Graduate Research and Discovery Symposium (GRADS)

Research and Innovation Month

Spring 2013

Improving the Usability and Security of Digital Authentication

Kevin Juang

Joel Greenstein

Marlena Fraune

Sanjay Ranganayakulu

Improving the Usability and Security of Digital Authentication

Kevin Juang[1], Joel Greenstein[1], Marlena Fraune[2], Sanjay Ranganayakulu[3]

[1]Clemson University, [2]Beloit College, [3]ANSYS

Abstract

The need for both usable and secure authentication is more pronounced than ever before. Due to their ubiquity, recoverability, and low barrier of entry, passwords remain the most common means of digital authentication. However, fundamental human nature dictates that it is exceedingly difficult for people to generate secure passwords on their own. System-generated random passwords can be secure but are often unusable, which is why most passwords are still created by humans. We developed a simple system for automatically generating mnemonic phrases and supporting mnemonic images for randomly generated passwords. We found that study participants remembered their passwords significantly better using our system than with existing systems. To combat shoulder surfing – looking at a user's screen or keyboard as he or she enters sensitive input such as passwords – we developed an input masking technique that was demonstrated to minimize the threat of shoulder surfing attacks while improving the usability of password entry over existing methods.

Introduction

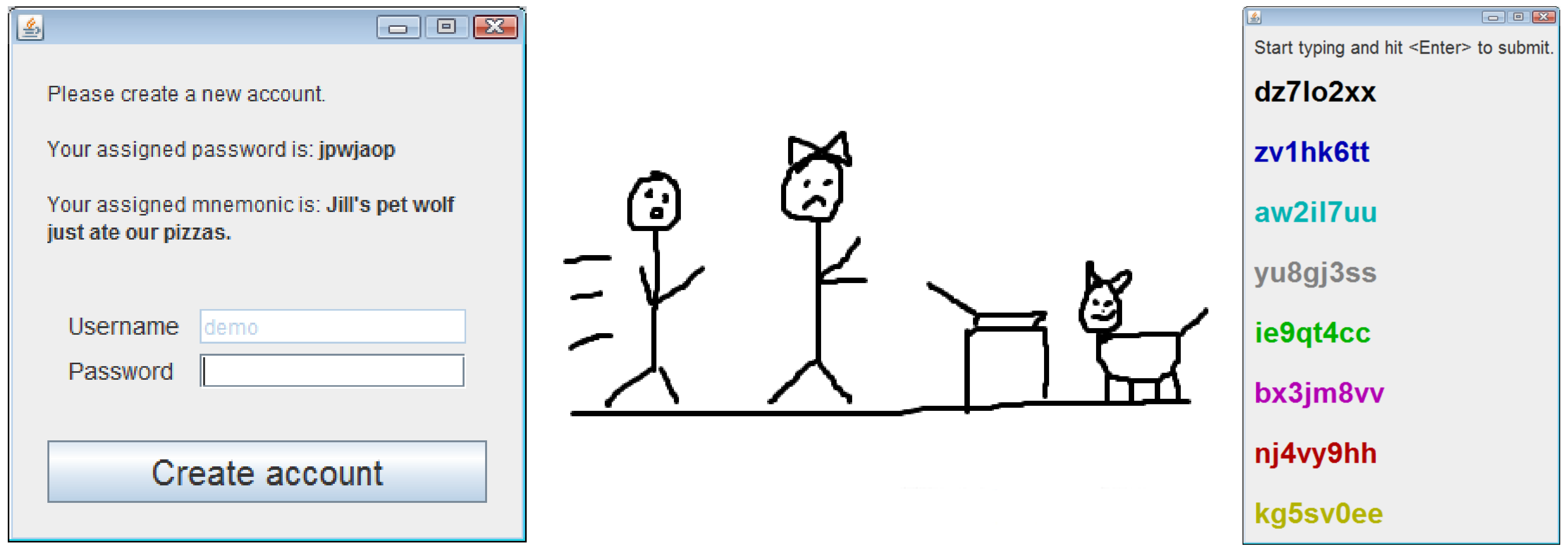
Although much more secure than user-generated passwords, random passwords are hard for people to use due to their inherent disorder. To counteract this fact, we can generate mnemonic phrases to better remember such passwords. These mnemonics can be created either by the user or the system. Converting random passwords into mnemonics can prove quite difficult for users, suggesting a potential advantage for system-generated mnemonics.

