The ever changing security landscape: Concerns, Challenges and Opportunities

Fredrick Mtenzi
School of Computing, Computer Science Department,
Dublin Institute of Technology, Dublin 8, Ireland
fred.mtenzi@comp.dit.ie

ABSTRACT

In the last few years we have witnessed an exponential growth in terms of networked computers and internet usage. This has led to the seamless fabric of interconnected computing and storage systems, mobile devices, software, wired and wireless networks, and related technologies. This pervasive, cost effective communication has enabled vast, constant flow of information that has transformed work environments and processes in nearly all walks of life, from government to business to research. While this trend is a welcome addition with new applications and services proliferating daily, it has spawn numerous security problems which, are threatening to wipe out all the growth achieved. These security threats have had major cost impact such as lower employee productivity, drain network resources, create financial losses and increase legal liability risks.

In this paper we discuss existing and emerging security threats. We then show that unless purposeful measures are taken such as encouraging businesses to invest more in security, educate users and come up with new paradigms of solving these and emerging security problems all gains of interconnectivity will be wiped out. Solutions for mitigating current security threats are discussed and we extend the threat modelling process to address security challenges posed by internal users.

Key Words: security, threats, awareness, perimeter, malware

1. Introduction

In the last few years we have witnessed an exponential growth in terms of networked computer and internet usage. This has led to the seamless fabric of interconnected computing and storage systems, mobile devices, software, wired and wireless networks, and related technologies. This pervasive, cost effective communication has enabled vast, constant flow of information that has transformed work environments and processes in nearly all walks of life, from government to business to research. This growth has led to new business ventures and modes of communications which we could have not imagined in the beginning of the 80s. While this trend is a welcome addition it has spawn a number of security threats, attacks and scams which a threatening to wipe out all the growth achieved.

Security used to be not an issue of concern to computer users and businesses a few years ago. This is not the case anymore; security concerns now are affecting nearly everyone, in all walks of life. These concerns come in all types and shapes and from different angles. They range from viruses affecting computer installation, worms, spyware, social engineering and financial scams. It is not surprising anymore nowadays to hear in the media of a new outbreak of worms or viruses or financial scams in the digital world. These attacks and threats cause a lot of losses to businesses. Thus security threats cause more than just annoyance they cost individuals and businesses. This cost can be evaluated in terms of time, money, brand, reputations, legal liability and going bankrupt.

It also true that the amount and quality of data that is collected to serve as reference of occurrence of security threats and attacks is very little and unreliable. There are no motivations for businesses or individuals reporting losses they have incurred as a result of security attacks. Reporting attacks causes more problems to businesses as it may lead to damaged reputation, loss of customer confidence and legal liability. However, this data is vital for making strategic decisions on how much businesses should invest in security and preparedness for any breach of security. Further, it may serve as evidence to law enforcement agencies in prosecuting businesses for negligence. Lastly, we need data for creating an on-going society wide awareness campaign where having accurate and current data may help. Vendors involved in developing tools for preventing security attacks rely on this data for improving and predicting trends in security threats.

The emergence of new, sophisticated, blended and targeted security threats suggests that existing approaches to solve them are not adequate. And it has been shown that security attackers now have a financial motivation. This means that solution procedures which worked yesterday may no longer be valid today and we must employ as many new solutions as possible to achieve a defense in-depth.

The white hacker is one group which has been ignored in the quest for finding a lasting security solution. This group has knowledge, experience, talent and enormous patience in security issues; it is high time its contribution is positively taken by the security community. It amazing to note that some security professionals do not want white hackers knowledge to be published, reviewed or make public [1]. While there may be valid reasons for this embargo it is denying the user community the wealth of experience possessed by white hackers.

Recently we have witnessed worrying trends in which the internet and mobile phone are used for bullying among children. One solution to this problem is to educate children of the evils of bullying and the effect it is going to have on bullied children. This awareness campaign should include parents, teachers and other members of community.

The rest of the paper is organised as follows. Section 2 takes a closer look at malware including viruses and worms. Phishing and pharming attacks are discussed in section 3 together with their economic impact. Section 4 covers the demise of the perimeter security as a result of development in mobile technology, changing work practices and globalization of businesses. Ways of mitigating security attacks are discussed in section 5. In section 6 current security challenges are discussed in detail. Opportunities arising from security threats are identified and discussed in section 7, we also extend the threat modeling process. Section 8 covers summary and discussions. Conclusions of the research are given in section 9.

