

Exploring the Usability of Pronounceable Passwords



Shing-Hon Lau, Stephen Siena, Ashutosh Pandey, Sroaj Sosothikul
Lorrie Cranor, Blase Ur, Richard Shay

Carnegie Mellon University
Pittsburgh, PA, USA



Introduction

System Assigned Text Password

- No additional hardware required
- Can be made Cryptographically complex
- Difficult to remember

Research Questions

- Are pronounceable passwords more memorable than random passwords?
- Do users like pronounceable passwords more than random passwords?

References

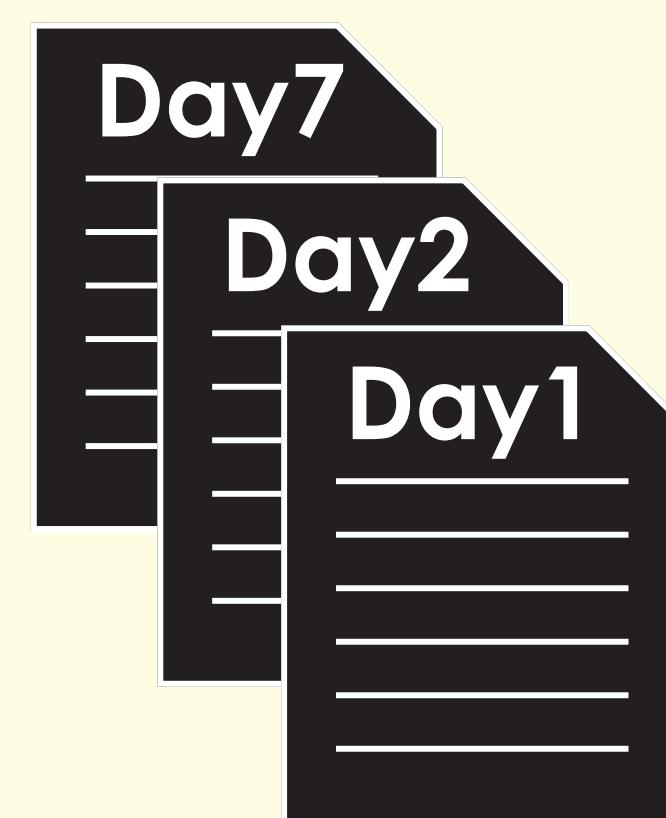
- R. Ganesan, C. Davies, and B. Atlantic. A new attack on random pronounceable password generators. In *Proceedings of the 17th {NIST}-{NCSC} National Computer Security Conference*, 1994.
- M. Gasser. A random word generator for pronounceable passwords. Technical report, DTIC Document, 1975.
- R. Shay, P. G. Kelley, S. Komanduri, M. L. Mazurek, B. Ur, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor. Correct horse battery staple: Exploring the usability of system-assigned passphrases.

