Proceedings of the 16th Colloquium for Information Systems Security Education
Lake Buena Vista, Florida June 11 - 13, 2012

Certifying a Textbook Under NSTISSI 4011

Richard E. Smith, *Senior Member, ACM and IEEE*

Abstract – In early 2012 the Information Assurance Courseware Evaluation (IACE) program certified a textbook as conforming with the training standard for information security professionals. The textbook was specifically developed to cover the training standard's requirements with the sole prerequisite of a basic computing course. This posed a series of challenges. The curriculum standard, published in 1994, does not attempt to outline an effective course of study and it is out of date in many ways. Some required topics are unlikely to appear in introductory or second-year courses. Moreover, the standard requires several technical topics whose details were previously classified and thus are poorly covered in the general literature. The textbook presents the material incrementally, building upon successively more complex computing environments. To address problems with the training standard, the textbook incorporates requirements from a more recent industry standard, provides tutorials to fill in missing prerequisites, and uses material from declassified documents to cover formerly classified topics.

Index terms – IACE, NSTISSI 4011, Textbook

I. Introduction

In 2005, the author developed and taught an undergraduate course in information security at the University of St. Thomas, St. Paul, MN. The course was intended to provide both a broad view of security and an understanding of its technical underpinnings. Very few of the department's majors had completed courses in computer organization, operating systems, and networking. This made it difficult to use an existing textbook, because appropriate books were often geared to graduate programs or to advanced undergraduates. The course was ultimately taught using professional books instead of textbooks.

The dean of the college recognized that information security was a growing field and directed the Computer and Information Sciences department to develop an information security curriculum. The department developed a curriculum designed to fulfill certification requirements for the Information Assurance Courseware Evaluation (IACE) program. This required additional courses for which no college textbooks existed. The curriculum also included an introductory course directed at first- or second-year students who had completed at least one introductory computing course.

The curriculum targeted the "National training standard for information security (INFOSEC) professionals" [1], since this best described the training objective. The standard was published in 1994 by the National Security Telecommunications and Information Systems Security Committee (NSTISSC), now called the Committee for National Security Systems (CNSS). The training standard is a "National Security Telecommunications and Information Systems Security Instruction" (NSTISSI) and commonly known by its publication number: NSTISSI 4011.

In 2007, the author developed a proposal for an introductory textbook in computer security. The book would include selected advanced topics so that it covered everything in the NSTISSI 4011 training requirements. Students could then use the book as a text in an introductory course and as a reference in one or more advanced courses that would together cover the U.S. government training requirement. The proposal was accepted by Jones & Bartlett Learning, and the textbook was completed in late 2011. The IACE program reviewed the textbook against the NSTISSI 4011 standard in 2012 and has certified that it fully covers that standard.

This paper reviews the process of developing the textbook and the issues that arose. The textbook's development process addressed the principal challenge of covering the required curriculum topics. The obsolescence of the curriculum standard was addressed as part of the development process by incorporating an additional, up-to-date curriculum recommendation. The lack of student prerequisites was solved by providing tutorial material to cover the essential technical topics. The problem of covering formerly classified information was addressed by using declassified documents and published government policies and standards as sources.

Richard E. Smith, PhD, CISSP, is President of Elementary Information Security LLC, Hastings, MN, email: rs@einsec.com

ISBN 1-933510-95-1/$15.00

II. The Development Process

Textbook development began with a list of topics required by NSTISSI 4011 and a general plan for the progression of topics. The progression is "geographical" in that it starts with a single computer and user, and expand to multiple users and to networks of multiple users. Here is the progression:

- Single desktop computer running one or more separate processes
- Computer with two or more users sharing files
- Authentication and cryptography, first with files and then with volumes
- Local networking
- Internet technology
- Enterprise computing
- Email and web applications
- U.S. Government security topics and concepts

Many requirements in NSTISSI 4011 expect students to examine government policies that are specific to the student's "agency." The IACE program recognizes that most students will be training for work in nongovernmental environments, and interprets "agency" to apply to any organization or enterprise. This allows most materials to be presented to a general audience, instead of focusing on government-specific policies. Topics that apply exclusively to government security environments appear in the book's final chapter.

NSTISSI 4011 requires coverage of system life cycle management. Today, this often involves a continuous improvement process, often built atop a requirements-driven development process. The textbook incorporates a simple six-phase security process that it uses in examples throughout the book. The process is both requirements-based and cyclical, to yield continuous improvement.

