EEC 693/793 Network Security & Privacy II

Instructor: Dr. Ye Zhu
Office: SH 433
Phone: 216-687-9749
Email: y.zhu61@csuohio.edu
TA: TBD (Will be Announced in Blackboard)
Class Hours: Monday/Wednesday 4:00pm -5:50pm
Office Hours: Monday/Wednesday 3pm-5pm or by appointment
Class Room: SH309
Class Website: http://academic.csuohio.edu/webct/
Prerequsite: EEC584

The course focuses on system aspects of network security and privacy. We will first review fundamentals of the theory aspects of network security and privacy including symmetric cipher, asymmetric ciphers, key management, and signatures. After the review, we continue on system security and privacy. The topics covered include reconnaissance, common security attacks at each layer and defense mechanisms, real-time communication security and privacy, traffic analysis attacks, virus/worms, DDoS attacks and countermeasures, email security, and anomaly detection. If time permits, we will also discuss advanced topics in network security and privacy area such as anonymous communication and security of wireless sensor networks.

No textbook is required. However it is highly recommended to purchase a copy of the reference book listed below by William Stallings. We will follow the reference book for the first half of the course. A set of research papers will be assigned for the second half of the course. There will be four homework assignments and one term project. The assignments are due on the designated due dates at midnight. **No late submissions will be accepted.** Please discuss unusual circumstances **in advance** with the instructor.

An open-book midterm examination will be scheduled in the middle of semester. There is no final examination.

Textbook:

No textbook is required.

Reference book:

Cryptography and Network Security, Fourth Edition by William Stallings

Network Security - Private Communication in a Public World by Charlie Kaufman, Radia Perlman, Mike Speciner

Network Algorithmics, 1st Ed. (2004), by George Varghese

Building Resilient IP Networks, 1st Ed. (2012), by Kok-Keong Lee and Beng-Hui Ong

Grading:

30% Homework, 30% Midterm, 40% class project (10% for presentation)

Scholastic Dishonesty: Scholastic dishonesty will not be tolerated. Examinations are meant to measure the knowledge or skill of each individual, so giving or receiving unauthorized assistance during tests and quizzes is cheating. It is assumed that college students know what is honest and what is not. Any identified instances of scholastic dishonesty will be dealt with in accordance with the procedures outlined in the university student rules.

Students with Disabilities: The Americans with Disabilities Act is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodation of their disabilities. If you believe you have a disability requiring an accommodation, please contact the Department of Student Life or call 687-2048.

What am I supposed to know before taking this course

EEC 484/584 Computer Networks or equivalent.

I will be assuming that you have knowledge on the following subjects. If you feel unfamiliar with the following topics, please refresh your memory. Some of the following topics will be briefly reviewed in class.

- computer networks (TCP/IP, UDP, FTP, Telnet …)
- distributed systems (RPC, NIS, NFS …)
- basic knowledge of statistical analysis (common distributions, mean, variance …)
- system administration (Windows and Linux/Unix)
- classical cipher
- symetric cipher (DES, AES)
- asymetric cipher (RSA)
- key management

Course Goals

By the end of this course, students will be able to

- List the common threats and vulnerabilities of networked systems
- Describe the network security goals, existing network security mechanisms and services
- Design defense systems to protect different services
- Understand fundamentals of contemporary cryptography and its application to network services, such as confidentiality, integrity, authentication, and non-repudiation
- Identify flaws in network protocols
- Design firewall configurations and rules to protect a given network
- Explain the basic concepts and general techniques in security auditing and intrusion detection
- List common security attacks and correspondent countermeasures