Methodology

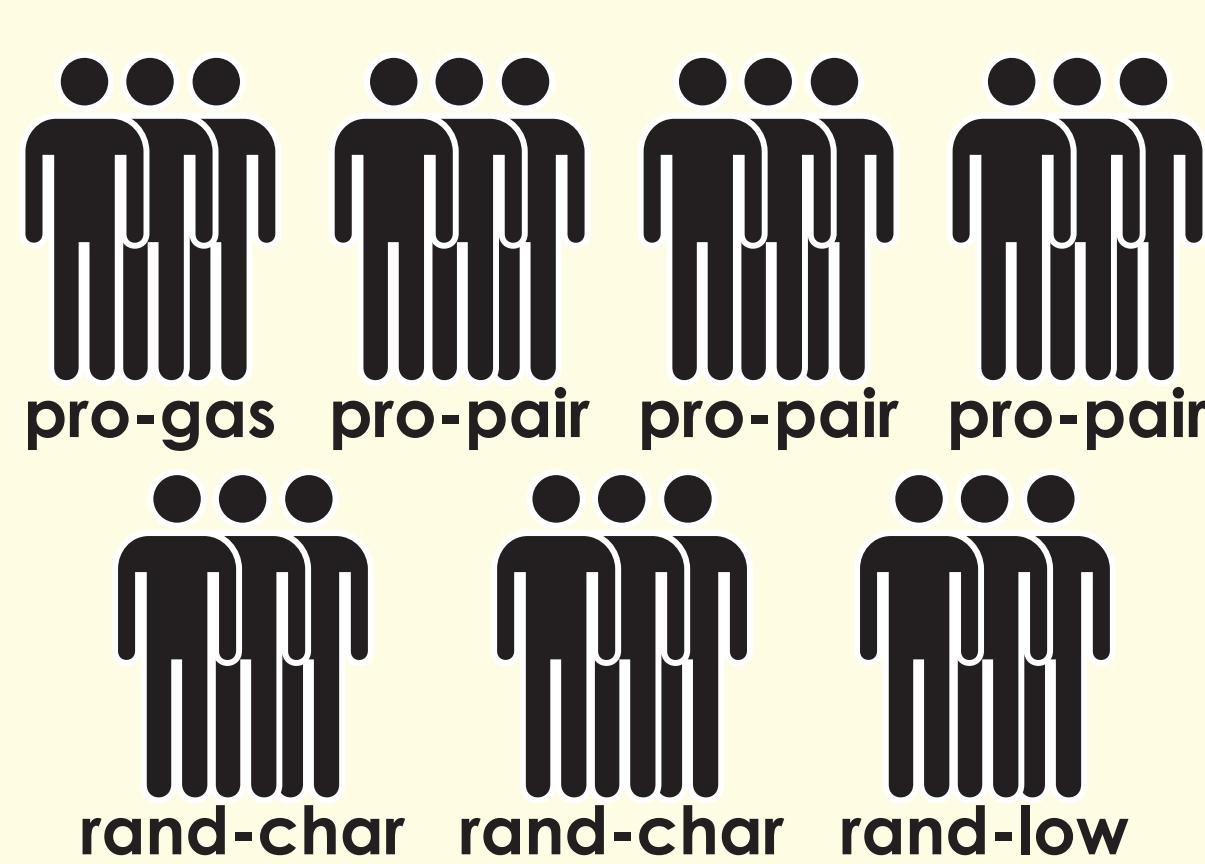
700 Participants



3 Day Survey



100 Participants
Per Condition



Condition	Entropy	Example
pro-gas	30.2	cytuchva
pro-pair-4	30.6	rishespuhi
pro-pair-5	38.2	huthuslawoce
pro-pair-3d2	45.2	sujohu46spucra
rand-char-5	30.0	y Qzw
rand-char-7	42.0	US\$#-P5
rand-low-7	32.9	vfkmlqc

