UNIVERSITY
OF OSLO

Security of Evolving Authentication Technologies

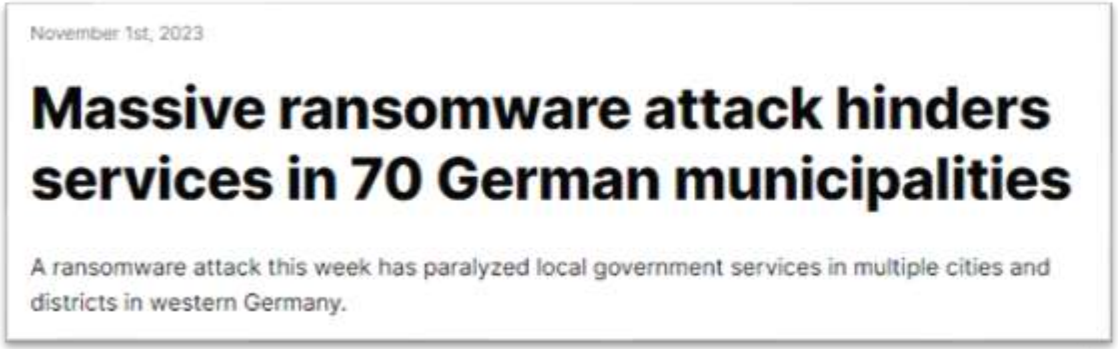
Multi-Factor Authentication, Passwordless Authentication, and Self-Sovereign Identity

Andre Büttner

Public defence for the degree of Philosophiae Doctor (PhD)

2nd September 2024

Motivation

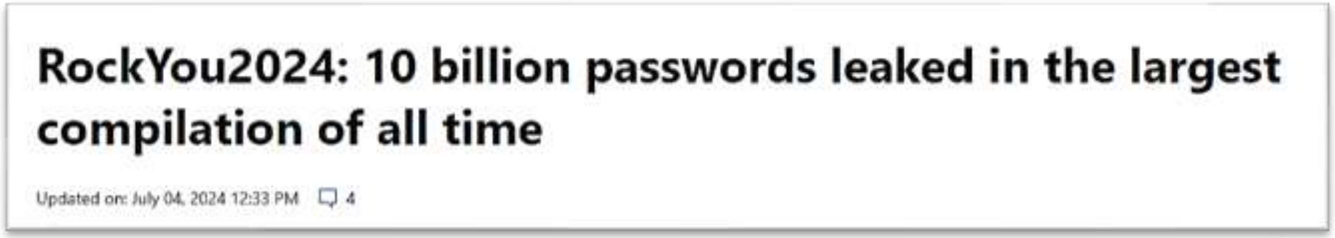


November 1st, 2023

Massive ransomware attack hinders services in 70 German municipalities

A ransomware attack this week has paralyzed local government services in multiple cities and districts in western Germany.

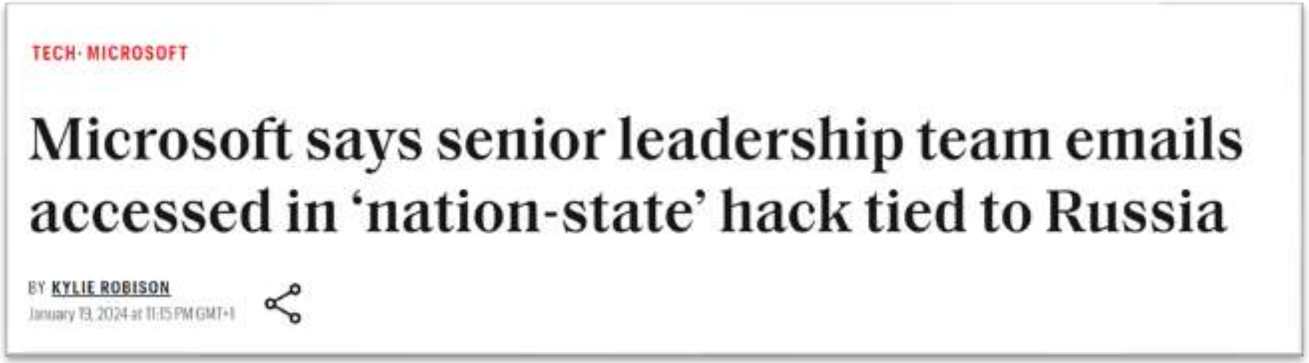
Source: https://therecord.media/massive-cyberattack-hinders-services-in-germany (2023)



RockYou2024: 10 billion passwords leaked in the largest compilation of all time

Updated on: July 04, 2024 12:33 PM 4

Source: https://cybernews.com/security/rockyou2024-largest-password-compilation-leak/ (2024)



TECH · MICROSOFT

Microsoft says senior leadership team emails accessed in 'nation-state' hack tied to Russia

BY KYLIE ROBISON

January 19, 2024 at 11:15 PM GMT+1

Source: https://fortune.com/2024/01/19/microsoft-senior-leadership-team-emails-accessed-russia-nation-state-hack/ (2024)

