“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

31st USENIX Security Symposium
August, 10 – 12, 2022
Boston, MA, USA

Security, Usability, & Privacy
Education & Research

The George Washington University

Ruhr University Bochum

University of Chicago

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?

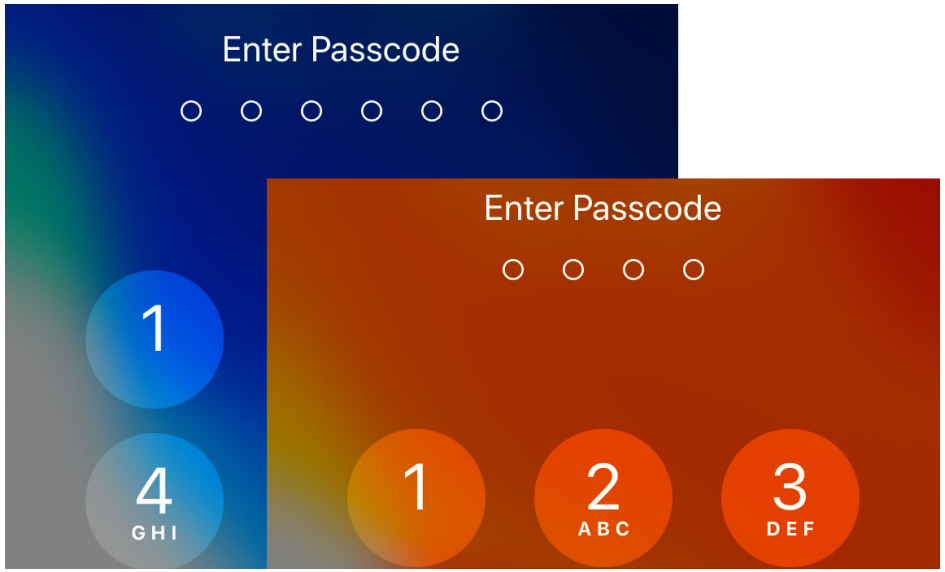
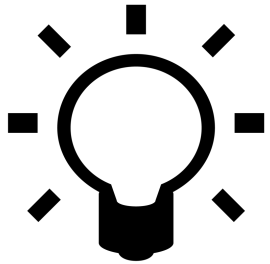


Photo: Philipp Markert | This PIN Can Be Easily Guessed (IEEE S&P 20')

Research Questions

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

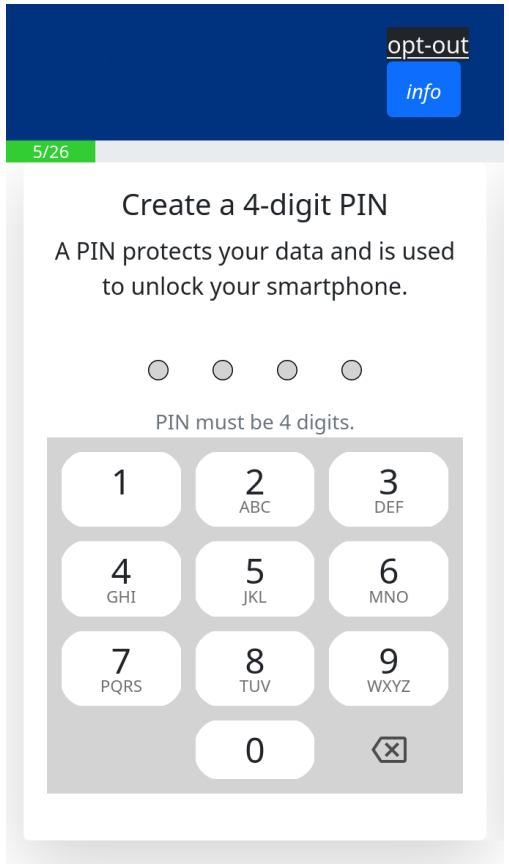


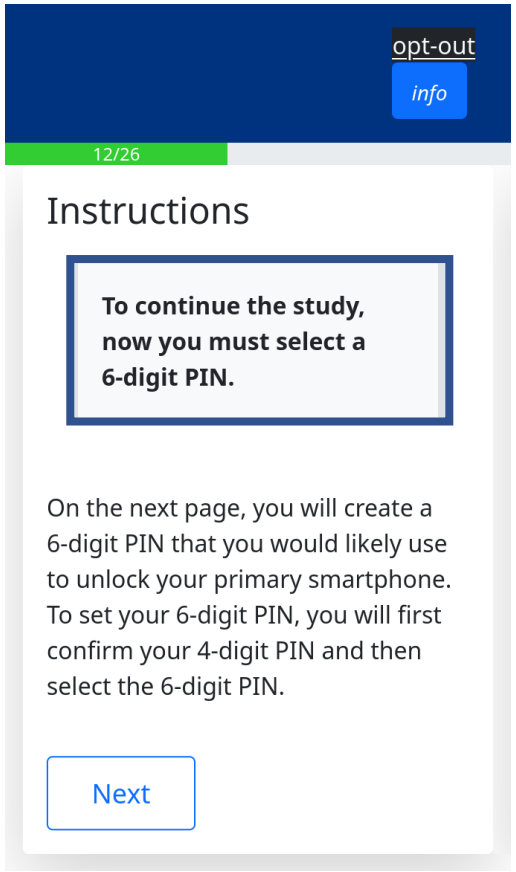
2. How does the **upgrade process** and **justification** provided impact security and usability?

