Framing the Corporate Security Problem: The Ecology of Security

Robert Joseph Skovira
Robert Morris University, Moon Twp, PA, USA

skovira@rmu.edu

Abstract

Security and information systems are intertwined. The costs of secure systems are in the billions of dollars. In the digital world, security vulnerabilities and threats work contrary to the security goals of confidentiality, integrity, and availability of information systems. The essay describes a view of organizations and their policies, network systems, operating systems, software applications, information, and people joined interactively and dependently in an environment. The paper presents an ecological conception of security.

Keywords: Security, Information security, Secure programming, Secure computing, Ecology

Introduction

Security and information systems are intertwined. The complex interactions and interconnections among people, software applications, networks, operating systems, and organizational policies create myriads of exploitable points. Daily newspapers present accounts of intrusions, stolen laptops, and other security breakdowns. The global implications of a security meltdown of apocalyptic proportions has been the guise of a novel (Brown, 1998). Intrusions and attempts at intruding are happening continuously at every moment of an information system's life. According to *Consumer Reports* (2006), in any given 24 hour period there are approximately 60 million intrusion attempts. The estimated cost of security defenses in the face of attacks is approximately $7.8 billion for 2004-2006; the costs of spamming and viruses are approximately $5.2 billion; the costs of spyware intrusions are approximately $2.6 billion. Phishing intrusions amount approximately $630 million (*Consumer Reports*, 2006). There are other estimates (Bodin, Gordon & Loeb, 2005; Kros, Foltz & Metcalf, 2004-2005). What the cost is now or will be in a year's time is anyone's guess. In the Information Age, where interconnectivity and information access and availability are paramount, malware and malicious exploitation of information system vulnerabilities have become epidemic (Seshadri, Luk, Perrig, Van Doorn, & Khosla, 2006; Whitman, 2003). Security and security awareness are necessary elements of a secure environment, even as people have access to required information and information resources. "Information security involves making information accessible to those who need the information, while maintaining integrity and confidentiality" (Carstens, McCauley-Bell, Malone, & DeMara, 2004, p. 68).

Security Vulnerabilities

In the digital world, where an individual's desk top computer is networked not only within the organization but also to the world via the WWW, it is safe to

say that everything: the computer and its operating system, the network and web site, the information on it or in corporate databases, the software used to conduct business and query the databases, and the person, is vulnerable and subject to some kind of malicious attack. “A vulnerability is a weakness…that might be exploited to cause loss or harm” (Pfleeger, 1997, p. 3).

Hardware is vulnerable to interruptions (also called “denial of service”) and interceptions (by stealing) (Pfleeger, 1997; Graff & van Wyk, 2003). The accessibility and visibility of computers (laptops are stolen), printers, even cables, and equipment (hard drives are recycled) of all kinds make them vulnerable to security breakdowns (Pfleeger, 1997; Whitman, 2003; Volonino & Robinson, 2004).

Software is open to interruptive (being deleted) threats. Software, at least in part, and its functionality can be captured and used without appropriate permissions. Software can be changed in unpermitted ways by unauthorized persons (Pfleeger, 1997; Whitman, 2003).

Information can be subject to unauthorized capture and use. Use of information can be disrupted. Unauthorized access to an information system can lead to information being inappropriately changed, even made up, or appropriated contrary to privacy laws (Pfleeger, 1997; Whitman, 2003; Volonino & Robinson, 2004).

People are especially prime points of exploitation for unpermitted access to and use of information and its system. People become opened gates for incursions into applications, operating systems, and networks (Carstens et al., 2004; Bailes & Templeton, 2006; Campbell, 2006). Information systems become vulnerable when key personnel are unavailable and are not reliable. This happens in many possible ways, but the chief manner is framed by and works through people’s mental models of trust. There is also a problem with usability designs of systems. For the user, security ought to be transparent. People will try to bypass system security whenever confronted with an accessibility choice allowed by an easy security routine as opposed to a difficult security check (Pfleeger, 1997; Howard, LeBlanc, & Viega, 2005; Mercuri, 2006).

