On the Memorability of System-generated PINs: Can Chunking Help?

Jun Ho Huh
Honeywell ACS Labs
Golden Valley
USA
junho.huh@honeywell.com

Hyoungshick Kim
Sungkyunkwan University
Suwon
Korea
hyoung@skku.edu

Rakesh B. Bobba
University of Illinois
Urbana Champaign
USA
rbobba@illinois.edu

Masooda Bashir
University of Illinois
Urbana Champaign
USA
mnb@illinois.edu

Konstantin Beznosov
University of British Columbia
Vancouver
Canada
beznosov@ece.ubc.ca

ABSTRACT

To ensure that users do not choose weak personal identification numbers (PINs), many banks give out *system-generated PINs*, using computers to generate random PINs. 4-digit is the most commonly used PIN length, but 6-digit system-generated PINs are also becoming popular. The increased security we get from using system-generated PINs, however, comes at the cost of memorability. And while banks are increasingly adopting system generated, and longer (than traditional 4-digit) PINs, the impact on memorability of such PINs is not really known.

We conducted a large-scale online user study to investigate how memorability can be affected by increasing the PIN length, and how number *chunking* techniques (breaking a single number into multiple smaller numbers) can be applied to improve memorability. Our study shows that system-generated 4-digit PINs outperform 6-, 7-, and 8-digit PINs in long-term memorability, but that there is no significant difference between 6-, 7-, and 8-digit PINs. Our results also show that chunking can improve memorability of system-generated PINs. For example, 8-digit PINs broken into three chunks of 2-2-4 digits (00—00—0000) outperformed non-chunked 6-, 7-, and 8-digit PINs in long-term memorability, without much increase in the time taken to authenticate. Our study shows that chunking is a cheap, practical, yet effective solution that can be implemented with a few small modifications on the front-end user interface.

1. INTRODUCTION

Over the years, many user authentication technologies have been designed and deployed on security-critical systems. Some popular technologies include: passwords, personal identification numbers (PINs), and digital certificates. Among these, "what you know" forms of authentication, generally, passwords or PINs are still the dominant technology, due to their familiarity and low costs in implementation and deployment. The goal of a PIN is to give the user quick and easy, yet sufficiently secure access to areas such as personal bank and credit card accounts. Most commonly used PINs are 4 digits long and are selected by users. User-selected PINs, however, are known to have low entropy [1], meaning that users choose their PINs from a small subset of PINs that are easy to remember and easy to guess (e.g., 1234, 0000). Such PINs are vulnerable to brute-force attacks.

This is why banks are adopting system-generated and longer (e.g., 6-digit) PINs, which take advantage of a larger search space. Randomly generated PINs, when used together with an account lock-out policy, can be highly effective against online brute-forcing attacks. The biggest drawback with longer, system-generated PINs, however, is their memorability [2]. Although banks are moving towards system-generated 6-digit PINs (e.g., Banks in Switzerland assign 6-8 digit PINs), the impact on memorability is not clearly known. Are the banks making the right decision in moving toward longer system-generated PINs?

We conducted a large-scale online user study through Mechanical Turk, recruiting a total of 1,904 participants to test the memorability of system-generated PINs of varying lengths, from 4 to 8 digits. Our study shows that even though 4-digit PINs clearly outperform PINs of all other lengths in memorability, there is no significant difference in memorability between 6-, 7-, and 8-digit PINs.

To investigate ways of improving memorability, we applied different techniques for "chunking" numbers [3] on system-generated PINs, and studied their effects through the same online study. Phone numbers are a good example of chunking numbers. In the U.S. a ten-digit phone number is chunked into smaller chunks of 3-3-4 (000-000-0000) to help people remember it easily. Our results suggest that chunking techniques can indeed help users better remember system-generated PINs. One of the effective chunking policies, 8:2-2-4, for example, outperformed all non-chunked 6-, 7-, 8-digit PINs in long-term memorability with statistical significance (one-sided chi-squared tests $P < 0.1$). To the best of our knowledge, this is the first large-scale study on the impact of applying chunking techniques to *randomly generated information* and specifically to PINs, including the 6-digit PINs that many banks are currently using. Previous studies [4] often focused on showing that chunking is useful for information that has some meaning to a user and have been based on small-scale lab studies, with small number of participants.

Another key contribution of our study is the investigation of a variety of chunking combinations (referred to as "chunking

policies") to investigate how different arrangements of smaller chunks can affect memorability. In total, we investigated 9 different chunking policies with varying PIN lengths, showing that 6:2-4 (00-0000) and 8:2-2-4 (00-00-0000) are very effective policies for memorability. Our results also show that the order in which the smaller chunks are arranged can affect memorability and usability.

