Curriculum for information security

Dr. Rick Smith
University of St. Thomas
Outline

• Genesis of a curriculum
• A look at ‘real practice’
• Textbook issues
• Curriculum standards
• Curriculum plan
• Introductory course
• Upper division course
Genesis of a curriculum

- Well-attended Security “Topics” courses
  - Other “technical” courses were empty
  - How can we give the students more?

- “Real” security textbooks
  - For grad students or sophisticated undergrads
  - What do most undergrads do?

- Curriculum and training standards
  - A “laundry list” of topics
  - Do-able
“Real practice” of computer security

• The lifecycle
  – Requirement analysis/policy development
  – Planning and design
  – Implementation
  – Monitoring and response
  – Repeat

• Perimeter analysis
  – Where are the perimeters?
  – How are they maintained?
  – Can we rely on them?

• Information flow assessment
Curriculum Objectives for Department

• Draw in new students (security is ‘sexy’)

• Introductory course that can reach non-majors
  – Lots of science majors take intro programming
  – Is that enough background?

• A program that’s obvious on a transcript
Textbook Issues

• **“Classic” textbooks**
  – Prerequisites: upper level courses
    • Operating systems
    • Network protocols
    • Number theory (somewhat optional)
    • Formal analysis of software
  – Develop security concepts from mathematical principles

• **“Test Prep” textbooks**
  – Prerequisites: none, really
  – Focus on facts: a “body of knowledge”
  – Little coverage of analytical techniques, security problem solving
Curriculum Standards

• ACM IT Curriculum (under revision)
  – Covers 23 “core hours” of an IT curriculum
  – Outlines lots of worthwhile topics
    • Security life cycle, policy, security domains, forensics, information states, threat analysis model, ...
    • Some useful ISO standards
    • I don’t see how it’s all done in 23 hours
      – “the 6 minute history of information security”
    – Includes some odd things
      • Obsolete technology/concepts: DES, RAS, CASPR
      • NIST’s risk assessment process (contradicts/overlaps)
      • “MSR Model” – variant of NSTISSI 4011’s McCumber model
        – Both seem awkward and pointless
Government Curriculum

• **1994: NSTISSI #4011 – Standards for training Infosec Professionals**
  – One of 5 training standards – most relevant
• **1998: IACEP – NSA’s course evaluation program for information security education**
  – Courseware evaluation – the school covers the correct topics for training those professionals
  – Centers of Excellence – schools have significant resources involved in information security education and research
NSTISSI 4011 Curriculum Areas

- Data communications
- Computing basics: hardware, software, firmware
- Security overview and model
- National information security uses, policies, models
- Specific communications systems and policies
- Planning and designing for security
- Specific vulnerabilities; technical and policy solutions
UST Security Program

• **Lower division courses**
  - Introductory course to procedural programming and computing
  - Object oriented programming and data structures
  - Applied statistics
  - Elementary information security (Sec 1)

• **Upper division courses**
  - Operating systems (OS)
  - Computer networks (Net)
  - Information security analysis (Sec 2)
  - System analysis and design
  - Elective course in the

• **Allied requirements**
  - Discrete math or digital logic design
  - Workplace communications
“Dry run” of introductory course

• Prerequisites
  – Introductory programming
  – College level math, preferably discrete math

• Textbook plus notes

• Labs
  – WireShark labs
  – Firewall labs
  – Tried to do network mapping – latest version of Ubuntu was a bit too stealthy
  – Demos of NetGoat
Objectives/Strategies

• Present technical concepts as solutions
  – Introduce a security problem
  – Identify a technology that helps solve it
  – Describe the technology

• Emphasis on observation and analysis
  – Diagramming security perimeters
  – Identifying information flows
  – Strength of mechanism: passwords, keys
Topic Progression

• Single desktop computer – introduce basics of physical security, security policy objectives (“Don’t touch my computer!”), intrusion recovery, etc.
• Shared desktop computer – introduce user based access control, process protection in operating systems, and then file and volume encryption as an alternative, which leads to cryptography.
• Local area network – introduce networking basics, and the concept of user roles.
• Viruses and worms – malicious logic that tries to spread.
• Wireless networking – introduces “link layer” encryption
• Internet access – the problem of safe browsing on the web, especially from a LAN. This introduces firewalls.
• VPNs – safely connecting LANs across the Internet. This introduces public key cryptography as used in IPSEC/IKE.
• Socket layer encryption – protecting traffic for Web browsers. This introduces RSA public key encryption.
• PKI – this introduces digital signatures, certificates, and their problems.
• E-Commerce – this introduces the risks to a site that provides service to the Internet, particularly Web service. This covers additional features of firewalls.
Missing Prerequisite Topics

• CPU Operation, to understand instruction stream
• Processes and process separation
• Layering in software architecture
• Role of message exchange in network protocols
• Role of “layering” in network protocols

• Introduce the concepts incrementally as needed
Textbook: “Internet Cryptography”

• Benefits
  – Architectural view of network crypto
    • Relationship of layers and crypto insertion
  – Presents trade-offs to achieve different security goals
  – Focus on basic concepts in network crypto
  – Basics of firewalls and web system architecture

• Problems
  – Copyright 1997
  – Lots of simplification to make the concepts accessible
    • Super simplified SSL
  – Older version of IPSEC (no IKE)
  – Crypto examples use older, weaker techniques
Senior Year Analysis Course

- Blend of the interesting and necessary
  - Labs with security tools (candy)
  - Federal security standards (castor oil)

- Security tools
  - LAN surveying
  - Honeypots
  - Self-teaching tools in system vulnerabilities

- Federal Standards
  - Laws, regulations, policies, evaluations, C&A

- Capstone Infowar Exercise
  - Two teams must secure desktop machines in an isolated lab environment, then attack each other
Textbook – Work in Progress

- Publisher: Jones & Bartlett for Fall '09 (!!)
- Topics follow the course outline (earlier)
- Goals
  - Weave together policy and analysis concepts with technical solutions
  - Teach how to think about information flow between components
  - Students should be able to construct simple security solutions
- Other goals
  - Cover NSTISSI 4011 and ACM IT security topics
  - Lots of diagrams
  - Readability
Questions for the Audience

• How to teach introductory security
  – 1. Don’t do it
  – 2. Do it with simplified things that might be misapplied
  – 3. Make it hard to scare out the incompetents

• At what level does simplification become ‘wrong’?
  – A dilemma that arose with ‘Internet Cryptography’
Thank You!

Questions?