Syllabus

USC Viterbi School of Engineering

CSCI 699 Advanced Computer Security

Units: 4

Fall 2018—Wed—2pm to 5:20pm

Location: VKC 111

Instructor: Muhammad Naveed

Office: SAL 344

Office Hours: 11:00am – 12:00pm

Contact Info: mnaveed@usc.edu

Course Website:

https://www.cryptoonline.com/csci699-fall18

The course is designed to equip students with the knowledge and skills to solve the security problems faced by people, businesses, and governments in today's digital world.

The goal of the course is to develop a security mindset, which is necessary for computer security research. A distinguishing aspect of computer security research is to think like an attacker to discover security problems. In this course, the students will learn how to discover security problems and how to develop security solutions.

This research-oriented course is aimed towards PhD students interested in computer security. Advanced undergraduate students and master's students are welcome to enroll with an approval from the instructor.

Learning Objectives

The objective of the course is to introduce students to the state-of-the-art research in computer security, and to learn how to conduct, evaluate computer security research, and develop a security mindset.

> **Prerequisite(s):** computer security and cryptography knowledge equivalent to an undergraduate course in security and/or cryptography

Course Notes

N/A

Technological Proficiency and Hardware/Software Required

N/A

Required Readings and Supplementary Materials

Links to all the required readings will be posted on the course website.

Description and Assessment of Assignments

Reading and critical assessment of papers

To introduce students to the state-of-the-art computer security research and enable them to evaluate such research, the students are required to read a paper and write a detailed review for each class. The review needs to be submitted on Piazza mid-night before the class.

Research Project

The students are required to do a research project, write a paper about it, and present it to the class. One of the goals of the course is to learn how to conduct computer security research; the research project will help achieve this goal. The students are encouraged to develop their own ideas for the project related to course theme; however, the students are welcome to ask for ideas and discuss them with the instructor. To track the progress of the project, the students will submit a weekly Piazza post about the project progress.

Grading Breakdown

Reading Assignment	% of Grade
Piazza Review	15%
Piazza Discussion	15%
Class Discussion	20%
Project	
Weekly Project Oral Reports	30%
Weekly Piazza Post	10%
Final Paper and Presentation	10%
TOTAL	**100%**

Assignment Submission Policy

The weekly paper reviews and project progress post need to be submitted on Piazza mid-night before the class in which the paper will be presented.

Additional Policies

The late paper reviews submitted before the class in which the paper is presented would incur a 10% penalty and reviews submitted after the class would incur a 25% penalty.

The project posts and the final project paper need to be submitted on time. Please contact the instructor if a timely submission is not possible.

	Topics	Readings
Week 1	Introduction	
Week 2	Verizon Data Breach Report Science of Security	**2018 Verizon Data Breach Investigations Report** **SoK: Science, Security, and the Elusive Goal of Security as a Scientific Pursuit,** C. Herley, P. Oorschot, *Oakland 2017*
Week 3	Authentication	**The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes,** J. Bonneau, C. Herley, P. Oorschot, F. Stajano, *Oakland 2012* **On the Economics of Offline Password Cracking,** J. Blocki, B. Harsha, and S. Zhou, *Oakland 2018*
Week 4	Authentication	**A Tale of Two Studies: The Best and Worst of YubiKey Usability,** J. Reynolds, T. Smith, K. Reese, L. Dickinson, S. Ruoti and K. Seamons, *Oakland 2018* **The Rewards and Costs of Stronger Passwords in a University: Linking Password Lifetime to Strength,** Ingolf Becker, Simon Parkin, and M. Angela Sasse, *Usenix Security 2018*
Week 5	Messaging	**SoK: Secure Messaging**, Nik Unger, Sergej Dechand, Joseph Bonneau, Sascha Fahl, Henning Perl, Ian Goldberg and Matthew Smith, *Oakland 2015* **Atom: Horizontally Scaling Strong Anonymity**, A. Kwon, H. Corrigan-Gibbs, S. Devadas, and B. Ford, *SOSP 2017*
Week 6	IoT Security	**IoT Goes Nuclear: Creating a Zigbee Chain Reaction**, E. Ronen, C. O'Flynn, A. Shamir, A. Weingarten, *Oakland 2017* **SoK: Exploiting Network Printers**, Jens Müller, Vladislav Mladenov, Juraj Somorovsky, Oakland 2017
Week 7	IoT Security	**BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid**, S. Soltan, P. Mittal, and H. Poor, *Usenix 2018* **Rethinking Access Control and Authentication for the Home Internet of Things (IoT),** W. He, M. Golla, R. Padhi and J. Ofek, M. Dürmuth, E. Fernandes, B. Ur, *Usenix 2018*
Week 8	Automobile Security	**Experimental Security Analysis of a Modern Automobile**, K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, *Oakland 2010* **Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel,** Andy Greenberg, *Forbes 2013* **Comprehensive Experimental Analyses of Automotive Attack Surfaces**, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H.

		Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno. *Usenix 2011* **Hackers Remotely Kill a Jeep on the Highway—With Me in It**, Andy Greenberg, *Wired 2015*
Week 9	Cryptocurrencies and Smart contracts	**Research Perspectives and Challenges for Bitcoin and Cryptocurrencies**, J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. Kroll and E. Felten, *Oakland 2015* **Arbitrum: Scalable, private smart contracts,** H. Kalodner, S. Goldfeder, X. Chen, S. Weinberg, and E. Felten, *Usenix Security 2018*
Week 10	Cryptocurrencies and Smart contracts	**teEther: Gnawing at Ethereum to Automatically Exploit Smart Contracts**, J. Krupp and C. Rossow, *Usenix Security 2018* **Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts**, L. Breidenbach, P. Daian, F. Tramer, A. Juels, *Usenix Security 2018*
Week 11	Adversarial Machine Learning	**Membership Inference Attacks against Machine Learning Models**, R. Shokri, M. Stronati, C. Song, V. Shmatikov, Oakland 2017 **DeepXplore: Automated Whitebox Testing of Deep Learning Systems**, Kexin Pei, Yinzhi Cao, Junfeng Yang, and Suman Jana, *SOSP 2017*
Week 12	Encrypted Databases	**CryptDB: Protecting Confidentiality with Encrypted Query Processing**, R. Popa, C. Redfield, N. Zeldovich, H. Balakrishnan, *SOSP 2011* **Inference Attacks on Property-Preserving Encrypted Databases**, M. Naveed, S. Kamara, C. Wright, *CCS 2015*
Week 13	Trusted Hardware	**EnclaveDB: A Secure Database using SGX** C. Priebe, K. Vaswani, M. Costa, Oakland 2018 **Iron: Functional Encryption using Intel SGX**, B. Fisch, D. Vinayagamurthy, D. Boneh, S. Gorbunov, CCS 2017
Week 14	Hardware Attacks	**Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution**, J. Bulck, M. Minkin, O. Weisse, D. Genkin, B. Kasikci, F. Piessens, M. Silberstein, T. Wenisch, Y. Yarom, R. Strackx, *Usenix 2018* **Meltdown: Reading Kernel Memory from User Space**, M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, M. Hamburg, Usenix 2018
Week 15	Transport Layer Security	**Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice**, D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, B.

		VanderSloot, E. Wustrow, S. Zanella-Beguelin, P. Zimmermann, *CCS 2015* **Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations,** C. Brubaker, S. Jana, B. Ray, S. Khurshid, and V. Shmatikov, *Oakland 2014*
Final	Project Presentations	

Statement on Academic Conduct and Support Systems

Academic Conduct

Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences. Please familiarize yourself with the discussion of plagiarism in *SCampus* in Section 11, *Behavior Violating University Standards* https://scampus.usc.edu/1100-behavior-violating-university-standards-and-appropriate-sanctions. Other forms of academic dishonesty are equally unacceptable. See additional information in *SCampus* and university policies on scientific misconduct, http://policy.usc.edu/scientific-misconduct.

Discrimination, sexual assault, and harassment are not tolerated by the university. You are encouraged to report any incidents to the *Office of Equity and Diversity* http://equity.usc.edu or to the *Department of Public Safety* http://adminopsnet.usc.edu/department/department-public- safety. This is important for the safety of the whole USC community. Another member of the university community – such as a friend, classmate, advisor, or faculty member – can help initiate the report, or can initiate the report on behalf of another person. *The Center for Women and Men* http://www.usc.edu/student-affairs/cwm/ provides 24/7 confidential support, and the sexual assault resource center webpage http://sarc.usc.edu describes reporting options and other resources.

Support Systems

A number of USC's schools provide support for students who need help with scholarly writing. Check with your advisor or program staff to find out more. Students whose primary language is not English should check with the *American Language Institute* http://dornsife.usc.edu/ali, which sponsors courses and workshops specifically for international graduate students. *The Office of Disability Services and Programs* http://sait.usc.edu/academicsupport/centerprograms/dsp/home_index.html provides certification for students with disabilities and helps arrange the relevant accommodations. If an officially declared emergency makes travel to campus infeasible, *USC Emergency Information* *http://emergency.usc.edu* will provide safety and other updates, including ways in which instruction will be continued by means of blackboard, teleconferencing, and other technology.