Global Information Assurance Certification Paper

Information security attacks cause $55 billion damage in 2003

What are we doing wrong?

Sulata Bhattacharjee
October 3, 2004

GIAC Security Essentials Certification (GSEC)
Practical Assignment version 1.4b option 1

ABSTRACT

Information security attacks caused $55 billion damage in 2003 and the damage bill continues to climb. Society is in a heightened state of vulnerability to information security attacks.

This paper will discuss key problem areas in information security that need to be addressed in order to reduce society's current vulnerability to information security attacks. It will then discuss the effect emerging threats and evolving business practices will have on information security going forward. And finally, this paper will suggest actions that can be used to reduce society's vulnerability to information security attacks in the future.

From this paper, it will be evident that the IT industry needs to analyse its shortcomings, reassess its strategy and develop effective countermeasures to reduce society's vulnerability to information security attacks in the future.

SCOPE

The purpose of this paper is to highlight some of the key problem areas that need to be addressed in order to reduce society's current vulnerability to information security attacks. A discussion on this topic could be very broad ranging from discussion about information security governance to discussion about the deficiencies of particular technological defenses.

This paper will focus on information security from the perspective of the IT industry. As such, it will not discuss security management issues as these fall under the responsibility of individual organizations. It will not delve into technical discussions about particular technological defenses such as firewalls or anti-virus products. It will present a non-technical discussion about problem areas that need to be addressed by the IT industry in order to reduce society's vulnerability to information security attacks. In doing so, this paper hopes to act as a starting point for ideas that the IT industry can implement to reduce this vulnerability.

ASSUMPTIONS

It should be noted that this paper assumes that the reader has a high-level understanding of well-known information security concepts such as 'defense in depth', perimeter security, anti-virus, etc. As such, the content of this paper will focus on highlighting problems within information security rather than explaining current information security practices.

INTRODUCTION

Sasser worm rips through the Internet. Phishing attacks on the rise. 'Slammer' worm cripples Internet. A few years ago, a worm was a soft-bodied animal found in household gardens. Today, they are small snippets of code, replicating their way through corporate networks, leaving billions of dollars worth of damage in their wake.

In recent years, information security incidents have dominated the headlines. Whilst the regular attention has heightened society's awareness of information security risks, it has also highlighted the interdependence of our computer networks and their vulnerability to such attacks. Corporate organizations have significantly increased their spending on information security solutions in a bid to stem the continual onslaught of attacks, yet these attacks continue to have a increasingly devastating effect, costing approximately $13 billion in 2001, $20-30 billion in 2002 and $55 billion in 2003.[1]

Whilst these figures are indeed extraordinary, the mounting cost of information security attacks is not our only cause for concern. In the past year, we have seen information security attacks impinge on our everyday lives. Recent virus activity caused at least 40 Delta planes to be grounded[2], the UK coastguard to be 'offline' for most of the day [2] and 13000 Bank of America ATM machines to fail.[3] In addition, many security professionals believe the Northeast America and Canada electrical blackout that occurred on August 14, 2003 was caused by the Blaster worm.[3] Such incidents have brought home a frightening truth, that the Internet has transformed software bugs from an annoyance into a global danger.[4] Not only are information security attacks having an increasingly devastating financial impact, they are moving dangerously close to having a deadly one. The rising financial cost of information security incidents suggests that we are not getting any closer to effectively mitigating the risks that threaten our IT environments. However, given that information security now extends beyond maintaining an organization's competitive advantage to protecting our national critical infrastructures and protecting the lives of our people, it is imperative that we reevaluate current defenses and develop adequate countermeasures to reduce society's current vulnerability to information security attacks.

