Chapter XXIX
Cyber War Defense:
Systems Development with Integrated Security

Murray E. Jennex
San Diego State University, USA

ABSTRACT

Cyber war is real and is being waged. Cyber terrorists and cyber warriors are attacking systems, but fortunately, they are attacking systems in much the same way hackers attack systems. This is good for system security designers as the security controls installed to protect against hacking will work to protect against cyber terrorists and warriors. However, while there are several tools that can be used to identify security requirements including checklists, threat and risk analysis, and security policies, these methods are not integrated into an overall design methodology that can be used to ensure that security requirements are identified and then implemented. This chapter proposes using barrier analysis and the concept of defense in depth to modify Siponen and Baskerville's (2001) integrated design paradigm that is more graphical and easier to understand and use methodology that is expected to improve security to be built into systems and improve defenses against cyber warfare.

INTRODUCTION

Cyber terrorists and cyber warriors attack systems much the same way as hackers and über hackers (the best hackers) attack systems. This is good for system security designers as the same protections used to defend against hacking will work against cyber terrorists/warriors. However, while there are numerous modeling methods and design methodologies for aiding system analysts in identifying information systems (IS) user requirements, the tools that can be used to identify security requirements are not integrated into an overall design methodology that can be used to ensure that security requirements are identified and then implemented when building a system or application. The result is that oftentimes systems and applications are built to meet end-user needs and then security is added or "bolted on" as an afterthought. Alternately, many system analysts/designers do not consider it their job to include security in the design of a system or

application, leaving or trusting security to the network technicians. This leads to an over reliance on firewalls and antivirus as the foundation of security with little use of robust programming, administrative controls, interface and database design, and back up and recovery to enhance security. Siponen and Baskerville (2001) attempted to resolve this by proposing a security design paradigm that relied on metanotation to abstract and document integrated security requirements into IS development methods. However, this paradigm has not been widely adopted.

This chapter proposes using barrier analysis and a defense-in-depth approach to modify Siponen and Baskerville's (2001) and Lee, Lee, and Lee's (2002) integrated design methodologies that are more graphical and easier to understand and use methodology. In addition to the metanotation proposed by Siponen and Baskerville (2001), this chapter proposes the use of barrier diagrams in conjunction with barrier analysis to provide a visual and integrative approach to adding security into systems analysis and design, and to ensure that adequate levels or layers of security are in place at all stages of the software development life cycle (SDLC). Barrier analysis is a concept developed by Haddon, Jr. (1973). Barrier analysis is most widely known in the nuclear energy arena and has been improved upon by the System Safety Development Center, a training division of the Department of Energy (Clemens, 2002). Barrier analysis is a method of identifying hazards or threats, and determining the effectiveness of the preventative/mitigating factors that are constructed to prevent the occurrence of the hazard/threat. Barrier analysis also can be used after an event has occurred to determine the root cause and to help develop barriers to prevent repeat occurrences (Crowe, 1990).

To document the validity and usefulness of the proposed methodology, barrier analysis and defense in depth was tested by a group of graduate students as part of their systems design project. The goal was to determine if the concept of barrier analysis and barrier diagrams could be effectively used in IS design, and whether or not this methodology was useful in discovering and implementing security requirements. The pilot study was done to determine if further studies and research should be performed to demonstrate that this is a useful methodology that should be adopted as an industry standard practice for ensuring that security requirements are thoroughly discovered, documented, followed, and tracked throughout the systems development life cycle.

BACKGROUND

Information and systems security is a continuing problem. According to a survey performed by the Computer Security Institute (CSI) and the FBI, more than 50% of respondents of large corporations and U.S. government agencies reported security breaches during 2004, with reported financial losses due to these violations of more $141 billion (Computer Security Institute (CSI), 2005). The losses included lost revenue and costs relating to clean up, data loss, liability issues, and, most importantly, loss of customer trust (Allen, Mikoaki, Jr., Nixon, & Skillman, 2002). While this is a declining trend seen since 2001, these figures coupled with the research finding from Jennex and Walters (2003) that current hacking tools require decreased intruder technical knowledge to effectively hack/penetrate security, suggests that there are greater numbers of potential hackers (Allen et al., 2002). It also suggests that despite the overwhelming efforts made on the part of organizations by means of security policies, practices, risk management, technology, security architecture, and design, security for information and systems is still a serious concern.

IS Security Design Paradigms

There are two main paradigms for designing security solutions in IS as defined by Baskerville (1993). The mainstream paradigm is based on the use of checklists, while the integrative paradigm uses engineering processes or logical abstractions and transformational models to combine viewpoints and functions into a single security model. These paradigms are discussed further.