Security Threats

Information systems and their components are threatened in at least four different ways. An information system suffers an “interruption” when a breakdown of functionality and use happens because of an unauthorized intrusion into the information system (Pfleeger, 1997; Volonino & Robinson, 2004). An “interception” occurs as the “hijacking” or “piracy” of an information system or one of its components in order to gain unauthorized rights to and use of available software applications or stored information (Pfleeger, 1997; Volonino & Robinson, 2004). A “modification” is the changing of informational content or software code without the correct permissions as a consequence of intrusions (Pfleeger, 1997; Schneier, 2000). A “fabrication” is the unpermitted change of software code or stored information as a result of an exploitative intrusion. The changes may be additive or subtractive (Pfleeger, 1997; Volonino & Robinson, 2004).

Security Goals

There are three goals which security plans and practices attempt to meet: confidentiality in the system, the system’s integrity, and the system’s continual ability to make information and other system resources available to users. Users ought to be confident about the proper use of the information system. This means that only the proper personnel are allowed to use the information system and its resources in the proper manner, namely information system access with permission (Hartman, Flinn, Beznosov, & Kawamoto, 2003). “Confidentiality” refers to the availability of system resources only to people permitted to access them. Having permission to use an information system’s resources means that the user must be authenticated—checked to see if the user is “legal”--in order to be authorized to use the system. Only authorized persons have permissions to

use the information system and its resources (Pfleeger, 1997; Thorsteinson & Ganesh, 2004; Greene, 2006). “Integrity” refers to permissions granted to users to do possible changes to software code and information in prescribed or allowed ways. Permission to modify any aspect of an information system is granted according to levels of roles of users. Integrity of a system indicates its state of ‘protection” of the information system’s resources. Integrity also refers to how “errors” are handled by a system (Pfleeger, 1997; Thorsteinson & Ganesh, 2004; Greene, 2006). “Availability” means that users have permission to retrieve and use the information system’s resources as required by roles or function in a timely fashion or convenient way (Pfleeger, 1997; Greene, 2006).

The Ecology of Security

An ecology (Davenport, 1997; Campbell, 2006) of security is a systematic approach to and view of an age-old problem of unauthorized access and use of information. Even Julius Caesar, the “Caesar Cipher,” devised and used a secure code (Thorsteinson & Ganesh, 2004). The perspective basically is a defensive stance maintained through cryptography and encryption and the placement of barriers to access, physically and logically. “Future systems will have to enforce security at multiple levels, from access control for legitimate users, to cryptographic protocols guarding against illegitimate users” (Venkatasubramanian, 2002, p. 51). In the Information Age, the approach is digital in nature, although physical procedures are still useful. The paper proposes that a security ecology consists of ecologies of security. The main components (see Figure 1 below) (the components are themselves ecologies) of ecology of security are: the organization, the networks, the operating systems, the software applications, the information, and the people involved at all these levels (ecologies). It is no surprise that the most significant (and most vulnerable or exploitable) parts of the system are the software applications and the people. Why? Because people want to do things with software, which exposed both to attackers. Being secure is understanding how the components interact and depend on each other and how these dependencies may be exploitable. The ecology of security is about being aware and forestalling exploitations.

