Practical security guidance for real-world users and designers of authentication systems

Joshua Tan

Monday, September 23rd, 2019
9:30 AM - 12:00 PM
Newell-Simon Hall 4305

A wealth of security guidance is available to users and security system designers. Much of this guidance assumes an idealized world in which users are motivated and attentive when completing security tasks interjected in front of their primary task; and in which system designers are free to design security systems that subject their user base to however poor a usability experience deemed necessary in order to maximize security benefits for those users. However, these idealized-world assumptions do not reflect reality. Users perform security as a secondary task, typically unmotivated to exert more than the minimum possible effort to accomplish security tasks, which they ultimately perform in an inattentive, error-prone manner.

I will demonstrate how practical guidance can be given to users that assumes real-world settings but that does not abandon the worthwhile goal of improving security for those who do not want to or cannot take the security-optimal approach. First, I will show how users can be guided to create strong passwords while minimizing negative usability impacts, using password policies that incorporate a minimum neural-network-derived password-strength requirement. Second, I will show how latent features of passwords can be learned that can then be leveraged to improve password-creation guidance with more relevant and comprehensive text feedback. Lastly, I will show how practical guidance can be given to system designers in authentication domains other than passwords, using public-key verification as a case study. Specifically, I will examine ways of exposing fingerprint verification to ordinary users that remain effective at protecting against man-in-the-middle attacks in low-risk situations or usability-focused environments.

Committee: Dr. Lorrie Faith Cranor (Co-Chair), Dr. Lujo Bauer (Co-Chair), Dr. Matt Fredrikson, Mary Ellen Zurko (MIT Lincoln Laboratory)