ScienceDirect

Computers & Security
Volume 31, Issue 4, June 2012, Pages 484-496

PIN selection policies: Are they really effective?

Hyoungshick Kim [a], Jun Ho Huh [b]

Show more

Share Cite

https://doi.org/10.1016/j.cose.2012.02.003
Get rights and content

Abstract

Users have conflicting sets of requirements when it comes to choosing Personal Identification Numbers (PINs) for mobile phones or other systems that use PINs for authentication: the conflict lies between the 'easy to remember' usability requirement and the 'hard to guess' security requirement. Users often ignore the security requirement and choose PINs that are easy to remember and reuse, making it also easy for attackers to guess and compromise them. Just as the password strength is controlled through various password policies, PIN selection policies may be used to help users choose stronger PINs and meet various security requirements. An example policy would not allow the use of the most commonly selected PINs.

An online user study was conducted to investigate the effectiveness of such PIN selection policies, requesting the participants to choose PINs under some carefully designed policies. The participants were also asked to record the memorability (remembrance difficulty) score of each PIN, indicating how easy/hard it was to remember the selected PIN. Based on the entropies calculated on the collected PINs and their memorability scores, this paper demonstrates that restricting some number of commonly used PINs (e.g. restricting the 200 most commonly used ones) is beneficial: this type of policy would significantly increase the randomness of PINs without incurring significant memorability overhead. Our results also showed that any PIN- or PIN-pattern-based blacklisting policy should be constructed with caution since the total PIN space may become too small, making it easier for attackers to guess PINs.

Introduction

Mobile phones used to be simple. One could simply make phone calls and send/receive text messages. With the emergence of smart phones, however, more and more people have also started using them as a digital-wallet, storing sensitive information like credit cards, identity cards, loyalty/gift cards, vouchers, and mobile banking tokens (Anderson, 2011). Just as one would try to safeguard a wallet full of cash and credit cards from strangers, a digital-wallet user also wants to protect its contents through strong user authentication mechanisms. Among many authentication mechanisms available, Personal Identification Numbers (PINs) are dominantly used. A PIN is a *numeric password* that the user must type into the mobile phone to authenticate its use.

Unlike biometric and smart card authentication, PINs are easy to implement and do not require extra hardware support. This is what attracts most of the mobile phone companies to use PINs as their primary authentication mechanism. However, PINs too have their own inherent limitations – namely, memorability and security. Problems arise because of the following two conflicting requirements:

1. usability – PINs should be easy to remember;
2. security – PINs should be secure, meaning they should be randomly distributed and difficult to guess; a user should change their PINs frequently, and use different PINs on different accounts.

In practice, it is difficult to satisfy all of these requirements. A PIN that is difficult to guess is also likely to be hard to remember. As one would imagine, many users choose PINs that are easy to remember without really paying close attention to the security implications. Trivial PINs like '1234' and '0000', users' birthdays or telephone numbers are often used. A recent study shows that among 204,508 recorded PINs, 15% of them were part of the top 10 most commonly used PINs (Amitay, Jun 2011). Similar trends are evident for passwords, which are a more general form of PINs (Vance, Jun 2010). Such a trend implies that the actual space of PINs used is much smaller than the theoretical space ($10^{\text{length of the PIN}}$), dramatically increasing the likelihood of an attacker compromising a PIN through brute-force type of attacks. One motivation of our work is to investigate the extent that this PIN space can be affected by helping the users choose stronger PINs.

Based on a large dataset of real PINs collected from an iPhone application (Amitay, Jun 2011), Fig.A.1 shows how frequent each button on the keypad was used. This clearly demonstrates a poor PIN selection practice: buttons '1', '2' and '0' were used much more often than '8', '6' and '7'. Such statistical information can be misused by attackers to make effective guesses for the PINs. To prevent users from using bad PIN selection practices and choosing weak PINs (that are easy to guess), devices/applications may enforce various PIN selection policies. These policies capture security requirements that must be satisfied upon selecting a PIN; an example policy might be that 'a PIN shall not have any duplicating number'. Such policies, in theory, should help users choose stronger PINs; but how do we know that they really work well in practice? Precisely predicting how the security and usability requirements stated above will be affected by different policies can be difficult. For instance, if a policy restricts the use of 10 most popular PINs, the next top 10 PINs will soon replace them, becoming the new 10 most popular PINs. Usability would definitely be affected by this policy, but have we really improved PIN security?

To answer these questions, an online survey was conducted, asking the 332 participants to select PINs while conforming with carefully designed PIN selection policies. To maximize consistency in the participants' attitude and perception towards choosing PINs, the scope of the study was set to focus on locking mobile phones – this information was made clear to the participants prior to starting the survey. By narrowing down the scope, we wanted the participants to have similar perception on the level of complexity required/necessary for their PINs. For instance, a participant's perception may be different when it comes to choosing PINs for banking purposes. Based on the survey results, the effectiveness of each policy was analysed and suggestions were made on how the policies should be designed. This paper contributes in the following areas: (1) an analysis of the characteristics of the PINs used on mobile phones, and (2) security and usability evaluation of the proposed PIN selection policies.

The following section explains the need for PIN selection policies and explores related work, mainly in the areas of password security and policies. Section 3 analyses the distribution of a sample PIN dataset for mobile phones that have been generated free from any PIN selection policies. This puts us in a position to describe the methodology of our own study in Section 4, and evaluate the effectiveness of different PIN selection policies in Section 5. Our conclusions and future work are in Section 6.

