CSE466: Computer Systems Security – Syllabus (Fall 2016)

Web page: Linked to http://cactus.eas.asu.edu/partha (also check the link for Class Policies)

Catalog Data:
Countermeasures to attacks to computer systems from miscreants (or hackers) and basic topics of cryptography and network security.

Textbook:
None

Course Objectives
The structure and operating of software systems that allow "hackers" to penetrate and malware to operate. A comprehensive study of vulnerabilities, object-code level attacks, security measures, software shortcomings and forms of attacks and countermeasures.

Course Outcomes:
After the course the student will be able to:

1. Understand the underlying vulnerabilities of systems from a software standpoint.
2. Understand the structure of bits and bytes, data and programs, stored at the object code level in memory and files.
3. Understand the basic of cryptography and computer security.
4. Understand the techniques used to hack into computer systems.
5. Understand the concepts "secure programming".
6. Understand how to program and deploy countermeasures for keeping software systems secure

Evaluation:
Students are assessed on grades received in projects, homeworks, exams. The grades are "curved" for determining grade cutoff points on an A, B, C scale. The weight distribution is Assignments: 35%; Mid-Term Exam: 30%; Final Exam: 35%. There will be **no makeup**, such as extra credit work, extra credit exams and/or other methods beyond what all students are expected to do. Extra credit warps class rankings.

Academic Integrity: You are responsible for understanding what constitutes academic dishonesty. No tolerance policy will be in effect and a grade of F or XE will be awarded and a report will be filed with Fulton School. Please refer to https://provost.asu.edu/files/AcademicIntegrityPolicyPDF.pdf for details -- also please note item N on Page 2.

Topics:

1. Risks and Trust

- Risks of Computer Systems

- Vulnerabilities and System Design
- How to steal information
- Basics of Attacks
- The Shared Secret Problem

2. <u>Threat Models</u>

- Internet Threat Model
- Ken Thompson and Software Trust
- Viral Threat Model

3. <u>Attacks</u>

- Attack Mechanisms
- System attacks and Network Attacks
- Virus, Trojan, Worms, Spyware, Adware, Browser attacks
- Buffer Overflows
- The “RootKit” Attack
- Malicious processes and computational power
- Network based attacks (man in the middle, denial of service, pharming)

4. <u>Data and Code Formats</u>

- How memory is organized
- Code, data and other in-core structures
- How the computer operates at the binary level
- Binary and I/O conversions
- File data and how data movement occurs

5. <u>Basic Cryptography</u>

- Random numbers, Cryptographic Hashes
- Symmetric Encryption
- Asymmetric Encryption
- Digital Signatures
- Digital Certificates
- Certificate Authorities and Certificate Chains
- Secure Sockets Layer (SSL) and IPSec

6. <u>Safe Programming Techniques</u>

- Coding practices and safety
- Code bloat and safety
- Feature Creep
- Versatility and Vulnerabilities
- Overall Design of Complex Systems

7. <u>Operating System Mechanisms</u>

- Identity and Authentication

- Protection in Operating Systems
- Interrupt handlers and System calls
- Redirecting services
- Reliable bootstrap, Address space protection

8. Virtual Machine Systems

- Types of Virtual Machines
- How they work
- Host Operating Systems and VMM interactions
- Trust and Virtual Machines
- Using Virtual Machines for Integrity Enforcement

9. Hardware Security Enforcers

- Trust and Hardware Modules
- The TCG approach
- The CoPilot approach
- Secure wallets
- Secure co-processors

10. Application Security

- Firewalls
- Virus Detection
- Fallibility of Virus detection
- Signatures and Software
- Integrity checking of software
- Combining schemes to harden the software environment

11. Personal Security

- How safe is your information?
- What is valuable to others?
- Protecting privacy
- Protecting finances
- Repudiation, spoofing and identity theft
- Devices for personal safety and identity

12. Smart Card Systems

- Types of Smartcards
- Personal Security and Smartcards
- Risks and Vulnerabilities of Smart Cards
- Financial Transactions
- Mobile Authentication
- System verification
- Trust model

Further Information: Will be provided on the class web-site.

Title IX is a federal law that provides that no person be excluded on the basis of sex from participation in, be denied benefits of, or be subjected to discrimination under any education program or activity. Both Title IX and university policy make clear that sexual violence and harassment based on sex is prohibited. An individual who believes they have been subjected to sexual violence or harassed on the basis of sex can seek support, including counseling and academic support, from the university. If you or someone you know has been harassed on the basis of sex or sexually assaulted, you can find information and resources at http://sexualviolenceprevention.asu.edu/faqs/students.