UNIVERSITY
OF OSLO

ICISSP 2024
Rome, Italy | 26-28 February 2024

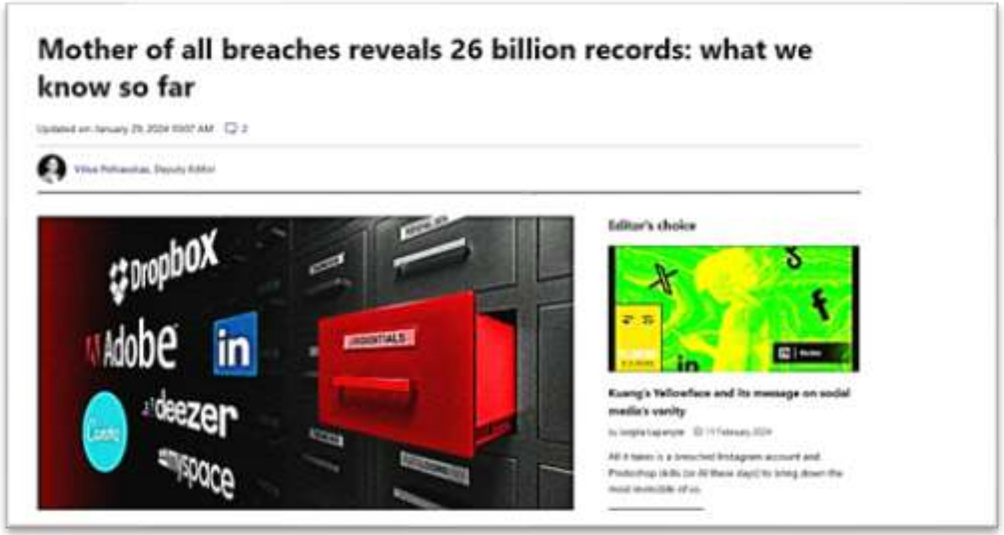
Evaluating the Influence of Multi-Factor Authentication and Recovery Settings on the Security and Accessibility of User Accounts

Andre Büttner and Nils Gruschka

University of Oslo (Norway)

27th February 2024

Motivation



Mother of all breaches reveals 26 billion records: what we know so far

Updated on: January 29, 2024 10:07 AM 2

Vilius Petkauskas, Deputy Editor

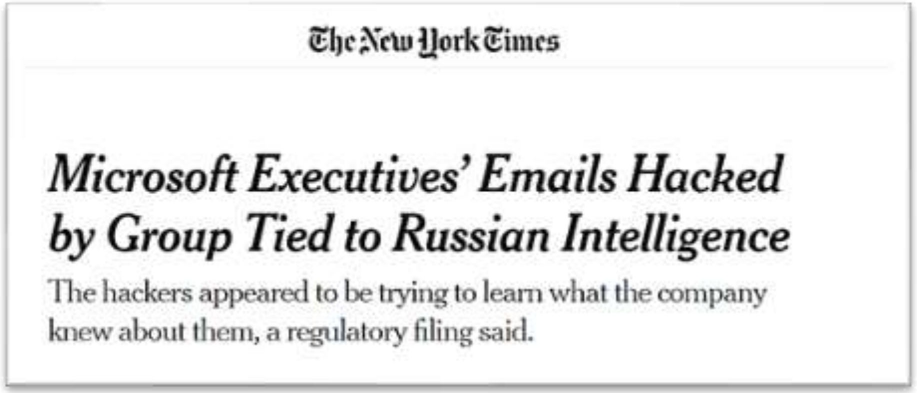
Editor's choice

Kuang's Yellowface and its message on social media's vanity

by Jurgita Lapienytė 11 February 2024

All it takes is a breached Instagram account and Photoshop skills (or AI these days) to bring down the most invincible of us.

