UNIVERSITY OF CHICAGO
DEPARTMENT OF COMPUTER SCIENCE

PRESENTS:

"Securing Deployed Cryptographic Systems"

Christina Garman

Johns Hopkins University

Abstract:
In 2015 more than 150 million records and $400 billion were lost due to publicly-reported criminal and nation-state cyber attacks in the United States alone. The failure of our existing security infrastructure motivates the need for improved technologies, and cryptography provides a powerful tool for doing this. There is a misperception that the cryptography we use today is a "solved problem" and the real security weaknesses are in software or other areas of the system. This is, in fact, not true at all, and over the past several years we have seen a number of serious vulnerabilities in the cryptographic pieces of systems, some with large consequences.

In this talk I will discuss two aspects of securing deployed cryptographic systems. I will first talk about the evaluation of systems in the wild, using the example of how to efficiently and effectively recover user passwords submitted over TLS encrypted with RC4, with applications to many methods of web authentication as well as the popular IMAP protocol for email. I will then address my work on developing tools to design and create cryptographic systems and bridge the often large gap between theory and practice by introducing AutoGroup+, a tool that automatically translates cryptographic schemes from the mathematical setting used in the literature to that typically used in practice, giving both a secure and optimal output.

Bio:
Christina Garman is a Ph.D. student at Johns Hopkins University where she is advised by Professor Matthew Green. Her research interests focus largely on practical and applied cryptography. More specifically, her work has focused on the security of deployed cryptographic systems from all aspects, including the evaluation of real systems, improving the tools that we have to design and create them, and actually creating real, deployable systems. Some of her recent work has been on demonstrating flaws in Apple's iMessage end to end encryption, cryptographic automation, decentralized anonymous e-cash, and decentralized anonymous credentials. Her work has been publicized in The Washington Post, Wired, and The Economist, and she received a 2016 ACM CCS Best Paper Award.

Thursday, February 23, 2017
3:00 pm
Ryerson 251
Host: Blase Ur