Shanghai Jiao Tong University

CS267 Computer Usability and Security

Instructor Information	Shuxi Wang Home Institution: University of International Business and Economics Email: wangshuxi@uibe.edu.cn Office Hours: Determined by Instructor		
Term	December 17, 2020 - January 8, 2021	**Credits**	4 units
Class Hours	Sunday through Thursday, 135 mins per teaching day		
Discussion Sessions	2 hours each week, conducted by teaching assistant(s)		
Total Contact Hours	64 contact hours (1 contact hour = 45 mins, 2880 mins in total)		
Required Texts (with ISBN)	1. Jonathan Lazar, Jinjuan Heidi Feng, Harry Hochheiser. Research Methods in Human-Computer Interaction. ISBN: 9780128053904. 2. Lorrie Cranor, Simson Garfinkel. Security and Usability: Designing Secure Systems that People Can Use. ISBN: 9780596008277.		
Prerequisite	Programming language, data structures, operating systems, computer organization, computer network, etc.		
The course might be moved to online delivery due to COVID-19 pandemic. The anticipated date is November 6, 2020.			

Course Overview

Human factors and usability issues have traditionally played a limited role in security research and secure systems development. Security experts should recognize the importance of human factors. Increasingly, well publicized security breaches are attributed to human errors that might have been prevented through more usable software. Regardless of how secure a system is in theory, failing to consider how humans actually use the system leads to disaster in practice. There is increasing agreement that we need to design secure systems that people can actually use.

This course bridges security and usability. This course will examine how to design for security and privacy from a user-centered perspective by combining insights from computer systems, human-computer interaction (HCI), and public policy. We will introduce core security and privacy technologies, as well as HCI techniques for conducting robust user studies.

This course has six parts: Realigning Usability and Security; Authentication Mechanisms; Secure Systems; Privacy and Anonymity Systems; Commercializing Usability: The Vendor Perspective; The Classics.

Topics will include: usable authentication, user-centered web security, anonymity software, privacy notices, security warnings, and data-driven privacy tools in domains ranging from social media to the Internet of Things. Students will complete weekly problem sets, as well as conduct novel research in a group capstone project. No prior experience in security, privacy, or HCI is required.

Learning Outcomes

There is much agreement among security practitioners that we need to find ways of designing secure systems that people can use. We discuss case studies of usable secure system design along with the latest thinking about how to approach this problem. This course will inform future design efforts and give developers important insights that will lead to successful designs. This course is expected to start an avalanche of discussion, new ideas, and further advances in this important field.

Successful participants can answer all the security/privacy and usability HCI questions as below:

1. How do users select graphical passwords? How can we help them choose passwords harder for attackers to predict?
2. As the password space increases, what are the impacts on usability factors and predictability of human selection?

Grading Policy

Attendance	10%
Middle Exam	20%
Projects	30%
Final Exam	40%

Grading Scale is as follows

Number grade	**Letter grade**	**GPA**
90-100	A	4.0
85-89	A-	3.7
80-84	B+	3.3
75-79	B	3.0
70-74	B-	2.7
67-69	C+	2.3
65-66	C	2.0
62-64	C-	1.7
60-61	D	1.0
≤59	F (Failure)	0

Class Schedule

Date	Lecture	Readings
Day 1	Course overview and introductions Introduction to security; usable encryption	Reading I
Day 2	Reasoning about the human in the loop	Reading II
Day 3	Introduction to privacy	Reading III
Day 4	Review & discussion	
Day 5	Introduction to experimental design: overview of methods, ethics/deception, and ecological validity Introduction to crowdsourced studies	Reading IV
Day 6	Participant recruitment and surveys Interviews, focus groups, and diary studies + analyzing qualitative data	Reading V
Day 7	Analyzing quantitative data with statistics Quantitative data collection, lab and field studies, simulating attacks	Reading VI
Day 8	Review & discussion	Reading VII
Day 9	Mid-term Exam	
Day 10	Analyzing quantitative data with statistics	Reading VII
Day 11	Security warnings	Reading VIII
Day 12	Passwords	Reading IX
Day 13	Review & discussion	
Day 14	Authentication beyond text passwords Privacy notice and choice	Reading X
Day 15	Evaluating disclosures Privacy and anonymity tools	Reading XI
Day 16	Social networks and privacy Privacy and security for mobile devices and IoT	Reading XII
Day 17	Review & discussion	
Day 18	Final Exam	

All reading materials will be provided by the instructor before the class.