We implemented a system with an iteratively developed wordlist that invariably generates drastically simpler phrases compared to previous research. We then added the ability for users to create pictures to be shown later during recall, as seen in Figure 1. To avoid relying on security through obscurity, potential attackers are assumed to have complete knowledge of our system, including the exact wordlist used and dedicated practice on attacking it.

Since the very act of authentication itself can also be a soft spot for unauthorized users to attack, we looked to mitigate the threat of shoulder surfing from observers or hidden cameras. Different techniques can be employed to hide sensitive input, such as the common practice of replacing entered text with bullets. Previous input masking research has focused exclusively on increasing resistance to shoulder surfing but with a large decrease in usability.

To address this gap, we developed Purloin: an input masking technique based on the concept of hiding something in plain view, from Edgar Allan Poe's "The Purloined Letter." By using decoys to mask legitimate input, we strive to combine the usability advantage of unmasked text with the security advantage of masked text.

Because the color and position of the genuine password remain consistent, Purloin users know where to look for feedback and make fewer errors, while attackers are beset by an assortment of false passwords. The system defends against camera attacks and repeated shoulder surfing attacks by locking out intrusion attempts based on any false passwords and notifying the legitimate user.



Please create a new account.

Your assigned password is: **jpwjaop**

Your assigned mnemonic is: **Jill's pet wolf just ate our pizzas.**

Username: demo

Password:

Start typing and hit <Enter> to submit.

dz7lo2xx
zv1hk6tt
aw2il7uu
yu8gj3ss
ie9qt4cc
bx3jm8vv
nj4vy9hh
kg5sv0ee

Figure 1. The mnemonic phrase (left) and picture complement each other as simple but effective memory aids. The decoy text (right) obfuscates the typed password while also acting as a trap for potential attackers.

Method

Our first study utilized a between-subject design to evaluate the usability and security of our mnemonic generation system. Fifty-four participants were assigned, based on a balanced Latin square, to one of the following three conditions: no mnemonic, user-created mnemonic following NIST guidelines (Scarfone & Souppaya, 2009), or our new system. Each participant was assigned three passwords to be recalled later during the first session as well as in a second session after roughly a week. Participants were instructed not to write down or rehearse their passwords or mnemonics. To evaluate the security of our system, twenty-four participants were extensively trained to attack the created accounts in a follow-up study.

Our second study examined the usability and security of input masking techniques using a within-subject repeated measures design. The experimental task was to enter 15 sets of random alphanumeric eight-character passwords. Fourteen participants were recruited in pairs and took turns as both legitimate users and shoulder surfers for all five investigated input masking techniques:

Cleartext	Invisible	Bullet	Interval	Decoy (Purloin)
bx3jm8vv		••••••••	•••••••v	bx3jm8vv nj4vy9hh

Objective variables measured in both studies included account creation time, login time, error rate, and success. The Damerau-Levenshtein distance (Damerau, 1964) and Jaro-Winkler proximity (Winkler, 1990) measured security. Subjective variables included NASA-TLX workload indices and SUS usability scores.

For the majority of our dependent variables, we used a one-way ANOVA with a 95% confidence interval to determine significance. When appropriate, a log transformation was first applied to achieve normality. Given significant results, Tukey's HSD test showed which conditions differed significantly from one another. Success was analyzed using a binary logistic regression.