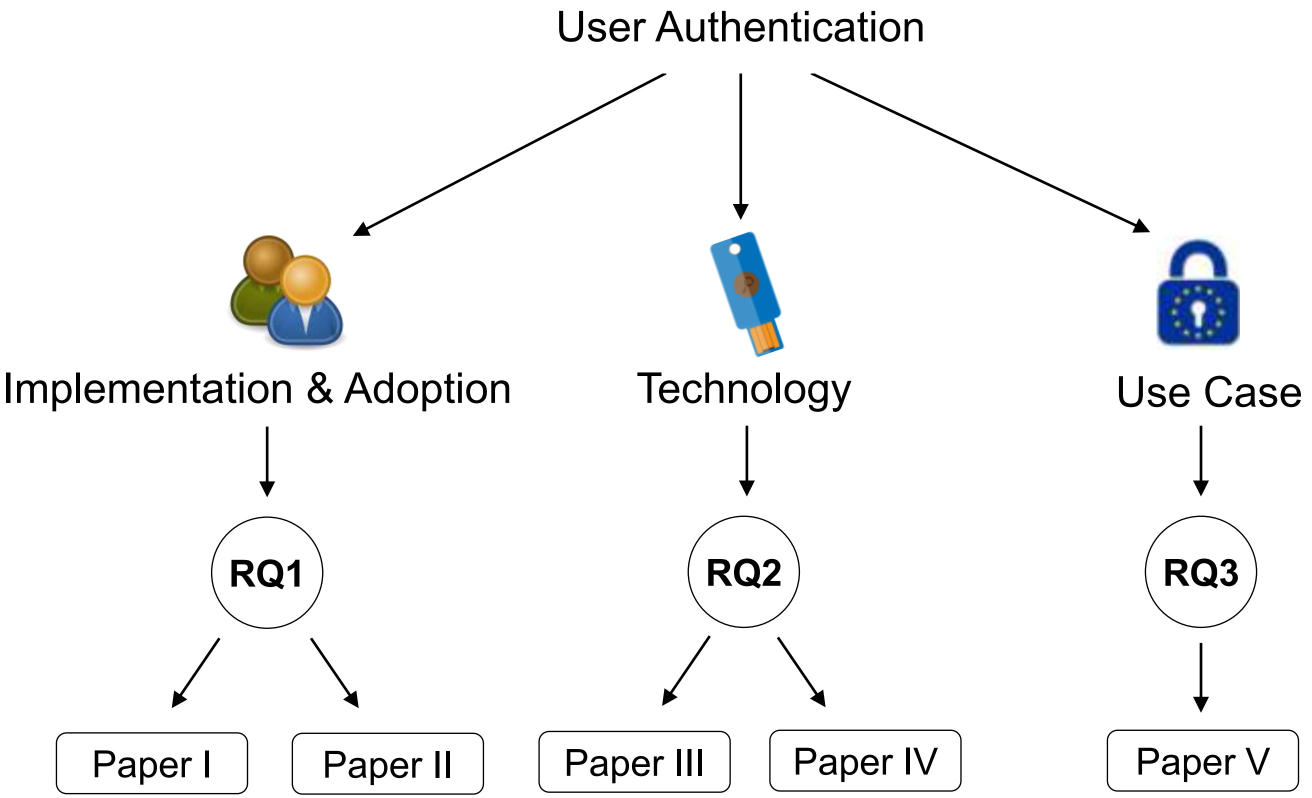
Motivation

Authentication on online services

- **Prevents unallowed access** to digital resources and **guarantees the authenticity** of a user's actions performed on such resources

- Crucial part of Identity and Access Management
- Security depends on **technology** and **human factor**
- Typical entry point for attackers

Research Overview



User Authentication

Implementation & Adoption

Technology

Use Case

RQ1

RQ2

RQ3

Paper I

Paper II

Paper III

Paper IV

Paper V

RQ1 How are online users authenticated in practice, and what implications does it have on the security and accessibility of their accounts?

Paper I

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

Andre Büttner and Nils Gruschka

ICISSP 2024

➔ User Account Study

Paper II

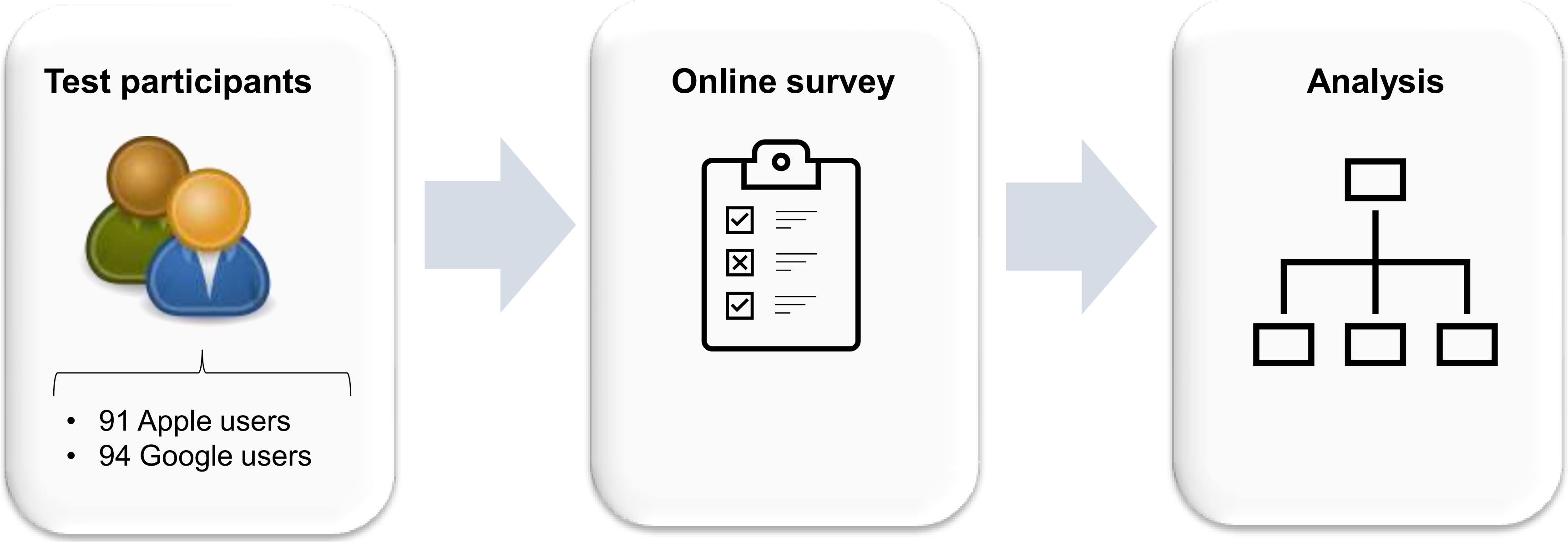
"Is it Really You Who Forgot the Password? When Account Recovery Meets Risk-Based Authentication"

