EEL 4347 — Introduction to Cybersecurity


Course (Catalog) Description:  The course will cover an introduction to the most important features of computer security, including topics such as symmetric ciphers, basic number theory, public key cryptosystems, digital signatures, hashes, message authentication codes, key management and distribution, authentication protocols, vulnerabilities and malware, access control, network security.

Prerequisite:  C/C++ Programming and EEL-3705


Course Objectives:

1. Distinguish the broad set of technical, social & political aspects of cybersecurity.
2. Describe the vulnerabilities and threats posed by criminals, terrorist and nation states to national infrastructure.
3. Relate the nature of secure software development, operating systems and data base design.
4. Interpret security guarantees. Assess the level of security provided by a cryptographic protocol.
5. Identify the role security management plays in cybersecurity defense.
6. Explain common vulnerabilities in computer programs, including buffer overflow vulnerabilities, time-of-check to time-of-use flaws, incomplete mediation.
7. Identify the security management methods to maintain security protection.
8. Discuss the legal and social issues at play in developing solutions.
9. Apply theoretical concepts in practice by using a programming language to implement attacks and defenses against computer systems.

Topics covered:

1. Overview, security mindset, ethics, design principles, threat modeling, attacks, defenses.
2. Basic tools in computer security (authentication, access control).
3. Basic tools in computer security (cryptography: symmetric and asymmetric crypto primitives).
4. Program security (non-malicious programming oversights).
5. Program security (malicious code, malware, countermeasures).
6. Web security (browser attacks, web attacks targeting users, obtaining user/website data, email attacks).
7. Review and Midterm.
8. Operating systems (permissions in Windows/Unix, security in the design, rootkits).
9. Network security (basic internet technology, denial of service, wireless security, crypto, firewalls, IDS/IPS).
10. Databases (security requirements, reliability, integrity, disclosure).
12. Hardware security (types of vulnerabilities and attacks, hardware Trojan prevention and detection, malicious hardware).
13. Cyber-physical systems security (definition and instances of CPS, vulnerabilities and attacks, defenses).
15. Management and incidents (security planning, handling incidents, risk analysis, dealing with disaster) + Emerging topics (cyber warfare).

Class Schedule: Three 50 minute or two 75 minute lectures per week (3 credit hours).

Subject Area: Engineering

Significant Design: No

Relationship to Assessed ABET Student Outcomes: None

Last Updated by: R.J. Perry Date: 4/30/2021