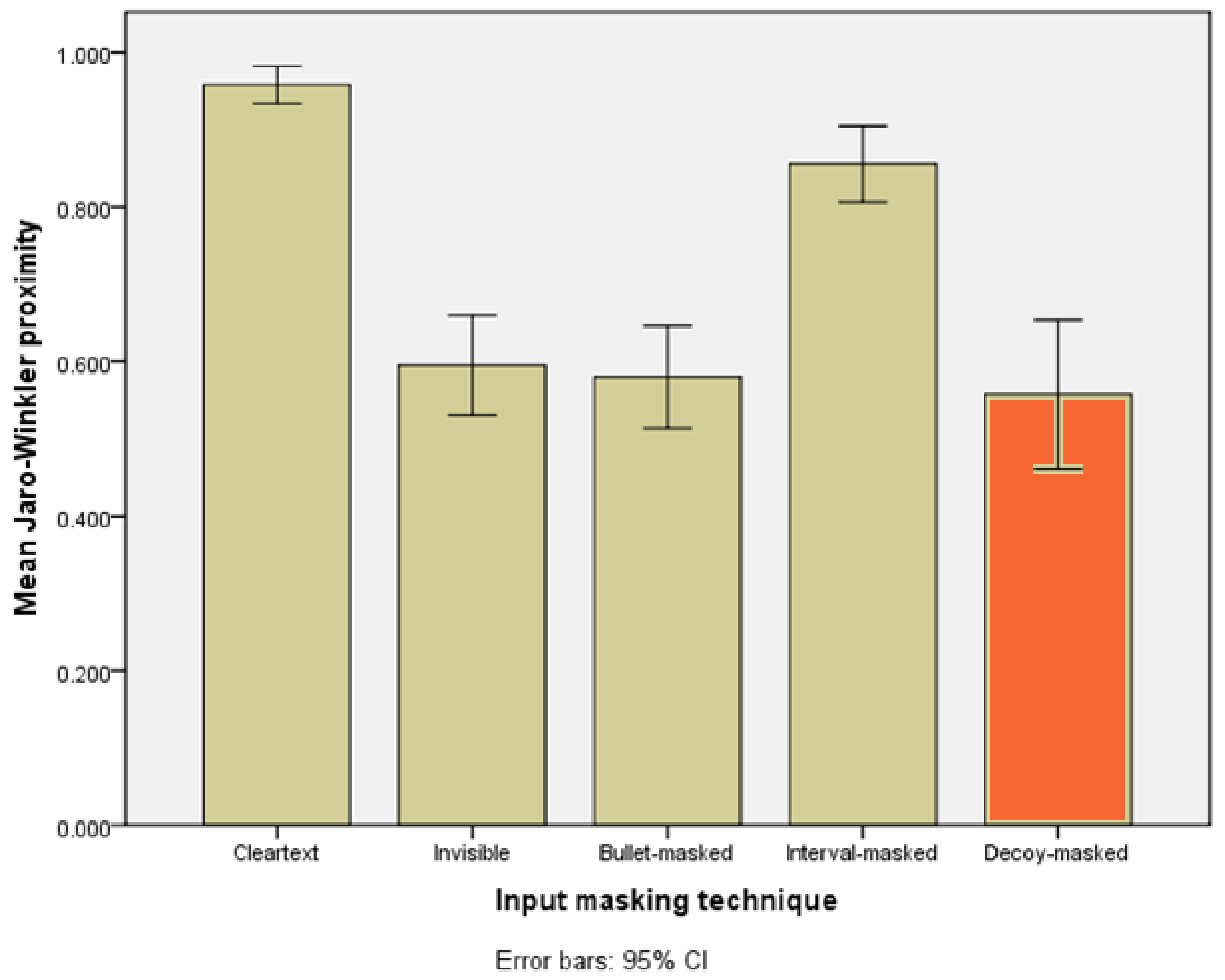


Figure 3. Jaro-Winkler proximity
(smaller values indicate increased security)

