THE ART OF PASSWORD CREATION

Blase Ur, Saranga Komanduri, Richard Shay, Stephanos Matsumoto, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Michelle L. Mazurek, Timothy Vidas

Carnegie Mellon University

THE UNIVERSITY of NEW MEXICO

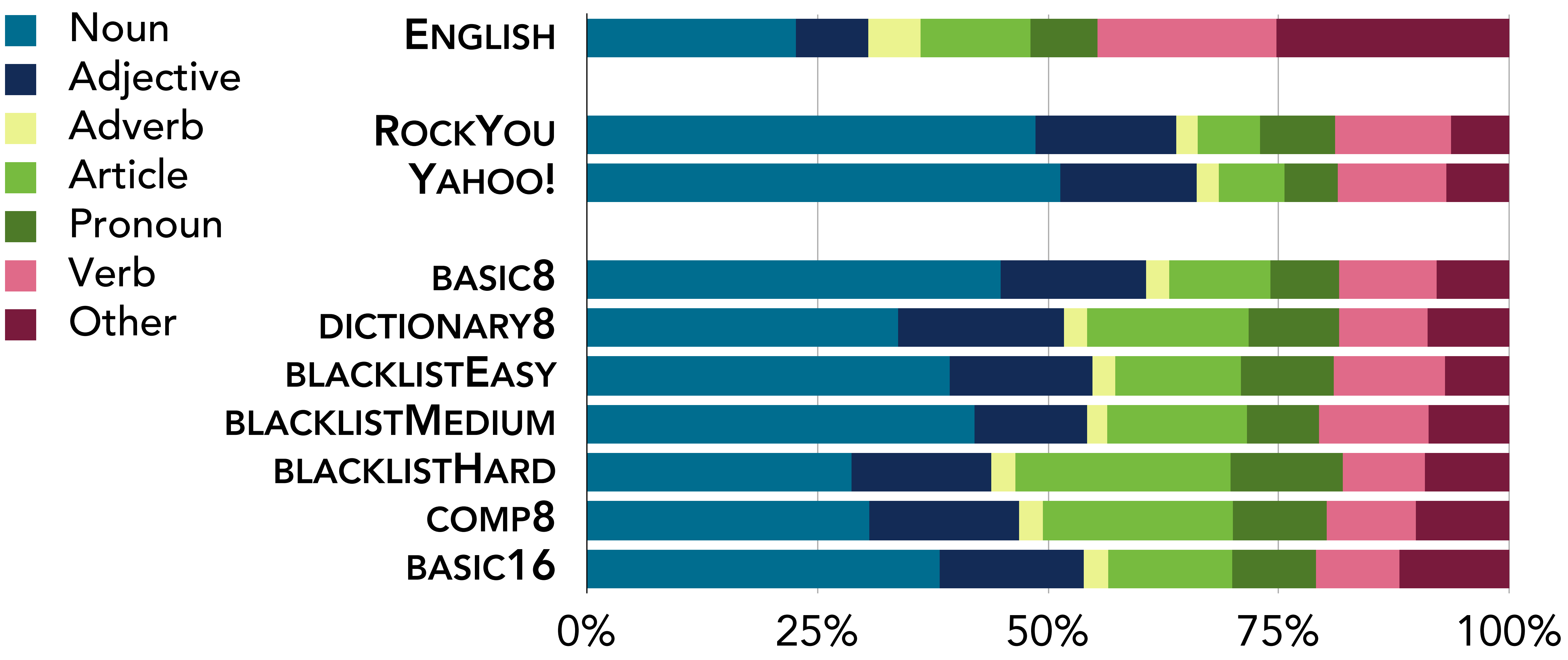
We consider not only how guidance affects password strength, but why

We examine in depth how users create passwords, which words they use, and how the component pieces of passwords relate to each other.

PASSWORD SETS

RockYou	32 million leaked passwords
Yahoo!	450,000 leaked passwords
Basic8	8 or more characters [3]
Dictionary8	Not in the free Openwall dictionary [4]
BlacklistEasy	Not in the Unix dictionary
BlacklistMedium	Not in the paid Openwall dictionary [4]
BlacklistHard	Not in a set of 5×10^9 passwords generated using a probabilistic cracking algorithm [6]
Comprehensive8	Dictionary8, plus an uppercase letter, lowercase letter, digit, and symbol
Basic8	16 or more characters

These seven conditions reference 12,000 passwords collected in an online study [3]



ADJACENT WORDS IN PASSWORDS

Does knowing one password piece help with guessing the next piece?

Using Word Breaker [5] and Google's Web N-gram Corpus3 [1]:

16% of passwords contained at least one digram AB such that p(B|A) > p(B).

40% of AB digrams ranked in the top 100 guesses for B given A; without context, B is ranked in the top 100 only 11% of the time.

WORDS USED IN PASSWORDS

Do passwords use words similarly to English?

Passwords, compared to English: more nouns and adjectives, many fewer verbs or adverbs [2].

Using Jensen-Shannon Divergence: most password sets were similar; **RockYou** was least similar; none very similar to English.

