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.

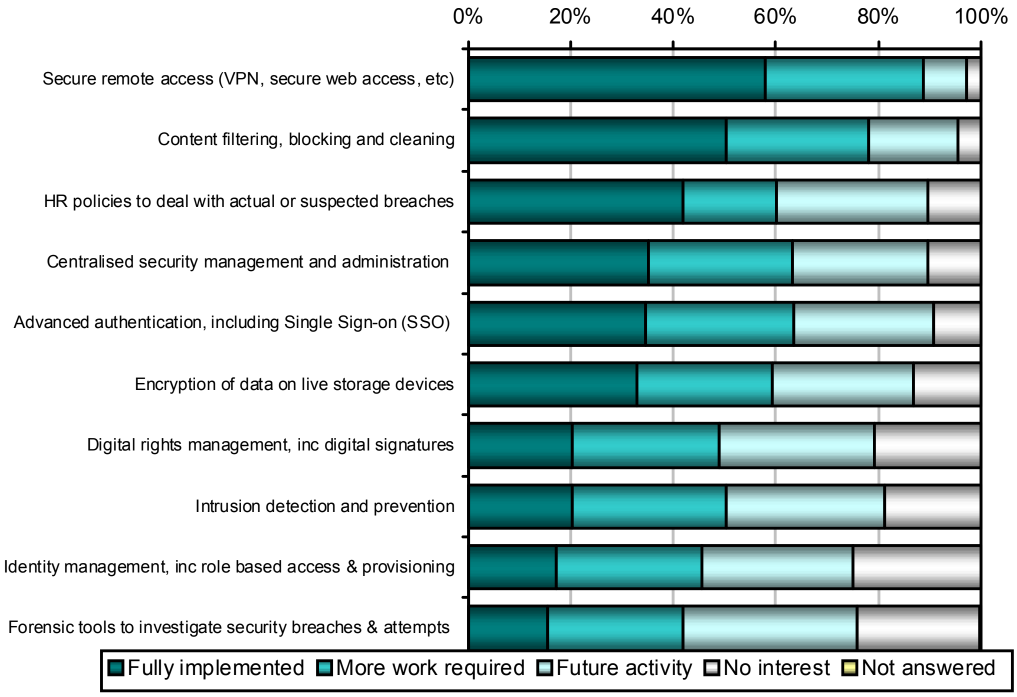

Figure 1 : Implementation of security measures (Source: Freeform Dynamics)

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.

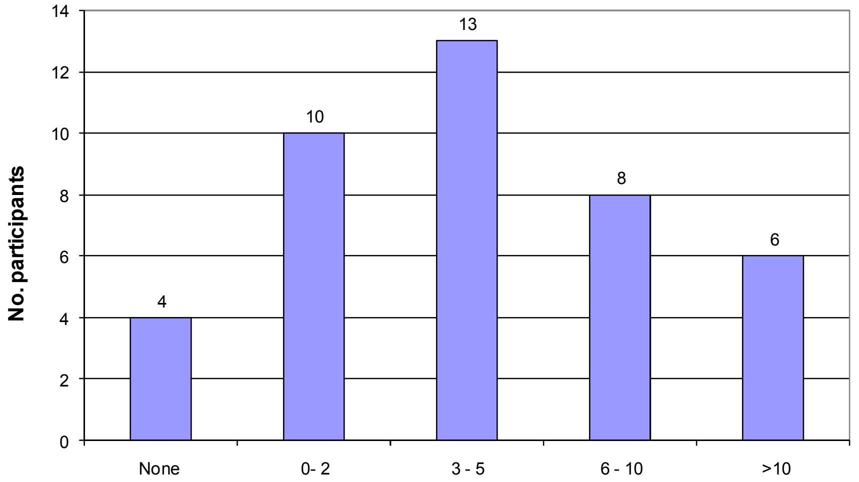

Figure 2 : IDS experience (years)

