CS 478 / ECE 478 – Network Security

Catalog Description: Basic concepts and techniques in network security, risks and vulnerabilities, applied cryptography and various network security protocols. Coverage of high-level concepts such as authentication, confidentiality, integrity, and availability applied to networking systems. Fundamental techniques including authentication protocols, group key establishment and management, trusted intermediaries, public key infrastructures, SSL/TLS, IPSec, firewalls and intrusion detection.

Credits: 4  Terms Offered: Spring

Prerequisites: (CS 372 or ECE 372) and (CS 370 recommended)

Courses that require this as a prerequisite: None

Structure: On campus, two 80-minute lectures per week

Instructors: Attila Altay Yavuz

Course Content:
- Basic network security services and their properties
- Authentication fundamentals: OTSs, hash-chains, MHT, DSA
- Security pitfalls, reflection attacks, nonces and protocol examples
- Authentication tokens, per-session keys
- Trusted Intermediaries, Needham-Schroeder, Otway-Rees
- Kerberos, Public Key Infrastructures (PKIs)
- SSL/TLS and IPSec
- Key management techniques (e.g., Iolus, Logical Key Hierarchy, Group-DH)
- Firewalls and intrusion detection
- Secure audit logging, (optional) compromise-resilient cryptography

Learning Resources:
- Jonathan Katz & Yehuda Lindell, “Introduction to Modern Cryptography”.
- 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 network security and its role in providing security/privacy guarantees
2. Apply authentication, identification, key management techniques and security protocols to protect network and computer systems
3. **Critically evaluate** network security protocols and cryptographic techniques and **identify** security weaknesses/vulnerabilities
4. **Assess** security requirements of network and software applications, **select** security/crypto tools that are appropriate
5. **Describe** common threats and attacks toward computer networks, their implications and prevensions

**Evaluation of Student Learning:**
- Homework (approx. 40%)
- Reports/projects or quizzes (approx. 20%)
- Exams (approx. 40%)

**Students with 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 737-4098.

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

Revised: Winter 2015