Department of Computer Science

Privacy for Proactive Intelligent Assistants, or: How To Design for Something That Doesn't Exist (Yet)

Nathan Malkin
University of Maryland

Hosted by Iulian Neamtiu

Date: Friday, February 17, 2023
Refreshments: 10:45 AM – 11:00 AM
Time: 11:00 AM – 12:00 PM
Location: GITC 4402 (4th Floor Seminar Lecture Hall)
WebEx Link: https://njit.webex.com/njit/j.php?MTID=m787137cf71c387e565d752223ead678c

https://cs.njit.edu/seminars

Abstract:
How do we protect people from privacy threats from new technologies on the horizon? For example, consider the future of intelligent voice assistants that are embedded in phones, smart speakers, and other devices around the house. Today, their always-on microphones capture all of our conversations but typically discard them immediately. But eventually, in order to understand context and act proactively, the assistants may start actively analyzing and storing everything we say. What should the privacy controls for these products be? A major challenge in answering this question is that we don't yet know the features, or even modalities, of these devices. In my talk, I will describe my approach for studying the problem of privacy for future intelligent assistants and demonstrate that, despite the unknowns, we can still apply quantitative and qualitative data collection techniques like surveys and user studies to understand people's preferences and identify solutions that are best for people's privacy. In addition, I will discuss my projects, related to smart speaker permissions and IoT access control, that demonstrate my approach to understanding and designing for privacy.

Bio:
Nathan Malkin is a postdoctoral researcher at the University of Maryland, working with Michelle Mazurek. He received his PhD in computer science from UC Berkeley, where he was advised by David Wagner and Serge Egelman. In his research, Nathan works to understand how human factors contribute to privacy and security problems; he then designs systems to overcome these challenges and empirically validates their performance. His research has appeared at conferences including IEEE Security & Privacy, CHI, CSCW, and PETS, and has been recognized with the Future of Privacy Forum's Student Paper Award and the Cal Cybersecurity Fellowship.