2. HYPOTHESES

This work was motivated by research questions such as how usable and memorable are system-generated 6-digit PINs compared to 4-digit PINs? Should banks also consider using 7- or 8- digit PINs? Can chunking techniques help improve the memorability of system-generated PINs, and if so, how?

Based on these research questions and out intuition, we hypothesized and examined the following three outcomes:

1. The memorability of system-generated 6-digit PINs is worse than 4-digit PINs.
2. The memorability of system-generated 6-digit PINs is better than 7- and 8-digit PINs.
3. The memorability of longer (6-, 7- and 8-digit) system-generated PINs improves with chunking.

Table 1. Long-term memorability

Policy	# Participants	# Failed	% Correct PIN
4	126	35	72%
6	135	64	53%
6:2-4	129	50	61%
7	133	65	51%
7:4-3	132	57	57%
8	125	61	51%
8:4-4	121	50	59%
8:2-2-4	113	42	63%
8:2-4-2	116	51	56%

3. DISCUSSION

3.1 6-digit versus 4-digit PINs

System-generated 4-digit PINs clearly outperformed 6-dgit PINs in both short-term and long-term memorability; both results show statistical significance (one-sided chi-squared tests $P < 0.1$). Hence, our results accept the first hypothesis. The memorability score difference in the short-term was marginal: 99% for 4-digit PINs versus 96% for 6-digit PINs. However, the gap was much bigger in the long-term test (see Table 1), in which 6-digit PINs (53%) scored 19% worse than 4-digit PINs (72%). 6-digit PINs also showed longer authentication times, with statistical significance (unpaired on-tailed t-tests $P < 0.1$), taking about 4 seconds longer on average in the short-term test and about 37 seconds longer in the long-term test. Banks should consider all of those memorability and usability trade-offs when moving from 4- to 6-digit system-generated PINs.

3.2 Should banks consider using 7 and 8-digit PINs?

Our results show that between system-generated 6-, 7-, 8-digit PINs, there is no statistically significant difference in memorability, rejecting the second hypothesis. As for authentication time, 6-digit PINs did outperform both 7- and 8-digit PINs in the short-term test, but not in the long-term test, indicating that over time, 6-digit PINs lose its shorter authentication time advantage. Looking at those results, there is no reason for banks to rule out 7- or 8-digit system-generated PINs if they are considering increasing the PIN length. If enhancing PIN security is a primary concern for a bank, lengths 7 and 8 should also be considered and carefully evaluated.

3.3 Can chunking technique improve PIN memorability?

Our results accept the third hypothesis on 6- and 8-digit PINs, showing that chunking policy 6:2-4 (00-0000) outperforms both non-chunked 6 and 7 policies, and that 8:2-2-4 (00-00-0000) outperforms all non-chunked policies (6, 7, and 8) in long-term memorability with statistical significance. In the short-term test, all chunked policies (except for 7:4-3) showed small improvement over their peer non-chunked PINs; all policies achieved very high short-term memorability scores, ranging between 96% and 99%. In the long term, however, we observed greater improvements in memorability (see Table 1), in that all of the chunked policies scored better than their peer non-chunked policies.

In the recall difficulty survey, policies 6:2-4, 7:4-3 and 8:2-2-4 scored better than all of the non-chunked 6, 7, and 8 policies. The percentage of participants who felt that 8:2-2-4 PINs were difficult to remember was smaller than the percentage who found 6 and 7 PINs hard to remember. Policy 7:4-3, however, failed to show a statistically significant difference from 7, rejecting the third hypothesis on 7-digit PINs. Likewise, other 8-digit chunking policies did not show a significant difference from policy 8. Although our analysis does indicate that chunking improves memorability, not all policies have the same effect; depending on the arrangements of smaller chunks, memorability can be affected significantly (see Table 1). Hence, if a bank is going to use a chunking policy, different chunking arrangements and PIN lengths must be carefully evaluated.

4. REFERENCES

[1] Bonneau J., Preibusch S., Anderson R., A birthday present every eleven wallets? The security of customer-chosen banking PINs. In FC' 12: The 16th International Conference on Financial Cryptography and Data Security 2012.

[2] Bishop M., Password management. In Compcon Spring '91. Digest of Papers, pages 167–169, Feb 1991.

[3] Gobet F., Lane P. C. R., Croker S., Cheng P. C. H., Jones G., Oliver I., and Pine J. M., Chunking mechanisms in human learning. Trends in Cognitive Sciences, 5(6), June 2001.

[4] Carstens D. S. and Malone L. C., Applying Chunking Theory in Organizational Password Guidelines. Journal of Information, Information Technology, and Organizations, 2006