Andre Büttner, Andreas Thue Pedersen, Stephan Wiefling, Nils Gruschka, and Luigi Lo Iacono

UbiSec 2023

➔ Risk-Based Account Recovery

RQ1 – User Account Study



Test participants

- 91 Apple users
- 94 Google users

Online survey

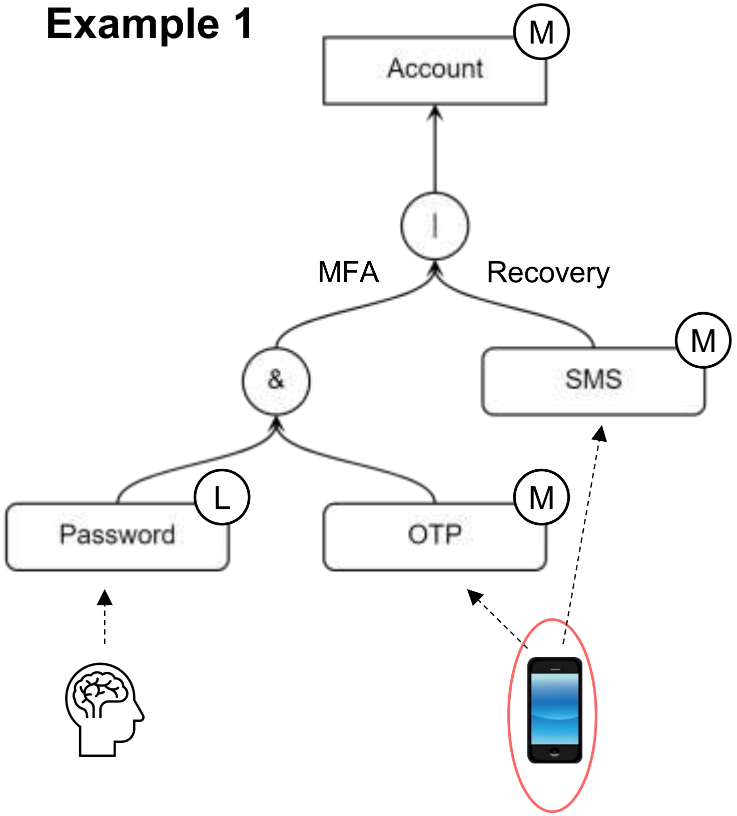
Analysis

RQ1 – User Account Study

Account Access Graphs[1]

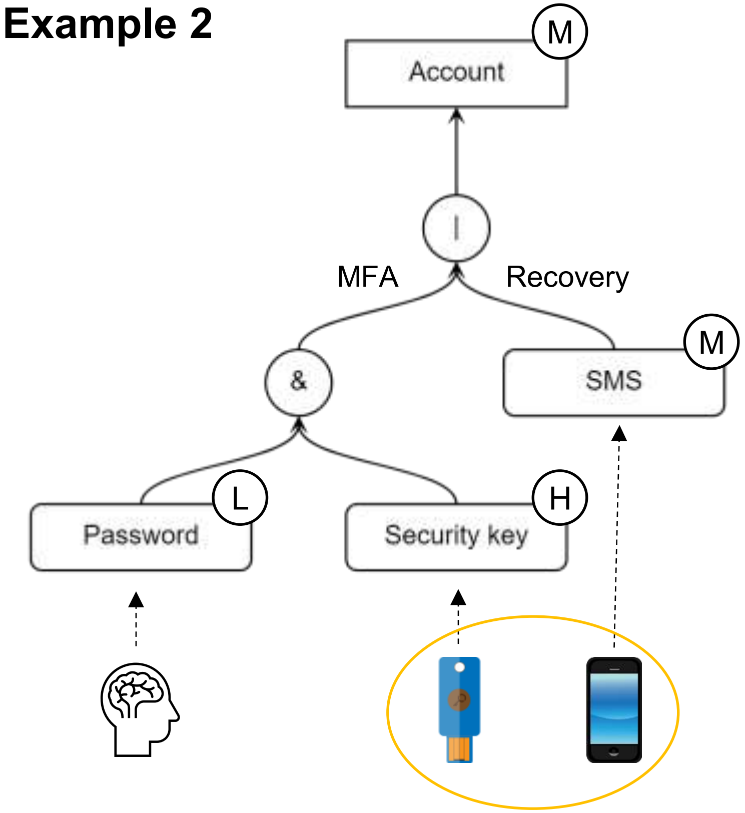
- Modelling account configurations
- Security score:
  - Low → Password, PIN
  - Medium → SMS, OTP
  - High → Security key
- Accessibility score:
  - Lowest number of devices whose <u>absence</u> can lead to account lockout

Example 1



$s_{acc} = 1$

Example 2



$s_{acc} = 2$

[1] Pöhn, *et al*. "Multi-account dashboard for authentication dependency analysis." Proceedings of the 17th International Conference on Availability, Reliability and Security (2022).