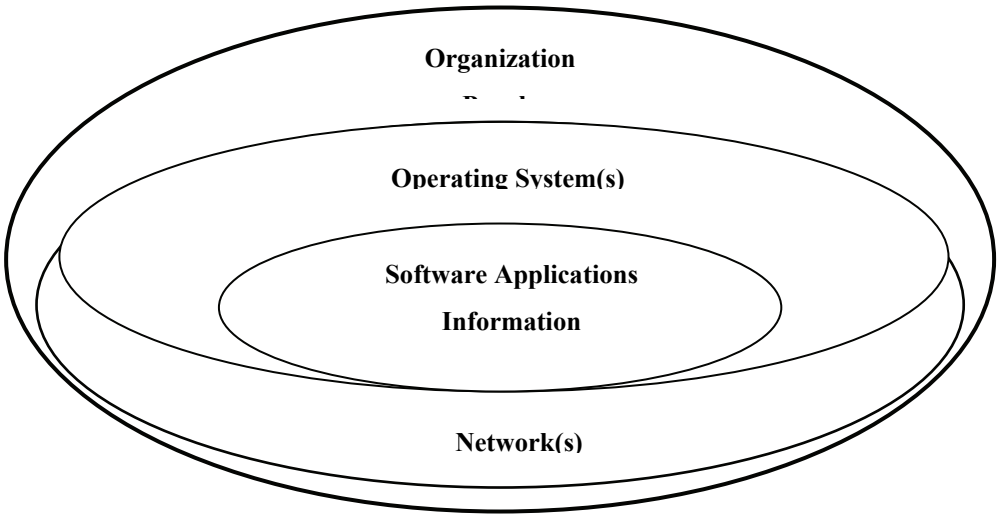

Figure 1. Ecology of Security

Organization

An ecology of security considers at the organizational level the necessary policies and procedures that frame a secure environment to protect information systems and information (Volonino &

Robinson, 2004). Security policies aim at supporting the security goals of information systems: confidentiality, integrity, and availability (Greene, 2006). Policies are instrumental in developing an understanding and awareness of kinds of security risks facing an organization.

Networks

Networks of information systems provide intraorganizational as well as interorganizational connectivity. System security is dependent upon proper user identification or authentication for permissions to be granted for access and use of information systems and information (Beaver, 2004; Thorsteinson & Ganesh, 2004). Network security is designed to manage risks at all interface levels and across all possible usages of information systems of an organization (Pfleeger, 1997; Hartman et al., 2003).

Operating Systems

Operating systems may be the most important component of a security ecology because of their intermediary position between applications, information, and networks; there is more dependence on operating systems than meets the eye (Greene, 2006; Pfleeger, 1997). An operating system deals with user identification, memory protection, input and output management, and access management which are salient exploitable features of an information system (Pfleeger, 1997).

Information

Information, its access, retrieval, and use, depends upon users trusting that it has not been compromised. Informational resources are to be managed according to their level of sensitivity, importance, and organizational use (Greene, 2006). Because of its importance, information ought to be protected through access and permission management (Howard, LeBlanc, & Viega, 2005).

Software Applications

Software applications are also a component of an ecology of security. Writing secure code begins with the design stage of program development (Graff & van Wyk, 2003; Greene, 2006; Lindner, 2006). “Software security…needs to be considered from the very beginning of the software development cycle” (Wang & Wang, 2003, p. 75). Insecurity of code increases as the applications, even when built using trusted, well-designed modules, become compositionally complex (Neumann, 2006). The “composition effect” shows up when programs and segments are reused to create a new system (Graff & van Wyk, 2003, p. 18).

People

People are the final component of a security ecology. People’s habits of information system usage often are the main culprits in compromising security measures and exposing information systems to threats. People pose security problems either because of ignorance or a desire to do wrong (Graff & van Wyk, 2003; Beaver, 2004; Battaglia, 2006; Campbell, 2006).

Problems of a Security Ecology

Technical factors

Every corporate ecology of security consists of components which are themselves security ecologies. One set of factors concern various technical aspects of the information systems, networks, operating systems, applications, and information. These are technical issues that deal with the complexities associated with the interactivity and dependencies of organizational systems. As a result of interconnectivity and task complexity, a typical database application relies on normal-

ized data for efficient retrieval but it also is dependent upon an operating system to handle some of the required functionality. It relies also on networks to share the information either within organizational arenas or across organizational boundaries. The situation is most complex and fraught with exploitable flaws. Complex systems are a response to complex tasks. The more complex the interaction of information systems the more possible security gaps exist (Graff & van Wyk, 2003; Neumann, 2006).

