Introduction to Network Security

CS 478 / ECE 478 (Spring 2016)

Syllabus

1. Course Information:

Instructor: Dr. Attila Altay Yavuz,
Office: KEC 3065
Phone: 541-737-3341
Email: Attila.Yavuz@oregonstate.edu
URL: http://web.engr.oregonstate.edu/~yavuza/
Classroom: CORD 3121
Class Hours: TR 10:00 AM – 11:20 AM
Office Hours: Monday 5:00 PM – 6:30 PM at KEC 3065
TA: Mr. Daniel Lin Tzu
TA Email: lintzu@oregonstate.edu
TA Office Hours: Wednesday 2:00 PM - 4 PM, Friday 2 PM - 4 PM at KEC Atrium

2. Course Content and Objectives:

This course covers basic concepts and techniques in network security such as risks and vulnerabilities, applied cryptography and various network security protocols. This course focuses on essential security services such as authentication, confidentiality, integrity, and availability applied to networking systems. This course also explores fundamental techniques including authentication protocols, group key establishment and management, trusted intermediaries, public key infrastructures, SSL/TLS, IPSec, firewalls and intrusion detection.

Course content:

• Basic network security services and their properties
• Basic Cryptographic Building Blocks: Properties of symmetric encryption, cryptographic hash functions, essential intractability assumptions and number, theoretical tools (e.g., extended Euclid, generators).
• Authentication fundamentals: OTSs, hash-chains, MHT, Schnorr, DSA, RSA signatures
• Encryption Fundamentals: DH, El-Gamal Encryption, RSA-PSS
• User authentication
• Security pitfalls, reflection attacks, nonces and protocol examples
• Trusted Intermediaries, Needham-Schroeder, Otway-Rees
• Kerberos, Public Key Infrastructures (PKIs)
• SSL/TLS and IPSec, X.509, STS
• Key management techniques (e.g., Iolus, Logical Key Hierarchy, Group-DH)
• Secure audit logging, (optional) compromise-resilient cryptography
• Secure Cloud Computing
• Privacy Enhancing Technologies such as Searchable Encryption
• Discussion on advanced building blocks (e.g., SCRA, ORAM)

3. Learning Resources:

• Slides, notes and research papers will be provided during the term (check the course website regularly for updates).
• Douglas R. Stinson, “Cryptography Theory and Practice, 3rd edition”.
• Jonathan Katz & Yehuda Lindell, “Introduction to Modern Cryptography”.

The above textbooks are not required, but just recommended as a learning resource.

4. Coursework and evaluations:

• Homework assignments (40%)
• Midterm (25%)
• Final (30%)
• Attendance/participation (optional quizzes) (5%)
• Optional extra credit assignments, potentially in the form of quizzes, scouting and/or research projects

Remarks:
(i) The above grading rule may be changed during the quarter.
(ii) Homeworks and all reports (e.g., extra credit projects, survey/scouting reports) must be typed using a text editor (very preferably with Latex, but Word is ok). Handwritten deliveries will not be accepted.
(iii) All deliveries must be submitted online via TEACH system no later than given deadline.
(iv) Midterm, final and homework dates cannot be changed based on personal or group requests (e.g., a change request for a job interview, business travels, wedding/invitation/social events, other course assignments, or personal matters).

5. Schedule of Assignments:

The scheduling of assignments and requirements are announced at the course website (and updated if required). Late homework will not be accepted (with the exception of critical
circumstances, but never after the solution is posted. A 30% reduction in grade for each day applies for such exceptional extensions).

6. Policies on incomplete grades and late assignments:

Late homework assignments are not accepted (see below for the expectation).

7. Policies on absences (excused/ unexcused) and scheduling makeup:

There will be no makeups for final exam and/or optional survey/research projects. Only exceptions is possible for homework assignments and midterm, if a student presents a police report or a formal doctor's note that show some emergency situation.

8. Course prerequisites:

CS 372 is required. CS370 and a basic understanding of computer networks and security mechanisms are recommended.

9. Academic integrity:

The university policies against academic dishonesty will be strictly enforced. Evidence of academic dishonesty in this course may result in a grade of "F" on the examination/assignment that involved cheating and/or an "F" in the course (for more details see http://ecampus.oregonstate.edu/services/proctoring/academichonesty.htm).

The instructor expects a student to complete his/her homework, projects and assignments without violating academic Integrity. A student's submission on any homework, projects and assignments indicates that the student neither gave nor received unauthorized aid.

10. Accommodation of Disabilities

Accommodations are collaborative efforts between students, faculty and Disability Access Services (DAS). Students with accommodations approved through DAS are responsible for contacting the faculty member in charge of the course prior to or during the first week of the term to discuss accommodations. Students who believe they are eligible for accommodations but who have not yet obtained approval through DAS should contact DAS immediately at (541) 737-4098.

REMARK: Every part of this syllabus and course website (including the course scheduling and assignments) are subject to adjustment as the term progresses. If you have concerns, please contact with the instructor.