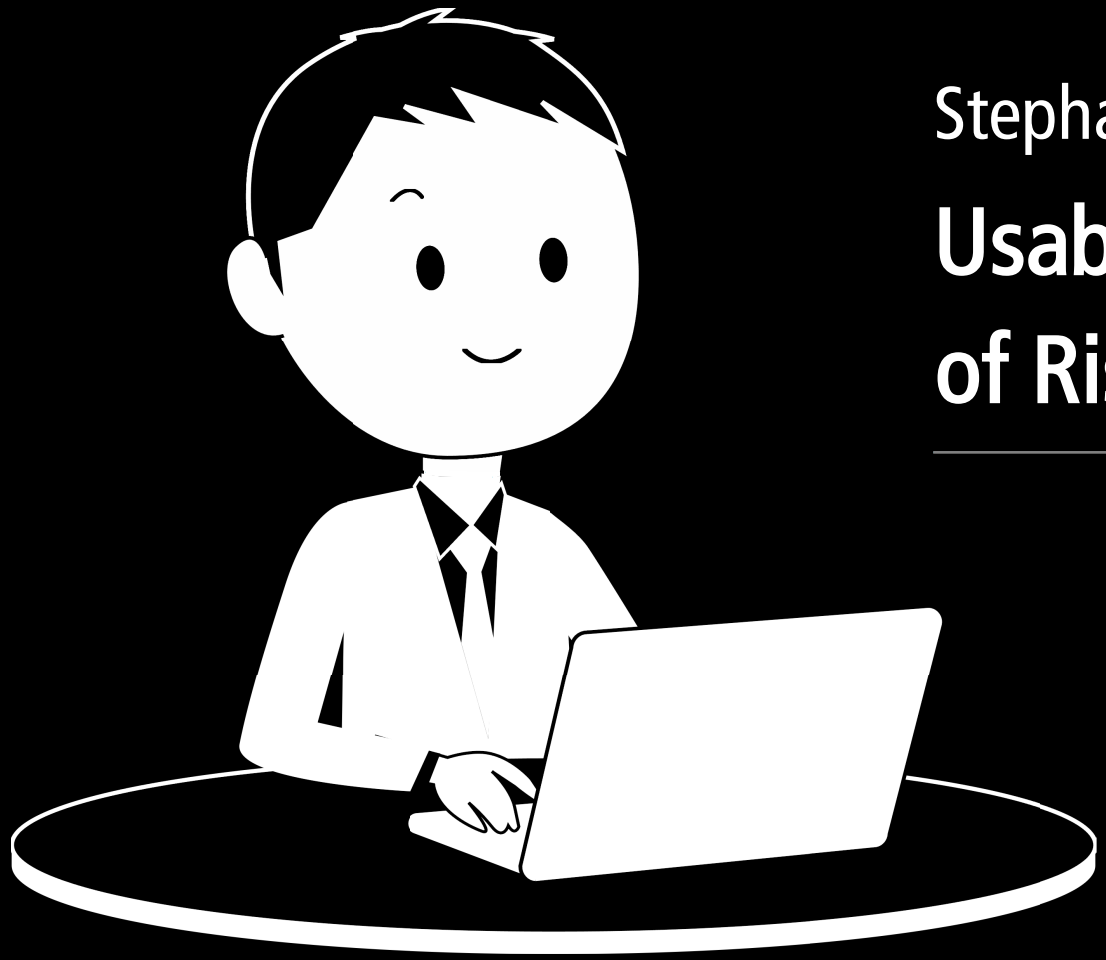
Hochschule Bonn-Rhein-Sieg
University of Applied Sciences

RUHR UNIVERSITÄT BOCHUM

RUB

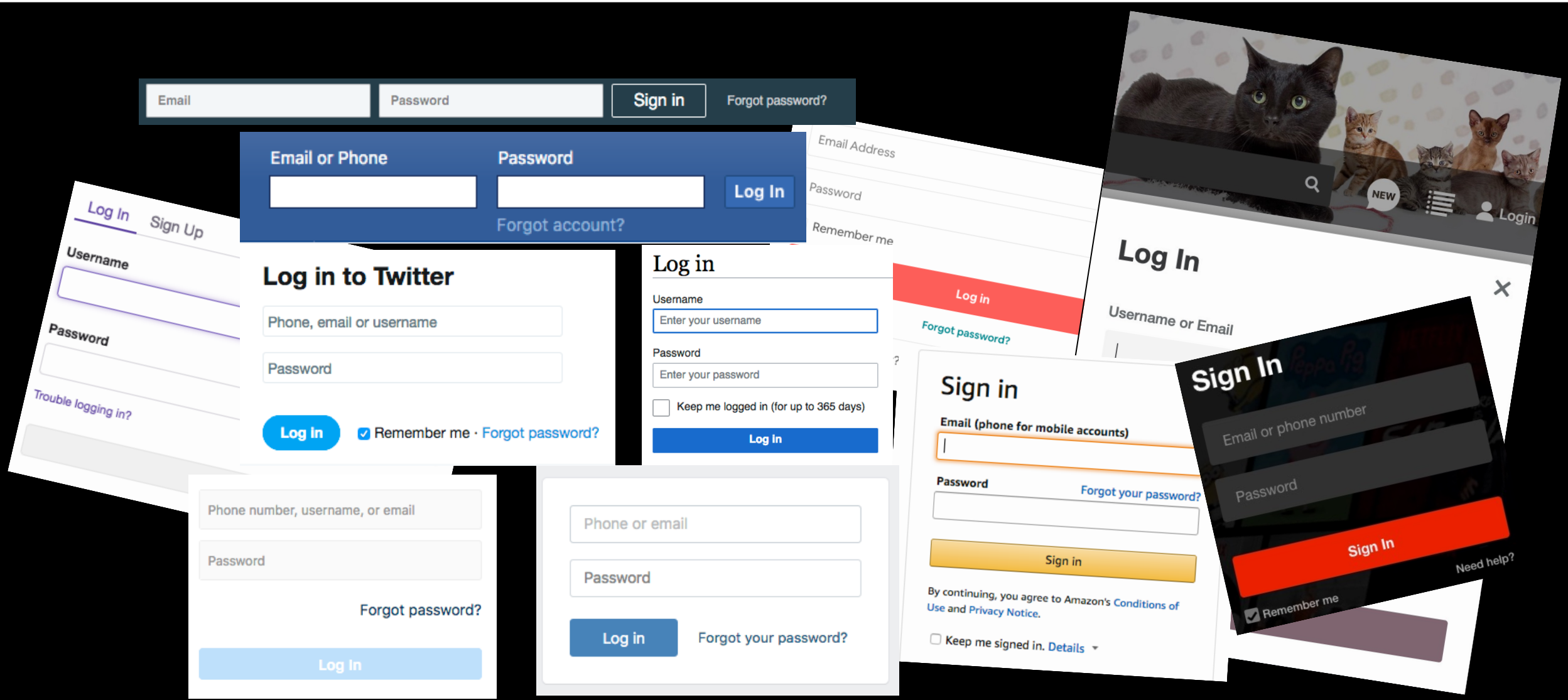


Stephan Wiefling

# Usability, Security, and Privacy of Risk-Based Authentication

Doctoral Examination

May 8th, 2023
Ruhr University Bochum


Email
Password
Sign in
Forgot password?
Email or Phone
Password
Log In
Forgot account?
Log In
Sign Up
Username
Password
Trouble logging in?
Log in to Twitter
Phone, email or username
Password
Log In
Remember me · Forgot password?
Log in
Username
Enter your username
Password
Enter your password
Keep me logged in (for up to 365 days)
Log In
Email Address
Password
Remember me
Log in
Forgot password?
Login
Log In
Username or Email
Phone number, username, or email
Password
Forgot password?
Log In
Phone or email
Password
Log in
Forgot your password?
Sign in
Email (phone for mobile accounts)
Password
Forgot your password?
Sign in
By continuing, you agree to Amazon's Conditions of Use and Privacy Notice.
Keep me signed in. Details
Sign In
Email or phone number
Password
Sign In
Need help?
Remember me

