UNIVERSITY
OF OSLO

Digital
Security
Research Group

Authentication Inconsistencies Across Online Services

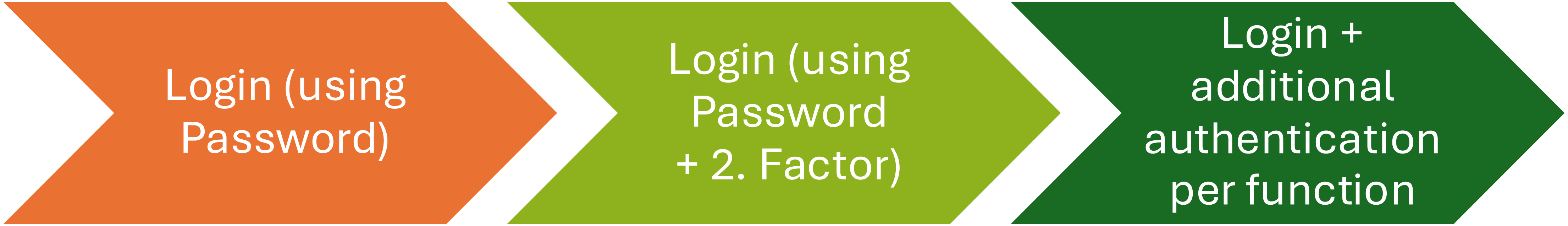
A Multi-Scenario Security Analysis

Andre Büttner, Nils Gruschka, Sverre Stafsengen Broen, and Daniela Pöhn

EDId - 2nd International Workshop on Emerging Digital Identities

Ghent (Belgium), 14th August 2025

“Evolution” of Authentication



Login (using Password)

Login (using Password + 2. Factor)

Login + additional authentication per function

Research Questions

- RQ1: How do authentication methods differ **across different usage scenarios**?
- RQ2: How do authentication methods differ **across various online services**?
- RQ3: How does **2FA influence the authentication methods** beyond the login?

Online Services

- 10 popular online services based on website rankings
  - Tranco Top Sites, Majestic Million, Chrome (CrUX) Top Million Websites

- Services:
  - Amazon
  - ChatGPT
  - Facebook
  - GitHub
  - Google
  - LinkedIn
  - Microsoft (Outlook)
  - Pinterest
  - Spotify
  - X (formerly Twitter)

