1. Course Information:

**Instructor:** Dr. Attila Altay Yavuz,
**Office:** GBAD 103
**Phone:** 541-737-3341
**Email:** Attila.Yavuz@oregonstate.edu
**URL:** http://web.engr.oregonstate.edu/~yavuza/
**Class Hours:** MWT 2:00 PM – 2:50 PM
**Office Hours:** Monday 4:00 PM – 5:30 PM

2. Course Objectives:

This course covers essential concepts of network security, network security primitives, and authentication techniques. This course also focuses on the latest security and privacy issues in networking and computer systems. Finally, this course explores the state-of-art network security and applied cryptography research problems and solutions via literature survey and research projects.

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

1. List the common threats and vulnerabilities of networked systems
2. Describe network security primitives, including
   a. One-way hash chain, use of multiple root chains,
   b. Merkle hash tree and its applications,
   c. Bloom filters,
   d. Secret sharing,
   e. Rabin’s information dispersal,
3. Gain in-depth knowledge on various Denial-of-Service (DoS) attacks and DoS-counter measures. Important techniques include:
   a. Hash-based puzzles against connection depletion attacks
   b. Variant client-server puzzle methods
   c. Client-server puzzle outsourcing techniques based on Discrete-Logarithm Problem (DLP)
   d. Message specific puzzles for DoS resiliency in Wireless Sensor Networks (WSNs)
   e. Using broadcast environment to revert client-server puzzles via semi-trusted third parties.
4. Explain the security requirements of broadcast authentication.
5. Describe and TESLA, EMSS, and BiBa broadcast authentication protocols.
6. Explain the security requirements and challenges of Wireless Sensor Networks (WSNs).
7. Describe compromise-resiliency for WSNs, explain compact authentication methods with forward-security, use of time factor for efficiency on such systems via HaSAFSS and SU-HaSAFSS schemes.
8. Describe security and privacy requirements of power-grid/smart-grid systems.
9. Acquire in-depth knowledge on real-time authentication methods, one-time/multiple time signatures such as HORS.
10. Learn "time-valid" signature concept via TV-HORS and variant authentication methods.
11. Describe challenges to implement security on resource-limited devices and prospective solutions.
13. Learn about the impact of user behavior on internet vulnerabilities.

Survey assignments, research projects and in-class presentations will enable student to follow, evaluate and improve some of the selected topics in network security and applied cryptography domain, including but not limited to:

- Real-time authentication for time-critical applications.
- Security and privacy in energy-distribution systems (e.g., smart-grid/power-grid, vehicular networks).
- Efficient key exchange, distribution and provisioning in Internet-of-Things and Systems.
- Vehicular and Ad-hoc network security, including Car-2-Car, Car-to-Infrastructure and Intra-car network security.
- Wireless sensor network security topics such as node replication attacks, worm-wholes and false-data injection, secure code dissemination.
- Security and privacy for resource-limited devices (e.g., RFID).
- Security in telemedicine and medical devices.
- Smart-phone security.
- Design and implementation of advanced Searchable Encryption (SE) schemes for cloud computing.
- Evaluation and implementation of computation outsourcing methods for biometric applications.
- Self-certified cryptography versus identity-based cryptography and their implementation for key exchange and distributions.
- Jamming and anti-jamming techniques for wireless networks
- Usability issues, privacy in social networks

3. Text:
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).
4. Coursework and evaluations:

- Homework assignments (20%) (late homework is not accepted)
- In-class paper presentation (15%) (may be increased if two presentation is required)
- Survey/Scouting Report (20%)
- Research project (40%) (extra credit is possible, may supersede survey/scouting report)
- Class attendance, participation/discussions (%5)

Possible topics for survey/scouting report and research projects will be announced at course website. Students either select one of those topics or come up with their own idea (always very welcomed!). Depending on the topic, students may forge a team with two/three person, or work individually (the scope will be adjusted accordingly).

It is possible that student(s) may just assume a research project without having separate survey assignment (i.e., research project will include a “related work section”. This possibility will be decided based on objective/scope of the research project and one-on-one discussions with the student(s).

Remark: Homework assignments, survey/scouting reports and research projects must be typed using a text editor (very preferably with Latex, but Word is ok). Handwritten deliveries will not be accepted.

All deliveries must be submitted online via TEACH system no later than given deadline. A hard-copy version must also be delivered either in-class or at office hours.

5. Schedule of Assignments:

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

6. Policies on incomplete grades and late assignments:
Late homework assignments are not accepted (see below for the expection).

7. Policies on absences (excused/ unexcused) and scheduling makeup:
There will be no makeups paper presentations, survey and/or research papers. Only exceptions is possible for homework assignments, if a student presents a police report or a doctor's note that show some emergency situation.

8. Course prerequisites:
A rudimentary understanding of computer networks and security is needed. It is strongly recommended that an undergraduate-level network security and/or cryptography course(s), has been taken.
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.