data collection process are that they are collected from different places and therefore their

amount is enormous. The other challenge is the weakness of the process of sharing standard information between the different defense layers implies that the human experience is vital in data collection and correlation (Peddisetty 2005). The latter challenge can be considered as separate challenge which entitled in another subsection called "requirement for skilled staff".

3.3.4 Understanding and Interpreting IDS Data

There is a requirement for an efficient methodology to log the network traffic and as a consequence, to analyze and validate the IDS alerts, in order to determine if actual intrusions are taking place. Moreover, the traffic logs and the alerts logs need to be presented in a meaningful and robust interface. It is worth to mention that the information in IDS alerts should be sufficient to conduct a valuable analysis (Xiao, M. and Xiao, D., 2007).

As will be mentioned, two of the major problems in the area of IDS are false positives and false negatives. Sometimes the signature is too specific which raise the problem of false negative, while sometimes the signature is too general which raise the problem of false positive. Therefore, a thorough construction of the signature (pattern) can alleviate the appearance of the false rates (Yegneswaran et al. 2005).

3.4 Detection Challenges

This section focuses on the following challenges:

- The large number of alerts
- IDS can miss too many genuine attacks (i.e. false negatives)
- IDS can raise too many erroneous alerts (i.e. false positives)
- Determining the alert severity level

- Alerts correlation

Each of these challenges are discussed in the following subsections.

3.4.1 The Large Number of Alerts

IDS can produce a large number of alerts, which in turn causes information overload. This is especially the case when IDS are not aware of the characteristics of protected assets (context aware), resulting in the generation of superfluous alerts (Xiao, M. and Xiao, D. 2007).

3.4.2 IDS Can Miss Too Many Genuine Attacks (i.e. False Negatives)

The initial idea of the IDS was to detect intrusions in a very early stage. Although, most IDS have good performance they still have the problem of that some attacks are elusive and can penetrate the IDS without any sign, this is called false negative (Gong, 2002). In other words, a false negative occurs when the IDS fails to detect malicious network traffic, which as a result goes undetected (Sommer and Paxson, 2010).

False negatives cause more damage to the organizations than false positives (Joo et al. 2003). Therefore, false negatives are considered to be the damage cost of the attacks in some articles, while others consider it to be a major element in the damage cost.

3.4.3 IDS Can Raise Too Many Erroneous Alerts (i.e. False Positives)

Most of the IDS have the problem of accuracy, IDS treat part of the normal network traffic as intrusions while they are not, this is called false positive. Therefore, false positives are one of the major problems in the IDS field (Gong 2002). In other words, false positive refers to the network traffic that the IDS considers malicious but are not (Chen et al. 2009)

The anomaly based IDS usually encounter the problem of identifying the network traffic (i.e. what is normal and what is not). After wise, the process of making a decision for triggering an alert have done carefully otherwise the number of false positive alarms will be too high. It worth to mention that, making a profile for humans computing and network activities is not trivial. However, it is well-known that the high number of false positives is one of major problems in anomaly based IDSs, which affect the performance of this kind of IDSs (Salour and Su 2007). Furthermore, (Xiao M. and Xiao, D., 2007) refers the high false positives alarms to weakness of integration process between multiple IDSs.

3.4.4 Determining the Alert Severity Level

There are no standard metrics for the alert severity level. Therefore, a combination of organization security policy and security operator experience is required in order to interpret and rank/prioritize the generated alerts. However, there were some attempts to state the level of severity for the alerts. (Koike and Ohno 2004) attempts to identify that if the alert has one of the following features then the possibility of the alert to be false positive is high, these features are:

- The alarm appears consecutively,
- The alarm appears many times in the log file,
- The alarm is not associated with any of the network services,
- The alarm does not belong at all to the current network (i.e. if an alarm for a network which is not monitored is found, it would be false positive).

3.4.5 Alerts Correlation

There is a requirement to study the relationship between the various IDS alerts to determine the occurrence of the attack scenarios. Hence, the alert correlation process is not trivial, and is often not without problems.

The methodology in which the IDS alerts are generated was discussed previously and the challenge of encountering the large number of the generated alerts was discussed as well. This section is focusing on how to deal with these alerts. Initially, it is very important to gather the alerts with the same message and merge them into one alert if possible. Meanwhile a complementary method to reduce the rate of the large number of IDS alerts is to combine alerts into smaller number of high-level alerts, the process of combinations varies according to various criteria (e.g. the incident which cause the alerts have the same source, the incident which causes the alerts have the same destination, the alerts have has the same main features, the alerts have a common pattern matching, etc.) (Xiao, M. and Xiao, D. 2007).

Alert correlation is the process of finding a relation between some of the generated IDS alerts. This relation usually is how each of these alerts (i.e. the incidents which generated these alerts) is dependable on each other. This sort of relations is well-know in the academic articles by the term "attack scenario" which clarifies the sequence of attacks, step by step, until the ultimate attack is in process .The methodology of performing the alert correlation varies from system to another. For instance, some systems initially start with an alert verification process, to assess the level of accuracy of an alert (Xiao, M. and Xiao, D. 2007).

3.5 Response Challenges

The aim of IDS is to detect the intrusion in an early stage and send an alert to the security administrator to decide what the best response is in this case. In reality, according to the large number of alerts, sometimes the response is too late, or it is not powerful enough. Therefore, the trend of research is Intrusion Prevention System (IPS) which has the aim of preventing the system from the attacks (Gong 2002). There are many ways to categorize the response process. However, one of the recent papers (Stakhanova et al. 2007 b) proposed an intrusion response

taxonomy which classified the response depending on two measures: firstly, the activity of the response, secondly, the degree of automation in the response.

According to the first measure, the response can be active or passive. Unfortunately, most of the IDS are passive, they just report the damage caused by an attacker and provide the administrator with the gained information. Examples of an active response are terminating the session or blocking the traffic.

Meanwhile, the second measure categorizes the response to two major components manual and automatic response. Moreover there are other subcategories such as:

a- Static or dynamic: most of the systems are static, in the case of the static response, the response action does not change until the detected attacked is finished, while in the case of the dynamic response, the response action has the ability to vary according to the situation.

b- Reactive or proactive: most of the systems are reactive, in the case of the reactive response, the response action occurs after the intrusion is detected, while in the case of the proactive response, the proactive action has the ability to in charge before even the attacks happened.

Even though the trend of the research is having automated response systems, the researchers realize that this aim in all the cases will need a human expert.

This section will focus on the following challenges:

- Requirement for skilled staff
- The potential for inappropriate and harmful responses
- Effectiveness of the IDS response

Each of the above challenges will be discussed in the following subsections.

3.5.1 Requirement for Skilled Staff

The requirement of highly skilled staff is the core of the IDS process. Without staff to manage the IDSs and analyze / validate considerable numbers of IDS alerts, the purpose of having an IDS becomes less and less useful.

It was discussed previously that IDS generates a large number of alerts and produces high rate of false positives (Xiao, M. and Xiao, D. 2007). Therefore, the manipulation of these problems requires high skilled analysts (i.e. to analyze IDS alerts and validate which is true and which is false). Moreover, there is a need for a high skilled response manager (i.e. to activate a previously prepared response plan or modify the response plan or even trigger a new response according to life circumstances)

There is a trend to have completely automated IDS but this is not going to happen so soon. Some IDS do have automating monitoring and analysis, but this type of analysis still needs high level analysis done by human experts. It is very dangerous to let these systems have a completely automated response.

There are few human experts in the IDS field as this science started from about two decades. It is not easily to find one of them to employ and their salary is very high (Peddisetty 2005). Moreover, they should be up-to-date of what is happening in the field of security to secure their systems.

In addition, one of the challenges in the IDS community is that sometimes experts detect intrusions by experience and, when they are asked about the methodology that was used to detect the attack, they cannot give a straightforward answer (Goodall et al. 2004). Another problem is that there are vulnerabilities in the systems that some commercial vendors had solved, but they do not give their experience to the IDS community for commercial reasons. Some others do not declare the vulnerability that they detect because they are afraid that it will be used by attackers before that IDS community finds a suitable solution for it. Some of the challenges might not be an intrinsic challenge to the IDS itself, but they affect the efficiency of the humans who use them. Hence, these challenges affect IDS as well.

3.5.2 The Potential for Inappropriate and Harmful Responses

Responses may cause harmful effects if issued on the basis of false positives (Stakhanova et. al. 2007 a). For instance, normal traffic might be blocked or a normal network session be terminated.

IDS alerts usually contain a small amount of information about the event that causes the trigger of these alerts. Therefore, the information within the alert alone is not sufficient to gain an overall knowledge of that event. Moreover, that event might be just a genuine event but have one or more of the features of the real attack. Therefore, it is worth mentioning that not all the IDS alerts have the same level of certainty.

One of the methods that are used to categorize the intrusion response system (IRS) is its ability to adjust (Stakhanova et al. 2007 b). The ability to adjust category has two subcategories:

- static and
- adaptive.

On one hand, the static response suffers from that it some sometimes produces inappropriate responses because the response system does change its reaction during the period of the attack. The responses are usually updated by the human expert according to some criteria such as a time table or the detecting of high level threat. In summary, the static response relies on the manual efforts, which is not quick enough to respond to the intrusions or suspicious events in real time, and as a result this causes inappropriate responses in some circumstances.

On the other hand, the adaptive response suffers from that it some sometimes produces harmful responses because the response system is able to change its reaction during the period of the attack. The responses are usually updated automatically without the inference of any human expert according to a preprepared set of responses. In summary, the adaptive response does not rely on the manual efforts, which let it more vulnerable to perform harmful responses especially if the appropriate response was not in the preprepared list.

3.5.3 Effectiveness of the IDS Response

Many IDSs are passive, they just report the damage caused by an attacker and provide the security operator with the collected information. Automatic response is cost-effective but most of the IDS responses are still manual, even though manual response is time consuming.

Existing IDSs have the ability to detect security events but they still lack in implementing an active response to make the protected systems more secure (Fessi et al. 2007). On one hand, reactive IDS requires a thorough knowledge of the detected security event, while on the other hand it requires the awareness of the system environment (i.e. operating systems, servers, services provided by these servers, ports opened or closed, etc.). Moreover IDS can never guarantee 100% the occurrence of the attack, it only triggers an alert that some kind of security event happened, which might be a false positive. Hence, many existing IDS are only passive

because they do not trust IDS alerts to perform a reactive response and even when some of them perform a reactive response usually this reaction will not be severe.

Passive	*Active*
Administrator notification: generate alarm *(through email, online/pager notification, etc.)* generate report *(can contain information about an intrusion such as attack target, criticality, time, source IP/user account, description of suspicious packets, etc. as well as intrusion statistics for some period of time such as number of alarms from each IDS, attack targets grouped by IP, etc.)* *Other responses:* enable additional IDS enable local/remote/network activity logging enable intrusion analysis tools backup tampered with files trace connection for information gathering purposes	*Host-based response actions:* deny full/selective access to file delete tampered with file allow to operate on fake file restore tampered with file from backup restrict user activity disable user account shutdown compromised service/host restart suspicious process terminate suspicious process disable compromised services abort suspicious system calls delay suspicious system calls *Network-based response actions:* enable/disable additional firewall rules restart targeted system block suspicious incoming/outgoing network connection block ports/IP addresses trace connection to perform attacker isolation/quarantine create remote decoy†

†Borrowed from (Wang, Reeves and Wu, 2001).

Table 2: List of common passive and active intrusion responses

Table 2 provides a list of the common passive and active intrusion responses. The aim of this table or any other similar table in other paper is to have an overview of the strength and the weakness in these response processes. Even though it was mentioned previously that sometimes there is a lack in understanding the meaning of the IDS concepts, it is worth to indicate that the same problem exists with the intrusion response terminology. Therefore, some researchers tend to give more description to the term to avoid confusion and misunderstanding (Stakhanova et. al. 2007 b).

3.6 Summary

No.	The IDS Challenges List	Section
	Deployment Challenges	
1	Scalability constraints	3.1.1
2	Switched Networks	3.1.2
3	Packet dropping and high speed network traffic	3.1.3
4	Encrypted traffic and IPv6	3.1.4
5	Initial deployment cost	3.1.5
	Management Challenges	
6	Volume of information	3.2.1
7	Ensuring effective configuration	3.2.2
8	Managing a heterogeneous IDS environment	3.2.3
9	Ongoing operational costs	3.2.4
	Technical Challenges	
10	Vulnerability to attacks	3.3.1
11	Difficulty in customizing and updating the IDS ruleset	3.3.2
12	Data collection and logging	3.3.3
13	Understanding and interpreting IDS data	3.3.4
	Detection Challenges	
14	The large number of alerts	3.4.1
15	IDS can miss too many genuine attacks (i.e. false negatives)	3.4.2
16	IDS can raise too many erroneous alerts (i.e. false positives)	3.4.3
17	Determining the alert severity level	3.4.4
18	Alerts correlation	3.4.5
	Response Challenges	
19	Requirement for skilled staff	3.5.1
20	The potential for inappropriate and harmful responses	3.5.2
21	Effectiveness of the IDS response	3.5.3

Table 3: IDS Challenges List

This chapter demonstrates the challenges encountered by the users of the IDS, trying to describe these problems sufficiently. The chapter includes five categories of challenges: the deployment challenges, the management challenges, the technical challenges, the detection challenges and finally the response challenges. Each of these categories has its own components. A list of all the challenges discussed in this chapter is illustrated in Table 3. The outcome challenges of this chapter will be the source of information for a questionnaire about IDS challenges that will be the topic of the next Chapter. The motive of addressing the challenges through a questionnaire is to evaluate how far the challenges based on the literature review match those encountered by the organizations in practice. Moreover, the descriptions of the challenges in this chapter will be used to extract a brief definition for each of them to be

guidance for the respondents of the questionnaire, because some of terminologies might have various interpretations.

Chapter 4

Practitioners View of IDS Challenges

4 Practitioners View of IDS Challenges

This chapter continues the investigation of the challenges that encounter by IDS in practice through a conducted questionnaire based on the points which were discussed in the previous chapter, to evaluate how far the challenges from the literature match those encountered by the organizations in practice. On one hand, the most appropriate participants to the questionnaire are those who are (or have previously been) in a position to make IDS deployment decisions, while, on the other hand, the participation of those who have experience with IDS solutions in their organization or others who feel able to offer an informed opinion, were also appropriate. Chapter 4 clarifies the reason behind selecting the questionnaire as a method to inquire information. Moreover, the web design of the web-based questionnaire is demonstrated. Furthermore, the results of the questionnaire are revealed and illustrated by the figures. Finally, a full analysis of the responses is provided based on various adopted methodologies for ranking the challenges to obtain more benefits for the responses.

4.1 Research Methodology

The questionnaire method is one of the efficient methods to collect data for the topic under research and to evaluate the participants' responses. However, this is not the only method to collect the data. These data can be collected through focus groups, interviews and even phone calls. At this stage of the research it was desirable to select the questionnaire method as a first choice for different reasons. These reasons vary according to the location where the research is conducted and the early stage of the research itself (i.e. the difficulty of finding many local experts in the field of IDS to interview). Therefore, the questionnaire method was selected to be the initial method to obtain the required information. Moreover, according to the results of the questionnaire, it will be decided if there will be an actual need for the other methods (i.e.

interviews and small groups) or whether the results will be sufficient for the next step of the research.

4.2 Survey Design

The aim of this section is to present the design of the questionnaire after it was selected to be the source of collecting the data. The context will be based on the provided information in Chapter 3, which gathered the IDS challenges according to a variety of prior published works (i.e. no single paper had previously gathered all these IDS challenges in it), each of which only focused on one or a few challenges, without mentioning anything about the others.

However, the questionnaire process begins with a trial hard copy questionnaire which were conducted and given to some Master and PhD students who are conducting research in network and network security. All of these students were examined in the subject of network security and attended or still attending a course in IDS. Hence, they are the available and appropriate next best group to assess their responses to the preliminary questionnaire.

The aims of this procedure were the following:

- to measure the required time to finish the questionnaire,
- to determine the clarity of the questions; to identify if the structure of any of the questions are misleading the participant and therefore, need to be written again to avoid misinterpretation.

Actually, the responses which were received from the previous participants were valuable and they were considered in improving the quality of the second stage of questionnaire (i.e. web-based questionnaire). Therefore, according to the results of the preliminary questionnaire, it was decided to decrease the time span of the questionnaire by decreasing the number of questions and leave the questions that focus on the main aim of the questionnaire, which are the

IDS challenges (i.e. the limitations that face the deployment of the IDS). Moreover, some of the participants complained that the title of some of the challenges were confusing and trapped them in a hesitating position before they made up their mind of the severity of the challenge. That confusion will lead to an increase in the time span of the questionnaire; hence, it was decided to append a brief description to each challenge, to be as guidance to the participants who might be hesitate onto about what it is meant by this challenge in the questionnaire.

The questionnaire begins with an introductory page illustrates the questionnaire and the aim of it. The page presents the type of required participants and makes the participants aware of the time span needed to accomplish the questionnaire (i.e. it is mentioned that responding to the questionnaire will consume roughly from 5 to 10 minutes). Moreover, it was important to inform the participants how to contact with the designer of the questionnaire, in case that that they have any questions or further interest in the result of the questionnaire. Finally, at the end of the introductory page, the participants have the option to continue; if they are related to subject and is interested to support this research with their contribution, by clicking on the "next" button or the option of exiting the questionnaire by clicking on "Exit and Clear Survey".

4.3 Survey Results

It is worth to mention that, the link of the web-based questionnaire was sent to more than 2000 persons who are related to the network security field. These persons were selected through adapting a collection of various methods; one of the methods was advertising the web-based questionnaire through the British Computer Society (BCS), another method was by having contacts with persons working in large organizations (i.e. banks, hospitals, universities and telecommunication). Moreover, there was the chance to meet some persons who are working with IDS solution or used to, hence, it was a chance to give the link of the questionnaire. Actually, the latter category was very helpful even that some of them volunteer to send the link

to some of their colleagues. Many of them recommended trying to reach the participants through a person who knows them, hence, they might be interested in responding. Usually, they are not interested in responding to this type of questionnaires because, in most of the cases, do not add value to their work and most of them are poor in their design and time consuming. However, after the first list was constructed and sent, the responses were very few. Hence, new lists were generated until the number of persons exceeds 2000. Unfortunately, only 41 of them answered the questionnaire completely. Therefore, it was decided to perform the analysis according to their responses, even that it is acknowledged that the result of the analysis would be better if the number of participants was higher. It was noticed that some persons started to answer the questionnaire but they decided not to finish it, the reason behind that might be because they did not suppose that the number of challenges would that high or because they usually focus on a special type of problems such as false positive. The questionnaire was organized into two major sections:

- Demographics
- IDS Challenges - these challenges are organized as five main sections as follows (based upon the categories previously identified in Chapter 3): deployment challenges, management challenges, technical challenges, detection challenges and finally, response challenges.

4.3.1 Demographics

The purpose of the questions in this section is to have a general view of the type of the participants; the organizations that they belong to, the size of their organizations, their job titles, and information about the participant's years of experience in the field of IDS. Meanwhile, the participant's were asked to reply to a major question about, if they are in a position to deploy (or taken the decision to deploy) an IDS or not. Furthermore, the type of IDS they decided to

use and the IDS approach that they used in detecting intrusions were of the concerns of the questionnaire.

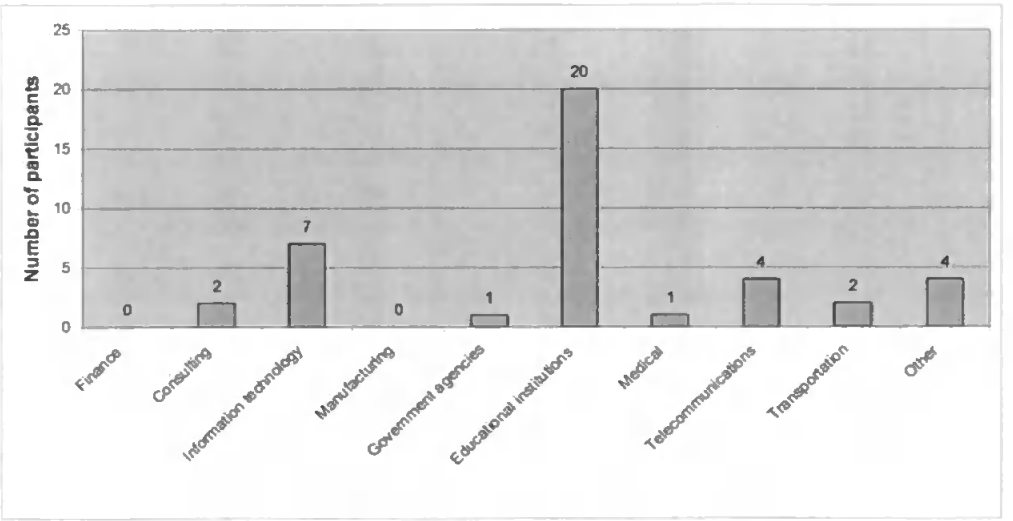


Figure 1: The sector that the participants belong to

Figure 1 is a chart that represents the sector that the participants belong to. From the selected organizations list, the responses were as follows the highest number was 20 belonged to educational institutions, but no responses were received from persons working in finance or manufacturing organizations. This result was expected as the questionnaire were sent to a higher number of persons who are working in educational institutions Moreover, one of the participants who selected the "Other" category wrote that he/she is related to the defense organization while another one wrote R&D organization. The selected list of organizations covers a wide range of organizations which have diversity in the environment that the IDS are deployed. The fact that only 11 (out of 41) of those that answered the questionnaire were from the IT sector does not affect the results as the current question asked about the organizations that the participants belongs to not their jobs.

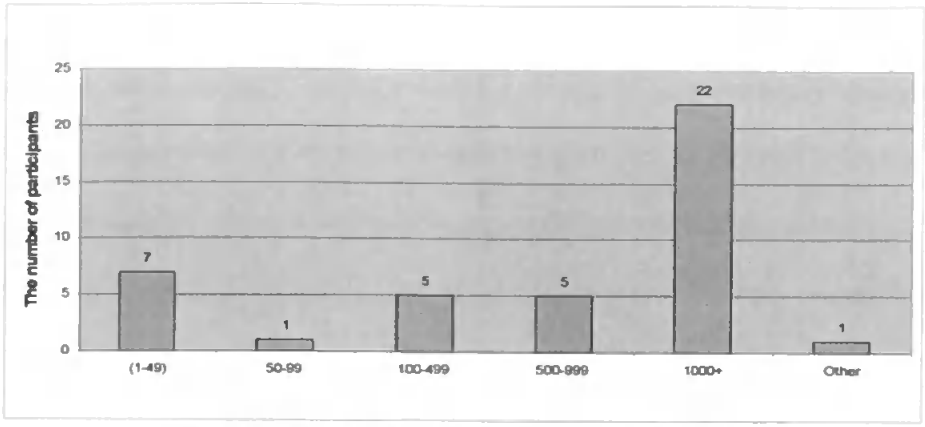


Figure 2: The size of the participant's organization

Figure 2 represents the size of the participant's organization. The chart demonstrates that the majority of the participants work in organizations which employ more than 1000 employee which indicate that the questionnaire will obtain valuable answers from this group of participants as they work in large organizations.

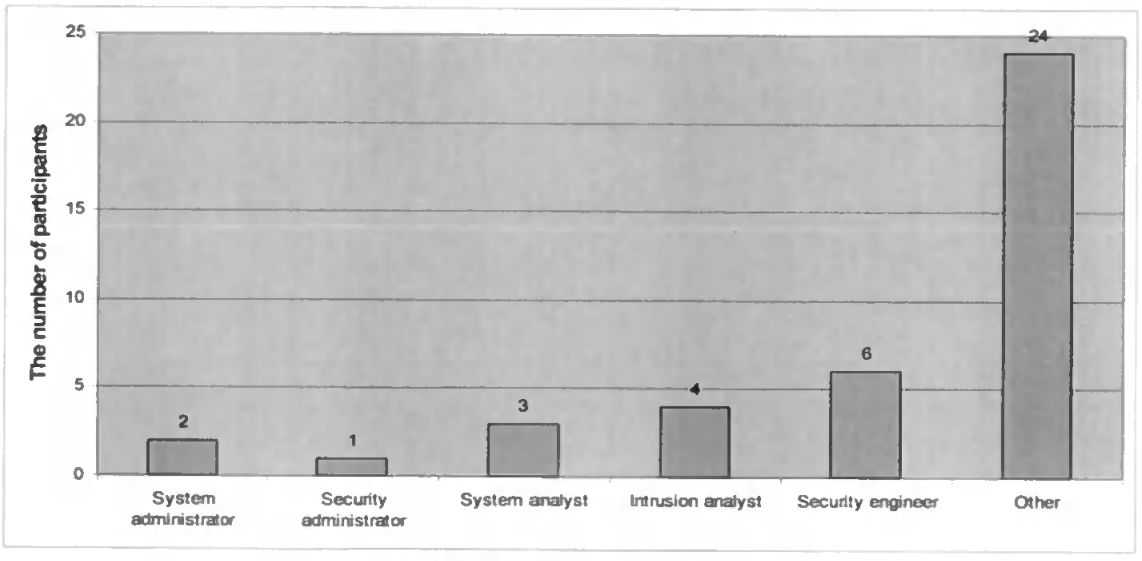


Figure 3: The participant's role/ job title

Figure 3 represents the participant's role/ job title. The chart demonstrates that the majority of the participants role/ job title do not belong to the questionnaire list. That does not mean that they are not security experts but it might mean that they have a different job title. The following titles appears during the participation; IT security manager, IT director, CTO, design engineer,

R&D security, technical director, senior security architect, visualization designer, security & compliance group leader and of course some various academic titles such as professor and researcher.

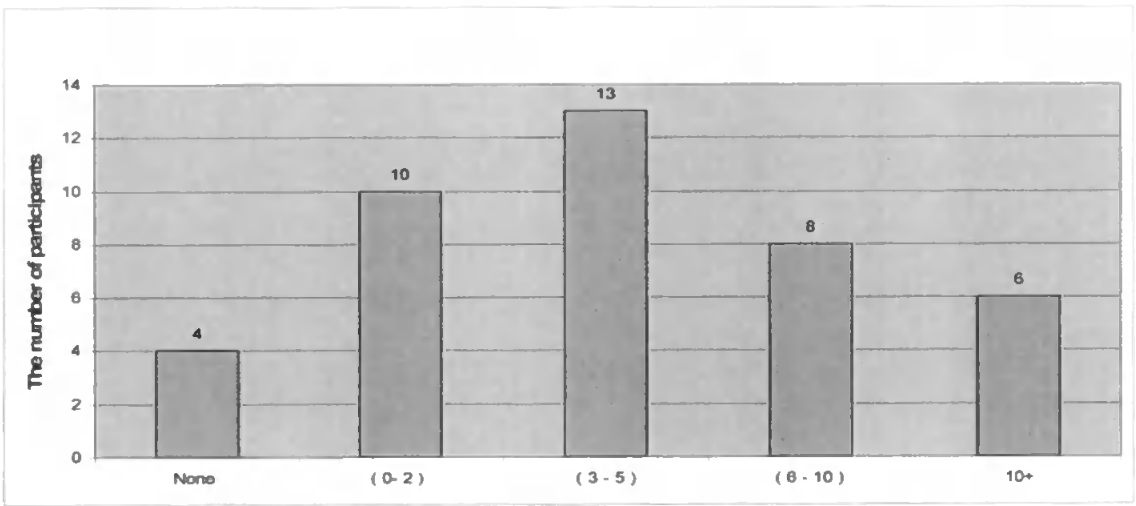


Figure 4: The number of years that the participants work with IDS

Figure 4 represents the number of years that the participants work with IDS. As the results demonstrated only four has no work experience with IDS while 6 have experiences more than 10 years with IDS. Hence, 27 participants have experience more than 3 years which is good to obtain valuable results for the questionnaire.

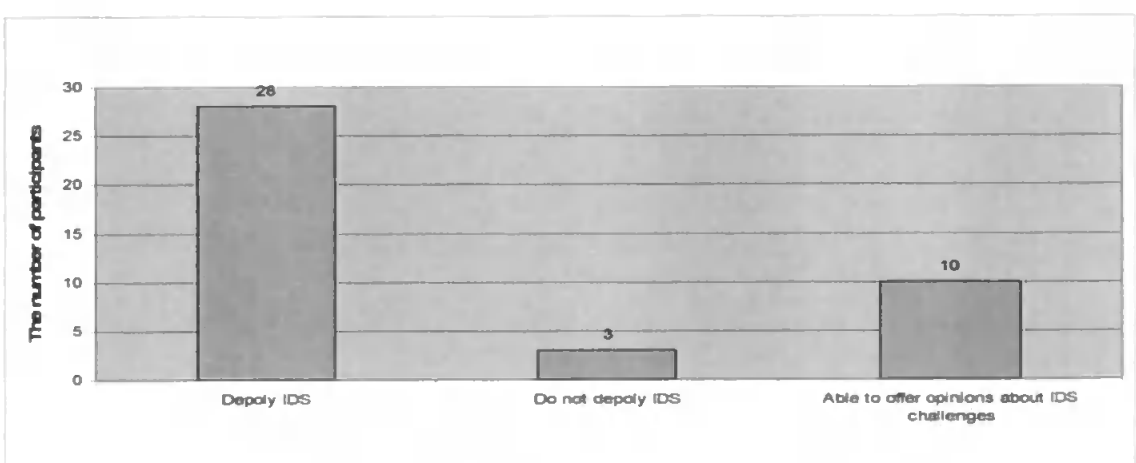


Figure 5: The participant's type

Figure 5 represents the participant's type according to the position that they occupy in their organizations and whether they have deployed (or taken the decision to deploy) an IDS before or not. Fortunately, the majority of the participants 68% belong to the category who had been able or were still able to take the decision of deploying an IDS while only 7% of the participants decided not to deploy an IDS. The rest 25% mentioned that they are not in a position to take the decision of deploying an IDS or not but they decided to accomplish the questionnaire based on there opinions and other experiences in the field.

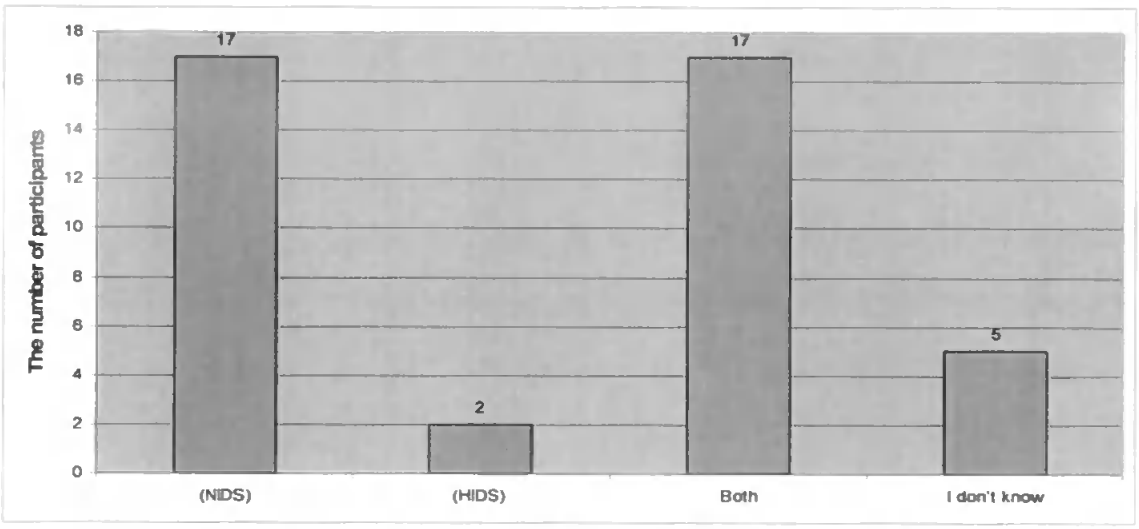


Figure 6: The type of IDS that the participant's prefer to deploy

Figure 6 represents the type of IDS that the participant prefers to deploy. It is obvious from the results, that if the participants have to select only between (NIDS) and (HIDS), they would select (NIDS), since 41.5% of the participants selected (NIDS) while only 5% selected (HIDS). While 41.5% of the participants decided that they prefer to use both of them. Finally, only 12% participants selected the answer "I do not know". The entire results indicate that 83% of the participants are using NIDS and 46.5% are using HIDS. Hence, the participants decided that NIDS have more privilege verses the HIDS in the real world but they still want to provide their systems with the privileges of the HIDS.

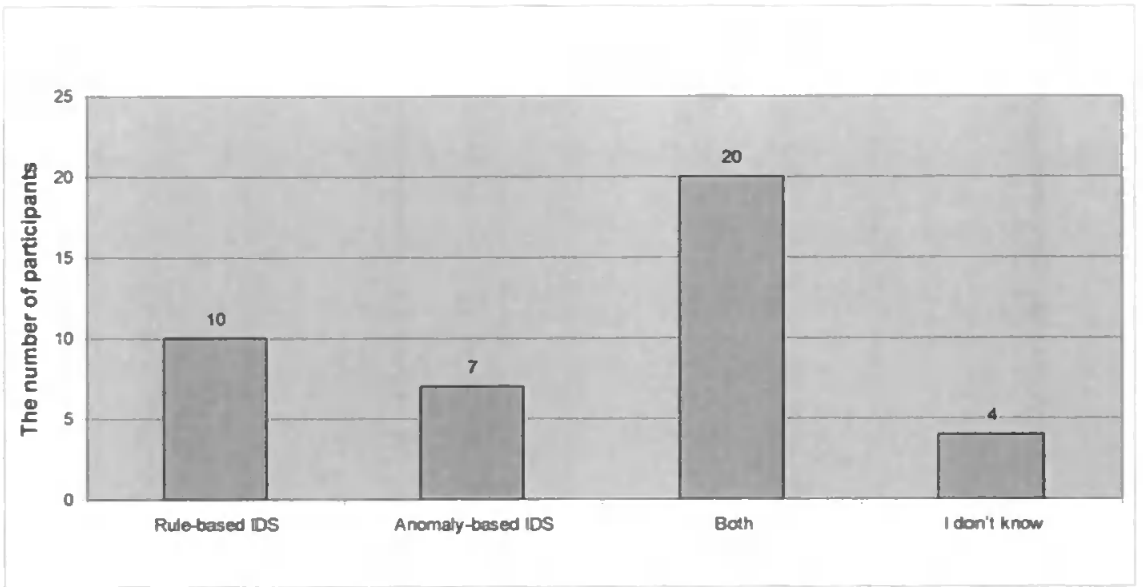


Figure 7: The approach that the participant's use in detecting intrusions

Figure 7 represents the approach that the participant uses in detecting intrusions. The result determines that 25% of the participants prefer to use rule-based IDS while only 17% prefer to use anomaly-based IDS but it was obvious that a large number of participants 49% prefer to use both of them. Finally, only 10% participants selected the answer "I do not know". The entire results indicate that 74% of the participants prefer to use rule-based IDS and 65% prefer to use anomaly-based IDS. Hence, the participants decided that rule-based IDS have more privilege verses the anomaly-based in the real world but they still want to provide their systems with the privileges of the anomaly-based. It is not surprising to find in Figure 6 and Figure 7 there are 5 and 4 persons respectively that answer "I don't know" because a group of participants are categorized as able to offer opinion about IDS challenges. Hence, it is not strange that some of the users do not know what type of IDS is used in detecting intrusions.

4.3.2 Deployment Challenges

The deployment challenges section is the first one of the five sections of the IDS challenges. The purpose of these sections is to focus on the core of the questionnaire and to measure the

participant's degree of agreement about the challenges that will be applied to them through the questions.

Figure 8 represents the deployment challenges that are investigated by the questionnaire. Moreover, each one of them was appended with a brief description to avoid misinterpretation. Furthermore, this methodology is applied to the rest of the challenges in Section B.

Figure 8: Deployment Challenges

The deployment challenges that were investigated are as follows:

- Scalability constraints,
- Switched Networks,
- Packet dropping and high speed network traffic,
- Encrypted traffic and IPv6, and
- Initial deployment cost.

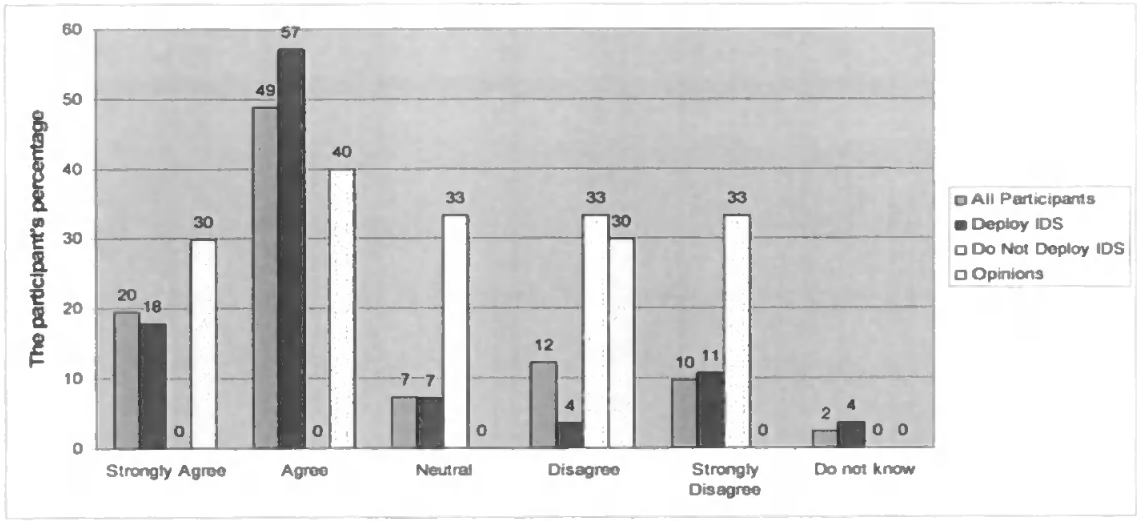


Figure 9: Scalability constraints challenge

The asked question was Scalability constraints: The size of the network can affect the efficiency of the IDS. For instance, as the size of the network increases, the efficiency of signature-based IDS decreases. The participant's responses to the scalability constraints challenge is shown in Figure 9. It was anticipated during the design period of the questionnaire that the percentage of the participants who will agree would be higher and the percentage of the participants who will disagree would be much less. Actually, this anticipation is not only for this challenge but also for all the challenges in the rest of the questionnaire. Meanwhile, the percentage of the passive participants was not very strange. Therefore, there was a requirement for a having a look at the results in depth. Hence, it was decided to analyze the responses according to the participant's role in their organizations. It was found that 100% of the systems administrators agree, 67% of the system analysts agree while 33% did not, 17% only of the security engineers agree and 33% were passive while 50% did not agree, 75% of the intrusion analysts agree and 25% were passive and 100% security administrator agrees. Moreover, the responses of the other participants vary as well, hence, it was decided to do further analysis on the basis's of the results according to their experience (i.e. participants with more than 10 years

of experience), there results were 66% agree and 17% were neutral while 17% did not agree. Moreover, it is decided to follow the same strategy of analysis with the following challenges.

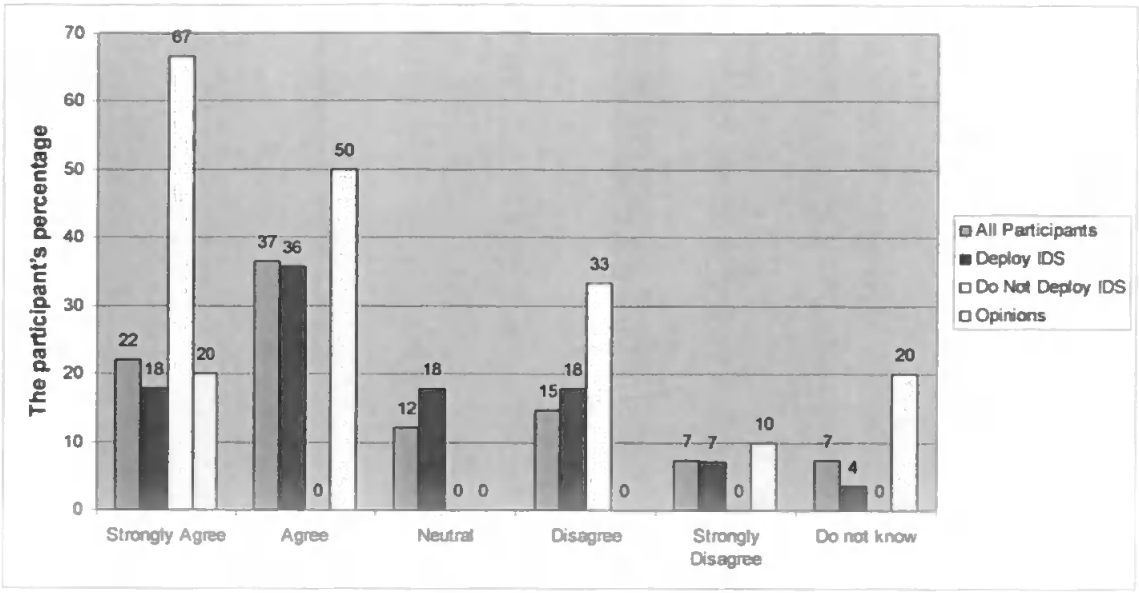


Figure 10: Switched networks challenge

The asked question was Switched Networks: In the presence of switching technology, monitoring the network efficiently requires the deployment of more IDS to inspect the several network segments traffic. The participant's responses to the switched networks challenge is shown in Figure 10. It was found that 100% of the systems administrators agree, 67% of the system analysts agree and 33% were passive, 67% of the security engineers agree and 17% were passive while 16% did not agree, 75% of the intrusion analysts agree and 25% were passive and 100% security administrator did not agree. Moreover, the responses of the participants with more than 10 years of experience results were 66% agree and 17% were neutral while 17% did not agree. The latter results are more acceptable to the questionnaire than the general participant's responses (59%) all participants results.

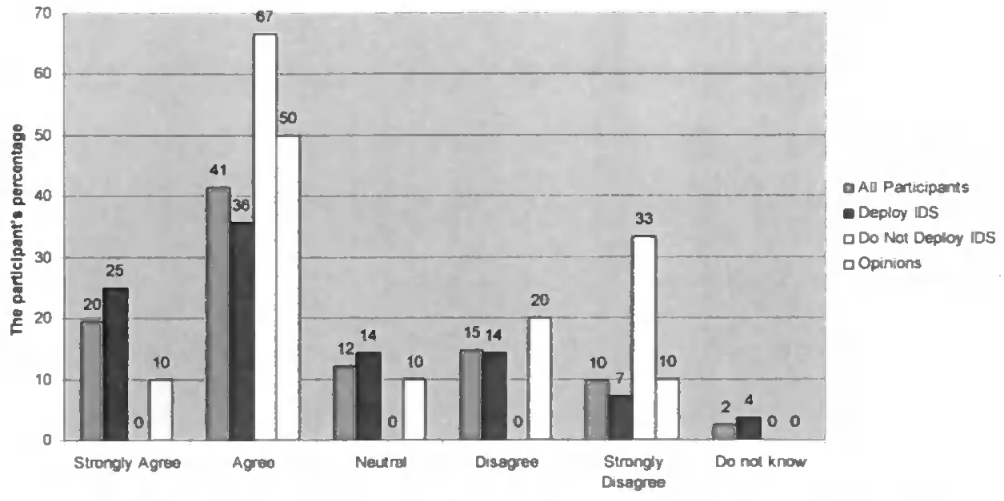


Figure 11: Packet dropping and high speed network traffic challenge

The asked question was Packet dropping and high speed network traffic: The high speed of network traffic combined with the information overload can cause packet dropping. Therefore, the probability of missing attacks increases. The participant's response to the packet dropping and high speed network traffic challenge is shown in Figure 11. It was found that 100% of the systems administrators were passive, 33% only of the system analysts agree while 67% did not agree, 83% of the security engineers agree while 17% did not agree, 50% of the intrusion analysts agree and 25% were passive while 25% did not agree and 100% security administrator did not agree. Moreover, the responses of the participants with more than 10 years of experience results were 50% agree and 17% were neutral while 33% did not agree.