Scenarios

S1 – Login

S2 – Modify Email

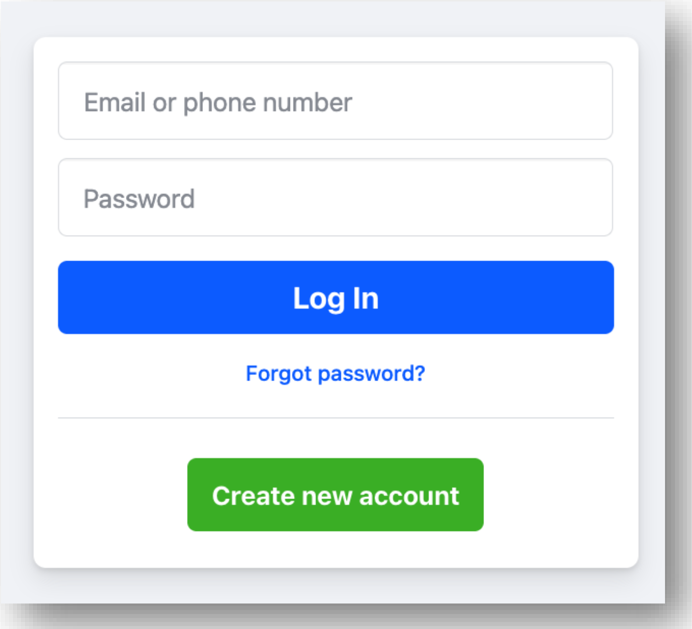
S3 – Toggle 2FA

S4 – Change Name

S5 – Right of Access Request

S6 – Password Reset

Screenshot: Facebook Login



Scenarios

S1 – Login

S2 – Modify Email

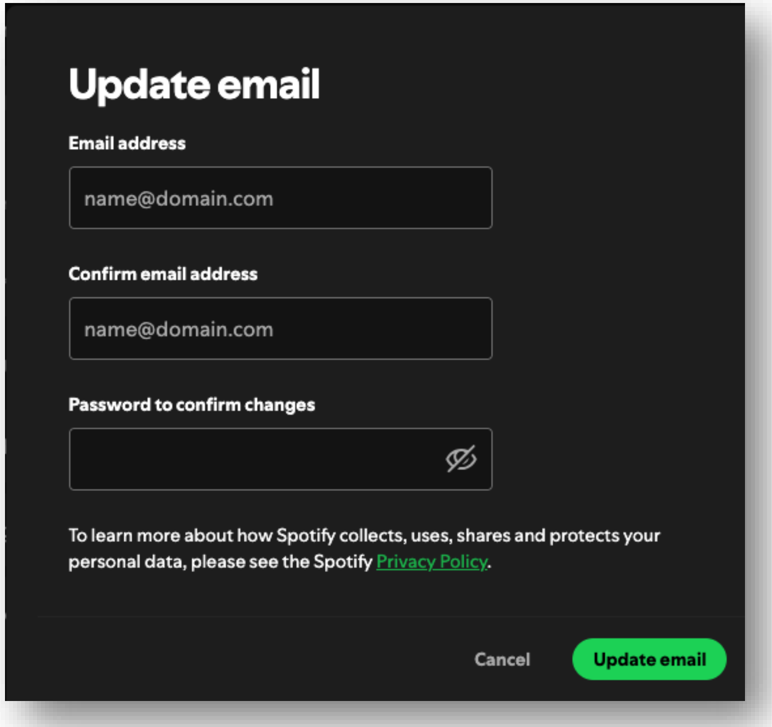
S3 – Toggle 2FA

S4 – Change Name

S5 – Right of Access Request

S6 – Password Reset

Screenshot – Spotify Update Email



Update email

Email address

name@domain.com

Confirm email address

name@domain.com

Password to confirm changes

To learn more about how Spotify collects, uses, shares and protects your personal data, please see the Spotify Privacy Policy.

