

Integrating Information Security into the CS/IT Curriculum

Dr. Guillermo A Francia, III
Jacksonville State University

Information Security

" ... set of measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation..."

--National Security Agency (NSA), 2002

Information Security Education

■ Current State:

- **Undeveloped** ← most prevalent
- **Emerging** ←
- **Mature**

-- Dark, et. al., 2005

NSF Proposal

- Vertical Integration of Information Security and Assurance (VIISA)
- participation of all disciplines in security-related knowledge acquisition
- methodology that intertwines three approaches: **threading of security topics** into existing course materials, **infuse** existing courses with **security course modules**, and addition of one or more **capstone security courses**

NSF Proposal

- Course materials will be designed based on the **Committee on National Security Systems (CNSS) Training Standards**
- **Multiple research and pedagogical avenues available** in security using established areas in CS/IT such as AI, Systems, Networks, Software Engineering, Internet Technologies, etc.
- Opportunities for **international collaboration** and **funding are numerous** and readily available

The Need

- **The pervasiveness and the convenience of information technology (IT) tend to make most of society deeply dependent on its reliability and availability**
- **The 2006 CSI/FBI Computer Crime and Security Survey reveals a \$52.5 billion loss**
- **It is the responsibility of every organization to establish a reasonably secure system to protect its own interests as well as those of its customers**

The Need

- **The trend is moving towards requiring secure software engineering practices in every sector of IT application development:**
 - **Microsoft's Trustworthy Computing Initiative**
 - **The US Department of Justice has published a guideline for integrating security in the development process.**
 - **Public and private institutions are slowly demanding secure applications from their IT developers.**

The Need

- **We can no longer ignore this issue and our charge is to prepare our students to lead in tackling the impending, if not ongoing, information warfare.**

Security Course Objectives

- To provide an understanding of basic information security terminologies and concepts
- To present the practical realities of information security through hands-on experimentations and case studies

Security Course Objectives

- To provide an understanding of security design models, principles, and theories
- To introduce the concepts of basic cryptography and access control.

Approaches to Teaching InfoSec

- Thread Information Security topics into existing courses
- Infuse existing courses with Information Security course modules
- Addition of one or more capstone security courses

Threading of InfoSec Topics

- Introduction to Information Systems Threads
 - Strong password creation
 - Social Engineering
 - Spam/Phishing/Online dangers
 - Spyware
 - Firewall
- Computer Networks Threads (7 Layer hacks)
 - Physical—facility, perimeter, and device security, scanning and sniffing, cabling and wiretapping.
 - Data Link—Packet analysis using Wireshark, Address Resolution Protocol (ARP) flooding and poisoning.
 - Network—Internet Protocol (IP) attacks and defense, Internet Control Message Protocol (ICMP) attacks and defense, spoofing, DOS.
 - ...Transport...Session...Presentation...Application... and even People.

Threading of InfoSec Topics

- Computer Organization/Architecture Threads
 - Memory protection hardware (DEP)
 - Instruction set architecture: privileged instructions and dual-mode operation
 - Encryption/decryption hardware
 - Virtual machine support: to isolate multiple, heterogeneous users working on the same system

Threading of InfoSec Topics

- Ethics and Legal Issues Threads
 - Confidentiality and integrity of information
 - Policy and Laws
 - Ethical hacking
 - Legal aspects of technology
 - Generally accepted security
 - Digital forensic investigation

Rationale for Security Course Modules

- Infuse a reasonable amount of security issues into a typical CS/IT course
- The amount of material related to these topics and their importance necessitate incorporating them into standalone modules
- Each module should require about three hours of instruction time supplemented by out-of-class readings, experiments, and assignments

Security Course Modules

- Database Security
 - Statistical databases, SQL Injection, Access control
- Web Services Security
 - Web services security specifications

Security Course Modules

- **Secure Software Engineering**
 - Threat Modeling, Security Testing
- **Operating Systems Security**
 - ACL, File encryption, Authentication, Security logs

Capstone Courses

- **Management of Information Security**
 - Emphasis is on developing security policies, security management and practices, risk management, security project management, and protection mechanisms.
- **Computer Security**
 - study of network security architectures and models, cryptography, authentication and authorization protocols, secure application and systems development.
- **Digital Forensics**

Security Projects

- **Systems Reconnaissance**
 - Utilize nmap and UMIT for system fingerprinting
- **Packet Capture and Analysis**
 - Utilize Wireshark and/or Snort for packet capture
- **Web Exploit**
 - The objective is to familiarize students with the Common Vulnerability Exposures (CVEs), web server fingerprinting, Unicode directory and command execution vulnerability, and web server exploits.

Security Projects

- **Intrusion Detection System**
 - The objective is to familiarize students with Intrusion Detection Systems (IDS), IDS signatures and rules, the configuration and implementation of common open-source IDS tools, and the analysis and identification of possible incidents.
- **Vulnerability Assessment**
 - Usually a group term project. Includes a preliminary prospectus, actual penetration testing, executive and technical reports, recommendations and analyses, and a presentation.

Security Projects

■ Digital Forensic Investigation

- The objective is to familiarize students with basic digital forensic analysis. Forensic investigation skills will be tested specifically on the following areas: evidence preservation and retrieval, data encryption/decryption, steganographic analysis, file sector analysis and retrieval, and file type recognition.

Security Projects

■ Applied Cryptography

- The objective is to provide students with hands-on exercises in implementing applications that utilizes the symmetric and asymmetric encryption, decryption, and hash/message digest generation APIs found in the .Net and Java frameworks.

Security and Forensics Laboratory

- Four (4) Dual-boot computers (Win-XP, Win-2000, Fedora/Red-hat Linux).
- A virtualization software (MS Virtual PC, VMWare, Bochs, PearPC)
- Hub or a switch to interconnect an isolated private LAN
- Open source software: Nmap, UMIT, Wireshark, Metasploit, Snort, Stools, MySQL, Apache, PHP, Hping, and Nemesis.

Textbooks

- Stamp, Mark, *Information Security Principles and Practice*. John-Wiley and Sons, 2006.
- Bishop, Matt, *Computer Security, Art and Science*. Addison-Wesley 2005.
- Howard, M. & LeBlanc, D. *Writing Secure Code*. Microsoft Press, 2002.
- Whitman, M. and Mattord, H., *Principles of Information Security 2nd Ed*. Thompson Course Technology, 2005.
- Hoglund, D. & McGraw, D. *Exploiting Software How to Break Code*. Addison-Wesley, 2004.
- Stallings, William, *Cryptography and Network Security 4th Ed*. Prentice-Hall, 2006.
- Gollman, David, *Computer Security*. Wiley, 1999.
- Schneier, Bruce, *Applied Cryptography*. John-Wiley and Sons, 1996.

References

- Dark, Melissa, and Davis, Jim, "Report on Information Assurance Curriculum Development." Website: http://www.cerias.purdue.edu/education/post_secondary_education/past_offerings/curriculum_development/information_assurance/report_info_assurance_cur_dev.pdf. Access date: September 18, 2006.
- Vaughn, R. B., Boggess III, J. E., "Integration of Computer Security into the Software Engineering and Computer Science Programs." *The Journal of Systems and Software. Elsevier Science, North Holland, vol 49 (149-153) 1999.*
- Vaughn, R. B., Dampier, D. A., and Warkentin, M. B., "Building an Information Security Education Program." *InfoSecCD Conference 2004. 41-45.*

Questions ???