2. Malware

In computer security technology, a virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. A computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. Extending the analogy, the insertion of the virus into a program is termed infection, and the infected file (or executable code that is not part of a file) is called a host. Viruses are one of the several types of malware or malicious software. However, a basic rule is that computer viruses cannot directly damage hardware, only software is damaged directly. The software in the hardware however may be damaged. Examples of viruses include W32/HIV, W95/Boza, W64/Rugrat.3344, and Linux/Jac.8759 [2].

A computer worm is a self-replicating computer program, similar to a computer virus. A worm is self-contained and does not need to be part of another program to propagate itself. They are often designed to exploit the file transmission capabilities found on many computers. In addition to replication, a worm may be designed to do delete files on a host system or send documents via email. More recent worms may be multi-threaded and carry other executables as a payload. However, even in the absence of such a payload, a worm can wreak havoc just with the network traffic generated by its reproduction. Mydoom, for example, caused a noticeable worldwide Internet slowdown at the peak of its spread [3].

A common payload is for a worm to install a backdoor in the infected computer, as was done by Sobig and Mydoom worms. These zombie computers are used by spam senders for sending junk email or to cloak their website's address. Spammers are thought to pay for the creation of such worms, and worm writers have been caught selling lists of IP addresses of infected machines [4]. Others try to blackmail companies with threatened DoS attacks [5]. The backdoors can also be exploited by other worms, such as Doomjuice, which spreads using the backdoor opened by Mydoom [6].

Trojan horses are programs that pretend to be legitimate software, but actual carry out hidden, harmful functions [7]. Example is a DLoader which arrives in an email attachment and claims to be an urgent update from Microsoft for Windows XP [8].

Spyware is a broad category of malicious software intended to intercept or take partial control of a computer's operation without the user's informed consent. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

Spyware differs from viruses and worms in that it does not usually self-replicate. Like many recent viruses, spyware is designed to exploit infected computers for commercial gain [9]. Typical tactics used in furthering this goal include delivery of unsolicited pop-up advertisements; theft of personal information (including financial information such as credit card numbers); monitoring of Web-browsing activity for marketing purposes; or routing of HTTP requests to advertising sites. In some cases, spyware may be used to verify compliance with a software license agreement (or EULA) [2].

A rootkit is a type of program designed to mask the existence of malware so that it appears hidden from routine malware searches by security software. The rootkit is designed to replace components of the operating system at the user or kernel level [10], [11]. This might be done, for example, by hooking an API so the rootkit filters particular information in a way that deceives the operating system. This is achieved by hiding processes, services, TCP/IP ports, files, directories, and other operating system properties [12], [13].

Attackers are becoming sophisticated and extremely clever in creating rootkits that are highly effective in masking their presence. Once a rootkit infects a computer, it may be nearly impossible for anyone other than highly skilled experienced specialist to detect its existence and remove it [10]. The rootkit authors are becoming more adept at anti-detection methods and they are even writing them for sale to other users.

Currently, we are seeing a move toward attacks directed at a specific company or individual. Instead of attackers designing a new piece of malware and launching it widely, the attacker targets his/her new innovation with the goal of stealing data from a single company, or conducting a ransomware attack (an attack designed to leave an individual victim or targeted company being forced to pay ransom to the attacker) [10]. This may be for personal gain, or the attacker may be on ``assignment" from a competititor or criminal organisation. The proliferation of ransomware leaves companies with no help from security vendors and experts leading to it persisting for a long time.

3. Phishing and Pharming

In computing, phishing (also known as carding and spoofing) is a form of social engineering, characterised by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an email or an instant message. The term phishing arises from the use of increasingly sophisticated lures to "fish" for users' financial information and passwords [14]. With the growing number of reported phishing incidents, additional methods of protection have been needed. Attempts include legislation, user training, and technical measures [15].