RQ1 – User Account Study

Main findings

Security

- Many Google accounts (~68%) have enabled MFA
- Even more (~80%) have enabled email recovery ➔ weak protection
- Apple implicitly enables MFA when signed-in with a device
- Almost all Apple accounts had a medium security score

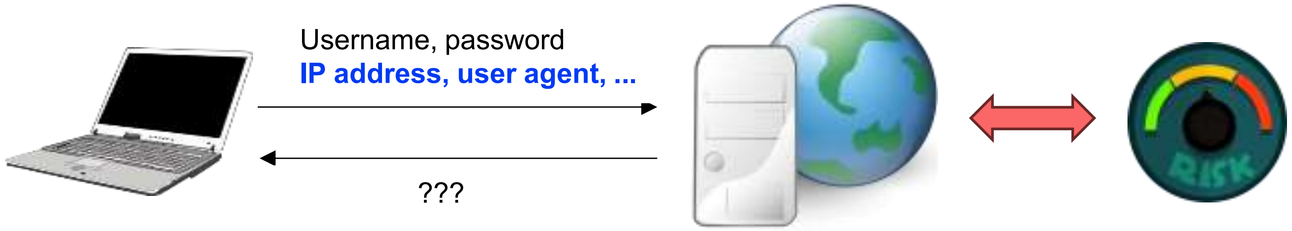
Accessibility

- Majority of Apple and Google accounts had a low account lockout risk
- 17 Apple and 10 Google accounts depend on a single device
- Primary smartphone usually most critical device

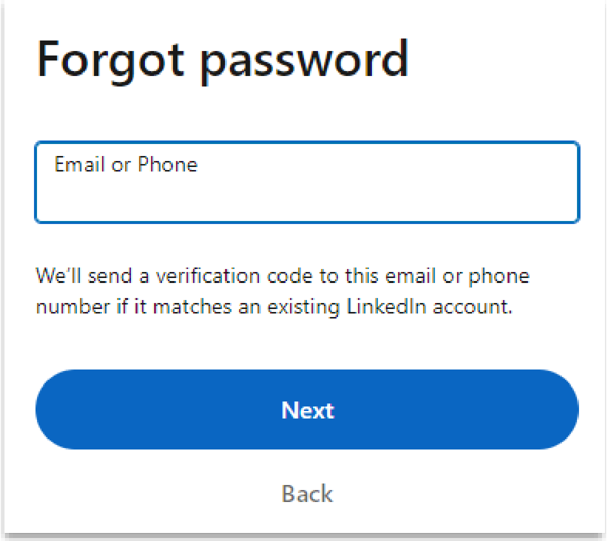
RQ1 – Risk-Based Account Recovery

Risk-based authentication[1]

- Risk assessment based on login history
- Additional authentication methods (or denial) for suspicious clients



➔ Do online services apply similar methods during account recovery?



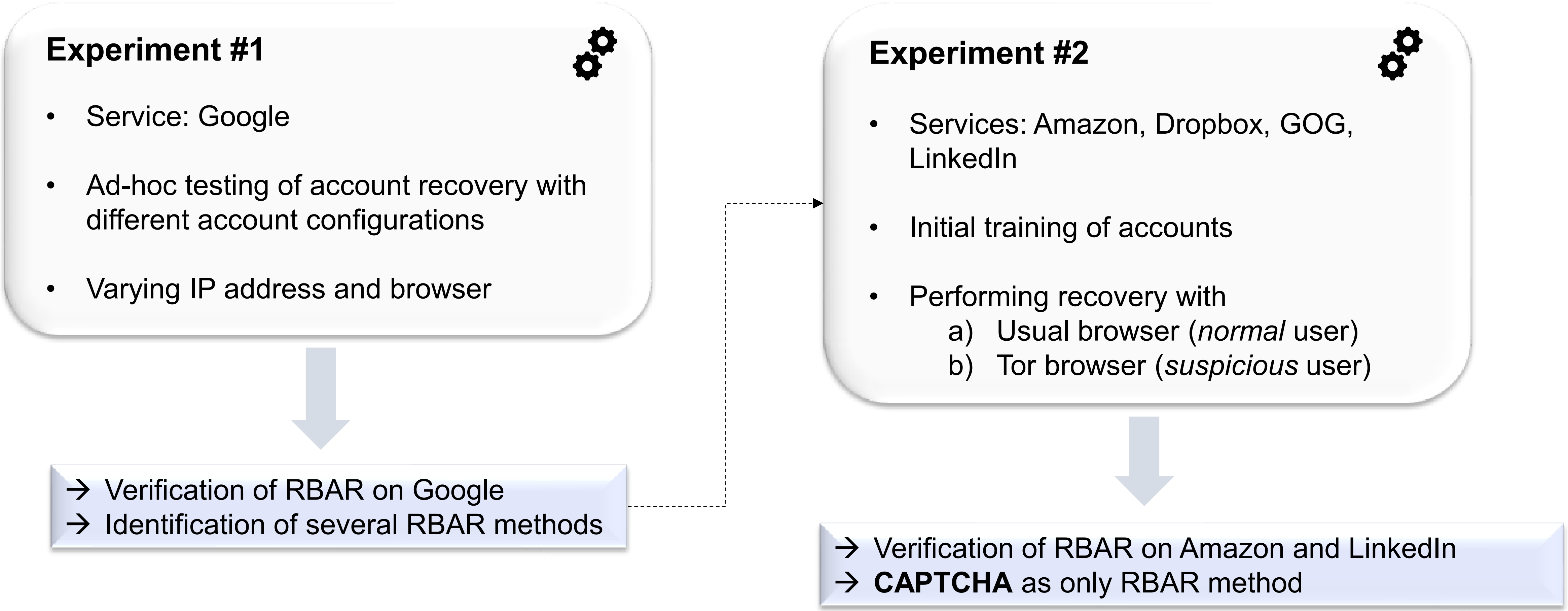
Forgot password

Email or Phone

We'll send a verification code to this email or phone number if it matches an existing LinkedIn account.

[1] Wiefling, *et al*. "Is this really you? An empirical study on risk-based authentication applied in the wild." ICT Systems Security and Privacy Protection: 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, Proceedings 34. Springer International Publishing, 2019.

RQ1 – Risk-Based Account Recovery



Experiment #1

- Service: Google
- Ad-hoc testing of account recovery with different account configurations
- Varying IP address and browser

→ Verification of RBAR on Google
→ Identification of several RBAR methods

Experiment #2

- Services: Amazon, Dropbox, GOG, LinkedIn
- Initial training of accounts
- Performing recovery with
  a) Usual browser (*normal* user)
  b) Tor browser (*suspicious* user)

→ Verification of RBAR on Amazon and LinkedIn
→ **CAPTCHA** as only RBAR method

RQ1 – Risk-Based Account Recovery

Summary

Maturity level	RBAR challenge	Identified on
3	Pre-configured MFA	Google
2	Background knowledge	Google
1	CAPTCHA	Amazon, LinkedIn
0	None	Dropbox, GOG

RQ2 To what extent is FIDO2 authentication vulnerable to Man-in-the-Middle attacks, and how can this be mitigated?

