View metadata, citation and similar papers at core.ac.uk brought to you by CORE
provided by Clute Institute: Journals

Managing Security Issues

Aristotelis Glentis, National & Kapodistrian University of Athens, Greece
Anastasios Panopoulos, Athens University of Economics and Business, Greece
Ilias Kapareliotis, Athens University of Economics and Business, Greece

ABSTRACT

Security is coming more and more in the spotlight of today's news. Several reasons have lead to this, like the maturity of computer technology, which gave access to more people to computer systems, and the evolution of the internet and computer networking in general. Security, as most technology issues, doesn't evolve in general directions, but follows the direction of technology innovation. This focused direction of security research creates a number of different trends that evolve during time. This study will focus on the trends that have been emerging lately and the implications they have in security management. Suggestions will be proposed in order to accommodate the forthcoming changes.

Keywords: Security trends, Security policies, Network technologies

INTRODUCTION

Computer technology is becoming more mature and more widespread. More and more people are participating in the advantages that technology offers. The internet has a key role in this change since it provided the medium for people to communicate and interconnect (Ashenden 2009). This fact caused cultural and social changes as people had the chance to participate in a global communication sphere. New technologies and applications have been invented in order to facilitate communication using the internet like p2p networks, social networks and so on (Fogel & Nehmad 2009). This boom of the internet era, however, has also attracted people with malicious intentions. Before the internet, a security problem would affect only a small number of computers, while the spreading rate was quite slow (Botha et al. 2009). Nowadays any security problem affects a large number of computers that are connected and the spread rate is very fast (Weir et al. 2009). As a result, more and more attention is paid to security since a lot of private and sensitive data are available in the internet (Zhao et al. 2008). Security technologies and measures have been taken in different directions in order to protect users from malicious activities and the network itself (Assaf 2008). Security strategy changes through time as new attack and defense techniques are created and new technologies are adopted (Computer Security Institute 2008). These changes are a result of trends that rise. By studying these trends one can make assumptions about the implications on security management and suggest changes that can help to accommodate the security scenery change.

SECURITY TRENDS

1.1 Spam volumes increment with more sophisticated methods

Many information security experts anticipated that spam will reduce because of the advances in the antispam technology and the heavy use of antispam software by users (Cakanyildirim et al. 2009). Although many companies have adopted the SPF protocol in order to stop the spammers (http://www.openspf .org/Statistics) the spam phenomenon continues to grow rapidly. The reason for that is that the advantages in the information security sector in software and protocols feed the spammers leading them to further developments creating a vicious circle (Hancock 1998). As a result spammers instead of basing their efforts on open relays, they have found other ways in order to circumvent the extra measures, like bot networks or identity theft. Furthermore there has been an increase in phishing attempts while the attacks were more sophisticated (Bose & Leung 2008). Translation engines have been used, to automate the translation of websites or phishing e-mails to specialized user groups, bringing spear phishing in a new era (http://www.microsoft.com/protect/yourself/phishing/spear.mspx). The problem is so big that a special anti-phishing group backed up by big companies was created in order to deal with this type of attack (http://www .antiphishing.org).

1.2 BotNets

Bots are software applications that run automated tasks over the internet. BotNets are a collection of bots running autonomously and automatically. Initially the term was not used for malicious purposes but this has changed over time. Bots can be installed to a number of computers with the use of different techniques like hacking, worms, trojan horses, backdoors etc. Modern bots scan their environment and when they find a vulnerable target they try to propagate themselves. Botnets are used usually either as spam gateways or as blackmail for DDOS attacks to big companies (Computer Security Institute 2008). Previous generations of botnets used the IRC servers in order for the bots to communicate with each other and the attacker to command and control (C&C) them. As a result their architecture was centralized based on the existing services. That was the reason why it was easier to detect and prevent their function since there was a lot of strain on the IRC servers prompting the information security expert to investigate for spurious activities. As the botnets evolved they started to use private IRC servers but this was also traceable since their activities could be monitored through the IRC use on the network level. The modern generation of botnets has moved to a de-centralized operation mode. The command and control channel (C&C) is now based on a point to point network between the nodes of the botnet. This architecture with the use of encrypted protocols and ports randomization makes the detection and prevention of botnets extremely difficult. Consequently although some of the old botnets are terminated new ones spring up using better stealth technology (http://www.secureworks.com/research/threats/topbotnets/?threat=topbotnets).