Pharming is the exploitation of a vulnerability in the DNS server software that allows a cracker to acquire the Domain name of a site, and to redirect that website's traffic to another web site [16]. DNS servers are the machines responsible for resolving internet names into their real addresses the "signposts" of the internet. The term pharming is derived from the term phishing, the use of a social engineering attack to obtain access credentials such as usernames and passwords. To date however the use of pharming to perform Internet crime for profit has not been demonstrated.

Botnet is used to refer to a collection of compromised machines running programs such as viruses, worms, spyware and being remotely controlled. Botnet attacks typically appear simultaneously from dozens, hundreds, or even thousands of unrelated computers all acting from orders send remotely [17], [18]. Examples of bot software include Agobot, Phatbot, Forbot, XtremBot, and SDBot [19].

4. The demise of perimeter security

Traditionally all efforts have been spend in preventing harm to networks by creating an iron curtain which kept unwanted outsiders away. However, in reality it has been demonstrated that the network is highly vulnerable from threats which originates from within the perimeter. Threats from trusted network users are increasing at an alarming rate. These insider threats are extremely difficult to detect and prevent and are leading to loss of confidential information and customer trust. For example, an authorized insider might be able to disable certain network security mechanisms to allow a collaborator on the outside to gain access [20].

The well defined perimeter is disappearing and the networks now are like sieve. This has been the result of mobile workers, wireless access, web-based application, remote workers, contractors, and business partners. These factors have innocently or maliciously opened attacks on the network and jeopardized confidential information, corporate assets and intellectual property [20]. Now attacks can come from anywhere at any time.

New types of technologies and devices are creating cavities on and within the network perimeter often without the notice of companies. Companies must realize that endpoint devices - such as personal computers, PDA's, blackberries, and smart phones - must be secure on the network as well as when they are connecting from outside the perimeter, such as through a VPN or wireless connection. If these endpoints are not secure, they can easily inadvertently introduce malicious code and other security threats to the inside of the perimeter.

As perimeter walls have been falling down, security professionals agree that the insider threat is more potent than originally thought. Currently, we need powerful, proactive security practices for all systems that connect to our internal network. New business demands, processes and technology will continue to expand our perimeter, increasing the risks to our network. Without a plan to secure inside perimeter, employee productivity, revenues, information, computing resources, and company brand are highly susceptible to being damaged. Therefore, internal security has become an obligation and a necessity. Customer confidence relies upon it, and laws and regulations require it. At the technology level the time has come to pervasively secure inside the network perimeter.

The occurrences of employees with authorized access to company ICT resources committing fraud are likely to continue to increase in the near future. It is difficult to ascertain the current numbers for such crimes because they are under-reported to law enforcements and prosecutors. Companies are often reluctant to make such reports because of insufficient level of damage to warrant prosecution, lack of evidence or insufficient information to prosecute, and concerns about negative publicity.

Countries and companies to whom you outsource your IT activities may not have the motivation or knowledge to adequately secure their activities. This means if you connect your network to the companies where you have outsourced you IT activities, their security threats, vulnerabilities, and risks become yours. This may have far reaching consequences as demonstrated by recent events where companies which outsourced their IT activities had their fingers burned [20].

5. Mitigating security threats and attacks

In order to mitigate security threats and attacks companies must focus on securing their internal network with the same zeal and vigilance that they are applying at the perimeter. The same techniques developed and applied for the perimeter may be used in their internal networks such as follows:

- Defending against malicious code and worms and containing their spread
- Ensuring only safe devices and endpoints access the network
- Ensuring the privacy and integrity of data in motion
- Protecting critical applications from misuse and abuse
- Establishing an effective program for patching vulnerable systems
- Educating network users about how to apply security

There is an increased urgency to address old problems with new solutions. Companies have always had to face the problems of technology evolving faster than the associated security solutions. This same phenomenon takes place in the laws and regulatory framework in security which is always playing catch-up. Therefore, keeping employees vigilant with their security practices as new computing devices become ever more mobile, affordable and pervasive has been one of the major challenges.