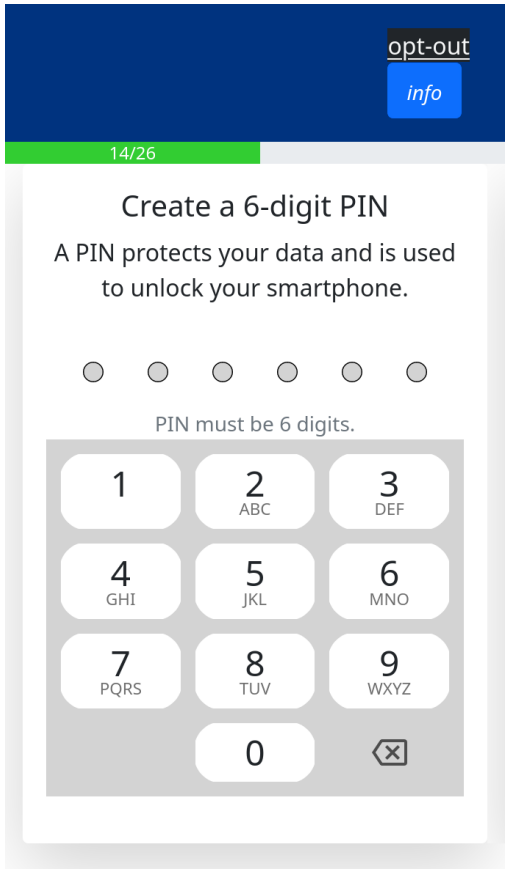
3. How **predictable** is a user's 6-digit PIN if their previous 4-digit PIN is known?

Study Design

4-digit PIN Selection → Device Use Questions → 6-digit PIN Instructions → 6-digit PIN Selection → Follow-up Questions







"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

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.

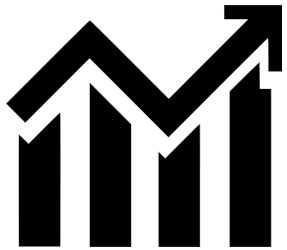
1234

001234
120034
123456

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?



