Preparing for the CISSP Exam (2)

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

In my last column, I began responding to a former student recently wrote to me with a request for suggestions on what to read in preparing for the CISSP exam. In this second article, I review some valuable Web sites for such preparation.

* * *

The National Institute of Standards and Technology Information Technology Laboratory Computer Security Division’s Computer Security Resource Center (I guess that would be the NIST ITL CSD CSRC – whew!) has a several good resources for CISSP review.

First, the NIST Special Publications (SP) page <http://csrc.nist.gov/publications/nistpubs/index.html> has a wealth of valuable papers for anyone interested in reviewing and extending security knowledge – especially security-management knowledge. I have reviewed many of these documents in this column will be reviewing new ones in upcoming columns.

A related page is the NIST ITL CSD CSRC Draft Publications list <http://csrc.nist.gov/publications/drafts.html> which offers even more recent documents plus the opportunity for CISSP-preparers to apply their analytical skills to improving proposed documents. Some of the drafts are also linked from the previously-mentioned SP page, but on the draft page each is described in a one-paragraph summary that includes the deadlines for comments.

Even if CISSP candidates are not currently working in the US federal government, they would do well to read many of the Federal Information Processing Standards (FIPS) available from the NIST ITL CSD CSRC <http://csrc.nist.gov/publications/fips/index.html>. In particular, I draw your attention to the more recent documents such as

- 2001-05 FIPS 140-2 Security requirements for Cryptographic Modules
- 2006-03 FIPS 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors
- 2001-11 FIPS 197 Advanced Encryption Standard
- 2002-03 FIPS 198 The Keyed-Hash Message Authentication Code (HMAC)
- 2002-08 FIPS 180-2 August 2002, Secure Hash Standard (SHS)
- 2004-02 FIPS 199 Standards for Security Categorization of Federal Information and Information Systems

A collection of interesting white papers on security-related topics is maintained by Entrust <http://www.entrust.com/resources/whitepapers.cfm>. At latest count, there are 110 papers freely
available from that source (some of them in German) without having to sign up for anything. Some of the ones I recommend:

- AITE Online Banking Security: FFIEC Deployment Experiences
- An Introduction to Cryptography and Digital Signatures v2.0
- Authentication: The Cornerstone of Secure Identity Management
- Best Practices for Choosing a Content Control Solution
- Common Criteria Evaluation
- Countering On-Line Identity Theft: New Tools to help Battle Identity Theft on the Internet
- Did security go out the door with your mobile workforce?
- Enhanced Online Banking Security - Behavioral Multi-Factor Authentication
- Entrust Internet Security Survey - European Survey Overview and Report Methodology
- GIGA Report: Total Economic Impact of Entrust TruePass and Token-based Authentication
- Information Security Governance: Toward a Framework for Action (BSA white paper)
- Myths and Realities in Content Control for Compliance
- Protecting Information on Laptops and Mobile Devices
- Quantum Computing and Quantum Cryptography
- Security In A Web Services World
- Trends in Outbound Content Control: A White Paper by Ferris Research
- Trusted Public-Key Infrastructures
- Understanding Secure Sockets Layer (SSL): A Fundamental Requirement For Internet Transactions
- Using a PKI Based Upon Elliptic Curve Cryptography
- Web Portal Security Solution
- Web-Services Security Quality of Protection.

More resources in my next newsletter.

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msia.norwich.edu> at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 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.