Source: https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/

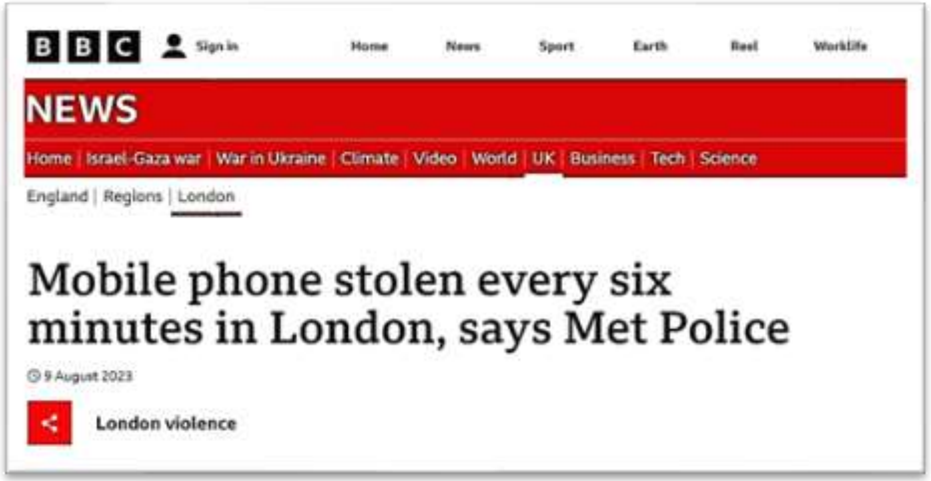


The New York Times

Microsoft Executives' Emails Hacked by Group Tied to Russian Intelligence

The hackers appeared to be trying to learn what the company knew about them, a regulatory filing said.

Source: https://www.nytimes.com/2024/01/19/technology/microsoft-executive-emails-hacked.html



BBC
Sign in
Home
News
Sport
Earth
Reel
Worklife
NEWS
Home | Israel-Gaza war | War in Ukraine | Climate | Video | World | UK | Business | Tech | Science
England | Regions | London

Mobile phone stolen every six minutes in London, says Met Police

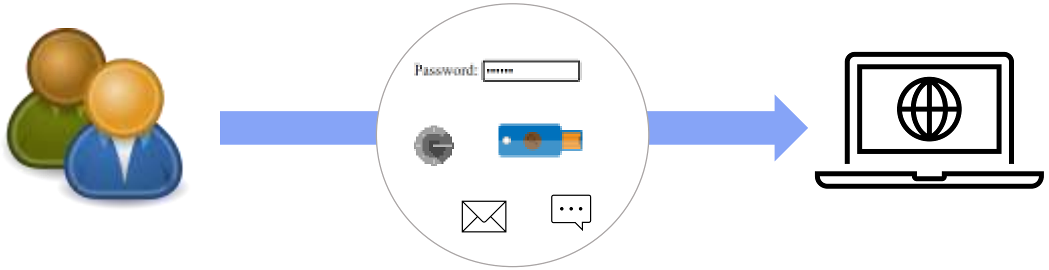
9 August 2023

London violence

Source: https://www.bbc.com/news/uk-england-london-66442069

Motivation

- Online services offer different authentication methods
  - Password
  - Multi-Factor Authentication (MFA)
    - SMS
    - Authenticator app
    - Security key
  - Account recovery methods
    - Email
    - SMS



- Well-known problems with passwords: phishing, credential stuffing, dictionary attacks, etc. [1]
- Problems with MFA and Recovery: usability[2], authentication bypass / account lockout[3]

[1] Taneski, Viktor, Marjan Heričko, and Boštjan Brumen. "Systematic overview of password security problems." *Acta Polytechnica Hungarica 16.3* (2019): 143-165. 2019.
[2] Das, Sanchari, Bingxing Wang, and L. Jean Camp. "MFA is a Waste of Time! Understanding Negative Connotation Towards MFA Applications via User Generated Content." *arXiv e-prints* (2019): arXiv-1908. 2019.
[3] Amft, Sabrina, et al. "We've Disabled MFA for You": An Evaluation of the Security and Usability of Multi-Factor Authentication Recovery Deployments." *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. 2023.

Problem Statement

➔ Analysis of **security** and **accessibility** for Apple and Google user accounts

With respect to Apple and Google users…

- **RQ1** How do the users access their passwords?
- **RQ2** Which MFA and recovery methods did the users enable?
- **RQ3** How secure are the account setups?
- **RQ4** How many access methods do the user accounts depend on?

Account Access Graphs I

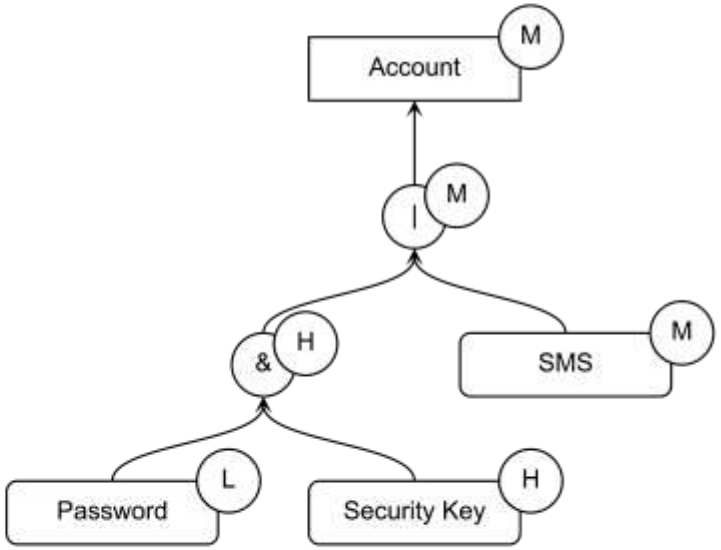
Account access graphs (AAGs)[4,5] can be used to model authentication methods and account interdependencies.