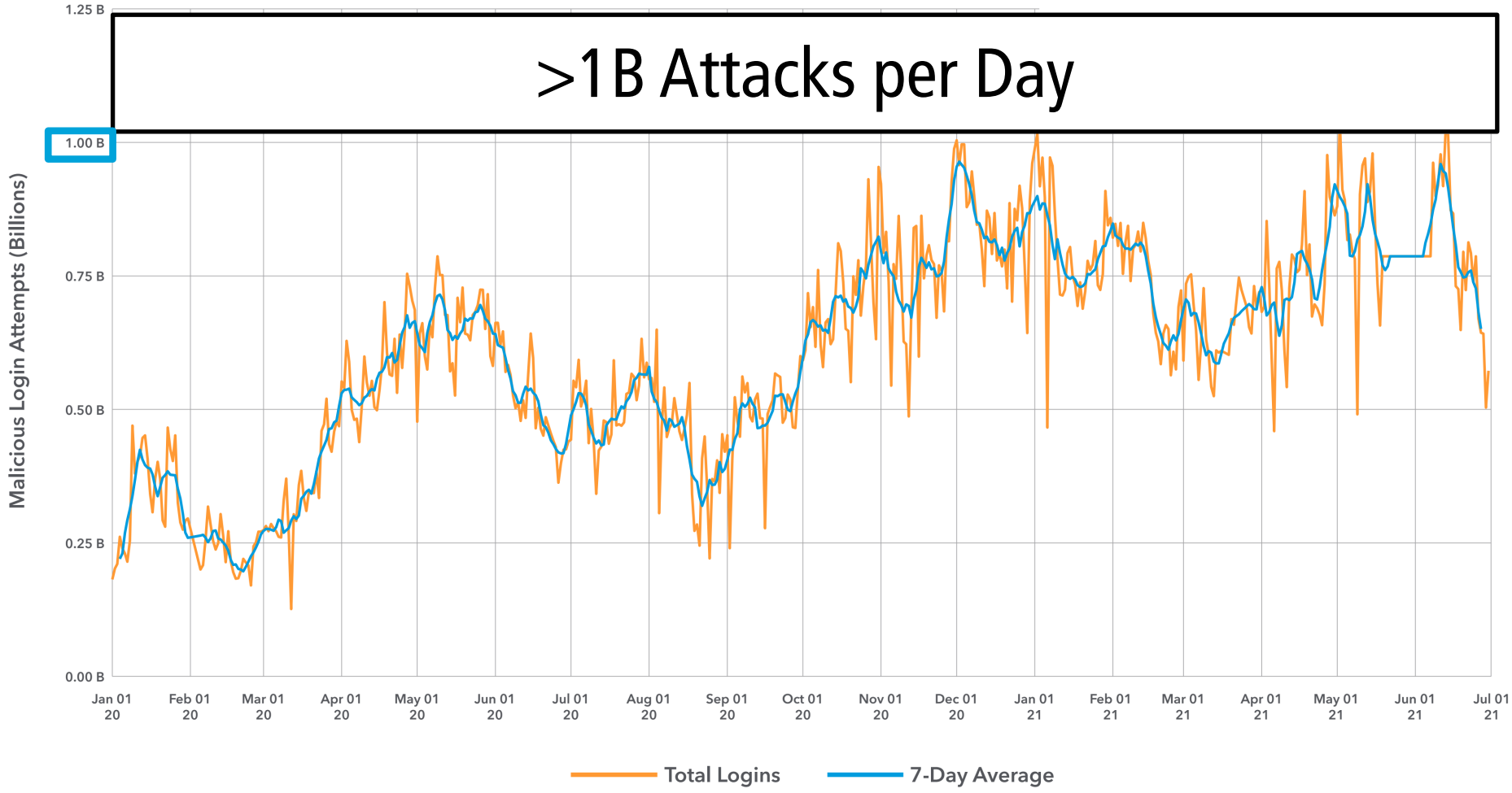
# >50% Password Re-Use*

*Representative survey conducted by Bilendi & respondi in February 2022; n=1000 German Internet users >18 years old
Also:
Das et al.: The Tangled Web of Password Reuse. In: NDSS (2014)
Pearman et al.: Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat. In: CCS (2017)

# Credential Stuffing

## Daily Credential Abuse Attempts

January 1, 2020 – June 30, 2021




Akamai: API: The Attack Surface That Connects Us All. In: [state of the internet] (2021).

# Phishing


2FA

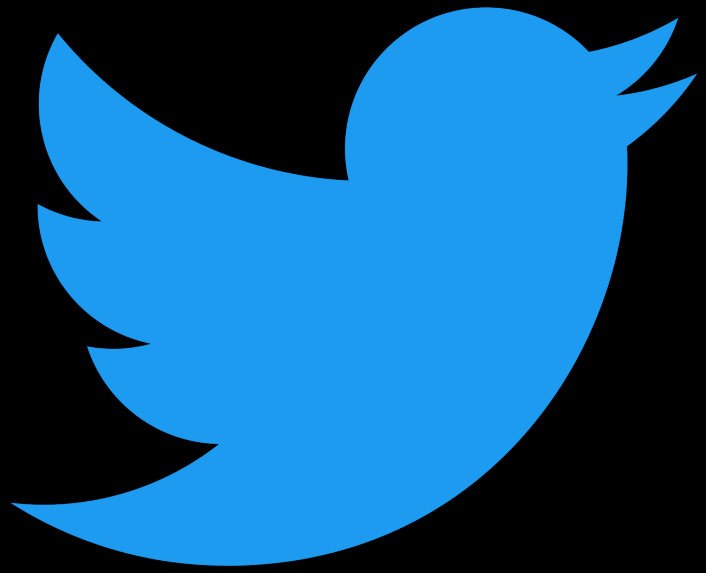
# Low 2FA Adoption in Practice

<10%*

*In January 2018
Milka, G.: Anatomy of Account Takeover. In: Enigma 2018. USENIX (Jan 2018)

~4%*

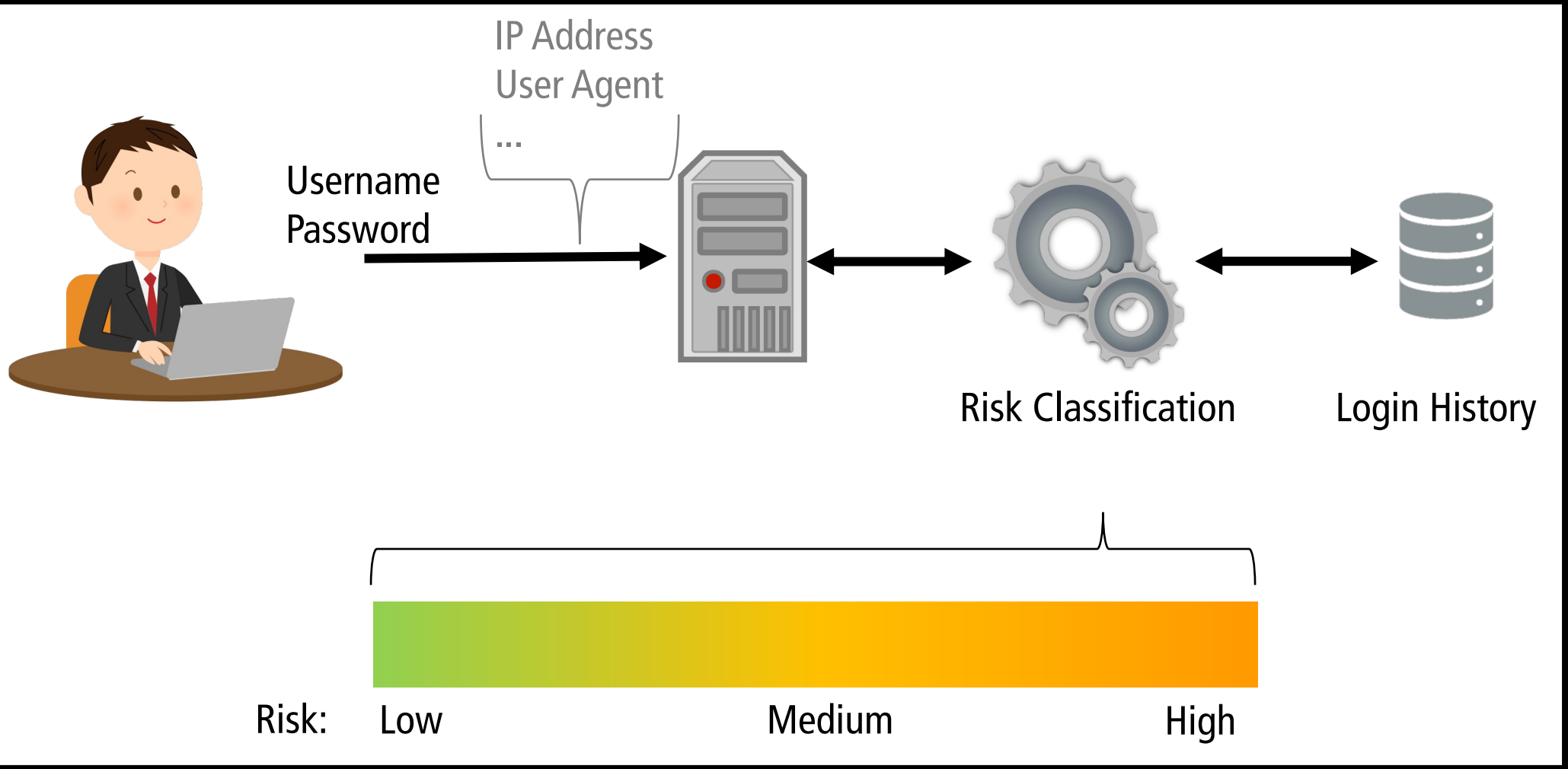
*In December 2021
Newman, L. H.: Facebook Will Force More At-Risk Accounts to Use Two-Factor. In: Wired (Dec 2021)



# 2.6%*

*In December 2021
Twitter: Account Security. In: Twitter Transparency Center (Jul 2022)

# Risk-Based Authentication (RBA)


IP Address
User Agent
...
Username
Password
Risk Classification
Login History
Risk:
Low
Medium
High

IP: Mallorca, ES
Chrome
Android 12
...

Username
Password

„There's something different here"

Risk Classification

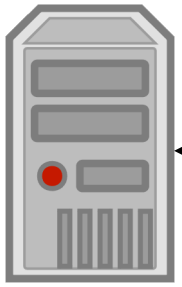
Medium

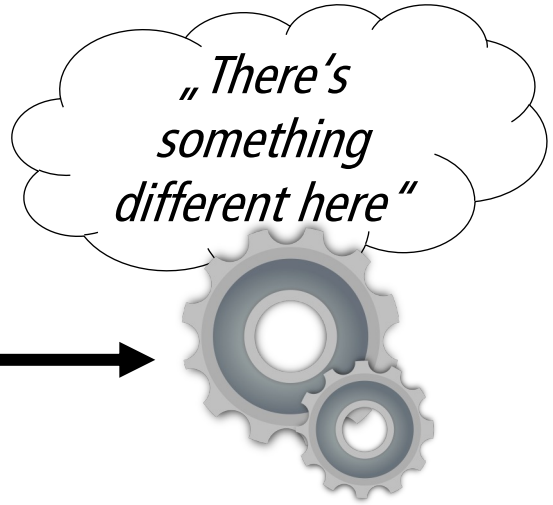
Additional Authentication

Proof for Additional Authentication

IP: Mallorca, ES
Chrome
Android 12
...