Scenarios

S1 – Login

S2 – Modify Email

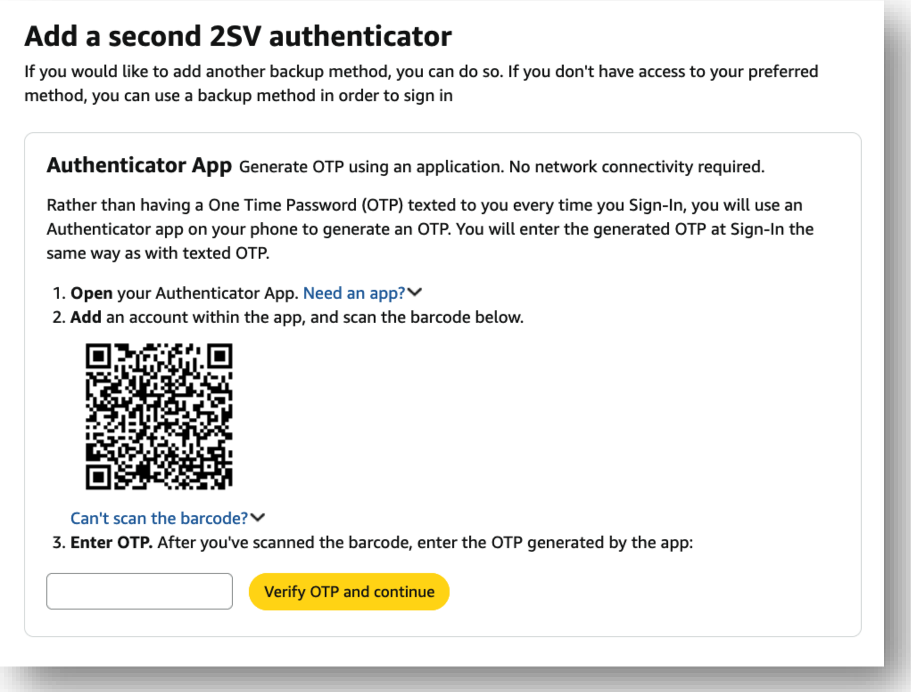
S3 – Toggle 2FA

S4 – Change Name

S5 – Right of Access Request

S6 – Password Reset

Screenshot: Amazon Two-Step Verification



Add a second 2SV authenticator

If you would like to add another backup method, you can do so. If you don't have access to your preferred method, you can use a backup method in order to sign in

Authenticator App Generate OTP using an application. No network connectivity required.

Rather than having a One Time Password (OTP) texted to you every time you Sign-In, you will use an Authenticator app on your phone to generate an OTP. You will enter the generated OTP at Sign-In the same way as with texted OTP.

1. **Open** your Authenticator App. Need an app?
2. **Add** an account within the app, and scan the barcode below.

Can't scan the barcode?

3. **Enter OTP.** After you've scanned the barcode, enter the OTP generated by the app:

Scenarios

S1 – Login

S2 – Modify Email

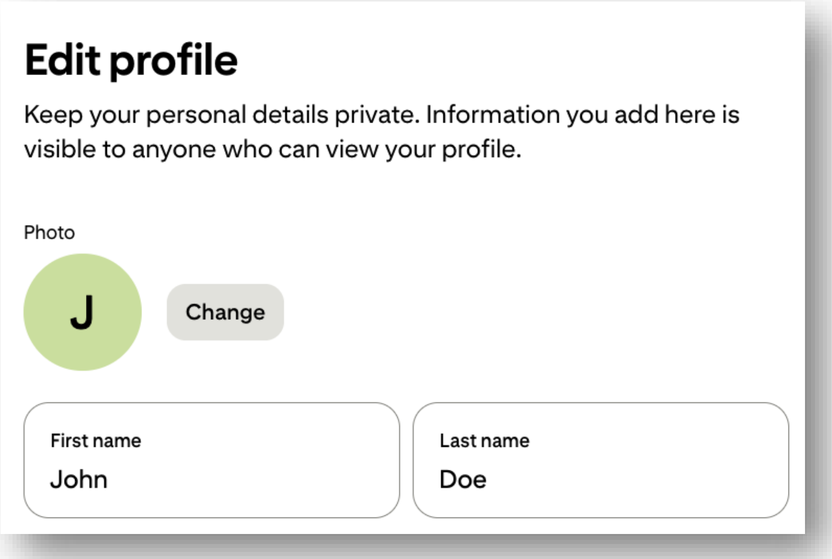
S3 – Toggle 2FA

S4 – Change Name

S5 – Right of Access Request

S6 – Password Reset

Screenshot: Pinterest Settings



Edit profile

Keep your personal details private. Information you add here is visible to anyone who can view your profile.

