“The Same PIN, Just Longer”: On the (In)Security of Upgrading PINs from 4 to 6 digits

Collins W. Munyendo, Philipp Markert, Alexandra Nisenoff, Miles Grant, Elena Korkes, Blase Ur, and Adam J. Aviv
Motivation

- 4-digit PINs have previously been the default method of mobile authentication.
- Companies like Apple now encourage users to select a 6-digit over 4-digit PINs.

Is this a good thing?
Research Questions

1. How do users select a 6-digit PIN having previously selected a 4-digit PIN?

2. How does the upgrade process and justification provided impact security and usability?

3. How predictable is a user’s 6-digit PIN if their previous 4-digit PIN is known?
Study Design

4-digit PIN Selection
A PIN protects your data and is used to unlock your smartphone.

Creating a 4-digit PIN

Device Use Questions

Instructions
To continue the study, now you must select a 6-digit PIN.

On the next page, you will create a 6-digit PIN that you would likely use to unlock your primary smartphone. To set your 6-digit PIN, you will first confirm your 4-digit PIN and then select the 6-digit PIN.

Follow-up Questions

Create a 6-digit PIN
A PIN protects your data and is used to unlock your smartphone.

12/26

1
2
3
4
5
6
7
8
9
0

GW
RUB
6-digit PIN Treatments

Neutral
“To continue the study, now you must select a 6-digit PIN.”

Upgrade
“Imagine you are upgrading your smartphone that requires PINs longer than 4 digits, so now you must select a 6-digit PIN.”

Security
“Research has shown that the 4-digit PIN you selected is insecure and can easily be guessed. To continue the study, now you must select a 6-digit PIN.”

Breach
“Imagine someone learned your 4-digit PIN and to protect your smartphone, now you must select a 6-digit PIN.”

No-sub Blocklist was enforced.

1234
001234
120034
123456

"The Same PIN, Just Longer": On the (In)Security of Upgrading PINs from 4 to 6 digits
Collins W. Munyendo, Philipp Markert, Alexandra Nisenoff, Miles Grant, Elena Korkes, Blase Ur, and Adam J. Aviv
Recruitment & Demographics

- Recruited 1,010 participants from the US using Prolific.
- Each treatment was assigned at least 200 participants.
- Participants used their own smartphones for the study.
What did we find?
Untargeted Attacker

- Used to guess both 4- and 6-digit PINs.
- Attacker has no information about the victim.
- Use datasets from prior work [1,2] to do guessing.
- Guesses the PINs in descending frequency order.

"The Same PIN, Just Longer": On the (In)Security of Upgrading PINs from 4 to 6 digits
Collins W. Munyendo, Philipp Markert, Alexandra Nisenoff, Miles Grant, Elena Korkes, Blase Ur, and Adam J. Aviv

Guessability Results

Fraction Guessed

Number of Guesses

Terrible

Great
4-digit PINs’ Security

"The Same PIN, Just Longer": On the (In)Security of Upgrading PINs from 4 to 6 digits
Collins W. Munyendo, Philipp Markert, Alexandra Nisenoff, Miles Grant, Elena Korkes, Blase Ur, and Adam J. Aviv
4-dig v 6-digit PINs’ Security

Similar number of 4- and 6-digit PINs are guessed!

"The Same PIN, Just Longer": On the (In)Security of Upgrading PINs from 4 to 6 digits
Collins W. Munyendo, Philipp Markert, Alexandra Nisenoff, Miles Grant, Elena Korkes, Blase Ur, and Adam J. Aviv
Impact of Treatment on 6-digit

"The Same PIN, Just Longer": On the (In)Security of Upgrading PINs from 4 to 6 digits
Collins W. Munyendo, Philipp Markert, Alexandra Nisenoff, Miles Grant, Elena Korkes, Blase Ur, and Adam J. Aviv
Impact of Treatment on 6-digit

Fraction Guesed

Number of Guesses

Neutral
Breach
Security
Upgrade

Neutral & Upgrade
Security & Breach

worse
Impact of Treatment on 6-digit PINs

The graph shows the fraction of PINs correctly guessed over the number of guesses for different treatments:

- Neutral
- Breach
- No-sub
- Security
- Upgrade

The graph indicates that the upgrade treatment performs worse compared to the other treatments, as the fraction of guesses is higher for the upgrade treatment across all number of guesses.
Targeted Attacker

- The attacker knows the victim’s 4-digit PIN.
- Initial guesses by the attacker are targeted.
- Other guesses are in descending frequency order.
- Attacker is aware of blocklist for no-subsequence.
Transition from 4- to 6-digit PINs

**Appends**
1. First two digits: 7733 → 773377
2. Last digit twice: 4576 → 457666
3. Last two digits: 5109 → 510909

**Common PINs**
- 123456
- 654321
- 159357

**Prepends**
1. Prepend 00: 9997 → 009997
"The Same PIN, Just Longer": On the (In)Security of Upgrading PINs from 4 to 6 digits
Collins W. Munyendo, Philipp Markert, Alexandra Nisenoff, Miles Grant, Elena Korkes, Blase Ur, and Adam J. Aviv

Targeted Attack

Untargeted Attack

Targeted Attack

Better

Worse

Fraction Guessed

Number of Guesses

Neutral, Breach, No-sub, Security, Upgrade

Fraction Guessed

Number of Guesses

Neutral, Breach, No-sub, Security, Upgrade
Targeted Attack

Untargeted Attack

Targeted Attack

Over 25% of PINs guessed
Summary

- 6-digit offer a **minimal security** improvement over 4-digit PINs.
- Users select 6-digit PINs that are **related** to their 4-digit PINs.
- Security-oriented upgrade messages can **improve** security.
- Overall, **encouraging a secure** PIN once is more beneficial.
Thank You! Questions?

Collins W. Munyendo
cmunyendo@gwu.edu

Philipp Markert
philipp.markert@rub.de

Alexandra Nisenoff
nisenoff@uchicago.edu

Miles Grant
milesgrant@gwu.edu

Elena Korkes
ekorkes@gwu.edu

Blase Ur
blase@uchicago.edu

Adam J. Aviv
aaviv@gwu.edu

"The Same PIN, Just Longer": On the (In)Security of Upgrading PINs from 4 to 6 digits
Collins W. Munyendo, Philipp Markert, Alexandra Nisenoff, Miles Grant, Elena Korkes, Blase Ur, and Adam J. Aviv