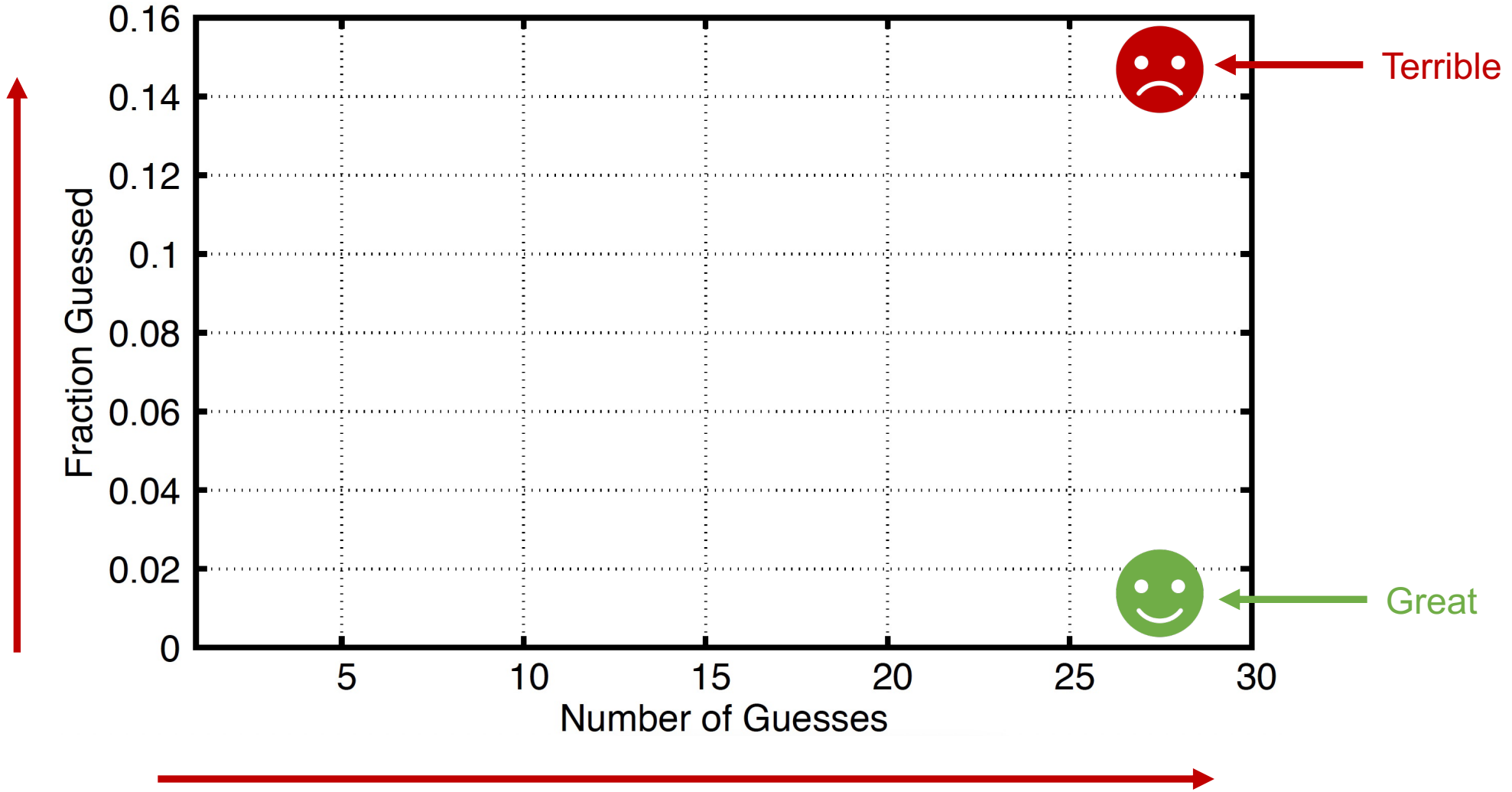
Untargeted Attacker

- 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.

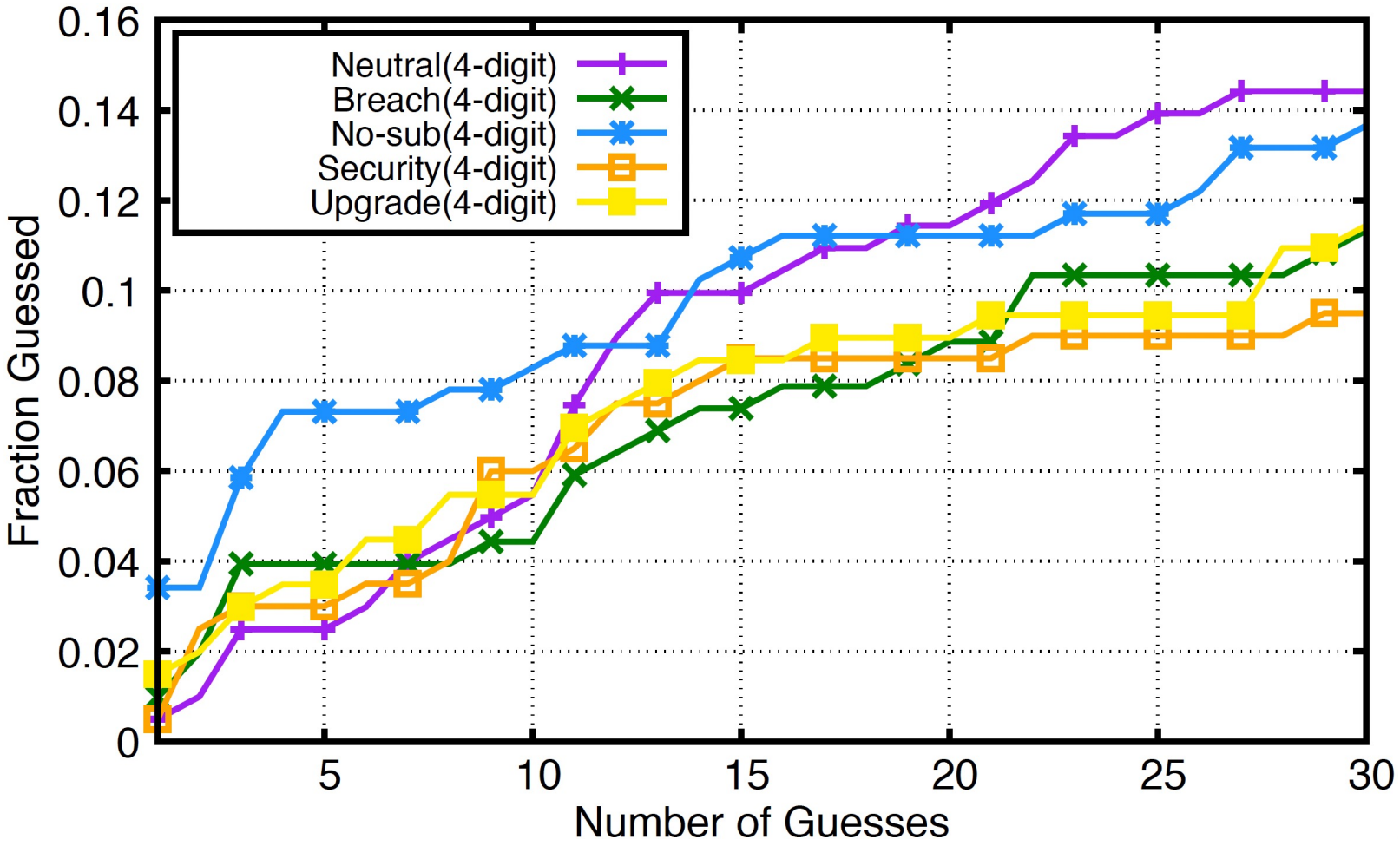
[1] https://www.danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes

[2] https://wiki.skullsecurity.org/index.php/Passwords

Guessability Results

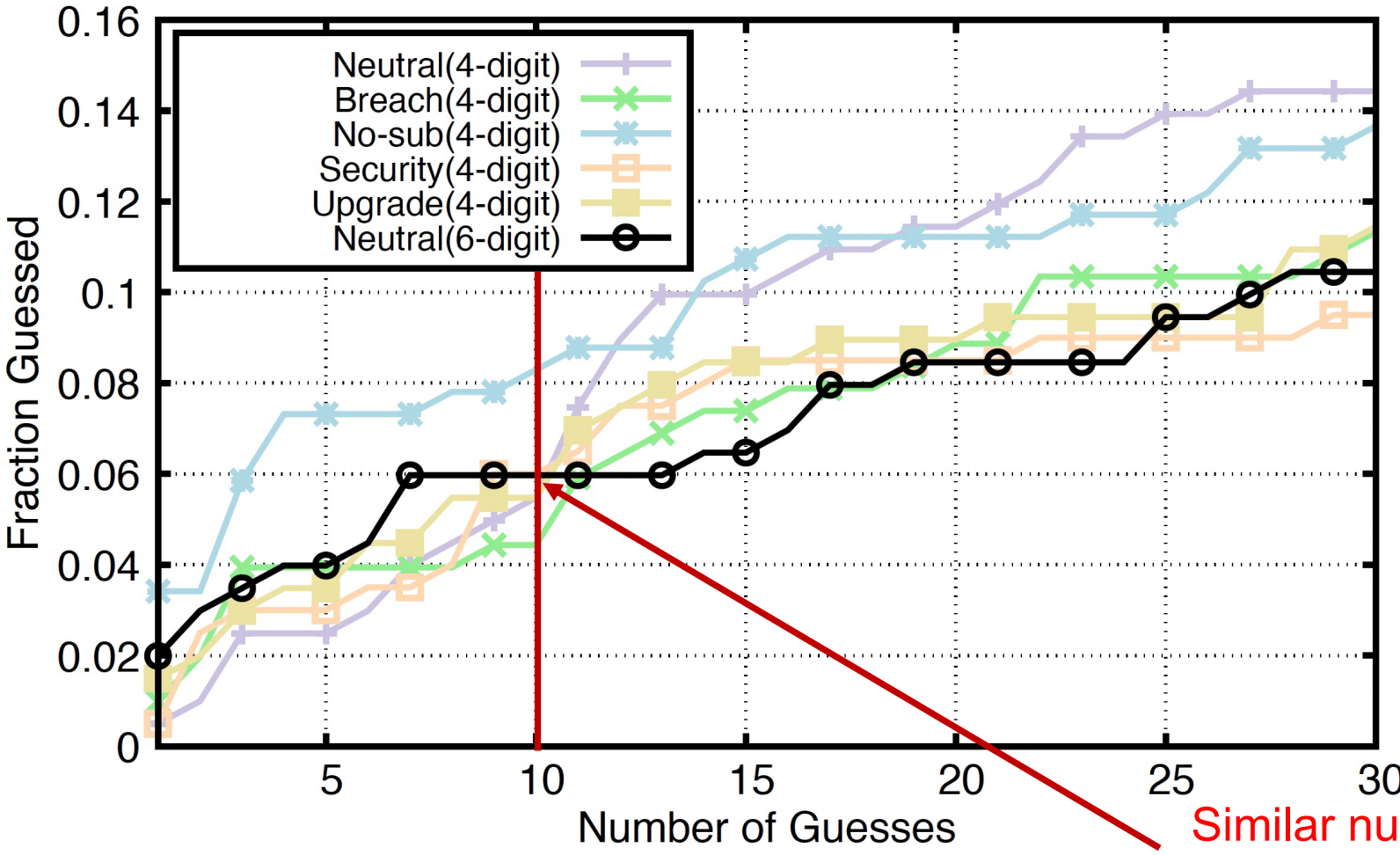


4- digit PINs' Security



better

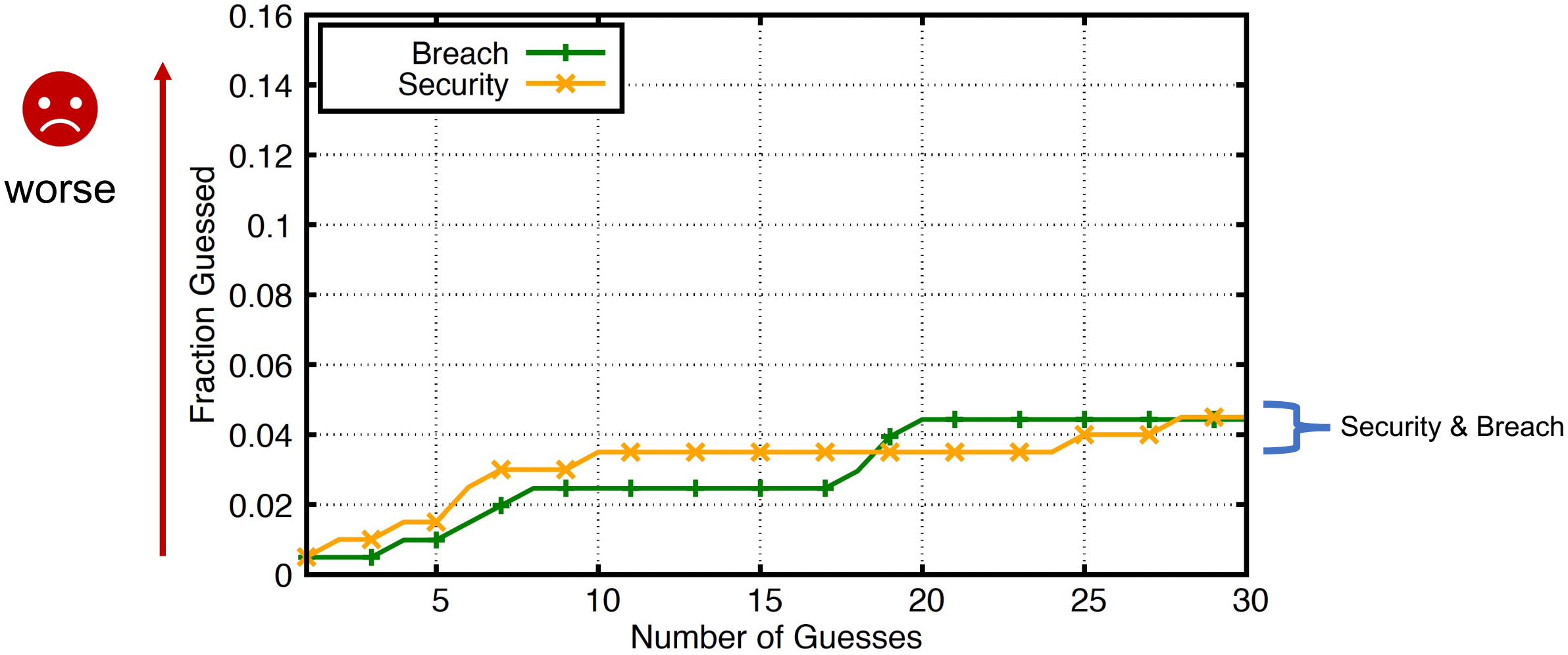
4- v 6-digit PINs' Security



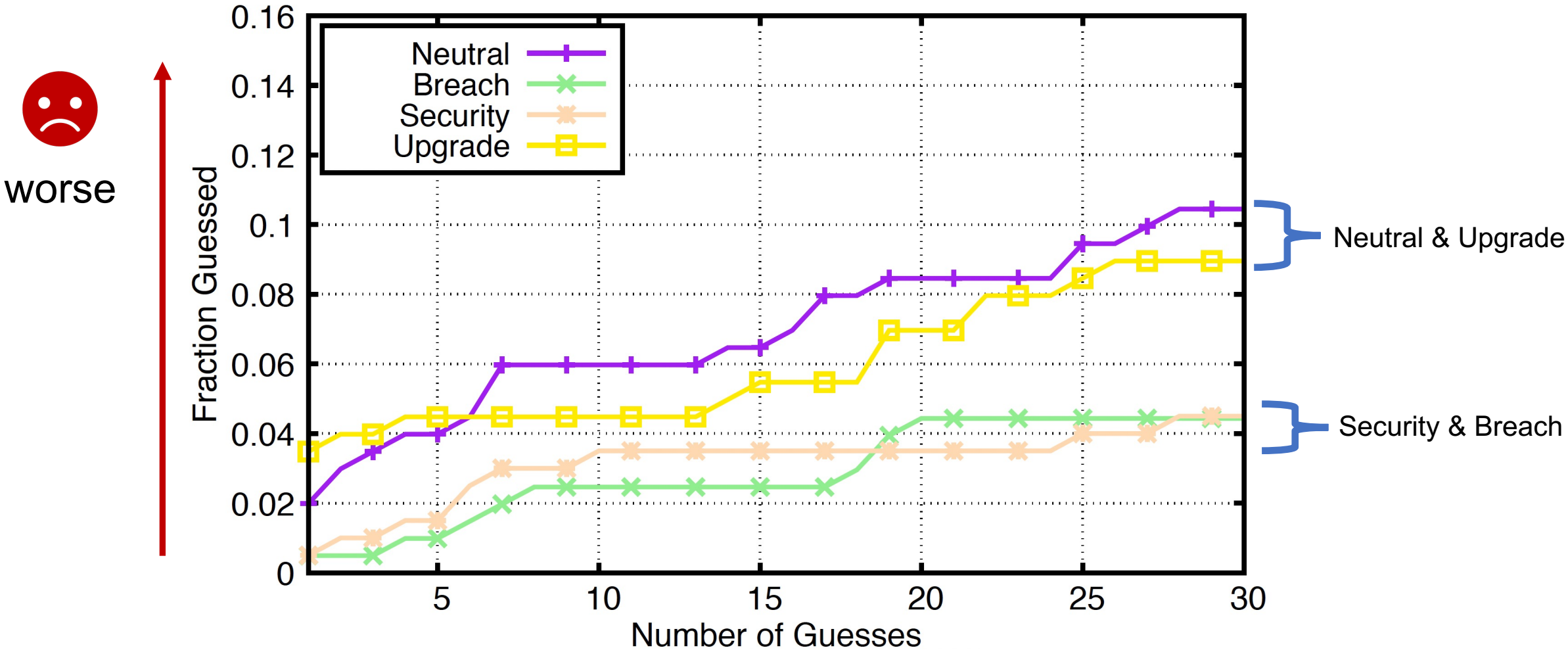
better

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

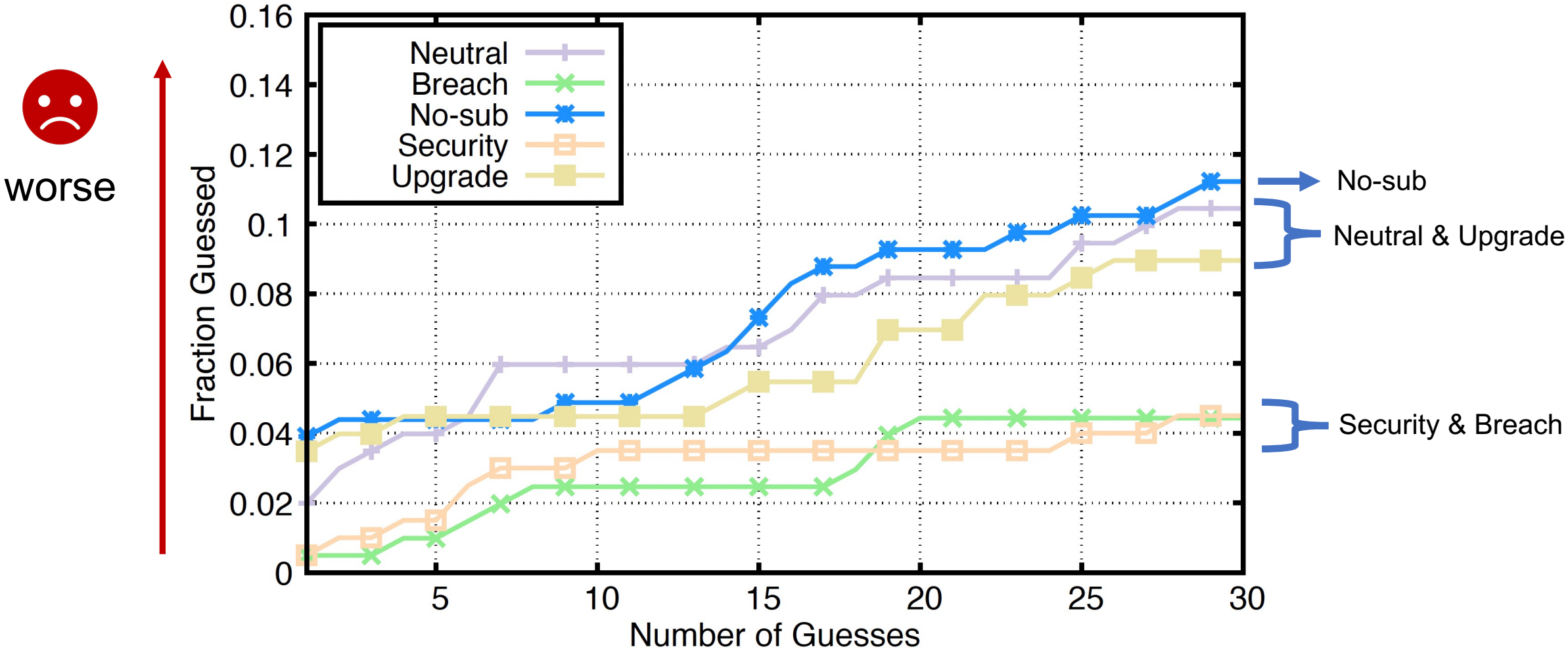
Impact of Treatment on 6-digit



Impact of Treatment on 6-digit



Impact of Treatment on 6-digit



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

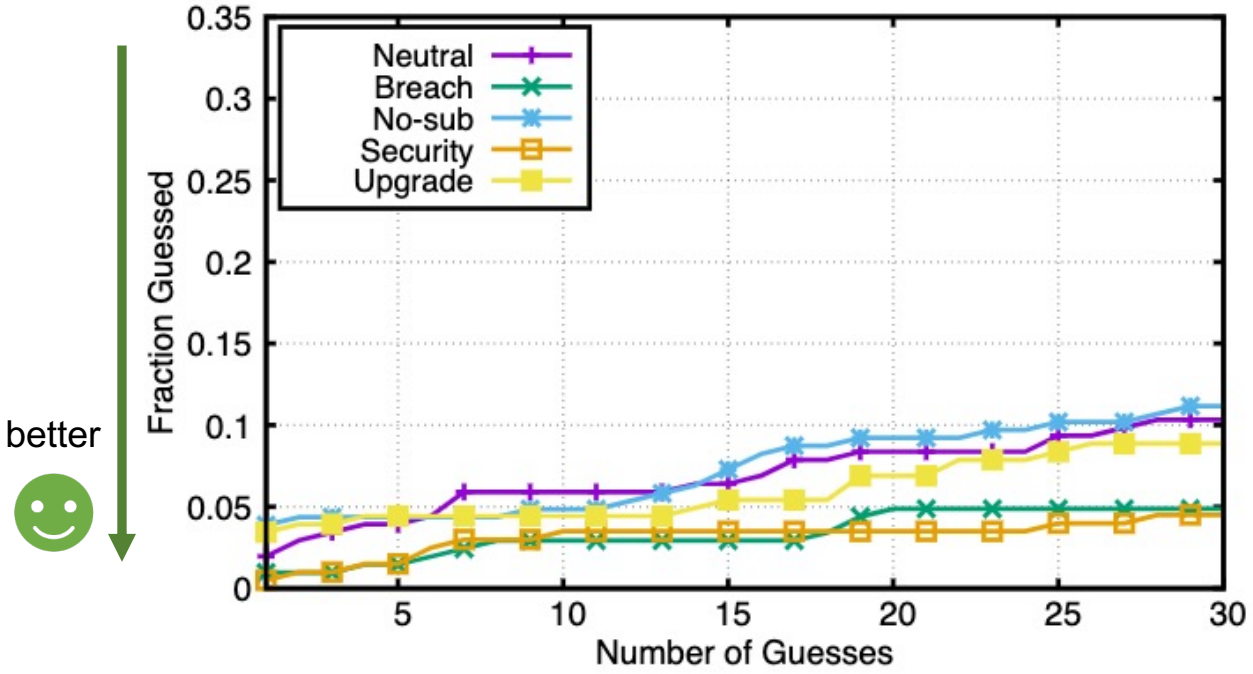
159357

Prepends

1. Prepend 00:
9997 → 009997

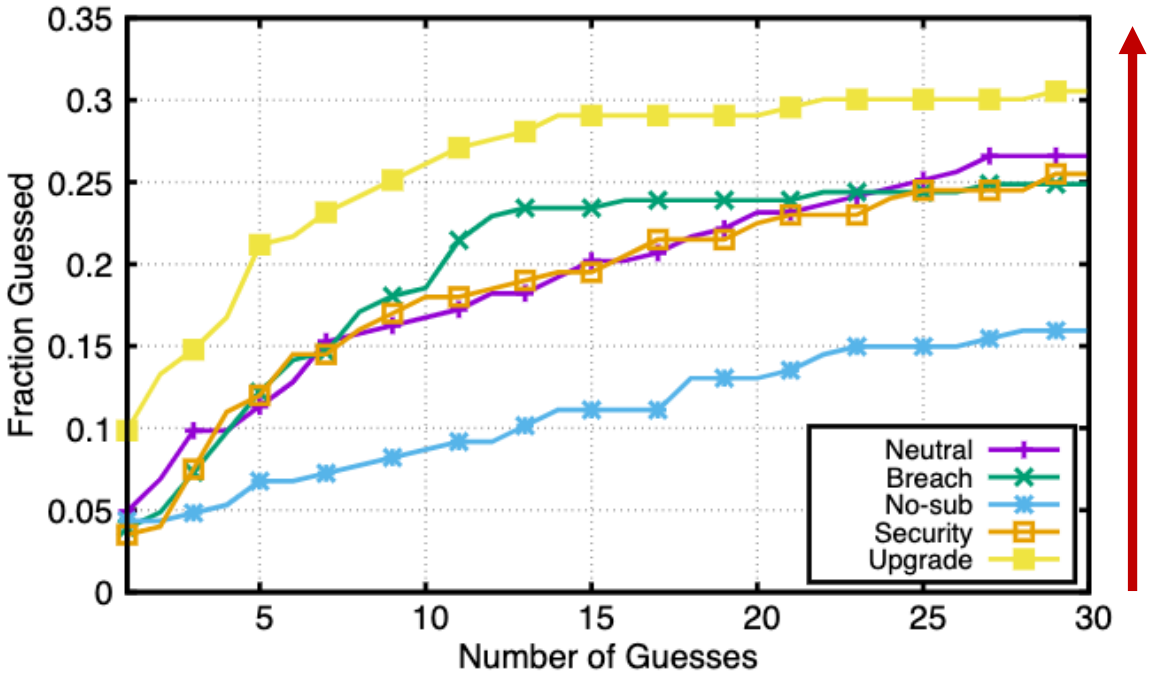
Targeted Attack

Untargeted Attack



better

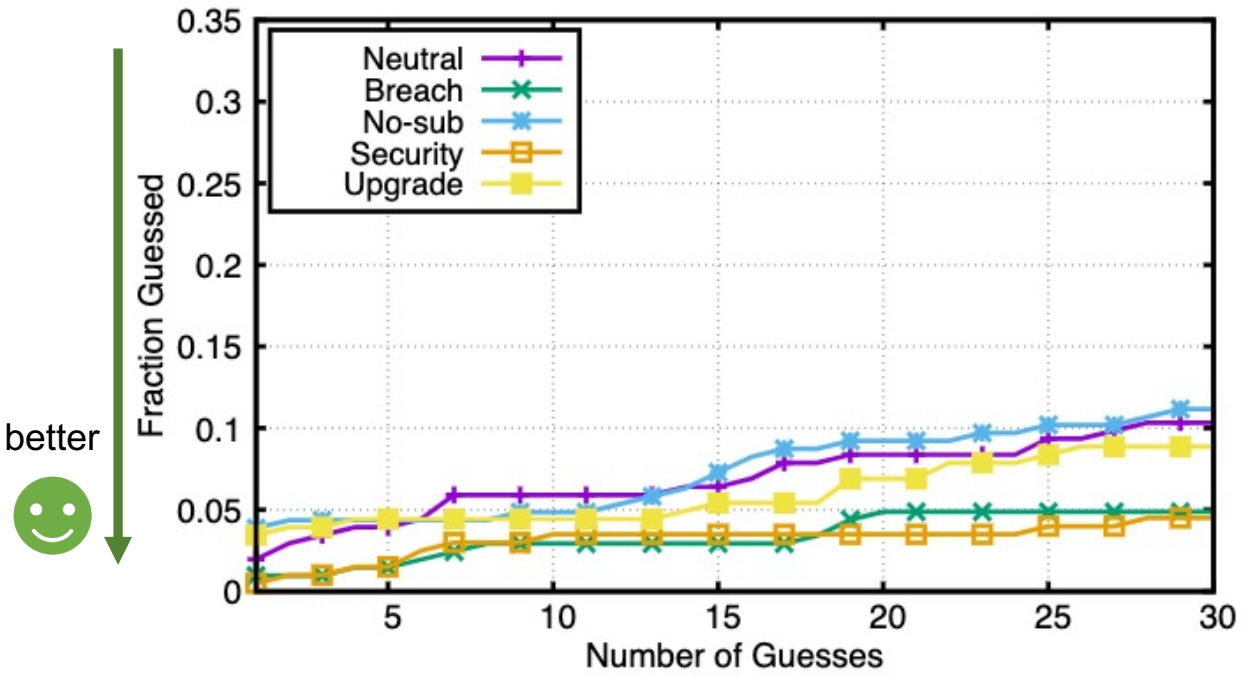
Targeted Attack



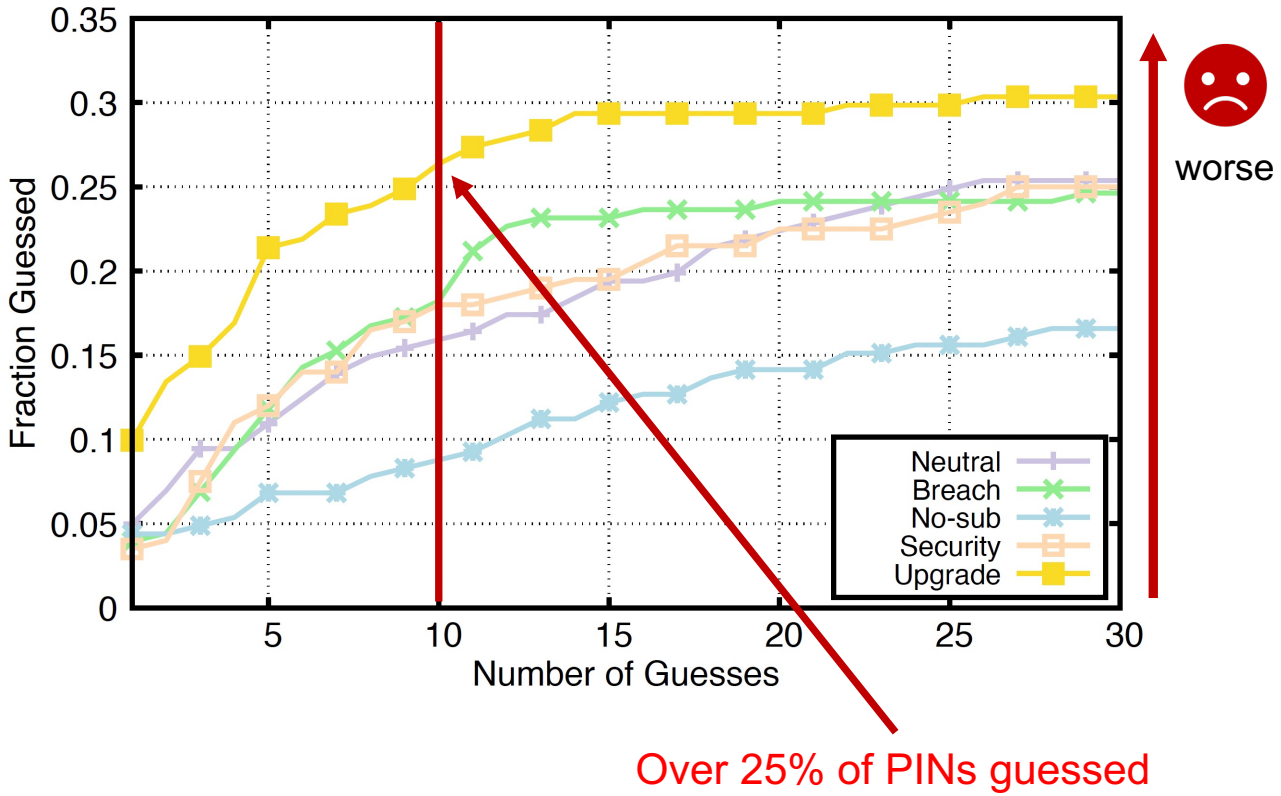
worse

Targeted Attack

Untargeted Attack



Targeted Attack



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 GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

RUHR UNIVERSITÄT BOCHUM