So what are we doing wrong? Why do information security attacks continue to be such a problem despite implementation of current best practice solutions? The IT industry has recently come under fire for its handling of information security issues and its inability to adequately protect business against the continual onslaught of cyber attacks. We all know there is no such thing as a perfect state of security. As with the real world, it is impossible to pre-empt and avoid all threats. Recent global terrorist acts such as September 11 and the Bali bombings are a chilling reminder of this all too real fact. However, if we look at the real world we see numerous examples of how implementation

[1] Virus Related Statistics: http://www.securitystats.com/virusstats.html
[2] Lessons to be learnt from Sasser: http://www.zdnet.com.au/insight/security/print.htm?TYPE=story&AT=39147792-39023764t-10000105c
[3] Digital pearl harbor: it's already happened: http://reviews-zdnet.com.com/AnchorDesk/4520-7297_16-5114419.html
[4] NYC: Cybersecurity goes beyond IT industry: http://www.atnewyork.com/news/article.php/3287951

of appropriate countermeasures can effectively reduce the likelihood and impact of attacks. The same, then, can be said for information security. So have we developed effective solutions that adequately combat current and emerging threats?

This paper hopes to answer the above questions by highlighting key problem areas in information security that need to be addressed in order to reduce society's current vulnerability to information security attacks. In addition, this paper will discuss the effect emerging threats and evolving business practices will have on information security going forward. And finally, this paper will suggest actions that can be used to reduce society's vulnerability to information security attacks in the future.

THE FALLING SHORT OF THE MARK: Key challenges within information security today

As previously mentioned, the significant financial impact of information security attacks indicate there are fundamental changes that need to be made to current information security defenses in order to reduce society's vulnerability to information security attacks. So how are we falling short of the mark?

This section of this paper will explore some of the key issues plaguing information security today, including the:

- ⇒ prevalence of vulnerable software;
- ⇒ absence of true information security;
- ⇒ lack of education of key elements required to manage information security; and
- ⇒ lack of enforced security.

The prevalence of vulnerable software

What is one word that is sure to send chills down a network administrator's spine? VULNERABILITY. It is no secret that vulnerable software has been a key contributing factor to society's current vulnerability to information security attacks. Yet it is an issue that remains un-addressed. To date, software development houses have solely focused on one thing – functionality. And why wouldn't they? Until recently, there has been little, or no, market demand for security features in commercial software. IT vendors, like all other organizations, are commercial businesses that need to survive in a fiercely competitive market. Given the lack of demand and the fast moving nature of the commercial software market, the cost of developing secure software, and the significant impact it would have on their time to market, simply could not be justified.

However, whilst understandable, the fact remains that the production, and prevalence, of vulnerable software is a key contributing factor to society's current vulnerability to information security attacks. One only needs to scratch the surface of current attack techniques to discover that vulnerable software is the vehicle for the majority of these attacks. Worms that propagate through the Internet at lightning speed by exploiting unpatched systems, attackers that compromise thousands of unpatched home PCs and use them to launch distributed denial of service attacks, vulnerabilities that are exploited to escalate privileges and compromise the security of a system, the list goes on and on and on.

The existence of vulnerable code would not pose such a problem if the exploitation of this code were not such a popular sport. It is this popularity that makes it necessary for network administrators to be vigilant in applying patches to all devices on their network. This exercise, commonly referred to as patch management, whilst manageable in small scale IT environments becomes a nightmare in large scale IT environments. Not only do network administrators have the challenge of rolling out patches to the thousands of machines within their network, they also face an ever-increasing number of vulnerabilities that have to be applied within a shrinking exploitation window. In addition, they are forced to wrestle with patches that break services, leaving the organization with the option of suffering financial loss through lost productivity resulting from system downtime or suffering financial loss through a security breach of the unpatched system.

As Graham Ingram, General Manager of AusCERT, points out we have reached a point in time where "organizations simply cannot keep up with the rate at which vulnerabilities are now being discovered and disclosed and respond accordingly."[5] In 2003, 7 new vulnerabilities were reported daily.[6] The CERT Coordination Center is projecting 15 new vulnerabilities will be reported daily by 2005.[4]

This excessive number of vulnerabilities and the nature of patches have contributed to the astronomical cost of patch management. A recent Yankee Group survey reported that the average cost of patching desktops was "$234 per desktop. For a company with 5,000 desktops, that means over $1 million spent annually just for patching."[7]

Whilst it is acknowledged that there will never be such a thing as vulnerability-free software, given the cost and ineffectiveness of current patch management solutions, it is evident that the IT industry needs to reevaluate current software development practices and reengineer them to reduce the current number of vulnerabilities in commercial software.