Psychological factors

Another group of factors are psychological in nature. The issue here is the "mental models' or the habitual and unconscious ways of thinking about and creating the code of the complex interacting system. Project managers, software designers, and software programmers become mired in their customary ways which are conceptual blind stops (Graff & van Wyk, 2003). Mental models are habits of doing, seeing, hearing, etc. they are metaphors-in-use. They show up as styles of action and decision making. An important mental model for security concerns is a user's "trust model" (Schneier, 2000; Kim & Ahn, 2006, Kruck & Kruck, 2006). This is the basis for social engineering intrusions because a trusting person acts upon the "…perceived benevolence and integrity of a participating party…" (Kim & Ahn, 2006, p. 85).

Corporate Worldview factors

Another collection of factors is the corporate worldview. This perspective frames the enterprise affecting social, and financial situations and goals. This is a perspective about results-driven activities and financially-driven situations which raises issues about security costs and benefits difficult to overcome. The results-driven approach deals with activities which are deadline-driven. The financially-driven view is cost-driven (rather than benefit-driven) (Graff & van Wyk, 2003; Volonino & Robinson, 2004).

Organization(s) as a Security Ecology

The environment of security measures at the corporate level is important. The most vulnerable are people and their habitual activities. Policies are components of this ecology. Policies are important benchmarking documents for compliance checking (Greene, 2006).

Exploitative techniques are more common at this level against personnel. This is call "social engineering" by some (Beaver, 2004). It is a "con game" played to dupe unsuspecting victims into giving up essential information that exposes flaws in the outer ring of corporate security defenses.

At the corporate level, use of information systems and information access are necessary to daily business. Users are identified as legitimate and given permission to access information systems. Such permissions are limited in terms of user roles or user group memberships.

Network(s) as a Security Ecology

Networks, both within and between organizations, are ways of sharing afforded information resources. As such they are more exploitable situations of information use (Graff & van Wyk, 2003; Carstens et al., 2004). Because networks are complex affairs, stretching out into cyberspace, either wired or, increasingly, wireless, the boundaries of the networks are virtually unknowable. Networks provide multiple attack points. Attackers attach, especially with wireless implementations, from almost anywhere (Beaver, 2004, Howard, LeBlanc, & Viega, 2005). There are multiple unknown paths for breeching corporate security defenses. Attackers "ride the rails" in anonymity into the "sleepy village" of the corporation.

Operating System(s) as a Security Ecology

The security ecology of operating systems, a component of any corporate ecology of security, is a very exploitable arena for attackers. Operating systems, in a symbiotic relationship with application systems and information storage devices, are responsible for protecting the shared corporate resources, file and database access, and input and output functionality (Erickson, 2003; Graff & van Wyk, 2003). Operating systems are protectors of computer memory, a prime exploitable aspect of information systems. As a consequence of their role in security, they are responsible for the authentication of the identities of users (Howard, LeBlanc, & Viega, 2005).

Software Applications as a Security Ecology

Software applications create a security environment nightmare (Erickson, 2003; Kalinovsky, 2004). Being complex, task-oriented systems, they are corporate workhorses. Applications are designed to be reliable and usable within the security ecologies of networks and operating systems upon which they depend for much of the user interfaces and functionality. The designers and programmers should do their work with an acute awareness of the possible security flaws inherent in complex environments of networks and operating systems (Graff & van Wyk, 2003). As a result, software applications ought to be designed and tested to requirements and nothing more (or less). The writing of insecure code gives rise to all kinds of possible intrusions (Howard, LeBlanc, & Viega, 2005). Secure software code is about affording actionable use and access to other vulnerable ecologies: networks, operating systems, and information resources (Stiegler, Karp, Yee, Close, & Miller, 2006). “Frankly, it doesn’t matter what operating system or programming language you use, and it doesn’t matter how secure the underlying platform is. If your code is insecure, your customers could be open to attack” (Howard, LeBlanc, & Viega, 2005, p. xxi). While it is difficult, and some would say impossible, to write secure code, the golden rule is that software code should not do more than required. A corollary might be that permitted use and access be no more than required (Stiegler et al., 2006).