Username
Password






Risk Classification

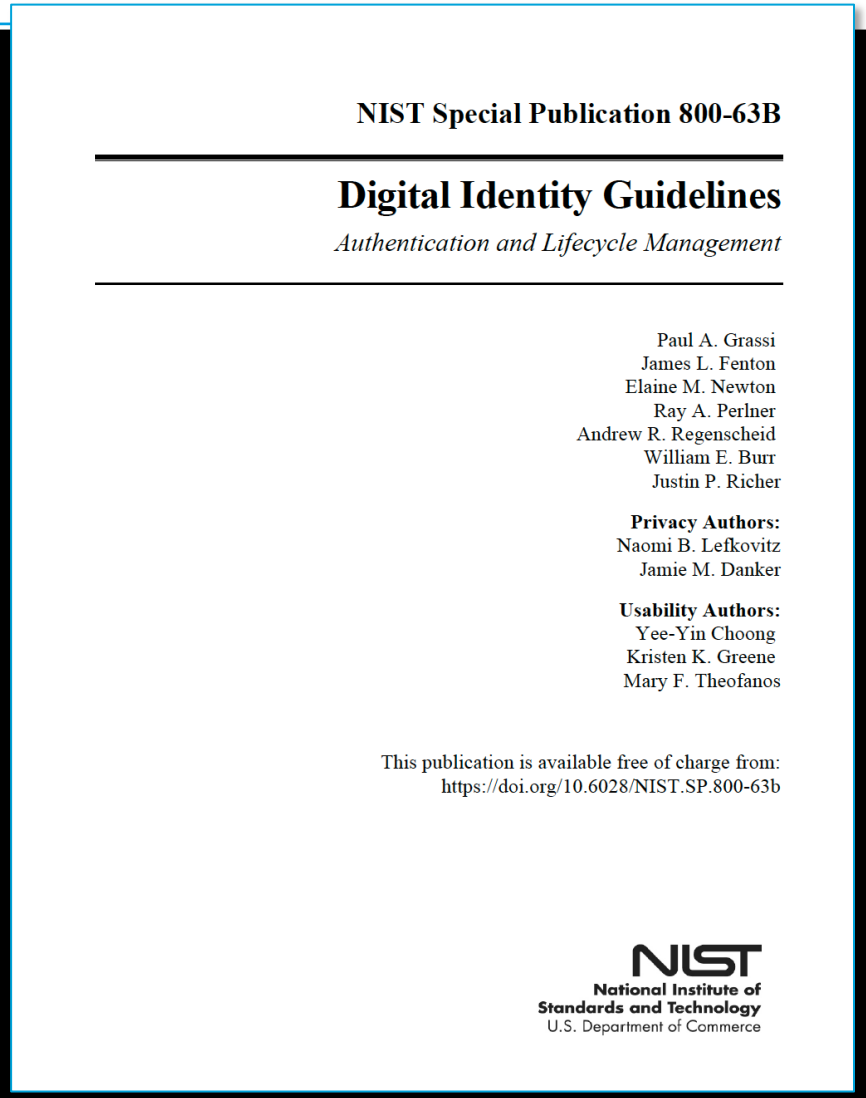
Medium

Additional Authentication

Can't Access Additional Authentication

# Risk-Based Authentication

- Recommended by NIST[1]



NIST Special Publication 800-63B

Digital Identity Guidelines

*Authentication and Lifecycle Management*

Paul A. Grassi
James L. Fenton
Elaine M. Newton
Ray A. Perlner
Andrew R. Regenscheid
William E. Burr
Justin P. Richer

**Privacy Authors:**
Naomi B. Lefkovitz
Jamie M. Danker

**Usability Authors:**
Yee-Yin Choong
Kristen K. Greene
Mary F. Theofanos

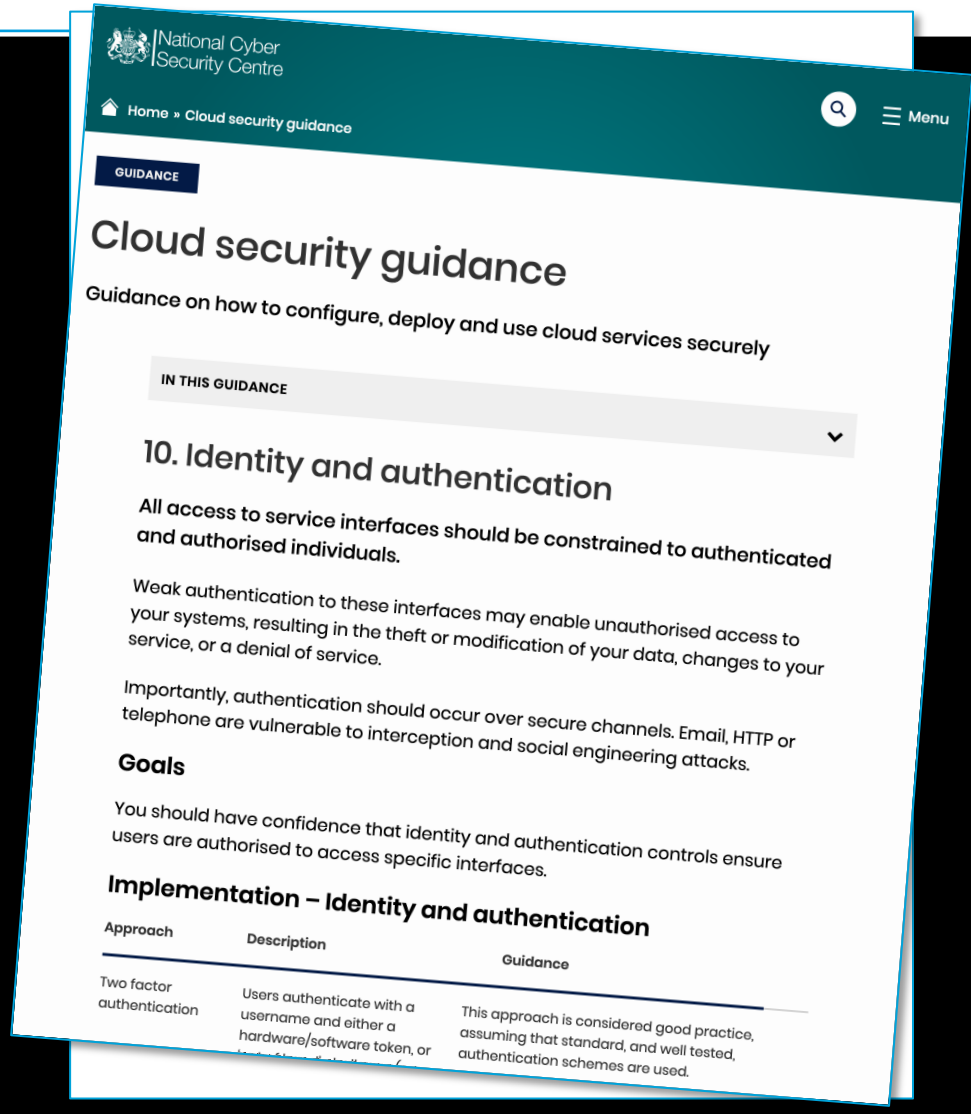
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63b

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

[1] Grassi et al.: Digital identity guidelines. Tech. Rep. NIST SP 800-63b (2017)

# Risk-Based Authentication

- Recommended by NIST[1], NCSC[2] and others


National Cyber Security Centre

Home » Cloud security guidance

Menu

GUIDANCE

## Cloud security guidance

**Guidance on how to configure, deploy and use cloud services securely**

IN THIS GUIDANCE

### 10. Identity and authentication

**All access to service interfaces should be constrained to authenticated and authorised individuals.**

Weak authentication to these interfaces may enable unauthorised access to your systems, resulting in the theft or modification of your data, changes to your service, or a denial of service.

Importantly, authentication should occur over secure channels. Email, HTTP or telephone are vulnerable to interception and social engineering attacks.

**Goals**

You should have confidence that identity and authentication controls ensure users are authorised to access specific interfaces.

