Performing Security Analyses of Information Systems

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

One of the textbooks that I chose for seminar five of Norwich University's graduate program in information assurance is _Performing Security Analyses of Information Systems_ by Charles L. Smith, Sr, PhD, CISSP [1]. Seminar 5 is entitled, “Detection & Response” and covers the following areas:

* Vulnerability assessment and intrusion detection systems
* Monitoring and control systems
* Applications controls
* Honeypots
* Computer emergency quick-response teams
* Data backup and recovery
* Business continuity planning
* Disaster recovery
* Forensics, and
* Insurance relief.

In addition to these interesting topics, I assigned a long-term reading project for the 11 weeks of the seminar: Dr. Smith’s excellent manual. The students read one or two chapters of this 500 page text every week and apply what they learn to their weekly field exercises (our students have to interview their colleagues and analyze aspects of security in their own place of employment throughout their program).

Dr. Smith's book begins with a fine review of basic principles of information security and of the information processing infrastructure in Chapter 1.

Chapter 2, "An Overview of Security Analysis," is a short review of threats, vulnerabilities, countermeasures, working with users, and related topics.

Chapter 3 looks at network security policies with special attention to US government requirements.

Chapter 4 is "A Comprehensive Security Analysis Process" which includes the following elements (explained in detail):
* Formulate a security policy
* Formulate a security rules base
* Formulate the security requirements
* Perform a risk assessment
* Develop a security architecture
* Develop and overall architecture
* Develop a migration plan
* Implement the migration plan steps, and
* Perform a security test and evaluation.

Chapter 5, "Security Architectures," looks at security considerations for the Web, voice and data networks and client/server systems.

Chapter 6, "Risk Assessment," is the longest part of the book at almost 100 pages. The chapter is packed with useful information presented in tables, equations, figures and clearly written text.

Chapter 7 looks at countermeasures and reviews communications protocols, distributed denial-of-service attacks, and methods for selecting among countermeasures.

Chapter 8, "Migration Process," focuses on how to implement change in production systems without causing more disruption than we are trying to prevent.

Chapter 9, "Security Test and Evaluation," briefly examines how to manage testing in four phases:
* Test planning
* Test operations and data collection
* Test analysis and evaluation, and
* Reporting of test results.

Chapter 10 concludes the text with a summary of recommendations. It is followed by
* A 90 page glossary
* A 20 page list of acronyms and abbreviations
* A sample questionnaire for system assets and values
* A sample security policy, and

* Several other useful tables.

The author provides extensive references for further reading at the end of every chapter.

My only complaints about the book are relatively trivial:

* I wish the author had not used justified text in tables (there are often big gaps between words in the short lines);

* The index is a bit skimpy for such a densely-packed book;

* I would have liked to see at least a brief review of the six fundamental attributes of information that we protect as defined in the Parkerian Hexad (confidentiality, control or possession, integrity, authenticity, availability and utility)[2].

I hope that readers will take advantage of this extraordinary value: at $6 for an electronic version and $20 for a paper version you can't afford to pass it up.

***


[2] For an explanation of the Parkerian Hexad, see <http://www.techweb.com/encyclopedia/defineterm?term=Parkerian+Hexad&Define.x=24&Define.y=14>:
For a book that discusses Donn Parker’s ideas in detail, see

***

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without
limit on any Web site, and to republish it in any way they see fit.