Security scores

- Security of authentication methods
- Evaluation:
  - Scores (adopted from NIST[6] / eIDAS[7])

Score	Category	Authentication methods (examples)
High	Hardware-based	Security key, smart card
Medium	Software-based	SMS Code, OTP Apps
Low	Knowledge-based	Password, PIN

  - & = maximum of child node scores
  - | = minimum of child node scores

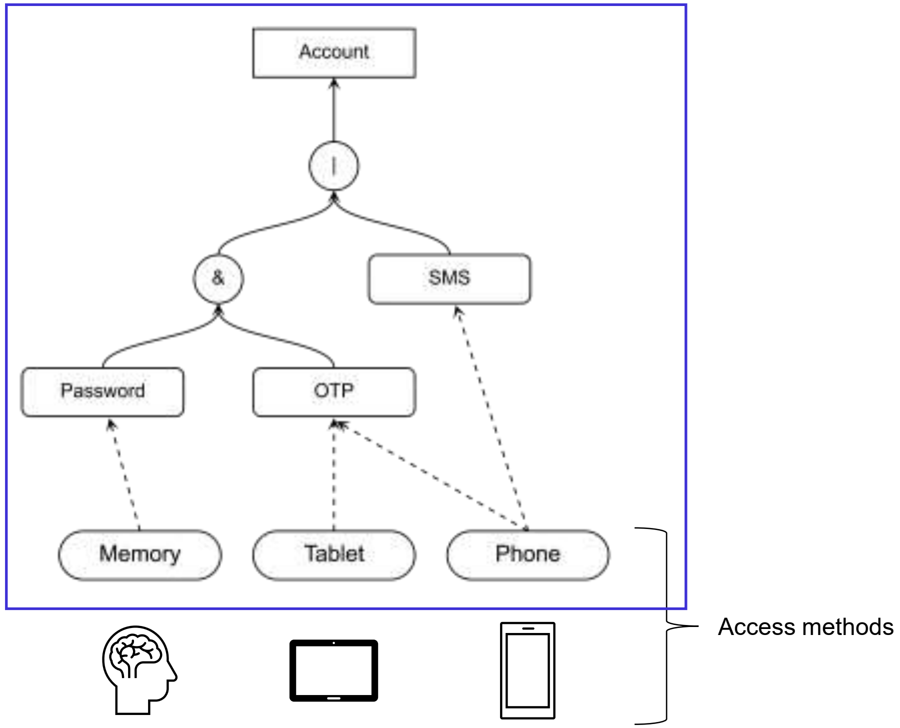


[4] Hammann, Sven, et al. "User account access graphs." *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2019.
[5] Pöhn, Daniela, et al. "A framework for analyzing authentication risks in account networks." *Computers & Security 135* (2023): 103515. 2023.
[6] Grassi, et al. "Digital Identity Guidelines: Authentication and Lifecycle Management". https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf. 2020.
[7] European Comission. "eIDAS Levels of Assurance". https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eIDAS+Levels+of+Assurance. 2023.

Account Access Graphs II

Accessibility scores

- Lower bound number of access methods required to access the account
- Evaluation:
  - Derive boolean term and simplify
  - Scores $s_i = \frac{1}{n_i}$ $(n_i = \text{number of occurrences})$
  - & = minimum
  - | = sum



- Example:

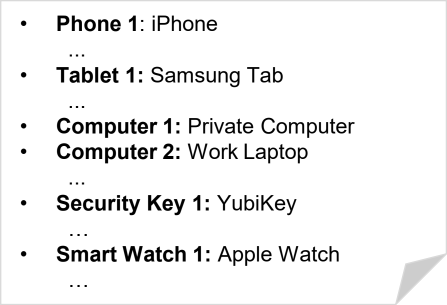
```
(Memory ∧ (Tablet ∨ Phone)) ∨ Phone
(Memory ∧ Tablet) ∨ (Memory ∧ Phone) ∨ Phone
(Memory ∧ Tablet) ∨ Phone
```

$$s_{acc} = \min(1,1) + 1 = 2$$

Online Survey

- Study participants acquired through Prolific*

- Questionnaire tasks:
  1. Create an enumerated list of devices



- **Phone 1**: iPhone
  …
- **Tablet 1:** Samsung Tab
  …
- **Computer 1:** Private Computer
- **Computer 2:** Work Laptop
  …
- **Security Key 1:** YubiKey
  …
- **Smart Watch 1:** Apple Watch
  …