Paper III

"Enhancing FIDO Transaction Confirmation with Structured Data Formats"

Andre Büttner and Nils Gruschka

NISK 2021

➔ Transaction Confirmation

Paper IV

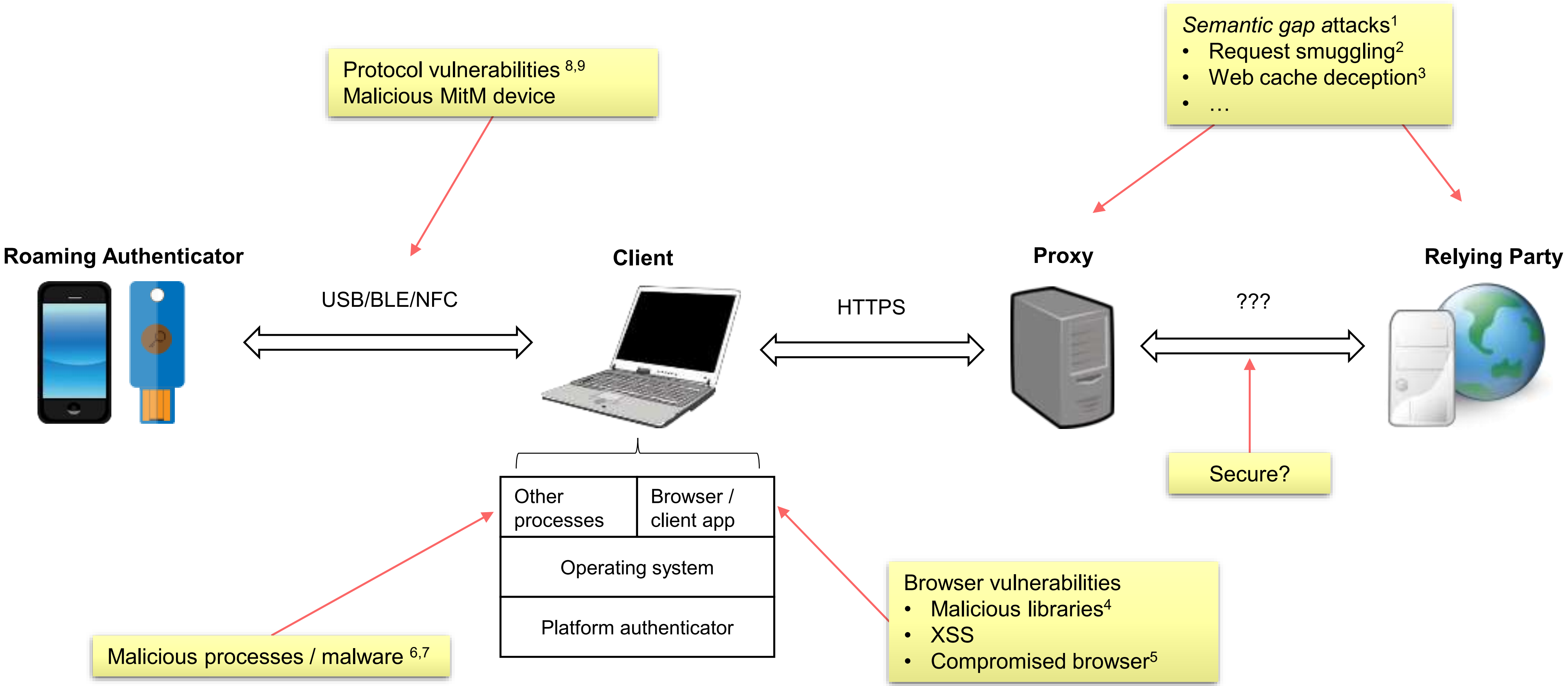
"Protecting FIDO Extensions against Man-in-the-Middle Attacks"

Andre Büttner and Nils Gruschka

ETAA 2022

➔ Protecting FIDO Extensions

RQ2 – FIDO Attack Surface



Protocol vulnerabilities [8,9]
Malicious MitM device

Semantic gap attacks[1]

- Request smuggling[2]
- Web cache deception[3]
- …

Roaming Authenticator

USB/BLE/NFC

Client

HTTPS

Proxy

???

Relying Party

Other processes

Browser / client app

Operating system

Platform authenticator

Secure?

Malicious processes / malware [6,7]

Browser vulnerabilities

- Malicious libraries[4]
- XSS
- Compromised browser[5]

1. Büttner, *et al.* "Less is Often More: Header Whitelisting as Semantic Gap Mitigation in HTTP-Based Software Systems." IFIP International Conference on ICT Systems Security and Privacy Protection. Springer, Cham, 2021.
2. Linhart, *et al.* "Http request smuggling" (2005).
3. Gil. "Web cache deception attack." Black Hat USA 2017 (2017).
4. Arshad, *et al.* "Include me out: In-browser detection of malicious third-party content inclusions." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2016.
5. Dougan and Curran. "Man in the browser attacks." International Journal of Ambient Computing and Intelligence (IJACI) 4.1 (2012): 29-39.
6. Bui, et al. "Man-in-the-Machine: Exploiting Ill-Secured Communication Inside the Computer." 27th USENIX security symposium (USENIX Security 18). 2018.
7. Zhang, et al. "Secure display for FIDO transaction confirmation." Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. 2018.
8. Sun, *et al.* "Man-in-the-middle attacks on Secure Simple Pairing in Bluetooth standard V5. 0 and its countermeasure." Personal and Ubiquitous Computing 22.1 (2018): 55-67.
9. Lahmadi, *et al.* "MitM attack detection in BLE networks using reconstruction and classification machine learning techniques." Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Springer, Cham, 2020.