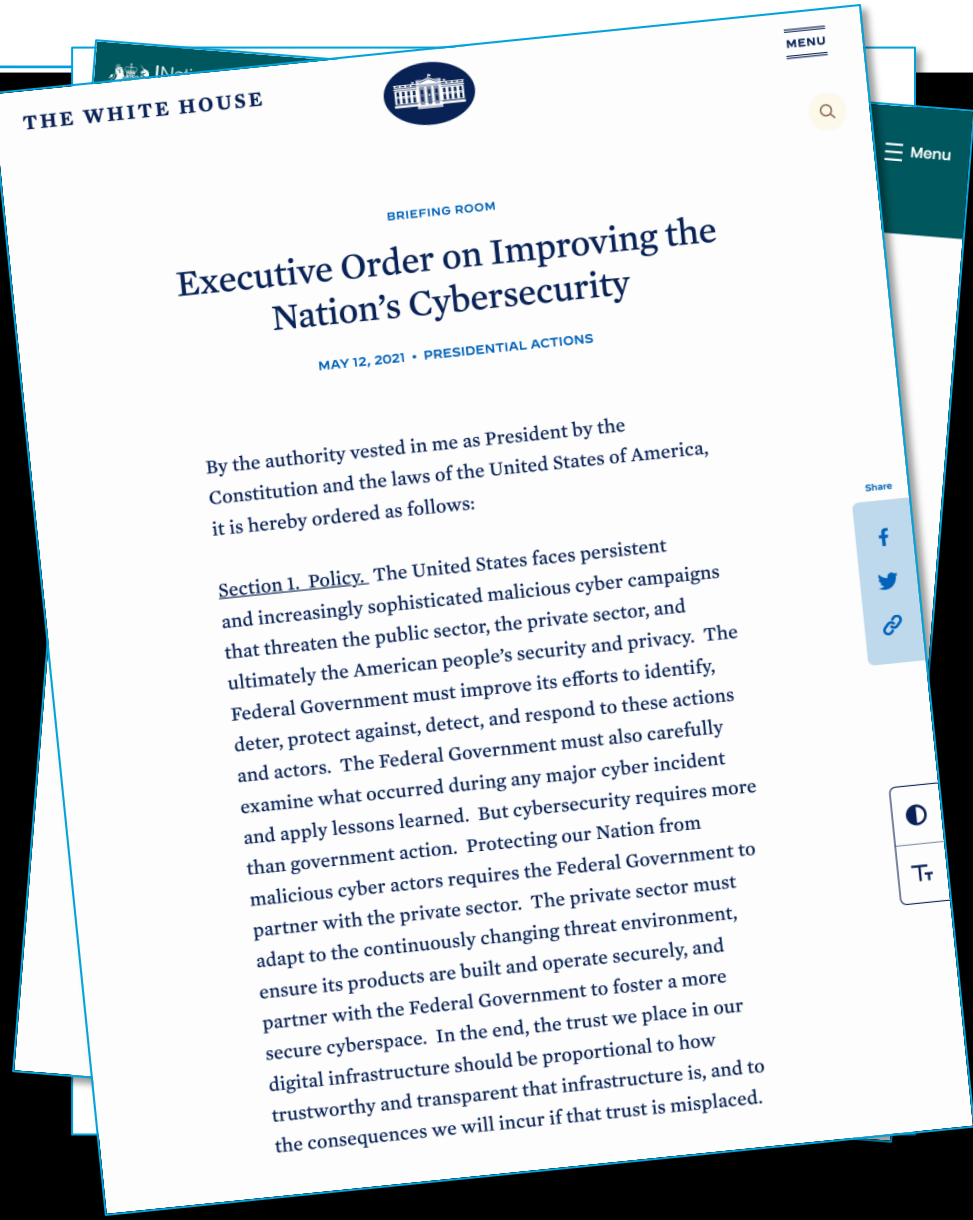
**Implementation – Identity and authentication**

| Approach | Description | Guidance |
|---|---|---|
| Two factor authentication | Users authenticate with a username and either a hardware/software token, or | This approach is considered good practice, assuming that standard, and well tested, authentication schemes are used. |

[1] Grassi et al.: Digital identity guidelines. Tech. Rep. NIST SP 800-63b (2017)
[2] National Cyber Security Centre: Cloud security guidance: 10, Identity and authentication. (2018)

# Risk-Based Authentication

- Recommended by NIST[1], NCSC[2] and others
- Required in the US by Presidential Order[3]
- But: Little or no research
  (before this thesis)

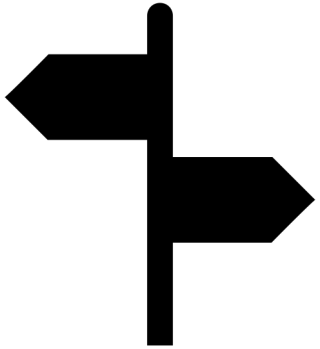



[1] Grassi et al.: Digital identity guidelines. Tech. Rep. NIST SP 800-63b (2017)
[2] National Cyber Security Centre: Cloud security guidance: 10, Identity and authentication. (2018)
[3] Biden Jr., J.R.: Executive Order on Improving the Nation's Cybersecurity. The White House. (2021)

# Main Motivation

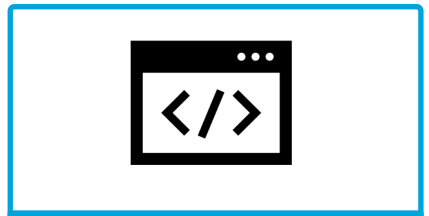
- Achieve broad understanding of RBA's usability, security, and privacy aspects
- This can foster widespread user acceptance and deployment of RBA on online services

State of Practice



## RQ1

"How do popular online services use RBA in practice, [...] and how do their user interfaces and requested additional authentication factors look like?"



State of Practice

IFIP SEC '19

Rank: CORE B

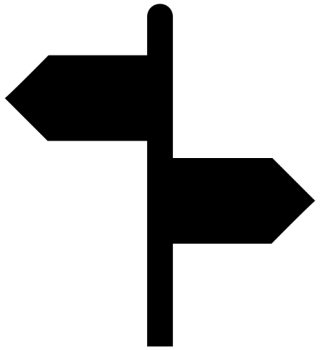
# Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild

Stephan Wiefling[1(✉)], Luigi Lo Iacono[1], and Markus Dürmuth[2]

[1] TH Köln - University of Applied Sciences, Cologne, Germany
{stephan.wiefling,luigi.lo_iacono}@th-koeln.de
[2] Ruhr University Bochum, Bochum, Germany
markus.duermuth@rub.de

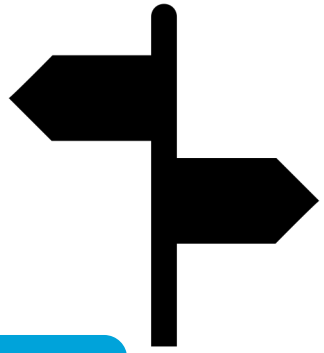
**Abstract.** Risk-based authentication (RBA) is an adaptive security measure to strengthen password-based authentication. RBA monitors additional implicit features during password entry such as device or geolocation information, and requests additional authentication factors if a certain risk level is detected. RBA is recommended by the NIST digital identity guidelines, is used by several large online services, and offers protection against security risks such as password database leaks, credential stuffing, insecure passwords and large-scale guessing attacks. Despite its relevance, the procedures used by RBA-instrumented online services are currently not disclosed. Consequently, there is little scientific research about RBA, slowing down progress and deeper understanding, making it harder for end users to understand the security provided by the services they use and trust, and hindering the widespread adoption of RBA.

In this paper, with a series of studies on eight popular online services, we (i) analyze which features and combinations/classifiers are used and are useful in practical instances, (ii) develop a framework and a methodology to measure RBA in the wild, and (iii) survey and discuss the differences in the user interface for RBA. Following this, our work provides a first deeper understanding of practical RBA deployments and helps fostering further research in this direction.



State of Practice

IFIP SEC ‘19



Rank: CORE B

Usability

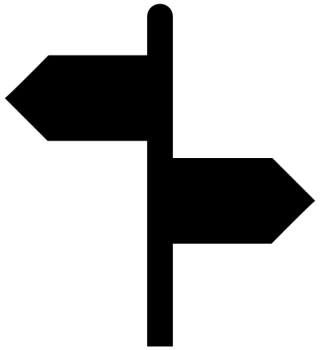
## RQ2

“How do users perceive RBA’s usability and security compared to 2FA and password-only authentication [...]?”

State of Practice

IFIP SEC ‘19

Rank: CORE B



Usability

## RQ3

“How can RBA’s re-authentication state of practice be improved regarding usability [...]?”

State of Practice

IFIP SEC '19

Rank: CORE B

Usability

ACSAC '20

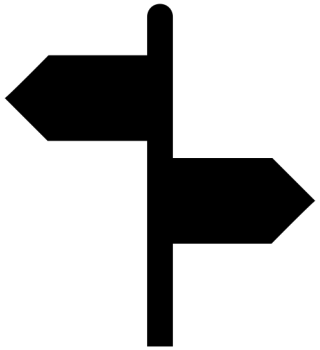
Ranks: CORE A

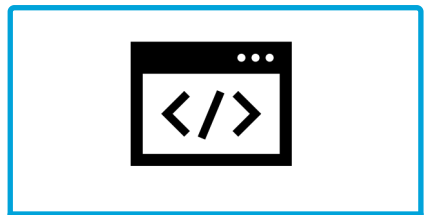
**More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication**


Stephan Wiefling
H-BRS University of Applied Sciences
Ruhr University Bochum
stephan.wiefling@h-brs.de

Markus Dürmuth
Ruhr University Bochum
Bochum, Germany
markus.duermuth@rub.de

Luigi Lo Iacono
H-BRS University of Applied Sciences
Sankt Augustin, Germany
luigi.lo_iacono@h-brs.de



