Intrusion Prevention Systems: The Future of Intrusion Detection?

Corinne Lawrence

University of Auckland

26th October 2004

Table of Contents

Abstract:

Computers and computer networks have become essential to our way of life and with this dependency comes the need to maintain the security of these systems. This paper looks at the early assumptions behind Intrusion Detection Systems (IDSs) and how they led to certain intrusion detection approaches still in use today. It continues with the pitfalls of legacy as well as modern IDSs, and why the way we approach security has been shifting from detection to prevention. In conclusion, it looks at Intrusion Prevention Systems (IPSs) as a possible replacement for current IDSs as well as other future possibilities to help improve the protection of our computer systems.

I Introduction

With more people using computers and connecting to the Internet than ever before, there has been an increase in the reach of cyber vandals. From the mid-to-late 1980's, when networks became widespread, to now, when they are ubiquitous, the pervasiveness of computer systems and networks has been accompanied by a more than proportional increase in the ways in which these systems can be attacked. Worms, viruses and Trojans now have the capability of wreaking even more havoc than was previously possible and less technical expertise is required to achieve this crippling of computer systems. This has led to an intensification in the need for IDSs that prevent a system from being compromised and also protect data whose sensitivity is critical to the organizations success.

Security has not been the main concern for companies, especially since security gains cannot easily be measured and also because security more often than not means giving up an added feature or missing out on user convenience[1]. As a result, the goal of a reasonable amount of security for our computer systems is far from being achieved, with a faction of the industry believing that IDSs have past their use-by date.

This paper begins with an introduction to Intrusion Detection - a discussion of some of the assumptions behind early IDSs, how they relate to current approaches of intrusion detection: anomaly and misuse based detection as well as the problems with these assumptions. A considerable section of the security community are of the opinion that intrusion prevention is the way of the future. This paper compares intrusion detection and intrusion prevention, delving into the possible reasons why early IDSs did not incorporate more preventative measures. It goes on to describe the failures of IDSs as they stand today and why a change in the way we approach protection of our systems is needed. The paper concludes with a discussion of future possibilities of intrusion detection, with a focus on IPSs.

[1] [Lam] B. Lampson, "Computer Security in the Real World", IEEE Computer Society, 37-46, 2004.

II Early IDS Assumptions

According to John McHugh [McH], early intrusion detection work was based on two main assumptions: one, that certain kinds of intrusion would be easily able to be detected and rules to detect them could be easily written because the intrusions would be obviously expressed; and two, that deviations from what was considered to be normal behaviour by the user or programs could be taken as definite signs of intrusion or malicious activity[2].

McHugh wasn't the only one who considered that any digression from "normal" behaviour signalled intrusive activity. In her 1987 paper, "An Intrusion Detection Model", Dorothy Denning proposed a model for intrusion detection that was based on the premise that exploiting a system meant using it in a manner that was abnormal[3]. It therefore followed that recognizing abnormal patterns in the use of a system would mean the detection of instances where the system had been compromised. She goes on to give examples of how misuse of a system can be detected by abnormal patterns: attempted break-ins would have an unusually high amount of wrong passwords before they are let in, if they are let in at all; unauthorized users would have different login times, connection type and location to that of a legitimate user in addition to accessing different types of files (browsing directories and executing system status commands compared to a normal user who would go about his normal job, editing files, etc.); and other such examples [De].

The first assumption that certain kinds of intrusion would be manifested in obvious ways and would therefore be a simple matter to detect [McH] seems at first to be a reasonable one. If for example a cyber vandal gained access to your network resources, he would most likely use it for to perpetrate a denial of service (DoS) attack on an unsuspecting e-commerce site; if he got his hands on sensitive business data, he would probably sell it to your competitors for a bundle of money. Either way you'd know pretty quickly that your security had been compromised. But what if the

[2] [McH] J. McHugh, "Intrusion and Intrusion Detection", *International Journal of Information Security I*, 14-35, 2001.

[3] [De] D. Denning, "An Intrusion-Detection Model", *IEEE Transactions on Software Engineering*, Vol.SE-13, No.2, February 1987, 222-232.

attacker was very highly skilled? What if his purpose was not to use your resources to flood a website for whatever reason? What if his sole aim was to penetrate your system, masquerade as a legitimate user and slowly but surely accumulate information about the network: users, system resources, data, anything, for him to use as he wished at a later date. If he was expert enough, and there are very many of these diabolically talented hackers out there, there would be no manifestations, obvious or otherwise, of his presence in your network.