1.3 Security response: Focusing the network perimeter. What about Wifi technology?

Security experts' focus has been moved during the past years from the core to the network perimeter. In the past extreme importance was given to the core network services and the servers adopting a restrict policy on the services that were exposed to the perimeter of the network (Otrok et al. 2008). Desktop computers used by the simple users were considered as terminals with a special access to network services and as a result they were not considered part of the core security policy (Tutschku et al. 2008). Usually there is a strict security policy implemented by the security team that deals with security issues for the core services and a different security policy concerning authentication level and rules for the users' workstations. However this separation in the security attention between the core and the user network has started to change. Workstations are considered an important asset to secure against the numerous attacks in the internet, especially the ones from botnets and spam relays. Given the nature of workstations and more specifically their use for personal purposes (surfing, chatting, gaming etc.) except form performing working duties they are more exposed than well confined servers. Consequently the network perimeter is full of potential targets.

Another issue that complicates the security challenges that companies face today is the use of WiFi technology in today's enterprise business environment. The use of WiFi - even for home computers - has risen during the last years and it is expected to grow even more with the adoption of new protocols with higher speeds (802.11n). Unfortunately security that was provided in the physical layer by wired networks, since the data and the access were confined within the reach of the wires, is gone in wireless networks. The attackers can be in any place within signal reach. Data are transmitted in the air and this opens many possibilities of sniffing or impersonating another wireless device. Wireless devices are not secure since the device driver that they are running is a piece of software and could contain a bug. To make things worse usually device managers run in kernel mode or have escalated privileges and the exploitation of any software bug can give the attacker full control. Attacks on wireless device drivers are dated from 2006 but because of the number of manufacturers new bugs are discovered making the creation of a record difficult. Before the adoption of wireless access the network perimeter was not secure but the path that led to the workstations was well defined by the cables carrying the signals. That is why wireless networks are considered to be unsecured networks and users are request to use a VPN in order to access the internal services. However security doesn't come without a price which in this case is the ease of use. Many users prefer ease of use over security but this will change since workstations and wireless networks have become an important target for attackers.

1.4 Security focus study to the core protocols instead of simple programming bugs

Statistically most of the attacks that have been carried out are based on programmers' errors and the most usual methods of attack are buffer overflows, heap overflows or format string vulnerabilities. However, since this type of vulnerabilities have been studied over the years, tools in order to avoid their appearance have been developed, like new languages (Java or C#) that don't have this type of errors or operating system enhancement (smash stack protection, non executable stack, randomised library loading etc.). Security program bugs exist and will exist, even if security developments make it harder for these types of attack to take place, unless a drastic change in the way we develop software security happens.

A new attack target has been identified lately: internet protocols (Wang et al. 2009). The core of the internet services is a number of different protocols. These protocols are the arterial roads that interconnect computers in a network. Most of these protocols are quite old compared to the internet age. As a result those protocols were designed in times that the needs were different and users had to face serious challenges such as connectivity and robustness but security was not one of them. Security came as an extra problem when it was discovered that the cyberspace ha begun to be not a friendly neighbourhood. Consequently a lot of these protocols have security problems and attackers have been looking into these problems to identify and exploit them. Two security vulnerabilities have already been identified in two different protocols, one in the DNS (http://www.doxpara.com/DMKBO2K8.ppt) and one in BGP (https://www.defcon.org/images/defcon-16/dc16-presentations). DNS is the protocol that maps internet names with a unique IP number. The recent vulnerability discovered enables an attacker to poison a DNS server so that a domain name is sent to his IP address instead of the legitimate one. BGP is the protocol that makes routing possible in the internet. The recent vulnerability discovered enables an attacker to redirect all the network traffic from one host to another network that he controls and then relay the traffic back to the original destination most of the times without notice. Both of these attacks are not vulnerability of a specific application but of the protocol itself since it fails to fulfil certain security and cryptographic standards. The number of protocols that share the same problems with the two before mentioned protocols is not known and active research in finding and correcting these vulnerabilities is needed. Even the use of cryptographic methods is questioned these days, although new hash functions and stronger cryptography algorithms are developed trying to overcome the problems that were spotted in the previous ones, because of the loss of ease of use and connectivity. One of these examples is the MD6 function that will replace the MD5 providing new standards.

