Thesis Defense

Institute for Software Research
Societal Computing

Practical security guidance for authentication-system designers

Joshua Tan

Thursday, September 17th, 2020
Zoom Meeting ID: 939 4609 4387
Zoom Meeting Password: theehisss
4:00 p.m.—7:00 p.m.

Designers of authentication systems have a challenging task of balancing security requirements with organizational demands, including usability requirements and other practical constraints. They must design a system that is secure against modern attackers that are able to leverage increasingly large amounts of computational resources to undermine security protections. In some cases, system designers are subject to mandatory regulatory guidance that restricts that space of possible designs they are able to implement. Different organizations will have different levels of security requirements reflecting different threat models; designers must understand these requirements and design a solution specific to these requirements. Designers of authentication systems to be incorporated in consumer-facing products often must produce a solution that not only provides a given security level but that also does not undermine a high usability standard associated with the product brand. Different organizations will have different authentication needs; a single design solution will not work for all.

In designing an authentication system for an organization, system designers often rely on the guidance of security experts. Although system designers can often find security guidance on how to design an authentication system, this guidance may not always be applicable. For example, designers may be subject to regulatory requirements or usability constraints that preclude security solutions recommended by experts. In other cases, available security guidance may be incomplete, abstract, or incompatible with available resources. Security guidance for system designers should produce recommendations relevant for different scenarios; these recommendations should be both comprehensive and concrete.

In this thesis, I provide practical guidance for system designers tasked with designing an organizational password policy. This guidance is comprehensive, flexible to implementation requirements, concrete, and evaluated in experimental user studies considering both security and usability dimensions. Using a combination of machine-learning and statistical modeling methods, I explore techniques for expanding guidance available to system designers in the area of text feedback for password-creation meters. I also provide design recommendations for applications that incorporate public-key fingerprint comparison, using user studies that evaluate the effective security of solutions providing varying levels of usability.

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

isr institute for SOFTWARE RESEARCH | Carnegie Mellon University School of Computer Science