[5] Microsoft answers AusCERT security criticism: http://www.zdnet.com.au/news/security/0,2000061744,39148622,00.htm
[6] Page 3 - Symantec Internet Security Threat Report: http://enterprisesecurity.symantec.com/content.cfm?articleid=1539&EID=0
[7] Top Three Security Problems Remain Despite Increased Spending: http://seclists.org/lists/isn/2004/Feb/0063.html

The absence of true information security

Earlier this year, KPMG and nCipher released a paper titled 'Security in an Island World'[8]. Whilst the paper focused on how cryptography can enable business agility, it highlighted a very important issue – "that current approaches [to information security] focus on securing the enterprise network perimeter". [9] Any security professional that has performed internal and external vulnerability assessments will be able to support this statement and will be all too familiar with the weak control environments found in most large organizations.

The problem with this approach is that threats lie on either side of an organization's network perimeter. Gartner estimates that more than 70% of unauthorized access to information systems is committed by employees, as are more than 95% of intrusions that result in significant financial losses.[9]

By concentrating on the perimeter, organizations fail to mitigate the risk of internal threats that can result in significant financial loss. In addition, the outwardly growing boundaries of the enterprise and the increasing need to exchange of information between organizations and their partners, employees and customers, make this approach impractical for the future.

Lack of education of key elements required to manage information security

A recent article on securityfocus.com[10] discussed the need for knowledge and understanding to manage security. One of the fundamental problems that is contributing to society's current vulnerability to information security attacks is the apparent lack of education amongst the elements required to effectively manage information security. These elements include:

Developers: As Jason Miller of securityfocus.com points out, "an attacker wins when he understands the behavior of the application better than the developer of the software." [11] As previously mentioned, vulnerable code is a key contributing factor to society's current vulnerability to information security attacks. The production of more secure code, both commercial software and in-house developed applications, is dependent on developers gaining a better understanding of the underlying development language.

Administrators: Vulnerabilities are not only introduced by developers. In his article, Jason Miller also points out that "vulnerabilities [that] are configuration-based…are introduced (or in some cases left in) by an administrator that is not fully aware of the consequences of his configuration choices."[11] Misconfigured systems continue to be a major problem for organizations. According to John Pescatore, Vice President of Gartner Inc, 65% of attacks exploit misconfigured systems.[11] Better education of administrators about their

[8] Security in an Island World: http://www.kpmg.co.uk/pubs/beforepdf.cfm?PubID=811#
[9] Enterprises and Employees: The Growth of Distrust: http://security1.gartner.com/story.php.id.12.s.1.jsp
[10] The Panacea of Information Security: http://www.securityfocus.com/columnists/260
[11] Pescatore comments on state of enterprise security: http://searchsecurity.techtarget.com/qna/0,289202,sid14_gci905234,00.html?newsel=10.1

configuration choices is imperative if we are to reduce society's vulnerability to information security attacks.

Management: Introduction of legislation such as the Sarbanes-Oxley Act which requires executives to sign-off on their organization's internal controls has required executives to have a greater understanding of information security. Yet, despite the introduction of such legislation, understanding of, and support for, information security from senior management continues to be an issue in a number of organizations. This lack of support often leads to under-resourced security teams that cannot adequately manage the security needs of the organization. Better education of senior management is required for more effective management of information security.

Users: More and more security features are being seamlessly integrated into emerging commercial applications. Take, for example, commercial email clients. Most, if not all, commercial email clients have the capability to send and receive secure email. Yet the majority of individuals do not use these features, or worse, are not even aware of them. Likewise, Microsoft has automated patch management for home users through the automatic update feature in Windows Update, yet a vast number of home computers still remain unpatched. The fact that these features exist and are not being used highlights the need for greater education.

