CS/ECE 578 – Cyber-Security (Fall 2017)

Syllabus

1. Course Information:

Catalog Description: A broad overview of the field of computer & network security,

Instructor: Dr. Attila Altay Yavuz,
Classroom: ROG 230
Email: Attila.Yavuz@oregonstate.edu
URL: http://web.engr.oregonstate.edu/~yavuza/
Class Hours: MW - 14:00 – 15:20 PM

Course Content:

- Introduction to computer security: (1 lecture)
  ○ security topics, security properties, security principles
- Symmetric-key Cryptography: (4 lectures)
  ○ hash functions, birthday bounds
  ○ block ciphers and modes
  ○ CPA/CCA security definitions for encryption
  ○ message authentication vs confidentiality
- Public-key Cryptography: (4 lectures)
  ○ RSA encryption & signatures
  ○ Diffie-Hellman key agreement
  ○ Public-key infrastructures and X.509
  ○ DSA and Schnorr signatures
- Network Protocols: (4 lectures)
  ○ Authentication Protocols and Pitfalls:
    ■ Common security pitfalls/countermeasures (reflection attack, nonces, time stamp, low-entropy randomness)
    ■ Needham-Schroeder, Otway-Rees, Kerberos authentication protocols
  ○ Network & transport layer security:
    ■ TLS, SSH, IPsec
- System Security: (3 lectures)
  ○ Access control paradigms (DAC, MAC, RBAC)
  ○ Denial of service attacks and mitigations
- Broad Topics with Guest Lectures (6 lectures, topics depend on guest and/or co-designing instructor; sample topics listed below):
  ○ Privacy enhancing technologies (e.g., searchable encryption),
  ○ Secure computation techniques (e.g., garbled circuits),
  ○ Trusted computing, OS and hardware-security,
  ○ Cloud security
Learning Resources:
- Jonathan Katz & Yehuda Lindell, “Introduction to Modern Cryptography”.
- Mike Rosulek, lecture notes on cryptography (available free online)
- Slides and Lecture Notes

Measurable Student Learning Outcomes:
At the completion of the course, students will be able to…
1. Understand the main principles of computer and network security, cryptography and their role in providing security/privacy guarantees for computer systems,
2. Apply authentication, identification, key management techniques and security protocols to network and computer systems
3. Critically evaluate network security protocols, cryptographic constructions and computer security tools, identify security weaknesses / vulnerabilities
4. Assess security requirements of applications and systems and select cryptographic tools that are appropriate
5. Describe common threats and attacks toward computer networks, their implications and preventions

Credits: 4

Prerequisites: Graduate standing

Courses that require this as a prerequisite: Advanced graduate courses on cyber security topics (including cryptography, applied cryptography, network security and system security --- to be given permanent course numbers) will require this as a pre-requisite unless the students have previously taken undergraduate level security and cryptography courses.

2. Learning Resources:

No textbook is required. Handouts (i.e., lecture slides) and reading papers will be provided during the term (check the course website regularly for updates). However, some optional books that may be useful, includes but are not limited to:
- Jonathan Katz & Yehuda Lindell, “Introduction to Modern Cryptography”.

3. Coursework and evaluations:
- homework (45%): 3 or 4 substantial problem sets
- Exams (50%): 1 midterm + 1 final exam
- In-class participation (5%)
- Optional assignments for extra-credit are possible
4. Schedule of Assignments:

The scheduling of assignments and requirements are announced at the course website (and updated if required).

5. Policies on incomplete grades and late assignments:

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

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

There will be no makeups for mid-term, final and assignments. Only exceptions is possible, if a student presents a police report or a doctor's note that show some emergency situation.

7. Student with disabilities

Accommodations for students with disabilities are determined and approved by Disability Access Services (DAS). If you, as a student, believe you are eligible for accommodations but have not obtained approval please contact DAS immediately at 541-737-4098 or at http://ds.oregonstate.edu. DAS notifies students and faculty members of approved academic accommodations and coordinates implementation of those accommodations. While not required, students and faculty members are encouraged to discuss details of the implementation of individual accommodations.

8. 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/academicintegrity.htm).

The instructor expects a student to complete his/her homework 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.

Link to Statement of Expectations for Student Conduct, i.e., cheating policies http://oregonstate.edu/studentconduct/offenses-0