EEC 693/793 Network Security & Privacy I

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: Online
Office Hours: Monday/Wednesday 1pm-3pm or by appointment
Class Room: Online
Class Website: http://academic.csuohio.edu/webct/
Prerequsite: EEC584

The course covers the theory aspects of network security and privacy. We will begin the course with classical ciphers. Based on the understanding of the classical ciphers, we continue with the fundamentals of contemporary cryptography and its application to network services, such as confidentiality, integrity, authentication, and non-repudiation. The topics covered in the course include security architectures, modern block ciphers/symmetric ciphers, asymmetric ciphers, key management, ECC, linear cryptanalysis, differential cryptanalysis, message authentication, hash functions, and digital signatures. Three lectures on applied math such as finite field, related theories in number theory, and statistics are also included in the course to prepare you for better understanding of theoretical background of modern ciphers and cryptographic protocols. If time permits, we will discuss advanced topics in theory aspects of network security and privacy area such as honey encryption and threshold cryptosystem.

It is highly recommended to purchase a copy of the text book listed below by William Stallings. We will follow the text book for the most of the course. A set of research papers will be assigned for advanced topics if time permits. 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.

A close-book midterm examination will be scheduled in the middle of semester. The final examination is comprehensive. In other words, the final exam

covers course material taught from the beginning of semester.

Textbook:

Cryptography and Network Security, Fourth Edition by William Stallings

Reference book:

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

Grading:

25% Homework, 25% Midterm, 25% Final Exam, 25% class project (5% 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)

Course Goals

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

- Describe the network security goals, existing network security mechanisms and services
- Understand fundamentals of contemporary cryptography and its application to network services, such as confidentiality, integrity, authentication, and non-repudiation
- Identify flaws in cryptographic protocols
- List common security attacks on cryptosystems and correspondent countermeasures
- List the requirements and mechanisms for identification and authentication. Identify the possible threats to each mechanism and ways to protect against these threats.