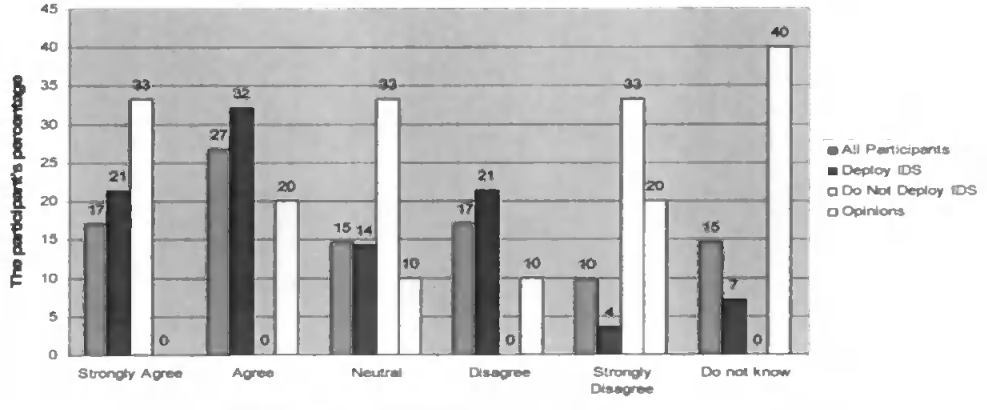


Figure 12: Encrypted traffic and IPv6 challenge

The asked question was Encrypted traffic and IPv6: Encrypted traffic attacks successfully reach the destination without being monitored by IDS. Encrypted traffic and IPv6 are combined together in the same question because IPv6 are encrypted. The participant's response to the encrypted traffic and IPv6 challenge is shown in Figure 12. It was found that 50% of the systems administrators agree while 50% did not agree, 67% of the system analysts were passive while 33% did not agree, 50% of the security engineers agree and 17% were passive while 33% did not agree, 25% only of the intrusion analysts agree and 50% were passive while 25% did not agree and 100% of the security administrators agree. Moreover, the responses of the participants with more than 10 years of experience results were 34% agree and 33% were neutral while 33% did not agree.

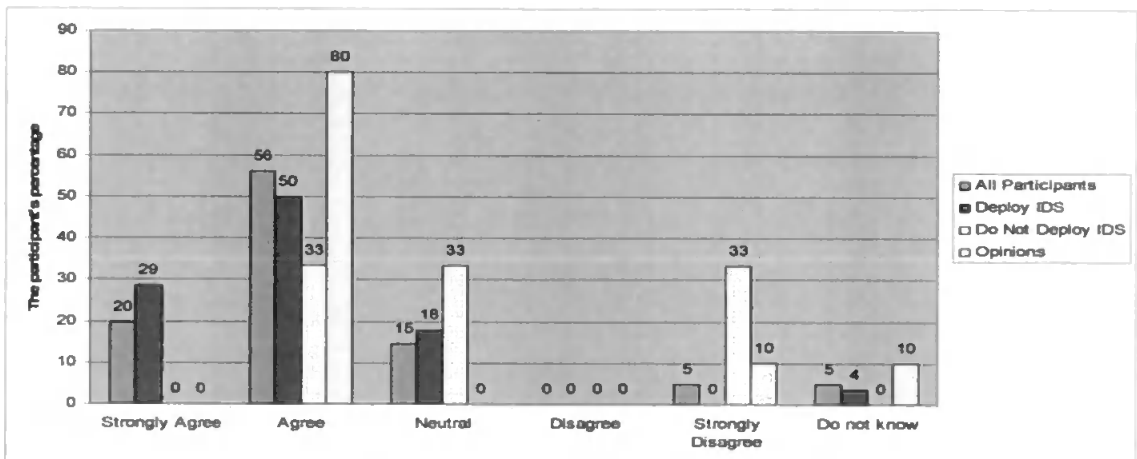


Figure 13: Initial deployment cost challenge

The asked question was Initial deployment cost: Deployment costs may include the cost of purchasing the IDS and the initial training for those who will be responsible for managing it. The participant's response to the initial deployment cost challenge is shown in Figure 13. It was found that 100% of the systems administrators agree, 67% of the system analysts agree while 33% did not agree, 83% of the security engineers agree and 17% were passive, 75% of the intrusion analysts agree and 25% were passive and 100% of the security administrators

agree. Moreover, the responses of the participants with more than 10 years of experience results were 83% agree while 17% did not agree. The latter results are more acceptable to the questionnaire than the general participant's responses (76%) all participants results.

4.3.3 Management Challenges

The management challenges that are investigated by the questionnaire are represented in Figure 14. The management challenges investigated were as follows:

- Volume of information,
- Ensuring effective configuration,
- Managing a heterogeneous IDS environment, and
- Ongoing operational costs.

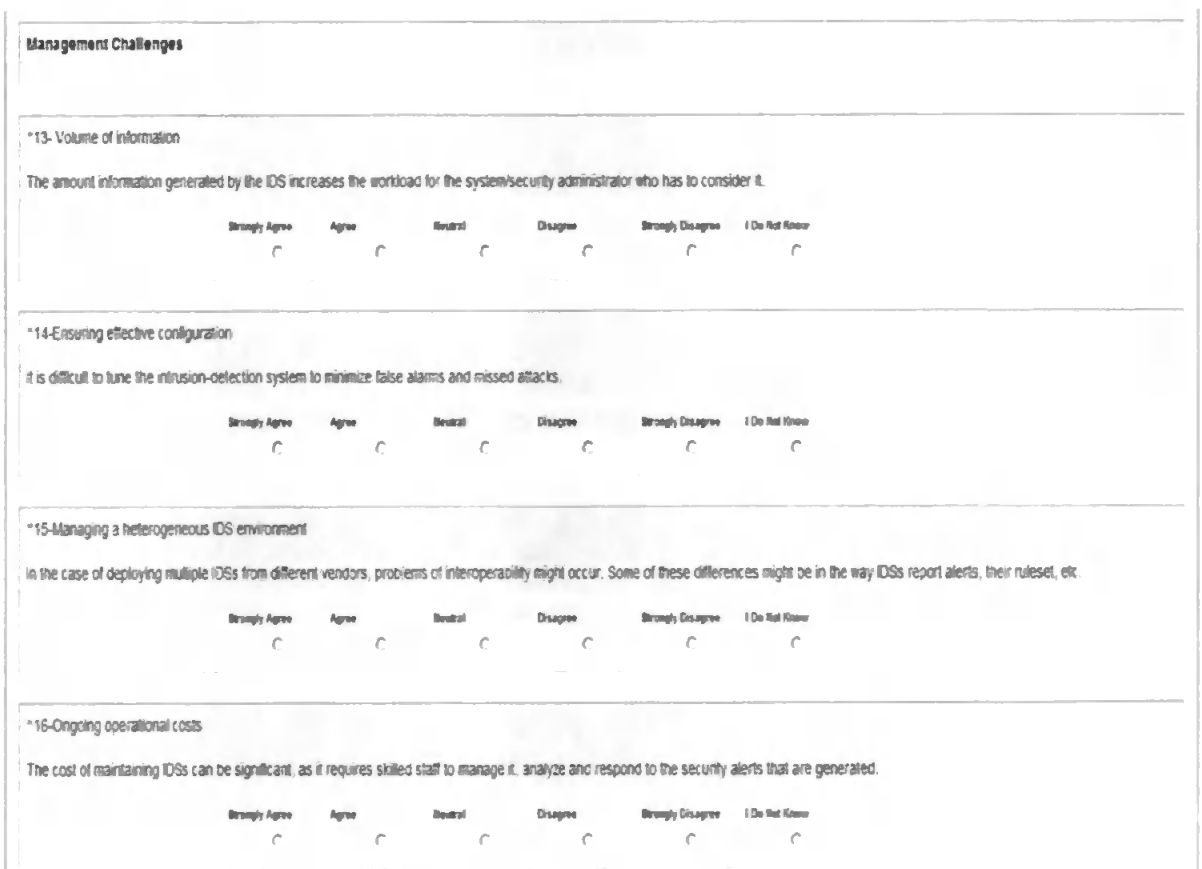


Figure 14: Management Challenges

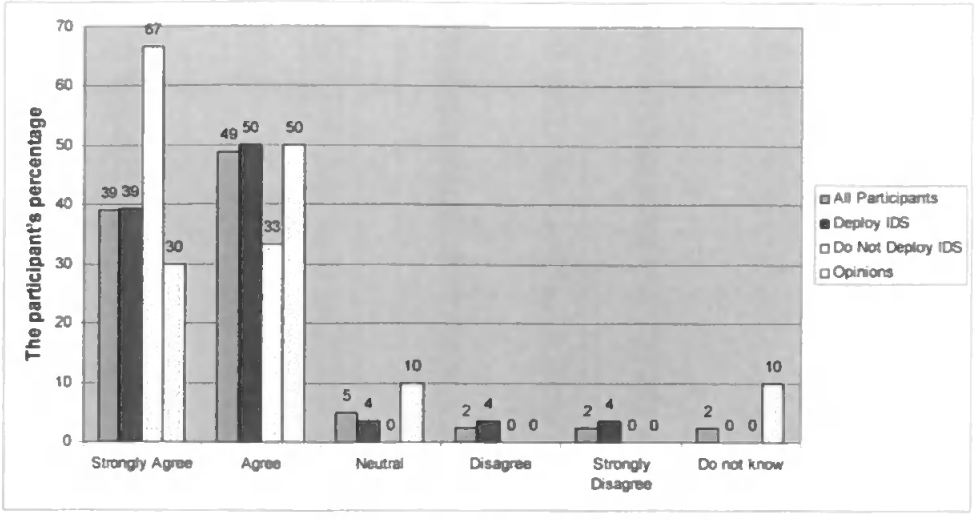


Figure 15: Volume of information challenge

The asked question was Volume of information: The amount information generated by the IDS increases the workload for the system/security administrator who has to consider it. The participant's response to the volume of information challenge is shown in Figure 15. It was found that 100% of the systems administrators agree, 100% of the system analysts agree, 100% of the security engineers agree, 75% of the intrusion analysts agree while 25% did not agree and 100% of the security administrators did not agree. Moreover, the responses of the participants with more than 10 years of experience results were 83% agree and 17% were neutral.

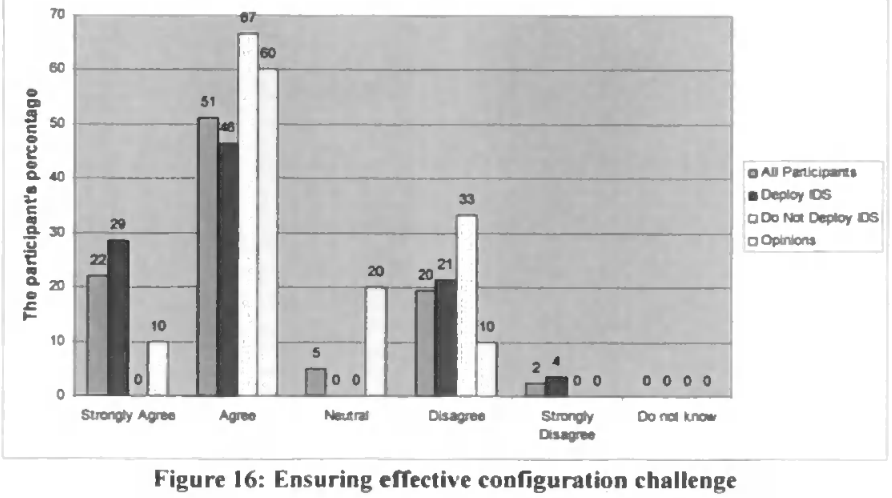


Figure 16: Ensuring effective configuration challenge

The asked question was Ensuring effective configuration: It is difficult to tune the intrusion-detection system to minimize false alarms and missed attacks. The participant's response to the ensuring effective configuration challenge is shown in Figure 16. It was found that 50% of the systems administrators agree while 50% did not agree , 33% only of the system analysts agree while 67% did not agree, 83% of the security engineers agree while 17% did not agree, 75% of the intrusion analysts agree while 25% did not agree and 100% of the security administrators agree. Moreover, the responses of the participants with more than 10 years of experience results were 50% agree while 50% did not agree.

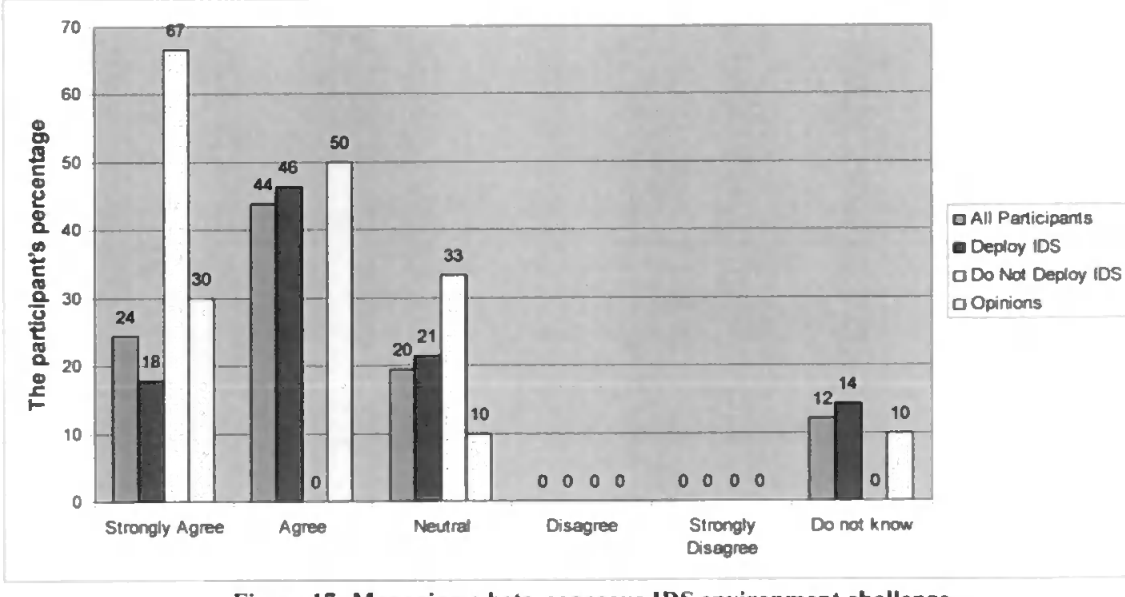


Figure 17: Managing a heterogeneous IDS environment challenge

The asked question was Managing a heterogeneous IDS environment: In the case of deploying multiple IDSs from different vendors, problems of interoperability might occur. Some of these differences might be in the way IDSs report alerts, their ruleset, etc. The participant's response to the managing a heterogeneous IDS environment challenge is shown in Figure 17. It was found that 50% of the systems administrators agree and 50% were neutral, 67% of the system analysts agree and 33% were passive, 67% of the security engineers agree

and 33% were neutral, 75% of the intrusion analysts agree and 25% were neutral and 100% of the security administrators agree. Moreover, the responses of the participants with more than 10 years of experience results were 50% agree and 50% were passive. Therefore, the analysis will consider managing a heterogeneous IDS environment as a challenge.

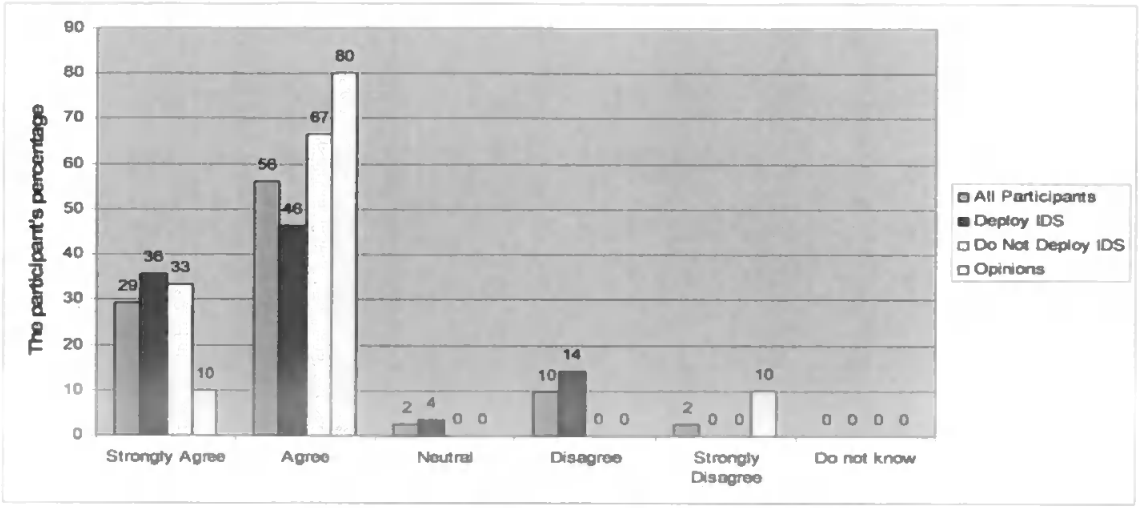


Figure 18: Ongoing operational costs challenge

The asked question was Ongoing operational costs: The cost of maintaining IDSs can be significant, as it requires skilled staff to manage it, analyze and respond to the security alerts that are generated. The participant's response to the ongoing operational costs challenge is shown in Figure 18. It was found that 100% of the systems administrators did not agree, 100% of the system analysts agree, 83% of the security engineers agree while 17% did not agree, 75% of the intrusion analysts agree and 25% were neutral and 100% of the security administrators did not agree. Moreover, the responses of the participants with more than 10 years of experience results were 83% agree while 17% did not agree.

4.3.4 Technical Challenges

The technical challenges that are investigated by the questionnaire are represented in Figure 19. The technical challenges that were investigated are as follows:

- Vulnerability to attacks,

- Difficulty in customizing and updating the IDS ruleset,
- Data collection and logging, and
- Understanding and interpreting IDS data.

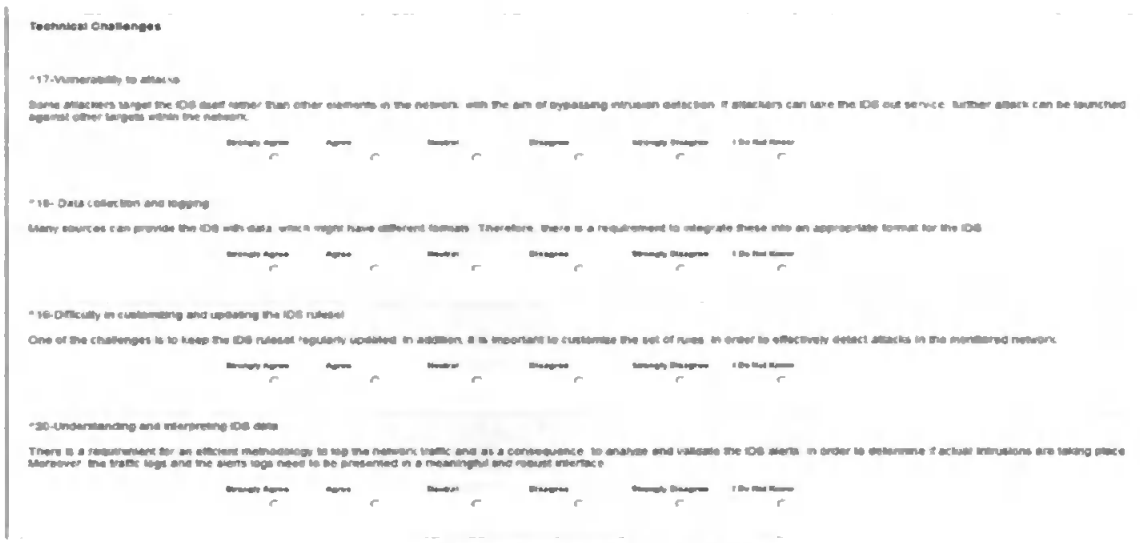


Figure 19: Technical Challenges

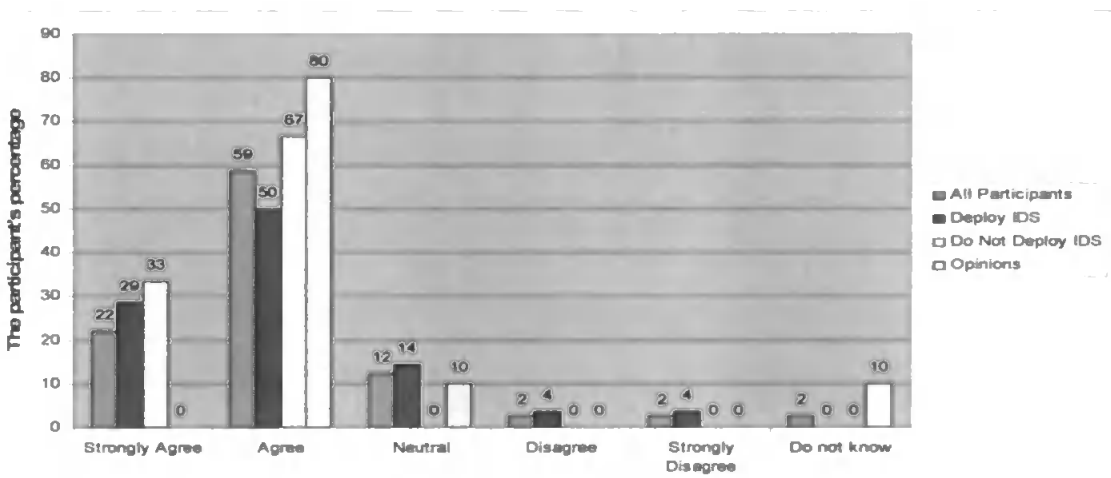


Figure 20: Vulnerability to attacks challenge

The asked question was Vulnerability to attacks: Some attackers target the IDS itself rather than other elements in the network, with the aim of bypassing intrusion detection. If attackers can take the IDS out service, further attack can be launched against other targets

within the network. The participant's response to the vulnerability to attacks challenge is shown in Figure 20. It was found that 100% of the systems administrators agree, 100% of the system analysts agree, 83% of the security engineers agree and 17% were neutral, 100% of the intrusion analysts agree and 100% of the security administrators did not agree. Moreover, the responses of the participants with more than 10 years of experience results were 83% agree and 17% were neutral. The latter results support the (81%) the all participant's responses. Therefore, the analysis will consider vulnerability to attacks as a challenge.

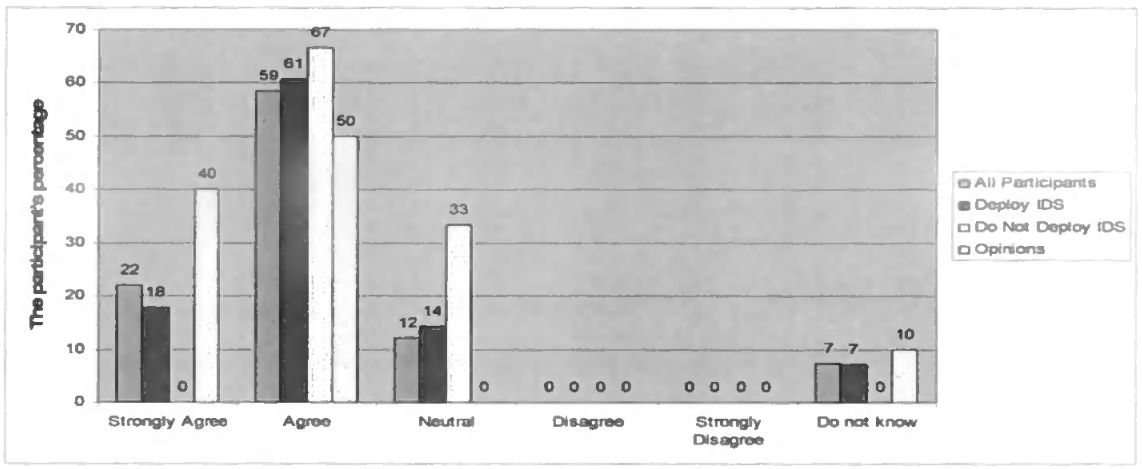


Figure 21: Difficulty in customizing and updating the IDS ruleset challenge

The asked question was Difficulty in customizing and updating the IDS ruleset: One of the challenges is to keep the IDS ruleset regularly updated. In addition, it is important to customize the set of rules, in order to effectively detect attacks in the monitored network. The participant's response to the difficulty in customizing and updating the IDS ruleset is shown in Figure 21. 0% of the participants selected any of the disagree options. It was found that 100% of the systems administrators agree, 100% of the system analysts agree, 67% of the security engineers agree and 33% were neutral, 100% of the intrusion analysts agree and 100% of the security administrators were neutral. Moreover, the responses of the participants with more than 10 years of experience results were 100% agree. The latter results support the (81%)

the all participant's responses. Therefore, the analysis will consider the difficulty in customizing and updating the IDS ruleset as one of the top challenges.

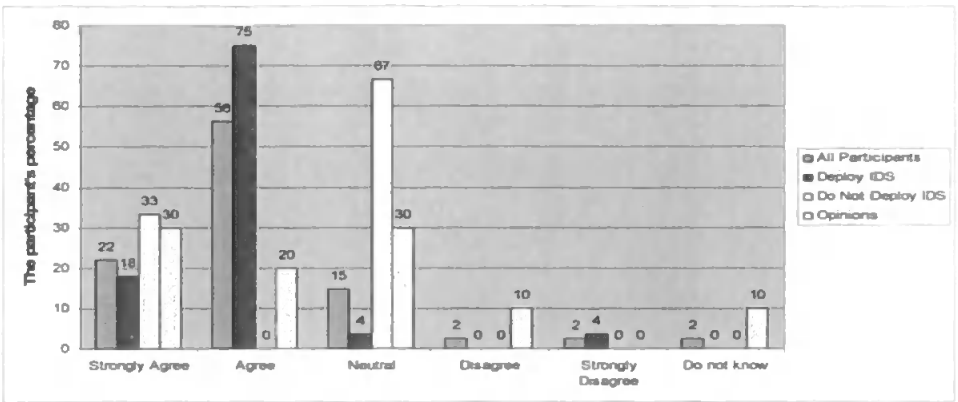


Figure 22: Data collection and logging challenge

The asked question was Data collection and logging: Many sources can provide the IDS with data, which might have different formats. Therefore, there is a requirement to integrate these into an appropriate format for the IDS. The participant's response to the data collection and logging is shown in Figure 22.It was found that 50% of the systems administrators agree while 50% did not agree, 100% of the system analysts agree, 50% of the security engineers agree and 33% were neutral while 17% did not agree, 100% of the intrusion analysts agree and 100% of the security administrators agree. Moreover, the responses of the participants with more than 10 years of experience results were 66% agree and 17% were neutral while 17% do not agree.

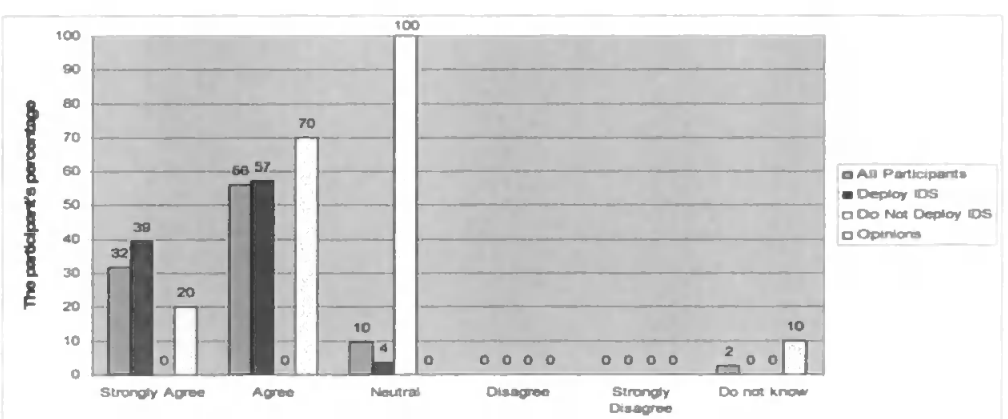


Figure 23: Understanding and interpreting IDS data challenge

The asked question was Understanding and interpreting IDS data: There is a requirement for an efficient methodology to log the network traffic and as a consequence, to analyze and validate the IDS alerts, in order to determine if actual intrusions are taking place. Moreover, the traffic logs and the alerts logs need to be presented in a meaningful and robust interface. The participant's response to the understanding and interpreting IDS data is shown in Figure 23. It was found that 100% of the systems administrators agree, 67% of the system analysts agree and 33% were neutral, 67% of the security engineers agree and 33% were neutral, 100% of the intrusion analysts agree and 100% of the security administrators agree. Moreover, the responses of the participants with more than 10 years of experience results were 100% agree. The latter results support the (88%) the all participant's responses Therefore, the analysis will consider understanding and interpreting IDS data as one of the top challenges.

4.3.5 Detection Challenges

The detection challenges that are investigated by the questionnaire are represented in Figure 24. The detection challenges that were investigated are as follows:

- The large number of alerts,
- IDS can miss too many genuine attacks (i.e. false negatives),
- IDS can raise too many erroneous alerts (i.e. false positives),
- Determining the alert severity level, and
- Alerts correlation.

Figure 24: Detection Challenges

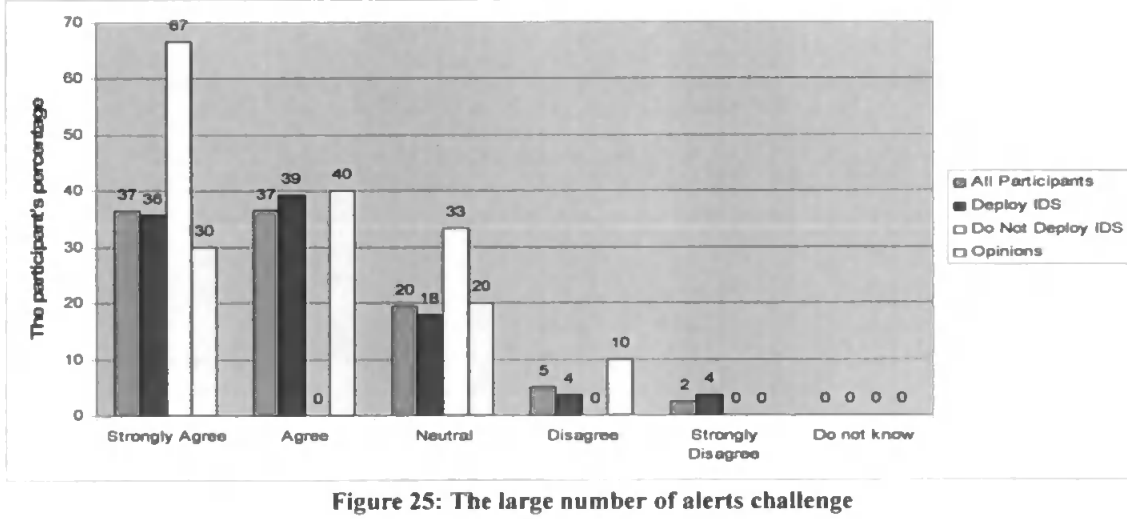


Figure 25: The large number of alerts challenge

The asked question was The large number of alerts: IDS can produce a large number of alerts and can therefore require significant effort to monitor. The participant's response to the large number of alerts is shown in Figure 25. It was found that 50% of the systems administrators are neutral while 50% did not agree, 67% of the system analysts agree and 33% were neutral, 67% of the security engineers agree and 17% were neutral while 16% did not

agree, 75% of the intrusion analysts agree and 25% were neutral, and 100% of the security administrators are neutral. Moreover, the responses of the participants with more than 10 years of experience results were 50% agree and 33% were neutral while 17% do not agree.

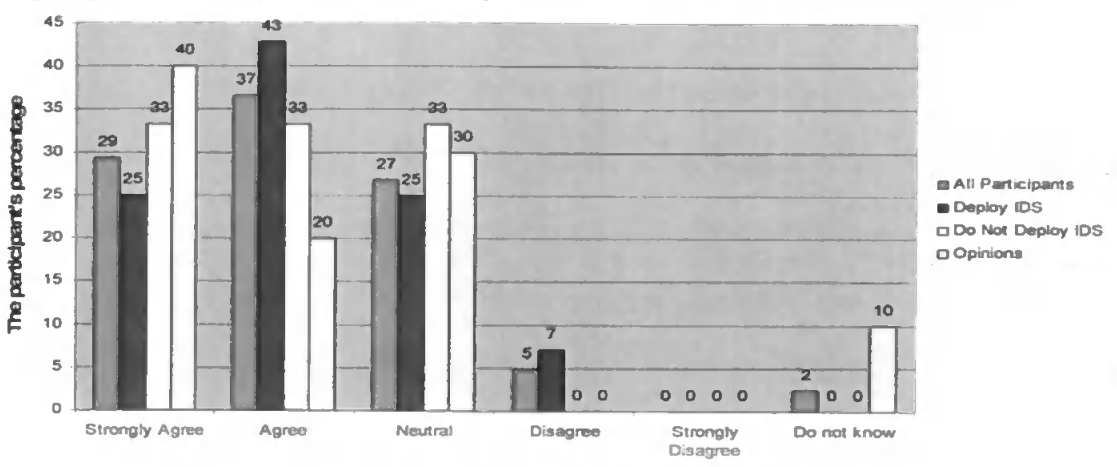


Figure 26: False negatives challenge

The asked question was IDS can miss too many genuine attacks (i.e. false negatives): A false negative occurs when the IDS fails to detect malicious network traffic, which as a result goes undetected. The participant's response to the false negatives is shown in Figure 26. It was found that 50% of the systems administrators agree while 50% did not agree, 67% of the system analysts agree and 33% were neutral, 83% of the security engineers agree and 17% were neutral, 100% of the intrusion analysts agree, and 100% of the security administrators are neutral. Moreover, the responses of the participants with more than 10 years of experience results were 33% agree and 50% were neutral while 17% did not agree.

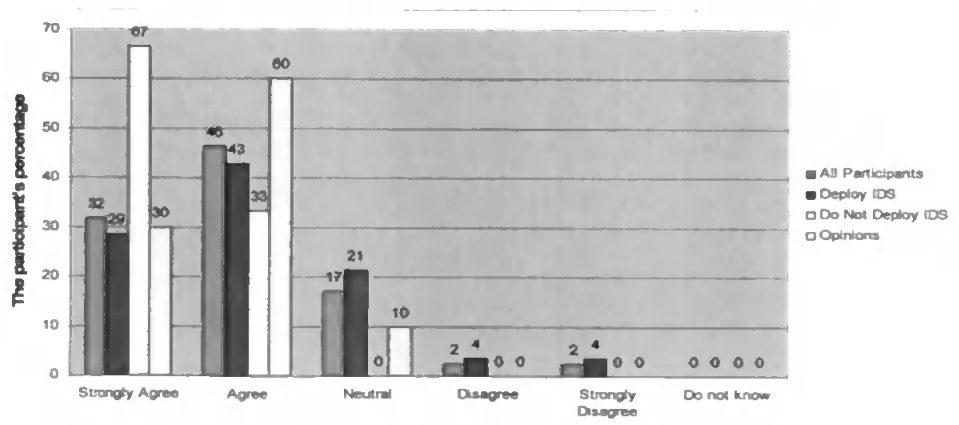


Figure 27: False positives challenge

The asked question was IDS can raise too many erroneous alerts (i.e. false positives): A false positive refers to the network traffic that the IDS considers malicious but are not. The participant's response to the false positives is shown in Figure 27.It was found that 50% of the systems administrators agree and 50% were neutral, 67% of the system analysts agree and 33% were neutral, 67% of the security engineers agree and 33% were neutral, 100% of the intrusion analysts agree, and 100% of the security administrators are neutral. Moreover, the responses of the participants with more than 10 years of experience results were 33% agree and 50% were neutral while 17% did not agree.

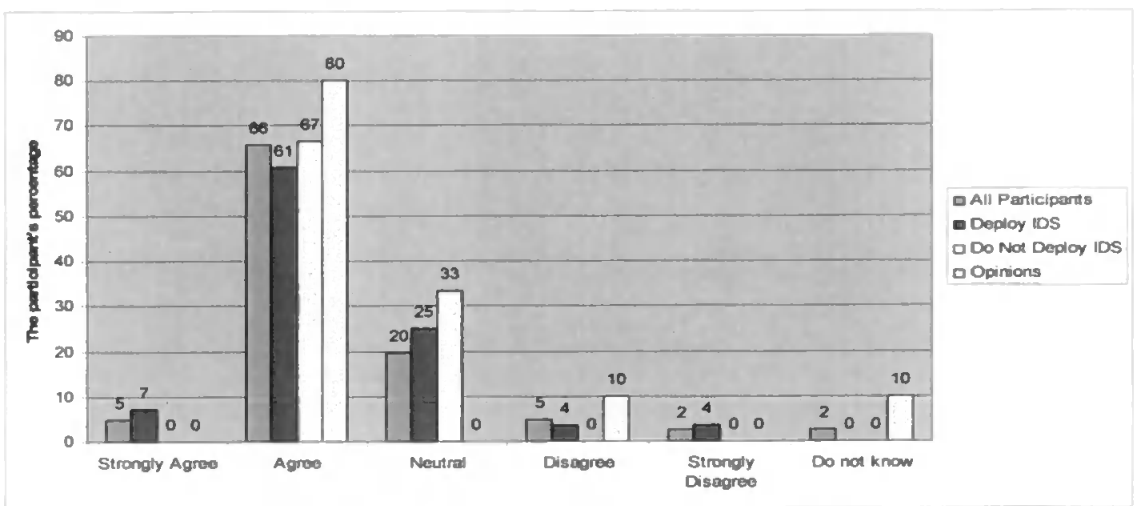


Figure 28: Determining the alert severity level challenge

The asked question was Determining the alert severity level: There are no standard metrics for the alert severity level. Therefore, a combination of organization security policy and security operator experience is required in order to interpret and rank/prioritize the generated alerts. The participant's response to determining the alert severity level is shown in Figure 28. It was found that 100% of the systems administrators agree, 100% of the system analysts agree, 67% of the security engineers agree and 17% were neutral while 16% did not agree, 50% of the intrusion analysts agree and 50% were neutral, and 100% of the security

administrators agree. Moreover, the responses of the participants with more than 10 years of experience results were 50% agree and 17% were neutral while 33% did not agree.

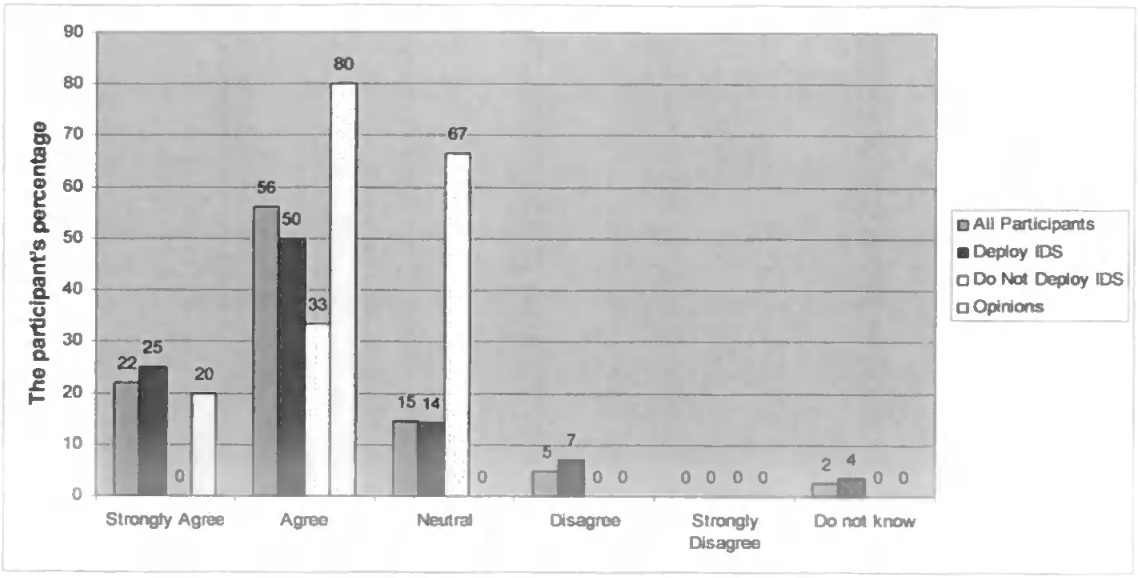


Figure 29: Alerts correlation challenge

The asked question was Alerts correlation: There is a requirement to study the relationship between the various IDS alerts to determine the occurrence of the attack scenarios. Hence, the alert correlation process is not trivial, and is often not without problems. The participant's response to the alerts correlation is shown in Figure 29. It was found that 100% of the systems administrators agree, 33% of the system analysts agree and 67% were passive, 83% of the security engineers agree and 17% did not agree, 75% of the intrusion analysts agree and 25% were neutral, and 100% of the security administrators are neutral. Moreover, the responses of the participants with more than 10 years of experience results were 66% agree and 17% were passive while 17% did not agree.

4.3.6 Response Challenges

The response challenges that are investigated by the questionnaire are represented in Figure 30 represents. The response challenges which were investigated are as follows:

- Requirement for skilled staff,
- The potential for inappropriate and harmful responses, and
- Effectiveness of the IDS response.