State of Practice

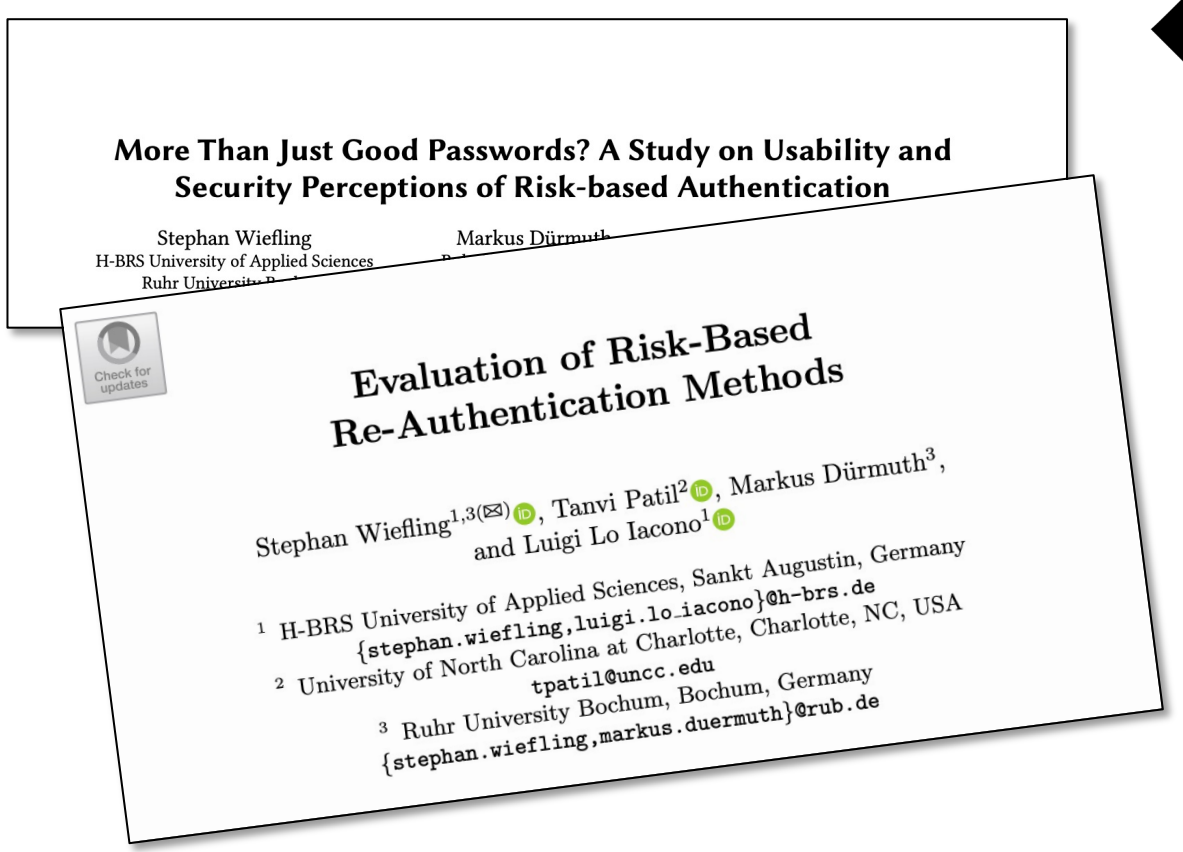
IFIP SEC ‘19

Rank: CORE B

Usability

ACSAC ‘20
IFIP SEC ‘20

Ranks: CORE A + B



More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication

Stephan Wiefling
H-BRS University of Applied Sciences

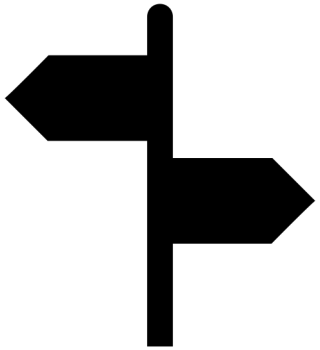
Markus Dürmuth

Check for updates

Evaluation of Risk-Based Re-Authentication Methods

Stephan Wiefling[1,3(✉)], Tanvi Patil[2], Markus Dürmuth[3], and Luigi Lo Iacono[1]

[1] H-BRS University of Applied Sciences, Sankt Augustin, Germany
{stephan.wiefling,luigi.lo_iacono}@h-brs.de
[2] University of North Carolina at Charlotte, Charlotte, NC, USA
tpatil@uncc.edu
[3] Ruhr University Bochum, Bochum, Germany
{stephan.wiefling,markus.duermuth}@rub.de



State of Practice

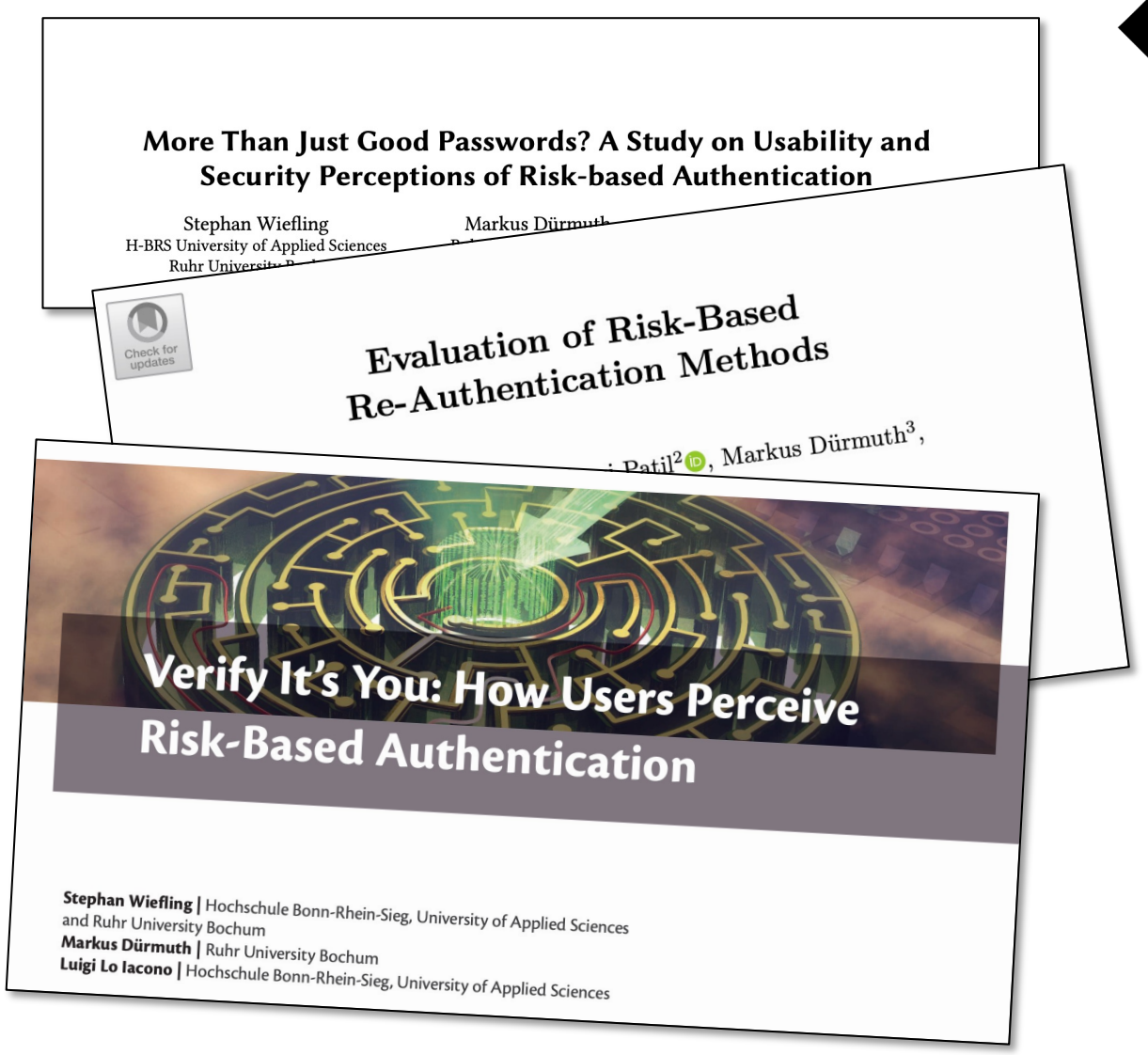
IFIP SEC ‘19

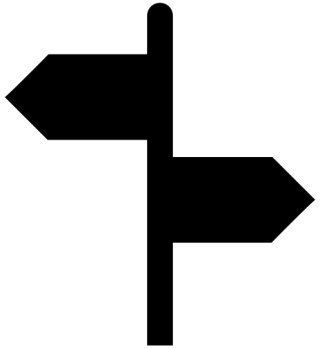
Rank: CORE B

Usability

ACSAC ‘20
IFIP SEC ‘20
S&PM ‘21

Ranks: CORE A + B
CiteScore 4.4

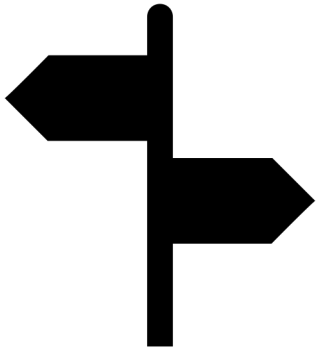


State of Practice

IFIP SEC ‘19

Rank: CORE B



Usability

ACSAC ‘20
IFIP SEC ‘20
S&PM ‘21

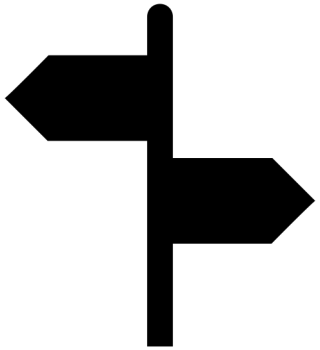
Ranks: CORE A + B
CiteScore 4.4

Security and Privacy

State of Practice

IFIP SEC ‘19

Rank: CORE B



Usability

ACSAC ‘20
IFIP SEC ‘20
S&PM ‘21

Ranks: CORE A + B
CiteScore 4.4

Security and Privacy

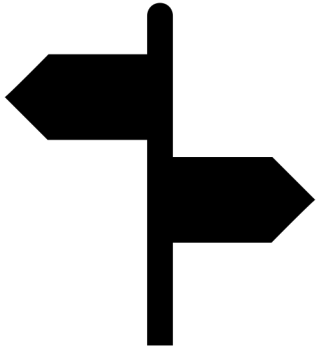
## RQ4

“How [...] does RBA have to be configured to achieve high usability and security [in a practical deployment]?”

State of Practice

IFIP SEC ‘19

Rank: CORE B



Usability

ACSAC ‘20
IFIP SEC ‘20
S&PM ‘21

Ranks: CORE A + B
CiteScore 4.4

Security and Privacy

## RQ5

“What privacy challenges may arise with RBA use, and how can RBA systems be privacy enhanced while balancing security and usability in practice?”

State of Practice

IFIP SEC '19

Rank: CORE B

Usability

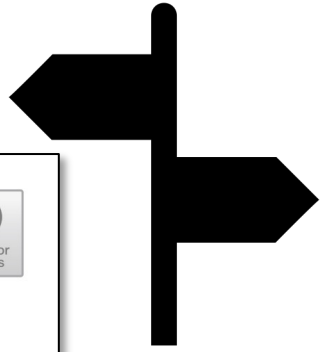
ACSAC '20
IFIP SEC '20
S&PM '21

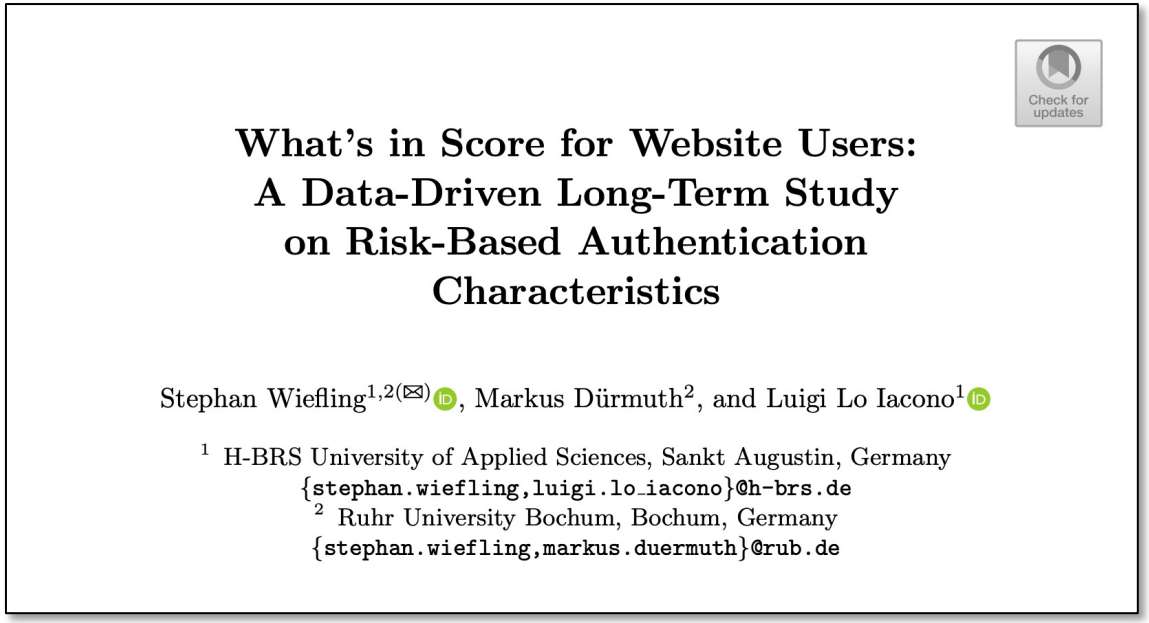
Ranks: CORE A + B
CiteScore 4.4

Security and Privacy

FC '21

Rank: CORE A



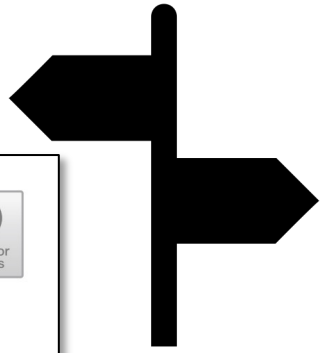


Check for updates

**What's in Score for Website Users: A Data-Driven Long-Term Study on Risk-Based Authentication Characteristics**

Stephan Wiefling[1,2(✉)], Markus Dürmuth[2], and Luigi Lo Iacono[1]

[1] H-BRS University of Applied Sciences, Sankt Augustin, Germany
{stephan.wiefling,luigi.lo_iacono}@h-brs.de
[2] Ruhr University Bochum, Bochum, Germany
{stephan.wiefling,markus.duermuth}@rub.de



State of Practice

IFIP SEC '19

Rank: CORE B

Usability

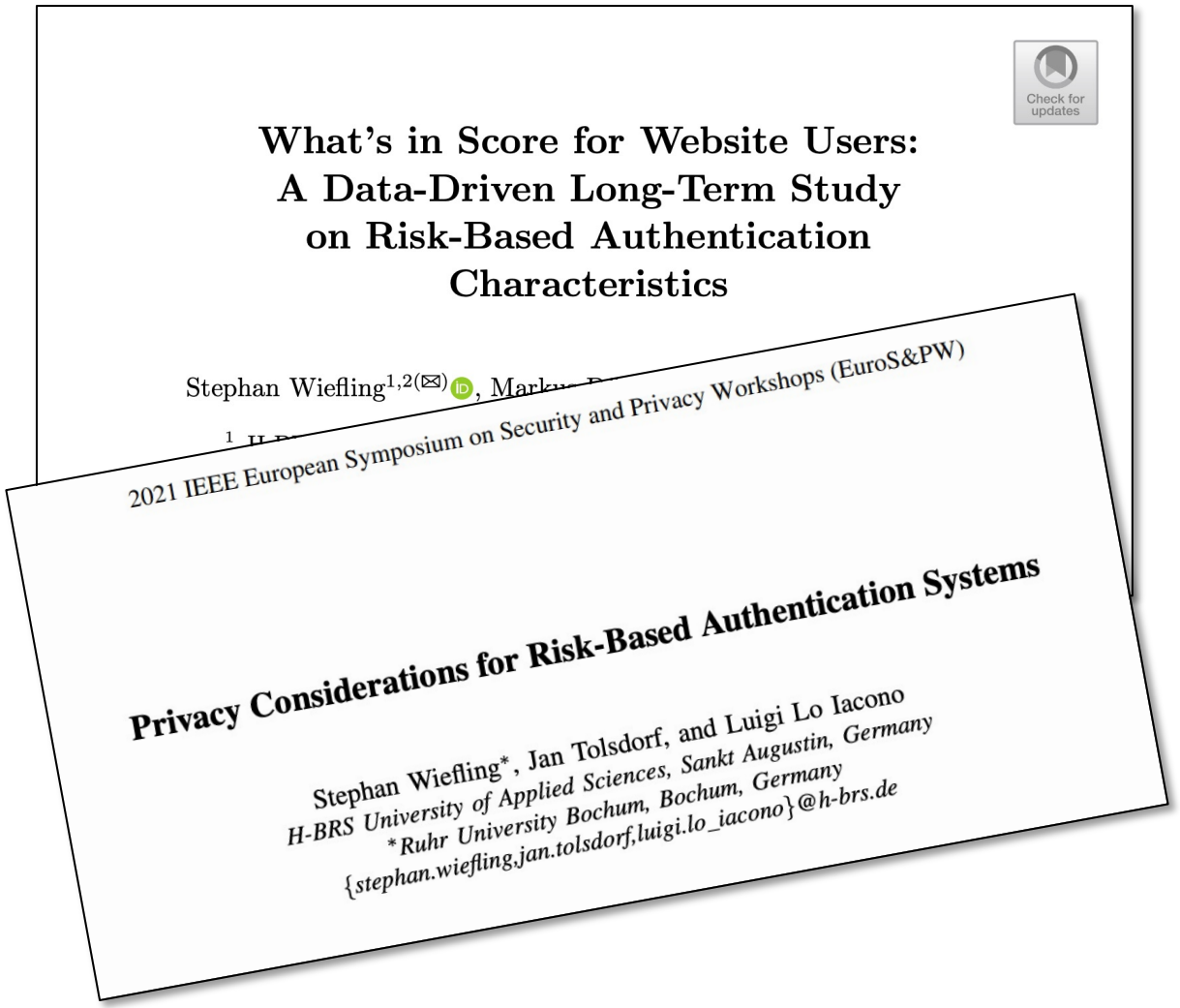
ACSAC '20
IFIP SEC '20
S&PM '21

Ranks: CORE A + B
CiteScore 4.4

Security and Privacy

FC '21
IWPE '21

Rank: CORE A
+ Workshop



What's in Score for Website Users: A Data-Driven Long-Term Study on Risk-Based Authentication Characteristics

Stephan Wiefling[1,2(✉)], Mark...

2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)

Privacy Considerations for Risk-Based Authentication Systems

Stephan Wiefling*, Jan Tolsdorf, and Luigi Lo Iacono
H-BRS University of Applied Sciences, Sankt Augustin, Germany
*Ruhr University Bochum, Bochum, Germany
{stephan.wiefling,jan.tolsdorf,luigi.lo_iacono}@h-brs.de

State of Practice

IFIP SEC ‘19

Rank: CORE B

Usability

ACSAC ‘20
IFIP SEC ‘20
S&PM ‘21

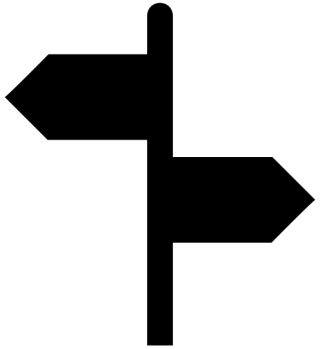
Ranks: CORE A + B
CiteScore 4.4

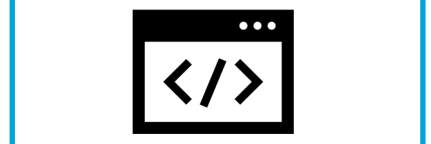
Security and Privacy

FC ‘21
IWPE ‘21

Rank: CORE A + Workshop

Large-Scale Online Service





State of Practice

IFIP SEC '19

Rank: CORE B

Usability

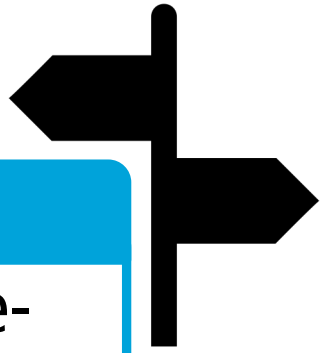
ACSAC '20
IFIP SEC '20
S&PM '21

Ranks: CORE A + B
CiteScore 4.4

Security and Privacy

FC '21
IWPE '21

Rank: CORE A + Workshop



## RQ6

"How are RBA characteristics on a large-scale online service and how can RBA [...] be optimized to achieve high usability, security, and privacy?"