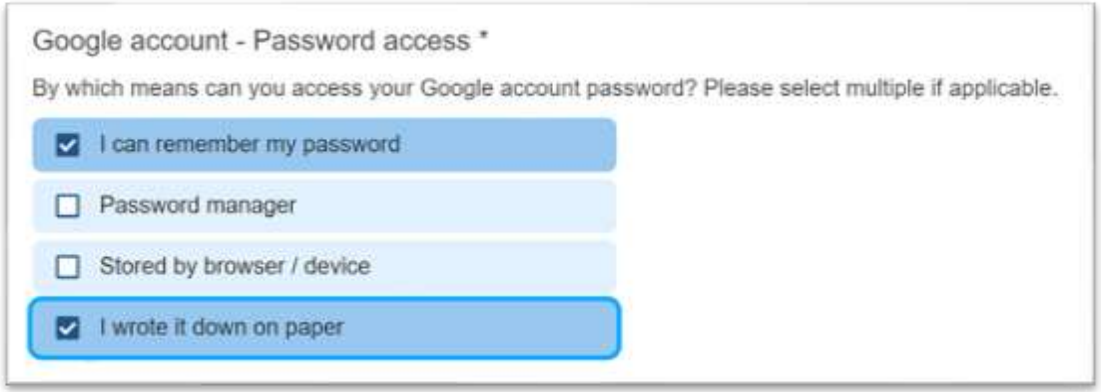
  2. Questions on Apple / Google account configurations and access methods

Category		Apple	Google
Gender	male	45	48
	female	46	46
Age range	11-20	5	3
	21-30	44	37
	31-40	23	30
	41-50	13	14
	51-60	5	9
	61-70	2	1
Country of residence	USA	44	47
	Germany	47	47
Total		91	94

Demographics of survey participants

* https://prolific.com (last accessed 2024-02-08)