Photo

First name: John

Last name: Doe

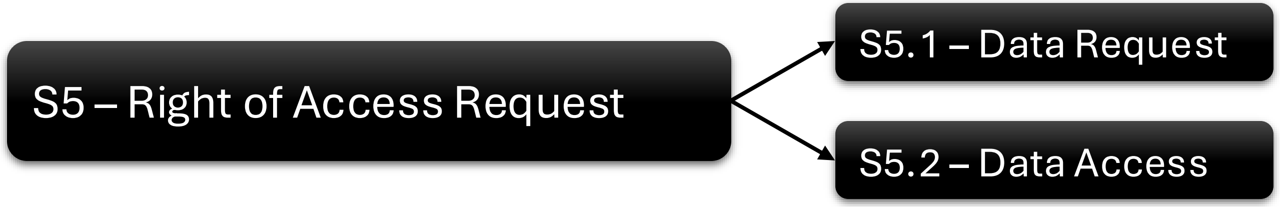
Scenarios

S1 – Login

S2 – Modify Email

S3 – Toggle 2FA

S4 – Change Name



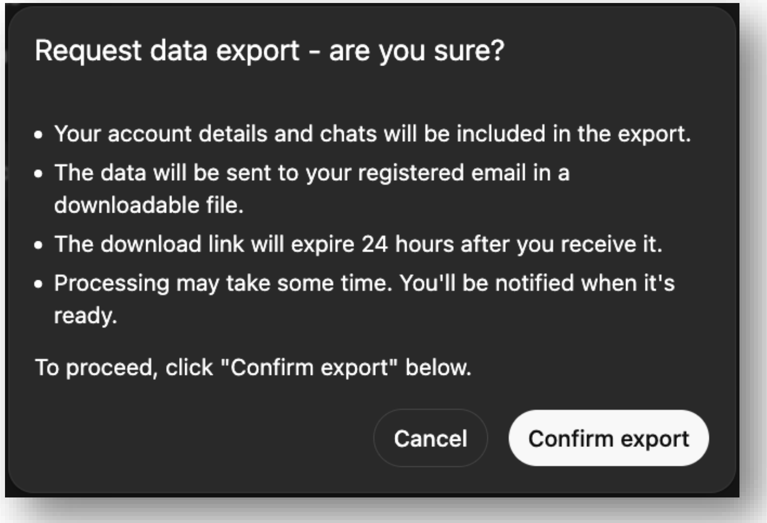
S5 – Right of Access Request

S5.1 – Data Request

S5.2 – Data Access

S6 – Password Reset

Screenshot: ChatGPT Request Data Export



Request data export - are you sure?

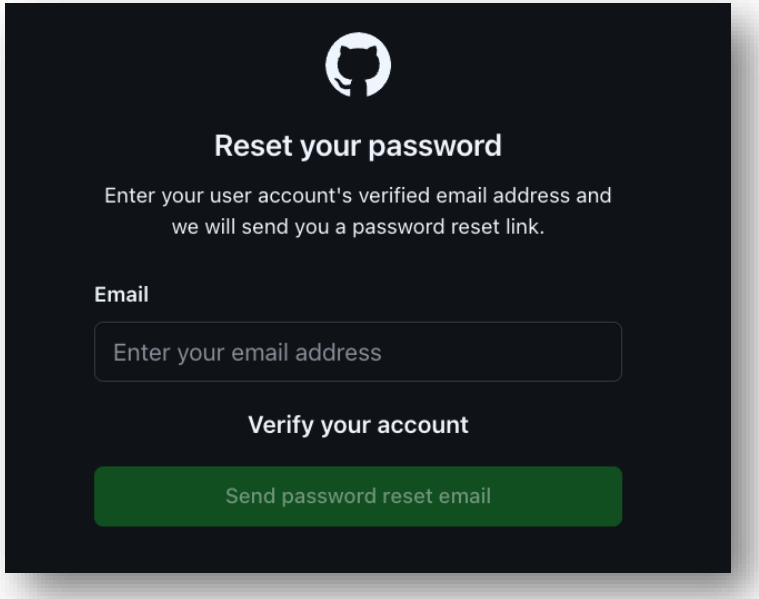
- Your account details and chats will be included in the export.
- The data will be sent to your registered email in a downloadable file.
- The download link will expire 24 hours after you receive it.
- Processing may take some time. You'll be notified when it's ready.

To proceed, click "Confirm export" below.

Scenarios

- S1 – Login
- S2 – Modify Email
- S3 – Toggle 2FA
- S4 – Change Name
- S5 – Right of Access Request
- **S6 – Password Reset**

Screenshot: GitHub Password Reset



Reset your password

Enter your user account's verified email address and we will send you a password reset link.

