Computer Security Curriculum at the Univ. of Wisconsin – Eau Claire

Paul J. Wagner
wagnerpj@uwec.edu
Background

- Attended week-long workshop at Indiana University of Pennsylvania in 2002 with colleague Andy Phillips
- Generated NSF Course, Curriculum and Laboratory Improvement (CCLI) Adaptation and Implementation (A&I) proposal to develop a computer security lab, two courses (Computer Security, Cryptography/Network Security), and security modules to be used in other courses
- Proposal was approved, grant funded 2003-2005
- Results:
  - 8-station Windows/Linux security lab created
  - Both courses developed
  - Approximately 10 modules developed for use in CS1, CS2, Architecture, Software Engineering, Database Systems, etc. classes
Computer Security Course - Overview

- **Course**
  - Computer Security (CS 370)
  - Prerequisite – Data Structures (CS 265)

- **Goals for course**
  - Develop understanding and background in:
    - Concepts / Principles
    - Tools
    - Ethics

- **Approach from perspective of security professional**
  - Learn as defenders of computer systems and networks
  - Look at what attackers do to understand their mindset and methods
  - Systems approach in an enterprise environment

- **Students sign an agreement that stresses ethical issues and behavior, limits their use of tools to scope of course**
Computer Security Course – Overview (2)

- **Topics**
  - Introduction, Central Principles/Concepts, Risk Analysis, Policies
  - Ethical/Privacy/Legal Issues, Social Engineering; System Mgmt.
  - Networking Basics, Network Hardware and Concepts
  - Firewall Configuration, Collecting Information
  - Packet Sniffing, Port Scanning
  - Passwords/Cracking, Cryptography Basics
  - Secure Application Development, Vulnerability Analysis
  - Types of Attacks, Malware, Access Control
  - System Hardening
  - System Logs, Intrusion Detection and Prevention Systems
  - Disaster Recovery/Forensics, Physical Security, Email Security
  - Operating System /Web / Database System Security
  - Cyberwar Lab Exercise
  - Presentations on Current Security Issues
Computer Security Course - Content

- Weekly Written Exercises
  - Policies
  - Ethics, Social Engineering

- Weekly Laboratory Exercises
  - Information Gathering Tools (general OS tools, Sam Spade)
  - Packet Sniffing (ethereal/wireshark)
  - Port Scanning (nmap/SuperScan 4)
  - Password Security/Analysis (john the ripper, SamInside)
  - Vulnerability Assessment (nessus, Nessus for Windows)
  - System Hardening (bastille, tripwire, MS Baseline Sec. Analyzr.)
  - Intrusion Detection (snort)

- Programming Assignments (Java)
  - Cryptography with Java Cryptography Extensions (JCE)
  - Secure Communication with SSL / Java Secure Socket Ext. (JSSE)
Changes Based on UMSSIA 2007

- No new sections / topics / modules, but…
- Significantly expanded content in many listed modules based on UMSSIA content
- Lab exercises modified / being further modified to use some material gained from UMSSIA 2007 labs; e.g.
  - OWASP.org
  - pfSense open source firewall
Computer Security Course – Final Cybersecurity Exercise

■ Goals
  ● Real-World Project
  ● Team-Based
  ● Focus on Defense in a Realistic Environment
    ✦ Defense – understand what needs to be done and how to accomplish it
    ✦ Attack – to experience the mindset and techniques of the attacker
  ● Gain Experience in:
    ✦ Technological security – with tools used in weekly labs
    ✦ Physical security
    ✦ Social security
The Cyberwar Exercise (2)

Exercise Structure

- Pre-lab
  - Set up heterogeneous isolated network
  - Group students into teams
  - Teams discover exact environment (shortly before exercise starts)

- Defense Period
  - Teams secure Linux and Windows systems within constraints of exercise
    - No major upgrades of OS allowed
  - Must keep certain services available; e.g. ssh, http, file share, 3rd party application
  - 24 hours
The Cyberwar Exercise (3)

Exercise Structure (cont.)

