Chapter XIX
Security Considerations in the Development Life Cycle

Kenneth J. Knapp
U.S.A.F. Academy, USA

ABSTRACT

To promote the development of inherently secure software, this chapter describes various strategies and techniques for integrating security requirements into the systems development life cycle (SDLC). For each major phase of the SDLC, recommendations are made to promote the development of secure information systems. In brief, developers should identify risks, document initial requirements early, and stress the importance of security during each phase of the SDLC. Security concerns are then offered for less traditional models of systems analysis and development. Before concluding, future trends are discussed. Practitioners who read this chapter will be better equipped to improve their methodological processes by addressing security requirements in their development efforts.

INTRODUCTION

A perception exists among some information system (IS) security professionals that systems developers generally do not consider security as an integral part of the development process. Instead, a perception exists that developers often treat security more as an afterthought. Considering today's high-threat cyber environment, it is essential that security requirements remain a priority throughout the systems development life cycle (SDLC). In this paper, a description of SDLC strategies and techniques is provided to promote the development of secure systems. The key to integrating security into the SDLC is by documenting security requirements early and making security considerations a priority during each phase of development. Practitioners who read this chapter will be equipped to improve their methodological processes by including security requirements in their development efforts.

BACKGROUND

The motivation to write this chapter initiated from a previous study that involved a set of interviews the author conducted with certified information security professions between 2004 and 2006. In 2004, the author conducted e-mail interviews with over 200 certified information systems security professionals (CISSP) located in over 20 countries worldwide. The interviews discussed what each participant felt were the most critical information security issues facing organizations today. A recurring perception among the participants was that security concerns are not a high priority among many system developers. One typical response stated, "It seems that unless the project is a security initiative, the involvement of a security resource to identify control requirements is an afterthought. By the time the security resource is formally involved, the project is so far ahead that insisting on changes to accommodate [security] controls is often viewed as a source of threat to the project's timelines." Another expressed frustration by stating, "Vendors are under constant pressure to meet their figures [deadlines], thus delivering the product with sacrifices in security and quality. The end customer assumes the risk when this software is delivered into the market space. This is a great concern these days and will continue to be a major security concern even 10 years from now." Another interviewee said, "Late security planning is (often) started well into the implementation phase of a project's SDLC. A current large organization is deploying a…management enterprise tool. This project has been in engineering and deployment for over a year and they are just now beginning to supply security."[1]

In 2006, the author conducted an interview with a certified information security professional with over 20 years of IT experience working for both government and Fortune 100 employers. The interviewee indicated that his own company recently cut security engineers by 50% in an effort to save costs and that top management typically does not place much priority on security unless they can be convinced that security requirements effect the financial bottom-line. Yet, demonstrating how security can bring about direct financial benefits or improve return on investment can be challenging for security professionals. Many find it difficult to quantify security in financial terms and stumble over simple questions asked by top managers, such as, "What am I getting for my security dollars?" One study found that U.S. companies spent only an average of .047% of their revenue on security (Geer, Hoo, & Jaquity, 2003). The difficulty of quantifying security benefits in financial terms that top management can appreciate is partially to blame for these low budgets.

One of the reasons that security is perceived as a development afterthought is that modern software systems often contain serious security flaws and require frequent patch updates. Yet, evidence suggests that by focusing on building security into software during development, money can be saved by minimizing the number of flaws that require patch updates. A 1981 IBM Systems Sciences Institute study reported that the cost to fix an error found after product release can be 100 times more costly than one identified during the design phase (Geer, 2002). For security defects, late fixes often cost more because in addition to having to remediate the flaw, successful exploits may lead to data theft, sabotage, or other cyber-related attacks (Berg, 2006). Security professionals should keep these facts in mind when asked by top management, "What am I getting for my security dollars?"

To promote the development of inherently secure software, this chapter describes various strategies and techniques of integrating security requirements into the SDLC. Secure software does not happen by itself, it requires process improvement and commitment from the development team and from management. The processes discussed in this chapter do not require the creation of a separate development process; instead, the processes can be integrated into an organization's existing methodology.

SECURITY CONSIDERATIONS IN THE SYSTEM DEVELOPMENT LIFE CYCLE

This section describes important security considerations for the major phases in a representative