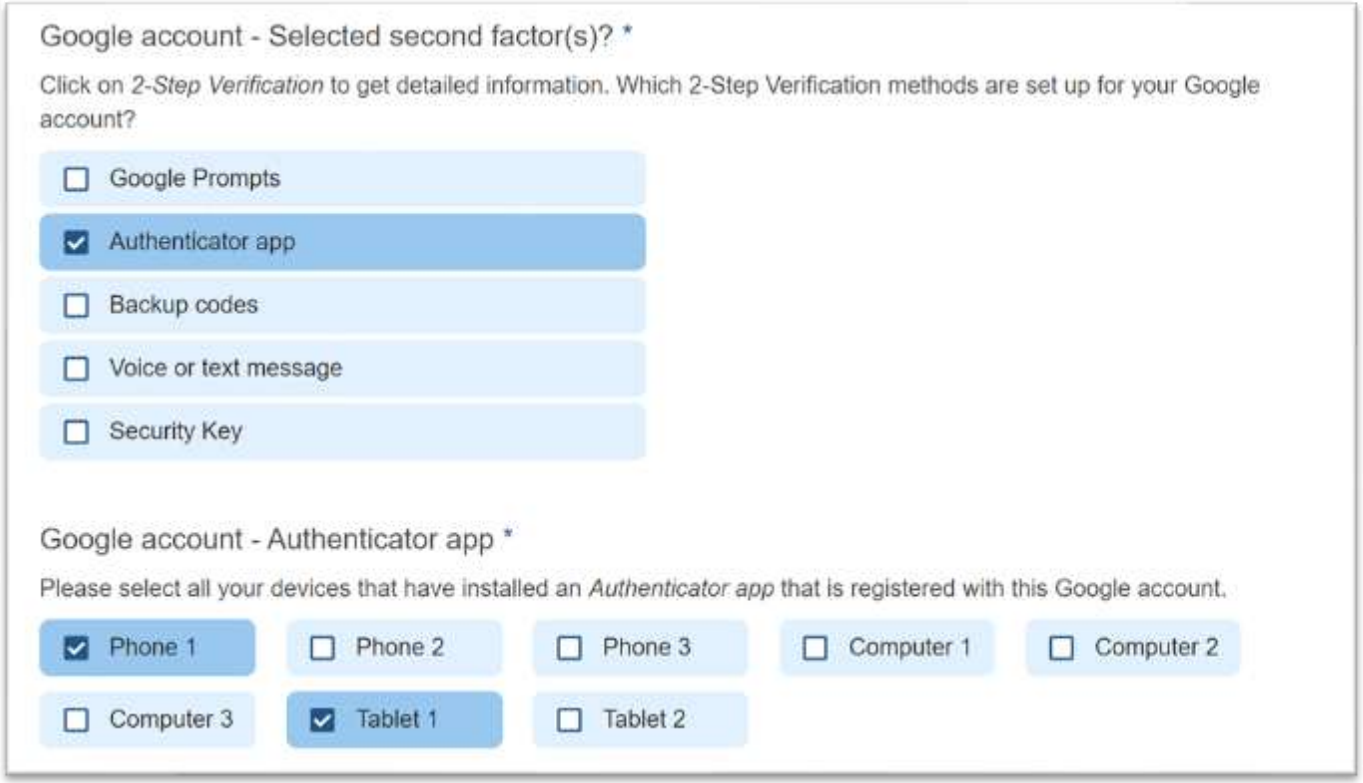
Survey Question Examples



Google account - Password access *

By which means can you access your Google account password? Please select multiple if applicable.

- ☑ I can remember my password
- □ Password manager
- □ Stored by browser / device
- ☑ I wrote it down on paper



Google account - Selected second factor(s)? *

Click on *2-Step Verification* to get detailed information. Which 2-Step Verification methods are set up for your Google account?

- □ Google Prompts
- ☑ Authenticator app
- □ Backup codes
- □ Voice or text message
- □ Security Key

Google account - Authenticator app *

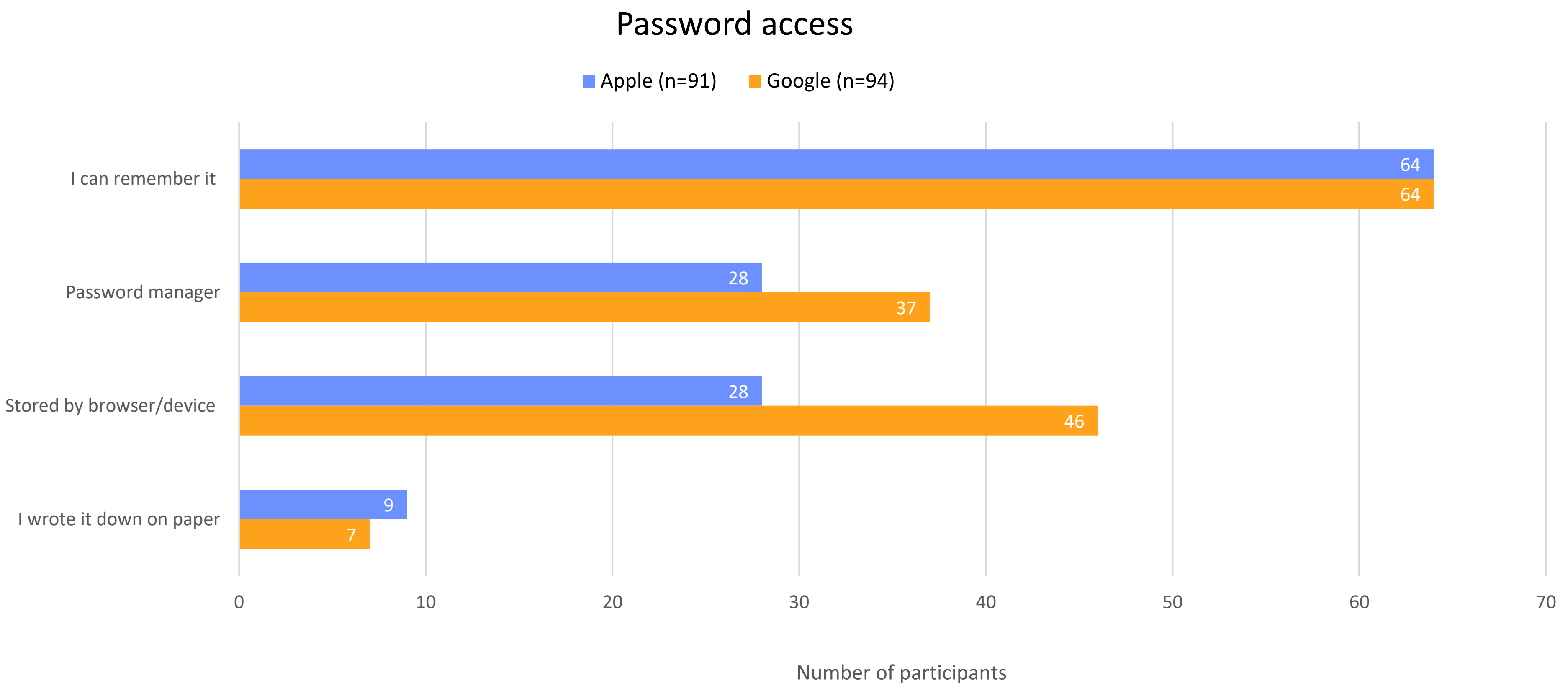
Please select all your devices that have installed an *Authenticator app* that is registered with this Google account.