Companies must plan ahead how they will react to internal security incidents and breaches. It is true that many companies are not aware and prepared [20]. The ways in which companies must respond to incidents and breaches fall in one of approaches:

- Locking down the affected sections of the network completely as soon as there is significant security event
- Shutting down the entire network completely when an event occurs
- Turning on monitoring, quarantining, and blocking right away
- Reacting chaotically in an ad hoc manner with no clear direction or plan

In practice most companies patch the perimeter and external servers much more quickly than the internal network resources. Since these resources are internal most company leaders assume they can take much more time to apply the security patches because the perception is that the risks are much lower within the perimeter. However, it helps companies to proactively use conventional countermeasures such as use of anti-virus software, restricting administrative rights to normal users, use digital signatures in all users files, endpoint blocking enabling DEP, auditing security events and disabling application features unnecessary to users [10].

6. Security Challenges

One of the major challenging aspect of today's environment is that the security market is still in its infancy [20]. There are few formal standards established for security products or services. Many vendors offer individual solutions such as firewalls that address only one type of security need. Companies are challenged with making disparate and widely ranging types and qualities of security solutions work together, creating patchwork security across the company. IT security staff bears the daunting task of stitching all these solution together, constantly deploying an expanded list of products and spending large amounts of time and money completing work to ensure that these components are working together.

The immaturity of security market creates other significant challenges for IT security staff:

- IT security staff must absorb huge amounts of information to understand and manage the computing environment. Each product generates alarms, logs, and other information that they must review to determine whether something is wrong.
- The software industry places relatively low priority on security. In fact, security is often sacrificed to make the software/hardware easier to use and less costly, resulting in an ever growing number of vulnerabilities.
- It is evident that security vendors will not offer mature solutions to adequately protect business any time soon. This means companies must develop strategies to mitigate risks for their own unique threats, risks, and vulnerabilities instead of depending upon a silver bullet solution to provide resolution.

The second challenge is the nature of the internal network environment which presents unique challenges when compared with the perimeter security. When considering internal and perimeter security, internal security posse’s significantly much greater challenge for the following reasons:

- Scale of the environment - protection requires numerous networks, sub-networks and potentially thousands of systems.
- Scope of the environment - there is significantly greater, widely varying company applications and underlying protocols - not just HTTP, FTP, SMTP, and the handful of others associated with the DMZ.
- Number of users - the number of individuals and groups authorized to use the internal network is much more than with external environment where there are typically very few defined groups with limited access privileges. Internally, the different roles can easily number in the hundreds or thousands, resulting in a much more complicated set of policies and controls.
- Speeds and volumes of traffic - internet connections and associated DMZ resources rarely face more than 45 Mbps, while internal networks and systems routinely operate at two to ten that bandwidth. As a result, any controls that are implemented in the internal environment need to be capable of conducting the necessary inspections and dispositions at a much greater rate.

More details on the comparison of security challenges between internal and perimeter security are given in [20].

The third challenge is vulnerabilities in computer systems which are a function of software designers and implementers plus the personalities who manage, maintain, built and design these systems [21]. Hackers have used this strategy of understanding people before they can attack computer systems. The insight they gain enables them to penetrate computer systems which normal uses perceive to the very secure. Literature in security is littered with examples of hackers penetrating government, financial and academic institutions computing infrastructure with easy.

The fourth challenge is the internet which is accessible from most locations in the world and most large companies are now multi-national, which makes it important to understand and operate in compliance with worldwide regulations. Some of these regulations are very strict and difficult to ensure security compliance. Examples of these regulations include the European Union Protection Directive [22], Canada's Personal Information Protection and Electronic Documents Act [23], Japan's Personal Information Protection Act [24], Australia's Federal Privacy Act [25] and Sarbanes-Oxley Act [26]. The challenge is increased because laws and regulations are generally enacted on a country by country or regional basis while electronic commerce is conducted globally.

7. Security opportunities

According to AV-Test, a German virus research group, the response times of anti-virus vendors to the emergence of a new virus vary dramatically among vendors [27]. Table 1 shows the response times of data based on four virus outbreaks, Dumaru.Y, MyDoom.A, Bagle.A and Bagle.B. Even in the speediest case, the potential for serious amount of destruction to occur while waiting for new virus signature files to be developed is considerable. To make matters worse it has been shown that in some cases even anti-virus software can have security vulnerabilities such as buffer overflow [28]. This leaves users susceptible to attacks and reduces their confidence. However, there is room for improvements in both cases which is an opportunity not to be missed by security companies.