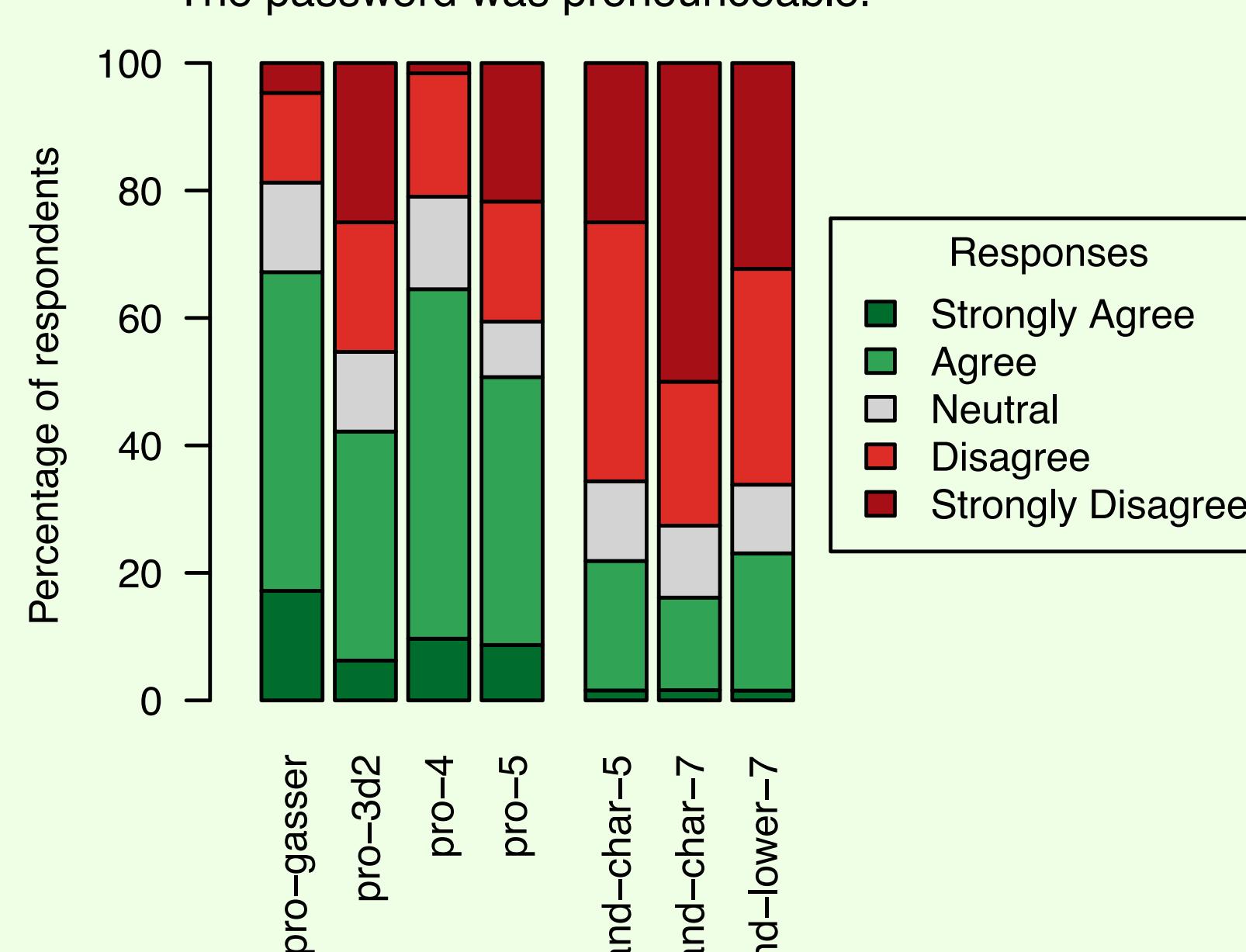
Table 1: Password conditions, Bits of Entropy, and Examples.

Results

Quantitative results

- There was no significant differences, across conditions, in terms of gender, age, degree type, or education.
- There was no statistically significant differences in the dropout rate between conditions.
- There was no statistical difference, across conditions, for storage usage reported for the second or third studies. 251 (56%) of our subjects reported that they did not use storage.
- There was no significant difference between conditions in the number of attempts required to enter the password or the fraction of subjects that successfully recalled the password.

The password was pronounceable.



The password was easy to remember.

