By
Raymond Greenlaw

United States Naval Academy, Annapolis, Maryland
Chiang Mai University, Chiang Mai, Thailand

ANATOMY AND DISSECTION OF AN INTRODUCTION TO CYBER-SECURITY CLASS

Dr. Raymond Greenlaw
United States Naval Academy

OUTLINE

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

OUTLINE

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

HISTORY

- **May 2009** President's 60-day Cyberspace Policy Review completes. Action item to *"expand and train the workforce, including … cybersecurity expertise in the Federal government*."
- **July 2009** *Cyber Warfare Ad Hoc Committee* forms at USNA to define the scope of understanding of cyber security needed by midshipmen as future naval officers.
- **August 2009** *Committee* recommends creation of a required core course in CS and IT that provides the technical foundations of Cyber Warfare. Course will be technical, relevant to naval officers, and hands-on.
- **January 2010** CS Department offers Fundamentals of Cyber Security as an elective.

HISTORY

- **April 2010** *Ad Hoc Committee on Cyber Security Curriculum Options* forms to examine integration of "cyber" into the USNA curriculum.
- **May 2010** *Committee* recommends a sequence: Cyber-1 during 4/C year and Cyber-2 during 2/C year.
- **September 2010** Dean requests Cyber-1 technical course proposal from CS Department.
- **November 2010** Two proposed Cyber-1 course syllabi formulated by the *CS Department Cyber Warfare Committee,* and approved and endorsed by the *CS Department Curriculum Committee*.
- **January 2011** CS Department offers a revised Intro to Cyber Security as a prototype Cyber-1 course.

HISTORY

- **Spring 2011** Sup directs that Cyber-1 be offered in Fall 2011 for USNA Class of 2015.
- **March 2011** Formal curriculum change request to add a plebe-year course. Cyber-1 Tiger Team forms to put together course from prototype. Team is a mix of faculty from CS, Math, and EE.
- **Summer 2011** Numerous faculty work on course materials; course hardware and software infrastructure is acquired and tested.
- **August 2011** Two-week charm school given for instructors. Lectures recorded.
- **August 22, 2011** First day of class; SI110 begins.

OUTLINE

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

COURSE OVERVIEW OUTLINE

- Mission
- Goals
- Personnel
- Mechanics
- Materials

COURSE OVERVIEW (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.

COURSE 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.

COURSE OVERVIEW (PERSONNEL)

- 600 plebes per semester
- 15 instructors handling 30 sections
- Average section about 20 students
- Course coordinator
- Several course helpers
- Departmental technical support
- Course scheduler
- University-level technical support

COURSE OVERVIEW (MECHANICS)

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

COURSE OVERVIEW (MATERIALS)

- Websites—student, instructor, external
- Instructor notes
- Student notes
- Common exams
- Common homework
- Common labs—activity sheets
- Custom textbook

OUTLINE

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

THE CYBER BATTLEFIELD 1

- Introduction
- Digital Data 1 & 2
- Computer Architecture
- PC Vivisection Lab
- Operating Systems 1 & 2
- Programs Parts 1–5
- Web: Servers, Browsers, and HTML
- Web: Build Your Webpage Lab

THE CYBER BATTLEFIELD 2

- Web: Client-Side Scripting: non-event driven, event driven, and forms
- Web: Server-Side Scripting
- Web: Injection Attacks & XSS
- 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

OUTLINE

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

MODELS AND TOOLS

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

OUTLINE

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

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

OUTLINE

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

SOME THOUGHTS (RESOURCES)

- Diverse group of instructors
- Man power required
- Instructor commitment
- Investment in software, hardware, and support
- Materials
- Ongoing

SOME THOUGHTS (STUDENTS)

- Non-technical students
- Performance
- Retention
- Workload
- Recruitment of majors for CS and IT
- Awareness
- Big picture
- Little picture

OUTLINE

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

DISCUSSION

Questions?

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

http://www.raymondgreenlaw.com