Security Education
Practical Lessons learned

FISSEA

March 2006

Objective

- This presentation is aimed at sharing the pitfalls and processes attempted in imparting knowledge and skills to students interested in performing the responsibilities of administration and management of Computer Systems Security for enterprise information systems.

Problem Statement

- The process of imparting knowledge and skills to students for Information Assurance brings with it a need to impart a respect for ethical behavior as well as an understanding of the legal, moral, and ethical issues associated with the responsibilities of Computer Systems Security.

What Is Security?

- “The quality or state of being secure—to be free from danger”

- Security is achieved using several strategies simultaneously

- What Is Information Assurance
- You and I used to call it computer security or perhaps privacy
- It is much more than that...
  - Integrity
  - Trust
  - Confidentiality

Scope

- Information technology is critical to business and society
- Computer security is evolving into information security
- Information security is the responsibility of every member of an organization, but managers play a critical role

Goals

- Increase awareness of Security Issues
- Teach security improvement techniques
- Explain how exploitable errors have been made in the development of software.
- Raise the level of ethics awareness
- Bring attention to legal issues
- Encourage Responsibility

Learning Objectives

1. Describe ways in which connecting to the Information Infrastructure can create risks to your systems.
2. Discuss the importance of training to the separation of duties required of the DAA.
3. Explain DAA responsibility for preventing unauthorized disclosure of information.
4. Extrapolate risk management concepts to multiple scenarios.
5. Make decisions based on reasoned judgment.

How do we Blur the Boundaries in IA Training versus education?

As information security becomes increasingly important, it can no longer be left to the realm of mere technical training.

1. Standards need to be de-obfuscated - made less government-focused and include real-world industry focus.
2. The standards need to focus on Information Assurance than just INFOSEC as the former defines thinking and behavior and the latter just behavior/actions.

Learning Experience

- Considerable amount of “wow” effect.
- “We really learned a lot!”
- Practical Education – Hands on
    - Difficult in a “Normal” academic environment
    - More so in an Online setting
    - Impetus on Student “interest” to motivate

Goals Achieved

- Awareness of Security Issues
- Teach security assessment techniques
- Explain how exploitable errors have been made in the development of software.
- Raise the level of ethics awareness
- Bring attention to legal issues
- Taught Yes, Learned Yes, Believed In . . . Well maybe.

By-Products: Students are ...

- More at ease with real hardware and real software – not a black box any more.
  - Not always ‘fluent’ with concepts
  - Hands on promotes curiosity
- Amazed at the Open Source movement, but do not understand the corporate hesitation to use

Security and Control

- Examples
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security

- Controls
    - Physical Controls
    - Technical Controls
    - Administrative
  - Prevention – Detection – Recovery
  - Masking actions
  - Deterrence, Corrective

Key Concepts: Accountability; Assurance

- Accountability
  - The characteristic of accountability exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process
- Assurance
  - Assurance that all security objectives are met

Assumptions in the Course Design

- Beliefs on privacy and user rights?
  - Most have NOT had Ethics Training
- Lab-oriented
  - Difficult especially in Online
- Participation levels
  - Very dependant upon interest generated
- Student Background & Experience
  - Extremely diverse and varied

The course needs hands-on work . . .

“I hear and I think.
I see and I remember.
I do and I know.”

-- Confucius

Principles Of Information Security Management

- The extended characteristics of information security are defined as the six Ps:
  - Planning
  - Policy
  - Programs
  - Protection
  - People
  - Project Management

Policy

- Policy: set of organizational guidelines that dictates certain behavior within the organization
- In InfoSec, there are three general categories of policy:
  - General program policy (Enterprise Security Policy)
  - An issue-specific security policy (ISSP)
    - E.g., email, Intenert use
  - System-specific policies (SSSPs)
    - E.g., Access control list (ACLs) for a device

People

- People are the most critical link in the information security program
  - Human firewall
- It is imperative that educators continuously recognize the crucial role that people play
- Include information security personnel and the security of personnel

The Security Gap

- Security technology is essential
  - Firewalls, anti-virus, intrusion detection, encryption etc.
- Technology is not enough
  - Gartner: 80% of downtime is due to people and processes
- Tighter the security controls, the harder they are to break and the target becomes the user
  - Technology can make it difficult to forge IDs but can’t stop people getting real IDs under fake names
- Technology can never stop social engineering
  - People are still tricked into disclosing their passwords
  - Creating

Awareness, Training & Education

Comparative Framework			
	Awareness	**Training**	**Education**
Attribute	What	How	Why
Level	Information	Knowledge	Insight
Learning Objective	Recognition & Retention	Skill	Understanding
Example Teaching Method	*Media* -Videos -Newsletters -Posters	*Practical Instruction* -Lecture and/or demo -Case study -Hands-on practice	*Theoretical Instruction* -Seminar and discussion -Reading and study -Research
Test Measure	True/False Multiple Choice (identify learning)	Problem Solving Recognition & Resolution (apply learning)	Essay (interpretive learning)
Impact Timeframe	Short-Term	Intermediate	Long-Term

From "The Human Factor in Training Strategies" by Dorothea de Zafra, Nov. 1991

Information Security Culture

- Information Security culture must be shown to complement the Organizational culture
  - Congruent with the mission
  - Commensurate with risk level of acceptance
- Common elements of a security culture across organizations
  - Privacy, internal controls
  - Protection of proprietary information
  - Laws and legal considerations

Attitude Adjustment

- Attitude is important
  - Motivator of Behavior
  - Source of Risk
  - Behavior based on ‘passion’
- Attitude can be changed
  - Responsibility & Ethics awareness

The Threat

- “The greatest threat you face is not the viruses or the hackers or the whatever, but rather complacency.”