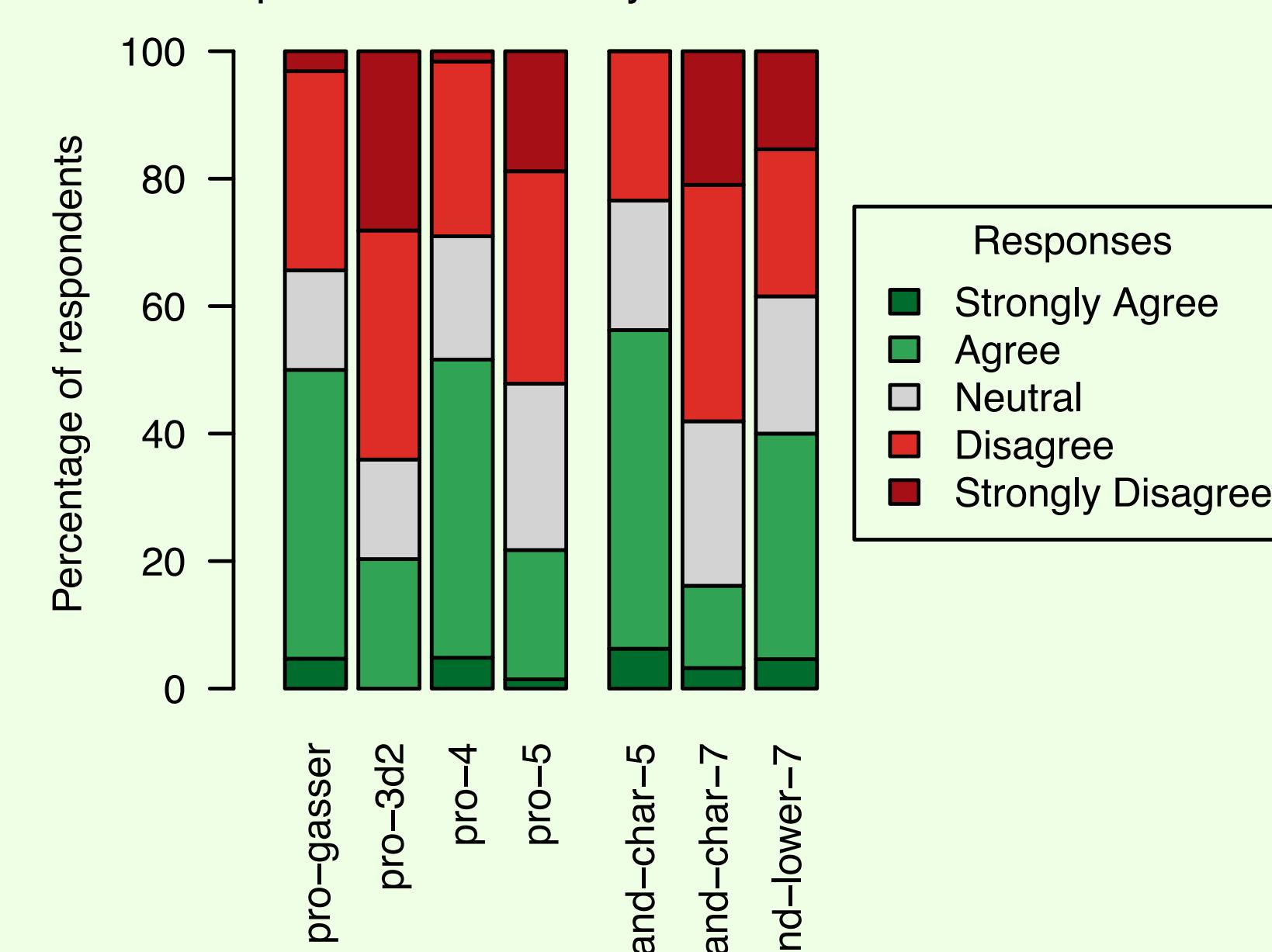


Figure 1: User sentiment towards passwords. Subject responses to sentiment questions are displayed for each password condition. Responses that indicate the password is "good" are colored in green; responses that indicate the password is "bad" are colored in red.

Qualitative results

- Users were concerned about finding the "correct" pronunciation of a password.
- Users were concerned that the shorter passwords may not offer enough security since they did not have uppercase letters, digits, or symbols, which are typically associated with Strong passwords.

Discussion

- The Results suggests that pronounceable passwords may be able to offer additional security without negatively affecting user ability to recall passwords.
- Users need to be told the advantages of the benefits of pronounceable passwords.
- Users must be assured that they are secure, despite the deviation from what is generally considered a strong password.

Participants Quotes

- "ch" can sometimes make different sounds in different contexts
- Participant for pro-pair-4 "gludrechibla"
- It is unlike any word that I have ever seen before and that makes it harder to associate it with something.
- Participant for pro-pair-4 "yuludiwi"
- I disliked the password because it is probably pretty easy to crack via dictionary attack.
- Participant for pro-pair-4 "loflushufa"