However, the problem is further compounded by the perception that IT security is hard. It is a perception that is held by the majority of the general public and, for the majority of users, this perception is reality. Real-time anti-virus scanning, spyware utilities, software firewalls, hardware firewalls, patching… the list of software required to adequately secure the humble home computer is seemingly endless and can be quite daunting for the average end user. Whilst there may be a case to simplify security controls to ensure one does not require a computing degree to configure a secure computer, education and assistance with current technologies will go a long way to reduce our vulnerability to information security attacks.

The lack of enforced security

Something I have always found intriguing about the field of information security is its detachment from real world security. Security professionals are the law enforcement agents of the cyber world. Like our real world counterparts, we have a responsibility to 'fight crime' and ensure we protect society against information security attacks by implementing appropriate countermeasures to reduce the likelihood and impact of such attacks. As such, you would think we would leverage off the experience of real world law enforcement agents to increase the security posture of the Internet. However, on close analysis, it is evident that traditional crime fighting techniques that exist in the real world have not transferred across into cyberspace.

Take, for example, the notion of enforced security. In the 'real' world, authorities enforce security at centralized points of control in situations where the actions of an individual may have a detrimental effect on the wider community. A classic example of this is the installation of security scanners at airports to prevent passengers from carrying sharp objects in their hand luggage. Authorities perceived a threat, i.e. passengers with sharp objects in their hand luggage, and enforced security measures, i.e. security scanners, to mitigate the risk of that threat. By removing the threat, authorities reduce the likelihood of attacks, thus increasing security for travellers on passenger jets. Why, then, has this thinking not been applied to the cyber world?

One information security risk that warrants such action is the threat of users with insecure home PCs. To date, security professionals have solely relied on user awareness to mitigate the risk of this threat. However, in doing so, we have failed to realise that we are relying on the threat to mitigate its own risk. If we revisit our airport analogy, a campaign to increase passenger awareness about the risks of carrying sharp objects in hand luggage would have done little, if anything, to increase airline security. In the same way, home user awareness of information security risks has done little to mitigate the risk of the insecure home PC.

Lack of action in this area has provided hackers with the opportunity to commandeer armies of vulnerable machines and use them in coordinated, large-scale attacks like the distributed denial of service attack against the SCO UNIX website earlier this year. Not only that, but the growing popularity of Secure Socket Layer (SSL) Virtual Private Networks (VPN) that allow employees to connect to corporate networks to check their corporate email and various other applications via the Internet will make the insecure home PC an increasing threat to corporate security.

Given the success of recent information security attacks, and the potential impact of future information security attacks, it is evident that we cannot continue to allow users the freedom of deciding whether they mitigate the risks their home PCs pose to the security posture of the Internet. We, as security professionals and the law enforcement agents of the cyber world, must enforce security at centralised points of control to mitigate the risk of such threats.

THE CHANGING LANDSCAPE

So far this paper has discussed some of the key problem areas that are challenging information security today. Whilst these issues need to be addressed, time stands still for no man. Our way of doing business, and the technology that facilitates it, continues to evolve, as do the threats that threaten the confidentiality, integrity and availability of our information.

Our role, as information security professionals, is to allow business to take advantage of emerging technologies by developing appropriate solutions that adequately mitigate the risk of emerging threats.

This section of this paper will explore these emerging threats, technologies and evolving business practices and the impact these changes will have on future information security practices and defences. This will include looking at:

- ⇒ the increasing frequency, scale and speed of attacks;
- ⇒ zero-day attacks;
- ⇒ blended attacks;
- ⇒ emerging threats from existing technologies;
- ⇒ emerging technologies; and
- ⇒ the extended enterprise.

Emerging threats

Increasing frequency, scale and speed of attacks

One of the major challenges that information security professionals face in the future is the increasing frequency, scale and speed of attacks.

The increased awareness of information security has not only served to heighten society's awareness of information security issues, it has also sparked greater competition in the hacker community. This has resulted in a significant increase in virus activity, which continues to grow each year. For example, by May 2004, the total number of viruses released in 2004 exceeded the total number of viruses released in 2003.[12] The problem this increase in virus activity causes is that it significantly increases the likelihood of infection. The SANS Institute recently released figures on the average survival time of a machine, that is, the amount of time a machine is connected to the Internet before it is compromised or infected by a virus. The SANS Institute estimated this to be approximately 20 minutes. As the SANS Institute points out, the issue we face is that the time required to download critical patches will exceed this survival time.[13] Whilst we cannot stem the flow of viruses that are being released, there is a need to develop effective methods to prevent infection.