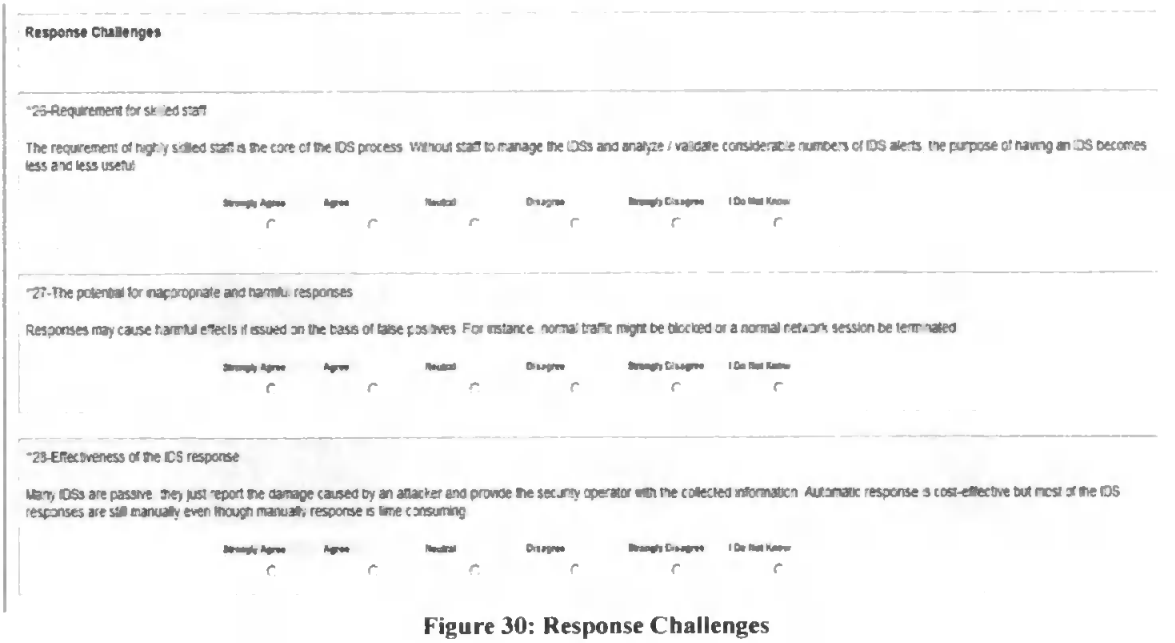


Figure 30: Response Challenges

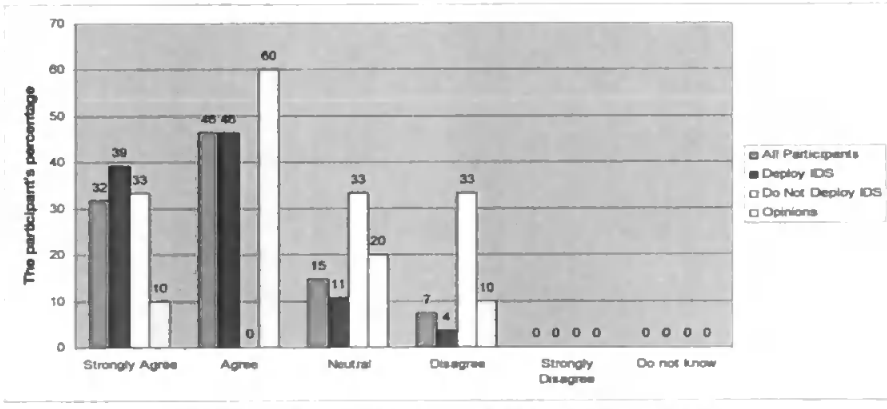


Figure 31: Requirement for skilled staff challenge

The asked question was Requirement for skilled staff: The requirement of highly skilled staff is the core of the IDS process. Without staff to manage the IDSs and analyze / validate considerable numbers of IDS alerts, the purpose of having an IDS becomes less and less useful. The participant's response to the requirement for skilled staff is shown in Figure 31. It was found that 100% of the systems administrators agree, 100% of the system analysts agree,

50% of the security engineers agree and 17% were neutral while 33% did not agree, 75% of the intrusion analysts agree and 25% were neutral, and 100% of the security administrators are neutral. Moreover, the responses of the participants with more than 10 years of experience results were 83% agree while 17% did not agree. The latter results support the (78%) the all participant's response.

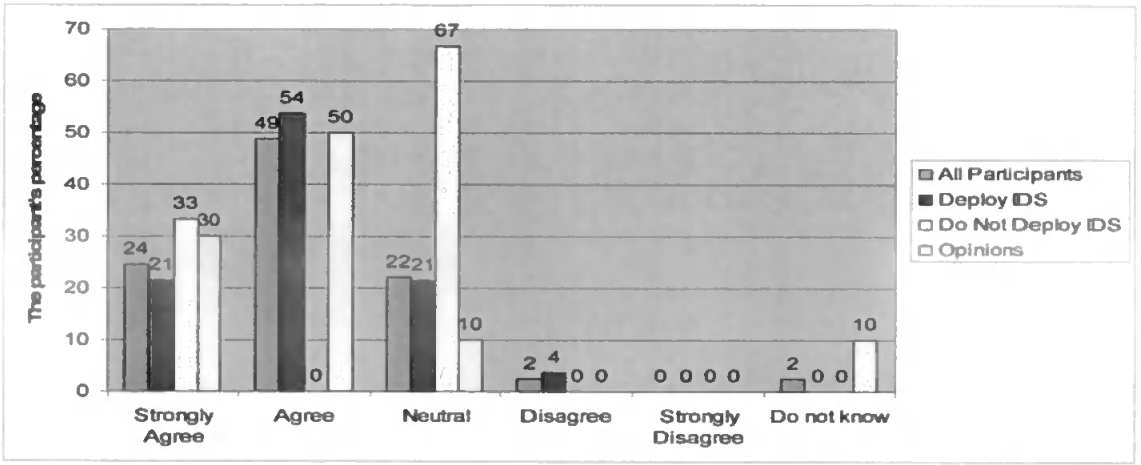


Figure 32: The potential for inappropriate and harmful responses challenge

The asked question was The potential for inappropriate and harmful responses: Responses may cause harmful effects if issued on the basis of false positives. For instance, normal traffic might be blocked or a normal network session be terminated. The participant's response to the potential for inappropriate and harmful responses is shown in Figure 32. It was found that 50% of the systems administrators were neutral while 50% did not agree, 33% of the system analysts agree and 67% were neutral, 83% of the security engineers agree and 17% were neutral, 100% of the intrusion analysts agree, and 100% of the security administrators agree. Moreover, the responses of the participants with more than 10 years of experience results were 83% agree and 17% were neutral. The latter results support the (73%) the all participants' responses.

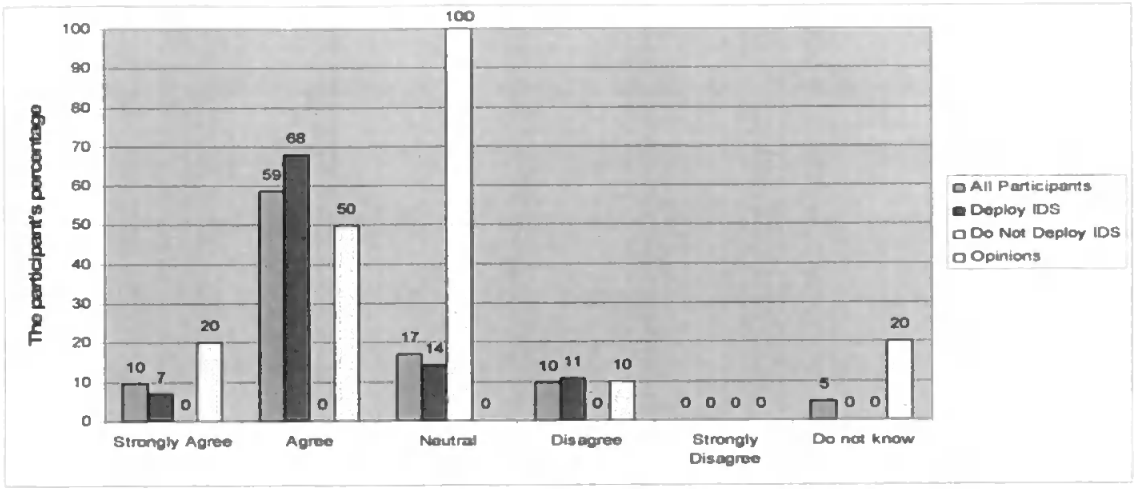


Figure 33: Effectiveness of the IDS response challenge

The asked question was Effectiveness of the IDS response: Many IDSs are passive, they just report the damage caused by an attacker and provide the security operator with the collected information. Automatic response is cost-effective but most of the IDS responses are still manually even though manually response is time consuming. The participant's response to effectiveness of the IDS response is shown in Figure 33. It was found that 100% of the systems administrators agree, 33% of the system analysts agree and 67% were neutral, 50% of the security engineers agree and 33% were neutral while 17% did not agree, 100% of the intrusion analysts agree, and 100% of the security administrators were neutral. Moreover, the responses of the participants with more than 10 years of experience results were 66% agree and 17% were neutral while 17% did not agree.

4.3.7 The Challenges Rate

The current results of the questionnaire are sufficient to mention that all the composed challenges (i.e. the selection of the challenges within the questionnaire which were based originally on the academic published papers) are challenges that encounter practitioners in their organizations in reality. Hence, there is a requirement to rank these challenges based on various criteria. Therefore, the results in the previous sub-sections (4.3.2-4.3.6) will be the bases for the

various methods which will be described among the current sub-section and the rest of the chapter.

In order to provide a clear view, of the participants answers and to summarize some of the provided results, Figure 34 represents the challenges that the participants were strongly agree with, the figure clarifies that 39% of the participants strongly agree that the volume of information is a major challenge which implies the difficulty in the process of manipulating with them. Therefore, as a result it was obvious that the large number of alerts challenge appears as the second challenge that the participants strongly agree with. Moreover, the answers of the questions in the previous sub-sections (4.3.2-4.3.6) reveal that some of the challenges are considered to be a very serious challenge to at least some of the participants while others were not very significant such as determining the alert severity level, and the effectiveness of IDS response. However, Figure 34 gives an overall view, in percentages, of the challenges that were selected by the strongly agree option.

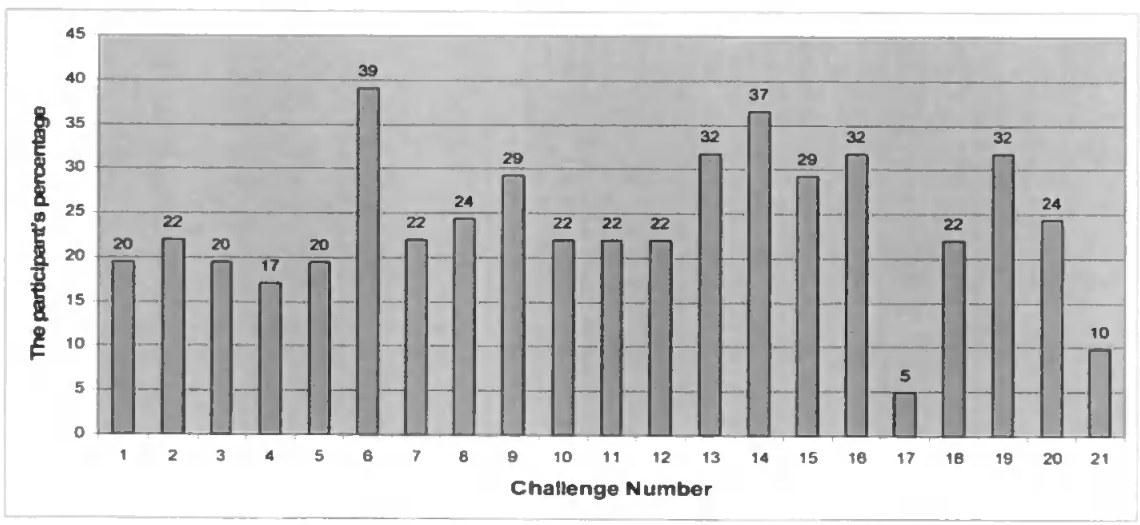


Figure 34: Challenges that participant "Strongly Agree"

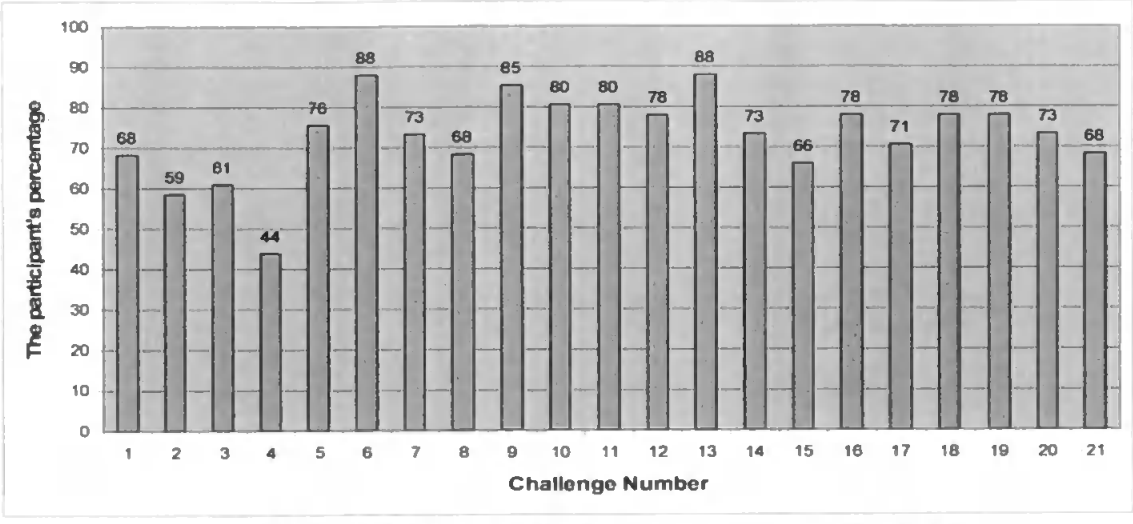


Figure 35: Challenges that participant "Agree" + "Strongly Agree"

Another method was adopted to have the advantage of the responses of the participants who only agree and their agreement was not a strongly agreement. Hence, it was decided to sum the results of the participants who only agree and those who strongly agree, as variant method to rank all the challenges. In contrast to the previous method, Figure 35 illustrated that the volume of information is still the challenge with the highest agreement while understanding and interpreting IDS data moved upwards to share the same level with 88% of agreement while it was in the third level in the previous method. Furthermore, the encrypted traffic and IPv6 moves downwards to be considered the less sever challenge. For the completeness of this demonstration, it worth to mention that the percentage of agreement for the two challenges which were considered to be the less severe ones in the previous method have raised significantly as can be shown from Figure 34 and Figure 35.

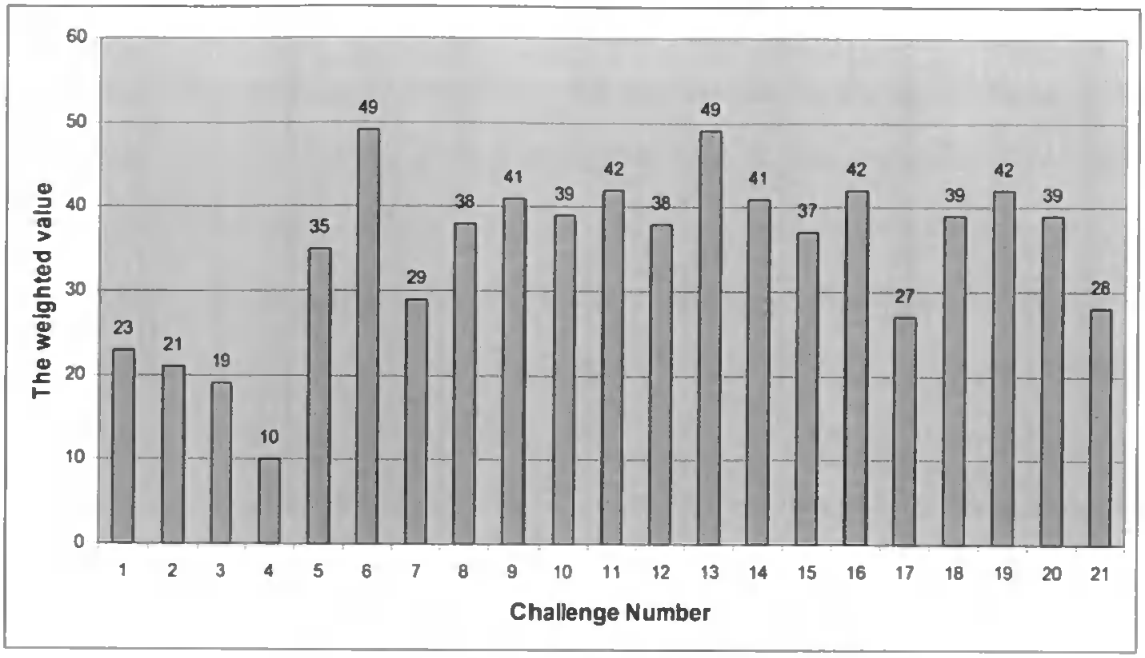


Figure 36: The positives and negatives weighted method

The previous two methods focused only on the positive responses but the negative results were not considered. However, these negative should be considered in ranking the challenges and their impact on the overall severity of the challenges. Therefore, Figure 36 represents a weighting method which combines the positive and the negative responses that will be implemented. The weighting method is a simple and will be applied by giving the value 2 to the "Strongly Agree", the value 1 to "Agree", the value (-1) to "Disagree" and the value (-2) to the "Strongly Disagree", while the value of "Neutral" and "I do not Know" will be zero. As shown in Figure 35 and Figure 36, the main aspects of the two methods are almost the same. The complete findings of the previous three methods are presented in Appendix A.1-Table A.

The previous three methods of ranking were based only on the answers of the questions in the previous sub-sections (4.3.2-4.3.6) (i.e. the responses to the already prepared list of IDS challenge). Therefore, it was decided to give the opportunity to the participants to add other challenges that might were absent or ignored in the questionnaire and worth to be mentioned in the survey. Hence, the question that was appended to give more freedom to the participants to

add any further challenges. Unfortunately, a few participants respond to that question (for more information have a look at Appendix A.2), may be one of the reasons is that the question was optional.

Figure 37 represents the construction of the question which was given to the participants to select the five Top challenges of the challenges which were mentioned in the previous sub-sections (4.3.2- 4.3.6). The purpose of the question is to rank severity of these challenges from the participant's perspective. The list of the questionnaire challenges which were repented at the beginning of this sub-section will appear to the participants as a drop down list:

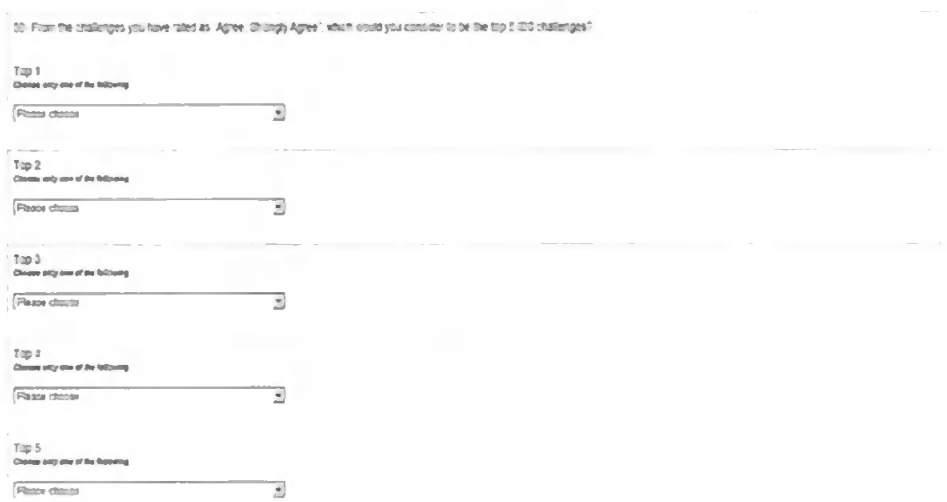


Figure 37: The top five challenges ranking question

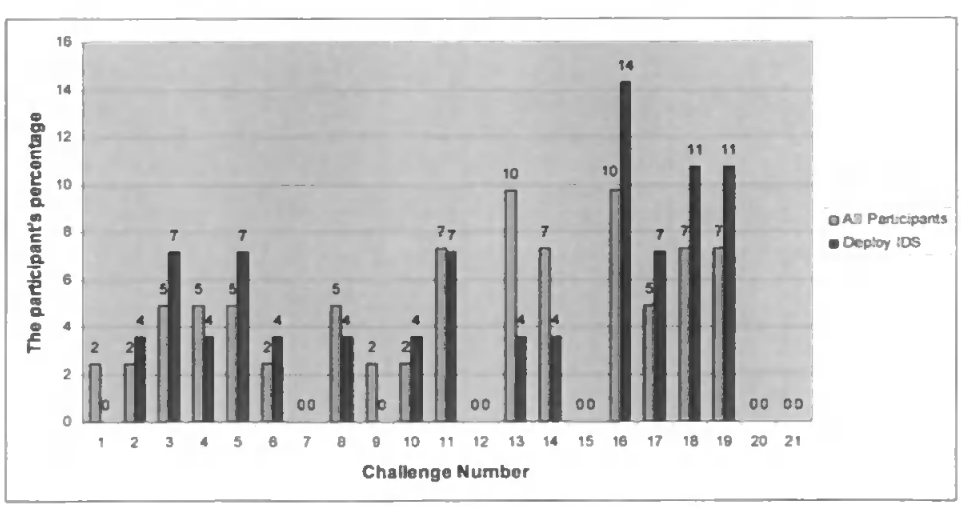


Figure 38: The highest rank Challenge

Figure 38 illustrated not only the responses of all the participants but also the participants who deploy IDS. Hence, the highest rank of the challenges which the whole participants selected as the Top 1 challenge is as follows.

- Understanding and interpreting IDS data, 88% of the whole participants selected it as a challenge and 12% were passive. Meanwhile, the responses of the participants with more than 10 years of experience results were 100% agree that it is a challenge.

- IDS can raise too many erroneous alerts (i.e. false positives), 78% of the whole participants selected it as a challenge and 17% were neutral. Meanwhile, the responses of the participants with more than 10 years of experience results were 33% agree and 50% were neutral while 17% did not agree.

It is obvious from Figure 38 that some of the challenges were not selected at all as the first selection. Hence, the current assumption is that these challenges might appear in the Top 2 challenge selections. However the ones that were not selected in the current stage are the following challenges:

- Ensuring effective configuration,
- Data collection and logging,
- IDS can miss too many genuine attacks (i.e. false negatives),
- The potential for inappropriate and harmful responses, and
- Effectiveness of the IDS response.

The results of the Top 2 Challenge question demonstrated that the highest selection went towards:

- Requirement for skilled staff, 78% of the whole participants selected it as a challenge and 15% were neutral. Meanwhile, the responses of the participants with more than 10 years of experience results were 83% agree while 17% did not agree.

Even that some of the challenges that were not selected in the Top 1 challenge are currently selected in the Top 2 challenge question but the following challenges are still not selected by any of the participants:

- Ensuring effective configuration,
- The potential for inappropriate and harmful responses, and
- Effectiveness of the IDS response.

The results of the Top 3 Challenge question demonstrated that the highest selection went towards:

- The volume of information, 88% of the whole participants selected it as a challenge and 7% were passive. Meanwhile, the responses of the participants with more than 10 years of experience results were 83% agree and 17% were neutral.

By the end of the Top 3 challenge selection question all the presented challenges were selected by at least one participant, as one of the Top 1, Top2 or Top 3 challenges.

It was remarkable in the Top 4 Challenge question that the highest selection went towards the understanding and interpreting IDS data challenge which was selected before to have the highest rank in the Top 1 Challenge question.

Finally, the results of the Top 5 Challenge question demonstrated that the highest selection went towards:

- Determining the alert severity level, 71% of the whole participants selected it as a challenge and 22% were neutral. Meanwhile, the responses of the participants with more than 10 years of experience results were 50% agree and 17% were neutral while 33% did not agree.

- Effectiveness of the IDS response, 68% of the whole participants selected it as a challenge and 22% were neutral. Meanwhile, the responses of the participants with more than 10 years of experience results were 50% agree and 17% were neutral while 33% did not agree.

However, the responses to the categories Top 1 challenges, Top 2 challenges, Top 3 challenges, Top 4 challenges and Top 5 challenges are available in Appendix A.1- Table B.

4.3.8 False Positives Problem

In the field of the IDS research, it is well-known that the high rates of false positives are a nightmare to the administrators. Therefore, there was no doubt that the participants will select it among the five Top challenges. Actually, they select it to be one of the two highest ranks in the Top 1 challenge question.

The results of the false positive rate question are represented in Figure 39. It was not strange to find that 19.5% of the participants did not know the answer, which is normal because many of the participants are not in a position to provide this type of information. Otherwise, the rest of the participants provide a variety of answers depending on their experience with the IDS that they use. Figure 39 is constructed to illustrate the responses of the whole participants, then, the participants who have more than 3 years experience, the participants who have more than 6 years experience and finally the high level experts, the participants who have more than 10 years experience. Moreover, their answers depend on the traffic environment that they monitor and the efficiency of the configuration of these IDS.

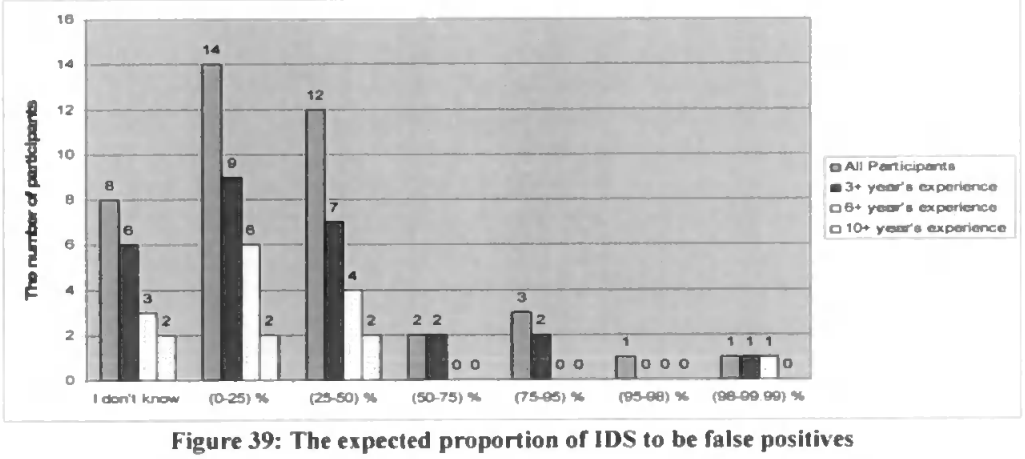


Figure 39: The expected proportion of IDS to be false positives

4.4 Analysis and Discussions

The previous sections discussed the web-based questionnaire design and how did the participants respond to it. Furthermore, charts expressing the data and also some analysis were provided. The final question within the questionnaire was an optional one to give the participants the opportunity to provide their suggestions of how to improve the performance of the IDS and to have the chance to append any further comments. We received some valuable feedback to that question, however, one suggests modifying the design of the questionnaire to have more valuable results while another comment was a sort of joke such as "do not connect

the computer to the network", even that it is a trivial solution but is not practical. Moreover, all the comments are included in Appendix A.3.

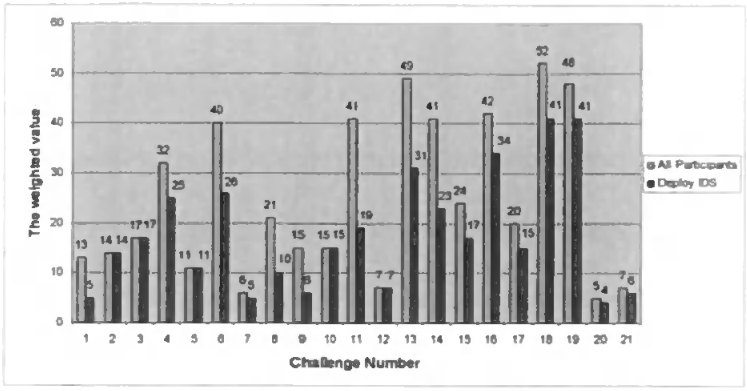


Figure 40: Top Challenges by using a weighting method

One of the most important concerns in this research is to determine and evaluate the severity of the IDS challenges. Hence, the aim of this questionnaire is to obtain the answers based on the participant's responses. Previously, the severity of the challenges was ranked in section (4.3.7) by three different methods. Furthermore, another method was adopted which was manipulating the results of each of the five questions of the Top five challenges separately. Therefore, it was decided to employ other methods to rank the challenges. One of the adopted methods was to weight the challenges in each of these five classes in the previous method (i.e. the challenges which were selected in Top 1 Challenge class have the weight 5, the challenges which were selected as Top 2 have the weight 4, the challenges which were selected as Top 3 have the weight 3, the challenges which were selected as Top 4 have the weight 2 and the challenges which were selected as Top 5 have the weight 1). The results of classifying the challenges based on this strategy are represented in Figure 40. The remarkable notice is that the highest weighted challenge selected by the whole participants was the "alerts correlation", even that it was not selected as the top choice in any of the previous five Top Challenges classes. It was obvious from Figure 40 that the results of the whole participants and the participants who deploy IDS went towards the following challenges:

- Alerts correlation,

- Understanding and interpreting IDS data,
- Requirement for skilled staff,
- IDS can raise too many erroneous alerts (i.e. false positives),
- The large number of alerts,
- Difficulty in customizing and updating the IDS ruleset,
- Volume of information,

For ease of reference, the top-ranked challenges are summarised in Table 4, showing the order of the four most challenging aspects as identified across the whole respondent group and within the subset that had IDS deployment experience.

Rank	All respondents	Respondents deploying IDS
1	Alert correlation (52)	Alert correlation (41)
2	Understanding and interpreting IDS data(49)	Requirement for skilled staff (41)
3	Requirement for skilled staff (48)	IDS can raise too many erroneous alerts (i.e. false positives)(34)
4	IDS can raise too many erroneous alerts (i.e. false positives)(42)	Understanding and interpreting IDS data(31)

Table 4: Top-ranked IDS challenges

The numbers in Table 4 represent the sum of each challenge after using the weighting method as shown in Figure 40.

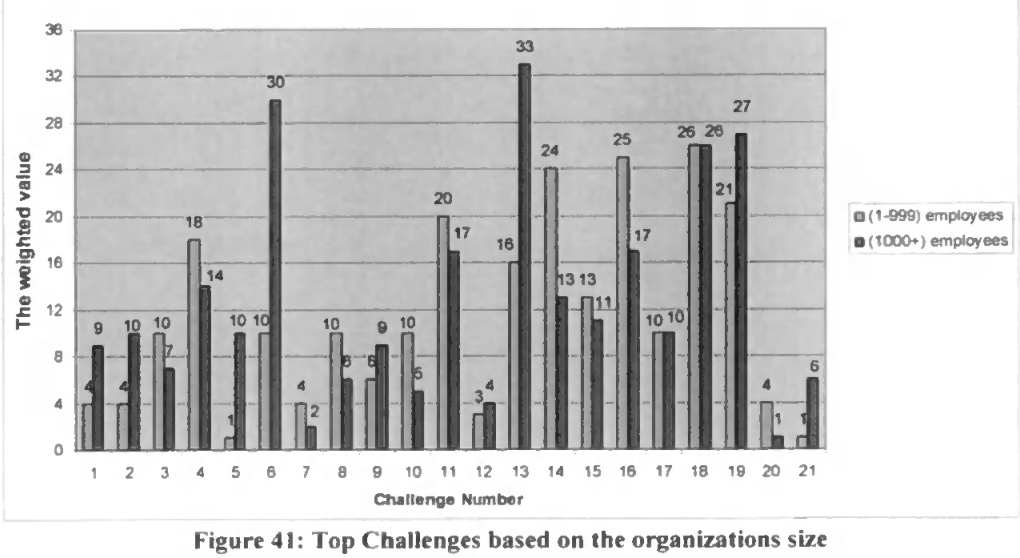


Figure 41: Top Challenges based on the organizations size

The third suggested method was to rank the whole challenges according to the size of the organizations. Figure 41 is constructed to illustrate the responses of two categories participants belong to organizations employ between (1-999) persons and participants belongs to organizations employ more than 1000 persons. The purpose of this methodology is to determine if there is any significant variation in the challenges that encounters these organizations. Moreover, it was preferred to have the advantage of the latter weighted method to obtain the challenges severity which will be based on the organizations size. It was remarkable that the alerts correlation challenge and the requirement for skilled staff challenge were selected to be of the highest selected challenges in the both classes. Moreover, for clarity, the highest challenges in organizations with (1-999) employees are as follows:

- Alerts correlation,
- IDS can raise too many erroneous alerts (i.e. false positives),
- The large number of alerts,
- Requirement for skilled staff,
- Difficulty in customizing and updating the IDS ruleset

While the highest challenges in organizations with (1000+) employees are as follows:

- Understanding and interpreting IDS data,
- Volume of information,
- Requirement for skilled staff,
- Alerts correlation.

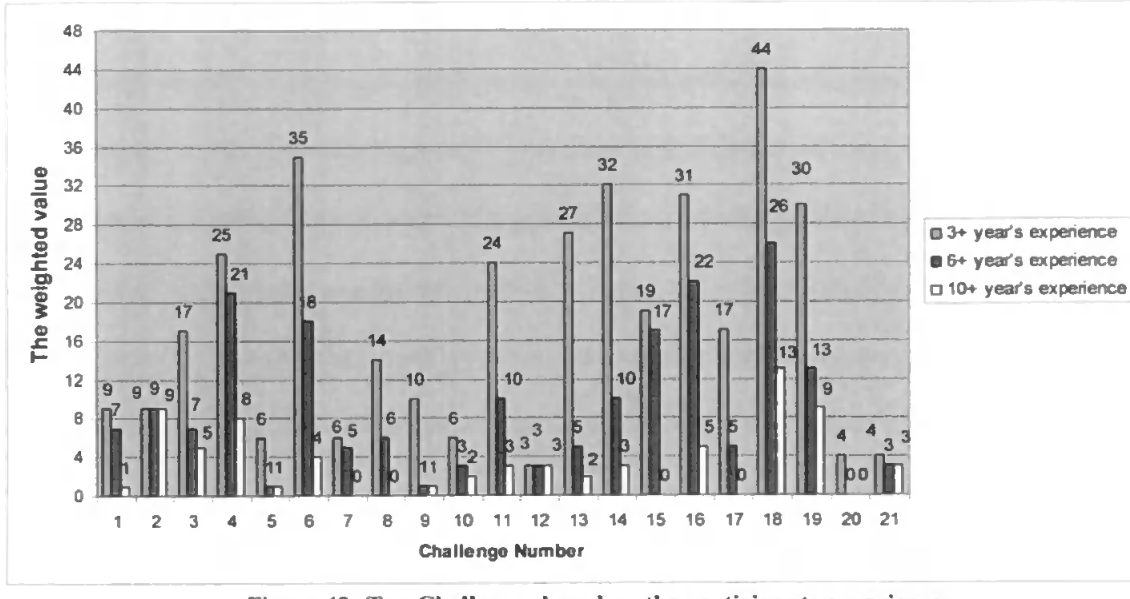


Figure 42: Top Challenges based on the participants experience

The fourth suggested method was to rank the whole challenges according to the participant's level of experience. Figure 42 is constructed to illustrate the responses the participants who have more than 3 years experience, then the participants who have more than 6 years experience and finally the high level experts (i.e. the participants who have more than 10 years experience). Moreover, it was preferred to have the advantage of the previous weighted method to obtain the challenges severity which will be based on the participant's level of experience. It was remarkable that the three previous classes of experts selected alerts correlation to be the largest problem that encounters IDS technologies. Moreover, for clarity, the highest challenges in 3+ years experience class are as follows:

- Alerts correlation,
- Volume of information,
- The large number of alerts,
- IDS can raise too many erroneous alerts (i.e. false positives),
- Requirement for skilled staff.

The fifth suggested method was to rank only the challenges that had no negative responses from the whole participants of the questionnaire. Moreover, during the investigations through the responses it was found that none of the participants claimed that the following three challenges are not a challenge, their responses varied between positive and passive but none of them were negative. It was preferred to consider the weighted method during sorting these challenges. Hence, these challenges are sorted, in order, as follows:

- Understanding and interpreting IDS data, approximately 88% of the whole participants selected understanding and interpreting IDS data as a challenge and 12% responses were passive.
- Difficulty in customizing and updating the IDS ruleset, approximately 80% of the whole participants selected it as a challenge and 20% responses were passive.
- Managing a heterogeneous IDS environment, approximately 68% of the whole participants selected managing a heterogeneous IDS environment as a challenge and 32% responses were passive.

Finally, it was noticed that there are five of the challenges that all participants are aware of (i.e. none responded with 'do not know'). Therefore, it is worth to highlight these challenges and to investigate the correlation between them and the previous methods of ranking the challenges. Hence, these challenges are as follows:

- Ensuring effective configuration,
- Ongoing operational costs,
- The large number of alerts,
- IDS can raise too many erroneous alerts (i.e. false positives),
- Requirement for skilled staff.

4.5 Conclusion

Several methodologies were adopted in Chapter 4 to determine the severity of the IDS technologies challenges. From these methods, the focus will be on four of them, the two weighted methods, ranking based on the organization size and ranking based on the level of experience. However, the analysis of these methods provides valuable results, from these results it was found that alert correlation is almost the most dominant challenge in even that it was not selected as the top choice in the Top 1 Challenge question. The dominance of alert correlation and some other challenges was very obvious in Table 4 (i.e. understanding and interpreting IDS data, requirement for skilled staff, and false positives). However, there was some variation in the level of severity of challenges when the various methods were applied. These variations are illustrated in the figures but this variation was very remarkable in the ranking based on the organization size, specially, the volume of information challenge. Moreover, in the Response Challenge category the requirement for skilled staff was the main challenge that participants were interested with while the other challenges did not have much interest which might imply that the participants consider IDS major purpose is to detect intrusions and the response to intrusions is a minor activity for it.

It was found from the results of the current chapter, that the requirement for skilled staff, based on the various methodologies used for ranking, is one of the challenges which scores high values. The solution of employing skilled staff for every system is out of discussion. This solution is not available in reality, especially, for small organizations. Moreover, the case of a normal end-user has to be considered because it is not possible to let all the network users' experts in manipulating with intrusions. Therefore, the aim of the next stage of the research will be to perform an efficient analysis to the received IDS alerts and provide the end-user with the results in a simpler form through meaningful graphical user interface (GUI). The purpose of

this GUI is to inform the user about an intrusion or a suspicious event when it occurs in his system and to provide him with an appropriate response.

The initial aim of designing the IDS challenge survey was discovering and identifying the other major IDS challenges apart of false positives, from a practitioner perspective. As it was anticipated that the false positive problem will score the highest rate, as it is the most widely mentioned challenge in the IDS literature. Therefore, the research concern during designing the structure of the survey was to confirm the priority of the false positive challenge and to determine what is the next IDS challenging problems. The combination of the highest challenges would be the basis of the future research. The findings of the survey did not exactly match the expectations, especially in the results related to the false positive challenge. However, the findings reveal and direct the attention to remarkable issue which is that the major correlation of the top IDS challenges are the human-being side of the security process. It is considered that solving and alleviating the impact of these challenges will reduce the amount of false positive. Therefore, the rest of the study will focus on integrating Human Computer Interaction (HCI) and Security.

Observing the problem of IDS in a workplace scenario it would seem reasonable to suspect that the challenges facing end users in smaller organizations or even domestic scenarios (i.e. where no expert help is available) will be even more acute. On this basis the research now moves to consider the usability issues that may exist in the security tools targeting these audiences.

Chapter 5

Establishing Usability Criteria for End-User Security Tools

5. Establishing Usability Criteria for End-User Security Tools

The previous chapter determined that the top IDS challenges are related to the human skills. Therefore, it is important to consider the security interfaces that are presented to end-users. Hence, to further explore the challenge at this level, this chapter focuses on home users and how could they manipulate with IDS alerts. The focus will be on the Human Computer Interaction (HCI) and how it contributes in alleviating the IDS challenges encountered by end-users. The ultimate aim is to establish an adequate set of design/evaluation criteria to develop enhanced security user interfaces that meet the security conditions; meanwhile matching the expectation of a wide range of end-users, from a security and usability perspective. It is anticipated that the novel criteria will lead to better-designed user interfaces. The popularity of the Internet and all the services it provides has driven the demand for computers in the home. Unfortunately, these home users typically represent a group of users who are generally poorly educated about the dangers and threats that exist when connected to the Internet. To this end, security vendors have provided a variety of integrated security solutions that provide Anti-Virus, Firewalls and Intrusion Detection Systems to enable home users to become better protected. However, the need to rely upon users to make decisions about potential threats they have little or no information about is concerning at best. An analysis of user interfaces that relate to security have shown they frequently lack in providing usable interfaces that users are able to make informed decisions from (West, 2008). The aim of the chapter is to support these home users by proposing a set of novel design criteria to enable the development of usable security alerts that are triggered by their security mechanisms. Drawing from literature, the criteria that

are proposed take into account the unique usability issues that exist when dealing with information security: explicit and useful information, the ability to make a timely response and a consistent presentation of information. A walkthrough using a potentially problematic dialog from Norton 360 is used as a case study to highlight the current issues with the interfaces and to evaluate the proposed criteria. The findings of the evaluation reveal that the novel criteria are promising and the assessment of other security tools are required to make consistent and valuable recommendations.

Sometimes end-users encounter usability problems while performing their normal computer tasks. Frequently, these problems are not in performing the primary intended tasks, but relate to alerts and warning messages triggered by other software, such as security tools. Arguably some novice users will get annoyed, particularly in the case when the system is bombarding alerts at the them; which causes them to subsequently decide to uninstall the security software after a short time (i.e. hours or days) leaving them insecure (Herzog and Shahmehri, 2007). A significant inconvenience to the user is the inability to make an informed decision, with factors such as, lack of security knowledge and poor interface design hindering the decision making process. This can result in them often guessing as to whether to allow or deny a particular alert or action. This problem is amplified because security notifications rarely form part of the primary activity the user is engaging with on the system and are therefore merely considered an inconvenience.

The ability to understand the alert notifications that many modern security applications use is no simple task. Prior research looking into what issues exist for commercial Intrusion Detection Systems identified skilled staff as a key element to an effective system, as shown

in Chapter 4. Obviously, however, the idea of skilled staff within a home user context is simply not feasible. Therefore, it is imperative that security tools for home users must interface with the home user in such a manner to provide sufficient information for the user to make an informed decision in a timely manner but at the same time provide an interface that is friendly and usable. The purpose of this chapter is to enhance the home user experience and provide the ability to deal with the security alerts effectively by proposing novel usability design criteria.

5.1 Usability Criteria for End-User Security Tools

This section focuses upon the related research including security criteria for designing a usable graphical user interface (GUI). Many studies have been completed in the field of (HCI) and the use of the term HCI is widely aligned with the term usability in the research discipline. Jacob Nielsen developed ten usability criteria which many subsequent studies have used as a basis of their work (Nielson, 1994; Nielsen, 2005). Shneiderman and Plaisant (2005) presented a refined version of eight usability criteria, based upon the authors experience over more than two decades. For the study purposes, the limitation of both these studies is that they are general usability criteria and the authors did not consider the impact of security in their design. Chiasson et al. (2006), Chiasson et al. (2007), Garfinkel (2005), Johnston et al. (2003), Whitten and Tygar (1999), Yee (2002) and Zhou et al. (2004), have all presented alternative guidelines that consider security. Whitten and Tygar (1999) seminal HCI-SEC paper 'Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.' is considered to be one of the most established studies in the usable security research area. They conducted a case study to evaluate the usability of the email encryption by assessing the Pretty Good Privacy (PGP). Another example is Johnston et. al. (2003) who developed a set of six HCI criteria suitable for security and introduced a new term is

the usable security field, called HCI-S. The term was defined as, *'the part of a user interface which is responsible for establishing the common ground between a user and the security features of a system. HCI-S is human computer interaction applied in the area of computer security.'* .The authors kept the *Visibility of the System Status* criterion from (Nielsen, 2005) and appended a new criterion entitled *Convey Features* (which shows users the availability of security features in the system, whereas the 'visibility' of features refers to their current status). Chiasson et al. (2007) in particular propose a set of design guidelines for designing security management interfaces. Whilst the study looks to design them with respect to administrators they can be usefully applied to home-users. Herzog and Shahmehri (2007) proposed more sophisticated guidelines for applications that set a security policy. The authors are interested in the limitation of some current security policies and the difficulty that novice users encounter when using it; especially for the first time. Figure 43 summarizes some of the well-known usability guidelines.