RQ2 – Transaction Confirmation

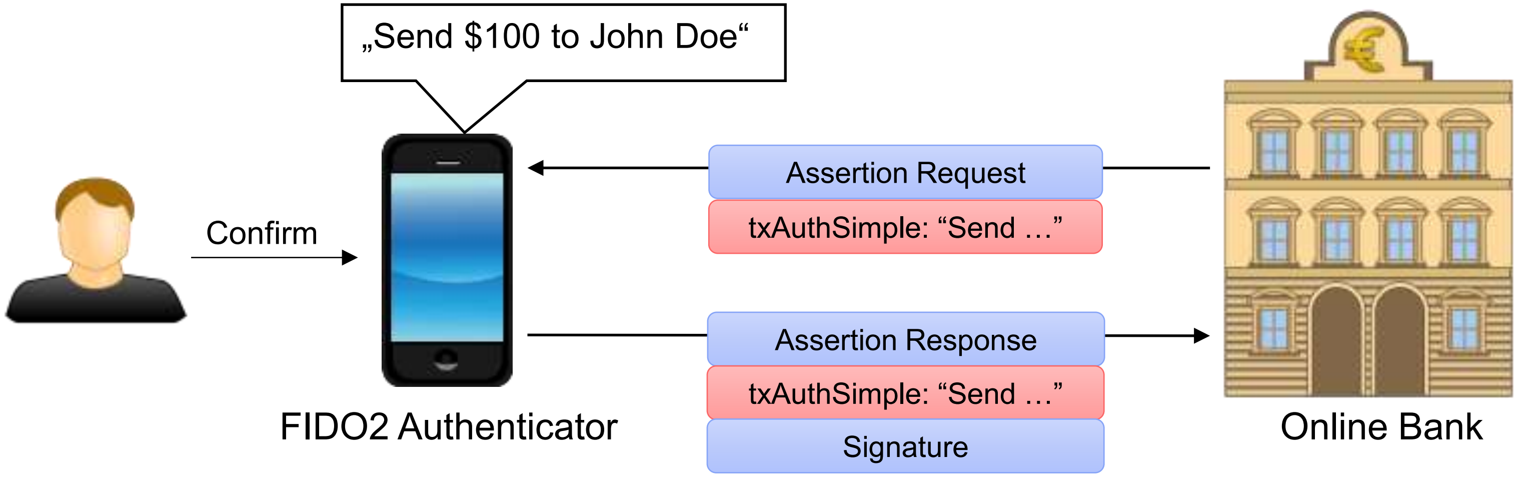
FIDO Transaction Confirmation[1]:

- Extension for online transactions

Risks:

- Ambiguous transaction text
- Homograph attacks

➔ Violation of what-you-see-is-what-you-sign[2]



[1] Lindemann and Leddy. "FIDO Transaction Confirmation White Paper". https://fidoalliance.org/wp-content/uploads/2020/08/FIDO-Alliance-Transaction-Confirmation-White-Paper-08-18-DM.pdf.

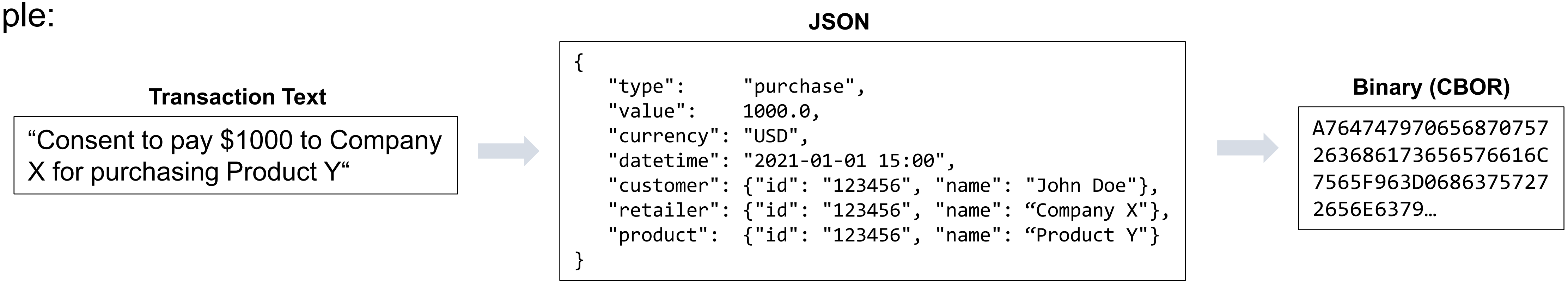
[2] Landrock and Pedersen. "WYSIWYS?—What you see is what you sign?." Information Security Technical Report 3.2 (1998): 55-61. https://doi.org/10.1016/S0167-4048(98)80005-8.

RQ2 – Transaction Confirmation

Countermeasure: structured data

- Avoid ambiguities
- Machine-readable → Applying policies to limit transaction values

Example:



Transaction Text

“Consent to pay $1000 to Company X for purchasing Product Y“

JSON

```
{
   "type":     "purchase",
   "value":    1000.0,
   "currency": "USD",
   "datetime": "2021-01-01 15:00",
   "customer": {"id": "123456", "name": "John Doe"},
   "retailer": {"id": "123456", "name": “Company X"},
   "product":  {"id": "123456", "name": “Product Y"}
}
```

