On a University-Wide Required Cyber-Security Course

By Raymond Greenlaw

Collaborators

Christopher Brown, Frederick Crabbe, Rita Doerr, Chris Hoffmeister, Justin Monroe, Donald Needham, Andrew Phillips, Anthony Pollman, Stephen Schall, John Schultz, Steven Simon, David Stahl, and Sarah Standard

Outline

1. History
2. Course Overview
3. The Cyber Battlefield
4. Models and Tools
5. Cyber Operations
6. Some Thoughts
7. Questions

History

- US Naval Academy (USNA) Mission
- President Obama’s May 2009 Cyberspace Policy Review
- USNA Cyber Warfare Ad Hoc Committee
- USNA Ad Hoc Committee on Cyber-Security Curriculum Options
- Six Months to Implement

Overview: Course Mission

Educate each midshipman about cyber infrastructure and systems, inherent cyber vulnerabilities and threats, and appropriate defensive security procedures, thereby enabling them to make principled decisions regarding the potential benefits, consequences, and risks from a proposed use of an information system in today's cyber-warfare environment.

Overview: Goals

1. Understand basic physical and virtual architecture of cyberspace—individual computer and program, physical components and protocols of network and Internet, and web,
2. hands on experience with components of physical and virtual architecture of cyberspace and ability to relate that experience to larger system,
3. an understanding of DoD’s pillars of IA (CIANA), inherent vulnerabilities of information systems that endanger these properties, defensive measures to ensure information systems retain these properties, and offensive measures to violate these pillars, and
4. hands on experience with defensive and offensive practices in cyberspace, and ability to relate that experience to new or more sophisticated attacks and defenses.

Overview: Mechanics

- 2 hours lecture, 2 hours lab; 3 credits
- Laptops
- Software installation
- Resource page
- Weekly instructors’ meetings
- Email list
- Networking issues

The Cyber Battlefield 1

- Introduction
- Digital Data 1 & 2
- Computer Architecture
- PC Vivisection Lab
- Operating Systems 1 & 2
- Programs Parts 1–5

The Cyber Battlefield 2

- Web: Servers, Browsers, and HTML
- Web: Build Your Webpage Lab
- Web: Client-Side Scripting: non-event driven, event driven, and forms
- Web: Server-Side Scripting
- Web: Injection Attacks & XSS

The Cyber Battlefield 3

- Networks, Protocols, the Internet: Parts 1–4
- Networks: Build a LAN Prep
- Networks: Build a LAN Lab
- Networks: Wireless Networking
- Networks: Build a Wireless-Network Lab

Models and Tools

- Information Assurance
- Firewalls
- Authentication/Cryptography Parts 1–4
- Authentication/Cryptography: X.509 Certificates Lab

Cyber Operations 1

- Forensics
- Phases of a Cyber Attack/Recon
- Forensics Lab
- Network Attack
- Cyber Recon Lab
- Network Defense
- Malware

Cyber Operations 2

- Cyber Attacks: Case Studies
- Cyber Attack Lab
- Attack Lab Debrief
- Cyber Defense Lab
- Defense Lab Debrief

Some Thoughts

- Diverse group of instructors
- Manpower required
- Instructor commitment
- Investment in software, hardware, and support
- Materials
- Assessment
- Ongoing development
- Non-technical students
- Student performance
- Student retention
- Workload

Questions?

http://www.usna.edu/cs/si110

Dr. Raymond Greenlaw
United States Naval Academy
www.raymondgreenlaw.com
greenlaw@usna.edu