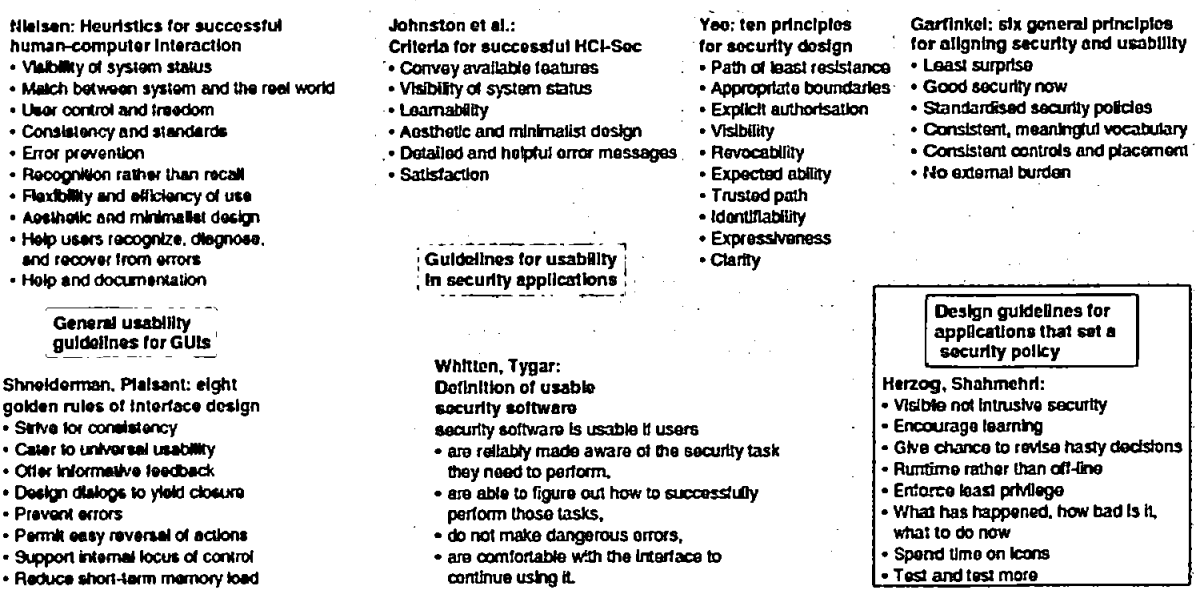


Figure 43: Structured overview of guidelines for usability in security applications (Herzog and Shahmehri, 2007)

Based upon the prior literature, the following 16 guidelines were developed:

1- Interfaces Design Matches User's Mental Model

The designer of alert interfaces should attempt to think as home-users to develop alert interfaces matches the users mental model. Initially, the user who receives a security alert will need to know the name of the security tool which triggered that alert. The user also needs to know how to respond correctly to that alert as fast as possible. Finally, the user who failed to respond or/and could not understand the response options, will need more help. In summary, the main interface of the alert should consist of four sectors: the alert detector sector, the alert description sector, the alert response sector and the alert support sector.

In general, the criteria of Chiasson et al. (2006), Chiasson et al. (2007), Herzog and Shahmehri (2007) Johnston et al. (2003), Nielsen (2005), Shneiderman and Plaisant (2005, Whitten and Tygar (1999) and Yee (2002) guides to the current criterion, Interfaces Design Matches User's Mental Model.

2- Aesthetic and Minimalist Design

Irrelevant or rarely needed information should not be displayed in the security alert. The alert interface design should determine the cause of the alert and impose the available response options to support the user to respond effectively. Bombarding the user with a lot of information might distract the user and force him to react randomly, just to return back to the indented primary task. Some alert interfaces manage to have a minimalist design but they do not have an aesthetic design. The current criterion is quoted from Nielsen (2005).

3- Visibility of the Alert Detector Name

The appearance of the security tool name, which triggers the alert, is useful, specially, with the existence of more than one installed security tool on the home-use machine. This feature might guide the user to adjust the security settings of this particular tool. The reader should notice that the current criterion is not the same as the *Visibility of System Status* (Nielsen, 2005) criterion

but perhaps a subset of it. Even though this criterion seems to be a subset of criterion one, it was preferred to write it as a standalone criteria.

4- Establish Standard Colours to Attract User Attention

Users are most often attracted by the use of colours in the interfaces. Therefore, it is very important to focus on the use of colours as a major usability criterion. In general, the use of red and yellow colours in security alert interfaces are fairly standard, for example, the red colour informs the user that the alert severity is high; while the (orange or yellow) colour informs the user that severity of the alert is low. Moreover, we can consider this criterion as a subset of the *Visibility of the System Status* (Nielsen, 2005) criterion.

5- Use Icons as Visual Indicators

Users are most often affected by the use of pictures and icons in the interfaces. Therefore, it is very important to utilise this human feature to enhance the criteria. Muñoz-Arteaga et al. (2008) usefully utilised the image of the traffic light to declare the security situation. This also supports the previous criterion, *Establish Standard Colours to Attract User Attention*. Finally, we can describe the icon and the previous colour criteria together as an implementation of the *recognition* feature from *Recognition Rather than Recall* guidelines (Nielsen, 2005).

6- Explicit Words to Classify the Security Risk level

The use of informative colours and icons, in the security alerts, to inform the user of the security risk level, as demonstrated in the previous two criteria, is excellent but not arguably enough. The user requires written confirmation of the security risk level and that information must be obvious in the main alert interface, not hidden in a secondary interface.

7- Consistent Meaningful Vocabulary and Terminology

The alert sentence(s) should be simple, short and informative and the words used in these sentence(s) should be familiar to the user. It is recommended that security terms that some users might be not aware of, such as the term *phishing attack*, should be avoided. Moreover, if possible, it would be better that each alert sector consist only of one sentence. However, the current criterion includes the main features of the Neilson criteria *Match Between System and the Real World*, *Consistency and Standards* and *Aesthetic and Minimalist Design*. Moreover, the current criterion is similar to the criterion *strive for consistency* within Shneiderman and Plaisant (2005).

8- Consistent Controls and Placement

Users need to be able to find the security features they need in an appropriate location and in a reasonable time. Buttons are one of the most common user controls that are provided in interfaces. Unfortunately, in some security tools the appearance of these buttons reflects the existence of a poor design, at least from a usability perspective. For example, *Allow* and *Block* buttons exists in some security alerts without providing the user with any clue about the impact of this selection (i.e. the allowance or the blocking might be permanent or temporary). Therefore, this sort of information should be designed explicitly in the screen to give the user more control and freedom.

9- Learnability, Flexibility and Efficiency of Use

The security alert should be flexible and efficient to use, and enhance the user ability to learn the required security basics. The current criterion stresses on the use of explanatory tooltips for concepts or/and security terms which appears in the alert window to enhance the system flexibility, while providing links to access a built-in library or/and an Internet web page, in

some other cases to increase the system efficiency. Learnability is an explicit criterion within Johnston et al. (2003).

10- Take Advantage of Previous Security Decisions

This criterion consists of two parts as follows:

- The home user alert history: only the user's previous experience with the alert: The user deserves to obtain information about the triggered alert. This information reports whether this type of alert has occurred before or not, and how the user previously reacted to it. The use of simple statistics which summarize this information will also be very helpful for the user in the decision making process. Moreover, these statistics should also be available to the user to give them the chance to investigate later, to evaluate the effect of his decision.

- Social feedback: other home-users previous experience with the alert: Develop a process by where users are able to benefit from other users' experiences. For instance, a security software database could receive reports of the user responses for every alert generated in the home user's machines. All users should have access to that database as soon as one of these alerts is triggered in the user machine. The existence of the criterion increases the home-user *learnability,* one of Johnston et al. (2003) HCI-S criteria. Moreover, the criterion is an enhancement of (Nielsen, 2005) *Help Users Recognize, Diagnose, and Recover from Errors* criterion.

11- Online Security Policy Configuration

The security tool designers should develop an efficient default configuration for the security policy. The aim of the criterion is in guiding the user to adjust the security settings to avoid, if

possible, any conflict between the intended primary tasks and the security configuration (i.e. for instance, to avoid the triggering of frequently low level security alerts). It is anticipated that the current criterion would enhance (Johnston et al. 2003) HCI-S criterion *Convey Features.*

12- Confirm / Recover the Impact of User Decision

The security alert interfaces should be designed carefully to prevent home user errors. Sometimes, user errors are inevitable and vary from simple mistakes to dangerous errors, as follows:

- The user might press a button or click a link unintentionally by mistake.
- The user might respond randomly to the security alert and feels later that he/she made a mistake.
- The user decision might have an unanticipated impact on the configuration.
- The user decision might have a vital impact that seriously affects the security of the machine.

Therefore, the user should receive a confirmation message after performing any response which will affect the security of the system. The confirmation message should contain information about the possible impact of the decision. This facility gives the user the chance to recover the error, modify the response, extract a rough evaluation of the reaction and make a more informed decision. Moreover, the current criterion, to some extent, match Nielsen (2005) criterion *Help users recognize, diagnose, and recover from errors,*

13- Awareness of System Status all the Time

The user deserves to obtain a simple report declaring the state of the system as a result of the home user response to the alert. This report could be raised immediately after the user responds

to the security alert or/and could be saved, where the user can access it after performing his intended task.

14- Help Provision and Remote Technical Support

The security alert should be designed to let the users be self-sufficient; however, some will still require further support. Tools should therefore provide built-in help and remote technical support. In this chapter the term "help" means providing the user with extra information at the time of the alert and advice on an appropriate response. In practice, information in the accompanying help is not always sufficient to enable the user to respond correctly. Therefore, they can use the "remote technical support" facility as a final attempt to solve the security problem via support from the security vendor. The current criterion, to some extent is similar to Nielsen (2005) criterion *Help and documentation.*

15- Offer Responses that Match User Expectations

Home-users usually make security decisions based upon factors such as the security alert feedback, the response options available, and their own hypothesis of the impact that the response would have. However, the *actual* impact of the available alert responses options does not always match the user's expectation. Therefore, good alert design is not only what is required to obtain a secure system but also to ensure the user's correct comprehension and understanding.

16- Trust and Satisfaction

Home-users typically trust the security tool on their computers until the occurrence of a performance failure. Unfortunately, the lack of understanding or/and the inability of some home-users to react correctly to some alerts can have a strong influence on the trust or/and

satisfaction factors. In some cases, such events might lead them to improve their security knowledge (i.e. they still trust the security tool), but others might prefer to uninstall the software and thereby avoid further inconvenience.

	Proposed Criteria	Chiasson (2006)	Chiasson (2007)	Garfinkel	Herzog	Johnston	Nielson (2005)	Shneiderman	Whitten	Yee	Zhou
1	Design Interfaces Match User Mental Model	✓	✓	-	✓	✓	✓	✓	✓	✓	
2	Aesthetic and minimalist design	-	✓	-	✓	✓	✓	✓	-	✓	
3	Visibility of the Alert Detector Name	-	-	-	✓	-	✓	✓	-	-	
4	Establish standard colours to attract user attention	-	-	-	-	-	✓	✓	-	-	
5	Use icons as visual indicators	-	-	-	✓	✓	✓	✓	-	-	
6	Explicit Words to Classify the Security Risk level	-	-	-	✓	-	-	-	-	✓	
7	Consistent Meaningful Vocabulary and terminology	-	-	✓	-	✓	✓	✓	-	✓	✓
8	Consistent Controls and Placement	-	-	✓	-	-	-	✓	-	✓	
9	Learnability, Flexibility and Efficiency of Use	-	-	-	✓	✓	✓	✓	-	-	✓
10	Take Advantage of Previous Security Decisions	-	✓	-	-	-	-	-	-	-	
11	Online Security Policy Configuration	-	✓	✓	✓	-	-	-	-	✓	
12	Confirm / Recover the impact of User Decision	✓	✓	-	✓	-	✓	✓	✓	✓	
13	Awareness of System Status all the Time	✓	✓	-	-	✓	✓	✓	-	✓	✓
14	Help Provision and Remote Technical Support	-	-	-	-	✓	✓	-	-	-	✓
15	Offer Responses Match User Expectations	✓	✓	✓	-	-	-	✓	-	✓	
16	Trust and Satisfaction	✓	-	-	-	✓	-	✓	✓	-	

Table 5: Comparing the proposed criteria against existing usability guidelines

Table 5 presents a comparison between the proposed criteria and some established usability guidelines (note: the guidelines are referenced via the names of lead authors listed in the References section, with a year added in cases where multiple papers from an author have been listed). The main purpose of this comparison is to demonstrate the real-world requirement to develop usability criteria specifically for security alerts. The findings suggest that the criteria have a role to play, in the sense that no individual example from the established guidelines covers the full range of issues. The current criterion match to some extent Johnston et al. (2003) criterion *Satisfaction*.

5.2 Assessing Alerts in Practice

This section presents a detailed assessment of a typical security alert, and a walkthrough of the process that a user might take in order to understand it. The example is taken from

Norton 360; a package that is widely recognized and popular among end-users. The choice is not intended to imply that Norton 360 usability is worse than others in its class, and indeed it has actually scored highly on ease of use in comparative evaluations (Which, 2009). Therefore, it is expected some of the limitations mentioned here might also exist in some other well-known products. Indeed, the Norton case represents one example from a wider study being undertaken by the authors, and is intended to be illustrative of the problems that can be encountered in practice rather than being presented as a significant finding in its own right.

The analysis presented here uses a simple alert that many users would have encountered. Having installed Mozilla Firefox and started the application for the fist time, an alert appeared, as illustrated in Figure 44. This is a trivial case compared to others that might occur, but is notable in that it may still confuse some users (particularly novices), and cause them to devote time to an event that actually would not cause any harm to their system.

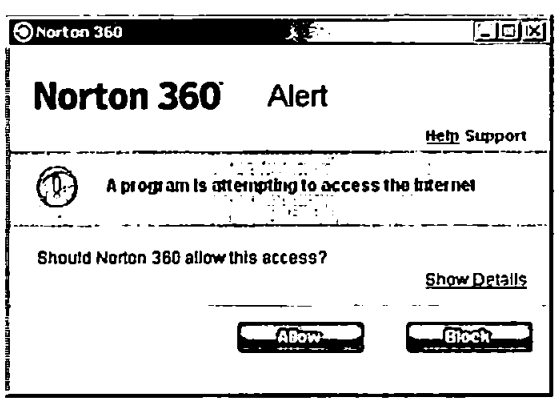


Figure 44: A real example of Norton 360 security alert

The events and thought processes from this point are documented from the perspective of the user. The first comment is that the main interface provides no information about the cause of the alert and there are no explanatory tooltips (the cause was relatively obvious in this case, because the user had intentionally launched Firefox immediately beforehand, but other cases

may be less clearcut). Arguably therefore, the main interface of the alert did not achieve the *Learnability, Flexibility and Efficiency of Use* criterion. Moreover, it is clear that the user's *mental model* was not completely considered during designing of this alert.

Assuming that the user decides to read the rest of the content (rather than investigating the *Help* and *Support* links), the alert wording is direct and simple, which satisfies the proposed seventh criterion. The user can assume that the exclamation mark icon and the yellow colour indicate only a warning case, which increases assurance that there is no high risk. This confirms the importance the proposed fourth and fifth criteria *Establish Standard Colours to Attract User Attention* and *Use Icons as Visual Indicators*, respectively. Nonetheless, the summary view of the alert did not mention explicitly, by words, the risk level status, which represents a design limitation, from the usability perspective.

At this stage, the user has a general idea about the alert and is presented with an explicit question, *"Should Norton 360 allow this access?"* (consequently managing to mention *Norton 360* for a third time in the same dialog, while other relevant information is missing). The user may assume that the *Show Details* link will give more guidance about how to respond, but this actually reveals more details about the cause of the alert (see Figure 45). This consequently reveals a minor conflict with the *Consistent Controls and Placement* criterion, as the link has been placed at a point in the dialog where the user is making a response rather than understanding the alert.

Looking at the consequence of selecting *Show Details* (Figure 45), it can be noted that all of the terms are mentioned without any further links. The user can now see the *Name* of the executable program that raised the alert, and the related *Path*. Moreover, further down the list,

the user is given an explicit indication of the *Risk Level*. However, of the eight items listed, these are likely to be the only ones that will be meaningful to a wider audience. The inability to get any further description (e.g. via tooltips) will mean that many users are confused rather than informed by items such as the *Remote Url*, *Protocol* and *Direction*. No links in the *Show Details* interface is a remarkable limitation. In fact, even items such as the *Name* could merit further assistance. While the user might well be expected to recognise it in this example, other cases may not be so readily obvious and having a lookup to reference the names of known applications could be beneficial.

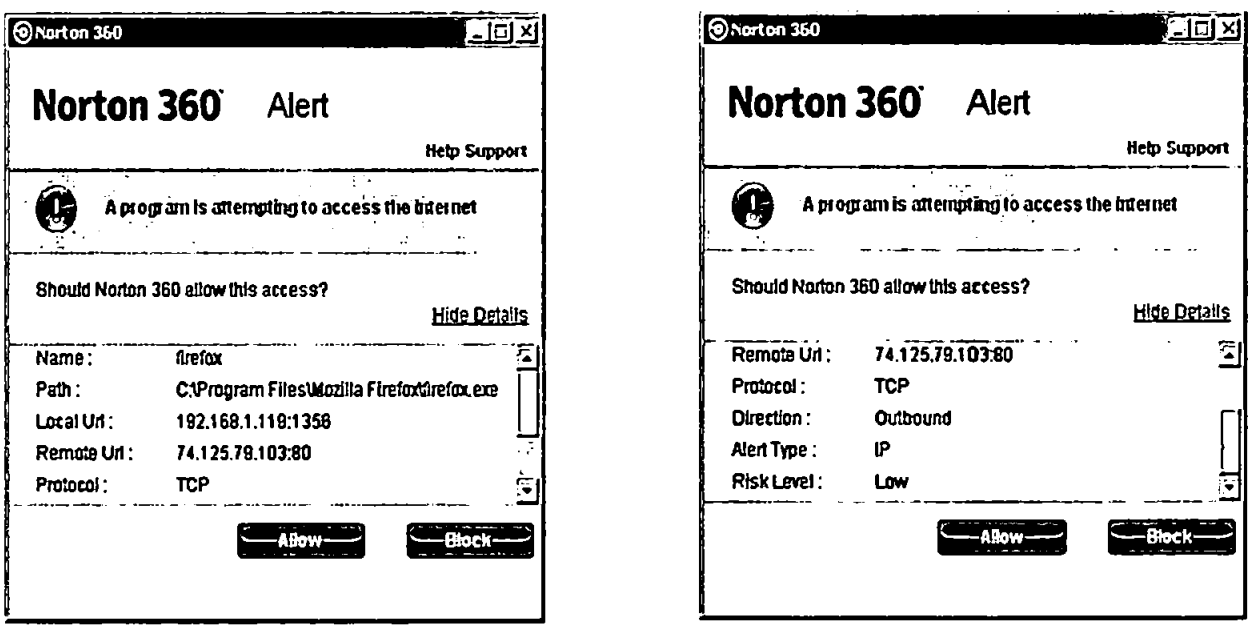


Figure 45: The expanded view of the alert, having selected the Show Details link

Let us assume the user felt stuck at this point, and still wanted to obtain more information about exactly what was causing the alert. The use of Norton 360 *Help* is shown in Figure 46. The user wrote the terms *Firefox* and *firefox.exe* separately in the *Index* but failed to provide any result. Next, the user wrote the same terms in the *Search* but the user did not find any useful information.

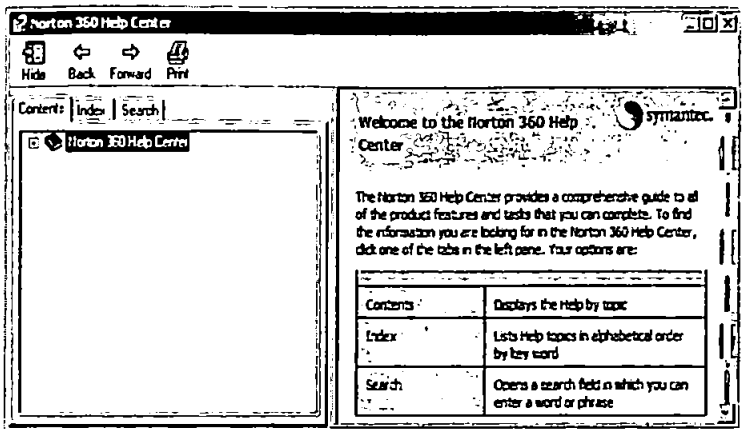


Figure 46: Norton 360 Help

Trying another route, the user may select the *Support* option from Figure 44. Selecting *Search Solution Library* yields the dialog shown on the right hand side of the Figure 47. Once again the user typed the term *Firefox*, the results focused upon the cause of the alert but only indicated Internet Explorer web browser and requested the user to check whether it is the default web browser or not. Hence, the user may assume that the cause of the alert was related to a default web browser issue, which is a computer setting rather than a security issue.

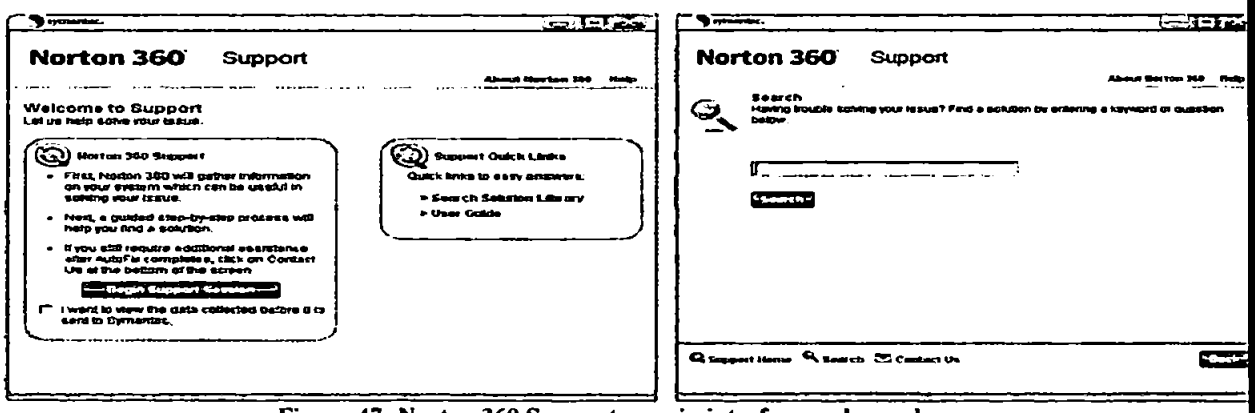


Figure 47: Norton 360 Support – main interface and search

From this point, the user only has one further line of investigation within the tool; namely to select the *Contact us* link shown at the bottom of Figure provide the user with three options to obtain Norton technical support; live chat, e-mail and phone calls, as shown in Figure 48. Although each of these are likely to yield a satisfactory result (especially in the case of this

specific example), it seems a rather long way for the user to have to go in order to obtain a fairly baseline level of clarification.

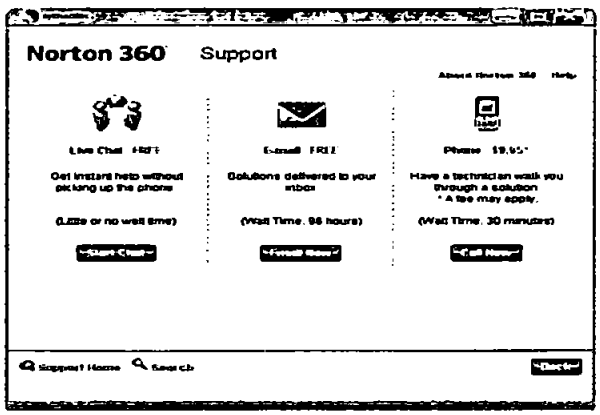


Figure 48: Norton 360 Contact us

The findings of this walkthrough suggest that some home-users who receive such alerts will require more help. The alert dialog provides three options which are *Help*, *Support* and *Show Details*. Unfortunately, they do not provide the user with the sort of information that might support a decision (for instance, there are no tooltips or links to more information). We applied the proposed criteria on this example and summarised the findings in Table 6.

No	Novel Criteria	Evaluation
1	Design Interfaces Match User Mental Model	Yes to some extent (the interface consists of the suggested four sectors but the contents does not match the user mental model)
2	Aesthetic and Minimalist Design	Yes (minimalist, but not aesthetic)
3	Visibility of the Alert Detector Name	Yes
4	Establish Standard Colours to Attract User Attention	Yes (e.g. Yellow = Low Risk Severity)
5	Use Icons as Visual Indicators	Yes (e.g. exclamation mark = Warning)
6	Explicit Words to Classify the Security Risk level	Yes but in a secondary interface
7	Consistent Meaningful Vocabulary and Terminology	Yes
8	Consistent Controls and Placement	Yes (but there is no indication of whether the effects of selecting an option are permanent or temporary)
9	Learnability, Flexibility and Efficiency of Use	No (no tooltips or links to web sites)
10	Take Advantage of Previous Security Decisions	No
11	Online Security Policy Configuration	No
12	Confirm / Recover the Impact of User Decision	No
13	Awareness of System Status all the Time	No (Norton 360 provides only a general status for the whole system)
14	Help Provision and Remote Technical Support	Yes ("Help" is not useful & "Support" is useful but time-consuming and sometimes costs money)
15	Offer Responses Match Expectations	No
16	Trust and Satisfaction	Medium

Table 6: Evaluating a real Norton 360 security alert using the proposed criteria

As an example of the proposed criteria in use, Figure 49 represents the same alert with some simple modification. The design helps the user to follow the scenario of the alert from the top to the bottom without distracting him to look at every single location in the security interface all the time. The user will be able to scan the alert without the need to go backward and forward to be sure that the user did not miss vital information. It is also worth mentioning that the alert was not overly serious in this example and the user was almost aware of what caused the alert. The user was not performing an important or an urgent task. The user was therefore not panicked and had the opportunity to investigate and confirm what had caused the alert and how to respond to it. The reader can imagine how painful the case would be if the user receives an alert, has no basis to understand what triggered it and does not have the time to investigate it.

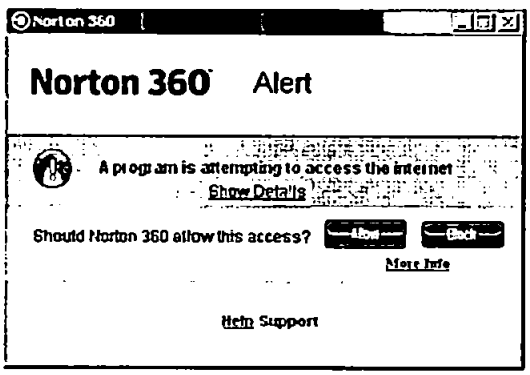


Figure 49: A simple modification on Norton 360 security alert

The proposed alert, in Figure 49, enhanced the original alert in at least two criteria *Design Interfaces Match User Mental Model* and *Consistent Controls and Placement.* The enhancement occurred by locating the *Help* and *Support* at the bottom of the alert interface, this location is better because the user will reach the help button after investigating the alert dialog which match the mental model for an average user. Moreover, the current design claims that *Show Details* location is in an appropriate place in which asking the user to know more information about the program that is attempting to access the Internet. perform a response. Meanwhile, the location of *Allow* and *Block* buttons next to the question of

allowing the access is more appropriate and better than locating them at the bottom of the alert interface.

5.3 Conclusions

Home users require an efficient security tool to protect them. Unfortunately, the analysis performed in this study has illustrated that the interfaces provided by such tools are not always sufficient to enable users to make intelligent and informed decisions. The criteria developed in this chapter are an attempt to rectify the problem; utilising existing HCI based design criteria and applying them specifically to the problem of security software. The Norton 360 example illustrates the nature of the problems that can be encountered, even in the case of a baseline, low risk alert.

The proposed criteria were deduced by investigating the established usability criteria in mentioned the above literature and including the personal opinion as well. First, the research started with focusing on the literature, then subjective analysis against a well-known security product (i.e. Norton 360) and finally examined a list of security products in the next chapter. Additional research will be undertaken to validate the proposed criteria, through focussing upon a number of security interfaces across the most common security tools. Using this evaluation, the criteria will be re-evaluated and subsequently applied to software to ensure they are appropriate and robust criteria to be utilised more widely within the security industry for designing systems.

Chapter 6

Assessing the Usability of End-Users Security Tools

6 Assessing the Usability of End-Users Security Tools

Home users are more vulnerable to Internet threats than those who work in organizations. Most home-users know to install anti-virus (AV) and today most home-user security products come in the form of an Internet security tool that combines several countermeasures in one. From a previous study we have determined that commercial security products can suffer from a usability perspective, lacking the necessary attention to design in relation to the security alert interface. Therefore, the aim of the chapter is to assess the usability of alerts in the some of the leading Internet security packages, based upon a related set of usability criteria. The findings reveal that the interface design combined with the home user's relative lack of security knowledge are two major challenges that influence their decision making process. The analysis of the alert designs showed that four of the criteria are not addressed in any of the selected security measures and it would be desirable to consider the user's previous decisions on similar alerts, and modify alerts accordingly to the user's previous behaviour.

Network security experts are aware of the risk that home users encounter during network connection sessions. For instance, the Symantec Internet Security Threat Report reveals that during the first half of 2007, 95% of Internet attacks were directed towards home-users (Symantec, 2007). Therefore, expert's recommendations always aim to convince home-users to install effective security solutions. For several years, home users could rely upon basic anti-virus (AV) as a sufficient security tool, at least from the home-users perspective. Unfortunately, standalone AV is no longer enough to protect end-users from security threats (House of Lords, 2007). Therefore, the deployment of other advanced solutions such as Firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) becomes more necessary. Meanwhile, the management and manipulation of these types of security solutions usually requires an appropriate and high level of IT literacy and security knowledge, which is likely to

be unavailable for the majority of home-users. The findings of Chapter 4 validate the requirement for high skilled staff to mange IDS in organizations, and it can easily be recognized that home users will face more difficulty in this respect. In recent years, security vendors have moved towards integrated AV, firewall and IDS tools, which are commonly marketed as 'Internet Security' solutions (Lai and Wren, 2009). However, although the combination of tools can provide users with a convenient and comprehensive solution, this does not necessarily guarantee attention to improving the usability. Chapter 5 proposed a set of novel HCI-S usability criteria and applied them to the evaluation of a typical alert raised by Norton 360. Even from a single example, this served to highlight a number of potential usability issues, and was considered sufficient to justify a wider evaluation of other tools against the same criteria. The current chapter therefore investigates and assesses the usability of security alert across a wider range of end-user security software.

6.1 Assessing Security Tools Alerts

This section outlines the selection of the Internet Security tools against which the usability criteria were applied, along with the method by which the tools themselves were tested in order to generate the required security alerts. To my knowledge there is no similar HCI-S case study for comparison.

6.1.1 Tool selection

Having already identified Norton 360 as part of the earlier study, a further nine popular Internet Security suites were selected in order to establish a wider basis for evaluation. The selections were made on the basis of products recommended in a related review (Top Security Software, 2009), plus the addition of products from F-Secure and Kaspersky (which are also popular options within the home and small business user communities). A further criterion was that

each product should incorporate an intrusion detection or/and prevention capability (so as to provide the capability to detect the type of attack to which it would be exposed).

The resulting list of tools was as follows (noting that free trial versions were used in some cases):

- BitDefender Internet Security 2009
- CA Internet Security Suite Plus 2009
- F-Secure Internet Security 2009
- Kaspersky Internet Security 2009
- McAfee Internet Security 2009
- Norton 360 Version 2.0
- Panda Internet Security 2009
- Security Shield 2009
- Trend Micro's Internet Security Pro 2009
- Webroot's Internet Security Essentials

The resulting set is considered to represent a sufficient and a real sample of the available security measures within the market. However, it should be noted at this point that the aim of the evaluation (and indeed this chapter) is not to identify the best product, but rather to determine the extent to which usability issues can be identified across a wider base of software.

6.1.2 Alert generation

Network scanning represents the initial step in many types of network intrusions, penetrations and attacks (Barnett and Irwin 2008). Attackers use the obtained information about the targets, such as the operating system and the open ports, to launch the subsequent attack, which then has higher possibility of success without being detected. Many tools can be used to perform

network scanning, for instance Nessus (2010) and Nmap (2010), which are two of the top network assessment tools. This study adopts the default profiles of Nmap command lines within Zenmap GUI (2010) to investigate the design of the alert interfaces that are triggered as a consequence of the scanning techniques. The evaluation experiments were held in a closed test bed environment consisting of two computers running Windows XP. Scanning processes were performed from the attacker computer running Zenmap GUI against the victim computer running the candidate security products. Table 7 illustrates the Zenmap GUI profiles and the correspondence Nmap command lines that are tested.

	Zenmap GUI Profile	Nmap Command Line
1	Intense scan	nmap -PE -PA21,23,80,3389 -A -v -T4 192.168.1.146
2	Intense scan plus UDP	nmap -PE -v -PA21,23,80,3389 -sU -A -T4 192.168.1.146
3	Intense scan, all TCP ports	nmap -PE -v -p1-65535 -PA21,23,80,3389 -A -T4 192.168.1.146
4	Intense scan, no ping	nmap -A -v -PN -T4 192.168.1.146
5	Ping scan	nmap -PE -PA21,23,80,3389 -sP 192.168.1.146
6	Quick scan	nmap -T4 -F 192.168.1.146
7	Quick scan plus	nmap -T4 --version-light -sV -F -O 192.168.1.146
8	Quick traceroute	nmap -p22,23,25,80,3389 --traceroute -PN 192.168.1.146
9	Regular scan	nmap 192.168.1.146
10	Slow comprehensive scan	nmap -PE -v -PS21,22,23,25,80,113,31339 --script=all -PO -PA80,113,443,10042 -sU -PP -A -T4 192.168.1.146

Table 7: Zenmap GUI profiles and the associated Nmap command lines

6.2 Analysis of End-Users Security Alerts According to HCI-S Criteria

During the evaluation alerts were generated by all of the tools apart from McAfee Internet Security 2009, which did not issue any visible responses to the scanning attempts (note: this is not to suggest that they were undetected, but rather that the user was not explicitly notified in real-time). The reason behind McAfee's behavior is beyond the aim of the research in this chapter and the variety of alerts generated via the other security products satisfies the aim of the study in this section. Indeed, the attempts to scan the victim computer in the test bed generated several types of alerts. The rest of the section focuses upon analyzing some key examples of these, according to the HCI-S usability criteria from Chapter 5. Rather than commenting

extensively against each tool, the discussion is structured according to the criteria headings, with examples being drawn from across the tools to illustrate significant issues.

6.2.1 Interface Design Matches User's Mental Model

Of the tools that explicitly notified the user of detecting a suspicious activity, all but Webroot's issued a response to the intrusion on behalf of the user. As shown in Figure 50, Webroot's was the only alert that did not provide the user with any explicit words to indicate whether the product had managed to handle the detected intrusion or not, nor give the user any further interaction options.

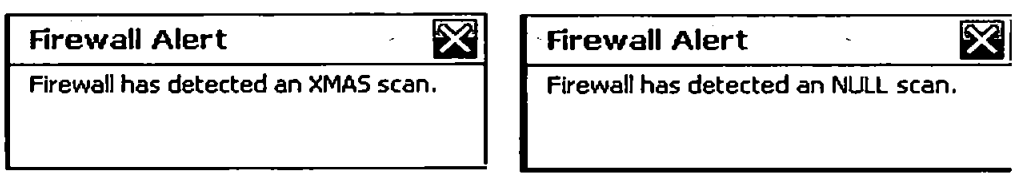


Figure 50: Webroot's Internet Security Essentials alert interfaces

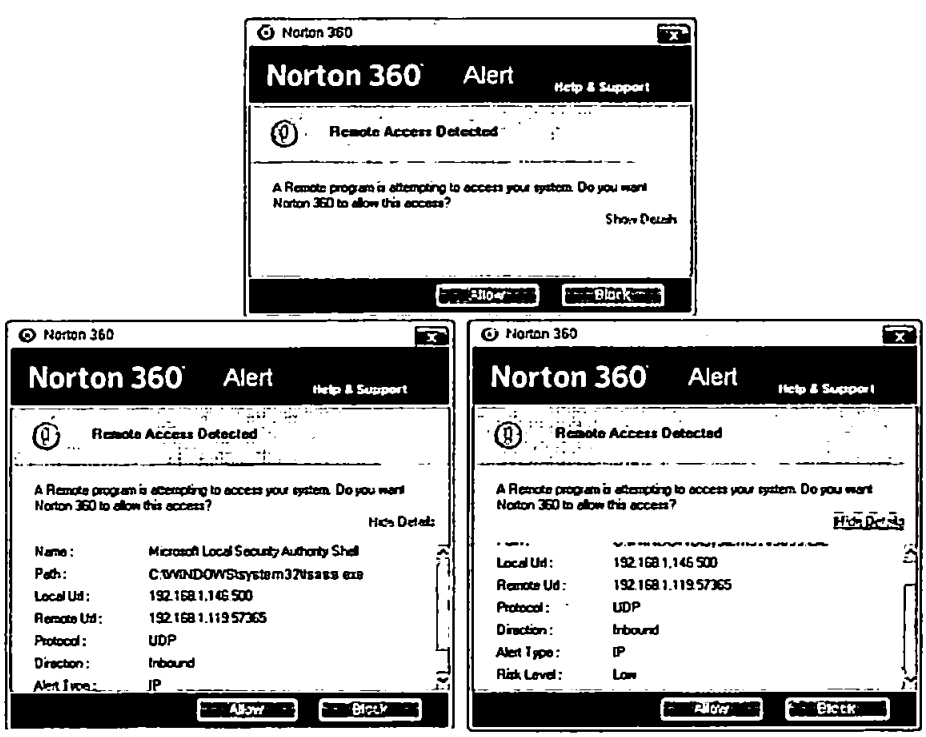


Figure 51: Norton 360 interactive alert interface

It is likely that alerts issued to home-users would be more usable through the occurrence of a user response sector in the bottom of the alert interface. For instance, Norton 360 (i.e. Figure

51) and Trend Micro are considered to be the only two products that match the current criterion as they implicitly identified that the perceived intrusion access is blocked and provides a user response sector consists basically of an *Allow* and *Block* buttons. Hence, the user has the benefit of both the automatic security response and the user feature to adjust and/or confirm the response.

By contrast, Figure 52 illustrates a different example of Norton's alert interface which does not match the mental model criterion because the alert does not include a description of the cause of the alert, or any links or tooltips to provide the user with more information.

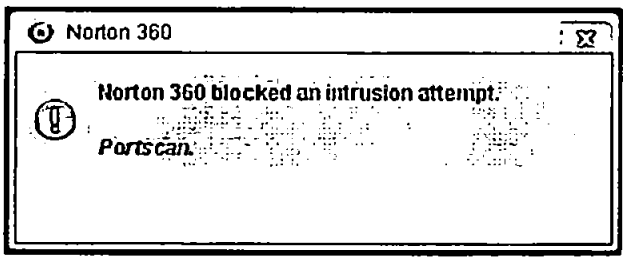


Figure 52: Norton 360 notification intrusion alert

6.2.2 Aesthetic and Minimalist Design

It is desirable that the design of the alerts should be aesthetic and minimalist. However in some cases they are too minimalist, with examples from Security Shield and BitDefender shown in Figure 53. In these cases the source of the intrusion should be identified to the novice in a more meaningful manner (as they are unlikely to be greatly informed by the IP address), the is could take place by adding a tooltip identifying the meaning of the IP address to novice user, whereas more informed users may be interested in additional options (such as the opportunity to suppress further notifications).

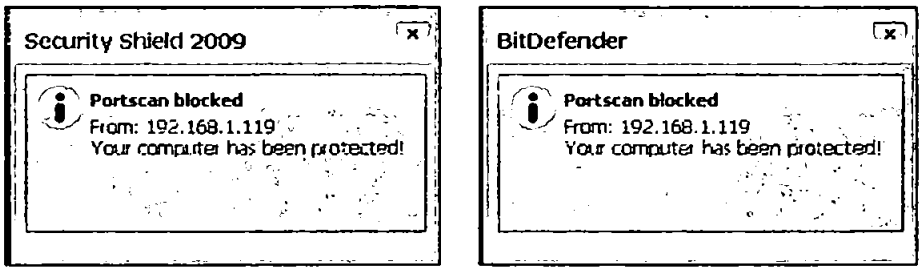


Figure 53: Security Shield & BitDefender alerts interfaces

6.2.3 Visibility of the Alert Detector Name

With the exception of Webroot, all of the security tools provide the name of the detector in the head of their alert interfaces. Instead of indicating the name of the product suite (i.e. the thing that the user may most likely recall installing or recognise that they are running), Webroot's alert is attributed to the firewall, as shown in Figure 50. Of course, many of the Internet security suites consist of integrated security solutions based on underlying components such as anti-virus, anti-spyware and firewall, and so it is perhaps not surprising that alerts appear under the name of these components rather than that of the wider suite. However, it would still be useful for the vendor name to appear so that the user has a basis for making the association back to the product they recognise. This, for example, is the approach with the CA product, where rather than indicating 'CA Internet Security Suite Plus' the alert identifies 'CA Personal Firewall', as shown in Figure 54. From the current criterion perspective, the advantage of the CA alert is that the name of the vendor is visible to the user, whereas in the Webroot alert the vendor name is completely absent. The problem with the rather anonymous alerts shown in Figure 50 is that the user may wonder if they were caused by something else (e.g. issued by the Windows firewall or faked by malware).