Section snippets

Related work

User authentication is an integral part of security-critical systems that manage sensitive information or provide personalised services. Some commonly employed user authentication technologies include passwords, PINs, digital certificates, physical tokens such as smart cards, one-time passwords, transaction profile scripts, and biometric identification. Among these, 'what users know' type of authentication – generally passwords or PINs – is still the dominant technology; this is due to its low…

What real world PINs look like

This section shows that the actual distribution of the real world PINs, generated free from any PIN selection policy, is quite different from the ideal uniform distribution. A large sample of PINs collected from an existing iPhone application called 'Big Brother Camera Security' (Amitay, Jun 2011) was used to show this: it anonymously collected PINs from 204,508 users that were used for locking the application. The users, through the end user licence terms of the application, have agreed that…

Methodology

Section 3 showed that the PIN distribution for mobile phones is highly skewed due to the tendency of the users to select weak PINs that are easy to remember. Such statistical information can be beneficial to an attacker whose goal is to compromise users' PINs. How can a better PIN distribution be achieved? As it was discussed in Section 2, one simple solution is to enforce PIN selection policies to ensure that users do not choose weak PINs (see Section 2). To examine the effectiveness of PIN…

Results and recommendations

This section looks at how effective the policies designed in Section 4.2 can be in improving the PIN distribution for mobile phones. Based on the results collected from the online survey, this section studies (1) the number of participants who had to change the PINs they selected first in order to conform with the stricter PIN selection policy, (2) how the participants felt about their changed PINs, and (3) the impact of the stricter policies on the randomness of the PINs selected.

For 4-short,…

Conclusions and future work

When it comes to choosing PINs for mobile phones or any other system, users face conflicting set of requirements between security and usability: how easy is it to remember versus how hard is it for an adversary to guess. The reality is that, the users often ignore the security requirements and choose ones that are easy to remember and reuse. This provides opportunities for attackers to efficiently make guesses and compromise PINs.

To help users choose stronger PINs, PIN selection policies may be …

Acknowledgements

We thank Daniel Amitay for sharing his collected PIN datasets with us. The authors would like to thank Ross Anderson, Mike Bond, and Katherine Kim for their careful attention and insightful comments. Not least, we would like to thank everyone who has participated in the user study.…

Hyoungshick Kim is a Ph.D. candidate in the Computer Laboratory at the University of Cambridge as a PhD student. He received the B.S. degree from the Department of Information Engineering at Sungkyunkwan University in Korea and M.S. degree from the Department of Computer Science at KAIST in Korea, in 1999 in 2001, respectively. He previously worked for Samsung Electronics as a senior engineer from May 2004 to September 2008. He also served a member of DLNA and Coral standardization for DRM…

Recommended articles

References (20)

K.-P.L. Vu *et al.*
Improving password security and memorability to protect personal and organizational information
International Journal of Human-Computer Studies (2007)

D. Amitay
Most common iPhone passcodes
(Jun 2011)

R. Anderson
Can we fix the security economics of federated authentication?

Apple Inc. Licensed application end user license agreement,...

A.S. Brown *et al.*
Generating and remembering passwords
Applied Cognitive Psychology (2004)

W.E. Burr *et al.*
Electronic authentication guideline
(2006)

A. Clauset *et al.*
Power-law distributions in empirical data
SIAM Review (2009)

S. Gaw *et al.*
Password management strategies for online accounts

D. Hart
Attitudes and practices of students towards password security
Journal of Computing Sciences in Colleges (2008)

P.G. Inglesant *et al.*

The true cost of unusable password policies: password use in the wild

There are more references available in the full text version of this article.

Cited by (32)

Story-based authentication for mobile devices using semantically-linked images

2023, International Journal of Human Computer Studies

Show abstract

Two-Thumbs-Up: Physical protection for PIN entry secure against recording attacks

2018, Computers and Security

> *Citation Excerpt :*
>
> …For comparison purposes, we also calculated the partial guessing entropy of the existing authentication methods: 4-digit PINs, 6-digit PINs and Android patterns. As for the traditional 4-digit PINs, we used a PIN dataset consisting of 204,508 PINs that was collected through an iPhone application (Kim and Huh, 2012). As for the traditional 6-digit PINs, we extracted 383,914 6-digit PINs from the popularly known "RockYou" (14 million) and "Yahoo" (0.5 million) password datasets.…

Show abstract

GestureMeter: Design and Evaluation of a Gesture Password Strength Meter ↗

2023, Conference on Human Factors in Computing Systems - Proceedings

ARJUNA: An accessible pin entry model in smartphones for persons with low vision ↗

2023, Internet Technology Letters

"The Same PIN, Just Longer": On the (In)Security of Upgrading PINs from 4 to 6 Digits ↗

2022, Proceedings of the 31st USENIX Security Symposium, Security 2022

PassMon: A Technique for Password Generation and Strength Estimation ↗

2022, Journal of Network and Systems Management

View all citing articles on Scopus ↗

Hyoungshick Kim is a Ph.D. candidate in the Computer Laboratory at the University of Cambridge as a PhD student. He received the B.S. degree from the Department of Information Engineering at Sungkyunkwan University in Korea and M.S. degree from the Department of Computer Science at KAIST in Korea, in 1999 in 2001, respectively. He previously worked for Samsung Electronics as a senior engineer from May 2004 to September 2008. He also served a member of DLNA and Coral standardization for DRM interoperability in home networks. His current research interest is focused on privacy and anonymity in complex networks and distributed systems.

Jun Ho Huh is a postdoctoral research associate in Information Trust Institute, University of Illinois at Urbana-Champaign. He received his Ph.D. degree from Oxford University, investigating new ways of applying Trusted

Computing and virtualization to the design of trustworthy audit/logging systems. At ITI, he is currently involved in the design and development of a least-privilege access control system for DCS/SCADA systems.

View full text