Annual ADFSL Conference on Digital Forensics, Security and Law 2010

May 20th, 1:00 PM

A Layered Framework Approach to Mitigate Crimeware

Mathew Nyamagwa
Metropolitan State University, mathew.nyamagwa@metrostate.edu

A Layered Framework Approach to Mitigate Crimeware

Mathew Nyamagwa
Metropolitan State University
Mathew.Nyamagwa@metrostate.edu

ABSTRACT

Crimeware attacks are growing at such an alarming rate and are becoming so prevalent that the FBI now rank cybercrime among its top priorities after terrorism and espionage. New studies estimate cyber crimes cost firms an astounding $1 trillion annually. But the good news? Over 80% of them are preventable. Crimeware is not a purely technical threat but more or a socio-technical affair. This clearly brings out the fact that computers do not commit a crime, but we (humans) do! In this paper I propose a layered approach that involves all stakeholders from end-users to service-providers and law enforcement to greatly mitigate the recent proliferation of crimeware.

Keywords: Crimeware, Jurisdiction, International space

1. INTRODUCTION

Malware is now not just about a lone hacker or bored college student, it now built and pushed by technologically sophisticated organizations, aided-by phishing-like deceit tactics and spread via advertisements, social networks and other IT electronic devices for financial gain. By exploiting known and undisclosed vulnerabilities, these malware help cybercriminals capture keystrokes of individuals, spies on corporations and politicians and threatens national security by means of serverjacking, information leakage and a potential deterioration of trust in the infrastructure[1]. Unlike earlier forms of code-based attacks that operated without any human intervention, these programs frequently exploit human credulity, cupidity, or naiveté to persuade or trick the computer user into downloading, installing, or executing them.

Crimeware is not a purely technical threat but more of a socio-technical affair. From the –technical perspective, traditional security mechanisms such as firewalls, antivirus solutions, and intrusion detection and prevention systems have been used to reduce its impact. Different yet sophisticated security frameworks such the Clark-Wilson Commercial Integrity model[2] by David Clark, a professor of computer science at MIT and David Wilson, accounting executive at Ernst and Whitney, and Risk Management Framework[3] by Dr. Gary McGraw of Cigital among others have been proposed and implemented but still agree that computer security is still incapable of thwarting sophisticated threats that morph and mutate rapidly.

From the socio- perspective, Cyber society lacks all of the requisite attributes of a state as outlined in the 1933 Montevideo Convention on the Rights and Duties of States, which specifies that a bona fide country (society) must have a permanent population, a defined territory, a government, and the capacity to enter into relations with other states[4].

This definition implies that cyber society is not a distinct and sovereign state. Rather, it is a composite of loose associations that transcend traditional geopolitical nation-state boundaries. Jurisdiction in cyberspace is therefore contingent on the laws of individual countries that govern human activities in physical places. In many respects, the Internet has obscured the question of national sovereignty and jurisdiction.

To this point, three fundamental questions arise: What if the transgressor resided in a country that does not have computer crime laws? Could they be charged under the laws of nations or states that do? If cyberspace extends beyond the geopolitical boundaries that traditionally define legal jurisdictions, what responsibility do governments have to protect individuals interacting in this transient realm?

Because the Internet has obscured the question of national sovereignty and jurisdiction, crimeware attacks are more precarious. New studies estimate that cybercrime cost firms an astounding $1 billion[5], and now the FBI ranks cybercrime among its top priorities after terrorism and espionage[6]. But the good news! Over 80% of cybercrime is preventable[7]. I propose a layered framework approach that involves all stakeholders including end-users, computer scientists, law enforcement, legal agencies and politicians should combine to develop a computer security framework, computer forensics and investigation techniques, cyber laws to curb and/or deter inter-geopolitical crimeware attacks.

Section 2 looks into related work, section 3 discusses this layered framework taking a defense mechanism that combines end-user literacy, aspects of law and order in cyberspace, the use of trusted computing platform, and secure infrastructure. Finally, section 4 is the conclusion.

2. Related Work

Crimeware can be defined as any malicious piece of software that satisfies at least one of the following criteria: 1). Stealing online credentials, personal data, or any other piece of information necessary for identity takeover, with the intent of using the stolen identity to steal funds; and /or 2). Performing unauthorized online transactions in order to steal funds; this includes Trojans that "hijack" online banking or other secure sessions of infected users and carry out fraudulent transactions after the user has logged out[8].

Technical frameworks[9,10] have been presented to mitigate specific unit areas of cybercrime. In [9], the design (Rubot framework) provides an experiment framework to set up customized botnet architectures on testbeds. The problem with botnet research is the scope (millions of victims) and the evasion techniques deployed by its propagators. Likewise in[10], the phishing-prevention framework is presented, derived from SANS 17799 that focus specifically on the problem of identity theft by phishing attacks. These frameworks among other have provided a secure technical platform but given the nature and current state of crimeware, a social framework needs to be attached.

Like David Johnson and David Post[11] have argued in a number of articles, cyberspace should be its own Jurisdiction, with its own courts (or "Virtual magistrates") to resolve disputes that occur entirely online.

3. Layered Framework Approach

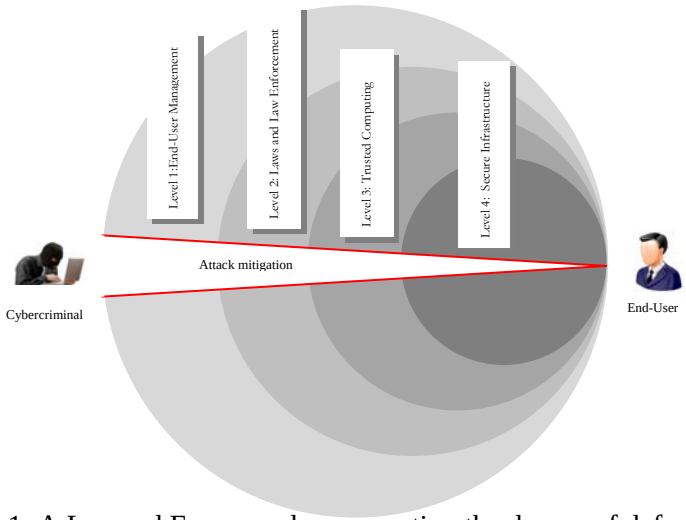

Fig 1: A Layered Framework representing the degree of defense.

3.1 End User Security Management (EUSM)

Reference [12] showed data that end users were concerned with security; however, they were both unsure of the appropriate action to take and frustrated by security practices extraneous to actual work.

As networked computing has become pervasive, the challenges of maintaining secure environments for end-user computing have increased enormously. End users are often cast as the "weak links" in computer security, as they tend not to be aware of the latest security attack techniques nor the rapidly-evolving preventive measures.

EUSM represents a tradeoff. Reducing users' responsibilities may result too much disengagement, but demanding too much attention may result in fatigue and confusion. Compliance is a similar issue: the needs of the organization and the abilities of the individual need to be balanced.

Most end users conflate security with general functionality; they see a security failure as not significantly different from any other failure. This can be a problem, since some security problems do not cause failures; this can also be a good sign that it is possible to motivate users to act.

While user behaviors for more widely spaced tasks, such as changing passwords and updating virus scanner profiles, were problematic end users, a number of security ensuring behaviors observed that are more regular and common. Examples include locking the computer when away, keeping passwords secret, and protecting the physical security of the computer.

A standard approach to ensuring more literate end users is to expand the computer literacy curricula that people are exposed to in their work settings. Informal learning (learning that happens during the enactment of everyday behaviors and problem solving) should be recruited to enhance users' EUSM practices; this type of learning is more amenable to constantly changing information (like EUSM), and easier for organizations to leverage than formal training, due to lower cost and higher value.

Users have no way to understand what is happening within a computer or a computer network; even if they do, they have no interest in a computer's internals. This leads at times to an inability to distinguish between different problem etiologies. This may be due to willful ignorance, frustration, or limited mental models of computer functionality and failure, but is likely to be caused at times by all three.

The general problem of software invisibility is both a benefit and a drawback to computing. Users are not interested in technical details, and when they are forced to understand these details to operate a computer properly.

As much as user are to get down to these technical details, policies must be designed, implemented and governed by a legal system can greatly deter crimeware.

3.2 Law and Order in Cyberspace

What is the identity nationality into cyberspace? Given the technologically evolving nature of cybercrime, this is a perfectly understandable attitude and a respectable position to take if we are willing to ignore, accept, and perhaps even help perpetuate confusion surrounding the dynamic technological aspects of computer-related crime and its effects throughout society.

The state of empirical research and general body of literature pertaining to these issues are extremely limited. Virtually no studies of a general population have yet been published that take into account the theoretically complex phenomenon of cybercrime, operationalized as activities in which computers or other electronic IT devices are used to facilitate illegal or socially abusive behaviors via the Internet.

Estimates of financial losses due to technology abuse are considered, and how much underreporting by corporations (and other types of victims) is assumed[13]. It has also long been known that most companies are reluctant to report cybercrimes to law enforcement for fear of losing public confidence

or exposing weaknesses in their information security[14]. Other major reasons for the lack of data and research on crimes committed with computers or other types of IT devices include:

1. The priority given to violent crimes by public officials and victim advocacy organizations
2. Relatively indifferent attitudes of many police and prosecutors to nonviolent crime
3. The technical and intimidating nature of crimes committed with computers and other IT devices
4. Easy treatment of cybercriminals by courts even when prosecuted
5. The inadequacy of training for police officers and security professionals to recognize and respond to, and adequately investigate cybercrimes, and
6. The ever-changing capabilities of computers and those who abuse them.

It is generally believed, for example, that a substantial portion of transnational financial crime constituting economic and security threats to many regions throughout the world originates in former Soviet Bloc countries such as Ukraine, Russia, and the Baltic States. Such crimes can be attributed to a number of factors:

1. Organized crime groups looking for ways to broaden their of influence
2. The lack of a mature model for policing such crimes and the resources to support it,
3. The resulting lack of fear of apprehension and retribution
4. The vast pool of potential victims, and
5. The ease with which financial resources can be transported around the globe.

3.2.1 Laws and Regulations in Cyberspace

Laws and regulations are extremely important because to some extent they affect virtually every aspect of administering criminal justice and increasingly to managing the security of data, information systems, and facilities that operate critical information infrastructures.

Laws and regulations can be thought of as tools governments' uses to maintain societal order, productivity, and well-being. This situation is exacerbated by cybercrime and information security being international concerns shared by many nations having different legal systems, traditions, and laws

It is important to understand from the onset that construction and enforcement of cyber-related laws and regulations is rapidly evolving in ways that cannot be fully anticipated, and that analysis of these issues depends on understanding the challenges computing and telecommunications technology pose relative to legal standards of behavior, and with respect to due care and diligence in the design and management of information security products and systems.

Most people agree that an individual, who sends a worm, Trojan, or virus into cyberspace, wreaking worldwide havoc on information systems and infrastructures, should be punished severely.

Matters of law arising from using, misusing, and even abusing computers, other electronic IT devices, and information systems are not as clear cut. The concept of law has various definitions and applications but is essentially a set of rules that defines standards of behavior and use of technologies by and among individuals in society.

Laws and accompanying regulations reflect the values, needs, and beliefs of the members of a society and they are designed to provide for the continuity of society, as well as safe, predictable, and reliable relationships among its members under changing conditions.

Laws are also intended to deter people from committing wrongs; to protect individuals, groups and organizations from harm; and to inform members of society of desirable behaviors and preferred

courses of action as well as punishments for not voluntarily complying with society's rules.

Laws and regulations pertaining to illegal use of computers or other electronic IT devices are designed for the protection of everyone in computerized societies. Cyber laws and regulations also provide for ranges of penalties and compensation that may be owed to victims of cybercrimes. They also typically specify legal remedies for victims of computer abuse or cybercrimes to seek damages for losses associated with damaged, manipulated, stolen, or destroyed data or information systems.

The trans-boarder nature of cybercrime presents additional conditions and challenges to concepts of jurisdiction. Administering justice in international cases is predicated on identifying, and charging or arresting defendants suspected of committing crimes and/or civil wrongdoing and finding a court system with legal authority to bind litigants to its authority that is also cost-effective and geographically accessible. This can be enormously difficult.

Cyber society lacks all of the requisite attributes of a state as outlined in the 1933 Montevideo Convention on the Rights and Duties of States, which specifies that a bona fide country (society) must have a permanent population, a defined territory, a government, and the capacity to enter into relations with other states.

This definition implies that cyber society is not a distinct and sovereign state. Rather, it is a composite of loose associations that transcend traditional geopolitical nation-state boundaries. Jurisdiction in cyberspace is therefore contingent on the laws of individual countries that govern human activities in physical places.

International agreements about managing crime are usually very difficult to establish because nations often have very different views as to what constitutes justice.

In 1983, the Committee of Experts on Computer Related Crime of the Paris-based Organization for Economic Cooperation and Development (OEDC) became the first international group to study what could be done to prevent, control, and reduce the harmful impact of computer-enabled abuse and crime internationally[15].

The committee's report, released in 1986, specified several types of computer-enabled activities that countries should consider making illegal, such as computer-enabled fraud and forgery, unauthorized alteration of computer programs or data, interception of communications, theft of trade secrets, and computer hacking – activities that constitute Crimeware. The report also noted several barriers to international management of computer-enabled crime problems, including:

1. Lack of global consensus regarding a legal definition of criminal conduct and by extension behavior constituting computer-related crime,
2. Lack of expertise of police, prosecutors, and the courts to understand computer-enabled activities in relation to existing national laws and legal principles,
3. Inadequacy of international legal powers to investigate and access computer systems and seize intangible data needed as evidence in national criminal hearings,
4. Inconsistent bodies of national laws applicable to computer-related crime matters and for guiding, supporting, or mandating investigation of computer-related crimes, and
5. The transnational character of many computer crimes coupled with lacking extradition and mutual assistance treaties, plus the inability of existing treaties to take into account the dynamic and special requirements of computer-enabled crime investigations and prosecution.

In this report the OECD committee called attention to the world's enormous computer-enabled abuse and crime problem, made worse by limited and incongruent legal mechanisms among nations for preventing and controlling such high-tech crimes.

All these attempts to create international agreements to manage cybercrime have been more or less effective. Clearly they indicate that progress is being made toward overcoming legal barriers to investigating and prosecuting cybercrime internationally.

This clearly indicates that laws deter crime but a trusted level of computing is needed to take care of the technical details that users have less interested in.

3.3 Trusted Computing

Trusted Computing technology partially addresses this question by providing a means for end-users (and third-parties) to derive increased confidence in the platforms with which they interface, as well as providing standardized mechanisms to protect user data and information from software attack[16].

Trusted Computing technologies can be used to impede the distribution, infection and execution of crimeware applications.

Cybercrime can broadly be defined as any crime that is facilitated or committed using a computer, network, or hardware device, where the computer, network or device may be the agent of the crime, the facilitator of the crime, or the target of the crime.

Irrespective of the actual motivation for such activity, a crimeware attack, or more generally a malware attack, must typically pass through three stages to fulfill its goal. These are distribution, infection and execution.

1. Distribution: Distribution refers to the means by which malware arrives at a platform.
2. Infection: Infection is the process by which malware penetrates a platform.
3. Execution: It is during this stage that the malicious objectives of the malware are revealed. The malware may attempt to gain unauthorized access to information, capture user-entered details or steal proprietary data. This data is collated by the crimeware and transmitted back to the attacker for processing.

A Trusted System is one that will behave in a particular manner for a specific purpose. The Trusted Platform Module (TPM) specifications form the core of all Trusted Computing implementations. These specifications describe a microcontroller with cryptographic coprocessor capabilities that provides a platform with the following functionality: A number of special purpose registers for recording platform state; a means of reporting this state to remote entities; secure volatile and non-volatile memory; random number generation; a SHA-1 hashing engine; and asymmetric key generation, encryption and digital signature capabilities[16].

Trusted Computing has become synonymous with three fundamental concepts: Integrity measurement and storage, attestation, and protected storage. However, recently the definition of what constitutes Trusted Computing functionality has been revised and extended to incorporate the concepts of secure boot and software isolation.

An integrity measurement is the cryptographic digest or hash of a platform component. Platform attestation enables a TPM to reliably report information about the current state of the host platform. Attestation provides a powerful technique to combat crimeware distribution and infection. A platform, upon requesting access to a company's intranet, may be required to demonstrate through attestation that it has up-to-date anti-virus software with the latest signature definitions, that its spam filters are operating correctly and that it has installed the latest OS security patches. Similarly, a client could request that a server attests to its operating environment prior to the disclosure of sensitive data.

Protected storage functionality uses asymmetric encryption to protect the confidentiality of data on a TPM host platform. The notions of binding and sealing are of fundamental importance to Trusted Computing. Binding refers to the encryption of data with a public key for which the corresponding private key is nonmigratable from the recipient's TPM. Sealing takes binding one step further. Sealing is the process by which sensitive data can be associated with a set of integrity metrics representing a

particular platform configuration, and encrypted.

A secure boot process extends the integrity measurement and storage functionality. During a secure boot, a platform's state is reliably captured, compared against measurements indicative of a trustworthy platform state and stored. If a discrepancy is discovered between the computed measurements and the expected measurements then the platform halts the boot process.

Secure boot functionality can detect the malicious or accidental modification or removal of security-critical software at boot time. Secure boot functionality could be used to prevent a maliciously modified server from helping to distribute crimeware; this would reduce the effectiveness of a server modification attack to a denial of service. Secure boot functionality is not currently described as part of the TPM specifications. However, there is a TCG specification describing how it can be enabled on a trusted mobile platform

An isolated execution environment, independent of how it is implemented, should provide the following services to hosted software

- No interference: Ensures that the program is free from interference from entities outside its execution space.
- Trusted path: Ensures the presence of a trusted path between a program and an input device.
- Secure inter-process communication: Enables one program to communicate with another, without compromising the confidentiality and integrity of its own memory locations.
- Non-observation: Ensures that an executing process and the memory locations it is working upon are free from observation by other processes.

Hardware-enforced software isolation enables the segregation of security-critical software and data so that they cannot be observed and/or modified in an unauthorized manner by software executing in parallel execution environments. Additionally, the presence of isolated execution environments can ensure that any infection is contained within the execution environment which the crimeware has infected. In this way, user I/O data can be secured in transit to protect it from crimeware, such as keyloggers, which may have infiltrated the platform.

Trusted Computing mechanisms may also be used as a means of enhancing crimeware functionality. For example, Trusted Computing provides trivial means for crimeware to launch denial of service attacks, of various types, against a platform. If a crimeware application can be installed on a platform, thereby altering the system state, then first, access to networked services may be denied, since the platform will (correctly) not be considered trustworthy. Second access to data may be denied, since the current state of the platform will not match the integrity metrics to which the data has been sealed. Third, system startup may be suspended if the presence of crimeware is detected during the boot sequence.

Trusted Computing, as currently deployed, can do little to protect an end-user platform from crimeware attack. Trusted Computing, as it currently stands, provides a limited, but useful, set of cryptographic functionality. Problems associated with software vulnerabilities will not be ameliorated by the presence of Trusted Computing.

An abundance of information exists on the potential positive applications of Trusting Computing. However, as the technology becomes more widely deployed, it seems likely that Trusted Computing functionality will be increasingly targeted by crimeware.

Today’s users are accustomed to installing all kinds of plug-ins on their client systems, so distributing a malicious plug-in wouldn’t be particularly difficult. All an adversary would need is a good (and

reasonable-looking) cover story to have the user install the plug-in or otherwise exploit software vulnerability. Many social-engineering techniques can be used for this purpose.

A combined use of these mechanisms can greatly mitigate these attacks. As networked computing has become pervasive, the challenges of maintaining secure environments for end-user computing have increased enormously.

3.4 Secured Communication

By shrinking time and distance, the Internet has accelerated globalization, connecting people and businesses worldwide. The Web is emerging as the dominant interface for information exchange and service delivery, and e-mail is becoming the communication tool of choice. At the same time, however, there is a growing perception of the Internet as an insecure environment, and these concerns may prevent the Internet from realizing its seemingly limitless potential. The recent proliferation of malware—including viruses, worms, Trojan horses, spam, phishing schemes, distributed denial-of-service (DDoS) attacks, spyware, and adware—has made the Internet a harrowing experience for many individuals and a severe headache for organizations[17].

Ironically, what has made the Internet so successful— its open and decentralized structure—is also what sustains malicious online activity. Information on newly discovered vulnerabilities propagates quickly, and tools to launch ever more sophisticated attacks are readily accessible.

Controls implemented by Internet service providers (ISPs), which are interested in protecting their own network— and customer base—from external attacks, predominantly target inbound traffic[9]. However, there is no similar economic incentive to control outbound traffic, as the potential damage is to other networks. This lack of clear lines of accountability derives from both the decentralized nature of datagram routing in the Internet as well as its decentralized organizational structure.

What the Internet needs is an institutional structure that strongly motivates ISPs, network service providers, equipment vendors, and users themselves to control attacks at their origin as well as to maintain security on a dynamic basis. One way to accomplish this is to introduce a certification mechanism that induces service providers to voluntarily accept some degree of accountability, without interfering with the underlying decentralized protocols.

Such a mechanism could propagate incentives through the network, ensuring that distributed participants coordinate their efforts to increase security as well as reduce congestion.

To improve Internet security, it is essential that service providers control outbound as well as inbound traffic. Outbound traffic control stamps out attacks at the source and thus stops them from spreading, without subjecting the network to congestion. Outbound control is especially effective when done by ISPs, which can leverage the direct relationship with their customers to hold them accountable and take punitive action against violators.

The most effectively and efficiently way to secure the Internet is to block malware as it leaves a network. Some ISPs and e-mail providers do curtail outgoing malicious content, but the practice must be universal or nearly universal to work[17].

3.4.1 Service Provider Certification

This is a security mechanism for service providers based on the notion of a certifying authority (CA). Membership in the scheme is voluntary: Providers that choose to join pay a subscription fee to the CA and are called certified providers, while those who opt out are known as noncertified providers; traffic originating from each type is labeled similarly. The CA requires certified providers to compensate: remote providers that receive malicious traffic from the certified providers' users; and their own customers who receive malicious traffic, regardless of the source.

The CA holds any certified source provider accountable for an attack originating from its domain, regardless of whether a human customer or a zombie node initiated the attack. To minimize

compensation payments, certified providers are motivated to filter all outgoing traffic.

This scheme encourages service providers to take up an offensive, rather than a defensive, posture against intrusions and spurious traffic that exploit the Internet's distributed structure. Tying penalties to the source of malicious activity shifts the responsibility for security to the originating provider. This is particularly important for attacks that rapidly escalate by replicating and targeting multiple destinations. The certification mechanism currently applies only to service providers supplying Internet connectivity, whether to residential or enterprise customers.

The effectiveness of inbound traffic control depends on the ability to correctly identify the source of incoming packets. This proposed certification mechanism will reduce such attacks, which rely on backbone networks for transportation, by motivating access networks to implement their own outbound traffic controls.

The game-theoretic analysis is used to evaluate the viability of this incentive mechanism and to determine its implications in terms of provider actions and collective security. The game-theoretic analysis uses the concept of the Nash equilibrium to characterize the likely choice of strategies by agents. In a Nash equilibrium, each agent chooses the best response to strategies that other agents employ, implying that agents' expectations are mutually correct and that they act rationally based on these expectations.

Following standard economic theory, service providers are divided into two types, those with a low-risk security profile (A) and those with a high-risk security profile (B), with the distribution of types but not the classification of individual providers being common knowledge. A high-risk profile indicates that the provider's customer base is more prone to sending out malicious traffic, either intentionally or by having less securely configured machines.

This analysis indicates that with a nonprofit certifying authority, all service providers will choose certification, leading to a net increase in system surplus. With a profit-maximizing CA, different equilibria may exist depending on the proportion of A-type providers in the network. When this proportion exceeds a certain threshold, only A-type providers get certified, leading to a separating equilibrium. When the proportion of A-type providers is below the threshold, all providers subscribe to the certification scheme, leading to a pooling equilibrium. These are Nash equilibria, wherein each participant chooses the best response to others' actions.

In the case of a separating equilibrium, the CA has enough A-type subscribers that it can afford to exclude the B-type providers by setting high subscription fees. For B-type providers, these fees, combined with the expectation of costly penalties due to the number of A-type providers that potentially receive traffic from them, makes certification prohibitively expensive.

In the case of a pooling equilibrium, the CA sets the subscription fee low enough to induce everyone to join, the high number of subscriptions compensating for the low fee. B-type providers choose to be certified along with A-type providers because they can draw on a potentially larger pool of providers for compensation, their need for insurance is lower, and their customers stand to benefit from being able to communicate with customers of all types.

This voluntary participation-based incentive mechanism achieves the benefits of segregation through economic means, robustly supporting communications without interfering with the Internet's basic structure.

Failure to combat the growing scourge of malware could lead to real fragmentation of the Internet. Service provider certification improves overall security without undermining the fundamental design philosophy of the Internet as an open, decentralized network.

Some certification service providers, CSP assessors, and browser manufacturers have jointly defined the notion of an extended validation SSL certificate[18]. An EV-SSL certificate is a normal server certificate that meets more stringent security requirements. As such, it aims to tell more reliably

whether the certificate is valid and meaningful in a given context. It's too early to tell whether EV-SSL certificates will significantly improve the level of protection against online channel-breaking and MITM attacks. Mainly because EV-SSL certificates may replace normal certificates and inherit their shortcomings and problems in everyday life.

4. CONCLUSION

This clearly brings out the fact that computers do not commit a crime, but we (humans) do![6] Security researchers have made tremendous progress in keeping pace with Internet threats, but there are limits to what technology alone can accomplish.

To effectively mitigate crimeware both technical and social aspects must be combined to form this layered defense framework. In the first layer, end users should be more literate by expanding the computer literacy curricula in their work setting. In the second layer, we find that the Internet has obscured the question of national sovereignty and jurisdiction, but a legal system is needed to control and hence deter crime. Trusted computing that constitutes the third layer increases the confidence in the platforms with which end users interface as well as provide a standardized mechanism to protect user data and information from crimeware. Finally, the growing proliferation of crimeware is raising doubts about the Internet's future. To improve Internet security, it is essential that service providers control outbound as well as inbound traffic. This forth layer, offer a certification scheme to motivate providers to control outgoing traffic, thus efficiently increasing overall security while preserving the Internet's open, decentralized structure.

5. REFERENCES

1. **FireEye Inc.** Stopping Crimeware In Its Tracks. *Crimeware.* [Online] 2007. [Cited: October 9, 2009.] http://www.elizabethhernandezjones.com/Portfolio/WP_Crimeware01022007.pdf.

2. **Parker, Donn.** *Fighting Computer Crime: A New Framework for Protecting Information.* New York : Wiley Computer Publishing, 1998.

3. **McGraw, Gary.** *Software Security: Building Security in.* Boston : Pearson Education, Inc, 2006.

4. **McQuade, Samuel.** *Understanding and Managing Cybercrime.* Boston : Pearson Education, Inc., 2006.

5. **McAfee.** Unsecured Economies: Protecting Vital Information. [Online] 2009. http://mcafee.tekgroup.com/images/10039/unsecured_economies_report.pdf.

6. **Markus Jakobsson, Zulfikar Ramzan.** *Crimeware: Understanding New Attacks and Defenses.* Cupertino : Symantec Press, 2008.

7. **Wired.** Senate Panel: 80 Percent of Cyber Attacks Preventable. *Threat Levels: Privacy, Crime and Security Online.* [Online] November 17, 2009. http:/www.wired.com/threatlevel/2009/11/cyber-attacks-preventable/.

8. **RSA: The Security Division of EMC.** Fighting the Enemy: Making Sense of the Growing Crimeware Threat. *Security Management* . [Online] June 2007. [Cited: October 9, 2009.] http://www.techshakers.com/whitepapers/RSA/Making_Sense_of_the_Growing_Crimeware_Threat.pdf.

9. **Lee, Christopher P.** Thesis: Framework for Botnet Emulation and Analysis. [Online] December 10, 2008. [Cited: February 17, 2010.] http://smartech.gatech.edu/bitstream/1853/28191/1/lee_christopher_p_200905_phd.pdf.

10. **Bechan, Upasna.** Dissertation: Towards a Framework for Securing a Business aganist Electronic Identity Theft. [Online] November 2008. [Cited: February 17, 2010.] http://etd.unisa.ac.za/ETD-db/theses/available/etd-05052009-134757/unrestricted/dissertation.pdf.

11. **Lemley, Mark, et al.** *Software and Internet Law.* New York : Aspen Publishers, 2006.

12. **Gross, Joshua B. and Rosson, Mary Beth.** Looking for Trouble: Understanding End-User Security Management. [Online] 2007. [Cited: October 9, 2009.] http://delivery.acm.org/10.1145/1240000/1234786/a10-gross.pdf?key1=1234786&key2=0245750621&coll=GUIDE&dl=GUIDE&CFID=66374829&CFTOKEN=29450171. ACM 1-59593-635-6/07/0003.

13. **Clarkson, K.W., et al.** *West's Business Law.* Mason, OH : Thomson South-Western, 2004.

14. **Girasa, R.** *Cyberlaw: National and International Perspective.* Upper Saddle River, NJ : Prentice Hall, 2002.

15. **United Nations.** *Manual on the Prevention and Control of Computer-Related Crime.* New York : United Nations, 1997.

16. **Shane Balfe, Eimear Gallery, Chris J. Mitchell, Kenneth G. Paterson.** Crimeware and Trusted Computing. *Information Security Group.* [Online] October 1, 2007. [Cited: October 9, 2009.] http://www.isg.rhul.ac.uk/cjm/catc.pdf.

17. **Parameswaran, Manoj, Zhao, Xia and Whinston, Andrew.** Reengineering the Internet for Better Security. *IEEE Computer Society.* [Online] IEEE, January 2007. www.ieee.org.

18. **CA/Browser Forum.** Extended Validation Certificates Add Verified Identity to SSL. *CA/Browser Forum.* [Online] CA/Browser Forum, 2008. [Cited: October 9, 2009.] http://cabforum.org/index.html.