POLICY COMPLIANCE STRATEGIES

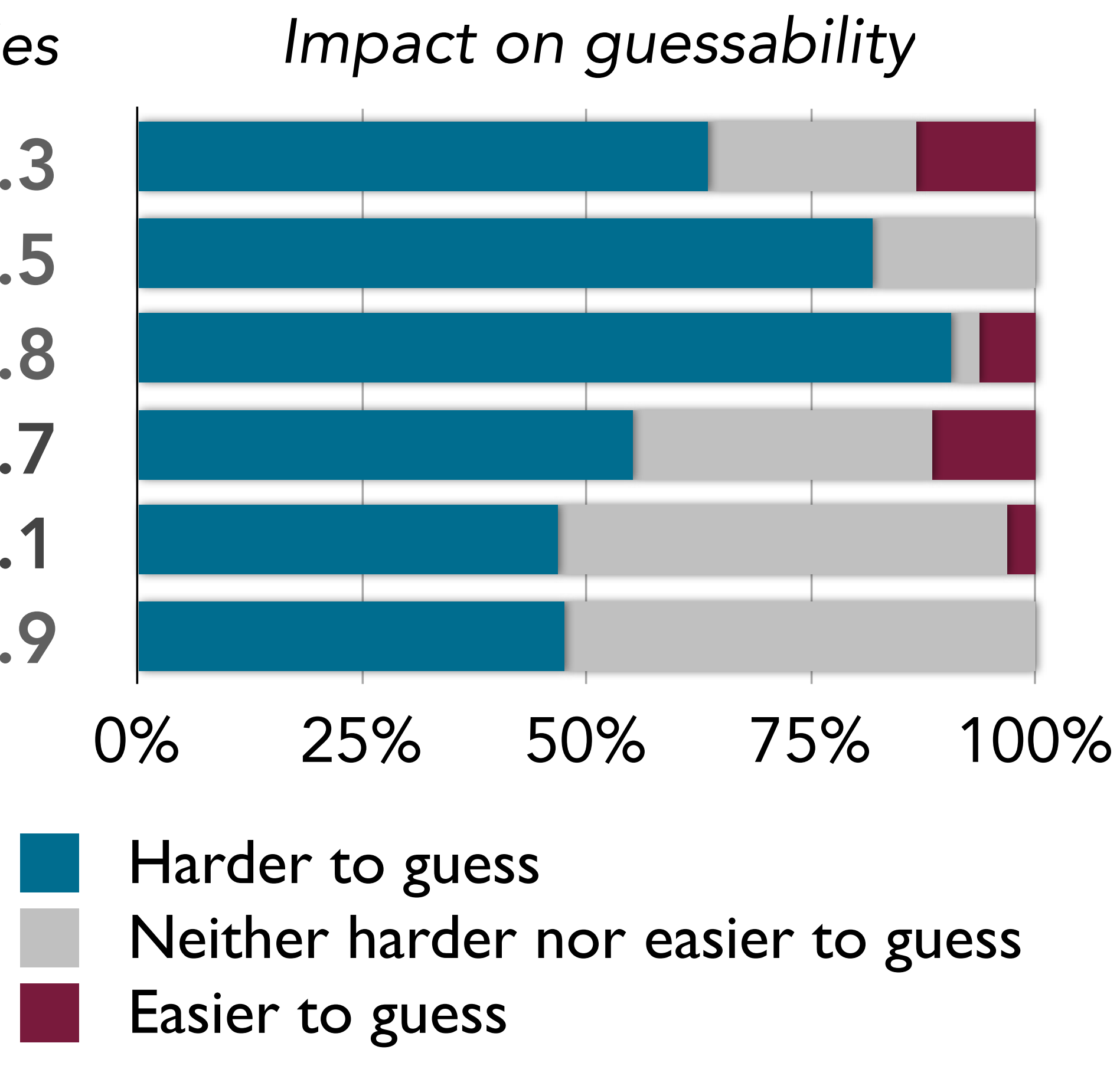
How do users modify rejected passwords?

Using a password-guessing calculator [3], we compared each user's initial (non-compliant) and final (compliant) password.

In all conditions, more passwords became harder to guess than became easier to guess.

Surprisingly, however, many users in **Dictionary8** (13.3%) and **BlacklistHard** (11.5%) ended up with weaker passwords.

	Required retries %	*Mean # of retries*
Dictionary8	19.0	2.3
BlacklistEasy	1.0	1.5
BlacklistMedium	6.0	1.8
BlacklistHard	20.1	2.7
Comprehensive8	52.0	3.1
Basic8	9.5	1.9



[1] T. Brants, A. Franz. Web 1T 5-gram Version 1. Linguistic Data Consortium, Philadelphia. http://www.ldc.upenn.edu/Catalog/CatalogEntry.jsp?catalogId=LDC2006T13 2006.

[2] M. Davies, "The corpus of contemporary American English: 425 million words, 1990–present," Available online at http://corpus.byu.edu/coca/, 2008.

[3] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, and J. Lopez, "Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms," in Proc. IEEE Symp. Security & Privacy 2012.

[4] Openwall. http://www.openwall.com/wordlists/

[5] K. Wang, C. Thrasher, and B. Hsu, "Web scale nlp: a case study on url word breaking," in Proc. WWW, 2011.

[6] M. Weir, S. Aggarwal, B. D. Medeiros, and B. Glodek, "Password cracking using probabilistic context-free grammars," in Proc. IEEE Symposium on Security and Privacy, 2009.

This research was supported by NSF grants DGE-0903659 and CNS-1116776, by CyLab at Carnegie Mellon under grants DAAD19-02-1-0389 and W911NF-09-1-0273 from the Army Research Office, by Air Force Research Lab Award No.~FA87501220139, and by a gift from Microsoft Research.