The textbook itself followed a similar process in its own development. The process consisted of the following steps:

1. Produce a list of topics required by the curriculum standard.
2. Assign topics to chapters.
3. Write chapters.
4. Review chapters for accuracy, coverage, readability, and size.
5. Make corrections, reorganize chapters, and/or add material to address errors and omissions.

As in iterative and continuous improvement processes, the steps repeated until all requirements were met. Variations in the projected and actual number of chapters reflect this process. The original book proposal was developed using the list of required topics entered into an *outliner*: a program that allowed hierarchical sets of headings and subheadings to be moved and manipulated in a tree structure. This made it simple to arrange sets of topics, assess the order, and rearrange to achieve the best result. This yielded working plan for the textbook and a starting point to estimate the writing requirements.

The textbook strives to use up-to-date terms and concepts. This yields apparent conflicts with NSTISSI topic requirements, since most requirements are presented using 1994-era terminology. It could even be misleading in some cases to use a now-obsolete term with a contemporary form of the same concept. To avoid misleading students while still meeting the letter and spirit of the published standard, the book includes an appendix that explains how several evolving terms and topics are covered.

A. Chapter Mapping

Most of the textbook's 17 chapters fall into three general categories:

- Access control: 4 chapters, including one on disk and file system structure
- Cryptography: 5 chapters, including one on authentication and another on network cryptography
- Networking: 6 chapters, including the one on network cryptography

Some chapters essentially stand on their own. The first chapter introduces information security and continuous process improvement, and leads students through a simple risk assessment process. A later chapter introduces enterprise security, including background information about enterprise structure and how it affects security. The final chapter, of course, focuses on U.S. government policies and technologies.

The following list summarizes the topics covered by each chapter. This illustrates how the contents map to NSTISSI 4011. The complete mapping is available online along with a description of the process [2].

ISBN 1-933510-95-1/$15.00

- Chapter 1 - Security From the Ground Up
  Basics of the security process and simple risk assessment
- Chapter 2 - Controlling a Computer
  Basics of hardware, software, memory, process protections, and of using security policies
- Chapter 3 - Controlling Files
  Basics of file protection
- Chapter 4 - Sharing Files
  Policy and implementation of file sharing and ACLs; basics of event logging and auditing
- Chapter 5 - Storing Files
  Forensics, disk drives, file systems, and file recovery
- Chapter 6 - Authenticating People
  Three authentication factors, examples of each, and the use of basic cryptographic building blocks to implement authentication
- Chapter 7 - Encrypting Files
  Basics of file encryption using stream ciphers
- Chapter 8 - Secret and Public Keys
  Key management using secret keys and public keys, and the use of digital signatures and certificates
- Chapter 9 - Encrypting Volumes
  Block ciphers, cipher modes, and volume encryption using software or hardware
- Chapter 10 - Connecting Computers
  Basic computer communication on a local network, including the fundamentals of wired Ethernet-style networks, and of wireless networks
- Chapter 11 - Networks of Networks
  Communications topologies, basic Internet addressing and routing, address resolution on a local network, and the use of networking tools like nmap and WireShark
- Chapter 12 - End-to-End Networking
  Transport protocols, domain names, firewalls, and the evolution of long distance networking technologies
- Chapter 13 - Enterprise Computing
  Enterprise-specific concepts, including enterprise management, threats applying to organizations, physical security elements, network authentication, and disaster planning
- Chapter 14 - Network Encryption
  Role of cryptography in network security, implications of encryption at different protocol layers, key distribution techniques, and policy implications
- Chapter 15 - Internet Services and Email
  Email formatting, transmission, and security issues, and enterprise firewalling
- Chapter 16 - The World Wide Web
  Fundamentals of hypertext and web protocols, modern content management systems, risks facing such systems, and assuring web confidentiality, integrity, and availability.
- Chapter 17 - Governments and Secrecy
  Government-specific threats, security classifications and clearances, national information security policy issues and typical policy elements, and government-specific security technologies
- Appendix: Alternative Terms and Concepts
  Guidance on how less-common terms and concepts appearing in NSTISSI 4011 are covered

B. Adding a Curriculum Standard

As the book progressed, it was obvious that NSTISSI 4011 provided poor guidance. The author could have chosen additional topics to cover based on self-developed criteria, but that wasn't consistent with the focus on a curriculum standard. After reviewing standards developed by the Association for Computing Machinery (ACM), the author decided to incorporate the core learning outcomes in Information Assurance and Security listed in the Information Technology 2005 draft curriculum recommendations [3].