Table 1: Average response times of Anti-Virus Vendors

Response Time (Hrs:Mins)	**Anti-Virus Vendor**
06:51	Kaspersky
08:21	Bitdefender
08:45	Virusbuster
09:08	F-Secure
09:16	F-Prot
09:16	RAV
09:24	AntiVir
10:31	Quickheal
10:52	InoculateIT-CA
11:30	Ikarus
12:00	AVG
12:17	Avast
12:22	Sophos
12:31	Dr. Web
13:06	Trend Micro
13:10	Norman
13:59	Comman
14:04	Panda
17:16	Esafe
24:12	A2
26:11	McAfee
27:10	Symantec
29:45	InoculateIT-VET

The job market in security area as a whole has increased in the last few years. While very few companies were employing security workers in the last few years, the trend has now changed. We are seeing small, medium and large companies employing security staff [29]. They employ staff in the following categories security analysts, security engineers, security auditors, information’s assurance engineers and managers, security architect, security consultant etc. The titles for security workers seem to increase by day and the type of jobs and qualifications required from them vary greatly [30].

The information security market is still its infancy. Security in most cases is incorporated as an afterthought not as an integral part of software/hardware design.

As a result we are now witnessing a culture of patching after software/hardware has been released for use to general public. Unless we change the incentive to vendors for producing good software/hardware this trend is here to stay. Bruce Schneier in [31] proposes a model which will make vendors liable for security holes in their software.

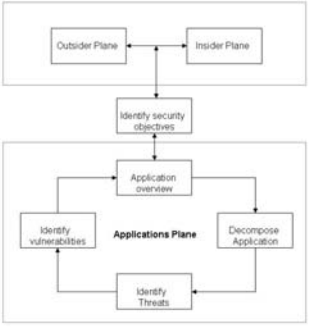

Figure 1. Threat Modeling Process

In order to provide a basis for mitigating security threats we have adopted a model from IBM and extended to include the threats poised by insider as shown in figure 1.

The computer science community has a lot to learn from the hacker's community especially the white hackers. They are passionate and independent-minded global community of highly skilled technical experts that frequently functions outside the mainstream of computer product development and conventional technology research [32]. These experts are responsible for innovation that pushes the limits of technology, sometimes in unintended or uncomfortable ways, as well as for prescient warnings about the threats of both technology and the government's technology-related policy and regulations. In many cases their research is ahead of what's being done in Universities, research centres and companies, but with results that are unlikely to ever appear in academic journals and conferences due to different ways of disseminating information [33], [34]. Therefore, unless deliberate efforts are done to unite the two communities' hackers' contribution in technology development will be missed to the detrimental of security users.

8. Summary and Discussions

Consequences of security attacks include among others the loss of reputation and customer trust. It is worthy noting that businesses are investing very little in Security, because they do not see it as being a major problem until when the business is faced with one. This is a very dangerous approach as it demonstrates lack of awareness, cavalier approach and really sitting like a lame duck. Changes in the security landscape calls for a more proactive approach to be adopted by all in decision making positions.

We need security by design and use of more than one security strategy (layered protection mechanism). Security has not always considered a priority due to the rush in delivering systems. As a result users are expected to be used as guinea pigs to test and report security problems. It is high time to challenge this mode of business, because users are being sold software which is not fully security tested.

It is important for users and businesses to realise that, it is nearly impossible to achieve perfect security. This is because applications become insecure over time. As a result of usage, patching and unanticipated interactions with other applications. This demonstrates a never ending quest to achieve perfect security. In this case an on-going user awareness programme will go a long way into protecting the business.

If we are to stand a chance in winning the security war then collaboration among all key players must be a paramount issue. This includes all users, businesses and government. No one is going to be secure until all interconnected computers and devices are secure, which is a monumental task. May be the only salvation will come from a paradigm change in terms of security thinking and approach.

The rate of change in the computing industry has led to machines being used for IT processing to be obsolete in short amount of time. This trend has led to a lot of PCs being disposed from companies. However, as they are being disposed evidence shows that either they are not wiped properly or sensitive personal data is left in these machines. If this data falls in wrong hands it is a major security threats to companies and/or individuals. Some of these PCs with valuable personal data have found their way in different countries far from the origin country.