Whilst the increased frequency is a concern, the increased scale of attacks is also major cause for concern. The popularity of distributed denial of service attacks is increasing. These types of attacks involve an attacker compromising armies of insecure machines that can be remote controlled into launching an attack against a single entity. In the past, these attacks caused financial loss through system downtime. Now, such attacks are being used to extort large sums of money out of online gaming sites.[14] How they will be used in the future is yet to be seen. The potential, however, is frightening.

The prevalence of vulnerable home PCs, the increasing computing power and storage capacity of home PCs and the increasing availability of attack tools that make it easy for individuals with limited knowledge to carry out such attacks make the increasing scale of attacks a growing threat. Given the

[12] Cost of Sasser is $500m and counting…: http://software.silicon.com/security/0,39024655,39120627,00.htm
[13] Survival Time History: http://isc.sans.org/survivalhistory.php
[14] Page 26, 2004 Australian Computer Crime and Security Survey: http://www.auscert.org.au/download.html?f=114

success of such attacks is dependent on the attacker's ability to compromise and remotely control numerous machines, it is evident that we need to control the prevalence of vulnerable home PCs to reduce the likelihood and impact of such attacks.

The greatest concern, however, is the increasing speed of attacks. Gone are the days when viruses took several hours to infect their victims. In 2001, the Code Red II worm worked for almost 14 hours to infect 359,000 machines, Nimda took 30 minutes and Slammer spread at lightning speed taking just under 10 minutes to bring the Internet to a grinding holt.[15] Current anti-virus solutions depend on known virus signatures to prevent infection. We are now in a position where the time required to propagate virus definition updates exceeds the time required for the virus to propagate. Again, the challenge of the future highlights the inadequacies of current defenses and requires us to devise other methods to effectively mitigate the risk of such attacks.

Zero-day attacks

Probably the most ominous threat that lurks over the horizon is that of the zero-day attack. The term 'zero-day attack' refers to an attack that exploits a vulnerability that is not yet known to the wider security community. Whilst it is surprising that such attacks have not been popular to date, their increasing popularity will prove to be a significant challenge for current defences. This is because the majority of current security defences rely on known signatures to prevent attacks. Given the time of the zero-day attack is the first time the vulnerability is revealed to the wider security community, attack signatures can only be updated after the attack, thus making it increasingly difficult to prevent such attacks using current methods.

Not only will zero-day attacks have an impact on current signature-based defences, they will also reduce our reliance on patches to prevent attacks. Again, as the time of the attack is the first time the vulnerability is disclosed to the wider security community, patch management will inevitably become reactive. Today, current best practice solutions rely on administrators promptly applying patches to devices within their networks. Tomorrow, we face a situation where patches won't be available before a malicious individual takes the opportunity to launch an attack and vendors will be forced to reverse engineer patches and attack signatures from the actual attack.

The growing popularity of these attacks will require current defences to evolve. The need for patching will become less significant and the IT industry will be required to develop new methods to combat unknown attacks or improve the robustness of code to reduce the likelihood of such attacks.

[15] Infected in 20 minutes: http://www.theregister.co.uk/2004/08/19/infected_in20_minutes/

Blended attacks

Whilst zero-day attacks lurk over the horizon, blended attacks are already here. These kinds of attacks combine one or more attack techniques such as propagation techniques of worms with the ability to exploit vulnerabilities. As such, these attacks have the potential to spread rapidly and cause widespread damage.

As with zero-day attacks, blended attacks are also increasing in popularity. As Mark Sunner, chief technology officer at MessageLabs advised, “Almost without exception, every virus we have seen during 2004 has compromised infected machines and allowed them to be remotely commandeered."[16]

The increasing popularity of this threat will increase the need for greater control of insecure PCs to reduce the likelihood and impact of such attacks.

