VirginiaTech

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Computer Science Seminar Series

National Capital Region

Measuring Password Guessability for an Entire University

Speaker: Dr. Michelle Mazurek
Department of Computer Science
University of Maryland
Friday, Jan 29, 2016
1:00PM - 2:00PM, NVC 325

Abstract

Despite considerable research on passwords, empirical studies of password strength have been limited by lack of access to plaintext passwords, small data sets, and password sets specifically collected for a research study or from low-value accounts. Properties of passwords used for high-value accounts thus remain poorly understood. We fill this gap by studying the single-sign-on passwords used by over 25,000 faculty, staff, and students at a research university with a complex password policy. Key aspects of our contributions rest on our (indirect) access to plaintext passwords. We describe our data collection methodology, particularly the many precautions we took to minimize risks to users. We then analyze how guessable the collected passwords would be during an offline attack by subjecting them to a state-of-the-art password cracking algorithm. We discover significant correlations between a number of demographic and behavioral factors and password strength. We also compare the guessability and other characteristics of the passwords we analyzed to sets previously collected in controlled experiments or leaked from low-value accounts. We find more consistent similarities between the university passwords and passwords collected for research studies under similar composition policies than we do between the university passwords and subsets of passwords leaked from low-value accounts that happen to comply with the same policies.

Biography

Michelle L. Mazurek is an Assistant Professor of Computer Science at the University of Maryland. Her research interests span security, systems, and HCI, with particular emphasis on how human factors impact security and privacy. She has worked on projects related to usable access control, distributed systems, usable encryption, security decisionmaking by developers, and passwords.