Email

Enter your email address

Verify your account

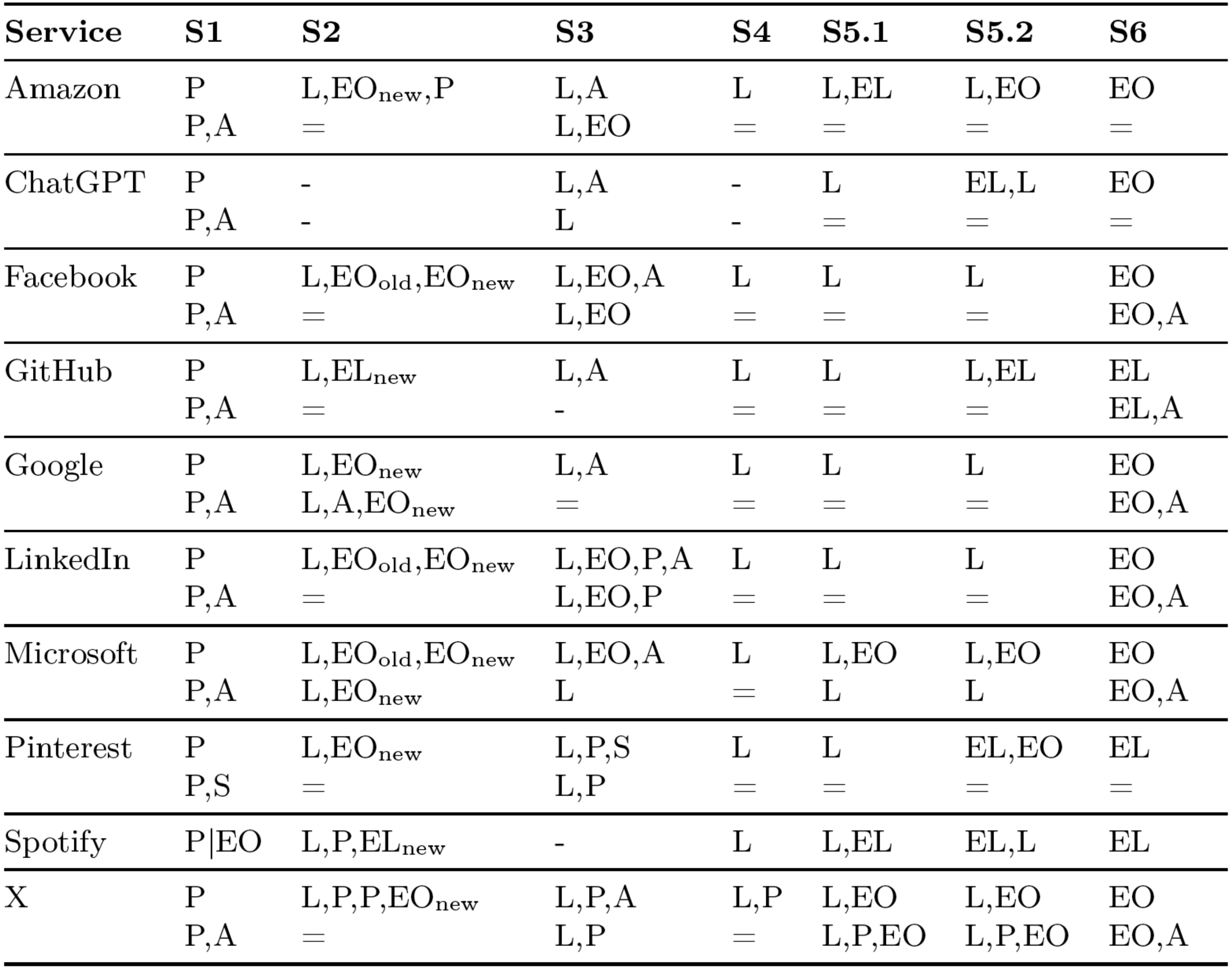
Experiment Procedure

1. **Create test accounts**
    - Minimal account setup → Email Address & Password

