University of Washington

Department of Electrical Engineering

EE 595 Security and Privacy of Biomedical Cyber-Physical Systems

Spring 2016

Time: Wednesdays from 6:00-9:30pm in EEB TBD and EEB Lab TBD

(Lab part starts at 8:00pm)

Instructor: Tamara Bonaci (tbonaci@uw)

Office hours: By appointment

Course website: https://canvas.uw.edu/courses/1061960

Course assignments and dropbox: TBD

Course discussion board: TBD

Course gradebook: TBD

Course mailing list: TBD

Course Overview:

Advances in biomedical and health technologies have a great potential to improve safety of many medical procedures, and to decelerate the rising cost of medical services. Developments of new biomedical technologies, along with improvements to the existing systems are expected to facilitate:

- More efficient and effective delivery of medical treatments,
- Safer and faster execution of medical procedures, with less negative outcomes,
- Increase in medical practitioners' abilities, as well as
- Increase in patients' willingness to accept and use medical technologies.

However, rapid development of new biomedical technologies, and their hasty adoption, combined with often archaic, insufficient, and lacking regulations, has resulted in a variety of safety, security and privacy problems with medical cyber-physical system. In this course, we will focus on the recent issues.

We will begin by defining some common properties and requirements on all biomedical systems, and understanding some common threats, vulnerabilities and attackers. We will then dive into security and privacy issues within several major subareas of medical cyber-physical systems, including health monitoring and body sensor-actuator networks, implanted medical systems, neural engineering systems, and biomarkers and biometric-based systems.

The course will assume that all participants have an understanding of concepts such symmetric key and public key cryptography, hash functions, digital signatures and authentication.

Course Progression:

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

Week 1: Basic properties and requirements for biomedical cyber-physical systems

Week 2: Electronic medical records and HIPAA

Week 3: Systems for health monitoring

Week 4: Body-sensor-actuator networks

Week 5: Systems based on biomarkers and biometric data

Week 6: Implanted medical devices

Week 7: Implanted medical devices

Week 8: Neural engineering systems

Week 9: Systems relying on genetic data. Pharmacology

Week 10: Surgical systems

Finals week: Project presentations

About the Course:

The course will consist of ***readings and discussion***, ***classroom presentation, lab 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 get familiar with some fundamental concepts and ideas before the lecture time, so that during lectures we can work together on understanding broader implications of the state-of-the-art research from the domain of security and privacy for biomedical cyber-physical systems.

Each week, ***up to three papers*** related to the next lecture will be assigned. You will be expected to ***read all the papers*** before the class, and to post to the class discussion board about ***two of the assigned papers.*** You will decide which of the assigned papers you will make comments about, and 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.

Your posts should contain something original beyond what others have already posted.

All post will be due by ***1pm on the day of each class*****,** and they will be graded on the scale of 0-4, where the total number of points represents a sum of points for each individual post. An individual post will be graded on a scale 0-2, where:

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

Post submitted after 1pm 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.

Classroom presentations:
This course is concerned with security and privacy of biomedical cyber-physical systems. In order to understand potential vulnerabilities and threats against such systems, however, it is important to first understand the systems themselves. In doing so, we will want to understand ***when, how and why*** the systems are being used. Gaining the necessary background knowledge about the considered biomedical system is the goal of classroom presentations.

Topics covered by classroom presentations will be announced during the first week of classes, but may include concepts such as EEG, EKG, DNA, etc. You will be expected to sign up for ***one presentation***. Each topic will be covered by ***at most two persons***, who will be expected to work together in preparing a 15-minutes long presentation. The presentation may consist of slides, a poster, a demo, or any combination thereof, and that material will be due by **5:30pm on the day of your presentation**.

You (as a group) will be graded based upon the quality of your presentation.

Lab:
Labs are an important part of this course, as they are expected to give you a more practical, hands-on experience with some important security and privacy concepts. There will be ***up to four labs*** through the quarter, and you will have at least two lab sessions to work on those assignments. You are encouraged to work in groups of two persons, but if you prefer, you can work on those assignments individually.

Each lab will be graded based upon deliverables, which will be defined in each individual lab assignment.

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 – 25%
- Classroom presentations – 10%
- Lab – 30%
- Project – 35%

Course Material:

Course material for this course will consist of peer-reviewed conference and journal papers, presented recently at relevant security and privacy venues. They will be provided on the course website.

Some additional resources you may want to consider:
- C. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World, Prentice Hall, 2002*
- 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 blog by Professor Kevin Fu on Medical Devices Safety and Security: http://blog.secure-medicine.org
- A blog by Professor Avi Rubin on (among other things) Security in Healthcare Information Technology: http://avi-rubin.blogspot.com

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. 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 (classroom presentations, labs and project) 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 1pm on the day of the class**, and no late turn-ins will be accepted. Classroom presentations are due **by 5pm on the day of your scheduled presentation**. All other assignments are due **by 6:00pm on an assigned Saturday,** 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.