ECE 8484 Fall 2015

Jim Solderitsch

Syllabus Outline

Subject to Variation

Working Syllabus 1

- Introduction
  - Class, audience, approach
  - Intro to Cyber Security
    - Jim Solderitsch's view
    - Text Book View (included ISC^2 Course Material for SSCP certificate)
- 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

Working 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: Symantec DLP
  - GRC: Archer or Agiliance

Working Syllabus 3

- Web Security: concepts and issues
  - Browser security model
  - Session Management and Authentication
  - SSL/HTTPS
  - Web Application Security
- Introduction to Penetration Testing (Virtual labs provide some of this)
- Hands-on Samurai WTF, Security Onion, Kali Linux
- 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

Working 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 Acquisition
  - 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) – Text covers this in several places
- 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 5 over course of semester
  - 10 points per quiz (total: 50 points)
  - Short answer/multiple choice
  - Questions from text material and topics covered in class or selected readings
- Final Exam
  - Conducted through Blackboard
    - Comprehensive over semester
    - Some short answer (half of exam) – 50%
    - Some essay – 50%
  - 100 points
- Other
  - Virtual Labs included with text materials
    - 5 required: tentative selection: Labs 1, 2, 5, 8 and 10
    - Contributions will be graded based on submitted materials as required per lab
    - 20 points per lab (total points: 100)
  - CyberSecurity research paper OR Completion of labs 3, 4, 6, 7, 9
    - Paper topic choice is up to the student (recommend Black Hat or Defcon 2015 presentations) – details to follow
    - 50 point for completed paper or 10 points per each completed lab
- Total points for course: 300
  - Probable grade dividing lines A: 93 and above, A-: 90, B+; 86, B: 83, B-: 80, C: 70 (hope no one lands here!)
  - Expect to be somewhat flexible, but…