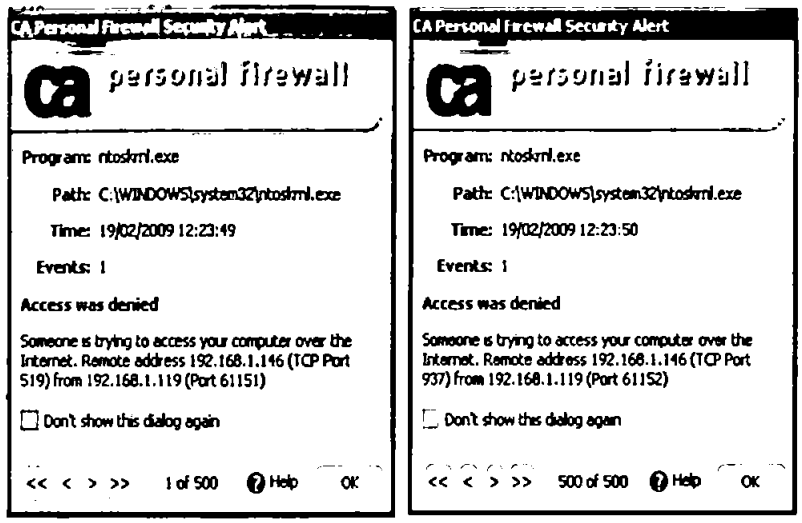


Figure 54: CA alerts interfaces

6.2.4 Establish Standard Colours to Attract User Attention

The use of standard colours to express information to home-users in a simple and rapid way should be considered and addressed better to improve the design of home-users alerts. With the exception of the traffic light colours, there are almost no other standard colours to represent the alert severity. Therefore, most likely, the use of the green colour indicates that the system status is secure, the use of the yellow colour indicates a low risk level and the red colour indicates a high risk level. The methods for adopting colours to support the message of the alert vary among the evaluated products such as the colours within icons, the border and the background colours. For instance, Norton 360 and F-Secure used yellow in the exclamation icon to indicate the risk level of the detected activity. In contrast, Panda used the red colour within the 'No Entry' symbol to indicate that an intrusion attempt is blocked. However, it is noticed that the border colour of most of the studied alerts are blue apart of Norton and Webroot's that are yellow and green, respectively. The use of the blue border could be significant in case that these products are adapting a standard colour-coding such as the Homeland Security Advisory System (HSAS), where a wider range of colours are adopted (i.e. green, blue, yellow, orange, or red) to determine the severity of the threat level (Siraj and Vaughn, 2007). Finally, despite

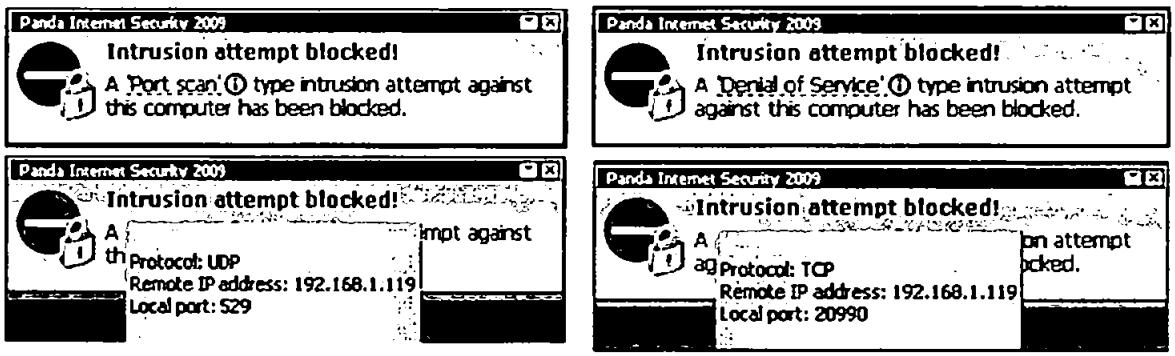
Webroot's serious alert limitations (as it does not use any explicit words to determine what happen after the detection of the scan activity), it is arguable that the green colour provides a secure impression to the home-user. Therefore, it is recommended to design home-users alerts that have an appropriate border colour as an indicator to the threat level, and to avoid insignificant and misleading ones.

6.2.5 Use Icons as Visual Indicators

The use of icons as visual indicators should be essential, relevant and significant. Likely, home-users receive the primary alert message through the colours and icons. Then, the message requires explicit words within the alert interface to confirm the acquired message. For instance, both F-Secure and Norton 360 (i.e. Figure 51) use an exclamation mark icon as a visual indicator to indicate an intrusion attempt. Most likely, the yellow colour used within the icons indicates a low threat level. Unlike F-secure, Norton 360 alert confirms that indication explicitly through assigning *Risk Level: Low* within a secondary alert interface. Meanwhile, Panda does not use the exclamation icon but instead it uses the 'No Entry' symbol aligned with a padlock icon, as shown in Figure 55, to indicate that an intrusion attempt is detected and blocked. However, it is suggested to deploy appropriate icons that does not contradict criterion 4, *Establish Standard Colours to Attract User Attention.* Furthermore, Security Shield, BitDefender and Trend Micro, use the information mark icon at the top-lift of the main alert interface. Arguably, there is no significant benefit from using this icon as an indicator. Therefore, it is recommended not to use unnecessary icons that contradicts criterion 2; *Aesthetic and Minimalist Design.*

The former metaphors demonstrate several instances of accommodating icons on the top-left of the main alert interface. Icons could also be located in other position within the alert, CA uses the question mark icon aligned with the word *Help* as an indicator. The accommodation of the

icon at the bottom of the alert should be relevant as the home-user already scanned the alert content and hence the user might seek for help. Unfortunately, the result of the *Help* link is not as expected because the link provides no specific information relevant to the present alert. Hence, as although having such a visual indicator could be useful for the user, it could also be misleading. Finally, as shown in Figure 55, Panda is the only product that uses two methods for deploying icons in the alert interface; the information mark icon is used within the content of the alert next to the technical term *Denial of Service* to indicate that there is more information if required. The use of this icon is relevant and it would be more usable if the icon colour is more visible such as blue.



a) a port scan intrusion attempt **b) a denial of service intrusion attempt**

Figure 55: Panda Internet Security 2009 alert interfaces and tooltips

6.2.6 Explicit Words to Classify the Security Risk Level

This criterion identifies one of the remarkable limitations within the design of the studied alerts. With the exception of Norton and Trend Micro, none of the evaluated products explicitly classify the security risk level. Norton 360 (i.e. Figure 51) determined the security risk level information in a complementary interface. The information is obtained through selecting the *Show Details* link within the main alert interface and the security risk level is declared as *Risk Level: Low.* Meanwhile, Trend Micro is more explicit by determining the security risk level in the main alert interface as the *Risk* is declared to be *Safe.* However, assigning the risk in the current alert to be 'safe' raises a question of the benefit of issuing the alert in the first place.

From the usability perspective, addressing the optimal location for assigning the security risk level is required. Therefore, it is recommended to present the risk level explicitly in the alert main interface, and then offer the associated reason for assigning this classification within a secondary interface.

6.2.7 Consistent Meaningful Vocabulary and Terminology

In general, the sentence(s) in most of the security alerts are simple and short, but there is no guarantee that the words used in these sentence(s) are familiar to the user. For instance, Panda used the term 'denial of service' in the main alert interface aligned with a tooltip, but the provided information is neither a description nor a definition for the technical term. Firstly, as most of the products make security decisions on behalf of the user, the user's main concern is likely to be whether the product that raised the alert has managed to deal with the problem or not. The words 'denied' and 'protected' are used in a few alert interfaces to describe the product's response, but the most dominant word is 'blocked' (as in '*Intrusion attempt blocked!*') and the use of the exclamation mark at the end of the sentence to emphasize the content is pleasant. However, the methodology of locating the former instance as the first sentence in the alert body content as shown in Figure 55, would satisfy an amount of novice users who might decide not to run through the rest of the alert. In contrast, BitDefender and Security Shield alerts use the sentence '*Your computer has been protected!*' to emphasize that the product had successfully protected the user from a security threat but the location of the sentence was in the bottom of the alert. Secondly, the focus of analyzing this criterion was upon assessing the terminology within the alerts that requires the user interaction. It was found that the terminology within those alerts, Trend Micro's and Norton 360 (i.e. Figure 51), does not impede the home-user from making a security decision. Finally, from a scientific perspective, CA as shown in Figure 54 is the only product which does not completely satisfy the current criterion mainly because it is strange that the victim IP address is classified as a remote address

in the alert interface (i.e. a serious mistake), while the attacker is classified correctly as a remote address within the *Log Viewer* of the product.

6.2.8 Consistent Controls and Placement

Most of the alert interfaces do not supply users with explicit control features. F-Secure provides buttons that enable the home-user to investigate the alert. Meanwhile, the alert interfaces generated from Norton 360 (i.e. Figure 51) and Trend Micro consists of feasible control components located at the bottom of the alert interface. The location of the response buttons (*Allow* and *Block*) is appropriate as a logical assumption that the user reaches the buttons after running out through the alert content. The main limitation of these buttons is that there is no indication of whether the impact of the user action is temporary or permanent. One solution could be appending another two buttons to alert design and assign explicitly the impact on the buttons such as *Allow Once* and *Allow Always*. A further solution is to make benefit of criterion 5, *Use Icons as Visual Indicators*, and criterion 9, *Learnability, Flexibility and Efficiency of Use*, via appending a small information mark icon next to each button and that icon access an explanatory tooltip that clarify the impact of the button.

6.2.9 Learnability, Flexibility and Efficiency of Use

The use of explanatory tooltips for concepts that appears in the alert window and/or the adoption of links to Internet web page are rare among the evaluated security alerts. For instance, the Panda alert interfaces from Figure 55 include the terms 'Port scan' and 'Denial of service', both of them are linked with an explanatory tooltips but neither of them provides detailed information of the nature of the attack and instead of that they determine the protocol, the remote IP address and the ports used in the attack. Furthermore, as shown in Figure 56, Kaspersky includes the link → *View report* within the bottom of the main alert interface, but the report does not provide the user with extra information and the report only includes the

same information of the main alert in a more organized style. The alert interfaces of Kaspersky and Panda share the same feature of having a drop list in the title bar at the top-right of the main alert interface. Kaspersky provides the user with a drop list consists of three options *Disable this notification*, *Disable all notifications* and *Settings...*. Meanwhile, Panda's list consists of two elements, *Help* and *Non-serious message settings*, with the *Help* option guiding the user to access a general built-in help and its introductory interface explains that the intrusion attempt is blocked via the built-in firewall. Therefore, relocating these features from the drop list to a better location within the alert interface (such as the bottom of the alert) would be more visible and useful.

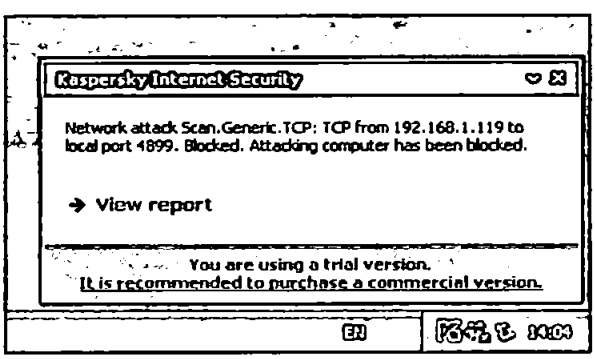


Figure 56: Kaspersky Internet Security alert interface

6.2.10 Take Advantage of Previous Security Decisions

While all of the previous criteria were addressed by at least some of the evaluated security alerts, none of the products explicitly enabled users to leverage previous decisions to help them cope with the current alert. Therefore, the focus is upon assessing the alerts that required the user interaction such as Trend Micro's and Norton 360 (i.e. Figure 51). These products do not impede the home-user from making a security decision as the products already perform a blocking decision, identify the security risk level and provide response buttons. The novice user who does not have an experience with the cause of the present alert and does not have any further advice to call upon might find it more secure to implement the alert default response as

these products did not specify any explicit recommendation to follow, such as accompanying the *Block* button with the word (recommended).Therefore, it is worth establishing an alert history that stores the user's previous decisions, to provide a source of reference if a similar alert arises in the future. Furthermore, it is suggested that the use of the social navigation method (Chiasson et al. 2007), would enrich the alert and to some extent support the user. Social navigation is considered to be a promising method in guiding novice users to make security decisions based on relevant individual decisions from those who have previously encountered similar alerts in their own environments.

6.2.11 Online Security Policy Configuration

This criterion is interested with integrating security policy features within the design of the alert itself. There are some attempts to provide this feature within some of the evaluated security products. For instance, CA and F-Secure provide a check box alongside text to the effect of '*Don't show this alert dialog again*'. Meanwhile, the Trend Micro alert, as shown in Figure 57, is more specific in using a check box aligned with the text; *Stop warning about this program.* Since the name of the program occurred in the main alert, the user's decision is clearly affecting future events involving this program whatever the source IP address, while in the previous alerts it is not clear whether the decision affects the program or the IP address or the port or all the alerts. Another advantage of the Trend Micro version is that the checkbox is ticked by default, so that the product is giving an explicit recommendation to the novice user. In contrast, Panda and Kaspersky adopt a different type of online configuration by providing a drop list contains the element *Non-serious message settings* option which consists of a variety of checkboxes to adjust the events that pop-up the alerts. Moreover, Kaspersky provides the options *Disable this notification, Disable all notifications* and *Settings...*, but the impact of the first option is unexplained to the user. As such, they may be unclear about whether the impact of selecting this option is to disable the future similar alerts (i.e. with the same details), to

disable all alerts associated with the same type of attack regardless of the source, or to perform some other action. The previous examples are not the expected level of online security policy configuration and need to be enhanced as the exact impact of some options were not completely clear to users and some other options were irrelevant (i.e. related to configuring other types of notifications that are not correlated to the current alert) which overloads the user with unnecessary secondary security issues at an inappropriate time. However, they are the only available examples in this study and one of the suggestions to make this criterion valid is providing an option in the alert to avoid triggering of frequently low level security alerts.

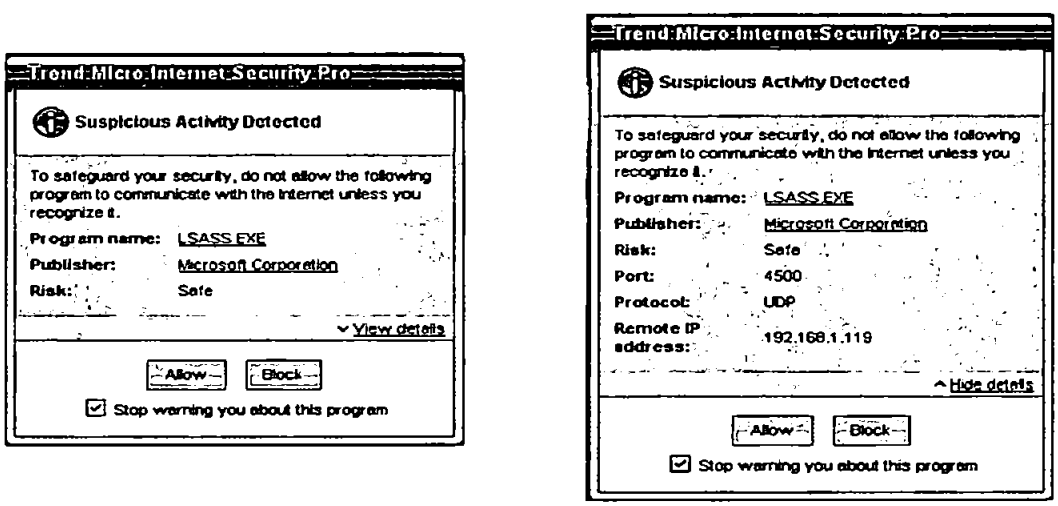


Figure 57: Trend Micro Pro alert interface

6.2.12 Confirm / Recover the Impact of User Decision

Confirming and recovering the impact of home-users decisions is the second HCI-S usability criterion that is not addressed amongst the evaluated products. The absence of this criterion is illustrated by assessing Norton 360 (i.e. Figure 51) and Trend Micro, which provide control buttons that implement user's responses immediately without warning or reminding the user of the response impact, neither before nor after making the decision. Furthermore, there is no obvious method that informs the user of how to recover from wrong or inappropriate decisions. It is suggested that the security measure should issue a confirmation message after the user performs the response decision. The objective of the message is to display the user current

decision and the perceived impact, and whether the user prefers to proceed accomplishing the decision or return back to main alert interface to alter the response. However, the current suggestion combines both the benefit of confirming the user decision and a primary recovery method. Moreover, in some cases the user might perform inappropriate decision that affects the functionality of their intended tasks. Therefore, developing usable methods to recover from undesired decisions is a requirement. A suggested solution is to make benefit of criterion 10, *Take Advantage of Previous Security Decisions*, where all the previous user decisions are stored to be used when required. Hence, the user could access the recently issued alerts and the corresponding decisions, and attempt to change a previous decision if possible (e.g. if the user subsequently wishes to allow a program that was previously blocked by mistake). Furthermore, embedding an icon within the Windows notification area, next to the product icon in the tray, could be a primary method to access the recent alerts. Finally, the product can make use from criterion 4, *Establish Standard Colours to Attract User Attention*, and decrease the possibility of the recovery situations by appending a green border around the recommended response button.

6.2.13 Awareness of System Status all the Time

This is the third HCI-S usability criterion that is not fully addressed through the evaluated products. Most likely, home-users who installed security measures within their personal computers presume that the security situation is under control and there is no need to worry until they receive a security alert. When that happens, most of the evaluated security alerts declare that an intrusion attempt is detected and blocked. Hence, this is the type of awareness of the system status that these products provide to the user who will subsequently believe that he/she is protected. Meanwhile, as mentioned earlier, the McAfee product did not issue any alert during the evaluation, even though that the logs confirmed that it managed to detect the incoming traffic from the attacker computer. Hence, the user is not aware of the system status

based on McAfee security policy. It is noticed that some products, such as Security Shield and BitDefender, pop up alerts that disappear quickly without the user's permission. Hence, there is a high possibility that the users would not notice the occurrence of the threat, especially if they were not looking at the screen at the time. If it is considered acceptable for users to miss them, then it questions the necessity of displaying the alerts in the first place. Furthermore, Norton 360 (i.e. Figure 51) and Trend Micro, which provide a response capability, do not inform the user with the impact of the response issued by the user. The user ought to receive a message informing him about the real impact of his response. Therefore, the awareness of the system status all the time is not available. For instance, if the user decided to use criterion 11, *Online Security Policy Configuration*, and disabled the appearance of all alerts, it would be useful to get the product icon in the notification area to produce yellow, orange, red pulses as the occurrence of low, medium, red security risk levels, respectively.

6.2.14 Help Provision and Remote Technical Support

The generated alerts by most of the security tools do not need real help provision or remote technical support; not because of their completeness, but because of the lack of user decision responsibility. Meanwhile, Panda and F-Secure provide a built-in help which might be useful to enhance user knowledge but it does not support the user response since there are not any response controls in the alert interface. In addition, the location of the help in Panda is not appropriate since it is embedded in a drop-down list, in the title bar, in the top-right of the main alert interface. In addition, CA uses the question mark icon as a visual indicator aligned with a help link to attract the user but the link provides no specific information relevant to the present alert. The assessment of the alerts generated by Trend Micro and Norton 360 (i.e. Figure 51), the two products that provide control features, reveals that no help or remote support is provided within Trend Micro apart of the explicit risk level is determined as *Safe*. Meanwhile, Norton 360 is considered to be the only product that satisfies the criterion, as it provides a

variety of help provision and remote support to the user. From a usability perspective, the main limitation is in the location of the options. For further details, an extensive discussion of Norton 360 is available within Chapter 5.

6.2.15 Offer Responses that Match User Expectations

This is the final criterion that is not fully addressed through the evaluated products. Firstly, most the security tools in the evaluation do not provide a user response component in the alert interface. Arguably, a portion of users would find it appropriate to have response options within the alert design. Secondly, Norton 360 (i.e. Figure 51) and Trend Micro are the only two products which satisfy this feature and the assessment of the generated alerts reveals that there is no obvious method provided for the user to assess whether the response matches their expectation or not. Those users who have the privilege to respond to the alert perform their actions based upon their individual understanding. It is suggested to raise an explicit message after the user response to identify the real impact of the response. Hence, the user will be able to determine whether the response has achieved what they expected.

6.2.16 Trust and Satisfaction

In all likelihood, security products that managed to address most of the former HCI-S usability criteria are also able to satisfy and obtain the trust of users. Looking at specific factors that may improve this potential, we can consider whether the user is likely to feel they are getting the extent of information and feedback that seems convincing. For example, the design of the security alerts of Norton 360 and F-secure provide users with a level of satisfaction because of the amount of relevant information they attempt to provide. For instance, as shown in Figure 58, the main interface of F-Secure provides *Details* >> button which let the user access more information about the cause of the alert and the user can access the alert logs through the *Show Alert log* button in a secondary detailed interface.

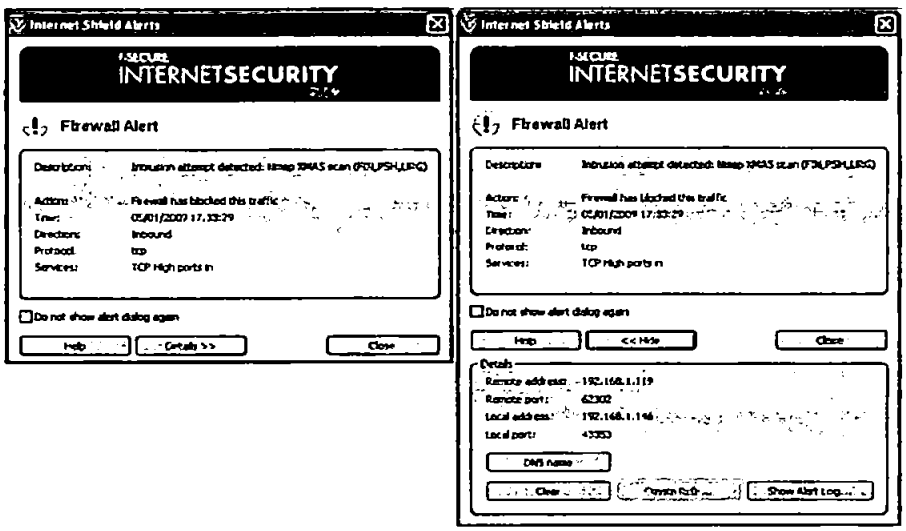


Figure 58: F-Secure Internet Security 2009 Firewall Alert

6.2.17 Summary results

Table 8 summarizes the findings across the full set of tools and criteria. During the evaluation, Norton 360 generates two different types of alerts. Therefore, the results of the assessment of the two interfaces are illustrated in two rows aligned with each usability criterion, whenever that is required, the first row represents the assessment of the alert represented in Figure 52 and the second one is related to the alert in Figure 51.

The findings reveal a remarkable limitation that choosing the *High* setting of the firewall alerts within the CA product bombards the home-user with hundreds of alerts and the maximum number of alerts that are accessible in the alert interface is 500, as shown in Figure 54. Most likely, the home-user will dismiss these alerts instead of suspending the intended task to investigate the massive amount of alerts. From a usability perspective, it is impractical to overwhelm the user, in one second, with this amount of alerts specially that they only vary in detailed information of hundreds of local and remote ports used during the penetration. From the usability perspective, although the use of the *Show Details* link within Norton 360 (i.e. Figure 51) is usable, it would be more preferable to avoid using the

vertical scroll bar within the complementary interface. Finally, the chapter demonstrated to what extent the HCI-S usability criteria are addressed through the evaluation of collection of home-users security products. The findings reveal the strength and the weakness within the design of the issued alerts and some primary solutions are suggested as an attempt to resolve these weakness. It is anticipated that integrating the adequate features of the evaluated alerts, avoiding their limitations, and implementing the unaddressed HCI-S usability criteria, will enhance the alert design and make it more usable for home-users.

No	Novel Criteria	BitDefender Internet Security 2009	CA Internet Security Suite Plus 2009	F-Secure Internet Security 2009	Kaspersky Internet Security 2009	Norton 360 Version 2.0	Panda Internet Security 2009	Security Shield 2009	Trend Micro's Internet Security Pro 2009	Webroot's Internet Security Essentials
1	Design Interfaces Match User Mental Model	✗	✗	✗	✗	✗ ✓	✗	✗	✓	✗
2	Aesthetic and Minimalist Design	✗	✓	✓	✗	✗ ✓	✓	✗	✓	✗
3	Visibility of the Alert Detector Name	✓	✓	✓	✓	✓	✓	✓	✓	✗
4	Establish Standard Colours to Attract User Attention	✗	✗	✓	✗	✓	✓	✗	✗	✗
5	Use Icons as Visual Indicators	✓	✗	✓	✗	✓	✓	✓	✗	✗
6	Explicit Words to Classify the Security Risk Level	✗	✗	✗	✗	✗ ✓	✗	✗	✓	✗
7	Consistent Meaningful Vocabulary and Terminology*	✓	✗	✓	✓	✓	✓	✓	✓	✓
8	Consistent Controls and Placement	✗	✗	✗	✗	✗ ✓	✗	✗	✓	✗
9	Learnability, Flexibility and Efficiency of Use	✗	✗	✓	✓	✗ ✓	✓	✗	✓	✗
10	Take Advantage of Previous Security Decisions	✗	✗	✗	✗	✗	✗	✗	✗	✗
11	Online Security Policy Configuration	✗	✓	✓	✓	✗	✓	✗	✓	✗
12	Confirm / Recover the Impact of User Decision	✗	✗	✗	✗	✗	✗	✗	✗	✗
13	Awareness of System Status all the Time	✗	✗	✗	✗	✗	✗	✗	✗	✗
14	Help Provision and Remote Technical Support	✗	✗	✗	✗	✗ ✓	✗	✗	✗	✗
15	Offer Responses Match Expectations	✗	✗	✗	✗	✗	✗	✗	✗	✗
16	Trust and Satisfaction	✗	✗	✓	✗	✓	✗	✗	✗	✗

* With the exception of the terminology that requires the assistant and the adoption of criterion 9 in some instances, the current criterion is rated according to the meaningful vocabulary to the end-user.

Table 8: The usability aspects of the security software

From the current study it is possible to adjust a primary ranking for the HCI-S usability criteria into groups (Low, Medium, and High) as shown in Table 9. Criteria rated as Low as

those that mainly relate to the user's ability to feel comfortable using the tool. Meanwhile, Medium-rated criteria are those affecting the user's ability to understand status and events. Finally, High represents those factors that influence the user's ability to make the right decisions; if they get this wrong it is the bit that has the most adverse impact on the actual security of their system.

Low
Aesthetic and Minimalist Design
Visibility of the Alert Detector Name
Establish Standard Colours to Attract User Attention
Use Icons as Visual Indicators
Trust and Satisfaction
Medium
Design Interfaces Match User Mental Model
Consistent Meaningful Vocabulary and Terminology
Consistent Controls and Placement
Learnability, Flexibility and Efficiency of Use
Online Security Policy Configuration
Awareness of System Status all the Time
High
Explicit Words to Classify the Security Risk Level
Take Advantage of Previous Security Decisions
Confirm / Recover the Impact of User Decision
Offer Responses Match Expectations
Help Provision and Remote Technical Support

Table 9: HCI-S Usability Criteria Ranking

In addition to the primary considerations listed above, the categorization of individual criteria may also be influenced by secondary considerations such as prioritising those issues that the user will encounter most frequently, or which could have the biggest adverse impact on their ability to use a product correctly. For example, the fact that it will be an ever-present issue could elevate the 'Trust and Satisfaction' point from being ranked Low to being ranked as Medium.

6.3 Conclusions

This chapter investigated the usability of security alerts issued via a range of security products. These alerts are triggered as a result of performing a penetration test conducted within a test-bed environment using the network scanner Nmap. The findings reveal that the trend of most of

the security software vendors is to respond to the security threat on behalf of the end-user. This is understandable, especially as end-users might not have the relevant security background to make informed decisions, or they might prefer to focus on their primary intended tasks instead of secondary security ones. The analysis of security tools according to the HCI-S usability criteria showed that four of the HCI-S usability criteria (10, 12, 13, 15) are not addressed in any of the selected security measures.

Specifically, none of the evaluated tools address criterion 10, to Take Advantage of Previous Security Decisions. Therefore, it would be desirable for a system to consider the user's previous decisions on similar alerts, and modify alerts accordingly to account for the user's previous behaviour. For example, if the user has consistently overridden the recommended option in a particular type of alert, the system can change the default option to the user's previous choice, or it can offer the user the option to repeat their decision in future occurrences, without the need for an alert. In order to give users this level of flexibility, it is important to enable them to make informed decisions, and to be able to recover from them if needed. Therefore, it is important to address criteria 12, 13, 15 as well (namely Confirm / Recover the Impact of User Decision, Awareness of System Status all the Time, and Offer Responses Match Expectations). Therefore, the next chapter focuses upon addressing these missing HCI-S usability criteria and increasing the end-user's opportunity to customize the security measure.

Chapter 7

Enhancing the Usability of End-Users Security Tools

7 Enhancing the Usability of End-Users Security Tools

The aim of this chapter is to address the four missing HCI-S usability criteria that were not fully covered by the investigated security products in the previous research. This chapter begins by suggesting solutions to address these criteria and then presents a case study experiment to assess the proposed solutions from the end user perspective. Actually, there are other several benefits could be obtained from the case study apart from assessing the proposed solutions for the unaddressed HCI-S usability criteria by the previously investigated security products. It will be a valuable opportunity to assess and validate the whole proposed HCI-S usability criteria, from the end user perspective, through a practical implementation.

7.1 Addressing HCI-S Usability Criteria

In this section a new security alert is designed to meet the requirements of the HCI-S usability criteria especially those who were not addressed in the previous chapter. The new design is an attempt to address the limitations within the selected set of security products evaluated in the previous chapter. The new design is not a fully functional system, but rather an operational prototype that was designed with the specific aim of allowing users to interact with particular features and provide feedback about them. The new design managed to also enhance some of the other criteria. For instance, as shown in Figure 60, the yellow border of the main alert interface alerts the user that the risk level is not high which support criterion 4; *Establish Standard Colours to Attract User Attention.* Meanwhile, *Explicit Words to Classify the Security Risk Level*, criterion 6 is satisfied in the main alert interface and supports the user to click on the recommended response, *Block Once*, which has the green colour. The current section focuses on enhancing the usability of security alerts that end-users face in a real environment. The nature of the project is that the user faced alerts in different scenarios and was asked to make decisions on how to handle them. The user responses were saved for further analysis, to

determine the benefits of the proposed interface. The project aims to evaluate some of the proposed solutions that make the security alert more usable for the end user.

The participants were briefed about the purpose of the study and then they were asked to answer a series of questions, which are grouped into the following 3 sections:

1- Demographic questions

2- End-user perception of security

3- Assessing the usability of new security interface

The above three groups are explained in the following sections. 31 participants volunteered to share in the case study. The demographic questions reveal that the gender of the participants is 83% Male and 17% Female. Meanwhile the age of the participants was in the range from 18 to 40 years old. The level of education they have already obtained is 13% Post 16 Education (e.g. A-levels, NVQ),17% Bachelor,70% Masters. The next question was about the numbers of years they had been using Internet and varies between 4 and 15. Only three participants mentioned that there experience is over 15 years. The participants were asked about their security expertise. The participant's answers were 3% Excellent, 53% Good, 33% Average, 3% Fair, 7% Poor. Moreover, the participants were asked about the rate of the current security solution on their computer. The participant's answers were 7% Excellent, 63% Good, 23% Average, 3% Fair, 3% Poor.

7.1.1 End-user perception of security

The participants received a questionnaire consisting of several questions starting with asking the user of selecting the types of security software that they use in their systems. 42% selects Integrated Security products (combining Antivirus, firewall, intrusion detection, etc.), 51%

Antispyware, 58% firewall, 3% None, 0% I do not know. The vast majority 74% use Antivirus product on there PC while only 19% use intrusion detection. The final result indicates that average users tend to use an Antivirus rather than intrusion detection. Arguably, Antivirus is more desirable because the ease of use of Antivirus products.

The second question interested with which Internet application do they use. 32% selects Peer to peer software (e.g. Gnutella, Kazaa, BitTorrent, etc), 83% Instant Messaging (e.g.Windows live messenger) 93% Email (e.g.Outlook), 100% Web browser (e.g. Internet Explorer, Safari, etc). The findings indicate that the user always needs a security product that protects him/her from malicious website as the users use a web browser on a regular basis.

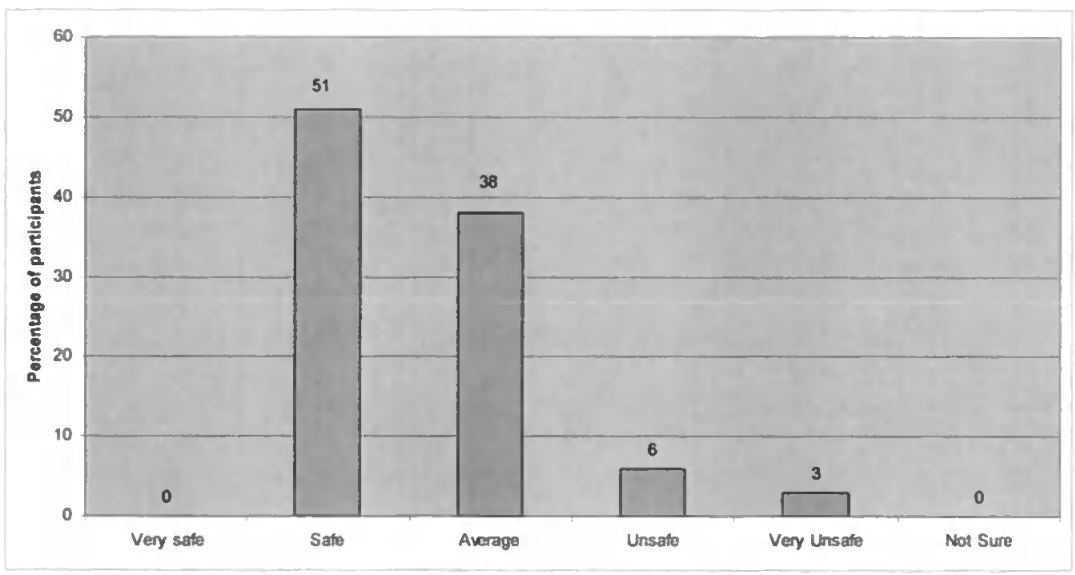


Figure 59: How safe do users feel their computers are against security breaches

The third question asks about how safe do they feel their computers are against security breaches. The participants answers were 0% Very Safe, 51% Safe, 38% Average , 6% Unsafe , 3% Very Unsafe , 0% Not Sure. Although the high number of security threats that counter the end-users every day, Figure 59 shows that more than half of the participants declared that they are safe.

The fourth question asks about how often do they encounter security alerts. The participants answers were 19% Daily, 19% Weekly, 13% Monthly, 45% Rarely, 3% Never.

The sixth question asks about the type of information that they think security alerts should have. The participants answers were 55% Log details of activity, 71% Information about the origin of the event, 90% Explanation for incident. The proposed alert attempts to provide this explanation in a simple method in the first sector of the alert interface, namely, Detected.

The seventh question asks about the participant's ability to configure the settings of their security software. The participants answers were 3% Excellent, 45% Good, 29% Average, 9% Fair, 13% Poor.

The eighth question asks if they experienced any security breaches in the past 5 years. The participants answers were 61% Yes, 32% No , 6% Not sure. Those who answered with 'Yes' received another question to identify the type of incident that they encountered. The participants answers were 61% Infection with malicious software (e.g. virus, Trojan, spyware, etc), 29% Adware, 3% Stolen password, 6% Stolen credit card details, 3% Denial of service, 3% Scan for vulnerable services. Although, the participants were randomly selected at least one of them experienced one of the selected security breaches. Hence, more research need to be done on protecting end-users and this research is a step towards achieving this aim as follows in the next sections.

7.1.2 Security Alert Encountered by End-user (Task One)

This is considered to be task1 that the user had to accomplish. The participants were told that a security alert, as shown in Figure 60, would be displayed after a few seconds and they were

asked to respond to the alert as they would do in a real environment. Then the participants received a questionnaire and they have to answer the questions.

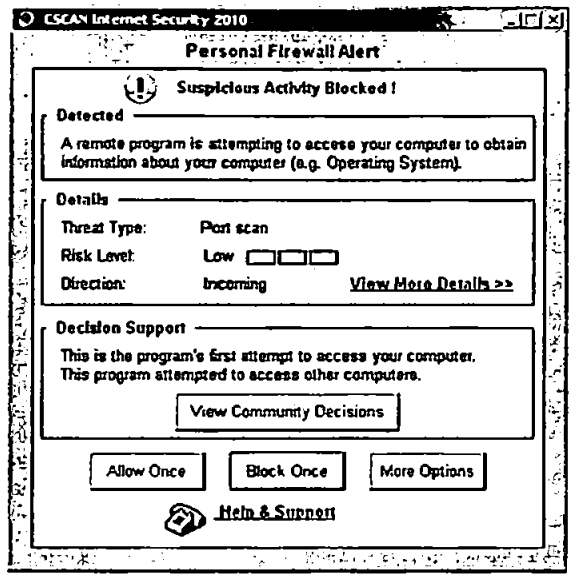


Figure 60: CSCAN main alert interface

Questions	SA	A	N	D	SD
Overall, did you feel the security alert was understandable?	6%	55%	22%	16%	0%
Do you feel the use of explicit words to determine the alert risk level is useful?	26%	58%	13%	3%	0%
Is the use of the colour border a good indicator to identify the alert risk level?	42%	42%	3%	13%	0%
When busy, would you feel safe to minimize and postpone dealing with this alert?	3%	32%	19%	39%	6%
Are the tooltips helpful in providing extra information in a flexible manner?	13%	48%	32%	6%	0%
Did you feel that the impact of the response options 'Allow Once' and 'Block Once' were understandable?	22%	64%	0%	13%	0%
Did the 'Allow Once' and 'Block Once' tooltips reveal and clarify the impact of the response buttons?	19%	39%	22%	19%	0%

Table 10: Task 1 questions

Table 10 represents the questions that were asked to the participants during Task 1 (note that the columns are headed as follows: SA – strongly agree; A – agree; N – neutral; D – disagree; SD – strongly disagree) and there was another question that is not in the table that asks the participants to identify the risk level of the displayed security alert. The participants answers were 0% Very High, 3% High, 9% Medium, 84% Low, 0% Very Low, 3% Not Sure.

During task 1 only one participant selected the option dismiss the alert (i.e. click the 'x' in the main alert interface). When the participant was asked about the reason of the behaviour, the answer was 'Because I hate these messages and several times I have run into fakes messages!'. The vast majority of the participants selected *Block Once* button. The green colour of the button attracts the users and could be the reason behind this behaviour.

Meanwhile the participant were not told to select the Help And Support option, it was noticed that during they were investigating the facilities that are provided by the security product interface, three participants select the *Help And Support* link at the bottom of the main alert interface. All of them mentioned that they prefer the occurrence of the three provided options live chat, email and phone as they give the user the opportunity to gain more information of the threat and how to deal with it.

It was noticed that few participants did not assign the risk level as low but instead one of them select the risk level to be medium and when the participant was asked about the reason he/she mentioned that the threat type is port scan which he/she consider it as medium risk not a low risk. Another one considered the risk as high, arguably assuming that if the security product triggers an alert then it should be serious.

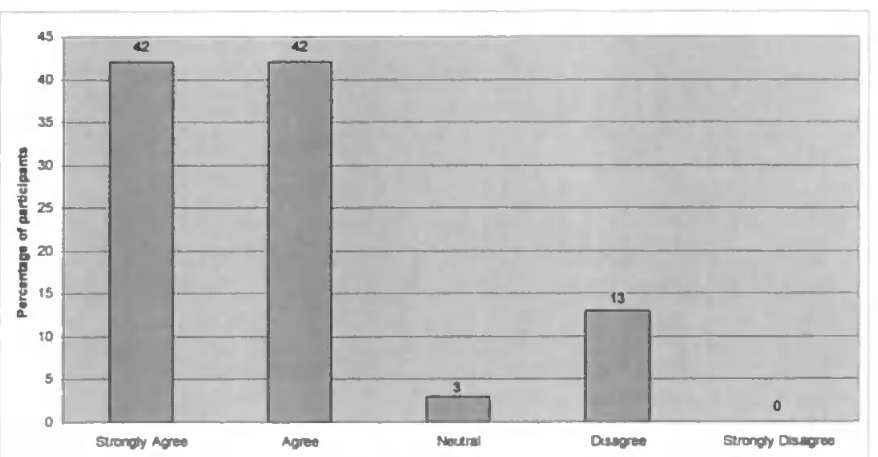


Figure 61: The colour border as a good indicator to identify the alert risk level

Figure 61 shows that the colour of the border of the security plays an important role to the vast majority of the participants in determining the risk level of the alert.

7.1.3 Security Alert Encountered by End-user (Task Two)

The same security alert that the participants experienced during Task1 was displayed again after a few seconds. The participants were told to try to find out more details about the cause of the alert. Then seek how other individuals managed to counter the same alert. Next search for other alternative responses that might match the participants expectations. Then respond to the alert after they discover the previous aspects. Then the participants received a questionnaire and they have to answer the questions.

The user can click on the link *View More Details*, if he/she requires more information about the cause of the alert. Then, the user receives this information as shown Figure 62.

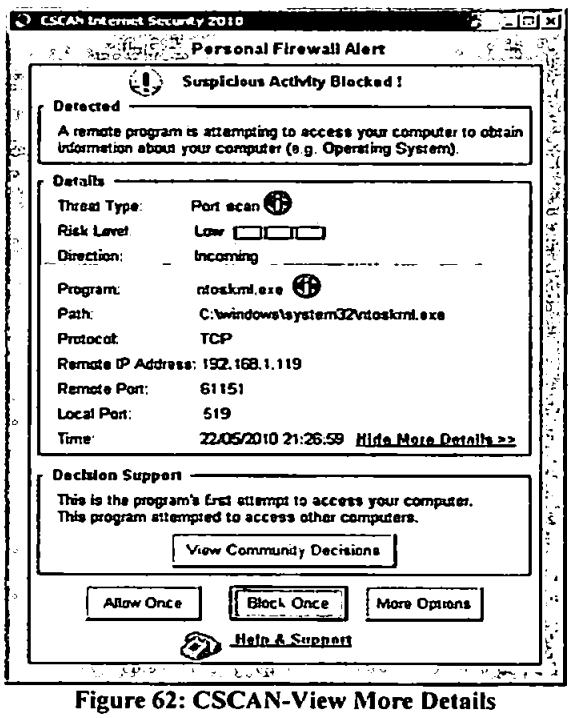


Figure 62: CSCAN-View More Details

In some situations the end-users counter security alerts but not able to deal with it. The purpose of the current criterion is to provide the user with tools that help the user to make a security

decision. The security product provide the *View Community Decisions* button, the users can click on it if they require information about how other individuals who managed to interact with the same alert in the past. For instance, the user could receive this information as shown Figure 63. This option satisfies criterion 10; *Take Advantage of Previous Security Decisions.* The solution is useful if the user had not receive this alert before. The limitation of this feature is that it could be vulnerable to attacks if an attacker runs the tool and allow the attack automatically several times. The current solution to avoid this sort of attack is that the allow option is provided with the perceived impact statement which states that the attacker managed to determine the operating system and the open ports.

The database of *View Community Decisions* could be updated centrally via a vendor or local centralisation (e.g. within the organization). The user response could be gathered and saved by the security product vendor to make benefit from it as source of information to others individuals who might counter a similar alert in the future. In the case of organizations the alert of each employee could be gathered by a security administrator who attempts to solve the problem from the core. However, the responses of the new users are collected to make benefit of them to end users.