The draft recommendations were undergoing revision as the book was being developed. The author took the opportunity to provide suggestions, and these were incorporated into the Information Technology 2008 (IT 2008) final recommendations [4]. The final version was published by the ACM in conjunction with the Computer Society of the Institute of Electrical and Electronics Engineers (IEEE). The IT 2008 recommendations were then used to guide textbook development. This introduced the following topics:

- Public-key cryptosystems, digital signatures, certificates, public key infrastructure
- Advanced Encryption Standard
- Using crypto algorithms to implement specific types of security services

ISBN 1-933510-95-1/$15.00

- Types of legal systems, rules of evidence, digital forensics fundamentals
- Security management standards, like ISO 27001
- NIST security assessment processes
- Modern network security threats and vulnerabilities, passive and active attacks
- Social engineering, hackers, crackers, black hat, white hat
- TCP/IP vulnerabilities, malware, buffer overflows.
- Web service availability

The original plans were based on a detailed breakdown of topics in the NSTISSI 4011 standard and the IT 2008 standard. While there has been no third-party attempt to validate compliance with the IT 2008 standard, the text contents were successfully submitted to the IACE courseware mapping program.

The IACE mapping requirements turn out to be slightly different from the contents of the actual standard. There are seven sections describing instructional topics. Each section includes three subsections: Instructional Content, Behavioral Outcomes, and Topical Content. The mapping process, however, only requires mapping of Topical Content to comply with NSTISSI 4011.

III. Bridging the Gap For First- and Second-Year Students

Having taught several introductory courses at different universities, the author made certain assumptions about what students were likely to learn in such a course.

- Computers execute sequences of instructions; each instruction performs an incredibly simple operation; complex programs are made up of hundreds, thousands, or millions of these instructions.
- Students will have written a simple program of some kind themselves.
- The computer executes instructions out of RAM, which serves as temporary storage, while persistent data is stored on a hard drive or flash memory.
- Computers need information to reside locally to work on it. If the computer needs data that resides somewhere on a network, the computer needs to fetch a copy of the data to work on it.

To introduce students to the topics required by the curriculum guidelines, they must be able to understand buffer overflow attacks, process separation, file system storage, and networking. Each of these topics poses its own challenge.

A. Buffer Overflow Attacks

The classic buffer overflow attack uses input data to redirect the CPU to execute an undesired program. The attacker tries to provide the program to execute, either as part of the buffer overflow data or through a different attack mechanism. The Morris worm provides the classic example of a buffer overflow.

Chapter 2 introduces students to the machine-level execution environment and then to buffer overflow. The chapter opens with a physical description of the computer's internals and a summary of execution behavior. To set the stage, the chapter organizes a program's RAM into parts: the *control section* containing the unchanging instructions and the *data section* containing the changeable data. Students also learn about the role of addresses in controlling program execution.

The buffer overflow attack rewrites data that is used to direct the program to a different set of instructions at the end of a procedure. The chapter breaks this down into an explanation of how overwriting a procedure's buffer can modify an instruction address stored near the buffer. The revised address points to data in the data section that was stored by the buffer overflow attack. The presentation includes several diagrams to clarify the example.

B. Process separation

Process separation is the bedrock of operating system security, which makes it the bedrock of information security. The chapter explains the concept of a process with easy-to-repeat examples based on the MSDOS command shell on Windows. This illustrates a single program running in multiple separate processes.

The chapter also introduces the notion of memory protection and of “kernel” versus “user” modes, and shows how these allow privileged programs to establish restrictions on application programs. This leads to an explanation of process dispatching, which yields the appearance of many programs running at once, even when only one processor is available.

ISBN 1-933510-95-1/$15.00

C. File Systems

The material on file systems was motivated primarily by IT 2008 recommendations. The section on "Forensics" includes "Media analysis" as a topic. To illustrate this, the book provides a basic introduction into data and file storage. Some topics, like parity, are also required by NSTISSI 4011. Chapter 5 describes file storage in detail, including systems used on Microsoft Windows, Apple's OS X, and classic Unix systems. It also uses file storage as a starting point to describe input/output on typical operating systems, and the use of layering to give structure to complex software.

Detailed examples of file storage use volumes formatted with the File Allocation Table (FAT) file structure. The textbook describes the directory structure, file storage, and free space management. This supports examples of recovering data from a deleted file or a "reformatted" volume. This also helps illustrate simple techniques for hiding data in the file system.

D. Networking

NSTISSI 4011 requires a broad range of networking information. Much of it is background information on networking technology that would otherwise be covered by a digital networking course. Nonetheless, many modern attacks became prominent after the standard was published, like network-borne malware and botnets. The standard also predates widespread use of firewalling and Secure Sockets Layer (SSL) to protect network traffic. Many of these topics arise in IT 2008. To ensure the most up-to-date coverage, the author also reviewed the latest forms of malware and ensured that the associated concepts and techniques were introduced.

