ECE 8484 Fall 2013

Jim Solderitsch

Syllabus Outline

Proposed

Draft Syllabus 1

- Introduction
  - Class, audience, approach
  - Intro to Cyber Security
    - Jim Solderitsch's view
    - CompTIA Security+ View
- State of CyberSecurity
  - Selected vendor viewpoints
  - User recommendations
    - NSA
    - US CERT
- Threats, Vulnerabilities, Malware
  - Highlight Web Application vulnerabilities
  - APTs and Insider Threat
- Attacks and Methods
  - Tactics, Techniques and Procedures (TTPs)
  - Examples: Stuxnet, Phishing, Botnets

Draft Syllabus 2

- Defenses
  - Approaches
  - Levels
  - Product Families
    - SIEM, DLP, GRC
- Security Operations Center (SOC)
- Examples
  - Phishing
  - Endpoint Protection
  - Intrusion Detection/Prevention
- Solution Examples (Demos)
  - Endpoint Protection (which vendor?)
  - Seamless Virtualization
  - SIEM: OSSIM
  - DLP: MyDLP
  - GRC: Archer or Agiliance

Draft Syllabus 3

- Web Security: concepts and issues
  - Browser security model
  - Session Management and Authentication
  - SSL/HTTPS
  - Web Application Security
- Introduction to Penetration Testing
- Hands-on Samurai WTF
- Security Business and Services
  - Application Security Testing
    - Static and dynamic analysia
    - Whitebox and Blackbox application scanning (including as a Service)
  - Threat and Vulnerability Management
    - Includes commercial grade Pen Testing
- Secure by Design
  - Engineering principles for Secure Development
    - SABSA and COBIT
    - Privacy by Design
    - Concepts in Trusted Computing

Draft Syllabus 4

- Security Issues and Cloud Computing
  - Survey of cloud computing practices and security implications
- Security Issues and Critical Infrastructure Protection
  - Industrial Control Systems (ICS)
  - SCADA: Supervisory Control and Data Acquistion
  - Issues for the Electricity Grid including Smart Meters/Grid
- Security Issues for mobile and wireless computing and devices
  - Mobile platforms: attack and defense
  - Data Protection and Privacy
  - Wireless transmission
- Identity and Access Management (IAM)
- Security Issues for/with social media usage and platforms
- Next Generation Security Operations
  - Big Data Analytics for Security
  - Security of Big Data Platforms
  - Active Defense
  - Internet of Things (IoT)

Evaluation Methods

- Quizzes – planning 10 over course of semester
  - 10 points per quiz (total: 100 points)
  - Short answer/multiple choice
  - Modeled on Coursera approach
- Final Exam
  - Possibly conducted through Blackboard
    - Timed
    - Comprehensive over semester
    - Some short answer (half of exam) – 50%
    - Some essay – 50%
  - 100 points
- Other ??
  - Blog posts
    - Both as originator and as comment provider to others
    - Contributions will be graded for quality/clarity/contribution
  - Presentations/short papers
    - First on selected Blackhat or Defcon presentation
    - Second on topic of student's choice
      - Suggestions will be provided
      - Can be implementation or case study of tool/technology
  - 100 points