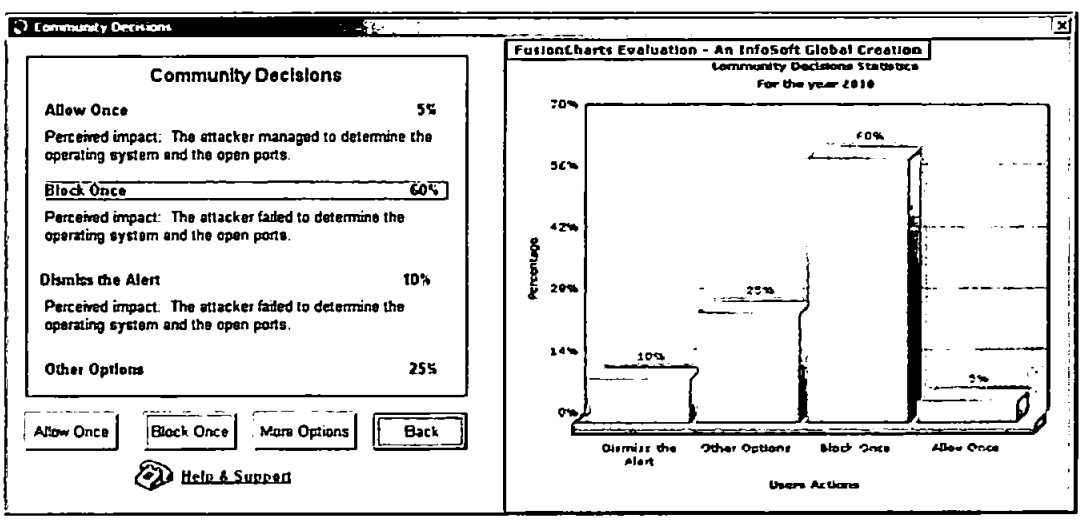


Figure 63: CSCAN - Community Decisions

In some situations, the security alert does not offer responses that match user expectations. Therefore, they do not know what action to take. The current criterion is an attempt to help the user to perform the right action. The alert main interface, as shown in Figure 60, represents the initial provided user response explicitly with a clear verbose as *Allow Once* and *Block Once* buttons. The colour *Block Once* button is green to attract the user and to emphasize that the current button is the recommended option by the security product.

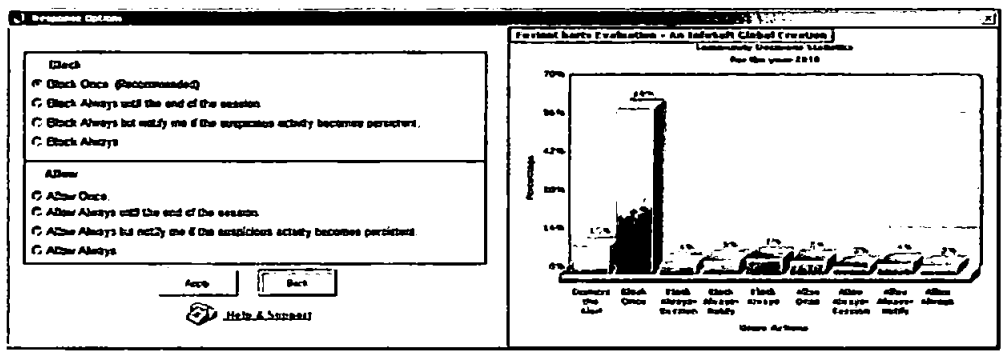


Figure 64: CSCAN-More Options

Moreover, Figure 64 illustrates an attempt to provide more response options than that was provided in Norton 360 and Trend micro is the previous chapter. This figure can be obtained if the user clicked on *More Options* button within the alert main interface.

Questions	SA	A	N	D	SD
Do you feel that some of the information provided by the 'View More Details' link, needs to be in the main interface?	3%	64%	13%	16%	3%
In general, do you like the guidance provided within the 'Community Decisions' interface?	32%	52%	9%	6%	0%
Is it useful to include the charts within the 'Community Decisions' interface?	35%	42%	19%	3%	0%
Do you feel that the impact of the response options within the 'Community Decisions' interface was clear?	32%	58%	3%	6%	0%
Did you find the additional responses within 'More Options' interface useful?	25%	71%	3%	0%	0%
Did you find the charts within the 'More Options' interface useful?	25%	58%	9%	6%	0%
Do you feel that the impact of the response options within the 'More Options' interface was clear?	25%	74%	0%	0%	0%
Was it easy to find the additional response options within the 'More Options' interface?	29%	48%	16%	6%	0%

Table 11: Task 2 questions

Table 11 represents the questions that were asked to the participants during Task 2. There is another two questions that is not in the table, the first asks if there are ways in which the information within 'View More Details' could be better presented or improved. One of the participants respond to this question by 'I think it is important to remember that terms like protocol, remote port, local port, and even pathway mean very little to most users. Websites must have info, as often there is a link but no knowledge on the specific threat type.'. The other question asks the participants if there are ways in which this information could be better presented or improved. One participant wrote 'I do not see the point of block once and blocked always. if it is a threat it should be blocked. this shows to me that the software that i m using is not sure about the threat and wants me to take responsibilty for an action that means nothing to me'. During answering this questionnaire the participants were advised to refer to the accompanying screenshots for reference if required.

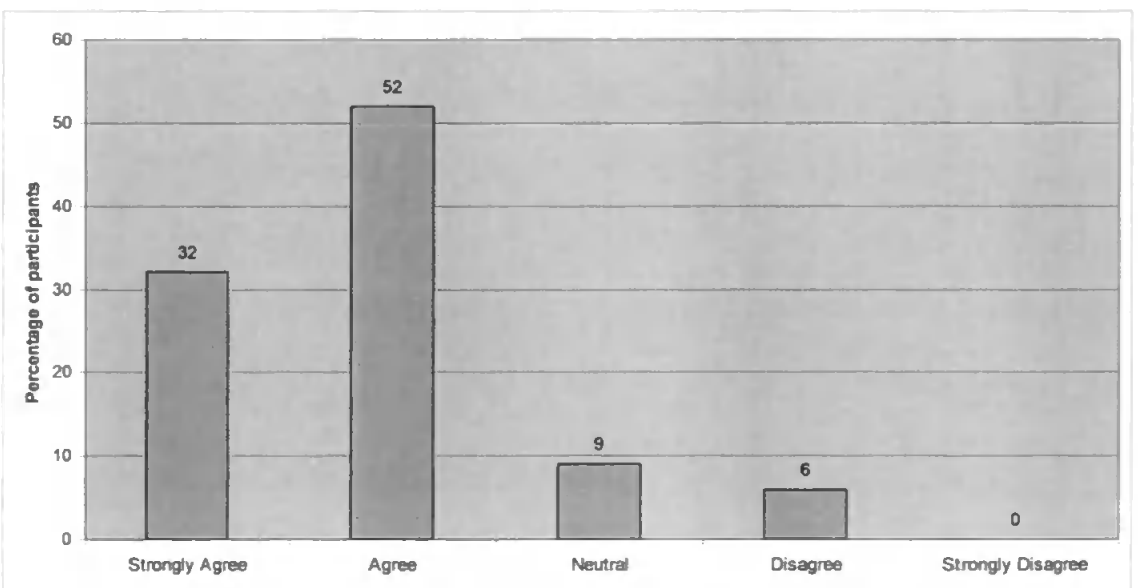


Figure 65: The guidance provided within the 'Community Decisions' interface.

Task2 is addressing criterion 10, *Take Advantage of Previous Security Decisions*, and criterion 15, *Offer Responses that Match User Expectations*. Criterion 15 is enhanced by providing the user with several options to response to the alert. Moreover it was noticed that only one

participant recognizes the benefit of the information icons in front *Threat Type: Port scan* and *Program: ntoskrnl.exe* as they guide the user to webpages which provide the user with more information. The results appear that the majority of the participants want more detailed information to appear in the alert main interface. Moreover the majority of participants like the *Community Decisions* interface which meets the requirement of criterion 10 as shown in Figure 65 . In addition, the majority of participants like the *More Options* interface which meets the requirement of criterion 15 as shown in Figure 66.

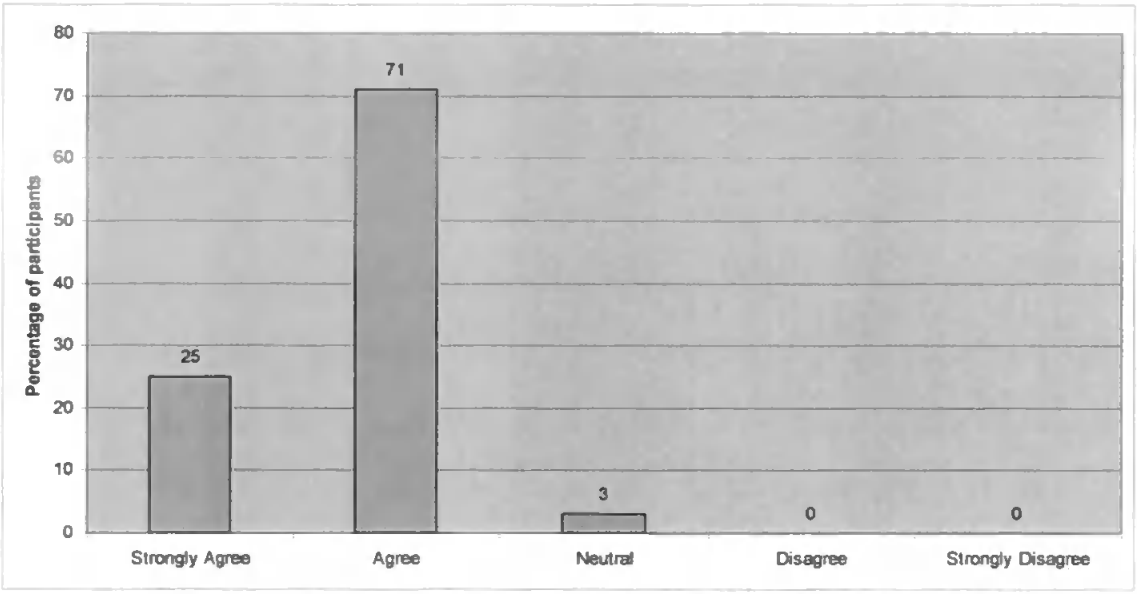


Figure 66: The additional responses within 'More Options' interface is useful.

7.1.4 Take Advantage of Previous Security Decisions (Task Three)

The following is an attempt to propose a useful feature to the users who already countered the alert in the past. In this case, the main interface will have the looking as shown in Figure 67, instead of the main interface shown in Figure 60.

If the users click on *View Your Previous Decisions* button, they will obtain Figure 68. This will let the user know his previous response to the alert and the impact of the user response on his computer.

Figure 67: CSCAN-User Previous Decisions

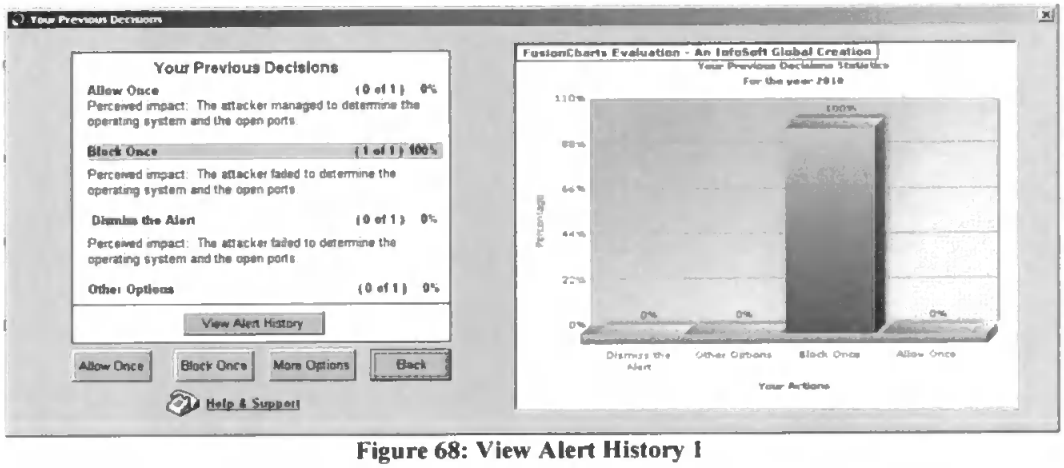


Figure 68: View Alert History 1

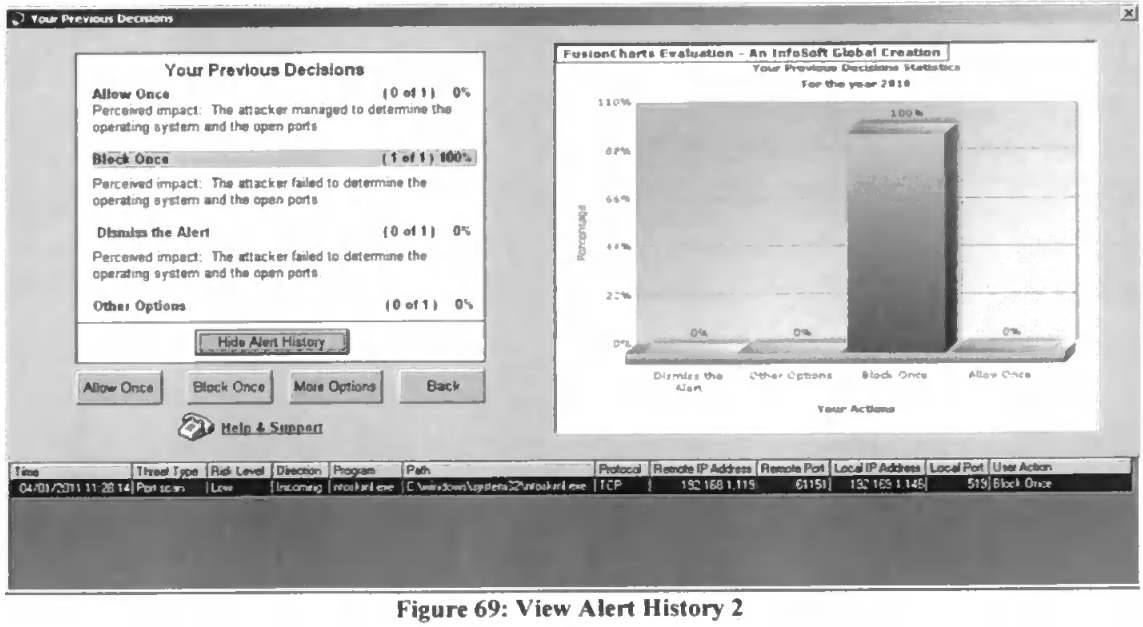


Figure 69: View Alert History 2

If the users click on *View Alert History* button, they will obtain Figure 69, which is an interface that contains more information about the threats that were detected previously.

A security alert that differed slightly from the security alert that the participants experienced in the previous task was displayed after a few seconds from running the task. The participants were told to assume that this is the second time to counter this type of alert and to assume that their previous response was 'Block Once'. Next they were told to try to find out more information about what was claimed to be their previous response. Then they were told to respond to the alert after they discover the previous aspect. Then the participants received a questionnaire and they have to answer the questions.

Questions	SA	A	N	D	SD
Was the ability to view your previous decisions useful?	32%	52%	3%	13%	0%
Did you find the 'View Alert History' option useful?	22%	65%	9%	3%	0%
Did you find the charts within the 'Your Previous Decisions' interface useful?	26%	55%	9%	9%	0%

Table 12: Task 3 questions

Table 12 represents the questions that were asked to the participants during Task 3. There is another question that is not in the table asks the participants if there are ways in which the participants feel that the 'Your Previous Decisions' interface could be improved or any other comments that they wish to make. One of the participants wrote 'have a simplified version for basic users, with an advanced mode for more experienced users'.

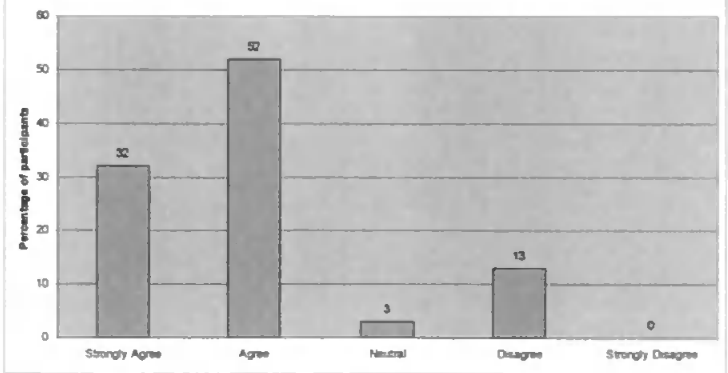


Figure 70: The ability to view the participant previous decisions is useful

Task3 is addressing criterion 10, *Take Advantage of Previous Security Decisions* but instead of focusing on the decisions taken by other individuals in similar situation it focuses on the users decisions that they had taken previously when they had already counter similar alerts in the past. The results appear that the majority of the participants like the *Your Previous Decision* interface, as shown in Figure 70, which meets the requirement of criterion 10.

7.1.5 Confirm / Recover the Impact of User Decision (Task Four)

In some situations the end-users perform a wrong action without being warned by the security product. Therefore, the current criterion is an attempt to issue a security warning if the user performed a wrong action. When the user clicks the *Allow Once* button from the alert main interface in Figure 60 and overrides the security product option the security warning will appear to the user as shown in Figure 71. This feature warns the use that his decision might be wrong and gives him the chance to confirm and correct his decision. This is considering the first protection against the user decision.

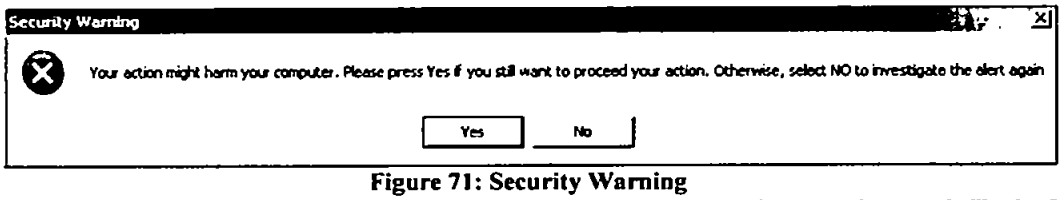


Figure 71: Security Warning

The same security alert that the participants experienced during Task1 and Task 2 was displayed again after a few seconds. The participants were told to try to override the security product recommendation, by clicking 'Allow Once'. Then the participants received a questionnaire and they have to answer the questions.

Questions	SA	A	N	D	SD
Overall, did you feel that the warning that appears after clicking 'Allow Once' was understandable?	29%	71%	0%	0%	0%
Do you feel this warning message would decrease the probability of computers being compromised?	35%	48%	3%	13%	0%
Do you feel that such warning messages can prevent users from accidentally making poor security decisions?	45%	39%	13%	3%	0%

Table 13: Task 4 questions

Table 13 represents the questions that were asked to the participants during Task 4. There is another question that is not in the table asks the participants if there are ways in which the participants feel that this warning feature could be improved or any other comments that the participants wish to make. One of the participants wrote 'Some type of 'WARNING' graphic would probably be helpful. Prehaps even a brightly coloured border in RED.' During answering this questionnaire the participants were advised to refer to the accompanying screenshots for reference if required.

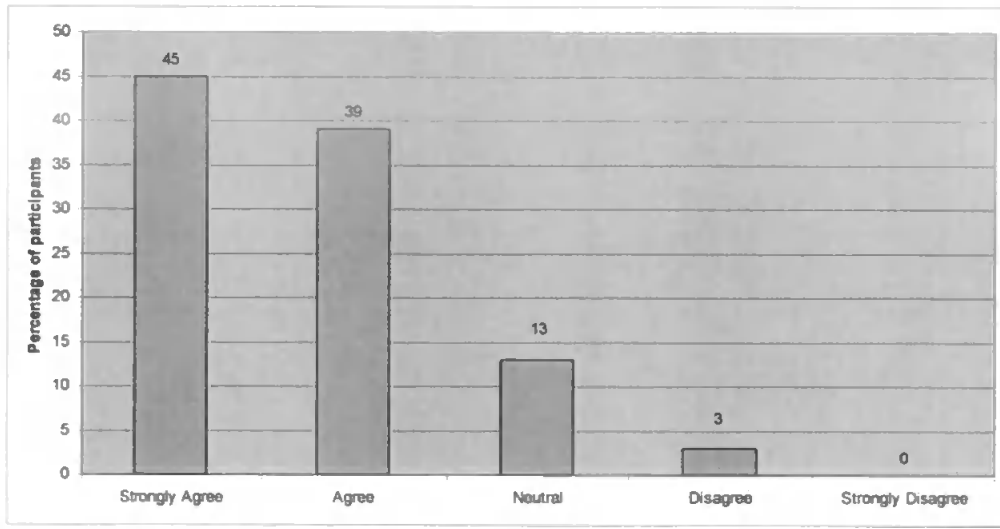


Figure 72: Warning messages can prevent users from accidentally making poor security decisions

Task 4 is addressing criterion 12, *Confirm / Recover the Impact of User Decision.* This task focuses on confirming the user action. During this task the user are told to override the security product, then he/she received a warning message to warn him/her the harm that could happen if he/she proceed his action. The results, as shown in Figure 72, appear that the majority of the participants like the warning message that warns them before proceeding a wrong action.

7.1.6 Confirm / Recover the Impact of User Decision (Task Five)

The second protection against the user decision is if the user select a response option and after that the user realized that he/she want change the option, the user still have the chance by use

the feature that exists in CSCAN icon within the tray and perform a right click on *Recover Previous Decisions*, an interface will appear to the user as shown in Figure 73. The user can selects the action that he/she wishes from *User Action*, then update the system.

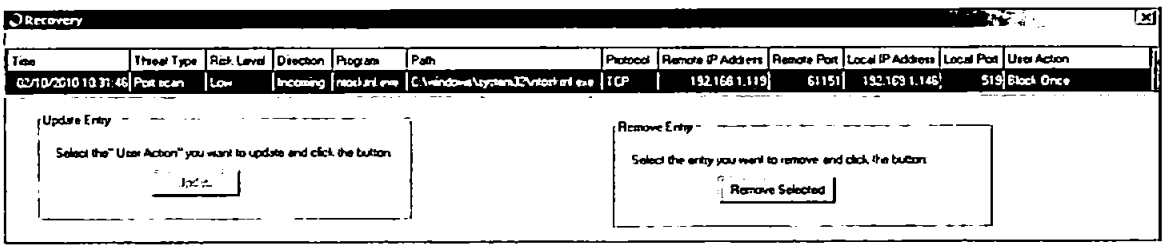


Figure 73: Recovery Interface

No security alert was displayed during this task. The participants were told to try to recover their previous decision by right clicking on the security product icon in the tray at the bottom of the screen. Then the participants received a questionnaire and they have to answer the questions.

Questions	SA	A	N	D	SD
Overall, did you feel the existence of this feature is understandable?	23%	52%	9%	16%	0%
Do you feel that this feature will support the user to recover from previous poor decisions?	39%	42%	13%	6%	0%

Table 14: Task 5 questions

Table 14 represents the questions that were asked to the participants during Task 5. There is another question that is not in the table asks the participants if there are ways in which the participants feel that this feature could be improved or any other comments that they wish to make. One of the participants wrote 'This seems like a useful feature, but when in the interface I was somewhat confused as to how to proceed, or even what was expected of me.' During answering this questionnaire the participants were advised to refer to the accompanying screenshots for reference if required.

Task 5 is addressing criterion 12, *Confirm / Recover the Impact of User Decision*. This task focuses on recovering the user action. This task shows that in some cases the user has the possibility to change some security decisions that he/she made previously. The results, as shown in Figure 74 , appear that the majority of the participants like this feature

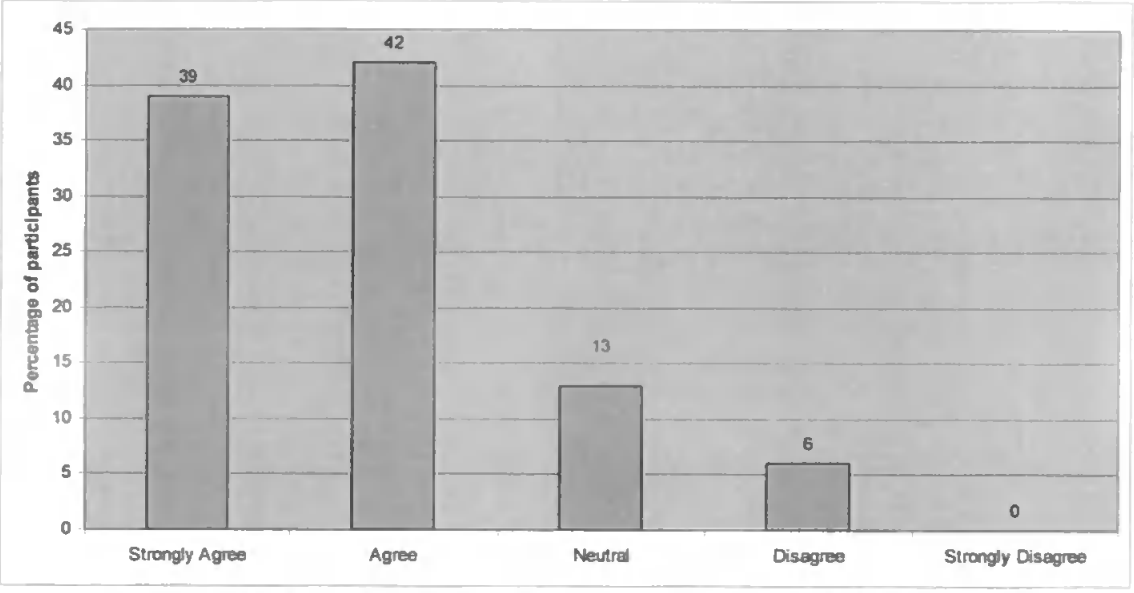


Figure 74: The feature will support the user to recover from previous poor decisions

7.1.7 Awareness of System Status all the Time (Task Six)

Figure 75: CSCAN icons

When the end-users select the Block always no security alert appear again to the end-users if the same cause of the alert occurred again which make the end-users unaware about what is going on their computers. Therefore, a secondary icon next to the CSCAN icon in the tray, as shown Figure 75, will appear if the event that cause the alert already happened before and the user took an action apart of *Block Once*, *Allow Once* or dismiss the alert. For instance, as shown Figure 76, assume that the user previous action was *Block Always*, and the cause of the alert occurred again, in this case the user will not receive an alert. The benefit of the CSCAN

system is that it offer the appearance of yellow icon next to the CSCAN to inform the user that the an event that causes previously a security alert has occurred but no usual security alert was issued based on the user previous response which was *Block Always*. The colour of the secondary icon will vary between yellow and red based on the severity of the events that occurs during the session.

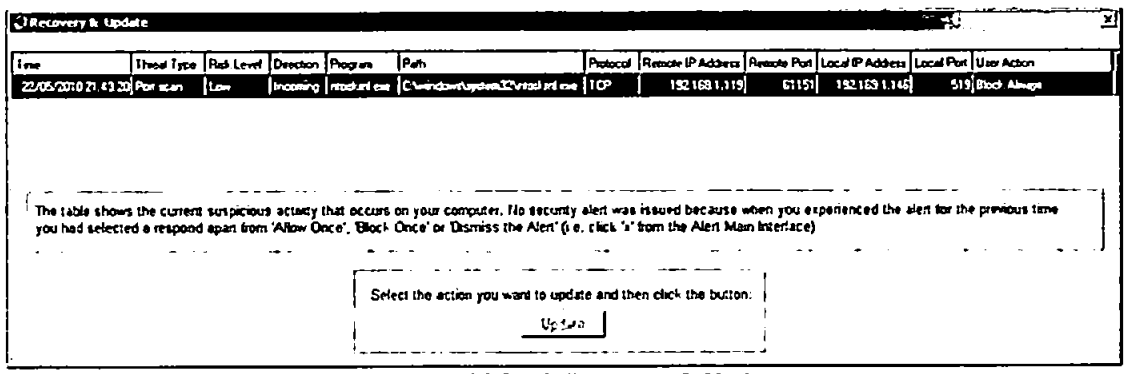


Figure 76: CSCAN- Recovery & Update

No security alert will be displayed during this task and the participants were told to wait for a few seconds for further instructions as follows: move the mouse towards the tray at the icon next to Security Product One icon. Next click the icon to investigate the situation (i.e. current system status), then explore the displayed interface. Then click on the interface close button 'x' after the participants accomplish their exploration. Then the participants received a questionnaire and they have to answer the questions.

The first question asks the participants if they had noticed the warning icon in the tray before they were prompted to view it. The participants' answers were 70% Yes, 30% No.

Questions	SA	A	N	D	SD
Do you think the appearance of this icon is intrusive?	10%	13%	20%	37%	20%
Was the icon easy to find in the tray?	33%	53%	3%	10%	0%
Do you think that this feature helps to inform users about the security status of the system?	27%	57%	13%	3%	0%
Overall, did you feel that the whole security alert was understandable?	27%	67%	6%	0%	0%

Table 15: Task 6 questions

Table 15 represents the questions that were asked to the participants during Task 6. There is another question that is not in the table asks the participants if there are ways in which the participants feel that whole alert could be improved or any other comments that they wish to make. One participant wrote 'I think the alert could be more intrusive, although the yellow icon is noticeable, i think if I was busy in a task i might not have picked up on it.'. During answering this questionnaire the participants were advised to refer to the accompanying screenshots for reference if required.

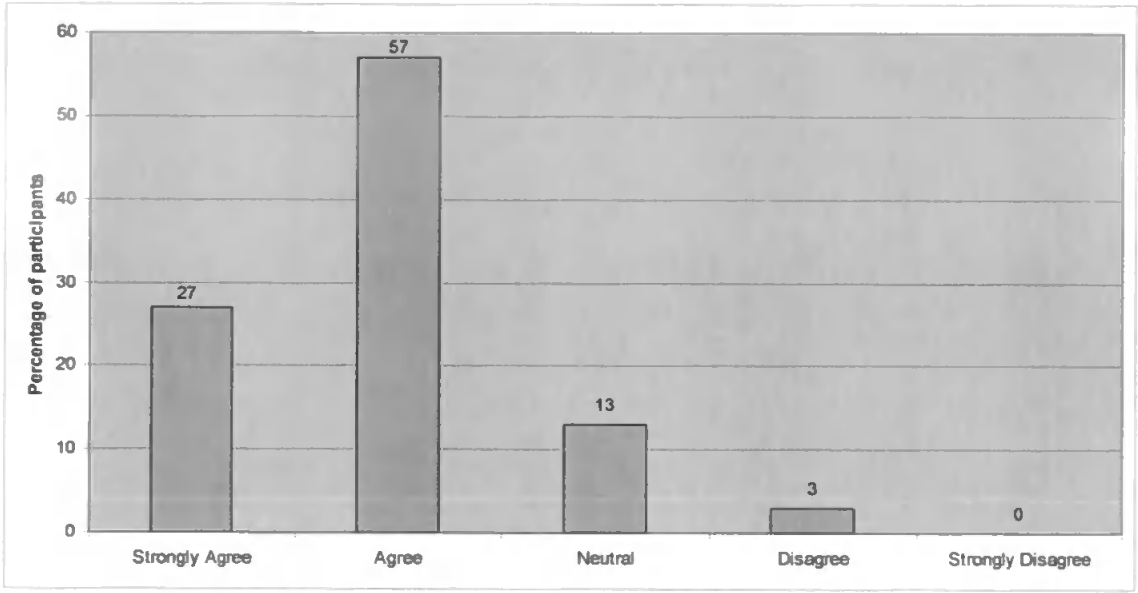


Figure 77: The feature helps to inform users about the security status of the system.

Task 6 is addressing criterion 13, *Awareness of System Status all the Time*. If the user selects the options *Allow Once* or *Block Once* he/she will receive an alert in the future if the threat occurs again. But if the user selects other option from the list of options provided in the *More Options* interface, no alert will appear to the user. Hence we provide an icon next to the security product icon to indicate the occurrence of the threat if it happened again. The results, as shown in Figure 77, appear that the majority of the participants like this feature.

7.2 Conclusions

This chapter attempts to focus on addressing the missing HCI-S usability criteria within the investigated security products in the port scanning case study without ignoring the rest of the criteria. The future work will focus on covering any limitations that was revealed during the prototype evaluation to make the next version of the prototype more user-friendly than the current one. This goal might be difficult to achieve because of the nature of the end users vary and the security treats are evolving and increasing in a rapid rate. However, identifying and developing usable design guidelines for developing and enhancing security products that meet end user expectations are still an evolving research discipline and it is anticipated that current studies will success to achieve an acceptable tradeoff between usability and security in the near future.

Chapter 8

Conclusions & Future Work

8 Conclusions & Future Work

This chapter concludes the thesis by summarising the achievements and the limitations of the research. The chapter proceeds to discuss the points were the future research could consider for further refinement.

8.1 Achievements of the Research

The objectives of the research programme have been met and the key achievements of the research are summarised below.

1- Limitations of the intrusion detection systems and the challenges preventing the adoption of IDS have been established in Chapter 3, based on the established literature. Chapter 3 focuses on determining the up-to-date IDS challenges within literature. A set of 21 IDS challenges was identified within five different categories. These challenges were ranked according to the findings from the respondents.

2- To complete this stage of the study, a web-based questionnaire was conducted to gather information from a range of persons, starting with persons aware of IDS until experts in the field (Chapter 4). Even though, only 43 persons fully participate in the web-based questionnaire but the results were astonishing. The findings revealed that the correlation between the top IDS challenges is the human being themselves. Therefore, the second part of the thesis focuses on the tradeoff between security and usability.

3- Investigating the relevant studies that are relevant to the thesis research reveals the requirement to develop novel criteria to meet the thesis goal (Chapter 5). Hence, a set

of 16 HCI-S usability criteria were created as basis to aid designers to develop and design security alerts that meet the end-user requirement, for a usability perspective. Norton 360 was selected as a well-known security product to implement the HCI-S usability criteria.

4- Implementing the criteria on a set of other security products was required to obtain solid results (Chapter 6). The findings reveal that four of the criteria were not fully addressed by the selected security products. Therefore, the final part of the thesis managed to develop a solution for each of the four problems and to evaluate to what extend to they success to solve the problems (Chapter 7).The prototype evaluation was promising as the participants were happy, as the results reveal, with the proposed solutions.

8.2 Limitations of the Research

Although the objectives of the research programme have been met, a number of limitations could not be avoided to obtain better results. The key limitations of the research are summarised below.

1- One of the limitations in the web-based questionnaire is the small number of participants (Chapter 4). This number would be sufficient in case that the majority of them have actual experience with the deployment of IDS in practice. Unfortunately, not all the participants have deployed (or taken the decision to deploy) an IDS and 25% mentioned that they are not in a position to take the decision of deploying an IDS or not (but decided to complete the questionnaire based on there opinions and other experiences in the field). Even though the participation of the last group are not going to provide us with the precise up-to-date IDS challenges, it is anticipated that they

have the necessary knowledge to participate and confirm to the severity of the IDS challenges covered in the survey and to some extent are able to address these challenges.

2- In the case study (Chapter 7) one of the limitations in the prototype evaluation is that the eye-tracker methodology was not used such as Tobii Technology AB (2010). This would have enabled more information to be obtained about the participants' behaviour during the case study. It is anticipated that the combination of analysing the user answers in the questionnaire, their actions that were stored in the database, and the information that would be obtained by an eye tracker, would enrich the analysis and make the findings even more valuable. The eye-tracker methodology will give the opportunity to know exactly where the participant was looking during the evaluation. This will let us know better what attracts the user and how the user is thinking. The current prototype evaluation is unable to obtain this type of information.

8.3 Suggestions for Future Work

This research programme has advanced the field of usable security for end-users. However, there is more to be done in this field of research and some related suggestions are detailed below:

1- The comments that were provided by some of the participants in the case study (Chapter 7) were not used efficiently during the current study. The combination of the thesis analysis and these comments will be the basis for the future work to develop a security interface that is more efficient and usable as we consider the current study as an initial step towards enhancing a usable security interfaces.

2- During the case study 42% of participants select Integrated Security products (combining Antivirus, firewall, intrusion detection, etc) and 19% intrusion detection. More study need to be done about what do end users understand about IDS and how can they use it. Moreover, investigating the factors that guide them to deploy IDS on their machines.

3- Although the participants agreed that they like the prototype features during Task 5 and Task 6 (Chapter 7), it seems that more work need to be done to make it more usable for an average end-user.

8.4 The Future of HCI-S for Intrusion Management

Intrusions and other related attacks will continue to present a challenge for Internet-based systems. There will consequently be an ongoing need for associated safeguards to protect these systems and their users against compromise. Therefore, there is always a need for efficient security defensive tools.

The current research managed to develop a set of HCI-S usability criteria, as attempt to achieve powerful IDS. Arguably, based on the case study results, these criteria meet the average end-user requirements but what about the case of novice end-users and experts. This group of participants should be considered and be asked if the implementation of the HCI-S usability criteria is useful to them or it is just useful for average end users.

The efficiency of the IDS is a major factor while making a decision of installing it. However, the focus of the current research was to improve the efficiency of IDS not by developing a powerful detection method but by developing suitable HCI-S usability criteria. The

combination of having an IDS with efficient detection method and meeting the requirement of the HCI-S usability criteria will guide the creation of more powerful IDS solutions.

References

1. Abimbola, A.A., Munoz, J.M., Buchanan, W.J. (2006) "NetHost-Sensor: Investigating the capture of end-to-end encrypted intrusive data", Computers & security, vol. 25, pp. 445-451.

2. Amoroso, E. (1999) "Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response", Second Printing, Intrusion.Net Books, New Jersey.

3. Barnett, R. J. and Irwin, B. (2008) "Towards a Taxonomy of Network Scanning Techniques". Proceedings of the 2008 annual research conference of the South African Institute of Computer Scientists and Information Technologists on IT *research in developing countries:* riding the wave of technology, *(SAICSIT '08),* Wilderness, South Africa, 6-8 October 2008, pp.1-7.

4. Bierman, E., Cloete, E., and Venter, L. M. (2001) "A comparison of Intrusion Detection Systems", Computers & Security, vol. 20, pp. 676-683.

5. Caelli,W., Dennis, L. and Shain, M. (1994) "Information Security Handbook". First edition. Wilthire: Macmillan Press Ltd. 833p.

6. Carey, N., Mohay, G. and Clark, A. (2003) "Attack signature matching and discovery in systems employing heterogeneous ids", Las Vegas, NV, USA, pp. 245-254.

7. Cavusoglu, H., Mishra, B. K., and Raghunathan, S. (2005) "The value of intrusion detection systems in information technology security architectures", Inf. Syst. Res., vol. 16, no. 1, pp. 28–46.

8. Chen, S., Pan, C. and Yang, C. (2009) "An Adaptive Feedback Mechanism Algorithm for Intrusion Detection System", 2nd International Conference on Computer Science and its Applications, 2009. CSA '09.

9. Cheswick, W. R. (1992) "An Evening with Berferd, in which a Cracker is lured, endured, and studied", in Proceedings of the Winter USENIX Conference.

10. Chiasson, S., van Oorschot, P. C. and Biddle, R. (2006) "A Usability Study and Critique of Two Password Managers", Proceedings of the 15th conference on USENIX Security Symposium, Vancouver, Canada, 31 July – 4 August 2006.

11. Chiasson, S., van Oorschot, P. C. and Biddle, R. (2007) "Even experts deserve usable security: Design guidelines for security management systems", Proceedings of Symposium on Usable Privacy and Security (SOUPS 07), Pittsburgh, PA, 18-20 July 2007.

12. Cho, S. (2002) "Incorporating soft computing techniques into a probabilistic intrusion detection system", IEEE Trans. on Systems, Man and Cybernetics-Part C: Applications and Reviews, vol. 32, no. 2, pp. 154-60.

13. Coit, C. J. , Staniford, S., and McAlerney, J. (2001) "Towards Faster Pattern Matching for Intrusion Detection or Exceeding the Speed of Snort", in Proc. 2nd DARPA Information Survivability Conference and Exposition.

14. Conti, G., Abdullah, K., Grizzard, J., Stasko, J., Copeland, J. A., Ahamad, M., Owen, H. L., and Lee, C. (2006) "Countering security information overload through alert and packet visualization", IEEE Computer Graphics and Applications, vol. 26, no. 2, pp 60-70.

15. Debar, H., Becker, M., Siboni, D. (1992) "A neural network component for an intrusion detection system", Proc. IEEE Computer Society Symp. on Research in Security and Privacy Oakland, CA, pp. 240-250.

16. Debar, H., Dacier, M., Wespi, A. (1998 a) "Fixed versus variable-length patterns for detecting suspicious process behavior", Technical Report RZ 3012, IBM Zurich Research Laboratory, Sa¨umerstrasse 4, CH-8803 Ru¨schlikon, Switzerland, submitted to Esorics'98.

17. Debar, H., Dacier, M., Wespi, A. (1998 b) "Reference audit information generation for intrusion detection systems", in Reinhard Posch and György Papp, editors, Information Systems Security, Proceedings of the 14th International Information Security Conference IFIP SEC'98, Vienna, Austria and Budapest, Hungaria, August 31- September 4,pp. 405-417.

18. Debar, H., Dacier, M. and Wespi, A. (1999) "Towards a taxonomy of intrusion-detection systems", in Computer Networks, vol. 31, no. 8, pp. 805-822.

19. Denning, D. (1986) "An Intrusion Detection Model", Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, pp.119-131.

20. Denning, D. (1987) "An Intrusion-Detection Model". *IEEE Transactions on Software Engineering, Vol. SE-13, No.2, February 1987, pp. 222-232.*

21. Dhamija, R., Tygar, J. D. and Hearst, M. (2006) Why Phishing Works. In Proceedings of SIGCHI Conference on Human Factors in Computing Systems (CHI "06), Montreal, Canada, 22-27 April 2006, pp581-590.

22. Dozier, G. V., Brown, D., Hurley, J. and Cain, C. (2004) "Vulnerability Analysis of AIS-Based Intrusion Detection Systems via Genetic and Particle Swarm Red Teams", in Proceedings of the 2004 Congress on Evolutionary Computation, pp. 111-116.

23. Durdag˘i,E. and Buldu, A. (2010) "IPV4/IPV6 security and threat comparisons", Procedia Social and Behavioral Sciences 2 (2010) pp. 5285-5291.

24. Eckmann S.T. (2001) "Translating Snort rules to STATL scenarios", in Proceeding Recent Advances in Intrusion Detection, Davis, CA.

25. Eckmann, S.T., Vigna, G. and Kemmerer, R.A. (2002) "STATL: An Attack Language for State-based Intrusion Detection", Journal of Computer Security, vol. 10. , no. (1/2), pp. 71–104.

26. Fadlullah, Z. M., Taleb, T., Vasilakos, A. V., Guizani, M., and Kato, N.(2010) "DTRAB: Combating Against Attacks on Encrypted Protocols Through Traffic-Feature Analysis", IEEE/ACM Transactions on Networking, Vol. 18, No. 4, August 2010. pp.1234-1247.

27. Fang, X. and Li, L.(2010), "An Improved Artificial Immune Approach to Network Intrusion Detection", 2nd International Conference on Advanced Computer Control (ICACC), 2010. pp. 39 - 44

28. Farid D. Md. and Rahman M. Z. (2010) "Anomaly Network Intrusion Detection Based on Improved Self Adaptive Bayesian Algorithm", *Journal of Computers*, Vol 5, No 1 (2010), pp. 23-31, Jan 2010

29. Fessi, B.A., Hamdi, M., Benabdallah , S. and Boudriga, N. (2007) "A decisional framework system for computer network intrusion detection", European Journal of Operational Research, vol. 177. pp. 1824-1838.

30. Fisk M. and Varghese G. (2001) "Fast Content-Based Packet Handling for Intrusion Detection", Technical Report CS2001-0670, UC San Diego.

31. Frincke, D., Wespi, A., and Zamboni, D. (2007) "From intrusion detection to self-protection", Guest Editorial / Computer Networks, vol. 51, pp. 1233–1238.

32. Garfinkel, S. L. (2005) "Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable", PhD thesis, Massachusetts Institute of Technology, May 2005.

33. Giacinto, G., Roli, F., Didaci, L. (2003) "Fusion of multiple classifiers for intrusion detection in computer networks", Pattern Recognition Letters, vol. 24, no. 12, pp. 1795-1803.