Although the networking chapters often contain a lot of basic networking information, each chapter focuses on particular types of network security problems. Chapter 10 focuses on a local network that relies on physical security for protection, and examines the residual vulnerabilities. Chapter 11 introduces the Internet Protocol and associated addressing and routing issues. The chapter also introduces WireShark as a tool to examine network traffic.

Chapter 12 focuses on end-to-end networking and long-distance networking. It also introduces the Domain Name Service and firewalls. The chapter builds on Chapters 10 and 11 to present a final section covering a smorgasbord of aging network technologies required by NSTISSI 4011.

Chapter 14 describes network encryption in terms *cryptographic building blocks*. Most of these were introduced earlier with file and volume-oriented encryption in Chapters 7 through 9. Chapter 14 also uses the concept of protocol layering from Chapter 10 to show how encryption at different layers achieves different results.

Chapters 15 and 16 introduce web-based applications, focusing on email and the web. Like the earlier chapters, these introduce the networking fundamentals and then use them to illustrate security issues affecting these services. Chapter 15 includes detailed information about email route tracing and email address forgery. Chapter 16 explains both basic web technology and the properties and risks facing modern, database-oriented content management systems.

IV. Addressing Sensitive and Formerly Classified Topics

There is a lot of misinformation and conjecture applied to sensitive and formerly classified topics. To avoid such errors, the textbook's coverage relies primarily on published and often declassified guidelines and recommendations from the U.S. military and intelligence communities. This arose when addressing the following topics:

- Communications security (COMSEC) – the U.S. government term for cryptographic system developed and managed by the government.
- Transmission security – the problem of protecting information that may be recovered by studying the visible properties of encrypted messages, like sources, destinations, amounts of traffic, and so on.
- TEMPEST – the term is a long-used code name applied to security risks arising from electromagnetic or acoustical "noise" from information processing equipment
- Operations security (OPSEC) – the problem of protecting details of sensitive activities whose details might be disclosed by publicly visible activities, like changes in vehicle traffic patterns, or in food ordering patterns.

While there is a rich literature on network security and applied cryptography, there are fewer sources that focus on U.S. government-specific technologies and procedures. Federal legislation has assigned the National Security

Agency (NSA) responsibility for protecting sensitive government communications. The NSA generally follows the tradition of other intelligence agencies of publishing as little information about itself as possible. Elements of this tradition changed gradually as the commercial network security and cryptography community produced increasingly sophisticated technologies and products.

Changes have also arisen through the Freedom of Information Act (FOIA). Individuals may request the declassification and release of information that is no longer sensitive under FOIA. Government agencies are obligated to consider and respond to such requests. While this does not guarantee that a particular document will be released, it seems to accelerate the release of significant if obsolete documents.

The following subsections provide an overview of unclassified and formerly classified information collected and reviewed to address the above list of topics. A lot of information comes from the Project on Government Secrecy hosted on the web site of the Federation of American Scientists [5]. Many of these documents were released through FOIA requests.

A. COMSEC

Organizations that use cryptographic systems to handle classified information must generally rely on technologies and procedures belonging to the NSA. While the NSA has approved the limited use of AES cryptography to protect classified information, the systems are still manged using NSA procedures. These procedures involve “COMSEC accounts” that track and manage all cryptographic keys and sensitive cryptographic equipment.

The FAS web site provides numerous relevant documents, particularly in the form of regulations and guidelines published by military commands like the U.S. Army in Europe [6]. Procedures and related information about COMSEC accounts are published in the National Industrial Security Program Operating Manual [7]. For a broader and more fascinating look at COMSEC developments up to the 1970s, consult the recently declassified David G. Boak Lectures, a publication that was used to instruct NSA employees [8].

B. Transmission Security

Transmission security is subtly different from COMSEC in that it tries to hide patterns in communications traffic that may disclose information even when the traffic is encrypted. The best way to find details about this subject is to track down the individual topics associated with it in NSTISSI 4011. Many of those topics refer to commercial technologies, including frequency hopping, optical systems, dial back, line-of-sight, and spread spectrum. Spread spectrum is widely used today in cell phone systems to reduce the effects of interference and to more efficiently use the available bandwidth.

Other transmission security topics lead to information about electronic warfare. While this is also often a classified topic, there are ample references available to describe the techniques, like jamming, screening, masking, and so on. It is also helpful to recognize that some topics are commonly discussed as *traffic analysis*.