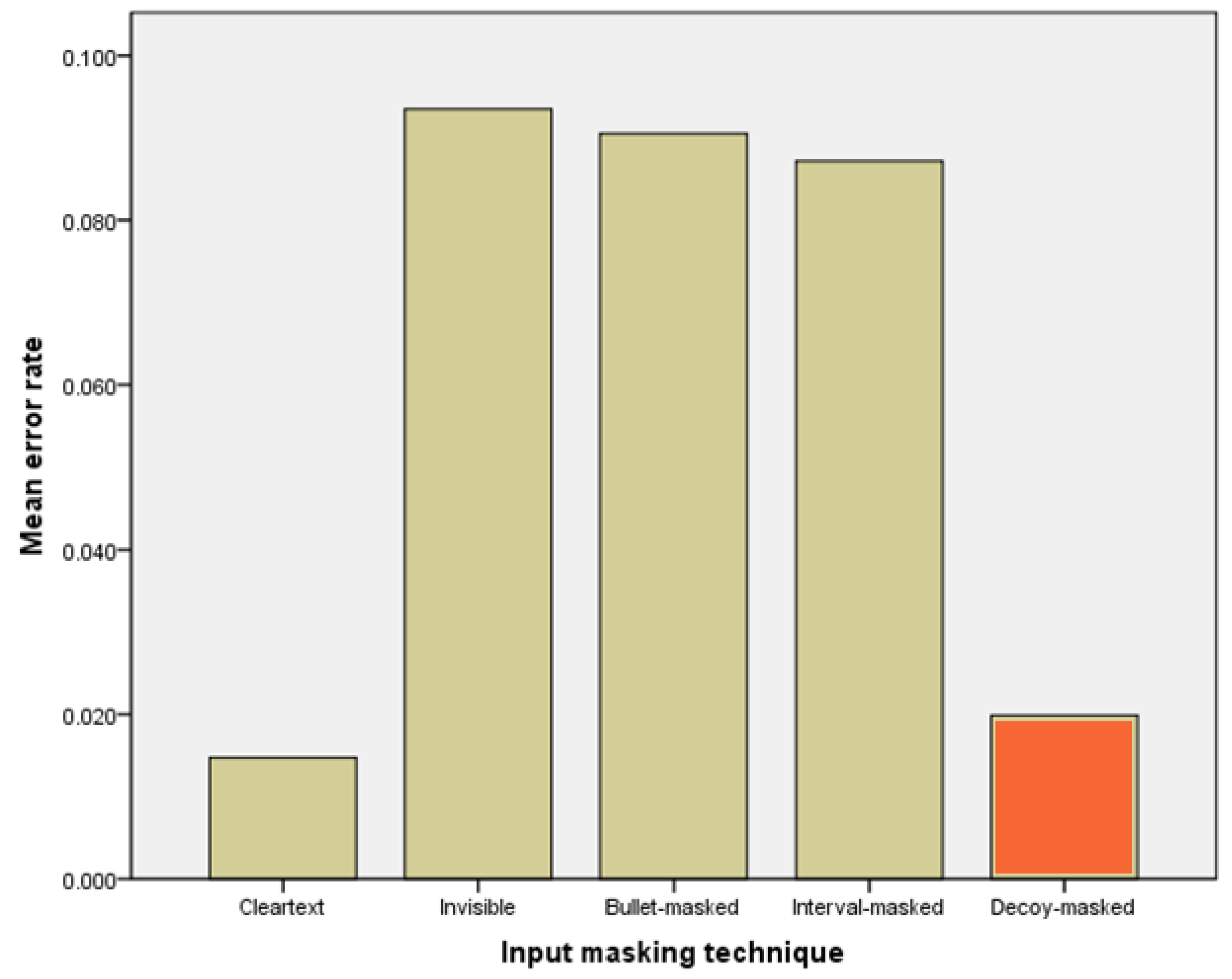


Figure 4. Error rate
(smaller values indicate increased usability)