34. Gong, F. (2002) "Next generation intrusion detection systems (IDS)", McAfee Network Security Technologies Group.

35. Goodall, J. R., Lutters, W. G., and Komlodi, A. (2004) "I know my network: collaboration and expertise in intrusion detection". In CSCW '04: Proceedings of the 2004 ACM Conference on Computer-Supported Cooperative Work, ACM Press, New York. pp. 342-345.

36. Gordeev, M. (2000) "Intrusion Detection: Techniques and Approaches", the Distributed Systems Group in the Information Systems Institute of Technical University of Vienna.

37. Green, I., Raz, T. and Zviran, M. (2007) "Analysis of active intrusion prevention data for predicting hostile activity in computer networks", Communications of the ACM, vol. 50, no. 4, pp. 63-68.

38. Helman, P. and Liepins, G. (1993) "Statistical foundations of audit trail analysis for the detection of computer misuse", IEEE Transactions on Software Engineering, vol. 19, no. 9, pp. 886–901.

39. Helman, P., Liepins, G., Richards and W. (1992) "Foundations of intrusion detection", Proceeding 5th Computer Security Foundations Workshop Franconic, NH, pp. 114–120.

40. Herzog, A. and Shahmehri, N. (2007) "Usable set-up of runtime security policies", Proceedings of the International Symposium on Human Aspects of Information Security and Assurance (HAISA 2007), Plymouth, United Kingdom, 10 July 2007, pp99-113.

41. House of Lords. (2007). *Science and Technology Committee. 5th Report of Session 2006–07. Personal Internet Security.* United Kingdom Parliament. HL Paper 165–I. London: The Stationery Office Limited. http://www.parliament.the-stationery-office.co.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf. (Accessed: 15/10/2010)

42. Iheagwara, C. and Blyth, A. (2002) "Evaluation of the performance of IDS systems in a switched and distributed environment", Computer Networks, vol. 39, pp. 93–112.

43. Johnston, J., Eloff, J. H. P. and Labuschagne, L. (2003) "Security and human computer interfaces", Computers & Security, 22, (8) pp675-684.

44. Joo, D., Hong, T. and Han, I. (2003) "The neural network models for IDS based on the asymmetric costs of false negative errors and false positive errors", Expert Systems with Applications, vol. 25, no. 1, pp. 69-75.

45. Koike, H. and Ohno, K. (2004) "Snortview: Visualization system of snort logs", in VizSEC/DMSEC, Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security. ACM, New York, pp. 143-147.

46. Kotov, V. D. and Vasilyev, V. I. (2009) "Artificial Immune Systems Based Intrusion Detection System", Proceedings of the 2nd international conference on Security of information and networks, pp. 207-212.

47. Kreibich, C. and Crowcroft, J. (2003) "Honeycomb – Creating Intrusion Detection Signatures Using Honeypots", in Proceedings of the USENIX/ACM Workshop on Hot Topics in Networks (HotNets-II), Cambridge, Massachusetts.

48. Lai, K. and Wren, D. (2009). Antivirus, Internet Security and Total Security Performance Benchmarking, http://www.passmark.com/ftp/antivirus_09-performance-testing-ed1.pdf (Accessed: 03/10/2010)

49. Lee, W., Fan, W., Miller, M., Stolfo, S., and Zadok, E. (2000) "Toward cost-sensitive modeling for intrusion detection and response", Journal of Computer Security, vol. 10 , Issue 1-2 , pp. 5-22.

50. Lindqvist, U. and Porras, P.A. (1999) "Detecting Computer and Network Misuse with the Production-Based Expert System Toolset (P-BEST)", in Proceedings of the 1999 IEEE Symposium on Security and Privacy, Oakland, California.

51. Mathew, S., Giomundo, R., Upadhyaya, S., Sudit, M. and Stotz, A. (2006) "Understanding Multistage Attacks by Attack-Track based Visualization of Heterogeneous Event Streams", Proceedings of the 3rd international workshop on Visualization for computer security, Alexandria, Virginia, USA, November 03 - 03.

52. Muñoz-Arteaga, J., González, R. M. and Vanderdonckt, J. (2008) "A Classification of Security Feedback Design Patterns for Interactive Web Applications", The Third International Conference on Internet Monitoring and Protection, 29 June– 5 July 2008, pp.166-171.

53. Nessus. (2010). The Network Vulnerability Scanner. http://www.nessus.org (Accessed: 26/10/2010).

54. Nielsen, J. (1994) "Enhancing the explanatory power of usability heuristics", Proceedings of ACM CHI'94 Conference. Boston, Massachusetts, USA. 24-28 April, pp152-158.

55. Nielsen, J. (2005). Ten usability heuristics. Available online at: http://www.useit.com/papers/heuristic/heuristic_list.html (Accessed: 14/10/2010)

56. Nmap. (2010). Nmap Security Scanner. http://insecure.org/nmap (Accessed: 26/10/2010).

57. O'Sullivan, S., Dojen, R., and Coffey, T. (2005) "Protecting Virtual Networks With A Distributed Cooperative Multi-layer Security Architecture" WSEAS Transactions on Computers, in Press, Dec. 2005. ISSN 1109-2750.

58. Overill, R. E. (2007) "Computational immunology and anomaly detection", Information Security Technical Report, vol. 12, issue 4, pp. 188-191

59. Parker, D.B. (1994), "Demonstrating the elements of information security with threats", in Proceedings of the 17th National Computer Security Conference, pp. 421-430.

60. Patton, S; Yurcik, W and Doss, D. (2001) "An Achilles Heel in Signature-Based IDS: Squealing False Positives in SNORT", in Proceedings of the 4th Intl. Symposium on Recent Advances in Intrusion Detection (RAID'2001).

61. Paxson V. (1999) "Bro: A system for detecting network intruders in real-time", Computer Networks, vol. 31, pp. 2435–2463.

62. Peddisetty, N.R. (2005) "State-of-the-art Intrusion Detection: Technologies, Challenges, and Evaluation", Master's Thesis, Linköping University, Sweden, 2005.

63. Perdisci, R. ,Giacinto, G., Roli, F. (2006) "Alarm clustering for intrusion detection systems in computer networks", Journal of Engineering Application of Artificial Intelligence 19 (2006) pp. 429–438.

64. Peters, S. (2009) "CSI/FBI Computer Crime and Security Survey", Computer Security Institute.

65. Porras, P.A, Valdes, A. (1998), "Live traffic analysis of tcp/ip gateways", in Proceedings of the 1998 ISOC Symposium on Network and Distributed Systems Security, San Diego, California, 11–13 March 1998.

66. Provos, N. (2003) "Honeyd - A Virtual Honeypot Daemon," in 10th DFN-CERT Workshop, Hamburg, Germany, February.

67. Ranum, M., Landfield, K., Stolarchuk, M., Sienkiewicz, M., Lambeth, A. and Wall, E. (1997) "Implementing a generalized tool for network monitoring", in Proceedings of the 11th Systems Administration Conference (LISA '97), San Diego, California, October.

68. Roesch, M. (1999) "Snort – lightweight intrusion detection for networks", In Proceedings of USENIX LISA '99, November.

69. Russel, D. and Gangemi, G.T. (1992) "Computer security basics". CA: O=Reilly & Associates Inc. 448p.

70. Safford, D.R. , Schales, D.L. and Hess, D.K. (1993), "The tamu security package: an ongoing response to internet intruders in an academic environment", in Proceedings of the 4th USENIX Security Symposium, Santa Clara, California, pp. 91-118.

71. Salour, M. and Su, X. (2007) "Dynamic Two-Layer Signature-Based IDS with Unequal Databases", Fourth International Conference on Information Technology: New Generations (ITNG 2007), Las Vegas, Nevada, 2-4 April 2007, pp. 77-82.

72. Sarle, W. S. (1994) "Neural networks and statistical models", Proceedings of the 19th Annual SAS Users Group International Conference. SAS Institute Inc., Cary, N.C., pp. 1538–1550.

73. Schultz, E. E. and Ray, E. (2007) "The future of intrusion prevention", Computer Fraud & Security, vol. 2007, issue 8, pp. 11-13.

74. Seliya, N. and Khoshgoftaar, T.M. (2010) "Active Learning with Neural Networks for Intrusion Detection", Information Reuse and Integration (IRI), 2010 IEEE International Conference. pp. 49 – 54.

75. Shneiderman, B. and Plaisant, C. (2005) "Designing the User Interface: Strategies for Effective Human-Computer Interaction" (4th edition), Addison Wesley.

76. Siraj, A. and Vaughn, R. (2007) "A Dynamic Fusion Approach for Security Situation Assessment", *Proceedings of the Fourth IASTED International Conference on Communication, Network, and Information Security (CNIS 2007)*, Berkeley, California, 24–26 September, 2007.

77. Smith, R., Estan, C., and Jha, S. (2006) "Backtracking Algorithmic Complexity Attacks against a NIDS", in Proceedings of 22nd Annual Computer Security Applications Conference (ACSAC'06), Miami Beach, Florida, 11-15 December, pp. 89-98.

78. Sommer, R., and Paxson, V. (2003) "Enhancing byte-level network intrusion detection signatures with context", Proceedings of the 10th ACM conference on computer and communications security, October 27-30, Washington D.C.,USA.

79. Sommer, R., and Paxson, V. (2010) "Outside the Closed World: On Using Machine Learning For Network Intrusion Detection", 2010 IEEE Symposium on Security and Privacy. pp. 305-316.

80. Sperotto, A. , Schaffrath, G. , Sadre, R. , Morariu, C., Pras, A. and Stiller, B. (2010). "An Overview of IP Flow-Based Intrusion Detection", IEEE Communications Surveys & Tutorials, Vol. 12, No. 3, Third Quarter 2010, pp. 343-356.

81. Spirakis, P., Katsikas, S., Gritzalis, D. , Allegre, F., Darzentas J., Gigante, C., Karagiannis, D., Kess P., Putkonen, H., Spyrou, T. (1994) "SECURENET: a network-oriented intelligent intrusion prevention and detection system", Network Security Journal, vol. 1, no 1, Nov. (Also in IFIP SEC94, Proceedings of the 10th International Conference on Information Security, the Netherlands).

82. Spitzner, L. (2003) "Honeypots: Tracking Hackers", Addison-Wesley, Longman Publishing Co., Inc., Boston, MA.

83. Stakhanova, N. , Basu, S. and Wong, J. (2007 a) "A Cost-Sensitive Model for Preemptive Intrusion Response Systems", Proceedings of the 21st International Conference on Advanced Networking and Applications, AINA'07, IEEE Computer Society, Washington, DC, USA, pp. 428–435.

84. Stakhanova, N. , Basu, S. and Wong, J. (2007 b) "A taxonomy of intrusion response systems", International Journal of Information and Computer Security, vol. 1, no. 1/2, pp.169-184.

85. Stibor T, Timmis J and Eckert C (2005) On the appropriateness of negative selection defined over hamming shape-space as a network intrusion detection system. In: Proceedings of the Congress on Evolutionary Computation (CEC-2005), Edinburgh, UK, September 2005, pp. 995–1002. IEEE Press

86. Stoll, C. (1986) "The Cuckoo's Egg", Addison-Wesley, 1986.

87. Sundaram, A. (1996) "An introduction to intrusion detection", Crossroads: The ACM student magazine, 2 (4), April.

88. Symantec (2007). *Symantec Internet Security Threat Report. Trends for January 07 – June 07*, vol. XII. Symantec Enterprise Security, September 2007.

89. Symantec (2009). *Symantec Global Internet Security Threat Report.* Trends for 2008, Volume XIV, Published April 2009

90. Tanase, M. (2001), "The Future of IDS", http://www.securityfocus.com/infocus/1518. (Accessed: 02 /10/ 2010).

91. Tian, L. and Xueming, Z. (2009) "Design and Implementation of an Initiative and Passive Network Intrusion Detection System". Second International Symposium on Information Science and Engineering (ISISE). pp.196 – 198.

92. Tobii Technology AB (2010). http://www.tobii.com. (Accessed: 02 /10/ 2010).

93. Top Security Software (2009). http://www.2009securitysoftwarereviews.com (Accessed: 26/01/2009).

94. Victor, G. J., Rao, M. S. and Venkaiah, V. CH. (2010) "Intrusion Detection Systems-Analysis and Containment of False Positives Alerts", *International Journal of Computer Applications, Volume 5- No.8, August 2010, pp. 27-33.*

95. Vokorokos, L. and Baláž, A. (2010) "Host-based Intrusion Detection System", 14th International Conference on Intelligent Engineering Systems (INES), 2010. pp. 43 -47.

96. Wei, H., Frinke, D., Carter, O. and Ritter, C. (2001) "Cost-benefit analysis for network intrusion detection systems", in Proceedings of the CSI 28th Annual Computer Security Conference, Washington, DC, October 2001.

97. West, R. (2008) "The Psychology of Security: Why Do Good Users Make Bad Decisions?" Communications of the ACM, Vol. 51, No. 4, pp. 34–40, April 2008.

98. Which. 2009. Security software. *Which? Computing*, January 2009, pp44-49.

99. Whitten, A. and Tygar, J. D. (1999) "Why Johnny can't encrypt: A usability evaluation of PGP 5.0", In Proceedings of the 8th USENIX Security Symposium, Washington, D.C., USA, 23–26 August 1999

100. Wu, B., Chen, J., Wu, J., and Cardei, M. (2006) "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks". *Wireless/Mobile Network Security*, chapter 12, 2006.Springer.

101. Xiao, M. and Xiao, D. (2007) "Alert Verification Based on Attack Classification in Collaborative Intrusion Detection", in Proceedings of Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 2007, (SNPD 2007), Qingdao, China, 30 July – 1 Aug 2007, pp. 739-744.

102. Yee, K-P. (2002) "User interaction design for secure systems.", In Proceedings of the International Conference on Information and Communications Security (ICICS 02), Lecture Notes In Computer Science, Vol. 2513, Springer-Verlag Berlin Heidleberg. pp.278–290.

103. Yegneswaran, V., Giffin, J., Barford, P., and Jha S. (2005) "An architecture for generating semantics-aware signatures", in Proceedings of the 14th USENIX Security Symposium, August 2005.

104. Yurcik, W. (2002) "Controlling Intrusion Detection Systems by Generating False Positives: Squealing Proof-of-Concept", in Proceedings of the 27th Annual IEEE Conference on Local Computer Networks (LCN'02), March 2002.

105. Zenmap GUI. (2010). http://insecure.org/nmap (Accessed: 26/10/2010).

106. Zhang, C. ,Jiang, J. and Kamel, M. (2005) "Intrusion detection using hierarchical neural networks", Pattern Recognition Letters, vol. 26, issue 6, pp. 779-791.

107. Zhang, S., Liul, S., Gao, Y., Ge, J., and Wang, L. (2010) "A Credible Network Intrusion Detection System Based on Grid". IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), 2010. pp. 528-532.

108. Zhou, A. T., Blustein, J. and Zincir-Heywood, N. (2004) "Improving intrusion detection systems through heuristic evaluation", 17th Annual Canadian Conference of Electrical and Computer Engineering (CCECE 2004), Niagara Falls, Canada, 2-5 May 2004, pp1641-1644.

Appendix A

A.1 Findings of the Participant's Response

Table A represents the sum of the individual's responses according to each of the challenges in the web-based questionnaire, represented in Chapter 4 (note that the columns are headed as follows: SA – strongly agree; A – agree; N – neutral; D – disagree; SD – strongly disagree; DK – don't know; A+SA – agree + strongly agree; WMS – weighted method score).

No.	Challenge	SA	A	N	D	SD	DK	A+SA	WMS
	Deployment Challenges								
1	Scalability constraints	8	20	3	5	4	1	28	23
2	Switched Networks	9	15	5	6	3	3	24	21
3	Packet dropping and high speed network traffic	8	17	5	6	4	1	25	19
4	Encrypted traffic and IPv6	7	11	6	7	4	6	18	10
5	Initial deployment cost	8	23	6	0	2	2	31	35
	Management Challenges								
6	Volume of information	16	20	2	1	1	1	36	49
7	Ensuring effective configuration	9	21	2	8	1	0	30	29
8	Managing a heterogeneous IDS environment	10	18	8	0	0	5	28	38
9	Ongoing operational costs	12	23	1	4	1	0	35	41
	Technical Challenges								
10	Vulnerability to attacks	9	24	5	1	1	1	33	39
11	Difficulty in customizing and updating the IDS ruleset	9	24	5	0	0	3	33	42
12	Data collection and logging	9	23	6	1	1	1	32	38
13	Understanding and interpreting IDS data	13	23	4	0	0	1	36	49
	Detection Challenges								
14	The large number of alerts	15	15	8	2	1	0	30	41
15	False negatives	12	15	11	2	0	1	27	37
16	False positives	13	19	7	1	1	0	32	42
17	Determining the alert severity level	2	27	8	2	1	1	29	27
18	Alerts correlation	9	23	6	2	0	1	32	39
	Response Challenges								
19	Requirement for skilled staff	13	19	6	3	0	0	32	42
20	The potential for inappropriate and harmful responses	10	20	9	1	0	1	30	39
21	Effectiveness of the IDS response	4	24	7	4	0	2	28	28

Table A: Individual assessment of IDS challenges

Table B represents the finial results of the individual's responses of sorting the challenges in the web-based questionnaire. The participants provide their opinions about the challenges that are considered to be of the top five challenges and rank them in order.

No.	The IDS Challenges List	Top 1	Top 2	Top 3	Top 4	Top 5
	Deployment Challenges					
1	Scalability constraints	1		1	1	3
2	Switched Networks	1	1	1	1	
3	Packet dropping and high speed network traffic	2		1	2	
4	Encrypted traffic and IPv6	2	2	2	4	
5	Initial deployment cost	2				1
	Management Challenges					
6	Volume of information	1	2	6	4	1
7	Ensuring effective configuration			1		3
8	Managing a heterogeneous IDS environment	2		2	2	1
9	Ongoing operational costs	1	2			2
	Technical Challenges					
10	Vulnerability to attacks	1	1	1	1	1
11	Difficulty in customizing and updating the IDS ruleset	3	2	3	2	1
12	Data collection and logging		1		1	1
13	Understanding and interpreting IDS data	4	3	2	5	1
	Detection Challenges					
14	The large number of alerts	3	3	4	1	
15	False negatives		4	1	2	1
16	False positives	4	3	2	1	2
17	Determining the alert severity level	2	1		1	4
18	Alerts correlation	3	4	4	3	3
	Response Challenges					
19	Requirement for skilled staff	3	6	1	2	2
20	The potential for inappropriate and harmful responses			1		2
21	Effectiveness of the IDS response			1		4

Table B: Individuals highest top 5 challenges

A.2 The Challenges Appended by Participants

"The success of IDS, particularly signature based IDS is partly a function of the range and type of traffic on the network. It is easier to implement in a corporate environment where application, services and protocols can be restricted more."

"Lack of effective and unbiased evaluation methods"
"Visualisation of results (particularly for correlated alert)"

"Snort is a good open source project"
"Other network appliances might be better"

"polymorphic attacks"
"encrypted attacks"
"non-malicious, yet disruptive traffic"

"Self-organization of various security components"
"Guarantees of Service"
"Distributed IDS"
"Cooperation between different security components"

"Detect polymorphic or 0-day attacks"

"Lack of educators knowledge of current systems."
"Differentiation of different generations of IDS technology."
"IDS does not equal SNORT"

"Integration into higher-level Security Management Systems"
"Impact on Wide Area Networks (WAN)"

A.3 The Participants Comments

"Better client protection (ie PC firewalls and anti virus software) can improve overall IDS performance. However, many networks now have IP peripherals (ie video servers, ip cameras, ip printers etc) that are essentially unprotected."

"Do not connect a machine in a network"

"As stated in the earlier questions, we implemented anomaly based IDS. This was a direct result of identifying many of the problems raised in the survey with signature based IDS and which do not apply, or do not apply to the same degree, with anomaly based IDS. Q31: The answer also depends on your definition of "false positive". With our anomaly detection system, those alerts that prove not to be a security issues, very often turn out to be network anomalies (i.e. changes in network behaviour) that are useful to know even if not directly related to a security incident. On this basis, I consider false positives from our system to be quite low, as indicated."

"better discrimination between real attacks which fail and real attacks which succeed"

"- Alert correlation and fusion techniques proposed by the research community are still not widely implemented by IDS manufacturers. - Anomaly-based detection systems are still inefficient in the sense they return a high false alarm rate."

"Create unbiased methods to evaluate and test the IDS"

"I wish you had comment boxes below each of the questions. There are so many cases where I would have strongly agreed if some condition but strongly disagreed if some other condition. For example, it does cost money to maintain the IDS, but if this system is in-line and blocking known and tested attacks then you are actually reducing the overall cost to maintain your network. The IDS will pretty much pay for itself with the reduction of infections on the network. I hope that any business that purchases an IDS will have first tested its scalability. If it scales properly then you don't have to worry if your organization grows or not."

"FWIW, we published: Investigating New Approaches to Data Collection, Management and Analysis for Network Intrusion, ACMSE 2007 Winston-Salem University E. Joseph Derrick Radford University Department of Information Technology Radford VA 24142-6933 (540) 831-5368 ejderrick@radford.edu Richard W. Tibbs Radford University Department of Information Technology Radford VA 24142-6933 (540) 831-5780 rwtibbs@radford.edu Larry Lee Reynolds Eastman Chemical Company 100 N. Eastman Road Bldg. 284, Office 4186 Kingsport, TN 37662 (423) 229-2000 leer@eastman.com We have done a series of projects. Behind this paper is a data analysis, data fusion and data logging facility. We used the 1999 project from DARPA for this work."

"distribute the whole system to all nodes with a dynamic and adaptive management introduce autonomous workflows identification of problems and infected nodes"

"Mixed anomaly/rule - based IDSs can help solving many of the problems, bud anomaly - based IDSs still have to mature. Anomaly - based IDSs should be more specific to the type of monitored service (HTTP, IMAP, etc.)."

"Early generations of IDS technology fired aways dozens of alerts that were generally meaningless in the hopes of analysts and data fusion engines to determine the real from the chaff. Current technology is able to understand the system being attacked, its operating system and vulnerabilities and leverage that in concert with multiphases of attack to determine if something is a threat versus a malicious packet. With these systems only valid threats are reported. I would hope this survey gets a little more focused on state of the art rather than reporting on circa 2000 enterprise fears and experience of IDS."

"Many of the challenges, while worthwhile are being looked at by various researchers. For example, folks are already considering detection schemes for hi-speed networks. I personally have looked into dealing with inspecting VPN traffic. One other challenge that is not listed is the intrusiveness of the technology-- if it makes your system slow and a hi false positive rate, the technology will not be well received in the community."

"The questions could be improved to get better answers."

"IDS (or IPS) should implement more abstract signatures for detecting a whole class of attacks (see http://www.infosys.tuwien.ac.at/Staff/tt/publications/dissertation_toth.pdf for abstract signatures). For evaluating the impact of responses, IPS and CMDBs should share one information pool to evaluate the impact of response actions. The usability of an IPS (and its gui) is VERY important. Not all the alerts are equally important - severity levels (as for example implemented in the McAfee Intrushield) can help very much in handling the generated results (e.g. by ignoring all the informational alerts and showing high and medium severity alerts only)."

"The IDS technology has disappointed the market, due to the problems you mention in this questionnaire. That is why they were repackaged and re-marketed as IPS, which to my opinion were even a much worse solution."

Appendix B - Publications

1. Ibrahim, T., Furnell, S. M., Papadaki, M., Clarke, N. L.: Assessing the Challenges of Intrusion Detection Systems. Proceedings of the 7th Annual Security Conference. Las Vegas, USA. 2nd-3rd June (2008)

2. Ibrahim, T., Furnell, S. M., Papadaki, M., Clarke, N. L.: Assessing the Usability of Personal Internet Security Tools. Proceedings of the 8th European Conference on Information Warfare and Security (ECIW 2009), Military Academy, Lisbon & the University of Minho, Braga, Portugal, 6-7 July (2009)

3. Ibrahim, T., Furnell, S. M., Papadaki, M., Clarke, N. L.: Assessing the Usability of End-User Security Software. Lecture Notes in Computer Science, Volume 6264/2010, pp177-189, 2010.

Assessing the challenges of Intrusion Detection Systems

T.Ibrahim, S.M.Furnell, M.Papadaki and N.L.Clarke
Centre for Information Security & Network Research, University of Plymouth, Plymouth, United Kingdom
cisnr@plymouth.ac.uk

Abstract

Intrusion Detection Systems (IDS) are a commonly recognised element of the Internet security arsenal, regularly considered alongside firewalls and anti-virus as options for protecting networked systems. However, despite the widespread availability, the actual deployment and use of IDS is considerably less than these other technologies, suggesting that practical factors are potentially constraining their adoption. This paper seeks to further investigate this issue, drawing upon prior literature to identify the range of challenges that may be posed by IDS, and then mounting a survey to determine their relative significance. A web-based questionnaire was used to solicit information and opinion from IDS users and other IDS-aware respondents. A total of 41 responses were obtained, which (although limited) was sufficient to reveal a notable finding in the overall response. Specifically, while the received wisdom suggests that the most pressing challenge of IDS is the volume of false positives, the survey results indicated that a number of human-related aspects (relating to understanding, skills and ability to correlate information) were actually more prominent problems.

Keywords: *Intrusion Detection Systems, Security, Challenges*

1. Introduction

In the face of a wide range of online attacks, Intrusion Detection Systems (IDS) represent a potentially valuable safeguard to identify and combat the problems. However, despite the fact that a variety of commercial and open source solutions are available across a range of operating system and network platforms, it is notable that the deployment of IDS is often markedly less than other well-known network security countermeasures. Evidence for this claim is provided by the CSI Computer Crime and Security Survey 2007 (Richardson, 2007), which shows that while anti-virus and firewall protection are used by 98% and 97% of respondents respectively, the adoption of IDS sits at a more modest 69% (with the percentages based upon a group of 484 respondents, two thirds of whom were from large organisations with 500+ employees). The point is further supported by findings from UK-based industry analysts Freeform Dynamics, as illustrated in Figure 1, which show IDS to enjoy a significantly lower level of implementation than other security technologies.

Such findings raise questions about why IDS are less prominent than other well-known countermeasures, including many that have appeared in the marketplace more recently and had less time to establish themselves. One possible reason could, of course, be that the threats that IDS seek to combat are not as prominent or significant as those targeted by the other, more popular countermeasures. However, given that IDS can actually assist in dealing with many of the same threats as firewalls and anti-virus, this would not be a valid conclusion. Similarly, another possible argument is that they may not represent an effective solution, and therefore many organisations chose not to use them. However, if this was the case then one would instinctively expect the level of penetration to be even lower. As such, it

appears likely that other factors are also coming into play, with potential users facing challenges that ultimately prevent IDS from being adopted.

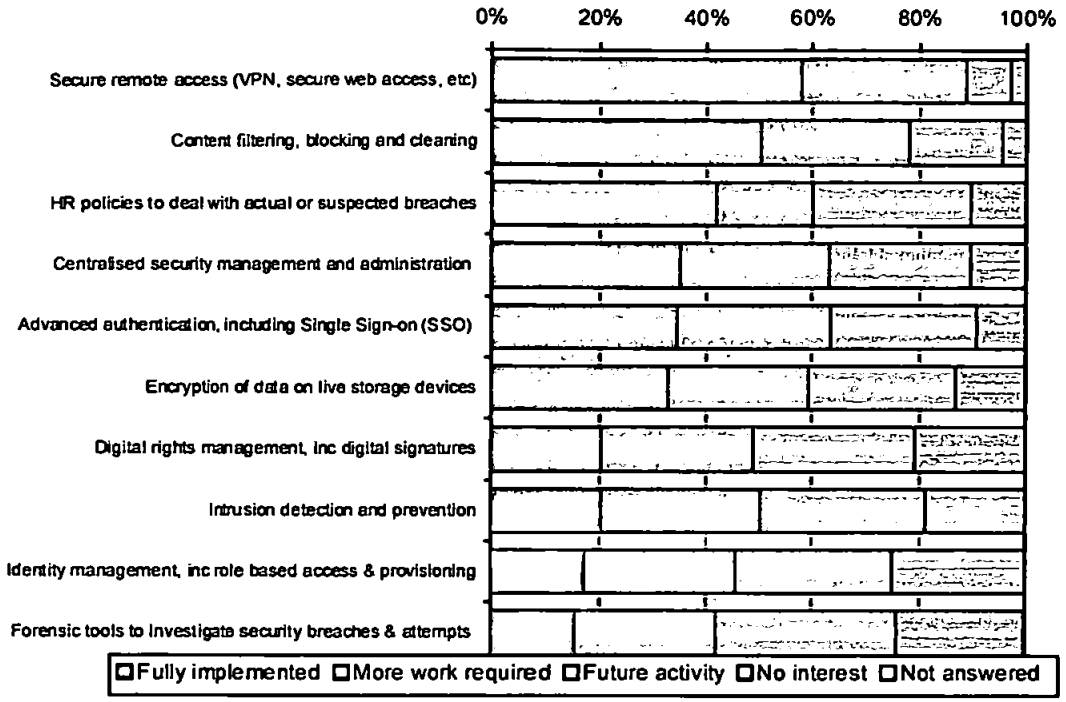


Figure 1 : Implementation of security measures (Source: Freeform Dynamics)

With the above in mind, this paper seeks to further explore the challenges posed by IDS technologies, drawing upon a literature-informed assessment of the potential problem areas in order to mount a survey amongst IDS users and others in a position to deploy the technology. The next section presents a summary of the potential challenges, with section 3 then proceeding to outline the survey methodology and the findings that were observed. The results suggest that the problems encountered in practice are somewhat different to the issues that tend to appear dominant in the literature and industry coverage, and resultant conclusions are drawn in the final section of the paper.

2. Challenges posed by Intrusion Detection Systems

In terms of challenges, one of the most commonly identified issues in relation to IDS is the problem of false alarms, resulting from situations in which legitimate and harmless activity is falsely judged to represent an attack. Indeed, the perceived problems of false positives (e.g. the consequent time wasted by investigating them, or the potential for genuine alerts to be overlooked in the noise) have led to significant changes in the marketplace, with the emergence of Intrusion Prevention System (IPS) technologies occurring as a direct response to this issue and the negative press surrounding IDS (Gartner, 2003). Having said this, false positives are far from the only issue that can present problems, and a review of IDS literature reveals that challenges may be faced at a number of levels, from constraints during the initial rollout of the technology through to its effectiveness in ongoing use. Experience of the problems (or perceptions of them based upon received wisdom) may prevent IDS adoption from occurring, or lead to solutions being abandoned as unworkable.

For the purposes of this investigation, a total of 21 potential issues were identified, which were then grouped into five broad categories to reflect the nature of the problems and/or the point in the process at which they occur. These are discussed in the sub-sections that follow, with the brief descriptions provided in each case mirroring those that were used in the questionnaire study described later in this paper.

2.1 Deployment Challenges

The challenges here relate to problems that may be faced in terms of deploying an IDS in the first instance, and depending upon their severity may prevent further progress to an operational phase (Peddisetty, 2005; Salour and Su, 2007; Wei et al. 2001).

- *Scalability constraints*
  The size of the network can affect the efficiency of the IDS. For instance, as the size of the network increases, the efficiency of signature-based IDS decreases.
- *Switched networks*
  In the presence of switching technology, monitoring the network efficiently requires the deployment of more IDS to inspect the several network segments traffic.
- *Packet dropping and high speed network traffic*
  The high speed of network traffic combined with the information overload can cause packet dropping. Therefore, the probability of missing attacks increases.
- *Encrypted traffic and IPv6*
  Encrypted traffic attacks successfully reach the destination without being monitored by IDS.
- *Initial deployment cost*
  Deployment costs may include the cost of purchasing the IDS and the initial training for those who will be responsible for managing it.

Having been deployed, a number of further challenges may then be faced during the ongoing operation and use of IDS technology.

2.2 Management Challenges

Once deployed, the IDS represents another element of the IT infrastructure that needs to be managed and maintained. As such, there are a number of difficulties that can potentially arise from this direction (Cavusoglu et al. 2005; Conti et al. 2006; Teo and Ahn, 2007).

- *Volume of information*
  The amount information generated by the IDS increases the workload for the system/security administrator who has to consider it.
- *Ensuring effective configuration*
  It is difficult to tune the intrusion-detection system to minimize false alarms and missed attacks.
- *Managing a heterogeneous IDS environment*
  In the case of deploying multiple IDSs from different vendors, problems of interoperability might occur. Some of these differences might be in the way IDSs report alerts, their ruleset, etc.
- *Ongoing operational costs*
  The cost of maintaining IDSs can be significant, as it requires skilled staff to manage it, analyze and respond to the security alerts that are generated.

2.3 Technical Challenges

Beyond the general maintenance of the IDS platform, a number of specific issues need to be considered in terms of ensuring that it can operate correctly and be used effectively (Salour and Su, 2007; Smith et al. 2006; Xiao and Xiao, 2007).

- *Vulnerability to attacks*
  Some attackers target the IDS itself rather than other elements in the network, with the aim of bypassing intrusion detection. If attackers can take the IDS out service, further attack can be launched against other targets within the network.
- *Data collection and logging*
  Many sources can provide the IDS with data, which might have different formats. Therefore, there is a requirement to integrate these into an appropriate format for the IDS.
- *Difficulty in customizing and updating the IDS ruleset*
  One of the challenges is to keep the IDS ruleset regularly updated. In addition, it is important to customize the set of rules, in order to effectively detect attacks in the monitored network.
- *Understanding and interpreting IDS data*
  There is a requirement for an efficient methodology to log the network traffic and as a consequence, to analyze and validate the IDS alerts, in order to determine if actual intrusions are taking place. Moreover, the traffic logs and the alerts logs need to be presented in a meaningful and robust interface.

2.4 Detection Challenges

The challenges here are those that arise directly as a result of the IDS performing its analysis and generating alerts (Joo et al. 2003; Koike and Ohno, 2004; Xiao and Xiao, 2007). There is a clear relationship between some of these points and those already highlighted under the 'management' category (e.g. the issue of effective configuration and the subsequent effect upon false positives and false negatives).

- *The large number of alerts*
  IDS can produce a large number of alerts and can therefore require significant effort to monitor.
- *IDS can miss too many genuine attacks (i.e. false negatives)*
  A false negative occurs when the IDS fails to detect malicious network traffic, which as a result goes undetected.
- *IDS can raise too many erroneous alerts (i.e. false positives)*
  A false positive refers to the network traffic that the IDS considers malicious but are not.
- *Determining the alert severity level*
  There are no standard metrics for the alert severity level. Therefore, a combination of organization security policy and security operator experience is required in order to interpret and rank/prioritize the generated alerts.
- *Alert correlation*
  There is a requirement to study the relationship between the various IDS alerts to determine the occurrence of the attack scenarios. Hence, the alert correlation process is not trivial, and is often not without problems.

2.5 Response Challenges

The final group of challenges essentially relate to the ability to handle the alerts that an IDS has generated (Goodall et al. 2004; Peddisetty, 2005; Stakhanova et al. 2007).

- *Requirement for skilled staff*
  The requirement of highly skilled staff is the core of the IDS process. Without staff to manage the IDSs and analyze / validate considerable numbers of IDS alerts, the purpose of having an IDS becomes less and less useful.
- *The potential for inappropriate and harmful responses*
  Responses may cause harmful effects if issued on the basis of false positives. For instance, normal traffic might be blocked or a normal network session be terminated.
- *Effectiveness of the IDS response*
  Many IDSs are passive, they just report the damage caused by an attacker and provide the security operator with the collected information. Automatic response is cost-effective but most of the IDS responses are still manually even though manually response is time consuming.

In summary, this section has identified a variety of challenges that could have bearing upon IDS deployment decisions and affect their ongoing use. However, these issues are unlikely to have an equivalent impact in practice, and further investigation is therefore required to determine their relative influence. To this end, the decision was taken to survey the views of IDS users and other IT professionals who are familiar with the technologies.

3. Assessing IDS challenges in practice

In order to assess the perceptions and experiences of IDS-related challenges in practice, a questionnaire was designed in order to elicit the opinions of respondents with knowledge and experience in the domain. Specifically, the study sought to target:

- those who are (or have previously been) in a position to make IDS deployment decisions.
- those who have experience with IDS solutions in their organization.
- others who felt able to offer an informed opinion.

Email-based invitations to participate in the study and complete the web-based questionnaire were sent over 2,000 potential respondents, taken from a mailing list of local organisations that was purchased to support the study. In addition, the survey was promoted via the website of the local British Computer Society (BCS) branch and via direct contacts with persons working in large organizations (i.e. banks, hospitals, universities and telecommunication). Unfortunately, despite the large-scale promotion, only 41 usable responses were received during the 2 month period in which the questionnaire was available online (over 90 people visited the site and began the questionnaire, but only a subset completed it fully). The limited nature of the response was likely to have been influenced by the perceived sensitivity of the topic-matter, and the fact that participation could potentially have given insights into the security stance of the respondents' organisations (albeit with the assurance on the questionnaire itself that the findings would be anonymous and would only be used for the purposes of the study). Nonetheless, the majority of responses were received from

participants who appeared to be well-placed to offer an opinion, and the results proved to provide useful insights into the challenges that are faced.

The vast majority of respondents were able to claim practical experience of IDS (Figure 2), with a smaller majority also having deployed them within their current organisation (Figure 3). As such, the group as a whole was considered fairly well-placed to provide opinions. It is worth remembering that even those respondents without practical experience of IDS were able to offer relevant opinions, in the sense that they may have decided not to deploy IDS because of the challenges that they perceived.

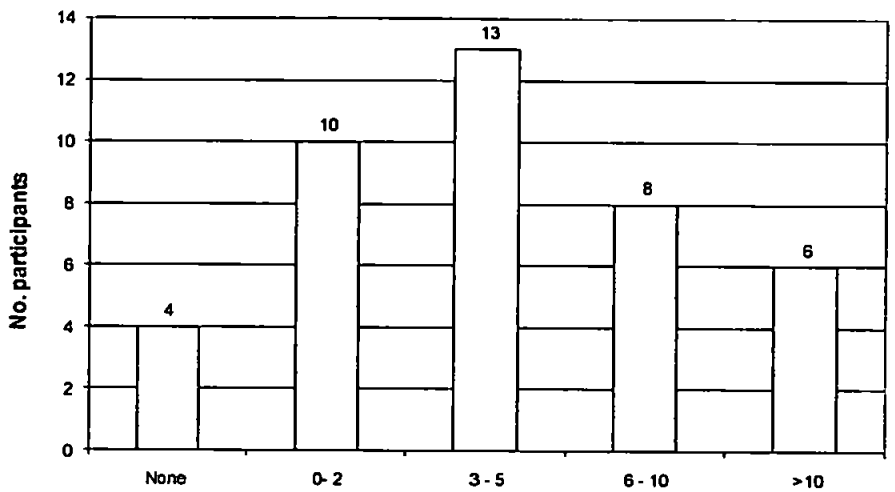


Figure 2 : IDS experience (years)

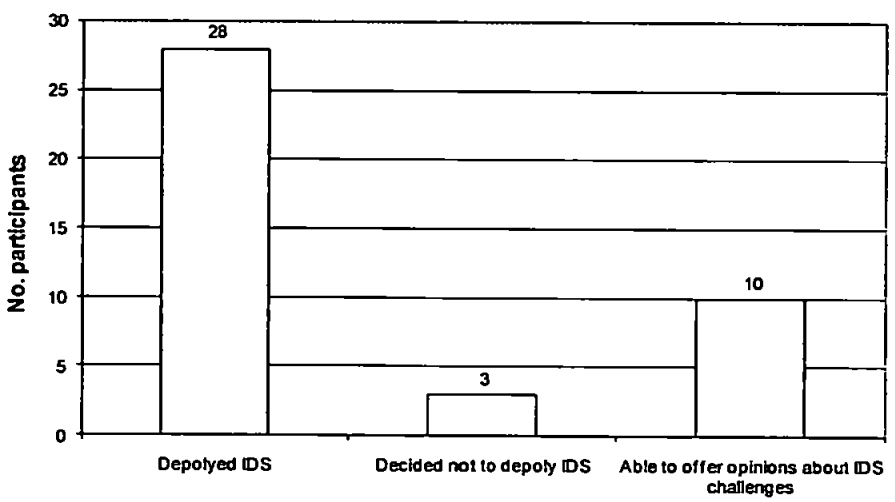


Figure 3 : IDS deployment within current organisation

More than two thirds of the respondents came from large organisations (500+ employees), while a fifth came from small organisations (<100 employees).

Having provided their background details, the respondents were asked to consider each of the 21 issues, and indicate whether they believed it to be a challenge or not. Each issue was rated

on a 5-point scale, from 'strongly agree' to 'strongly disagree', with a further option provided to allow 'Don't know' responses. At this stage in the questionnaire the potential challenges were considered individually, with no attempt to draw comparisons between them or rate the actual significance of each one. The findings are presented in Table 1, which shows the number of respondents in agreement for each issue (note that the columns are headed as follows: SA – strongly agree; A – agree; N – neutral; D – disagree; SD – strongly disagree; DK – don't know).

	Challenge	SA	A	N	D	SD	DK
	Deployment challenges						
1	Scalability constraints	8	20	3	5	4	1
2	Switched networks	9	15	5	6	3	3
3	Packet dropping and high speed network traffic	8	17	5	6	4	1
4	Encrypted traffic and IPv6	7	11	6	7	4	6
5	Initial deployment cost	8	23	6	0	2	2
	Management challenges						
6	Volume of information	16	20	2	1	1	1
7	Ensuring effective configuration	9	21	2	8	1	0
8	Managing a heterogeneous IDS environment	10	18	8	0	0	5
9	Ongoing operational costs	12	23	1	4	1	0
	Technical challenges						
10	Vulnerability to attacks	9	24	5	1	1	1
11	Data collection and logging	9	24	5	0	0	3
12	Difficulty in customizing and updating the IDS ruleset	9	23	6	1	1	1
13	Understanding and interpreting IDS data	13	23	4	0	0	1
	Detection challenges						
14	The large number of alerts	15	15	8	2	1	0
15	IDS can miss too many genuine attacks (i.e. false negatives)	12	15	11	2	0	1
16	IDS can raise too many erroneous alerts (i.e. false positives)	13	19	7	1	1	0
17	Determining the alert security level	2	27	8	2	1	1
18	Alert correlation	9	23	6	2	0	1
	Response challenges						
19	Requirement for skilled staff	13	19	6	3	0	0
20	The potential for inappropriate and harmful responses	10	20	9	1	0	1
21	Effectiveness of the IDS response	4	24	7	4	0	2

Table 1 : Individual assessment of IDS challenges

Respondents were also able to suggest other challenges in addition to the pre-defined set. In the majority of cases, no further suggestions were forthcoming, and thus those responses that were received would not usefully feed forward to influence the overall results. For the record, however, examples of the further issues flagged here included problems posed by polymorphic and zero-day attacks (which could arguably be linked to the issue of false

negatives already listed as challenge 15), and problems of visualising alerts (which can link to the challenges 14 and 18 from the table).

An examination of the table as a whole clearly reveals strong levels of agreement across the majority of the potential challenges. Indeed, this aspect is further illustrated by Figure 4, which presents the aggregate levels of response across the whole set and can therefore be taken as an overall measure of the degree to which respondents agree that IDS pose a challenge. It is clear from the overall volume of agreement-related responses that IDS are perceived as being far from problem free.