There Is Nothing To Worry About . . .(right!)

- This is one approach to the problem

Future goals

- Operational plan
  - Create revised IA program
    - Graduate & Undergrad
  - Develop articulation agreement with cooperative entities
- Long-term goal
  - Become CAE designated by NSA

Future Goals

- Take a leading role in IA curriculum development
  - Not Just locally . . .
- Collaborate with other universities & businesses regarding research & proposals
- Engage in IA research and publications
- Teach more IA courses
  - Expand offerings
  - Expand areas of focus

IA Program Challenges

- There is an increase in the student enrollment in the Information Assurance track
- There is a need for the further improvement of quality of existing courses
- There is a growing demand for the hands-on laboratory, even within the online courses

Future Goals

- Develop new Information Assurance courses
- Promote collaborative research and publication in Information Assurance
- Further improve the quality of existing Information Assurance courses

What Works!

1. Structure of the Program

- Benefits
  - Motivated learning
  - Better time management
  - Better management of work and family conflict
  - Development of pedagogical knowledge and skills
  - Teaching more effectively

Benefits

- Provided solid foundation for subsequent curriculum exposure
- Building capacity for IA at traditional institutions
- Improved knowledge and skills on IA
- Emphasis on writing skills

Collaboration

- One of the best features of our program
    - Students with diversified background
    - Sharing expertise and interests
    - Collaboration on writing/projects
        - Team projects
    - Continuing efforts in working together on research projects
        - Teams can cross Course/Class boundaries
            - Some teams have maintained contact even after graduation

Course Logistics

- Lectures on one *area* per week
- Lectures on one *tool or methodology* per week
- Emphasis on *"Work-like"* projects and task products – a 'professional learning model' approach.

Currently Available Materials

- Books
- Websites
- Open Source tools
- Courses elsewhere

Books on Security

- Many books, > 500
- Academic text books, in the tens.
- Garfinkel and Spafford 1996/2003, Practical UNIX & Internet Security, O'Reilly.
- Rubin 2001, White-hat Security Arsenal, Addison Wesley.
- Stallings 1998, Cryptography and Network Security, Prentice Hall.
- Bishop 2003, Computer Security, Addison Wesley.

Web Sites

- "There is an oceanic amount of material on network security available over the Internet." -- A Web Page.
- How do we define a "Security Web Site"?
- 1000+ web sites

A Few Chosen Security Websites

- www.incidents.org
- www.cert.org
- www.cerias.purdue.edu
- www.securityfocus.com
- lwn.net/security
- www.microsoft.com/security
- www.phrack.com
- www.sans.org

“Internet Security”

- Trojan Horses, Viruses and Worms
- Privacy and Authentication
- TCP/IP exploits
- Firewalls
- Cryptography
- Secure Config of Personal Machines
- Buffer Overflow and Other Bug Exploitation
- Writing Bug-free and Secure Software
- Secure e-Commerce Transactions
- Ethics and Legal Issues

Ethics

- Proposed Ethics Statement (see attached)
- *The Ethics of Hacking*. A discourse by "Dissident" www.attrition.org/~modify/texts/hacking_texts/hacethic.txt
- *The Hackers Ethic*. The six tenets from Steven Levy, "Heroes of the Computer Revolution". project.cyberpunk.ru/idb/hacker_ethics.html
- Codes of Ethics from ACM+IEEE.
- www.onlineethics.org
- www.ethics.org

Sample Ethics Statement

- In this class I am learning network and computer security principles. It is a 5.5-week long course, with the prerequisites of:
  - general understanding of operating systems and computer networks.
- I assure the instructor, the University, and the community that I am a responsible, and principled person. I will never engage in activity that deprives others in order to benefit from it.
- The techniques and links that I am exposed to are for educational purposes only. As a user of computers and potential network or systems administrator, I must be familiar with the tools that may be used to bring a system or network down.   I may engage in a legitimate form of ethical hacking, as a consultant who performs security audits. This is the driving force in learning the past attack techniques.
- I will not directly provide anyone with the tools to create mischief.   Nor shall I pass my knowledge to others without verifying that they also subscribe to similar principles as contained in this statement.
- I will not engage in or condone any form of illegal activity including unauthorized break-ins, cracking, or denial of service attacks.

______________________________ ______________________________________

Name of the student Signature and Date

Feeling Stuck between a rock and a hard place?...

Thank you for your time!

Questions or Comments?