III Misuse and Anomaly Detection

McHugh's first assumption goes on to say that because the intrusions are expressed in a manner that is obvious, it follows that writing rules to detect them would be an easy matter [McH]. In my opinion, this holds true to a very limited extent only. If the intrusion had been tried in the past, then there would already be a record of the patterns it produced. These could be matched against what was currently happening and the exact type of attack could be pin-pointed, leading to a quicker response to the attack in terms of counter-measures and also ways in which the wrong-doer could be apprehended. This is the principle on which misuse detection is based. IDSs that use misuse or signature based detection look for sets of events that match a predefined pattern of events or a "signature" that describe a known attack, as explained by Rebecca Bace and Peter Mell[4].

The main advantage of this type of intrusion detection is that false alarms are not triggered very often as each attack has a very explicit signature that has to be matched in order for an alert to be sparked off. Its very advantage though has a downside – specific and strict rules for generating matches with previous attacks mean that penetrations attempted using slight variations of previously used attacking techniques will probably go unnoticed. This has been overcome with the use of state based misuse detection, which uses one set of rules to detect not one specific attack but a series of potential attacks. Since state-based detection is not widely used in commercial IDSs however, the problem is still rife.

[4] [Ba] R. Bace and P. Mell, "Intrusion Detection Systems", *NIST Special Publication on Intrusion Detection System*, 1- 51.

The second assumption cited by McHugh and also mentioned by Denning was that any divergence from “normal” behaviour could be attributed to foul play with a fair amount of certainty and this is the premise on which anomaly based intrusion detection is based [McH], [De]. Since abnormal behaviour presupposes illegitimate use of the system, Bace says that systems detecting behaviour that deviates from the norm would also detect intrusions. Anomaly detectors build profiles of what constitutes “normal” behaviour by accumulating data for normal running of the system and then, after the profiles have been put together, use various techniques to measure any departure from this line of normal behaviour [Ba].

Anomaly based detection is advantageous because it doesn’t require a lot of details in order to earmark a particular set of events as being an attack. In this way, new and innovative methods of penetrating networks have been detected as attacks and damage kept to the minimum. As with misuse detection, its very advantage has a downside. Triggering alerts whenever a deviation from normal behaviour is detected means that a very large number of false alarms are set off. While anomaly based systems can be “taught” that some abnormal behaviour isn’t bad, for example a network technician doing making system calls to expose the weak points of a network, the false alarm feature of IDSs has been an important factor in the rise of IPSs as an alternative to IDSs.

IV Detection vs. Prevention

According to Bace and Mell, intrusion detection is analysing the events that occur in a computer system for attempts that have been made to “compromise the confidentiality, integrity, availability” of the system and its data or to bypass the networks security mechanisms. They defines IDSs as “hardware or software products that automate this monitoring and analysis process.” [Ba]

Dinesh Sequeira, in his very informative paper on Intrusion Prevention Systems (IPS) cites another explanation by Richard Kemmerer and Giovanni Vigna, “… intrusion

detection systems do not detect intrusions at all – they only identify evidence of intrusion, either while in progress or after the fact.[5], [6]"

According to Timothy Wickham [Wi], the reason for choosing to detect intrusions to the system rather than prevent them from occurring in the first place, were hardware and software limitations that led to accuracy problems, where instances where a system was compromised weren't detected as well as performance problems caused by false alarms[7]. Wickham also cites a statement made by Richard Stiennon, Gartner Research Director, "Legacy IDS technology was built on the belief that the number of security vulnerabilities and clever hackers targeting them is too daunting a task to prevent, thus enterprises have been relegated to monitoring activity, rather than attempting to block attacks."[Wi]

In my opinion, however, the early attempts at IDS were not conscious decisions at "detection" as opposed to "prevention". Since the use of computers and computer networks had only become widespread by the mid-to-late 1980's, as mentioned by McHugh, the field was new and the pioneers probably just played it by ear. Most penetrations around that time were because of careless administration – preset accounts with administrator privileges that weren't changed on being installed; guest accounts that could be exploited to penetrate the system and compromise a huge number of machines and other such scenarios. The Morris Worm in 1988 was an example of the direct attacks on system software that were also developed at that time. In Unix, file creation is not atomic, requiring one call for the creation of an i-node for the file being created, and another system call to link the file to the directory structure. The Morris worm exploited this by switching the context during the creation of .rhost files, thereby gaining control of the i –nodes controlling the .rhost files. Since the .rhost files, a kind of access list, contained the names of users from which scripts could be accepted, the worm was able to re-write these files and allow

[5] [Se] D. Sequeira, "Intrusion Prevention Systems – Security's Silver Bullet?", *SANS Institute2002*, GSEC Practical v1.4b, Option1, 2002.