C. TEMPEST

While TEMPEST has long been a classified subject, certain elements, like the importance of shielding, red/black separation, and restricting nearby access, have long been published in unclassified publications. Boak's lectures provide insight into previously classified details and examples [5]. Numerous reports and specifications, generally from FOIA requests, have also been posted on the Cryptome web site [9]. For example, the “Red/Black Installation Guidance” [10] on the Cryptome web site describes zoning distances and requirements for equipment and cable separation. Taken together, this information explains the specific terms and concepts cited in the NSTISSI 4011 standard.

D. OPSEC

In the government arena, this refers to Operations Security, the problem of disguising a sensitive activity even when overt evidence of it is visible to potential adversaries. The classic though possibly apocryphal example involves the 1991 Gulf War: several press reports arose of a reported spike in pizza orders from the Pentagon and the White House immediately before the U.S. invasion. The Operations Security Professional's Association (OSPA) claims that the methodology currently used by the US military arose during the Vietnam War [11].

The IACE web site points questions about OPSEC to the National OPSEC Program's web site [12]. This site clarifies many of the terms used in NSTISSI 4011. It also points to unclassified U.S. military OPSEC policies and procedures, which specifically identify OPSEC roles and specific requirements for OPSEC analyses.

ISBN 1-933510-95-1/$15.00

V. Conclusion

Although a textbook could be written that focuses exclusively on NSTISSI 4011 topics, such a textbook would be instantly out of date. The textbook described here incorporates more general and up-to-date topics taken from the IT 2008 curriculum recommendations produced by the ACM and IEEE. This may have increased the textbook's length, but it also makes the textbook relevant to today's students while it complies with the eighteen-year-old training standard.

The textbook incorporates a lot of non-security tutorial information. Some of this is specifically required by NSTISSI 4011, particularly on networking. Other tutorials provide students with the basis to understand both what security mechanisms are present and how they work. Tutorials also helped clarify malware behavior.

Ample unclassified sources exist for the topics covered in NSTISSI 4011. Some topics rely heavily on previously classified information, but sufficient information has been declassified to cover all topics. Moreover, many topics are the subject of unclassified policy and procedure documents. The obscure and specialized terminology of government security may have impeded some authors from covering such topics in earlier textbooks.

VI. References

[1] "National training standard for information security (INFOSEC) professionals," NSTISSI 4011, Ft. Meade, MD: National Security Telecommunications and Information Systems Security Committee, 1994.

[2] Richard E. Smith, "Elementary Information Security Topic Mapping for NSTISSI 4011," web site, http://www.cryptosmith.com/node/353, (retrieved on march 30, 2012).

[3] ACM, "Computing curricula: information technology volume." Association for Computing Machinery, October 2005.

[4] ACM and IEEE Computer Society, *Information Technology 2008 Curriculum Guideline*, 2008. http://www.acm.org/education/curricula/IT2008%20Curriculum.pdf, (retrieved March 1, 2012).

[5] FAS, "Federation of American Scientists: Project on Government Secrecy," web page, http://www.fas.org/programs/ssp/govsec/index.html, (retrieved March 5, 2012).

[6] U.S. Army Europe (USAEUR), "Safeguarding and Controlling Communications Security Material," USAEUR Regulation 380-40, 10 July 2003. http://www.fas.org/irp/doddir/army/aer380-40.pdf, (retrieved March 5, 2012).

[7] Defense Security Service, "National Industrial Security Program Operating Manual," Washington: Department of Defense, 2006. http://www.dss.mil/isp/fac_clear/download_nispom.html, (retrieved March 5, 2012).

[8] David G. Boak, *A History of U.S. Communications Security*, 2 volumes, Ft. George Meade, MD: National Security Agency, July 1973 (vol. 1) and July 1981 (vol. 2). www.nsa.gov/public_info/_files/cryptologic_histories/history_comsec.pdf, and http://www.nsa.gov/public_info/_files/cryptologic_histories/history_comsec_II.pdf, (retrieved on March 5, 2012).

[9] John Young, "NSA TEMPEST Documents," web site, http://cryptome.org/nsa-tempest.htm, (retrieved on March 5, 2012).

[10] NSTISSC, "Red/Black Installation Guidance," Advisory Memorandum TEMPEST/2-95, Ft. George Meade: National Security Agency, 12 December 1995. http://cryptome.org/tempest-2-95.htm, (retrieved on March 5, 2012).

[11] OSPA, "The Origin of OPSEC – from the dragon's mouth," web site, http://www.opsecprofessionals.org/origin.html, (retrieved on March 5, 2012).

[12] IOSS, "National OPSEC Program," web site, http://www.iad.gov/ioss/, (retrieved on March 5, 2012).