CSS 539: Security and Privacy in Emerging Environments

Course Description:

Computational systems and networks continue to emerge in many new environments that present different threats and constraints from traditional desktop computing environments. This course will explore security concerns and potential solutions in a variety of emerging environments and non-traditional computing platforms. Potential environments include vehicular networks, electronic voting, sensor and mobile ad-hoc networks, mobile phone systems, and other pervasive systems. Students will explore techniques for designing useable security mechanisms, managing trade-offs in resource-constrained systems, and reasoning with uncertain information. The goal of this course is to provide students with experience with innovative research in new fields, so that they have the confidence and training to pursue further research in these and related fields.

Work Load and Grading:

Course Work	Percentage	Grades	Approximately Corresponding Numeric Grade
Research Proposal	25%	90s	3.5 - 4.0
Reinforcement Exercises	25%	80s	2.7 - 3.4
Final Project/Paper	50%	70s	1.7 - 2.7

Textbooks/References:

This course has no required text books. Our reading material will generally be from recently published research papers.

Many of these can be found via Google Scholar, Microsoft Research, or Citeseer. Additionally, papers can often be found at:

IEEE XPloreLinks to an external site. -- Search for publications through IEEE
ACM Digital LibraryLinks to an external site. -- Search for publications through ACM.
Usenix ConferencesLinks to an external site. -- Listing of Usenix conferences

http://www.cs.cornell.edu/info/misc/latex-tutorial/latex-home.html (Links to an external site.)Links to an external site. -- LaTeX tutorial

http://www.maths.tcd.ie/~dwilkins/LaTeXPrimer/ (Links to an external site.)Links to an external site. -- LaTeX help

Software:

http://miktex.org/download (Links to an external site.)Links to an external site. -- Tex typesetting software

http://texstudio.sourceforge.net/ (Links to an external site.)Links to an external site. -- LaTex editor

http://www.texniccenter.org/ (Links to an external site.)Links to an external site. -- Another LaTeX editor

http://www.bobsoft-mac.de/texnicle/texnicle.html (Links to an external site.)Links to an external site. -- LaTeX editor (Mac)

Course Goals:

The overall goals of CSS 539, "Security and Privacy in Emerging Environments" include:

- Understand the properties of emerging environments that result in different security requirements than traditional systems
- Analyze and extend existing state of the art work in security and privacy in emerging environments

Assignments:

Assignments will consist primarily of research-based projects:

1. Reinforcement Exercises -- These reinforce the topics learned in class. They will be due (or will occur) regularly throughout the quarter. They will include quizzes, programming assignments, and discussions about security in emerging environments. Expect between 5-8 of these over the quarter, depending on the intensity of the exercises. Approximately 20 hours over the course of the quarter is expected.
2. Research Proposal -- You will write a research proposal. As other assignments are kept to a minimum, you are expected to spend most of your class-related work on this in the first 3 weeks. 30-50 hours of work is expected.
3. Final project -- This will be a culmination of the skills and techniques we have learned in the class. You will test your hypothesis about an open problem in the field of security in emerging environments and writeup and present your results. During the remaining 7 weeks, you are expected to spend most of your class-related work on this project. Approximately 100 hours of work outside of your research proposal is expected.

Topics covered and tentative 539 schedule:

Week	Topics	Additional Information
0	Introduction and Basics	

	Basics	
1	Reasoning with Uncertainty	
	Pervasive Computing	
2	Crowd Sensing	
3	Machine Learning	
	Adversarial Machine Learning	
4		
	Software Defined Networking	
5	Cloud Systems	
6	Electronic Voting	
	Opportunistic Computing	
7	Internet of Things/Sensors	
8	Privacy in Systems	
9	Data Set Privacy	
10	Final Presentations	