Module 0.5

Learning Objectives

Content of this Course

Part 1: Basics (architecting for security)

• Securing apps, OS, and legacy code
Isolation, authentication, and access control

Part 2:   Web security   (defending against a web attacker)

• Building robust web sites, understand the browser security model

Part 3: Network security   (defending against a network attacker)

• Monitoring and architecting secure networks

Course Content (cont.)

Part 4: Mobile security

- Android Security

Part 5: Critical Infrastructure Security

- Security of Industrial Systems

What is Security?

- Achieving something in the presence of adversaries
  - Internet is full of adversaries
  - There are insider adversaries for air-gapped systems
  - Thus design of systems need to worry about security

Major Learning Objectives

- Discover software bugs that pose cyber security threats
  - explain and recreate exploits of such bugs in realizing a cyber attack
  - explain how to fix the bugs to mitigate such threats

Major Learning Objectives (2)

- Discover cyber attack scenarios to web browsers, and web servers
  - explain various possible exploits
  - recreate cyber attacks on browsers and servers with existing bugs
  - explain how to mitigate such threats

Major Learning Objectives (3)

- Discover and explain cyber security holes in standard networking protocols
  - both in network architecture, standard protocols (such as TCP/IP, ARP, DNS, Ethernet, BGP etc),
  - explain mitigation methods and revisions of standards based on cyber threats.

Major Learning Objectives (4)

- Discover and explain mobile software bugs posing cyber security threats
  - explain and recreate exploits
  - explain mitigation techniques.

Major Learning Objectives (5)

- Articulate the urgent need for cyber security in critical computer systems
  - explain various threat scenarios

Major Learning Objectives (6)

- Articulate the well known cyber attack incidents
  - explain the attack scenarios
  - explain mitigation techniques

Major Learning Objectives (7)

- Explain the difference between
  - Systems Cyber Security
  - Network Cyber Security,
  - Cryptography
  - crypto-protocols etc.