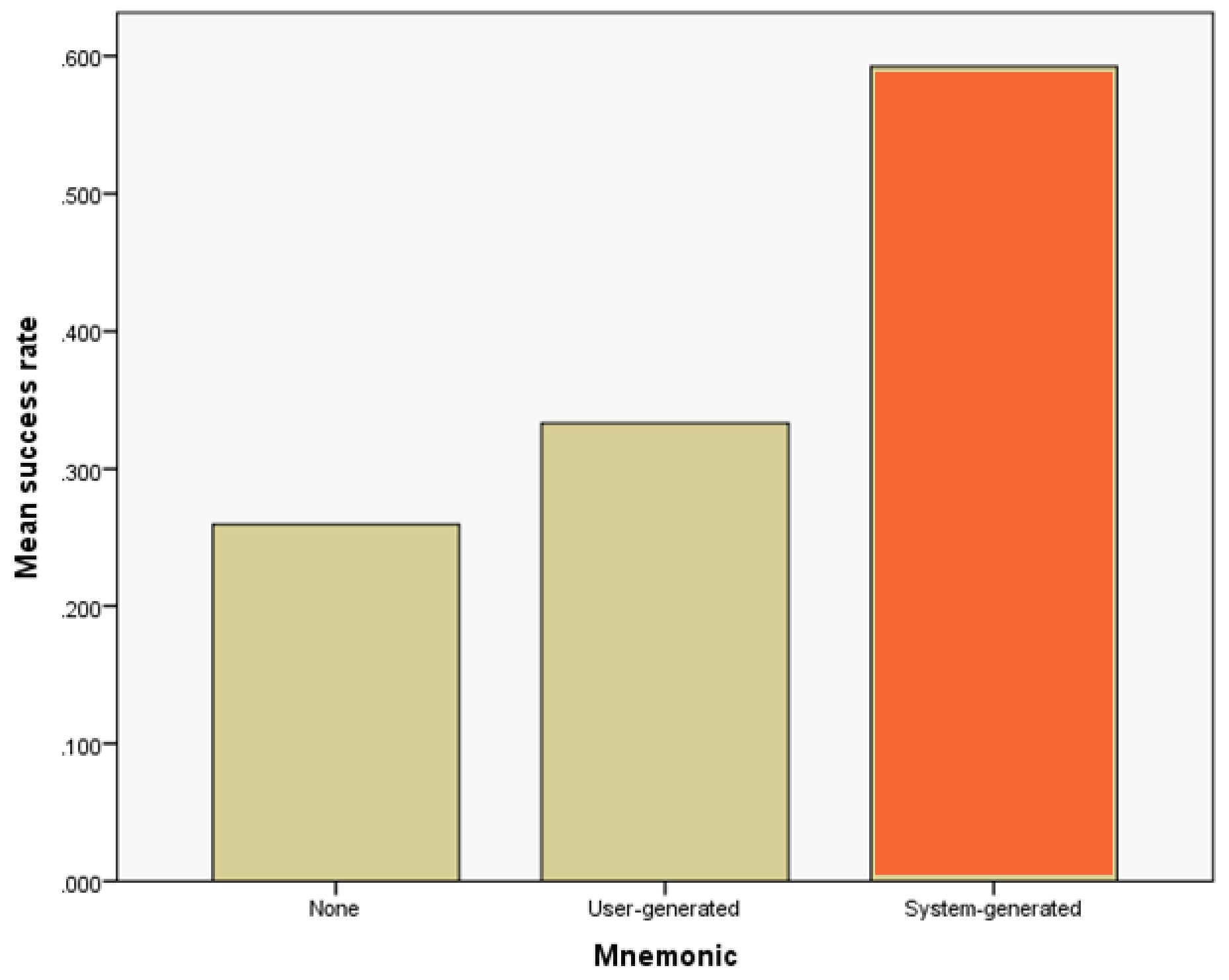


Figure 2. Second-session success rate
(larger values indicate increased memorability)

Results

Our mnemonic generation system performed very well across the board. Although account creation time for the system-generated mnemonic increased, recall time was unaffected. As seen in Figure 2, users were 1.8 times likelier to succeed with our system than with a user-generated phrase and 2.3 times likelier than with no phrase. Security with our system was slightly reduced – equivalent to losing less than three-fourths of a character in password length.

Purloin performed at the top of both security (see Figure 3) and usability (see Figure 4). Bullet masking was secure but near the bottom in usability. Interval masking was near the bottom of both.

Discussion

One of the greatest benefits of our systems is the ease of transition from existing security practices, as they are simple enough to require neither training nor special equipment such as a touchscreen or eye tracker. They work cleanly with the password systems and policies already in deployment today.

Not a single intrusion attempt against any of our systems was successful. Even so, the findings suggest that lengthening the passwords by even one character could increase net security while remaining much more usable than current systems.

We strongly recommend against the interval masking commonly seen in mobile devices. In light of threats from the ever-growing computing power widely available, we seek to expand our work to integrate both mobile devices and longer passphrases, which our systems are particularly well positioned to support.

References

1. Damerau, F. (1964). A technique for computer detection and correction of spelling errors. Communications of the ACM, 7(3), 171-176.
2. Scarfone, K., & Souppaya, M. (2009). Guide to enterprise password management (draft): Recommendations of the National Institute of Standards and Technology. Gaithersburg, MD: U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology.
3. Winkler, W. E. (1990). String comparator metrics and enhanced decision rules in the Fellegi-Sunter model of record linkage. Proceedings of the Section on Survey Research Methods, 354-359.