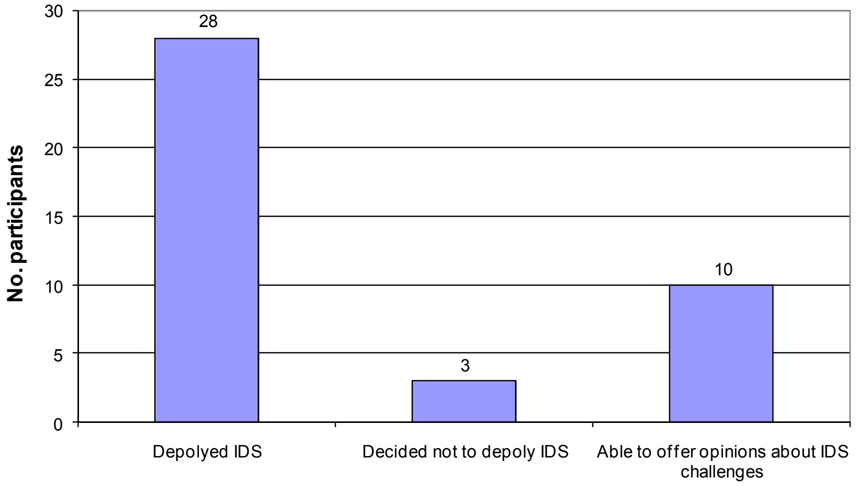

Figure 3 : IDS deployment within current organisation

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.

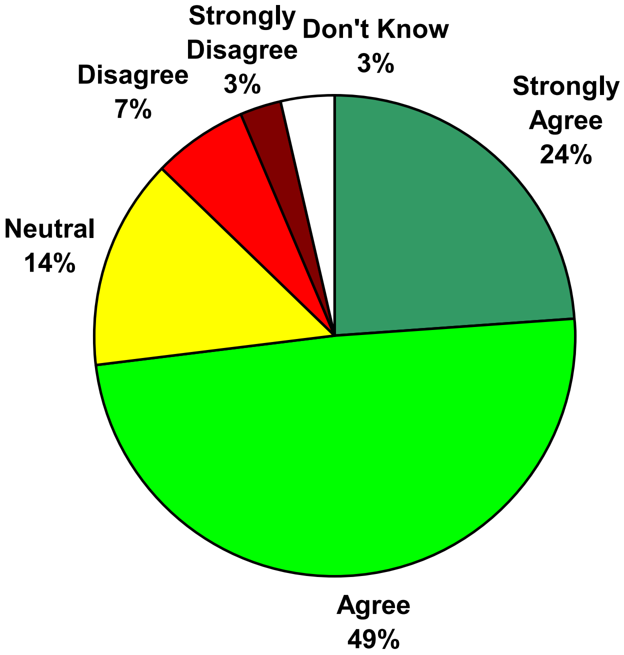

Figure 4 : Overall perception of whether IDS pose a challenge

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.

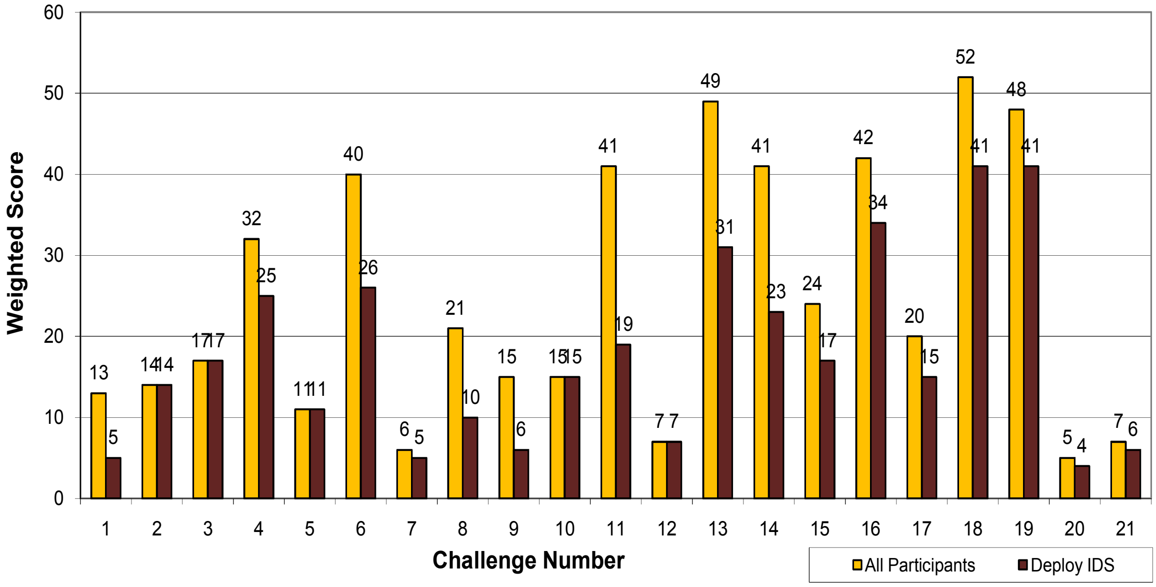

Figure 5 : Weighted ranking of top challenges

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.