[6] [Ke] R. Kemmerer and G. Vigna, "Intrusion Detection: A Brief History and Overview", *IEEE Security and Privacy*, 27-30, 2002.

[7] [Wi] T. Wickham, "Intrusion Detection is Dead. Long Live Intrusion Prevention!", *SANS Institute 2003*, GSEC Practical v1.4b, Option1, 2003.

rogue users to be on the "friendly" list, thereby allowing malicious scripts to be run on remote computers. This remote executing of scripts was made possible by a misconfiguration in the sendmail program that was left in the binary versions deliberately – to enable easy configuration and debugging since the program was very hard to set up [McH].

The reason for including these details on a paper on IPS is this; all the early attacks on software systems were the first of their kind. They were not expected so the option of *preventing* them from occurring did not arise. Once they had been perpetrated however, steps were taken to safeguard systems against this sort of an attack-tightening up of administrative practices, use of anti-virus programs and patches as well as IDSs to detect these penetrations in case they occurred in spite of these prevention measures. Thus early intrusion detection systems were "detection" rather than "prevention" based not because prevention seemed to daunting a task to even attempt, but because detection seemed to be the most logical answer to the problem at hand.

V Failures & drawbacks of IDS

With the increasing amounts of traffic through our networks, performance is an important factor in any decision that is made regarding an organization's network. As explained in the discussion of anomaly based intrusion detection above, modern IDSs generate a lot of false alarms. When deviations from the norm are detected, alerts are triggered. This gives rise to so many alarms, most of which tend to be baseless, that network administrators are wont to skim over the warnings and thereby miss the signals of a lethal attack as mentioned by Matthew Tanase [Ta] in his 2001 article[8]. One way of dealing with this is to specify stricter rules as to what constitutes an attack. With more comparisons that need to be made in order to trigger off an alarm, there are network performance hits, which is a very niggling worry for today's administrators. Besides the performance issue, more specific patterns for intrusion detection mean that in order to be detected, future attacks on the system must match every aspect of the new, stricter rules. This means that penetration

[8] [Ta] M. Tanase, "The Future of IDS", *SecurityFocus*, 2001. URL: http://www.securityfocus.com/infocus/1518

attempts that are slight variations of attacks that occurred in the past, but don't match them exactly, have a high likelihood of entering undetected.[Ta]

Another side to the performance worry, according to Ted Holland, is that most of today's IDSs, even with high performance components designed for maximum data capture still tend to drop packets during times of heavy throughput across the network[9], which doesn't really justify the considerable increase in cost of setting up an IDS just because it contains these high performance components that don't do what they're meant to anyway.

Increasing amounts of traffic through a network has also meant the slow but sure shift of modern networks to being switched ones. Switches provide better performance by sending the data to the required ports only and as Tanase pointed out, this also provides protection against packet sniffers getting hold of your data. The problem though is that switched networks, while preventing unauthorized systems to view data, also effectively keep Network Intrusion Detection Systems (NIDS) from doing their job. NIDS analyse packets over a particular stretch of the network, i.e., somewhere in between the sender and the receiver, which means that another problem they face is encrypted data [Ta]. Although the NIDS possess the signatures to match incoming or outgoing data against, with increasingly pervasive wireless networks and VPNs, they either don't get sent the data to match the signatures against, or, if they do get the data, it's in a form that they aren't in a position to understand [Wi].

In addition to this, attackers practice IDS evasion techniques, as stated by Sequeira. The key to this is feeding the IDS a different set of data than is sent to the victim, thereby fooling the IDS into thinking the data is legitimate and in no way dangerous. Sequeira goes on to list some evasive tactics used: hex encoding, path obfuscation and fragmentation, to name a few [Se].

[9] [Ho] T. Holland "Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth ", *SANS Institute 2004*, GSEC Practical v1.4b, Option 1, 2004.

IDSs, by their very definition only monitor computer systems for the occurrence of intrusions. They are reactive – wait passively for a penetration to occur and then tell you what it is that went wrong. Moreover, they aren't always able to do even this. With the wide variety of attacks that our systems have recently been under, it is not a done deal for an IDS to be able to identify what vulnerability or flaw made the penetration possible. Sometimes, with hackers that are sophisticated enough, the fact that the system has in fact been compromised is not always apparent at all. All of the above have led to the identification of a need to either augment IDSs to overcome these deficiencies or do away with them entirely, in favour of a more powerful and reliable system. The answer lies in intrusion prevention.

VI Intrusion Prevention Systems

IPSs are hardware or software tools that identify threats to a computer system and prevent them from penetrating it. More and more organizations are looking to IPS for their security needs because IPSs provide a means by which administrators can be proactive in their approach to securing their networks, as Wickham suggested, actively blocking attackers from penetrating the system, instead of passively waiting for a penetration to occur and then going about minimising the damage wrought on their networks [Wi].