1.5 Web applications. Ease of use, but also a security threat.

Usually in the past most of the users performed their operations to their personal computer while the internet was just another resource for some applications that were specially designed to take advantage of it. The increase of speed and bandwidth elevated the role of internet in everyday use. Also the creation of the HTTP protocol for the support of the World Wide Web acted as an aggregator for the other protocols in order to present them in a more unified and eye-appealing manner (Herzberg 2009). Today a number of users run their applications through the internet with their web browser or even they have their whole operation system running through the web browser (Van de Wijngaert & Bouwman 2009). Office applications running through the web (Google apps), instant messages (meebo), GIS systems (Google maps) etc. are few examples of the way that WWW becomes an application aggregator tool. These types of applications are programmed in a very different way than the software we use in our personal computer. Traditional application programming for software offline applications aimed to provide enough privileges to users in order to meet every need. On the other hand since the web is considered a highly unsecured environment these applications when running in the WWW should operate with as few privileges as possible. As a result new web applications have to balance both of these extremes. Enough privileges must be given to the user but at the same time a very careful design is needed in order to prevent attackers from gaining access to the user's computer. These new applications have opened the box of bringing internet attack methods to the desktop and desktop attack methods to the internet (Wei et al. 2008). The attackers know these vulnerabilities and they will try to get advantage of them while programmers will try to find ways to create libraries that will make these attacks hard to succeed. Security focus on this research region should be intense since more and more users are switching from traditional web tasks to web applications (for example universities buy Google apps services instead of Microsoft Office support). Finally the same problem occurs with the web-browsers since they were not developed according to strict security standards. When the first web browsers emerged the WWW provided only text environment and few could have seen the elevation to a dynamic full graphic and interactive environment. Therefore web browsers face security issues that now come in the attention of most people with the latest one called clickjacking (http://ha.ckers.org/blog/20081007/clickjacking-details/) which is a vulnerability that affects almost every web browser in the market (except of the primitive ones) permitting an attacker to control the clicks that a user makes over the internet.

1.6 Virtualisation as a security appliance

One of the biggest trends in computer science is virtualization. Initially virtualization was used as a server consolidation for power saving reasons and efficient CPU distribution. However security benefits had been realised and as a result a new direction to virtualization technologies with security perspective was given. Virtualization helps to keep the servers isolated from each other, so a security compromise on a virtual machine doesn't lead necessarily to the compromise of other virtual machines. This is very important particularly in co-location environments where different companies share the same hardware. In this case security policies are applied since the hypervisor or the host operating system is used to restrict or permit certain actions of the virtual machine. Three different technologies are in use (http://en.wikipedia.org/wiki/Platform virtualization) a) full virtualization where the host operating system creates a complete virtual machine for the guest operating system to run (like VMWare) b) paravirtualization where the guest operating system is modified in order to run by the host operating system (like Xen) c) kernel level virtualization system where the kernel is virtualized and all the virtual machines run the same kernel in different modes (like LVM, FreeBSD jails). Each approach has its strengths and weaknesses but they all provide a sandbox to security threats. On the other hand virtualization is used by attackers in order to hide malware which would then be undetectable by operating systems and malware removal tools (http://en.wikipedia.org/wiki /Blue pill).

1.7 Social networks and a new path to information leakage

Social networks have been the major new hype of the internet. Everyday more and more users are involved in the growing number of social networks. The first social network was Myspace, but soon others came up with Facebook being the most popular. Although we are very sensitive in giving away our personal information it is amazing how easily we give our personal data in the social networks websites. These data are the targets of many attackers since they can be used for spamming or scums. Also the threat of identity theft, when an attacker steals the identity of users and appear as them having access to other people's data, is possible to happen. Furthermore one of the aspects of modern social networks is that they export an API and they allow users to write and share applications. These applications cannot be easily verified and they can contain code for malicious purposes as it was demonstrated in a recent attack to Facebook (http://www.itworld.com/security/54718/researchers - build - malicious – facebook - application).

1.8 P2P networks used to circumvent security measures

Finally another application that gains popularity are P2P (point-to-point) networks. Their uses are numerous, but mostly they are used for file sharing. However since there is no central authority for monitoring the exchange of files, there are many attackers that use P2P networks to transfer malicious programs like Trojan horses or viruses. Furthermore it is quite hard to block the p2p applications by means of firewall usage, since the new software includes methods of firewall evasion (called firewalinkg in most cases). Encryption methods have been incorporated in the latest versions of p2p clients, so it is harder to detect their usage, or monitor and scan the files that are exchanged. Most users download the files and when they execute them the attacker gains access to their system which can be used as a botnet client or in order to steal personal data.

MANAGEMENT IMPLICATIONS

As the landscape of security changes by taking into account all these issues and trends the managing of modern computing security evolves in a way that has to accommodate these changes.

The first but essential step in order to manage security threats is to have always security in mind even in the initial phase of designing a product or a service. Security must be one of the top three goals in the designing phase. According to the software engineering literature (http://infolab.stanford.edu/~burback/watersluice/node2.html) mistakes that are made during the design phase of an information technology project are usually harder to fix, since the design of a system affects a number of different components. On the other hand a security mistake or weakness in the implementation phase usually affects only a specific part of a system and as a result it is easier to realize it and improve it (Khansa & Liginlal 2009). Furthermore design security mistakes or failures can affect all the users of a product whereas implementation security mistakes or failures can affect a large part of the user base but not everyone uses all the components of a product with the exception of the core parts. That is why security can't be seen as another 'future add-on' and should be treated carefully in the designing phase of an IT project. An example of what can happen if we do not consider security as a primary issue is the situation with the internet protocols. Almost every well known internet protocol was designed without having security as a primary objective and as a result they do not support cryptographic functions or strong user authentication. In order to deal with the previous situation new protocols were developed as an add-on to existing protocols but this led to an increase in complexity. That is why a lot of traffic in the internet is unencrypted and authentication methods designed even 20 years ago are still in use. A solution to this problem is the creation of security integrated products/services really easy to activate or even better to make sure that all products/services are security hardened and only in special cases users are able to fall back to non-secure versions.

Security can't be achieved without a significant cost both in time and money. A lot of time is needed in order to evaluate a product design from a security perspective, to test it for all the possible security problems and resolve the interactions of that product with other products (Humphreys 2009). However people responsible for product security should realize that it is better to have a bug free secure product, than rushing this procedure and provide security as an add-on.

Quality evaluation as part of the testing phase of the product is usually the last but extremely important step before the final release. Security checking should also be part of this stage. Since security is an important factor determining the quality of the product, the product should be tested against the initial security consideration to examine whether it meets the design needs. It is hard to imagine that a product has good quality when it fails to meet certain security standards, for example it is not possible claim that a browser has a good quality if it lets an attacker remotely have access to personal information of the user. Security quality evaluation of a product is a very important aspect of the security process (http://www.schneier.com/crypto-gram-0005.html), since in this phase a lot of security issues can be dealt and their origin can be traced back either to design or to implementation stage. In that way when the product is ready all the security issues that had been spotted would have been fixed or would have a well known workaround. This procedure can also improve the response time in case an incident comes up. From a quality evaluation perspective security tests are sophisticated quality instruments since when new vulnerabilities are detected, new answers must be found and incorporated in the tests and those tests should be run over again for new and old products. Furthermore usually security issues are not simple bugs or program errors and creating tests in order to evaluate products is a time consuming process that has to be done only by specialized personnel.

The previous paragraphs reveal the importance of having specialized personnel in the whole product construction phase. From the design phase to the final quality assurance and deployment phase there is a need for security experts to have an overview of the process. Even further all the people that are involved in the construction should at least have a minimal security education (Ng et al. 2009). This raises the need for more specialized training on security issues that affect the different positions. People should have special security skills depending on their position (designing, developing, deploying, evaluating) but they should also have a common background that will make communication easy and flawless. Security education should also be mandatory for users. An organization, besides of the people that are technical competent and take active participation in the production, has a lot of people in less technical positions that fulfill other needs. These people are also become an active target from an attacker perspective, and actually they are a more active target since they can be more easily fooled. Therefore the need to have at least a minimal security education to all the people that are evolved in an organization is important in order to have a good overall security policy. In many cases people say that ignorance is bless, but from a security perspective ignorance is the fastest way to be successfully attacked.

CONCLUSIONS

It is obvious that security is starting to gain more attention by the information industry. Attempts have been made to provide an international security standard but still security problems exist and evolve (Gerber & Von Solms 2008). In the past security was considered as an add-on to certain products but this is starting to change as the impact of security doesn't affect a small percentage of the users population – the few privileged who had access to technology products – but a larger number of people. Initial security problems, like buffer overflow or file system permissions, although still present have been examined and solutions have been found. However, the attack surface has increased and modern security problems, based on more sophisticated attacks focusing on core elements or design problems, have arisen. In the future, the re-evaluation of information products from a security perspective will continue while new methods of attacks will be discovered and a wider part of users population will be threatened. The burden of incorporating security issues to accommodate new security trends falls in the hands of security experts. They will have to find ways in order to accommodate the extra cost in time and money, and most important to focus on users' security training and perception. The key element would be to develop a security culture to every user or organization in order to face the challenges of the new digital era.

AUTHOR INFORMATION

Aristotelis Glentis is a PhD candidate at the Department of Information Technology and Telecommunications of the National & Kapodistrian University of Athens. Since 1999 he has been working at the Network Operation Center (NOC) of the university as a security administrator. His current research interests include new trends in security and security strategies.