Emerging threats from existing technologies

This year we saw the emergence of the first mobile phone viruses such as the Mosquit Trojan[17] which hit Nokia phones running the Symbian operating system. Once installed, the Trojan sends a number of SMS messages to premium rate services, leaving the owner to foot the bill. Although the Trojan will only install if the user ignores a number of warning messages, it is an indication of things to come in the future. Whilst manageable now, the challenge for security professionals will come as these types of threats continue to evolve and have an increasing financial impact.

The future brings more vulnerabilities and an increasingly aggressive threat environment that affects more and more devices, not just our data networks. Given our inability to adequately cope with current patching requirements, it is evident that we must re-assess our current defences and develop appropriate solutions that adequately mitigate the risks of these emerging threats.

Emerging technologies

Society is becoming increasingly IP-enabled. Everyday, we are introduced to new technologies be it an Internet-enabled fridge or some new wireless enabled gadget. Whilst the popularity and increased use of these technologies is inevitable, their popularity and increased use also has serious repercussions for information security. Today, we have reached a situation where we are struggling to apply patches in a timely manner. How, then, are we going to fare when we need to patch more than just our data networks?

There are a number of technologies emerging as security risks. Portable devices, wireless technologies, Voice over IP (VoIP) and instant messaging are just a few of the technologies that have recently generated much interest. Each of these technologies brings its own unique risks e.g. wireless

[16] UK companies in 'blissful ignorance' over spyware threat: http://www.zdnet.com.au/news/security/0,2000061744,39153573,00.htm
[17] Cell Phone Trojan Hits Nokia Devices Running Symbian: http://www.securitypipeline.com/29100090

technologies have the potential to seamlessly extend corporate networks, significantly increasing the vulnerability of these networks if the devices are not properly configured. Yet they all present one common risk - an ever-increasing number of devices that require protection.

The same security challenges that plague our data networks today threaten to plague these emerging technologies tomorrow. Again, considering we are still struggling to mitigate the risk of current information security attacks, it is imperative that we revisit our current defence strategies to ensure we have appropriate technologies and processes in place to adequately manage the security of existing and emerging technologies.

Extended enterprise

Technology has revolutionized the way we do business. 10 years ago, email was virtually non-existent. Today, it is considered a business critical application. As technology continues to evolve, so do our business practices. As KPMG and nCipher point out, enterprises are becoming 'increasingly virtual.'[9] As the boundaries of the enterprise move outward, organizations will be required to have increasingly flexible perimeters that allow information exchange with numerous parties including business partners, third party suppliers, customers and employees. This will make it increasingly difficult to differentiate between "insiders" and "outsiders".

As previously mentioned, current defenses focus on protecting enterprise IT environments from unauthorized access by external parties. This is achieved by securing the organization's network perimeter. The problem with this approach is that it does not enable the extended enterprise. The future will require organizations to reduce their reliance on traditional 'perimeter' security defenses and implement mechanisms that protect individual data objects. As Daniel Greer, Vice President of Verdasys, points out "security cannot be a barrier to growth, or people will inevitably work around it."[18] As such, current defenses must evolve to facilitate these open and accessible enterprise IT environments.

THE WAY OF THE FUTURE

As previously stated, the purpose of this paper is to highlight key problem areas within information security that are contributing to society's current vulnerability to information security attacks. In doing so, it hopes to stimulate new approaches to information security that can reduce this vulnerability in the future. Whilst this paper does not endeavour to provide the answers to today's information security challenges, the following hopes to provide a starting point for new approaches.