Large-Scale Online Service

State of Practice

IFIP SEC '19

Rank: CORE B

Usability

ACSAC '20
IFIP SEC '20
S&PM '21

Ranks: CORE A + B
CiteScore 4.4

Security and Privacy

FC '21
IWPE '21

Rank: CORE A
+ Workshop

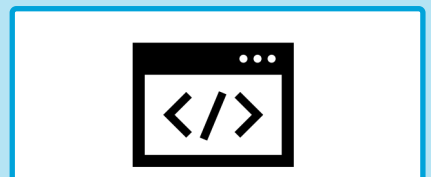
**Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service**

STEPHAN WIEFLING, H-BRS University of Applied Sciences, Germany and Ruhr University Bochum, Germany
PAUL RENÉ JØRGENSEN and SIGURD THUNEM, Telenor Digital, Norway
LUIGI LO IACONO, H-BRS University of Applied Sciences, Germany

Large-Scale Online Service

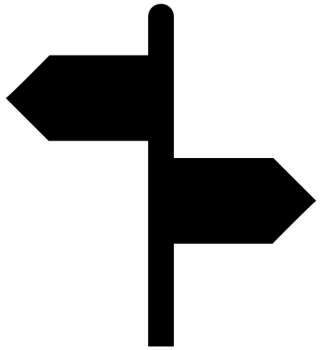
TOPS '22
Open Data Impact Award '22

Rank: CORE A
CiteScore 6.8



State of Practice

IFIP SEC ‘19

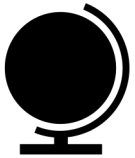


Usability

ACSAC ‘20
IFIP SEC ‘20
S&PM ‘21

Security and Privacy

FC ‘21
IWPE ‘21

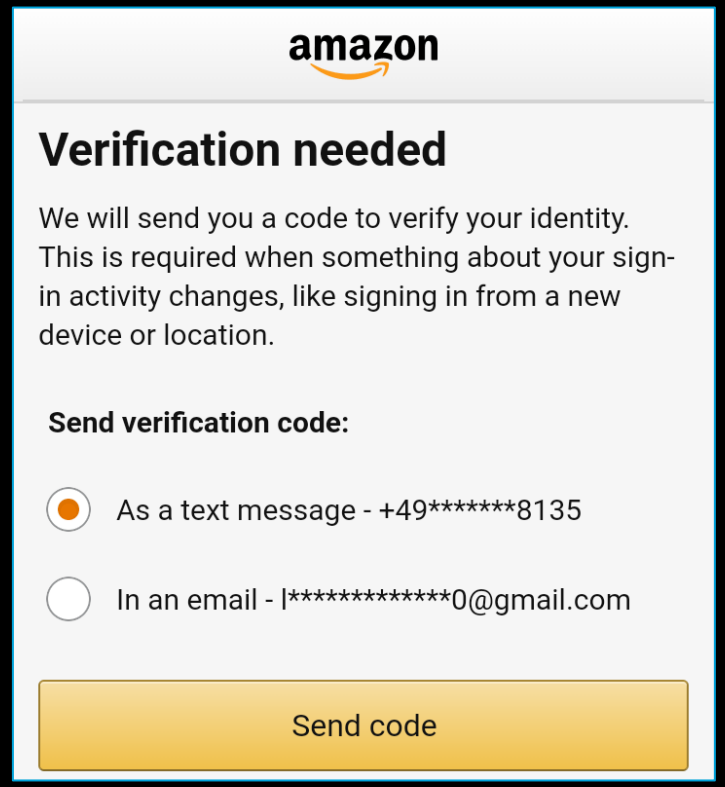


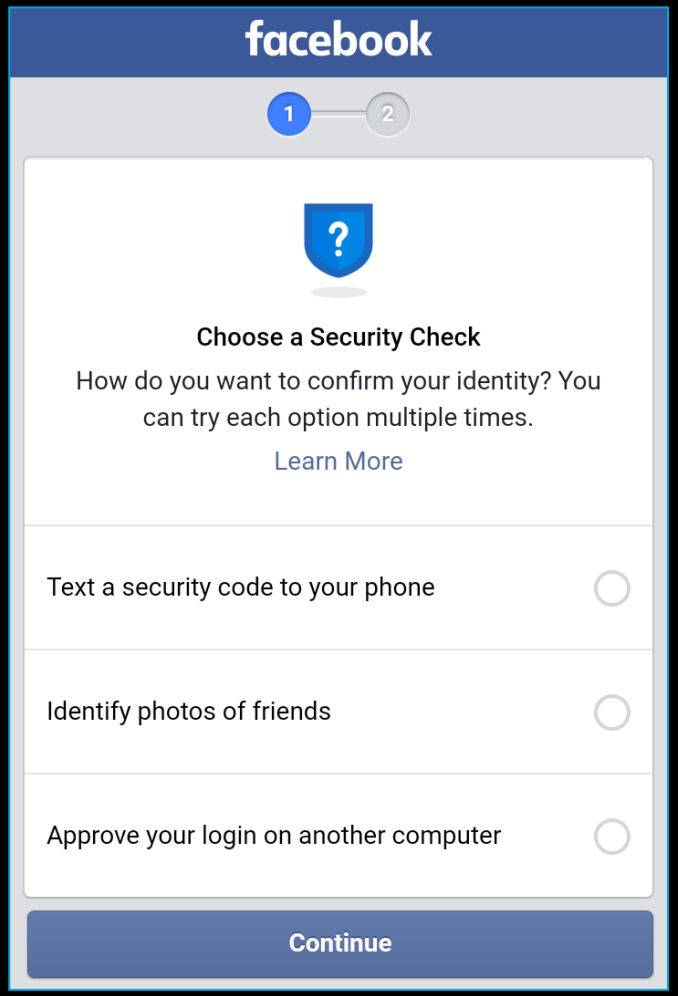
Large-Scale Online Service

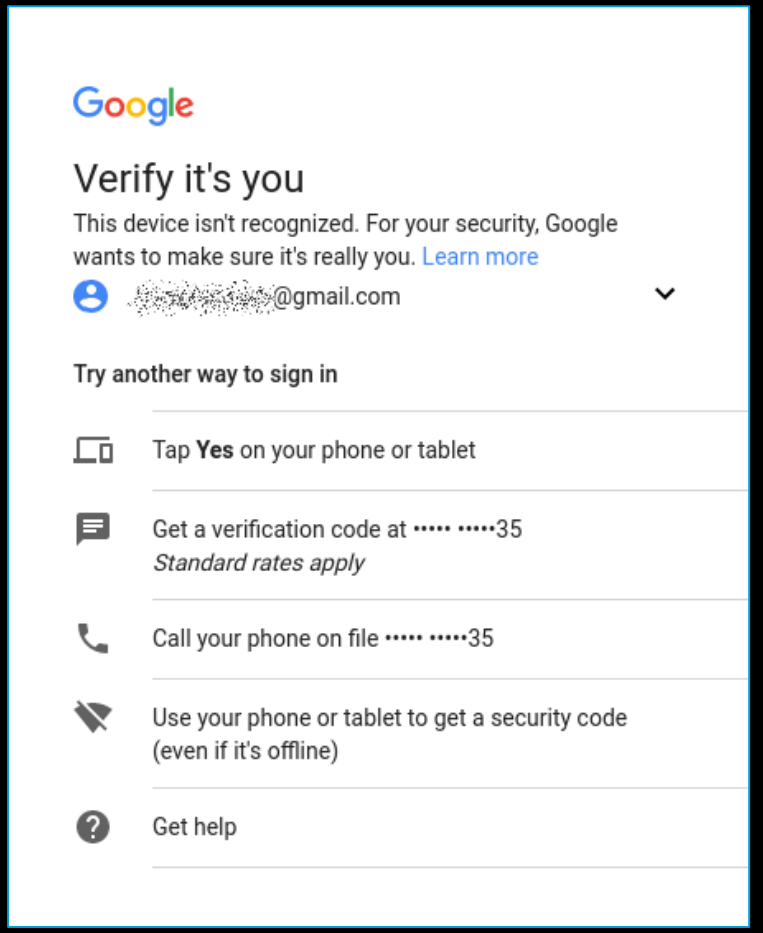
TOPS ‘22

## RQ1

"How do popular online services use RBA in practice, [...] and how do their user interfaces and requested additional authentication factors look like?"