☑ Phone 1 □ Phone 2 □ Phone 3 □ Computer 1 □ Computer 2

□ Computer 3 ☑ Tablet 1 □ Tablet 2

Results I

RQ1 How do the users access their passwords?



Results II

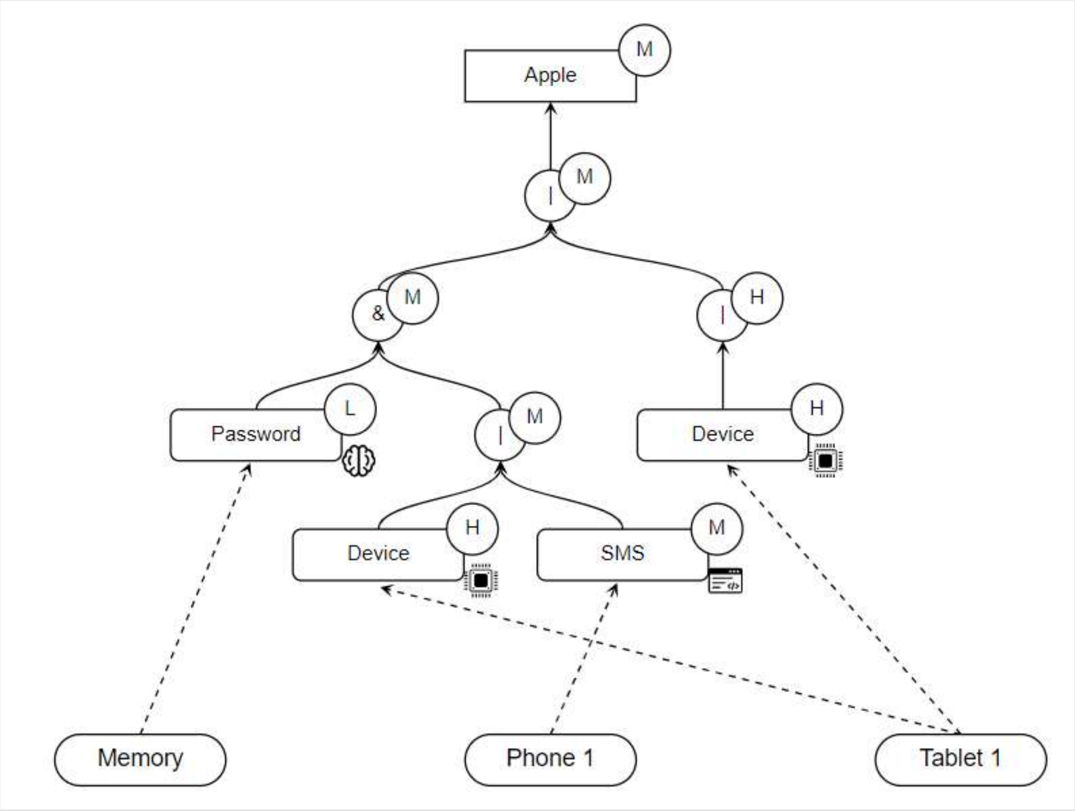
RQ2 Which MFA and recovery methods did the users enable?

- Apple
  - Linking to devices: ~96%
    → used for both MFA and recovery unless explicitly disabled
  - Text message enabled: ~97%
  - Recovery key enabled: ~19%

- Google:
  - 68% of the Google accounts had at least one MFA method enabled
  - Previous findings:
    - In 2015, less than 7% of Google users had MFA enabled[8]
    - In 2018, around 10% of Gmail accounts set up MFA[9]
    - Auto enrolment of MFA in Google accounts since 2021[10]

[8] Petsas, Thanasis, et al. "Two-factor authentication: is the world ready? Quantifying 2FA adoption." *Proceedings of the eighth European workshop on system security*. 2015.
[9] Milka, Grzergor. "Anatomy of account takeover." *Enigma 2018* (Enigma 2018). 2018.
[10] Risher, M. “A simpler and safer future - without passwords”. https://blog.google/technology/safety-security/a-simpler-and-saferfuture-without-passwords/. 2021.