[18] The Shrinking Perimeter: Making the Case for Data-Level Risk Management: http://www.verdasys.com/pdfs/ShrinkPerim.pdf?x=ism

Secure software and protocols

The old saying holds true. 'Prevention is better than cure'. Given the inability of organizations to cope with current patching requirements, it is evident that there is a strong need for less vulnerable commercial software. Market demand for secure commercial software is already increasing as executives realise that buying more secure software will reduce their maintenance costs. As Marty Lindner, team leader for incident handling at the CERT Coordination Centre, points out, "the root cause of problematic patches and problematic software is bad software engineering practices. That's where we have to fix things". Lindner suggests a two-fold approach, firstly the widespread adoption of better software engineering practices and, more importantly, the widespread adoption of developing foolproof architecting protocols.[19]

Many continue to argue that the cost of developing secure code is not justifiable. Several security professionals believe it is unnecessary as the UNIX operating system is a suitable, more secure alternative. Whilst some security professionals continue to flirt with the idea of a UNIX-enabled society, the fact still remains that computers exist to make life easier. This requires them to be as user friendly as possible. Even though some manufacturers such as HP seem to be responding to this idea and have introduced laptops with Linux as the default install, the notion that the general populus will jump on the Unix bandwagon is unrealistic. The only option then is to treat the root cause of the problem by building more secure code and developing more secure protocols.

Increased education

Education of the key elements that manage information security is essential if we are to reduce our current vulnerability to information security attacks. This includes education of:

- ⇒ Developers in how to develop secure code;
- ⇒ Administrators in how to configure secure servers/devices and maintain secure networks;
- ⇒ Management in how to develop appropriate security management strategies and make informed decisions about information security products/solutions; and
- ⇒ Users on how to use common security features.

Enforced security

Recent information security attacks have increased the level of awareness about information security risks, yet the cost of information security attacks continues to climb. Given information security attacks are moving dangerously close to having a deadly impact, awareness is no longer enough. Information security needs to be considered as a law enforcement issue and be enforced through centralised points of control.

[19] When Patches Aren't Applied: http://www.cioupdate.com/reports/article.php/2172051

One point of control that may be considered to reduce the prevalence of insecure home PCs is Internet Service Providers (ISPs). Users obtain access to the Internet via Internet Service Providers (ISPs). As such, it makes sense to use these points of aggregation to control the threat of insecure home PCs. Denying access to users that do not have adequate protection such as the latest patches or updated anti-virus definitions could be one such way of controlling insecure home PCs. This may be considered controversial. However, airline passengers not willing to comply with security restrictions are refused entry to increase the safety of all other passengers. In the same way, we need to enforce information security controls to increase the security posture of the Internet.

Data object level security

Given the changing needs of business and the increasing openness of enterprise IT environments, there is a need to shift our focus from protection of networks to 'protection of information assets, in transit and at rest' [9] to enable organizations to build closer relationships and exchange information with their business partners, customers and employees. KPMG and nCipher suggest using cryptographic methods such as SSL (Secure Socket Layer) and digital certificates to achieve this. Whatever the method, the key is shifting the focus from network security to true information, or data object level, security and developing effective security management systems that facilitate management of this distributed security model.

Behaviour-oriented defences

As previously mentioned, the signature-based nature of current defences will soon become ineffective in protecting our information. In the future, we face attacks that exploit unknown vulnerabilities and propagate faster than we can update our signature files. As such, it is important that we analyse the behaviours of current attack techniques and develop countermeasures to thwart attacks of a particular nature rather than a particular instance of an attack. For example, anti-virus vendors should analyse the behaviour of worms and develop defences that prevent all worms from propagating, as opposed to developing countermeasures that prevent infection from a single worm.

Such defences are already beginning to surface, e.g. virus throttling software that prevent worms from propagating by preventing the infected machine from connecting to other machines and Intrusion Prevention Systems (IPS). However, the perimeter nature of inline IPSs makes it just as easy to launch a Denial of Service condition against such a device. As such, future technologies should consider the shift to data object level security to ensure these devices are not easily defeated. These technologies are still evolving but they hold much promise for the future.

CONCLUSION

The purpose of this paper was to highlight some of the key problem areas that need to be addressed in order to reduce society's current vulnerability to information security attacks. If we revisit the two questions posed at the beginning of this paper, we see that information security attacks continue to be such a problem because of the:

- ⇒ prevalence of vulnerable software;
- ⇒ absence of true information security;
- ⇒ lack of education of key elements required to manage information security; and
- ⇒ lack of enforced security.