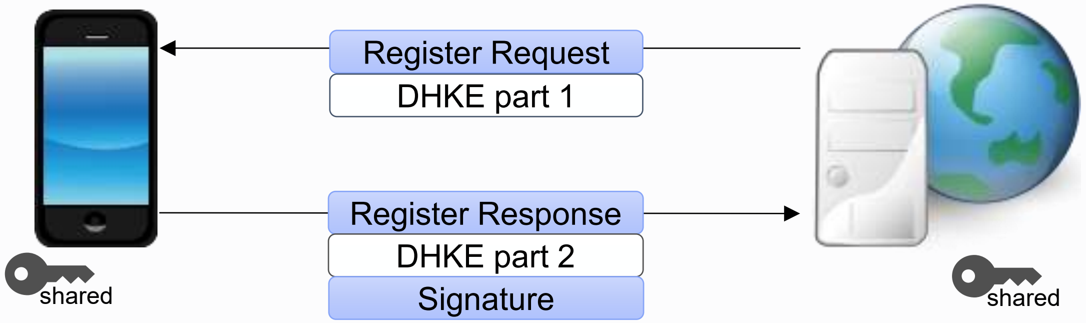
Binary (CBOR)

```
A764747970656870757
263686173656576616C
7565F963D0686375727
2656E6379…
```

RQ2 – Protecting FIDO Extensions

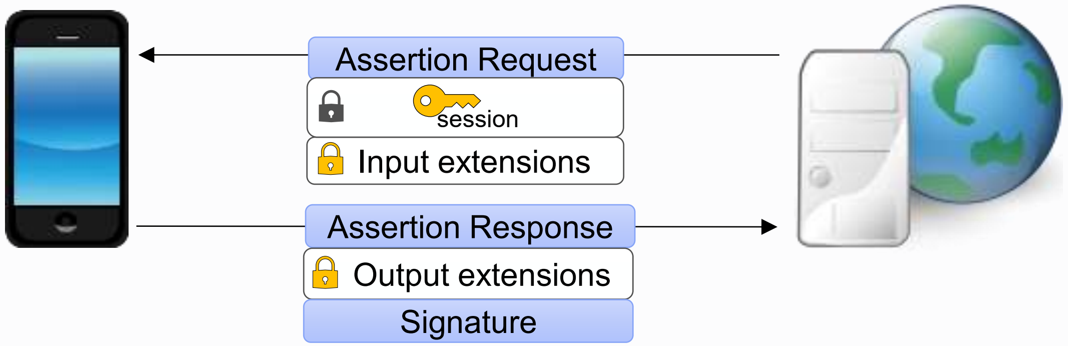
How to ensure confidentiality and authenticity of FIDO extensions?

Registration



Diffie-Hellman Key Exchange

Assertion



Key Wrapping & Authenticated Encryption

RQ3 How can data subjects be securely authenticated when exercising their data subject rights as required by GDPR?

Paper V

“Secure and Privacy-Preserving Authentication for Data Subject Rights Enforcement”

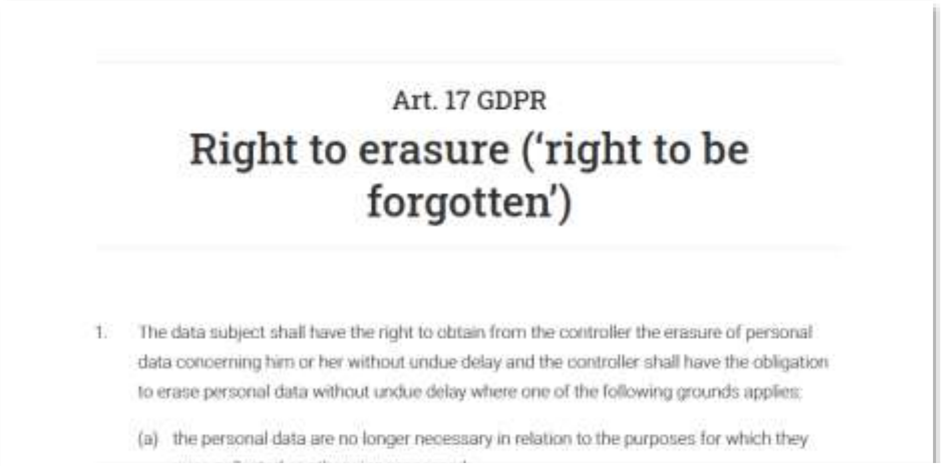
Malte Hansen and Andre Büttner

IFIP Summer School 2023

➔ Data Subject Right Authentication

RQ3 – Data Subject Right Authentication

- GDPR → Data Subject Rights
- Authentication challenging for third-party services
- Common verification methods:
  - Email address → **Improper validation[1]**
  - Passport / ID documents → **Information disclosure & forgeable[2]**