2. **Run scenarios**
    - 1FA: Password only
    - 2FA: Password + OTP app

3. **Compare required verification methods**

Results



Service	S1	S2	S3	S4	S5.1	S5.2	S6
Amazon	P	L,EO_{new},P	L,A	L	L,EL	L,EO	EO
	P,A	=	L,EO	=	=	=	=
ChatGPT	P	-	L,A	-	L	EL,L	EO
	P,A	-	L	-	=	=	=
Facebook	P	L,EO_{old},EO_{new}	L,EO,A	L	L	L	EO
	P,A	=	L,EO	=	=	=	EO,A
GitHub	P	L,EL_{new}	L,A	L	L	L,EL	EL
	P,A	=	-	=	=	=	EL,A
Google	P	L,EO_{new}	L,A	L	L	L	EO
	P,A	L,A,EO_{new}	=	=	=	=	EO,A
LinkedIn	P	L,EO_{old},EO_{new}	L,EO,P,A	L	L	L	EO
	P,A	=	L,EO,P	=	=	=	EO,A
Microsoft	P	L,EO_{old},EO_{new}	L,EO,A	L	L,EO	L,EO	EO
	P,A	L,EO_{new}	L	=	L	L	EO,A
Pinterest	P	L,EO_{new}	L,P,S	L	L	EL,EO	EL
	P,S	=	L,P	=	=	=	=
Spotify	P|EO	L,P,EL_{new}	-	L	L,EL	EL,L	EL
X	P	L,P,P,EO_{new}	L,P,A	L,P	L,EO	L,EO	EO
	P,A	=	L,P	=	L,P,EO	L,P,EO	EO,A

Results – Scenarios (RQ1)

- Modifying Email Address (S2) and Toggling 2FA (S3)
  - Additional steps: Re-enter old password, verify old email address

- Changing the name (S4)
  - Usually no additional steps

- Right of Access Request (S5)
  - Email access often required, particularly for Data Access (S5.2)

- Password Reset (S6)
  - Email verification
  - Usually also requiring 2FA

Results – Services (RQ2)

	Re-Enter Password	Verify Old Email	Email OTP	Email Link	Enter Email	2FA Backup Code
Amazon			✓	✓		
ChatGPT			✓	✓		✓
Facebook		✓	✓			✓
GitHub				✓		✓
Google			✓			✓
LinkedIn	✓	✓	✓			
Microsoft		✓	✓		✓	✓
Pinterest			✓	✓		✓
Spotify	✓		✓	✓		
X	✓		✓			✓

Results – 2FA (RQ3)

- Microsoft trusts user signed with 2FA **more**
  → Requiring less verification methods

- Google, Amazon, and X trust user signed with 2FA **less** (in certain scenarios)
  → Requiring more verification methods

- Some services do not require second factor for password reset

Results – Selected Services / Scenarios

Service		S2 (Modify Email Address)	S3 (Toggle 2FA Setting)
Amazon	1FA	⇥ ✉★ ***	⇥ 📱
	2FA		⇥ ✉
LinkedIn	1FA	⇥ ✉🕒 ✉★	⇥ ✉ *** 📱
	2FA		⇥ ✉ ***
Microsoft	1FA	⇥ ✉🕒 ✉★	⇥ ✉ 📱
	2FA	⇥ ✉★	⇥
X	1FA	⇥ *** *** ✉★	⇥ *** 📱
	2FA		⇥ ***

Additional Findings

Rate limiting when changing information

- Changing email address or authentication methods temporarily blocked → Facebook and X

CAPTCHA

- Account recovery → GitHub
- Changing name → Microsoft

Risk-Based Account Recovery

- Security question → Amazon

Security Impact

- 2FA sign-in treated differently
- Some methods rather weak, e.g., re-entering password
- CAPTCHAs only occurred in single cases
- Password reset cannot be exploited to bypass 2FA
- Right of access request does not seem to be an authentication backdoor

Conclusion

Main findings

- Services use various patterns for different scenarios
- 2FA can lead to higher or lower confidence in a user's identity
- Possible security and usability trade-offs

Future work

- Compare distinct patterns regarding their security
- Study user perceptions of the different approaches
- Extend experiment to other services
- Test behavior with passkeys

Thank you!

Contact author
Andre Büttner
University of Oslo
Email: andrbut@ifi.uio.no

Also on