Information as a Security Ecology

Information resources, as a component of a corporate ecology of security, are a security ecology of prime importance. Policies ought to be in place that identify and document the information resources (Greene, 2006). In this ecological environment, various laws (HIPPA, Buckley amendment, etc) mandate who deals with and handles information, who has access, where and how it is stored, and even displayed and used. Privacy is a major concern (Strickland & Hunt, 2005). Cryptography and encryption become defensive weapons providing protection for informational privacy (Thorsteinson & Ganesh, 2004; Muller, 2006). While information resources are to be available as required, and accessible, the information attributes of timeliness, validity and reliability must be protected against exploitations aimed at modifying or fabricating (Carstens et al., 2004; Howard, LeBlanc, & Viega, 2005).

People as a Security Ecology

The corporate ecology of security component of people is also a security environment. This component usually gets “no respect.” People are the most vulnerable to exploitation, being readily and easily “conned” by a hacker (who plays a “confidence” game) (Mercuri, 2006). A popular “game” is an email from a bank saying that your bank account security has been violated and to rectify simply click on the provided link. This is called “social engineering.” “Social engineering is ‘people hacking’ and involves maliciously exploiting the trusting nature of human beings for information that can be used for personal gain” (Beaver, 2004, p. 55). Users of information systems are vulnerable too. Content manipulation is another “game” which manipulates meanings

(and information use) people attach to content (Schneier, 2000). These are the users of the information systems and resources whose access is via such things as passwords. The usability of information systems affects individuals' responses to security measures. User identification and permissions-to-use are important aspects of this security ecology (Howard, LeBlanc, & Viega, 2005). While the mental models or mind sets of software designers and programmers are important to note, the mental models and attitudes of users have an effect, in some ways hazardous, on the security environment (Graff & van Wyk, 2003).

Conclusion

A corporate ecology of security consists of the security ecologies of the organization, the networks in place, the operating systems used, the software applications used, the information resources, and the people. Each security ecology contributes a defensive measure to the overall security environment. There are some final points about a corporate ecology of security. Security flaws are everywhere. The complexity of systems and tasks create unintentional and inherent exploitable points. Good design is the best security. Doing well-designed software or even policies promulgates an awareness of security. Good mental models and habits of use reflect an awareness of exploitable flaws and corporate and personal responses. No application is secure even if designed to the highest levels of quality.

References

Bailes, J. E. & Templeton, G. F. (2004). Managing P2P security. *Communications of the ACM, 47*(9), 95-98.

Battaglia, J. (2005). Techno-exegesis. *2600 The Hacker Quarterly, 23*(3), 49-50.

Beaver, K. (2004). *Hacking for dummies*. Indianapolis, IN: Wiley Publishing.

Bodin, L. D., Gordon, L. A. & Loeb, M. P. (2005). Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM, 48*(2), 79-83.

Brown, D. (1998). *Digital fortress*. New York: St. Martin's Press.

Campbell, S. (2006). How to think about security failures. *Communications of the ACM, 49*(1), 37-39.

Carstens, D. S., McCauley-Bell, P. R., Malone, L. C., & DeMara, R. F. (2004). Evaluation of the human impact of password authentication practices on information security. *Informing Science Journal, 7*, 67-84. Available at http://inform.nu/Articles/Vol7/v7p067-085-229.pdf

Cyberinsecurity. (2006). *Consumer Reports, 71*(9), 20-29.

Davenport, T. H. (Prusak, L.). (1997). *Information ecology: Mastering the information and knowledge environment*. New York & Oxford: Oxford University Press.

Erickson, J. (2003). *Hacking: The art of exploitation*. San Francisco: No Starch Press.

Graff, M. G. & van Wyk, K. R. (2003). *Secure coding*. Sebastopol, CA: O'Reilly.

Greene, S. S. (2006). *Security policies and procedures: Principles and practices*. Upper Saddle River, NJ: Pearson Prentice Hall.

