NIST Usable Security Project

Exploring Usability and Security Metrics for Passwords on Mobile Platforms

Kristen K. Greene
Information Access Division - kristen.greene@nist.gov

Joshua M. Franklin
Computer Security Division - joshua.franklin@nist.gov

ACKNOWLEDGEMENTS

The authors gratefully acknowledge John Kelsey of NIST's Computer Security Division for his help.

OBJECTIVE

Our objective is twofold:

- explore usability and security metrics applicable to passwords
- discuss our experiences in attempting to use these metrics in a real world situation

An overarching goal of this research is to propose a measurement method for quantifying theoretical effects on security resulting from optimizing the usability of password entry specifically for constrained input environments (i.e., mobile devices).

BACKGROUND

With the proliferation of mobile devices, the traditional problems of authenticating via passwords are transferred to this new form factor. Given the ubiquity of mobile devices and the usage of passwords, it is critical that we understand the security-usability balance in the mobile password space.

Mobile device constraints:

- smaller keys
- lack of tactile feedback
- complex passwords require navigation between multiple onscreen keyboards (three screen depths)

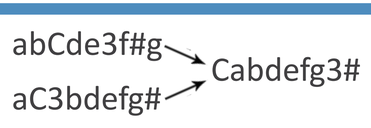
All combine to impact input errors and password entry times.

DEPTHS OF MOBILE OS KEYBOARDS

OUR APPROACH

1. Defined a usability permutation to make randomly generated passwords easier to enter on mobile devices.
   - Performed by grouping like character categories together in order to *minimize the number of times a user must switch back and forth between onscreen keyboards.*
   - Permutation categorizes the characters of a password into four sets: uppercase (U), lowercase (L), numbers (N), and symbols (S).
   - The rearranged password is then created by concatenating each set in the order U + L + N + S.
2. Created a python script (will be publicly available from https://github.com/usnistgov/PasswordMetrics) to perform the permutation which ensures all characters retain the order in which they were parsed by our tool.
3. Measured the effects on usability (specifically efficiency, measured by number of keystrokes).
4. Measured effects on security (specifically entropy, measured by Shannon entropy) to answer ***how much security is lost as a result of our usability permutation?***
   - Ran Monte Carlo simulations to estimate entropy loss by password length category, by determining the number of original passwords that when rearranged, result in the same permuted password.

PERMUTATION EXAMPLE



PERMUTATION AND KEYSTROKE RESULTS

Original Password	Permuted Password	Length	iOS Keystrokes: Original, Permuted	Screen Depth Changes: Original, Permuted	Keystrokes Saved via Permutation
5c2'Qe	Qce52'	6	11, 8	4, 1	3
3.bH1o	Hbo31.	6	11, 8	4, 1	3
a7t?C2#	Cat72?#	7	14, 10	6, 2	4
m3)61fHw	Hmfw361)	8	11, 10	2, 1	1
p4d46*3TxY	TYpdx4463*	10	18, 14	6, 2	4
q80<U/C2mv	UCqmv802</	10	19, 15	7, 3	4
d51)u4;X3wrf	Xduwrf5143);	12	19, 14	6, 1	5
6n04%Ei'Hm3V	EHVnim6043%'	12	24, 17	9, 2	7
m#o)fp^2aRf207	Rmofpaf2207#)^	14	24, 19	10, 4	6

SECURITY RESULTS

Length	Average Entropy Loss
6	7.3
7	8.8
8	10.4
9	12.0
10	13.6
11	15.3
12	17.0
13	18.7
14	20.4
15	22.2
16	24.0
17	25.7
18	27.6
19	29.3
20	31.2

DISCUSSION

We argue that only by empirically quantifying the security-usability tradeoff can we hope to measure and understand effects of changing passwords along either or both dimensions. Although alternative—and arguably better—mobile authentication mechanisms exist [e.g., Fastwords, biometrics], the unfortunate reality is that passwords are too deeply ingrained in our current digital world to be fully replaced in the near term. In the interim, our work is focused on evaluating ways to improve password usability for mobile devices without an unacceptably large sacrifice to security.

LEARN MORE:
http://csrc.nist.gov