- **Attack period**
  - Teams footprint network, other team systems, “bait” systems
  - Teams attempt to plant flag on as many systems on network as possible
  - Defense continues (adjustments, further work)
  - Systems Staff attempt seven attacks against student systems using Metasploit
  - Points given for keeping services up, footprinting, exploits, documentation
  - 24 hours

- **Report/Evaluation/Discussion**
  - Student teams keep log on patches, defensive steps, attack techniques, tools used, issues, problems
    - Useful to the students and the instructor
  - Whole class discussion after exercise completed
Original Laboratory Setup

**Physical Structure**

- **8 physical host machines (Windows XP)**
  - Can be used for general purpose work by other students, as network is connected / switched
- **Each host machine has two VMWare client images**
  - Fedora Core 4 (Linux)
  - Windows Server 2003 (Windows)
- **Client images run using VMWare Player (free)**
- **Students given root/administrator access on each client system**
- **Other VMWare images added to network as “bait” systems for exploration**
  - Run on VMWare Server
Original Laboratory Setup (2)

- Cybersecurity Exercise
  - Same lab, except:
    - Switch flooded to create hub-like environment
    - Lab network isolated from campus network
    - More bait machines added
Laboratory – Original (Now Using VMWare)
Laboratory Evolution 2008-on

- Laboratory was only used for Computer Security each spring semester
  - Dedicated usage (off-limits to other students) only for 3-day period around Cybersecurity exercise
- VMWare images have been made available in all three labs
  - Work not limited to our Security lab
- Space shortage in our Science building
  - Expansion of materials science / nanotechnology staff, others
- All of above factors have lead to reassignment of our lab starting 2008-2009 school year
- Changes necessary....
Laboratory Evolution 2008-on (2)

- Regular laboratory exercises will be done in other two computer science labs
- Cybersecurity exercise options:
  - In one of these labs
  - In another room, using portable laboratory/workshop technology that we’ve developed
    - Developed portable computer security workshop based on supplemental NSF CCLI grant
      - Offered at SIGCSE 2005, 2006, 2007; again in 2009?
    - Used laptops, cabled network, switch, VMWare, custom scripts and programs to quickly distribute images to network systems, execute commands on any participating system
    - CCLI phase 2 proposal submitted to further develop this portable laboratory system in general; wireless, use participant laptops by bringing in our virtual system from portable storage.
Cryptography / Network Security Course

Content (Selected Topics)

- Network Basics
- Historical Substitution and Transposition Ciphers
- Mathematical Background for Cryptography
- Feistel Networks, Symmetric Key Systems (DES, AES, Triple DES, Blowfish, etc.)
- Pseudo-random and random number generation
- Public Key Cryptography and Key Exchange (RSA, Diffie-Hellman, Elliptic Curve systems)
- Secure (and not so secure) Hashing (MD4, MD5, SHA1, etc.)
- Digital Signatures
- Network security (Kerberos, X-509 Certificates)
- Email Security
Security Course Modules

- **Examples**
  - RSA Implementation (CS1 (Java), Scientific Computing (Maple))
  - RC4 Implementation (Scientific Computing (Maple))
  - SDES Implementation (Scientific Computing (Maple))
  - Steganography (CS1 (Java))
  - Spam Filter (CS1 (Java))
  - Database Security (Database Systems)
  - Buffer Overflows (Computer Architecture)
Our systems and networking staff
- Very difficult and time-consuming to do this without them!

Dr. Andrew Phillips, UW-EC
- Co-PI on our NSF CCLI A&I Grant

CLICS – a Computational Laboratory for Information and Computer Security
- Development of Physical Lab, Courses, and Modules
- Supplemental Grant: Develop 2 3-hour hands-on computer security workshops (condensed version of labs/cybersecurity)
- More information: http://clics.cs.uwec.edu
- Supported by NSF Grant, DUE 0309818