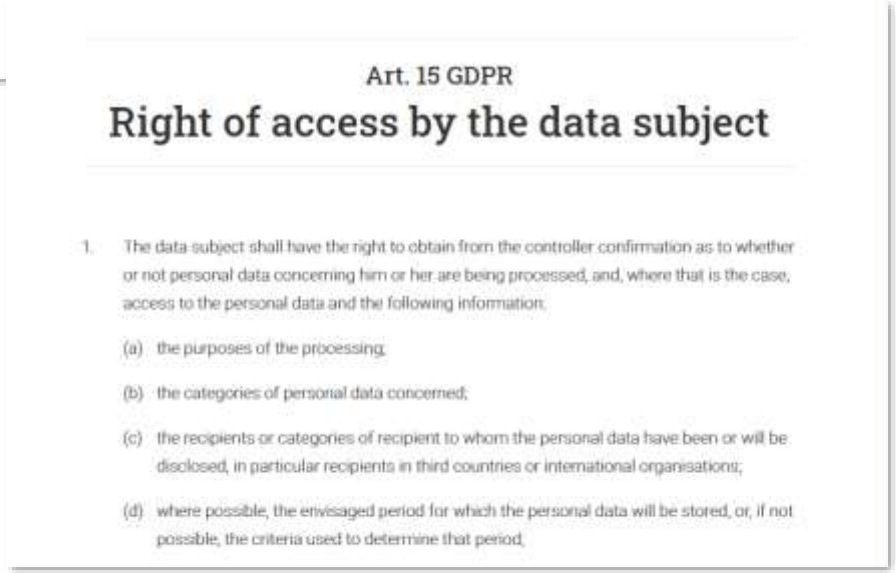


Art. 17 GDPR

Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they



Art. 15 GDPR

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

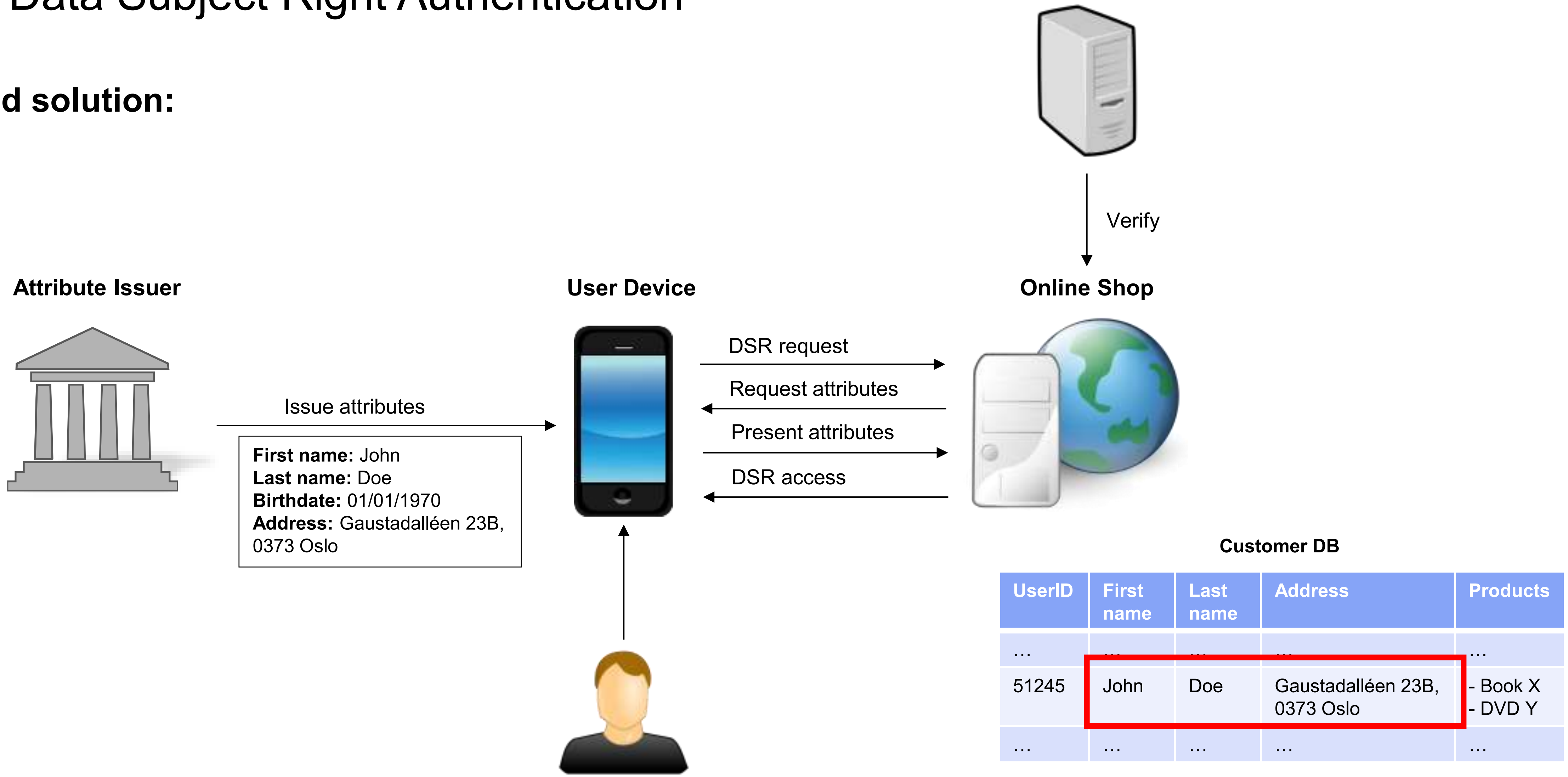
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

[1] Di Martino, *et al*. "Personal Information Leakage by Abusing the GDPR 'Right of Access'." Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019). 2019.

[2] Boniface, et al. "Security analysis of subject access request procedures: How to authenticate data subjects safely when they request for their data." Privacy Technologies and Policy: 7th Annual Privacy Forum, APF 2019, Rome, Italy, June 13–14, 2019, Proceedings 7. Springer International Publishing, 2019.

RQ3 – Data Subject Right Authentication

Proposed solution:



First name: John
Last name: Doe
Birthdate: 01/01/1970
Address: Gaustadalléen 23B, 0373 Oslo

Customer DB

UserID	First name	Last name	Address	Products
…	…	…	…	…
51245	John	Doe	Gaustadalléen 23B, 0373 Oslo	- Book X - DVD Y
…	…	…	…	…

Limitations

RQ1

- User account survey done with small set of test participants
- Both user account survey and RBAR experiments done on few services

RQ2

- Vulnerabilities discovered for FIDO extensions do not exclude other potential vulnerabilities

RQ3

- SSI-based approach for data subject authentication is not viable yet

Summary of Contributions

- Insights into security and accessibility risks of online users
- Risk-based implementations can affect security & accessibility

- FIDO extensions vulnerable to eavesdropping or manipulation
- Proposed protocol prevents attacks effectively

- Current data subject authentication involves security and privacy risks
- SSI-based architecture as strong alternative

- Federated credential management ➔ IdP behind almost all authentication methods
- Data subject right authentication ➔ Also related to accessibility
- Implicit user authentication ➔ Can generally benefit from SSI

Future Work

- ➢ Modelling risk-based approaches with account access graphs
- ➢ Analyzing the attack surface of FIDO2 passkeys
- ➢ Alternative methods for authenticating data subjects