AAG Example



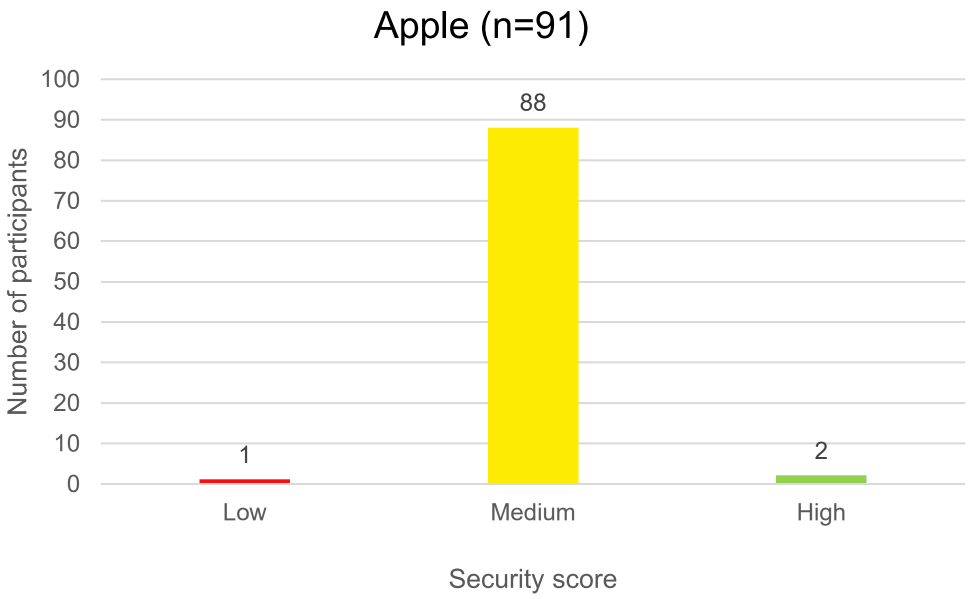
Apple P2

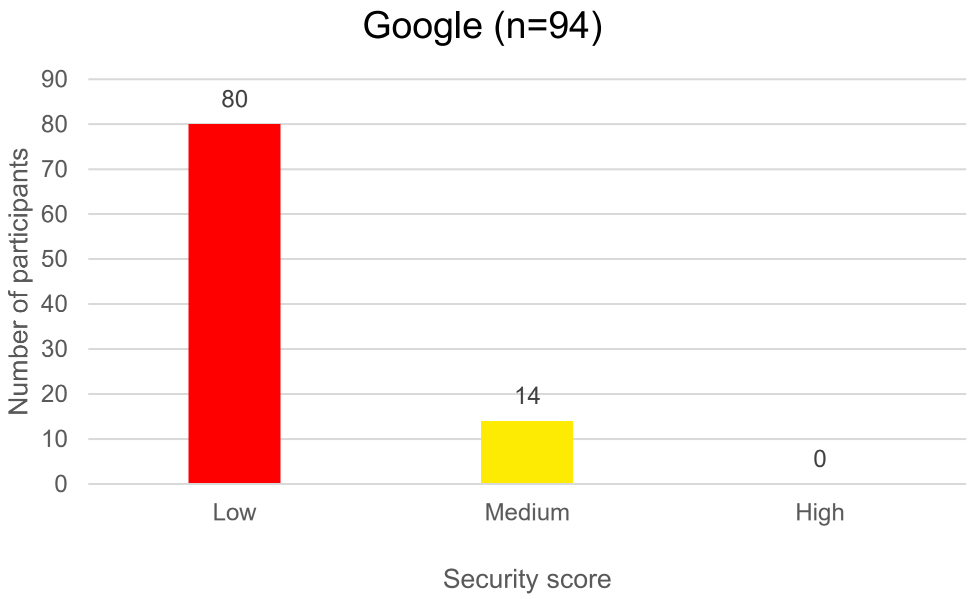
- Security score: Medium
- Accessibility score: 2

Results III

RQ3 How secure are the account setups?