Holland says that while IPS technology is a relatively new affair, the idea behind it has been around a while [Ho]. As far back as the Morris Worm, access control lists have been in place; switched networks that aren't conducive to packet sniffing, firewalls that block unwanted network traffic and antivirus programs that don't allow suspect programs to be run on your computer, all could be argued to be some sort of rudimentary IPSs.

According to Adrian Brindley in his paper titled Denial of Service attacks and the emergence of "Intrusion Prevention Systems" [Br], emerging IPS products will

assimilate anti-DoS capabilities as well as auto updates to ensure that the protection mechanism is as up-to-date as possible[10].

VII Approaches to Intrusion Prevention

There are a few different approaches taken towards achieving intrusion prevention mechanisms that were mentioned by Sequeira: using a mixture of methods like anomaly and misuse based detection to determine when attacks are imminent and then blocking potentially dangerous traffic; a heuristic approach that is similar to anomaly detection in IDS, only more proactive than its forbear; kernel based protection, which prevents malicious code from running system resources like memory, I/O functions, etc and finally a quarantining approach where executable scripts and applets are restricted to a monitored area and their level of danger is assessed [Se].

The evasive tactics mentioned above, that work to confuse the IDS, are also mentioned by Mike Bobbit[11]. He talks about them in terms of how harm to a system can be prevented: protecting the system resources from calls by malicious code or hacker tools; preventing ordinary or even guest users to exploit the system and extend their usage to encompass administrator privileges; checking whether executable scripts originated from a normal application or an overflowed buffer (the Morris Worm used the overflowing of a string variable to exploit the sendmail program). All of these counter-evasive techniques can form a part of systems IPS, protecting the network from attacks by vandals and preventing penetrations from occurring [Bo].

Wickham introduces two IPS vendor solutions that might not be as effective as the vendors would like us to believe – TCP resetting and Firewall shunning. TCP rests work by breaking the connection with the malicious traffic before the exploit can occur. While this sounds perfectly effective in theory, in practice the IDS/IPS combination spots the dangerous data at the same time the victim does, which means

[10] [Br] A. Brindley, "Denial of Service attacks and the emergence of 'Intrusion Prevention Systems'", *SANS Institute 2003*, GSEC Practical v1.4b, Option 1, 2002.

[11] [Bo] M. Bobbit, "Inhospitable Hosts", *Information Security*, Volume 5, No. 10 (2002): 35-47, 2002.

that the harm has already been done to the system. One way of averting this problem would be to have the TCP reset mechanism on the network portion of the IDS so as to enable it to detect attacks well before the victim is reached. This approach isn't the answer because if the attack was encrypted, then the IDS/IPS wouldn't even detect its potential danger, leave alone break the connection. Also, TCP resets only work for data using TCP and are completely useless with UDP and other data transport protocols.

Firewall shunning involves using a firewall or router to block the IP address sending the malicious data. While this has the same problem as TCP resets- the IDS/IPS detects it at the same time it reaches the victim, it has an additional disadvantage. A clever attack would include the spoofing legitimate addresses in order to cover the attackers tracks. This would mean that not only were you NOT preventing the attack when you thought you were, but also that you were denying service to a perfectly legitimate user. These two examples show hardware based IPSs that have not been properly implemented. When this is done correctly though, IPSs generally overcome the problems faced by networks that have implemented IDSs [Wi].

VIII The Future of Security

Tanase addresses the problem of increased traffic through networks which was a factor affecting the performance of the IDS. He points out very sensibly that it is safe to assume that hardware and software capabilities will match the increased throughput that we've been seeing lately, albeit at a higher price. Devices have been designed to circumvent the problem faced by NIDS in switched networks – they "sit invisibly between two networks and monitor all traffic exchanged, regardless of switches or hubs, while remaining immune to attack attempts. The future is off to a bright start."[Ta]

Another problem with traditional IDSs as mentioned before, has been performance. How to ensure that the maximum number of packets have been scanned without affecting the performance of the network? The answer of course is to increase the processing power of your systems. While this would not be the most cost-effective method of ensuring the most possible amount of data is monitored and scanned for

potential signs of danger, it definitely does the job. Wickham mentions specialised network processors that not only perform the required checks quick enough not to hamper network performance, but they also do the job regardless of the protocols used in communication and the type of network they reside in, which could be a real-life example of my suggested answer to the performance problem [Wi]

