

Thursday, January 26

Scaife Hall Auditorium

Room 125 at 4:30 p.m.

Refreshments at 4:00 p.m.



Lorrie Cranor

Associate Professor of CS, EPP
CMU

Lorrie Faith Cranor is an Associate Professor of Computer Science and of Engineering and Public Policy at Carnegie Mellon University where she is director of the CyLab Usable Privacy and Security Laboratory (CUPS). She is also a co-founder of Wombat Security Technologies, Inc. She has authored over 100 research papers on online privacy, usable security, phishing, spam, electronic voting, anonymous publishing, and other topics. She has played a key role in building the usable privacy and security research community, having co-edited the seminal book *Security and Usability* (O'Reilly 2005) and founded the Symposium On Usable Privacy and Security (SOUPS). She also chaired the Platform for Privacy Preferences Project (P3P) Specification Working Group at the W3C and authored the book *Web Privacy with P3P* (O'Reilly 2002). She has served on a number of boards, including the Electronic Frontier Foundation Board of Directors, and on the editorial boards of several journals. In 2003 she was named one of the top 100 innovators 35 or younger by *Technology Review* Magazine. She was previously a researcher at AT&T-Labs Research and taught in the Stern School of Business at New York University.

ECE Seminar Hosts

Gabriela Hug	ghug@ece.cmu.edu
Lujo Bauer	lbauer@cmu.edu
Soumya Kar	soumyak@andrew.cmu.edu
Jeff Weldon	jweldon@ece.cmu.edu

Designing Secure Systems That People Can Use

Many secure systems rely on a "human in the loop" to perform security-critical functions. However, humans often fail in their security roles. Whenever possible, secure system designers should find ways of keeping humans out of the loop. However, there are some tasks for which feasible or cost effective alternatives to humans are not available. In these cases secure system designers should engineer their systems to support the humans in the loop and maximize their chances of performing their security critical functions successfully. I will introduce some high-level approaches to usable security and discuss a proposed framework for reasoning about the human in the loop that provides a systematic approach to identifying potential causes for human failure. This framework can be used by system designers to identify problem areas before a system is built and proactively address deficiencies. System operators can also use this framework to analyze the root cause of security failures that have been attributed to "human error." I will discuss this approach to designing usable secure systems and also present some examples from CyLab Usable Privacy and Security (CUPS) Lab research projects.