Advanced Network Security

Special Topics CS 519/ECE 599 (Fall 2016)

Syllabus

1. Course Information:

Instructor: Dr. Attila Altay Yavuz,
Class Room: ROG 440
Office: KEC 3065
Phone: 541-737-3341
Email: Attila.Yavuz@oregonstate.edu
URL: http://web.engr.oregonstate.edu/~yavuza/
Class Hours: TR 12:00 – 1:20 PM
Office Hours: Monday 4:30 PM – 6:00 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 cryptographic tools and their properties to protect computer systems
2. Describe important Privacy Enhancing Technologies (PETs), including
   a. Incident Matrix-based Dynamic Symmetric Searchable Encryption (DSSE)
   b. Multi-Server Oblivious DSSE Approaches
   c. ORAM Constructions with Improved Constants
3. Explain privacy and security concerns in Cognitive Radio Networks (CRN)
   a. Location Privacy with LPOS for Centralized CRN
   b. Location Privacy with Cuckoo-filter solutions for DB-based CRN
   c. Anti-Jamming for CRN
4. Describe essential security primitives, including
   a. One-time signatures
   b. Hash to Obtain Random Subset (HORS) and its relation to traditional signatures
   c. One-way hash chain, S/KEY and further applications
   d. Merkle hash tree and its applications,
   e. Bloom filters,
5. 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)
6. Describe Authentication Techniques for IoTs
   a. ECDSA/Schnorr
   b. Efficient and Tiny Authentication
   c. Signcryption and Hybrid Primitives
7. Explain the requirements and properties of Group Key Establishment and Distribution
   a. Group DH protocols
   b. Tree-based Group DH protocols
   c. Logical Key Hierarchy and Iolus
8. User-Friendly Authentication and Key Generation

Survey assignments, research projects and in-class presentations will enable student to follow, evaluate and improve some of the selected topics in applied cryptography and network security domain, including but not limited to:
   • Overview of Privacy Enhancing Technologies (PETs) and their applications
   • Design and implementation of advanced Searchable Encryption (SE) schemes for cloud computing.
     o Symmetric Searchable Encryption
   • Real-time authentication for time-critical applications.
     o Time-Valid security concept and its in-depth analysis
     o E-SIGN signatures
     o NTRU Cryptosystem
   • Secure Audit Logging
   • Wireless sensor network security topics
   • Time permitting: Secure matching on encrypted systems, secure MPC

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:
   • In-class paper presentation (35%) (extra credit possible)
   • Survey/Scouting Report (Optional)
   • Research project (55%) (extra credit is possible, may supersede survey/scouting report)
   • Class attendance, participation/discussions (%10),
   • Take-home assignments (optional)
Possible topics for survey/scouting report and research projects will be either announced at course website or will be decided with the student via one-on-one meetings. 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:** (i) Take-home 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. (ii) Remark that the above grading rule may be changed during the quarter.

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 expectation).

**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:**

An Introduction-Level Cryptography (or a network security course with the permission of the Instructor) course is 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.