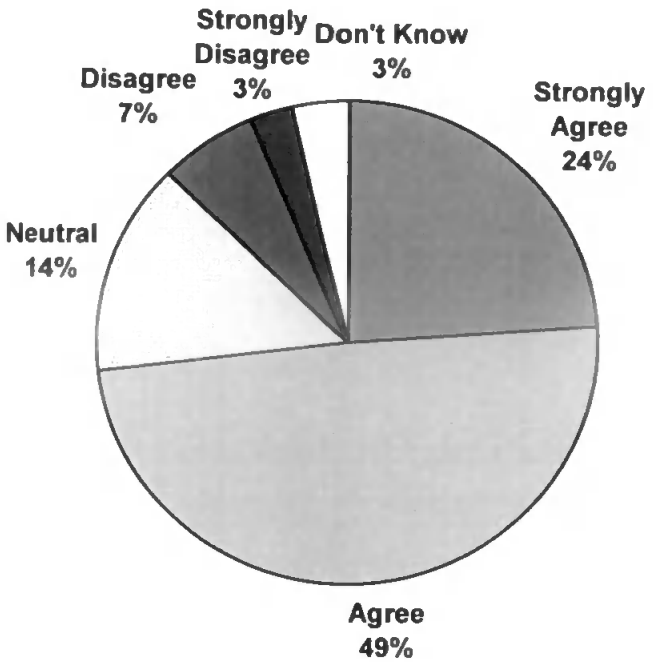


Figure 4 : Overall perception of whether IDS pose a challenge

Looking by category within Table 1, it is interesting to note that the highest levels of strong agreement are scored in relation to 'management' and 'detection' challenges, and with factors such as volume of information, the large number of alerts, and the occurrence of false positives drawing the highest scores across the set and a clear relationship able to be drawn between them. By contrast, the 'deployment' challenges category is most notable for the highest levels of disagreement, again tending to suggest that it is the ongoing operation of IDS rather than the initial establishment that poses the more significant challenge.

Having been asked about each of the challenges individually, the respondents were also asked to rate them relative to each other, by nominating a ranked list of the top 5 challenges. It is at this stage that the significance of the issues becomes more apparent, and it is notable that some points that were widely accepted as being challenges (e.g. the volume of information) no longer feature when the respondents were asked to consider them in this context. Figure 5 presents the results of this exercise, with the numbering of the challenges corresponding to the earlier list from Table 1.

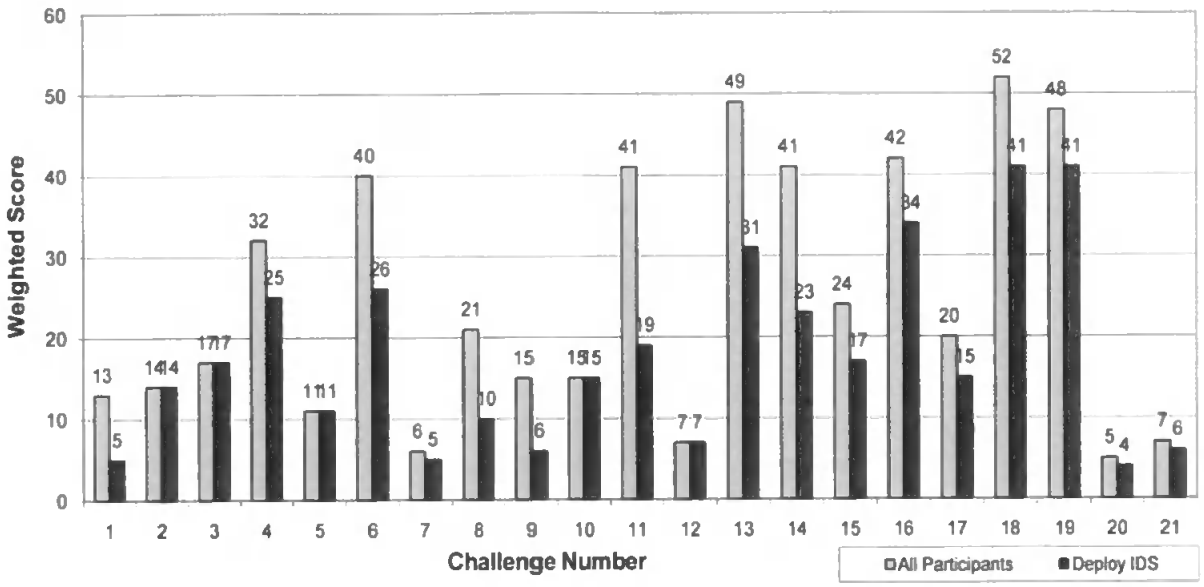


Figure 5 : Weighted ranking of top challenges

For ease of reference, the top-ranked challenges are summarised in Table 2, showing the order of the four most challenging aspects as identified across the whole respondent group and within the subset that had IDS deployment experience.

Rank	All respondents	Respondents deploying IDS
1	Alert correlation	Alert correlation
2	Understanding and interpreting IDS data	Requirement for skilled staff
3	Requirement for skilled staff	IDS can raise too many erroneous alerts (i.e. false positives)
4	IDS can raise too many erroneous alerts (i.e. false positives)	Understanding and interpreting IDS data

Table 2: Top-ranked IDS challenges

An examination of the results here reveals an interesting characteristic, in the majority of these issues can be related back to the effectiveness of people rather than the effectiveness of the technology. Specifically, the only factor from Table 2 that relates to the capability of the IDS is the issue of false positives. Meanwhile, alert correlation relies upon the ability of the IDS administrator to identify relationships and draw conclusions from the data, which in turn links to the challenges of understanding the data and the requirement for skilled staff. These findings are significant, in the sense that they are somewhat contrary to the received wisdom that the main impediment to the use of IDS is posed by the problem of false positives. Although it is still ranked much higher than many other potential issues, it does not emerge as the dominant issue that might otherwise be supposed. Of course, this is not to suggest that there is not a relationship between false positives and the other factors (e.g. with a larger volume of false positives there are more alerts to correlate, and thus more data to be understood by suitably skilled staff), but at the same time if we accept the likelihood that

some level of false positives are always likely to remain, then focusing attention towards reducing the other challenges would be a desirable approach.

4. Conclusion

From a conceptual perspective, IDS have the potential to provide a valuable contribution to the security of Internet-based systems. However, it is clear from the findings presented in this paper that they are considered to present a variety of challenges – the extent of which (or at least people's perception of them) could represent an obstacle to IDS being deployed at all.

Although there were significant levels of agreement for all of the suggested challenges when considered in isolation, it was interesting to observe the predominance of people-oriented issues when they were considered in a weighted ranking. Given that problems of skills and understanding were dominant even within a respondent group primarily composed from large organisations (i.e. where one would expect skilled staff to be available, or at least able to be hired), it can be assumed that the situation facing SMEs or end-users running IDS on personal systems would be even more severe.

The high placement of the people-related issues should not be interpreted to mean that technical challenges are insignificant or more easily resolved, but it would certainly be fair to say that greater attention has already been devoted towards addressing the technology issues. Consequently, what the findings here would suggest is a need to balance this with attempts to mediate the IDS and simplify the user experience. As such, these emerge as recommended areas for future research.

References

Cavusoglu, H., Mishra, B.K., and Raghunathan, S. 2005. "The value of intrusion detection systems in information technology security architectures", Inf. Syst. Res., vol. 16, no. 1, pp28-46.

Conti, G., Abdullah, K., Grizzard, J., Stasko, J., Copeland, J.A., Ahamad, M., Owen, H.L., and Lee, C. 2006. "Countering security information overload through alert and packet visualization", *IEEE Computer Graphics and Applications*, vol. 26, no. 2, pp60.70.

Gartner. 2003. "Gartner Information Security Hype Cycle Declares Intrusion Detection Systems a Market Failure", Gartner Press Release, 11 June 2003.

Goodall, J.R., Lutters, W.G., and Komlodi, A. 2004. "I Know My Network: Collaboration and Expertise in Intrusion Detection", in *CSCW '04: Proceedings of the 2004 ACM Conference on Computer-Supported Cooperative Work*, ACM Press, New York. pp342-345.

Joo, D., Hong, T. and Han, I. 2003. "The neural network models for IDS based on the asymmetric costs of false negative errors and false positive errors", *Expert Systems with Applications*, vol. 25, no. 1, pp69–75.

Koike, H. and Ohno, K. 2004. "Snortview: Visualization System of Snort Logs", in *VizSEC/DMSEC: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*. ACM, New York, pp. 143–147.

Peddisetty, N.R. 2005. State-*of-the-art Intrusion Detection: Technologies, Challenges, and Evaluation*, Master's Thesis, Linköping University, Sweden, 2005.

Richardson, R. 2007. *CSI Survey 2007: The 12th Annual Computer Crime and Security Survey*, Computer Security Institute. www.gocsi.com.

Salour, M. and Su, X. 2007. "Dynamic Two-Layer Signature-Based IDS with Unequal Databases", *Fourth International Conference on Information Technology: New Generations (ITNG 2007)*, Las Vegas, Nevada, 2-4 April 2007, pp77-82.

Smith, R., Estan, C. and Jha, S. 2006. "Backtracking Algorithmic Complexity Attacks against a NIDS", in Proceedings of 22nd Annual Computer Security Applications Conference (ACSAC'06), Miami Beach, Florida, 11-15 December, pp89-98.

Stakhanova, N., Basu, S. and Wong, J. 2007. "A taxonomy of intrusion response systems", *International Journal of Information and Computer Security*, vol. 1, no. 1/2, pp169-184.

Teo, L. and Ahn, G. 2007. "Managing heterogeneous network environments using an extensible policy framework". in *Proceedings of 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS'07)*, Singapore, March 2007, pp362-364.

Wei, H., Frinke, D., Carter, O. and Ritter, C. 2001. "Cost-benefit analysis for network intrusion detection systems", in *Proceedings of the CSI 28th Annual Computer Security Conference*, Washington, DC, October 2001.

Xiao, M. and Xiao, D. 2007. "Alert Verification Based on Attack Classification in Collaborative Intrusion Detection", in *Proceedings of Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 2007 (SNPD 2007)*, Qingdao, China, 30 July – 1 Aug 2007, pp739-744.

Assessing the Usability of End-User Security Software

T.Ibrahim[1,2], S.M.Furnell[1,3], M.Papadaki[1] and N.L.Clarke[1,3]

[1]Centre for Security, Communications & Network Research, University of Plymouth, Plymouth, United Kingdom
[2]Department of Mathematics, Faculty of Science, Assiut University, Assiut, Egypt
[3]School of Computer and Security Science, Edith Cowan University, Perth, Western Australia
{tarik.ibrahim, steven.furnell, maria.papadaki, nathan.clarke}@plymouth.ac.uk

Abstract. From a previous study we have determined that commercial security products can suffer from a usability perspective, lacking the necessary attention to design in relation to their alert interfaces. The aim of the paper is to assess the usability of alerts in some of the leading Internet security packages, based upon a related set of usability criteria. The findings reveal that the interface design combined with the user's relative lack of security knowledge are two major challenges that influence their decision making process. The analysis of the alert designs showed that four of the criteria are not addressed in any of the selected security measures and it would be desirable to consider the user's previous decisions on similar alerts, and modify alerts according to the user's previous behaviour.

Keywords: Security, Usability, Human Computer Interaction (HCI), Home Users, Intrusion Detection Systems, Security Software, Network Scanning

1 Introduction

Until relatively recently, home users could rely upon basic anti-virus (AV) as a sufficient level of protection for their systems. However, with evidence suggesting that as much as 95% of Internet attacks are directed towards home users [1], AV alone is no longer enough to protect against the range of threats [2]. Therefore, the deployment of other advanced solutions such as Firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) becomes necessary. Meanwhile, the management and manipulation of these solutions may require a level of IT literacy and security knowledge that many home users may not possess. The findings of [3] validate the requirement for high skilled staff to mange IDS in organizations, and it can easily be recognized that home users will face more difficulty in this respect. In recent years, security vendors have moved towards integrated AV, firewall and IDS tools, which are commonly marketed as *Internet Security* solutions [4]. However, although the combination of tools can provide users with a convenient and comprehensive solution, this does not necessarily guarantee attention to improving the usability. Ibrahim et al. [5] proposed a set of novel Human

Computer Interaction - Security (HCI-S) usability criteria and applied them to the evaluation of a typical alert raised by Norton 360. Even from a single example, this served to highlight a number of potential usability issues, and was considered sufficient to justify a wider evaluation of other tools against the same criteria. The current paper therefore investigates and assesses the usability of alerts across a wider range of security software.

The rest of the paper is organized as follows: Section 2 provides a brief description of our pre-proposed HCI-S usability criteria for end-user security tools. Section 3 then describes the approach that was used to generate alerts within the different tools, in order to yield a basis for evaluation. Section 4 then analyses and assesses the usability of the resulting alerts according to the HCI-S usability criteria. Finally, Section 5 presents conclusions about the findings and future directions of the research.

2 Usability Criteria for End-User Security Tools

Many studies have considered criteria for Human Computer Interaction (HCI). For example, Nielsen [6], [7] proposed a set of usability heuristics that are widely accepted and adopted. However, while numerous studies have addressed the issues of HCI and IDS individually, relatively little has been done to combine HCI and security together, and there is still an opportunity to integrate and extend the research in both disciplines to better support end users. For instance, Johnston et al. [8] modified Nielson's criteria and proposed a new set of usability criteria for security interfaces designed for end-users, evaluated via an analysis of Windows XP's Internet Connection Firewall (ICF). From this basis and other related work, Ibrahim et al. [5] proposed a further set of HCI-S usability criteria addressing the interface design of security alerts issued to end-user. These criteria are listed and summarised as follows:

1. **Interfaces Design Matches User's Mental Model:** Alert designers should attempt to think as users to develop interfaces match their mental model.
2. **Aesthetic and Minimalist Design:** Irrelevant or rarely needed information should not be displayed in the security alert.
3. **Visibility of the Alert Detector Name:** The appearance of the security tool name, which triggers the alert, is useful, specially, with the existence of more than one installed security tool on the user's system.
4. **Establish Standard Colours to Attract User Attention:** In general, the use of red and yellow colours in security alert interfaces is fairly standard. The red indicates a high severity alert; while the (orange or yellow) indicates a low severity one.
5. **Use Icons as Visual Indicators:** Users are most often affected by the use of pictures and icons in the interfaces.
6. **Explicit Words to Classify the Security Risk Level:** The user requires written confirmation of the security risk level and that information must be obvious in the main alert interface, not hidden in a secondary interface.

7. **Consistent Meaningful Vocabulary and Terminology:** The alert sentence(s) should be simple, short and informative and the words used in these sentence(s) should be familiar to the user.
8. **Consistent Controls and Placement:** The *Allow* and *Block* buttons exists in some security alerts without providing the user with any insight about the impact of this selection (e.g. the allowance or the blocking might be permanent or temporary).
9. **Learnability, Flexibility and Efficiency of Use:** The current criterion stresses the use of explanatory tooltips for concepts or security terms that appear in the alert to enhance the system flexibility, while providing links to a built-in library or/and an Internet web page, to increase the system efficiency.
10. **Take Advantage of Previous Security Decisions:** This criterion consists of two parts as follows: the user's own alert history (i.e. his previous responses to the alert) and community decisions (i.e. responses of other individuals to the alert).
11. **Online Security Policy Configuration:** Designers should develop an efficient default configuration for the security policy. The aim of the criterion is in guiding the user to adjust the security settings to avoid, if possible, any conflict between the intended primary tasks and the security configuration.
12. **Confirm / Recover the Impact of User Decision:** Sometimes, user errors are inevitable and vary from simple mistakes to dangerous errors. Therefore, the user should receive a confirmation message after performing any response, which will affect the security of the system.
13. **Awareness of System Status all the Time:** The user requires a simple report declaring the state of the system as a result of their response to the alert.
14. **Help Provision and Remote Technical Support:** The alert should be designed to let the users be self-sufficient; however, some novice users will still require further support. Tools should therefore provide built-in help and remote technical support.
15. **Offer Responses that Match User Expectations:** The actual impact of the available alert responses options does not always match the user's expectation. Therefore, good alert design is not only what is required to obtain a secure system but also to ensure the user's correct comprehension and understanding.
16. **Trust and Satisfaction:** Users' lack of understanding and/or inability to react correctly to alerts can strongly influence their resulting trust and/or satisfaction.

3 Assessing Security Tools Alerts

This section outlines the selection of the Internet Security tools against which the usability criteria were applied, along with the method by which the tools themselves were tested in order to generate the required security alerts. Having already identified Norton 360 during the earlier study, nine further Internet Security suites were selected to give a wider basis for evaluation. The selections were made on the basis of products recommended in a related review [9], plus the addition of products from F-Secure and Kaspersky (both

popular options within the home and small business user communities). A further criterion was that each product should incorporate an intrusion detection or/and prevention capability (ensuring the ability to detect attacks against systems). The resulting list of tools was as follows (noting that free trial versions were used in some cases): BitDefender Internet Security 2009; CA Internet Security Suite Plus 2009; F-Secure Internet Security 2009; Kaspersky Internet Security 2009; McAfee Internet Security 2009; Norton 360 Version 2.0; Panda Internet Security 2009; Security Shield 2009; Trend Micro Internet Security Pro 2009; and Webroot Internet Security Essentials. The resulting set is considered to represent a representative sample of the available security tools. However, it should be noted that the aim of the evaluation (and indeed this paper) is not to identify the best product, but rather to determine the extent to which usability issues can be identified across a wider base of software.

Network scanning represents the initial step in many types of attacks [10]. Many tools can be used, for instance Nessus [11] and Nmap [12]. This study adopts the default profiles of Nmap command lines within Zenmap GUI [12] to investigate the design of the alert interfaces triggered as a consequence. The evaluation experiments were held in a closed test bed environment consisting of two computers running Windows XP. Scanning processes were performed from the attacker computer running Zenmap GUI against the victim computer running the candidate security products. Table 1 illustrates the Zenmap GUI profiles and the correspondence Nmap command lines that are tested.

Table 1. Zenmap GUI profiles and the associated Nmap command lines

	Zenmap GUI Profile	Nmap Command Line
1	Intense scan	nmap -PE -PA21,23,80,3389 -A -v -T4 192.168.x.x
2	Intense scan plus UDP	nmap -PE -v -PA21,23,80,3389 -sU -A -T4 192.168.x.x
3	Intense scan, all TCP ports	nmap -PE -v -p1-65535 -PA21,23,80,3389 -A -T4 192.168.x.x
4	Intense scan, no ping	nmap -A -v -PN -T4 192.168.x.x
5	Ping scan	nmap -PE -PA21,23,80,3389 -sP 192.168.x.x
6	Quick scan	nmap -T4 -F 192.168.x.x
7	Quick scan plus	nmap -T4 --version-light -sV -F -O 192.168.x.x
8	Quick traceroute	nmap -p22,23,25,80,3389 --traceroute -PN 192.168.x.x
9	Regular scan	nmap 192.168.x.x
10	Slow comprehensive scan	nmap -PE -v -PS21,22,23,25,80,113,31339 --script=all -PO -PA80,113,443,10042 -sU -PP -A -T4 192.168.x.x

4 Analysis of End-Users Security Alerts According to HCI-S Criteria

During the evaluation, alerts were generated by all of the tools apart from McAfee, which did not issue any visible responses to the scanning attempts (note: this is not to suggest that they were undetected, but rather that the user was not explicitly notified in real-time). However, the variety of alerts generated via the other products satisfies the aim of the

study. The rest of the section focuses upon analyzing some key examples of these, according to the HCI-S usability criteria from [5]. Rather than commenting extensively against each tool, the discussion is structured according to the criteria headings, with examples being drawn from across the tools to illustrate significant issues.

4.1 Interfaces Design Matches User's Mental Model

Of the tools that explicitly notified the user of detecting a suspicious activity, all but Webroot's issued a response on behalf of the user. As shown in Fig. 1, Webroot's was the only alert that did not explicitly indicate whether the product had managed to handle the detected intrusion or not, nor give the user any further interaction options.

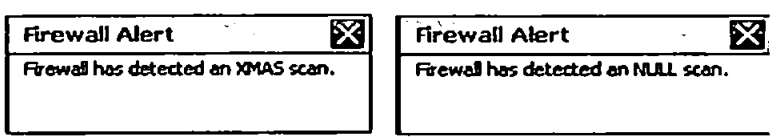


Fig. 1. Webroot's Internet Security Essentials alert interfaces

It is likely that alerts issued to users would be more usable through the occurrence of a user response sector in the bottom of the alert. For instance, Norton 360 (i.e. Fig. 2a) and Trend Micro are considered to be the only products that match the current criterion as they implicitly identified that the perceived intrusion access is blocked and present a user with *Allow* and *Block* options. Hence, the user has the benefit of both the automatic security response and the manual option to adjust and/or confirm the response. By contrast, Fig. 2b illustrates a different example of Norton's alert that does not match the current criterion because the alert does not include a description of the cause of the alert, or any links or tooltips to provide the user with more information.

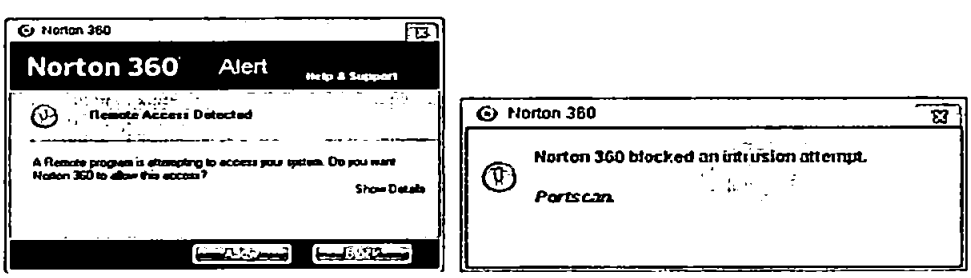


Fig. 2. Norton 360 intrusion alerts: (a) interactive (left) and (b) notification (right)

4.2 Aesthetic and Minimalist Design

In some cases alerts are too minimalist, with examples from Security Shield and BitDefender shown in Fig. 3. In these cases the source of the intrusion should be identified to the novice in a more meaningful manner (as they are unlikely to be greatly informed by the IP address), whereas more informed users may be interested in additional options (such as the opportunity to suppress further notifications).

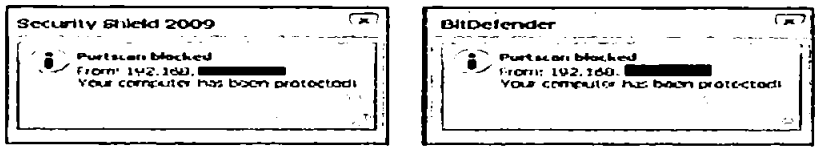


Fig. 3. Security Shield & BitDefender alerts interfaces

4.3 Visibility of the Alert Detector Name

With the exception of Webroot, all of the security tools provide the name of the detector in the head of their alert interfaces. Instead of indicating the name of the product suite (i.e. the thing that the user may most likely recall installing or recognise that they are running), Webroot's alert is attributed to the firewall, as shown in Fig. 1. Of course, many of the Internet security suites consist of integrated security solutions based on underlying components such as anti-virus, anti-spyware and firewall, and so it is perhaps not surprising that alerts appear under the name of these components rather than that of the wider suite. However, it would still be useful for the vendor name to appear so that the user has a basis for making the association back to the product they recognise. The problem with the anonymous alerts shown in Fig. 1 is that the user may wonder if they were caused by something else (e.g. by the Windows firewall or faked by malware).

4.4 Establish Standard Colours to Attract User Attention

The use of standard colours to express information to users in a simple and rapid way should be considered and addressed better to improve the design of alerts. With the exception of the traffic light colours, there are almost no other standard colours to represent the alert severity. Therefore, most likely, the use of the green colour indicates that the system status is secure, the use of the yellow colour indicates a low risk level and the red colour indicates a high risk level. For instance, Norton 360 and F-Secure used yellow in the exclamation icon to indicate the risk level of the detected activity. In contrast, Panda used the red colour within the *No Entry* symbol to indicate that an intrusion attempt is blocked. However, it is noticed that the border colour of most of the studied alerts are blue apart of Norton and Webroot's that are yellow and green,

respectively. The use of the blue border could be significant in case that these products are adapting a standard colour-coding such as the Homeland Security Advisory System (HSAS), where a wider range of colours are adopted (i.e. green, blue, yellow, orange, or red) to determine the severity of the threat level [13]. Finally, it is arguable that Webroot's use of the green colour provides a false secure impression to the user. Therefore, it is recommended to design alerts that have an appropriate border colour as an indicator to the threat level, and to avoid insignificant and misleading ones.

4.5 Use Icons as Visual Indicators

The use of icons as visual indicators should be essential, relevant and significant. Likely, users receive the primary alert message through the colours and icons. For instance, F-Secure and Norton 360 (i.e. Fig. 2a) use an exclamation mark icon as a visual indicator to indicate an intrusion attempt. Most likely, the yellow colour used within the icons indicates a low threat level. Unlike F-secure, Norton 360 alert confirms that indication explicitly through assigning *Risk Level: Low* within a complementary interface. Meanwhile, Panda uses the *No Entry* symbol aligned with a padlock icon, as shown in Fig. 4, to indicate that an intrusion attempt is detected and blocked. However, it is suggested to deploy appropriate icons that does not contradict criterion 4, *Establish Standard Colours to Attract User Attention*. Furthermore, Panda is the only product that uses two methods for deploying icons in the alert as an information mark icon is placed next to the technical term *Denial of Service* to indicate that there is more information available if required. The use of this icon is relevant and it would be more usable if the icon colour was more visible.

Fig. 4. Panda Internet Security 2009 alert interfaces and tooltips

4.6 Explicit Words to Classify the Security Risk Level

This criterion identifies one of the remarkable limitations within the design of the studied alerts. With the exception of Norton and Trend Micro, none of the evaluated products explicitly classify the security risk level. Norton 360 (i.e. Fig. 2a) determined the security risk level as *Risk Level: Low* in a complementary interface through clicking *Show Details*. In contrast, Trend Micro is more explicit by determining the security risk level in the main alert as *Risk: Safe*. However, assigning the risk to be *Safe* raises a question of the benefit of issuing the alert in the first place. From the usability perspective, addressing the

optimal location for assigning the security risk level is required. Therefore, it is recommended to present the risk level explicitly in the alert main interface, and then offer the associated reason for assigning this classification within a secondary interface.

4.7 Consistent Meaningful Vocabulary and Terminology

In general, the sentence(s) in most of the security alerts are simple and short, but there is no guarantee that these words are familiar to the user. For instance, Panda used the term *Denial of Service* aligned with a tooltip, but the provided information is neither a description nor a definition for the technical term. As most of the products make security decisions on behalf of the user, the user's main concern is likely to be whether the product has managed to deal with the problem or not. For instance, the words *denied* and *protected* are used to describe the product's response, but the most dominant word is *blocked* (as in *Intrusion attempt blocked!*). However, locating this sentence at the top, as shown in Fig. 4 , would satisfy some novice users who might decide not to run through the rest of the alert. In contrast, BitDefender and Security Shield use the sentence *Your computer has been protected!* to emphasize that the product had successfully protected the user from a threat, but the location of the sentence is at the bottom. Finally, it was found that the terminology within the alerts that requires user interaction such as Trend Micro's and Norton 360 (i.e.Fig. 2a), does not impede the user from making a security decision.

4.8 Consistent Controls and Placement

Most of the alerts do not supply users with explicit control features. Meanwhile, F-Secure provides buttons that enable the user to investigate the alert. In contrast, Norton 360 (i.e.Fig. 2a) and Trend Micro alerts consist of (*Allow* and *Block*) buttons located at the bottom of the alert interface. Most likely, this location is appropriate as the user reaches the buttons after running out through the alert. The main limitation of these buttons is that there is no indication of whether the impact of the user action is temporary or permanent. One solution could be appending another two buttons and explicitly defining the impact on the buttons such as *Allow Once* and *Allow Always*.

4.9 Learnability, Flexibility and Efficiency of Use

The use of explanatory tooltips for concepts that appears in the alert and/or the adoption of links to Internet web pages are rare among the evaluated alerts. For instance, Panda interfaces from Fig. 4 include the terms *Port scan* and *Denial of Service*, both of them are linked with explanatory tooltips but neither of them provides detailed information of the nature of the attack. instead, they determine the protocol, the remote IP address and the ports used in the attack. Furthermore, Kaspersky includes a *View report* link, but the

report does not provide the user with extra information and only includes the same information of the main alert in a more organized style. The alerts of Kaspersky and Panda share the same feature of having a drop list in the title bar at the top-right of the alert, Panda's list consist of two elements, *Help* and *Non-serious message settings*, with the *Help* option guiding the user to access a general built-in help and its introductory interface explains that the intrusion attempt is blocked via the built-in firewall. Therefore, relocating these features from the drop list to a better location within the alert interface (such as the bottom of the alert) would be more visible and useful.

4.10 Take Advantage of Previous Security Decisions

While all of the previous criteria were addressed by at least some of the evaluated security alerts, none of the products explicitly enabled users to leverage previous decisions to help them cope with the current alert. Therefore, the focus is upon assessing the alerts that required the user interaction such as Trend Micro's and Norton 360 (i.e. Fig. 2a). These products do not impede the user from making a security decision as the products already perform a blocking decision, identify the security risk level and provide response buttons. The novice user who does not have an experience with the cause of the present alert and does not have any further advice to call upon might find it more secure to implement the alert default response as these products did not specify any explicit recommendation to follow, such as accompanying the *Block* button with the word (recommended).Therefore, it is worth establishing an alert history that stores the user's previous decisions, to provide a source of reference if a similar alert arises in the future. Furthermore, it is suggested that the use of the social navigation method [14], would enrich the alert and to some extent support the user. Social navigation is considered to be a promising method in guiding novice users to make security decisions based on relevant individual decisions from those who have previously encountered similar alerts in their own environments.

4.11 Online Security Policy Configuration

This criterion is interested with integrating security policy features within the design of the alert itself. There are some attempts to provide this feature within some of the evaluated security products. For instance, CA and F-Secure provide a check box alongside text; *Don't show this alert dialog again.* Meanwhile, Trend Micro is more specific and uses a check box alongside the text; *Stop warning about this program,* and. since the program name occurs in the main alert, it would be clear that the user's decision affects only future events involving this program whatever the source IP address is, while in the previous instance it is not clear whether the decision would affect the program, the IP address, the port, or all the alerts. Another advantage of Trend Micro is that the check box is ticked by default as an explicit recommendation to the novice user. In contrast, Panda and Kaspersky adopt a different type of online configuration by providing a drop list.

Panda list contains the *Non-serious message settings* option which allows adjustment of alerts. While, Kaspersky provides the options *Disable this notification*, *Disable all notifications* and *Settings...*, the impact of the first option is unexplained to the user. As such, they may be unclear about whether the impact of selecting this option is to disable the future similar alerts (i.e. with the same details), to disable all alerts associated with the same type of attack regardless of the source, or to perform some other action. The previous examples are not the expected level of online security policy configuration and need to be enhanced as the exact impact of some options were not completely clear and some other options were irrelevant (i.e. related to configuring other types of notifications that are not linked to the current alert) which overloads the user with unnecessary secondary security issues at an inappropriate time. However, they are the only available examples in this study and one suggestion to satisfy this criterion is to provide an option to avoid frequent triggering of low-level alerts.

4.12 Confirm / Recover the Impact of User Decision

Confirming and recovering the impact of users' decisions is the second HCI-S usability criterion that is not addressed amongst the evaluated products. The absence of this criterion is illustrated by assessing Norton 360 (i.e. Fig. 2a) and Trend Micro, which provide control buttons that implement user's responses immediately without warning or reminding the user of the response impact, neither before nor after making the decision. Furthermore, there is no obvious method that informs the user of how to recover from wrong or inappropriate decisions. It is suggested that the security product should request additional confirmation, if the user overrides the recommended option. The objective of the message is to display the user's current decision and the perceived impact, and whether the user prefers to proceed accomplishing the decision or return back to the main alert interface to alter the response. However, the current suggestion combines both the benefit of confirming the user decision and a primary recovery method. Moreover, in some cases the user might perform inappropriate decision that affects the functionality of their intended tasks. Therefore, developing usable methods to recover from undesired decisions is a requirement. A suggested solution is to make benefit of criterion 10, *Take Advantage of Previous Security Decisions*, where all the previous user decisions are stored and then recalled when required. Hence, the user could access the recently issued alerts and the corresponding decisions, and attempt to change a previous decision if possible (e.g. if the user subsequently wishes to allow a program that was previously blocked by mistake). Finally, the product can make use from criterion 4, *Establish Standard Colours to Attract User Attention*, and decrease the possibility of the recovery situations by appending a green border around the recommended response button.

4.13 Awareness of System Status all the Time

This is the third criterion that is not fully addressed through the evaluated products. Most likely, users who installed security measures within their personal computers presume that the security situation is under control and there is no need to worry until they receive a security alert. When that happens, most of the evaluated security alerts declare that an intrusion attempt is detected and blocked. Hence, this is the type of awareness of the system status that these products provide to the user who will subsequently believe that he is protected. Meanwhile, as mentioned earlier, the McAfee product did not issue any alert during the evaluation, even though that the logs confirmed that it managed to detect the incoming traffic from the attacker computer. Hence, the user is not aware of the system status based on McAfee security policy. Furthermore, it is noticed that some products, such as Security Shield and BitDefender, display alerts that disappear quickly without the user's permission. Hence, there is a high possibility that the users would not notice the occurrence of the threat, especially if they were not looking at the screen at the time. If it is considered acceptable for users to miss them, then it questions the necessity of displaying the alerts in the first place. In contrast, Norton 360 (i.e. Fig. 2a) and Trend Micro, which provide a response capability, do not inform the user with the impact of the response issued by the user. The user ought to receive a message informing him about the real impact and the consequences of his response. Therefore, the awareness of the system status all the time is not available. For instance, if the user decided to use criterion 11, *Online Security Policy Configuration*, and disabled the appearance of all alerts, it would be useful to get the product icon in the notification area to produce yellow, orange, red pulses as the occurrence of low, medium, red security risk levels, respectively.

4.14 Help Provision and Remote Technical Support

The alerts generated by most of the tools do not need help or remote technical support; not because of their completeness, but because of the lack of user decision responsibility. Meanwhile, Panda and F-Secure provide a built-in help which might be useful to enhance user knowledge but it does not support the user response since there are not any response controls in the alert interface. In addition, as mentioned earlier, the location of Panda *Help* is not appropriate since it is embedded in a drop-down list. CA's product uses the question mark icon as a visual indicator aligned with a *Help* link to attract the user but the link provides no specific information relevant to the present alert. The assessment of Norton 360 (i.e. Fig. 2a) and Trend Micro - the two products that provide control features - reveals that no help or remote support is provided within Trend Micro apart from *Risk: Safe*. In contrast, Norton 360 is considered to be the only product that satisfies the criterion, as it provides a variety of help provision and remote support to the user. From a usability perspective, the main limitation is in the location of the options. For further details, an extensive discussion of Norton 360 is available within [5].

4.15 Offer Responses that Match User Expectations

This is the final criterion that is not fully addressed through the evaluated products. Firstly, most tools in the evaluation do not provide a user response component in the alert interface. Arguably, a portion of users would find it appropriate to have response options within the alert design. Secondly, Norton 360 (i.e. Fig. 2a) and Trend Micro are the only products that satisfy this feature and the assessment of the generated alerts reveals that there is no obvious method provided for the user to assess whether the response matches their expectation or not. Those users who have the privilege to respond to the alert perform their actions based upon their individual understanding. It is suggested to raise an explicit message after the user response to identify the real impact of the response. Hence, the user will be able to determine whether the response has achieved what they expected.

4.16 Trust and Satisfaction

In all likelihood, security products that managed to address most of the former HCI-S usability criteria are also able to satisfy and obtain the trust of users. Looking at specific factors that may improve this potential, we can consider whether the user is likely to feel they are getting the extent of information and feedback that seems convincing. For example, the design of the security alerts of Norton 360 and F-secure provide users with a level of satisfaction because of the amount of relevant information they attempt to provide. For instance, the main interface of F-Secure provides a *Details* button that lets the user access more information about the cause of the alert, and then onwards to access the alert logs via a *Show Alert Log* option.

4.17 Summary results

Table 2 summarizes the findings across the full set of tools and criteria (note that because Norton 360 generated two types of alerts the associated results column sometimes presents differing results, with the first relating to the alert represented in Fig. 2a and the other relating to Fig. 2b). The findings reveal a remarkable limitation is that choosing the *High* setting of the firewall alerts within the CA product bombards the user with hundreds of alerts (up to a maximum of 500). Most likely, the user will dismiss these alerts instead of suspending the intended task to investigate the massive amount of alerts. From a usability perspective, it is impractical to overwhelm the user, in one second, with this amount of alerts specially that they only vary in detailed information of hundreds of local and remote ports used during the penetration. From the usability perspective, although the use of the *Show Details* link within Norton 360 (i.e. Fig. 2a) is usable, it would be preferable to avoid using the vertical scroll bar within the interface. Finally, the paper demonstrated to what extent the HCI-S usability criteria are addressed through the evaluation of collection of users security products. The findings reveal the strength and

the weakness within the design of the issued alerts and some primary solutions are suggested as an attempt to resolve these weakness. It is anticipated that integrating the adequate features of the evaluated alerts, avoiding their limitations, and implementing the unaddressed HCI-S usability criteria, will enhance the design and make it more usable.

Table 2. The usability aspects of end-user security software

No	Novel Criteria	BitDefender	CA	F-Secure	Kaspersky	Norton	Panda	Security Shield	Trend Micro	Webroot
1	Design Interfaces Match User Mental Model	✗	✗	✗	✗	✓✗	✗	✗	✓	✗
2	Aesthetic and Minimalist Design	✗	✓	✓	✗	✓✗	✓	✗	✓	✗
3	Visibility of the Alert Detector Name	✓	✓	✓	✓	✓	✓	✓	✓	✗
4	Establish Standard Colours to Attract User Attention	✗	✗	✓	✗	✓	✓	✗	✗	✗
5	Use Icons as Visual Indicators	✓	✗	✓	✗	✓	✓	✓	✗	✗
6	Explicit Words to Classify the Security Risk Level	✗	✗	✗	✗	✓✗	✗	✗	✓	✗
7	Consistent Meaningful Vocabulary and Terminology*	✓	✗	✓	✓	✓	✓	✓	✓	✓
8	Consistent Controls and Placement	✗	✗	✗	✗	✓✗	✗	✗	✓	✗
9	Learnability, Flexibility and Efficiency of Use	✗	✗	✓	✓	✓✗	✓	✗	✓	✗
10	Take Advantage of Previous Security Decisions	✗	✗	✗	✗	✗	✗	✗	✗	✗
11	Online Security Policy Configuration	✗	✓	✓	✓	✗	✓	✗	✓	✗
12	Confirm / Recover the Impact of User Decision	✗	✗	✗	✗	✗	✗	✗	✗	✗
13	Awareness of System Status all the Time	✗	✗	✗	✗	✗	✗	✗	✗	✗
14	Help Provision and Remote Technical Support	✗	✗	✗	✗	✓✗	✗	✗	✗	✗
15	Offer Responses Match Expectations	✗	✗	✗	✗	✗	✗	✗	✗	✗
16	Trust and Satisfaction	✗	✗	✓	✗	✓	✗	✗	✗	✗

* With the exception of the terminology that requires the assistant and the adoption of criterion 9 in some instances, the current criterion is rated according to the meaningful vocabulary to the end-user.

5 Conclusions

This paper investigated the usability of security alerts issued via a range of security products. The analysis showed that four of the HCI-S usability criteria (10, 12, 13, 15) are not addressed in any of the selected security measures. Specifically, none of the evaluated tools address criterion 10, to Take Advantage of Previous Security Decisions. Therefore, it would be desirable to leverage previous decisions on similar alerts, and modify alerts accordingly to account for the user's previous behaviour. For example, if the user has consistently overridden the recommended option in a particular alert, the system can change the default option to their previous choice, or offer them the option to repeat their

decision in future without the need for an alert. In order to give this level of flexibility, it is important to enable users to make informed decisions and recover from them if needed. Therefore, it is important to address criteria 12, 13, 15 as well (namely Confirm / Recover the Impact of User Decision, Awareness of System Status all the Time, and Offer Responses Match Expectations). Future work will focus on addressing these missing criteria and increasing the end-user's opportunity to customize the security measure.

References

1. Symantec. Symantec Internet Security Threat Report. Trends for January 07 – June 07, vol. XII. Symantec Enterprise Security, September (2007)
2. House of Lords. Science and Technology Committee. 5th Report of Session 2006–07. Personal Internet Security. United Kingdom Parliament. HL Paper 165–I. London: The Stationery Limited.http://www.parliament.the-stationery-office.co.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf. (Accessed: 15/11/2009)
3. Ibrahim, T., Furnell, S. M., Papadaki, M., Clarke, N. L.: Assessing the Challenges of Intrusion Detection Systems. Proceedings of the 7th Annual Security Conference. Las Vegas, USA. 2nd-3rd June (2008)
4. Lai, K. and Wren, D.: Antivirus, Internet Security and Total Security Performance Benchmarking. http://www.passmark.com/ftp/antivirus_09-performance-testing-ed1.pdf
5. Ibrahim, T., Furnell, S. M., Papadaki, M., Clarke, N. L.: Assessing the Usability of Personal Internet Security Tools. Proceedings of the 8th European Conference on Information Warfare and Security (ECIW 2009), Military Academy, Lisbon & the University of Minho, Braga, Portugal, 6-7 July (2009)
6. Nielsen, J.: Enhancing the explanatory power of usability heuristics. Proceedings of ACM CHI'94 Conference. Boston, Massachusetts, USA. 24-28 April, pp. 152--158. (1994)
7. Nielsen, J. Ten usability heuristics. http://www.useit.com/papers/heuristic/heuristic_list.html. (Accessed: 14/12/2008).
8. Johnston, J., Eloff, J. H. P., Labuschagne, L.: Security and human computer interfaces. Computers & Security, vol .22, issue 8, pp. 675--684 (2003)
9. Top Security Software. http://www.2009securitysoftwarereviews.com. (Accessed: 26/01/2009)
10. Barnett, R. J., Irwin, B.: Towards a Taxonomy of Network Scanning Techniques. Proceedings of the 2008 annual research conference of the South African Institute of Computer Scientists and Information Technologists on IT research in developing countries: riding the wave of technology, (SAICSIT '08), Wilderness, South Africa, 6-8 October, pp. 1--7 (2008)
11. Nessus. The Network Vulnerability Scanner. http://www.nessus.org. (Accessed: 26/01/2009)
12. Nmap. Nmap Security Scanner. http://insecure.org/nmap. (Accessed: 26/01/2009)
13. Siraj, A., Vaughn, R.: A Dynamic Fusion Approach for Security Situation Assessment. Proceedings of the Fourth IASTED International Conference on Communication, Network, and Information Security (CNIS 2007), Berkeley, California, 24–26 September (2007)
14. Chiasson, S., van Oorschot, P. C., Biddle, R.: Even experts deserve usable security: Design guidelines for security management systems. Proceedings of Symposium on Usable Privacy and Security (SOUPS 07), Pittsburgh, PA, 18-20 July (2007)