Another probable direction of intrusion detection and security would be merging traditional IDS with prevention mechanisms to not provide an in-depth analysis of what went wrong, but instead protect your systems by preventing the attack from occurring in the first place and then providing a detailed analysis of what was prevented from happening. A considerable faction of the security community adheres to this way of thinking. Thomas Goeldenitz, in his 2002 paper [Go], says that a hybrid approach, using various kinds of IDSs together, is the way of the future[12]. It is also interesting to note that while he doesn't use the term IPS per se, Goeldenitz believes that "the term IDS will be used in the context of a combined arsenal of security tools that are integrated into a single management console." Besides including NIDS, Host Intrusion Detection Systems (HIDS) and the hybrid IDSs mentioned above, he also expects the aforementioned "arsenal" to include firewalls, routers and other hardware components – all of which are used to form IPSs [Go]. Tanase is another author who doesn't specifically mention IPSs while alluding to them. He says sees a management console that interacts with firewalls, routers and other IDSs, and expresses his belief in the need for a specific "IDS protocol or reporting format" to enable all the different components to properly communicate with each other. Tanase also trusts that future IDSs will be created by combining the different systems and tools used today [Ta], which I think alludes to IPSs. This is because most legacy systems and tools have been detection based while modern solutions like firewalls, routers and modern IPSs, are prevention-oriented. Merging these applications into a single console would result in a system that could not strictly be called an IDS but would have to be either an IPS or a combined detection and prevention system, which is why I think Tanase alludes to IPSs when he suggests an omnipotent IDS console of the future.

[12] [Go] T. Goeldenitz, "IDS – Today and Tomorrow", *SANS InfoSec Reading Room*, 2002. URL: http://www.sans.org/rr/papers/index.php?id=351

IX Conclusion

While quite a few people seem to believe that IDSs now have to be relegated to the past, I tend to agree with Holland, that the future of intrusion detection lies in combining traditional IDSs with modern IPS technology. Sequeira mentions that while a firewall can block traffic from certain port numbers, it is powerless with regards to the inspection of legitimate port numbers for possible attacks. IDSs on the other hand can identify any traffic that is suspect but aren't capable of preventing them from penetrating the network and wreaking their own special blend of havoc on the system resources [Se].

McHugh says that intrusion detection projects sponsored by the Defense Advanced Research Projects Agency (DARPA) were aimed at detecting 99% of the attacks that occurred with a less than 1% margin of error [McH]. This goal is far from being reached by current IDSs, and I think that the most logical answer to the discrepancy in what we'd like to have for our systems and what we have at present would be to combine IDS and IPSs. Merging the in-depth analysing and identifying capabilities of an IDS with the blocking and protection potential of IPSs will, in my opinion, go a long way towards achieving DARPA's admirable, but as of now, very unreachable goal.

References

- [La] B. Lampson, "Computer Security in the Real World", *IEEE Computer Society*, 37-46, 2004.
- [McH] J. McHugh, "Intrusion and Intrusion Detection", *International Journal of Information Security I*, 14-35, 2001.
- [De] D. Denning, "An Intrusion-Detection Model", *IEEE Transactions on Software Engineering*, Vol.SE-13, No.2, February 1987, 222-232.
- [Ba] R. Bace and P. Mell, "Intrusion Detection Systems", *NIST Special Publication on Intrusion Detection System*, 1- 51, 2002.
- [Se] D. Sequeira, "Intrusion Prevention Systems – Security's Silver Bullet?", *SANS Institute 2002*, GSEC Practical v1.4b, Option 1, 2002.

- [Ke] R. Kemmerer and G. Vigna, "Intrusion Detection: A Brief History and Overview", *IEEE Security and Privacy*, 27-30, 2002.

- [Wi] T. Wickham, "Intrusion Detection is Dead. Long Live Intrusion Prevention!", *SANS Institute2003*, GSEC Practical v1.4b, Option 1, 2003.

- [Ta] M. Tanase, "The Future of IDS", *SecurityFocus*, 2001. URL: http://www.securityfocus.com/infocus/1518

- [Ho] T. Holland "Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth ", *SANS Institute2004*, GSEC Practical v1.4b, Option 1, 2004

- [Br] A. Brindley "Denial of Service attacks and the emergence of 'Intrusion Prevention Systems'", *SANS Institute 2003*, GSEC Practical v1.4b, Option 1, 2002

- [Bo] M. Bobbit, "Inhospitable Hosts", *Information Security*, Volume 5, No. 10 (2002): 35-47, 2002.

- [Go] T. Goeldenitz, "IDS – Today and Tomorrow", *SANS InfoSec Reading Room*, 2002. URL: http://www.sans.org/rr/papers/index.php?id=351