The political structure of an organisation is a source of security threats. Hackers use the web of business relationships between the organisation and its subsidiaries, parent organisation, sister companies, service providers and business partners to find ways of compromising the computer systems [21]. In most cases all of these parties may own or manage systems that are vulnerable to attack, and could if exploited, allow attackers to compromise the internal space.

We have to remember that the company is impacted by insiders committing security breaches such as making it being the subject of a civil lawsuit. All security incidents impact the company. The value of a security breach can be measured by both tangible and intangible considerations. The tangibles can be calculated based on estimates of lost business, lost customers, lost productivity, increases in insurance premiums, legal costs for defending the business in liability suit and impact of breach disclosure on stock price. Intangible costs are difficult to calculate because they are not directly measurable, but still very important for the company. They are often related to a loss of competitive edge that results from the breach. A breach can affect the company's competitive edge through customer's loss of trust, failure to win new customers because of bad press associated with the breach and competitor's access to confidential or proprietary information.

9. Conclusions

Security is difficult because the threats are a moving target in computer systems and networks. Lately, we have started witnessing targeted attacks which are very difficult to detect and recover from it. These attacks are in most cases motivated by financial gains. Another similar and more worrying attack is cyber-extortion. Proliferation and advancement in mobile devices have lead to mobile devices attacks, which though not prevalent we should expect to see more and more of these types of attacks.

Recent research show that around 90 percent of a business confidential data is in electronic format. This figure varies depending on the level of computerization of a business. However, there is an agreement among security professionals that critical business data is in a form that requires it to be securely guarded.

The face of computer crime has not changed much. Computer crime is growing and will continue to grow. As Willy Sutton said about 100 years ago when asked why he robs banks, “That’s where the money is”. Today computers and the internet are where the money is, not only that, it is easy money. We have to accept that and act upon it [35].

It is important to note that security threats are asymmetric, surreptitious, and constantly evolving. For example it is true that a single individual or a group anywhere in the world can inexpensively and secretly attempt to penetrate systems containing vital information or mount damaging attacks. Attack tools and resources are widely and readily available on the internet and new vulnerabilities are continually discovered and exploited. This demonstrates that unless we come up with a paradigm change in security, this is never ending war.

The current security culture, greedy, poor training and lack of regulation is responsible for the state we find ourselves in. In a lot of systems in use today security has been implemented or incorporated as an after thought. Thus, a patching culture has emerged; this has led to unstable systems where the results of patching cannot be predicted for certain. Software companies have been more than happy to release half backed software and let users be the testing guinea pigs.

Computer Science programme offered in a lot of academic institutions until lately did not have any security components in them. The state of affairs is changing now as the number and variety of security courses now has increased considerably. Other professional security bodies offer training in security which has helped a lot to address the skills gap in the area. It is also worthy noting a significant contribution in training offered by security vendors.

The role of law and regulations in mitigating security threats cannot over-emphasised, even though they are lagging behind. Social norms influence the way society perceive about security. However, with a proper security awareness programme it is possible to dispel some of social misunderstandings and create an ethical and responsible way of addressing security issues.

References:

[1.] Pfleeger, C.P. and Pfleeger, S.L., *Why we won't review books by hackers*. IEEE Security and Privacy, 2006. **July/August**: p. 9.

[2.] Szor, P., *The Art of Computer Virus Research and Defense*. 2005: Addison-Wesley and Symantec Press.

[3.] Wong, C., Bielski, S., McCune, J.M., and Wang, C. *A study of mass-mailing worms*. in *WORM '04: Proceedings of the 2004 ACM workshop on Rapid malcode*. 2004. New York, NY, USA: ACM Press.

[4.] *Cloaking Device Made for Spammers,* http://www.wired.com/news/business/0,1367,60747,00.html *(last accessed 7 December 2006).*

[5.] *Hacker threats to bookies probed,* http://news.bbc.co.uk/2/hi/technology/3513849.stm *(last accessed 7 December 2006).*

[6.] *Doomjuice (computer worm),* http://en.wikipedia.org/wiki/Doomjuice *(last accessed 7 December 2006).*

[7.] *Trojan horse (computer worm),*http://en.wikipedia.org/wiki/Trojan_horse_(computing) *(last accessed 7 December 2006).*

[8.] *Xombe or Dloader,* http://security.yale.edu/xombe/index.htm *(last accessed 7 December 2006).*

[9.] Forte, D., *Spyware: more than a costly annoyance*. Network security, 2005. **12**: p. 8-10.

[10.] Mitnick, K., *Mitigating Malware in Userland*. 2006, Mitnick Security Consulting, LLC.

[11.] Felten, E.W. and Halderman, A., *Digital Rights Management, Spyware and Security*. IEEE Security and Privacy, 2006. **4**(1): p. 18-23.

[12.] Levine, J., Grizzard, J., and Owen, H., *Detecting and Categorizing Kernel-Level Rootkits to Aid Future Detection*. IEEE Security and Privacy, 2006. **4**(1): p. 24-32.

[13.] Alsbih, A., *How to write a Rootkit*. Linux Magazine, 2006. **69**: p. 22-28.

[14.] Dhamija, R., Tygar, J.D., and Hearst, M. *Why phishing works*. in *CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems*. 2006. New York, NY, USA: ACM Press.

[15.] Robila, S.A. and Ragucci, J.W. *Don't be a phish: steps in user education*. in *ITICSE '06: Proceedings of the 11th annual SIGCSE conference on Innovation and technology in computer science education*. 2006. New York, NY, USA: ACM Press.

[16.] Payton, A. *Determining the proper response to online extortion*. in *InfoSecCD '05: Proceedings of the 2nd annual conference on Information security curriculum* *development*. 2005. New York, NY, USA: ACM Press.

[17.] McKewan, A., *Botnets - zombies get smarter*. Network Security, 2006. **6**: p. 18-20.

[18.] McKenna, B., *Botnets armies and enterprise security*. Infosecurity Today, 2006. **3**(2): p. 4.

[19.] Schaffer, G.P., *Worms and Viruses and Botnets, Oh My!* IEEE Security and Privacy, 2006. **4**(3): p. 52-58.

[20.] Herold, R., *The Definitive Guide To Security Inside the Perimeter*. 2005: Realtimepublishers.com Apani.

[21.] van der Walt, C. and Phillips, G.M., *Penetration Tester's Open Source Toolkit*, ed. Long, J., Bayles, A.W., Foster, J.C., Hurley, C., Petruzzi, M., and Rathaus, N. 2006: Syngress Publishing Inc.

[22.] *European Union Protection Directive*, http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm *(last accessed 7 December 2006).*

[23.] Peyton, L. and Nozin, M. *Tracking privacy compliance in B2B networks*. in *ICEC '04: Proceedings of the 6th international conference on Electronic commerce*. 2004. New York, NY, USA: ACM Press.

[24.] *Japan's Personal Information Protection Act*, http://www.privacyexchange.org/japan/JapanPIPA2003v3_1.pdf *(last accessed 7 December 2006).*

[25.] *Australia's Federal Privacy Act*, http://www.privacy.gov.au/act/index.html *(last accessed 7 December 2006).*

[26.] *Sarbanes-Oxley Act,*http://www.law.uc.edu/CCL/SOact/soact.pdf *(last accessed 7 December 2006).*

[27.] Marx, A., *Outbreak response times: Putting AV to the test*. Virus Bulletin, 2004: p. 4-6.

[28.] Morgenstern, M., Marx, A., and Landesman, M. *Insecurity in security software*. in *Virus Bulletin conference october 2005*. 2005.

[29.] SecurityFocus, http://www.securityfocus.com/jobs/opportunities.

[30.] *The SANS 2005 Information Security Salary and Career Advancement Survey*, http://www.sans.org/salary2005/ *(last accessed 7 December 2006).*

[31.] Schneier, B., *Secret and Lies: Digital Security in a Networked World with new information about post 9/11 security*. 2004: John Wiley.

[32.] Conti, G., *Hacking and Innovation.* Communications of ACM, 2006. **49**(6): p. 36.

[33.] Ross, T., *Academic Freedom and the Hacker Ethic.* Communications of the ACM, 2006. **49**(6): p. 37-40.

[34.] Grand, J., *Research Lessons form Hardware Hacking.* Communications of the ACM, 2006. **49**(6): p. 45-49.

[35.] Winkler, I., *The Changing Face of Computer Crime*. The ISSA Journal, 2005: p. 6 - 8.