In addition:

- ⇒ the increasing frequency, scale and speed of attacks;
- ⇒ zero-day attacks;
- ⇒ blended attacks;
- ⇒ emerging threats from existing technologies;
- ⇒ emerging technologies; and
- ⇒ the extended enterprise;

will prove to be a significant challenge for current signature-based defences and network administrators who already cannot cope with current patching requirements.

We can remedy these problems by introducing:

- ⇒ more secure software and protocols;
- ⇒ increased education;
- ⇒ data object level security;
- ⇒ enforced security; and
- ⇒ behaviour-oriented defences.

We have arrived at a point in time where information security is not a luxury that is afforded to safeguard the competitive advantage of an organization. Information security has become a necessity that is required to protect our national critical infrastructure and the lives of our people.

Society is in a heightened state of vulnerability to information security attacks. As such, it is imperative that we analyse our shortcomings, reassess our strategy and develop effective countermeasures to reduce our vulnerability in the future.

REFERENCES

[1] Trend Mirco, Virus Related Statistics, 16 January 2004
URL:http://www.securitystats.com/virusstats.html

[2] Kevin Francis, Lessons to be learnt from Sasser, 17 May 2004
URL:http://www.zdnet.com.au/insight/security/print.htm?TYPE=story&AT=39147792-39023764t-10000105c

[3] Robert Vamosi, Digital pearl harbor: it's already happened, 22 December 2003
URL:http://reviews-zdnet.com.com/AnchorDesk/4520-7297_16-5114419.html

[4] Ryan Naraine, NYC: Cybersecurity goes beyond IT industry, 11 December 2003
URL:http://www.atnewyork.com/news/article.php/3287951

[5] Mathew Schwartz, Top Three Security Problems Remain Despite Increased Spending, 18 February 2004
URL:http://seclists.org/lists/isn/2004/Feb/0063.html

[6] Symantec, Page 3 - Symantec Internet Security Threat Report, March 2004
URL:http://enterprisesecurity.symantec.com/content.cfm?articleid=1539&EID=0

[7] Andrew Colley, Microsoft answers AusCERT security criticism, 25 May 2004
URL:http://www.zdnet.com.au/news/security/0,2000061744,39148622,00.htm

[8] KPMG (UK) and nCipher, Security in an Island World, April 2004
URL:http://www.kpmg.co.uk/pubs/beforepdf.cfm?PubID=811#

[9] Gartner, Enterprises and Employees: The Growth of Distrust, Date unknown
URL:http://security1.gartner.com/story.php.id.12.s.1.jsp

[10] Jason Miller, The Panacea of Information Security, August 12, 2004
URL:http://www.securityfocus.com/columnists/260

[11] Michael S. Mimoso, Pescatore comments on state of enterprise security, 9 June 2003
URL:http://searchsecurity.techtarget.com/qna/0,289202,sid14_gci905234,00.html?newsel=10.1

[12] Ron Coates, Cost of Sasser is $500m and counting…, 12 May 2004
URL:http://software.silicon.com/security/0,39024655,39120627,00.htm

[13] SANS Institute, Survival Time History, Date unknown
URL: http://isc.sans.org/survivalhistory.php

[14] AusCERT, Page 26, 2004 Australian Computer Crime and Security Survey, 24 May 2004
URL:http://www.auscert.org.au/download.html?f=114

[15] Scott Granneman, Infected in 20 minutes, 19 August 2004
URL:http://www.theregister.co.uk/2004/08/19/infected_in20_minutes/

[16] Munir Kotadia, UK companies in 'blissful ignorance' over spyware threat, 16 July 2004
URL:http://www.zdnet.com.au/news/security/0,2000061744,39153573,00.htm

[17] TechWeb News, Cell Phone Trojan Hits Nokia Devices Running Symbian, 13 August 2004
URL: http://www.securitypipeline.com/29100090
[18] Daniel Greer, The Shrinking Perimeter: Making the Case for Data-Level Risk Management, January 2004
URL:http://www.verdasys.com/pdfs/ShrinkPerim.pdf?x=ism
[19] Ryan Naraine, When Patches Aren't Applied, 31 March 2003
URL:http://www.cioupdate.com/reports/article.php/2172051

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor