Current Topics in Privacy Seminar

January 21st 2024

Speaker:
McKenna McCall

Talk title:
Formal Methods or Usable Security: Why Not Both?

Abstract:

Formal methods research involves using mathematical techniques to specify and verify properties of software and hardware systems. In security and privacy research, formal methods can lead to strong, provable security guarantees—and typically leave questions about how humans might interact with these systems unanswered. Indeed, formal methods and usable security are traditionally distinct areas of research. In this talk, McKenna will demonstrate how techniques from both research areas can be applied—or even combined—to create solutions that are simultaneously mathematically rigorous and usable. In one project, we revisit static analysis tools for home IoT users from a usable security lens and investigate the usability and utility of the workflow involved in using the tools. Later in the talk, she will describe a project with a formal methods focus where we propose a new technique for preventing undesirable information flows on the web. We argue that this approach is usable in more realistic scenarios than what is proposed by prior work—without sacrificing security.

Bio:

McKenna McCall is a postdoctoral researcher in the Software and Societal Systems Department at Carnegie Mellon University supervised by Lorrie Cranor and Lujo Bauer. She received her PhD from Carnegie Mellon University in 2023, advised by Limin Jia. McKenna's research spans fields from information flow control and programming languages to security and privacy for home IoT and confidential computing. She is particularly interested in research where formal methods and usable security intersect, and combines techniques from both research areas to produce results that incorporate mathematical rigor as well as usability.