Hartman, B., Flinn, D. J., Beznosov, K., & Kawamoto, S. (2003). *Mastering web services security*. Indianapolis, IN: Wiley.

Howard, M., LeBlanc, D., & Viega, J. (2005). *19 deadly sins of software security: Programming flaws and how to fix them*. New York: McGraw-Hill/Osborne.

Kalinovsky, A. (2004). *Covert Java™: Techniques for decompiling, patching, and reverse engineering*. Indianapolis, IN: Sams Publishing.

Kim, M. & Ahn, J. (2006, Fall). Comparison of trust sources of an online market-maker in the e-marketplace: Buyer's and seller's perspectives. *Journal of Computer Information Systems, XLVII*(1), 84-94.

Kros, J. R., Foltz, C. B., & Metcalf, C. L. (2004-2005 Winter). Assessing and quantifying the loss of network intrusion. *Journal of Computer Information Systems, XLV* (2), 36-43.

Kruck, G. P. & Kruck, S. E. (2006, Fall). Spoofing – a look at an evolving threat. *Journal of Computer Information Systems, XLVII*(1), 95-100.

Lee, J. K., Upadhyaya, S. J., Rao, H. R., & Sharmon, R. (2005). Secure knowledge management and the semantic web. *Communications of the ACM, 44* (12), 48-54.

Lindner, F. (2006). Software security is software reliability. *Communications of the ACM, 49*(6), 57-61.

Mercuri, R. T. (2006). Scoping identity theft. *Communications of the ACM, 49*(5), 17-21.

Muller, G. (2006). Privacy and security in highly dynamic systems. *Communications of the ACM, 49*(9), 28-31.

Neumann, P. G. (2006). Risks relating to system compositions. *Communications of the ACM, 49*(7), 128.

Pfleeger, C. P. (1997). *Security in computing* (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Schneier, B. (2000). Semantic network attacks. *Communications of the ACM, 43*(12), 168.

Seshadri, A., Luk, M., Perrig, A., Van Doorn, L. & Klosla, P. (2006). Externally verifiable code execution. *Communications of the ACM, 49*(9), 45-49.

Stiegler, M., Karp, A. H., Yee, K. Close, T., & Miller, M. S. (2006, Sept). Polaris: Virus-safe computing for Windows XP. *Communications of the ACM 49*(9), 83-88.

Strickland, L. S. & Hunt, L. E. (2005, February 1). Technology, security, and individual privacy; New tools, new threats, and new public perceptions. *Journal of the American Society for Information Science and Technology, 56* (3), 221-234.

Thorsteinson, P. & Ganesh, G. G. A. (2004). .*NET security and cryptography*. Upper Saddle River, NJ: Prentice Hall PTR.

Venkatasubramanian, N. (2002). Safe 'composability' of middleware sources. *Communications of the ACM, 45*(6), 49-52).

Volonino, L. & Robinson, S. R. (2004). *Principles and practice of information security*. Upper Saddle River, NJ: Pearson Prentice Hall.

Wang, H. & Wang, C. (2003). Taxonomy of security considerations and software quality. *Communications of the ACM, 46*(5), 75-78.

Whitman, M. E. (2003). Enemy at the gates: Threats to information security. *Communications of the ACM, 46*(8), 91-95.

Biography

Robert Joseph Skovira is a Professor of Computer Information Systems in the Department of Computer and Information Systems, School of Communications and Information Systems, at Robert Morris University, Pittsburgh PA USA. He teaches undergraduate and graduate (MS) courses including Java Programming, Secure Programming, Knowledge Management, Global, Economic, Social, and Ethical Issues of Computing, Decision Support Systems, Information Design, and Ethical and Legal Issues of Technology. In the Doctor of Science program he teaches Ethnography of Information Systems. He was a visiting professor at Comenius University, Bratislava, Slovakia, in 1997 and 2006. Dr. Skovira's research interests include information and information system use within organizations (politics of information, information system bias, secure programming), cultural and moral frameworks, decision making and knowledge mapping, and information design and thinking visually.