Security scores

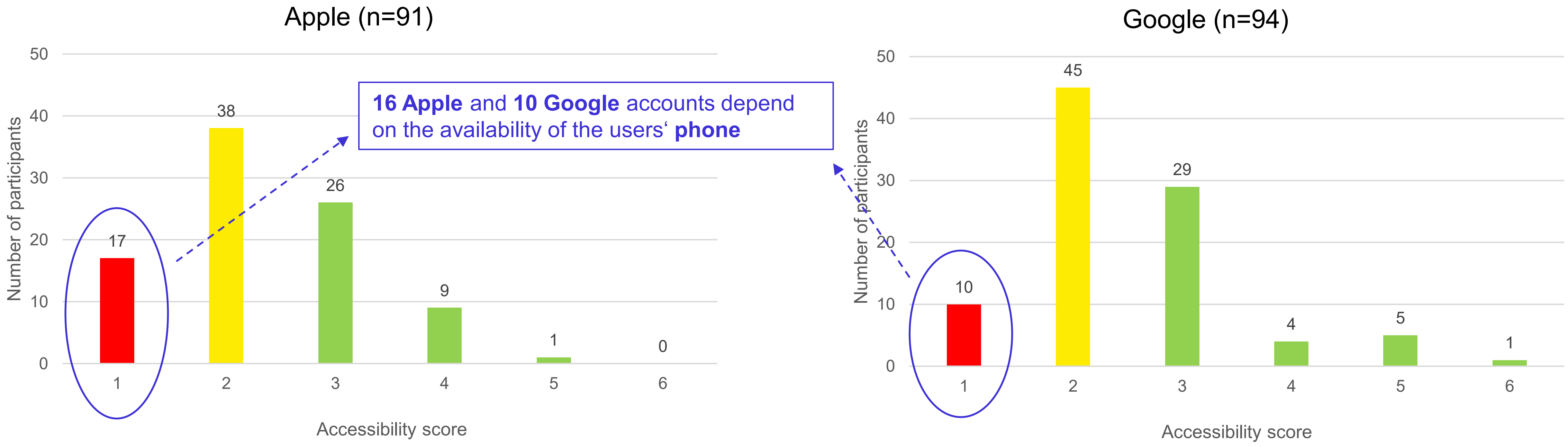




Results IV

RQ4 How many access methods do the user accounts depend on?

Accessibility scores



16 Apple and **10 Google** accounts depend on the availability of the users' **phone**

Conclusion

Summary:

- Majority of Apple accounts had a higher security score compared to Google accounts
- Several Apple and Google test participants could lose account access when only losing their phone
- Study data and tools available on GitHub: https://github.com/Digital-Security-Lab

Future work:

- Follow-up studies with more online services, e.g. lab studies (currently done in a Master's thesis project)
- Derive concepts for service providers to improve security and accessibility
- Consider risk-based authentication in AAG models

Thank you!
Any questions?

Contact
Andre Büttner
University of Oslo
Email: andrbut@ifi.uio.no
Web: https://www.mn.uio.no/ifi/english/people/aca/andrbut/index.html

Also on in RG

References

[1] Taneski, Viktor, Marjan Heričko, and Boštjan Brumen. "Systematic overview of password security problems." *Acta Polytechnica Hungarica 16.3* (2019): 143-165. 2019.

[2] Das, Sanchari, Bingxing Wang, and L. Jean Camp. "MFA is a Waste of Time! Understanding Negative Connotation Towards MFA Applications via User Generated Content." *arXiv e-prints* (2019): arXiv-1908. 2019.

[3] Amft, Sabrina, et al. "We've Disabled MFA for You": An Evaluation of the Security and Usability of Multi-Factor Authentication Recovery Deployments." *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. 2023.

[4] Hammann, Sven, et al. "User account access graphs." *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2019.

[5] Pöhn, Daniela, et al. "A framework for analyzing authentication risks in account networks." *Computers & Security 135* (2023): 103515. 2023.

[6] Grassi, et al. “Digital Identity Guidelines: Authentication and Lifecycle Management”. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf. 2020.

[7] European Comission. “eIDAS Levels of Assurance”. https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eIDAS+Levels+of+Assurance. 2023.

[8] Petsas, Thanasis, et al. "Two-factor authentication: is the world ready? Quantifying 2FA adoption." *Proceedings of the eighth European workshop on system security*. 2015.

[9] Milka, Grzergor. "Anatomy of account takeover." *Enigma 2018* (Enigma 2018). 2018.

[10] Risher, M. “A simpler and safer future - without passwords”. https://blog.google/technology/safety-security/a-simpler-and-saferfuture-without-passwords/. 2021.