ECE 478 – Network Security

Catalog Description: Security principles, models, and attacks. Overview of cryptography. Building secure systems and security evaluation criteria. Security in operating systems and computer networks. Management and analysis of security. Legal and ethical issues in computer security.

Credits: 4 **Terms Offered:** Spring

Courses that require this as a prerequisite: None

Structure: Varies; typically three 50-minute lectures per week

Instructors: M Rosulek

Course Content:

- Common web application vulnerabilities, including cross-site scripting attacks, SQL injection attacks, cross-site request forgery.
- Basics of applied cryptography: block ciphers & modes for achieving privacy; hash functions & MACs for achieving authenticity.
- Password-based security: authentication, rainbow tables, salted hashing
- Securing the internet protocol stack: IP/IPsec, DNS/DNSsec, SSL/TLS, man-in-the-middle attacks, ARP poisoning attacks
- Anonymity: mix-nets and Tor
- Advanced topics, guided by the students' selection of final projects

Measurable Student Learning Outcomes:

At the completion of the course, students will be able to…

1. **Explain, identify,** and **write software that avoids** the most common vulnerabilities of networked web applications (ABET Outcomes: a, b, c, e, k)
2. **Compare/contrast** different standard cryptographic tools and **identify** which tools are appropriate for common security tasks (ABET Outcomes: a, c, e)
3. **Describe** the threat/trust model and attack surface of a networked system (ABET Outcomes: a, e, g, j, k)
4. **Describe** the limits of security that the most widely deployed network protocols provide to users (ABET Outcomes: a, j, k)
5. **Identify** legal and ethical implications of discovering/using network vulnerabilities (ABET Outcomes: e, f, h)

Evaluation of Student Performance:

Students will be evaluated via hands-on assignments, quizzes, and a final project that includes a written component as well as an in-class presentation of findings.

Learning Resources:

- *Cryptography & Network Security: Principles & Practice* (6th edition), by W Stallings, Prentice Hall, 2014 (optional)
- Several online resources:
  - Open Web Application Security Project (OWASP) top 10 web application vulnerabilities
  - MITRE corporation: Top 25 Most Dangerous Software Errors

Students with Disabilities:
Accommodations are collaborative efforts between students, faculty and Services for Students with Disabilities (SSD). Students with accommodations approved through SSD 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 SSD should contact SSD immediately at 737-4098.

Link to Statement of Expectations for Student Conduct:
http://oregonstate.edu/admin/stucon/achon.htm