University of Washington

Department of Electrical Engineering

EE 595 Advanced Topics in Communication Theory –

Introduction to Security and Privacy

Winter 2017

Time: Wednesdays from 6:00-9:30pm in EEB 037

(**Voluntary** discussion about the assigned papers from 9-9:30pm)

Instructor: Tamara Bonaci (tbonaci@uw)

Office hours: By appointment

Teaching Assistant: TBD

Office hours: TBD

Course website: https://canvas.uw.edu/courses/1098578

Course assignments and dropbox: https://canvas.uw.edu/courses/1098578/assignments

Course discussion board: https://canvas.uw.edu/courses/1098578/discussion_topics

Course gradebook: https://canvas.uw.edu/courses/1098578/gradebook

Course mailing list: ee595a_wi17@uw.edu

Course Overview:

The importance of cyber and cyber-physical systems on the quality of our lives is growing rapidly. As these systems become more complex and ubiquitous, the need to ensure their safety, security and reliability is increasing as well. Security and privacy are disciplines dedicated to protecting cyber and cyber-physical systems, as well as their users from adversarial actions. This course is a foundational security and privacy course, providing an introduction to tools, concepts and ideas of modern security and privacy research.

We will begin by defining the fields of security and privacy and introducing the key concepts, such as attackers, threat models and risk management. We will then focus on several central themes of security and privacy: attack detection and modeling; cryptography and communication security (including symmetric encryption, hash functions and public key cryptography), privacy, mobile devices security; web-based security and privacy, and security and privacy of emerging technologies.

Course Progression:

The following is the class progression covering the 10 weeks for the course. The class will meet once a week on Wednesdays from 6:00-9:30pm.

Week 1: Course overview. Introduction to security and privacy

Week 2: Cryptography – Introduction and symmetric encryption

Week 3: Cryptography – Block ciphers (DES and AES) and modes of operation

Week 4: Cryptography – Public key cryptography

Week 5: Cryptography – Hash functions and MACs

Week 6: Cryptography – Digital signatures and key management

Week 7: Introduction to privacy

Week 8: Authentication protocols. Web-based security and privacy

Week 9: Mobile platform security and privacy

Week 10: Security and privacy of emerging technologies (biometrics; end-to-end encryption in instant messaging applications)

Finals week: Project presentations

About the Course:

The course will consist of ***readings and discussion***, ***homework assignments, security review assignment, and a project.***

Readings and Discussion:
Readings and discussions of the assigned papers are an important part of this course. The goal of this exercise is to work together on understanding broader implications of the seminal security and privacy research. Additionally, we will also try to keep up with the state-of-the-art security and privacy research.

Prior to each class a single research paper will be assigned, and you will be expected to post to the class discussion board about it. Your post should contain something original beyond what others have already posted. You may consider posting:

- A summary of the paper,
- Evaluation of the paper's strengths and weaknesses,
- Open research question on the topic, or
- Question you would like to discuss in class.

All post are due by **4pm on the day of each class,** and they will be graded on the scale of 0-2, where:

- 0 means missed or irrelevant post,
- 1 means a relevant post submitted, and
- 2 means a good and interesting post.

Post submitted after 4pm on the day of the class will receive no credit. There will be a total of nine reading assignments, and we will take eight best scores when determining your grade.

Homework:
There will be five homework assignments, related to the presented cryptography material. The assignments will be a mix of written questions and simulation problems, and you will have approximately two weeks for each assignment.

While coding/simulating parts of the homework may be designed with Matlab in mind, you are welcome to code them up using any software tool you prefer (e.g., Mathematica, Octave, Maple, Python). **You should, however, submit all your code and simulation models with your homework.**

Security Review:
This course aims to sharpen our so-called *security mindsets*, and to get us all to thinking about the world in a different way. In the light of that, this exercise is designed to get you to thinking about

security and privacy in a context you might not normally do that.

With security review, your goals is to evaluate the potential security and privacy issues of a new and/or emerging technology, and to discuss what could be done to address those potential threats. You will choose a technology to analyze (you might get an idea for a technology from various technology news sources), and in a short (2-3 pages) write-up, you will present:

- A short summary of the evaluated technology,
- An analysis of potential security goals and weaknesses of the technology,
- An analysis of possible adversaries and threats, and
- A short discussion about possible defense strategies.

The security review will be due in the middle of the quarter

Project:
The final component of this course is a project, and its goal is to give you a deeper understanding of how to think about, and how to solve a real-life problem from a security and privacy-oriented perspective.

For the project, you will be able to choose a topic related to any area of security and privacy (including those not directly covered in this course). You can work on the project either individually, or in groups of up to three persons. When working in a group, your end result should reflect the fact that it is a multi-person effort.

Your work on the project will consists of several milestones:

- Project proposal,
- Progress report,
- Final report, and
- Project presentation.

Grading:

Your grade in this course will be based on readings and discussion, homework assignments, security reviews and project. The expected grade breakdown is:

- Readings and discussion – 10%
- Security review – 10%
- Homework – 40%
- Project – 40%

Course Material:

There is no required textbook for this course, but some recommended books that you might want to consider include:

- **C. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World, Prentice Hall, 2002***
- N. Daswani, C. Kern, and A. Kesavan, *Foundations of Security, What Every Programmer Needs to Know,* Apress, 2007
- D. Stinson*, Cryptography Theory and Practice, Third Edition,* CRC Press, 2006
- W. Stallings, *Cryptography and Network Security, Principles and Practice, 5th Edition,* Prentice Hall, 2006
- B. Schneier, *Applied Cryptography, Protocols, Algorithms and Source Code in C,* Wiley, 1996
- A. Menezes, P. Van Oorschot, S. Vanstone, *Handbook of Applied Cryptography* (available online)

Course Policies:

Collaboration: In this course, we want you to learn from each other. Therefore, you are allowed (and encouraged) to talk to your classmates and other students about all course assignments. You may also consult outside reference materials, or the instructor. However, all material that you decide to turn in should reflect your own understanding of the subject matter at the time of writing. This means that you should write your own posts about the assigned papers, your own security review, and your own homework. If you work with someone else on any assignment, please include their names on the material that you turn in.

Assignment Turn-in: Posts about the assigned papers should be submitted using the course discussion board. All other material (security reviews, homework, and project-related material) should be submitted in a PDF form to the course dropbox. Please, ***do not use*** email for assignment submissions.

Late Assignment Turn-in: Discussion board posts are due **by 4pm on the day of the class**, and no late turn-ins will be accepted. All other assignments are due **by 11:59pm on the assigned date,** but we understand that you may have to sometimes turn them in late. The grading penalty is 20% of the grade that you would otherwise receive for each day, or part of the day, that you are late. No submissions will be accepted after 5 days.

Checking grades: Grades will be posted to the course gradebook.