Anastasios Panopoulos currently teaches at the Department of Business Administration of the Athens University of Economics and Business. He has a PhD, completed in 2007, and he is project manager in some national projects related to the enhancement of entrepreneurship and public relations. His current research interests include the role of new technologies in the public relations environment, the influence of the Internet for the execution of public relations strategies, and the strategic role of relationship marketing.

Ilias Kapareliotis has a PhD from the Athens University of Economics and Business. He is visiting lecturer at the Department of Business Administration of the Athens University of Economics and Business. His research interests are focused on brand valuation methods, qualitative research marketing methods, and strategies for public relations in an e- environment.

REFERENCES

1. Ashenden D., (2009), "Information Security Management: A Human Challenge?", Information Security Technical Report, (forthcoming).
2. Assaf D., (2008), "Models of critical information infrastructure protection", *International Journal of Critical Infrastructure Protection*, vol. 1, pp. 6-14.
3. Bose I. & Leung A.C.M. (2008), "Assessing anti-phishing preparedness: A study of online banks in Hong Kong ", *Decision Support Systems*, vol. 45, no. 4, pp. 897-912.
4. Botha R. A., Furnell S.M. & Clarke N.L., (2009), "From desktop to mobile: Examining the security experience", *Computers & Security*, (forthcoming).
5. Cakanyildirim M., Yue T.W. & Ryu Y.U., (2009), "The management of intrusion detection: Configuration, inspection and investment", *European Journal of Operational Research*, vol. 195, no. 1, pp. 186-204.
6. Computer Security Institute, (2008), "CSI promotes more security measures", *Network Security*, vol. 2008, no. 11, pp. 2.
7. Fogel J. & Nehmad E., (2009), "Internet social network communities: Risk taking trust and privacy concern", *Computers in Human Behavior*, vol. 25, no. 1, pp. 153-160.
8. Gerber M. & Von Solms R., (2008),“ Information Security Requirements-Interpreting the legal aspects", *Computers & Security*, vol. 27, no. 5-6, pp. 124-135.
9. Hancock B. (1998), "Security Views", *Computers & Security*, vol. 17, no. 4, pp. 280-292.

10. Hekmer G., Wong J.S.K., Honavar V., Miller L. & Wang Y., (2003), "Lightweight agents for intrusion detection", *Journal of Systems and Software*, vol. 67, no. 2, pp. 109-122.
11. Herzberg A., (2009), "Why Johnny can't surf (safely)? Attacks and defenses for web users", *Computers & Security*, (forthcoming).
12. Humphreys E., (2009), "Information Security Management Standards Compliance, governance and risk management", Information Security Technical Report, (forthcoming).
13. Khansa L. & Liginlal D., (2009), "Valuing the flexibility of investing in security process innovations", *European Journal of Operational Research*, vol. 192, no. 1, pp. 216-235.
14. Ng B., Kankanhalli A. & Xu Y., (2009), "Studying user's computer security behavior: A health believe perspective", *Decision Support System*, (forthcoming).
15. Otrok H., Mehrandish M., Assi C., Debbabi M. & Bhattacharya P., (2008), "Game theoretic models for detecting network intrusions", *Computer Communications*, vol. 31, no. 10, pp. 1934-1944.
16. Tutschku K., Tran-Gia P. & Andersen F.U., (2008), "Trends in network and service operation for the emerging future Internet", *International Journal of Electronics and Communications*, vol. 62, no. 9, pp. 705-714.
17. Van de Wijngaert L. & Bouwman H., (2009), "Would you share? Predicting the potential use of a new technology", *Telematics and Informatics*, vol. 26, no. 1, pp. 85-102.
18. Wang L., Cai L., Liu X., Shen X. & Zhang J. (2009), "Stability analysis of multiple – bottleneck networks", *Computer Networks*, (forthcoming).
19. Wei Y., Chellappan S., Wang X. & Xuan D., (2008), "Peer-to- Peer system-based active worm attacks: Modeling, analysis and defense", *Computer Communications*, vol. 31, no. 17, pp. 4005-4017.
20. Weir C.S., Douglas G., Carruthers M. & Jack M. (2009), "User perceptions of security, convenience and usability for e-banking authentication tokens", *Computers & Security*, (forthcoming).
21. Zhao X., Fang F. & Whinston A.B., (2008), "An economic mechanism for better Internet security", *Decision Support System*, vol. 45, no. 4, pp. 811-821.

NOTES