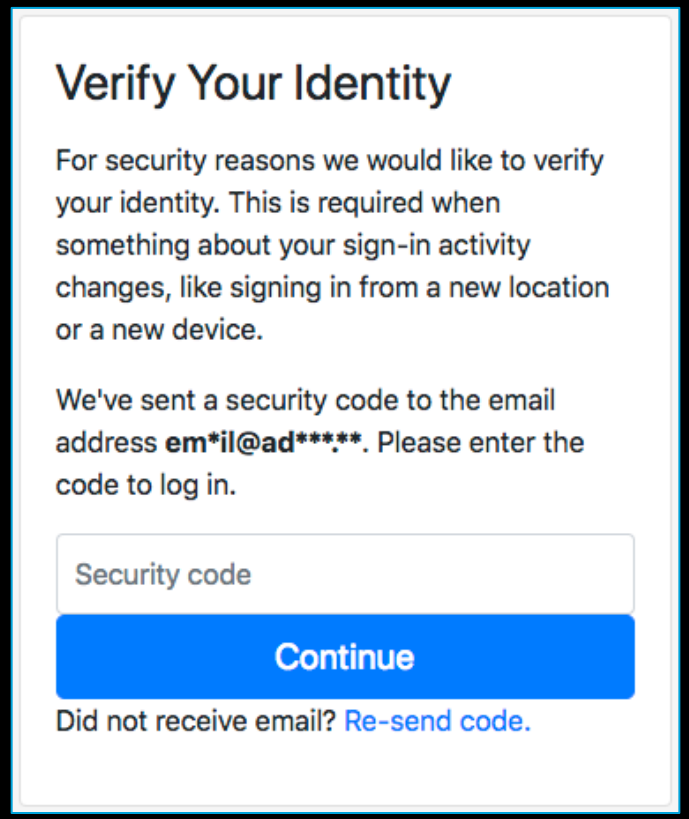

amazon
Verification needed
We will send you a code to verify your identity. This is required when something about your sign-in activity changes, like signing in from a new device or location.
Send verification code:
As a text message - +49*******8135
In an email - l**********0@gmail.com
Send code


facebook
1
2
Choose a Security Check
How do you want to confirm your identity? You can try each option multiple times.
Learn More
Text a security code to your phone
Identify photos of friends
Approve your login on another computer
Continue


Google
Verify it's you
This device isn't recognized. For your security, Google wants to make sure it's really you. Learn more
@gmail.com
Try another way to sign in
Tap Yes on your phone or tablet
Get a verification code at ••••• •••••35
Standard rates apply
Call your phone on file ••••• •••••35
Use your phone or tablet to get a security code (even if it's offline)
Get help

| Service | Requested authentication factors |
|---|---|
| Amazon | ▪ **Verification code (email*, text message)** |
| Facebook | ▪ Approve login on another computer<br>▪ Identify photos of friends<br>▪ Asking friends for help<br>▪ **Verification code** (text message) |
| GOG.com | ▪ **Verification code (email)*** |
| Google | ▪ Enter the city you usually sign in from<br>▪ **Verification code (email**, text message, app, phone call)<br>▪ Press confirmation button on second device |
| LinkedIn | ▪ **Verification code (email)*** |

# Combined State-Of-Practice RBA Dialog




Wiefling et al.: More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. In: ACSAC (2020). ACM

State of Practice

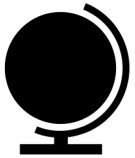
IFIP SEC ‘19

Usability

ACSAC ‘20
IFIP SEC ‘20
S&PM ‘21

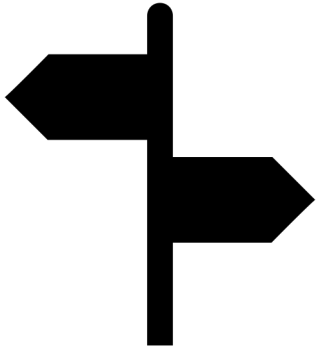
Security and Privacy

FC ‘21
IWPE ‘21



Large-Scale Online Service

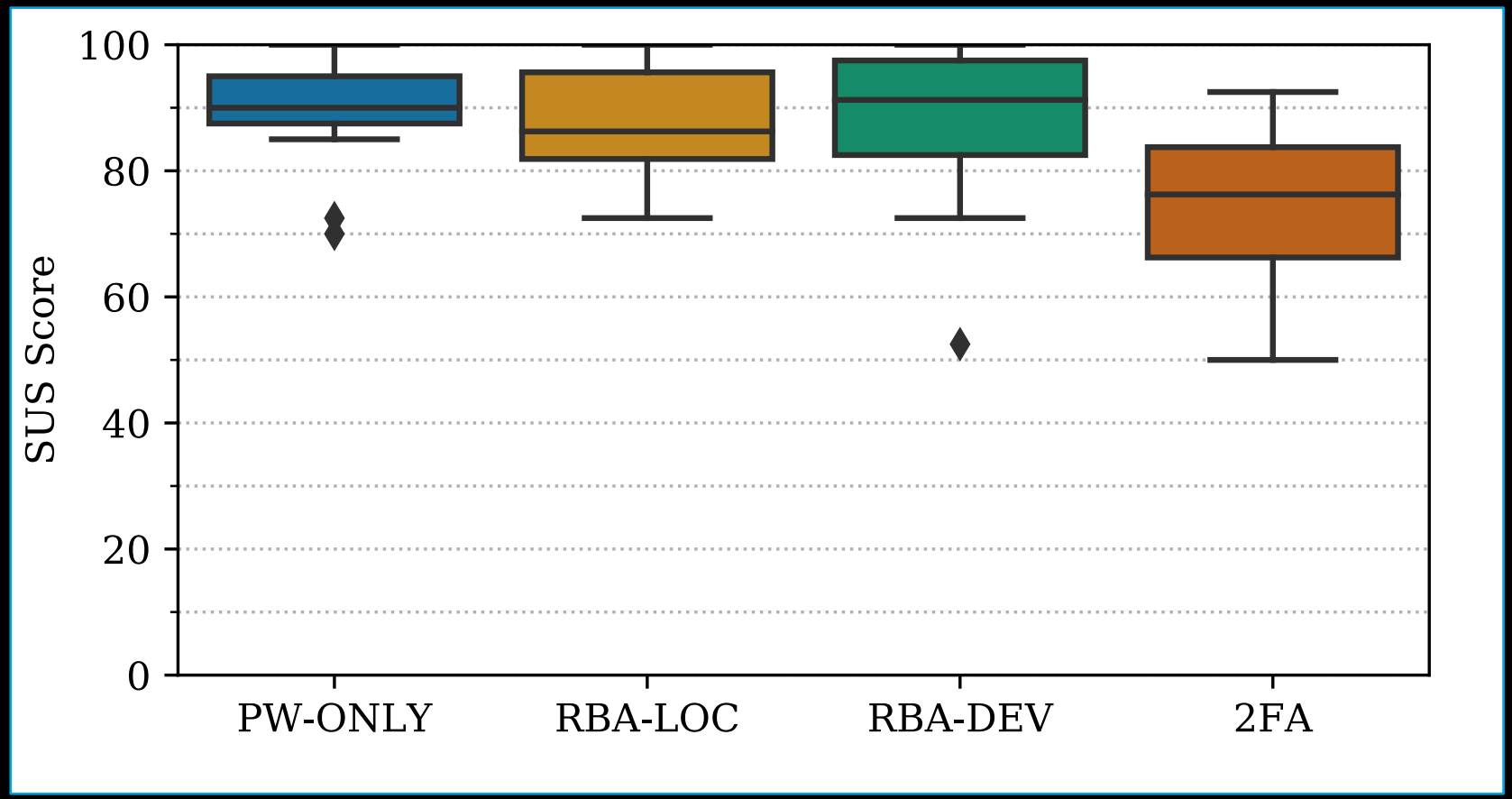
TOPS ‘22



## RQ2

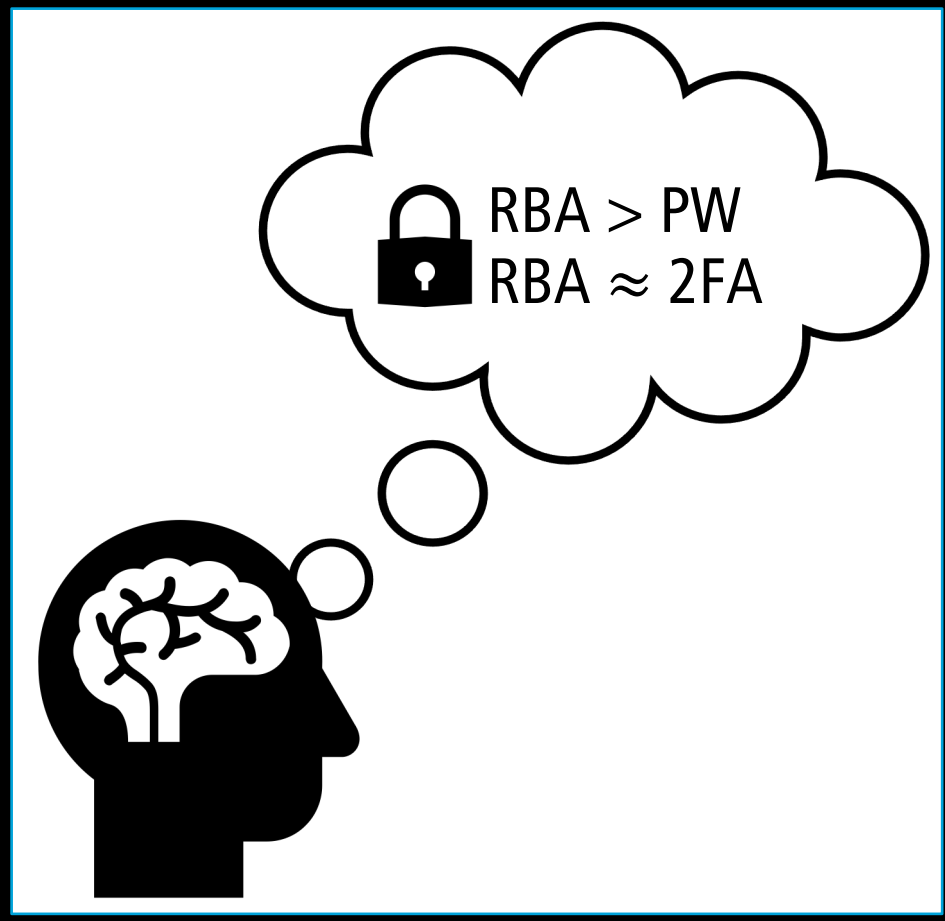
"How do users perceive RBA's usability and security compared to 2FA and password-only authentication [...]?"

# Users find RBA more usable than 2FA




Wiefling et al.: More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. In: ACSAC (2020). ACM

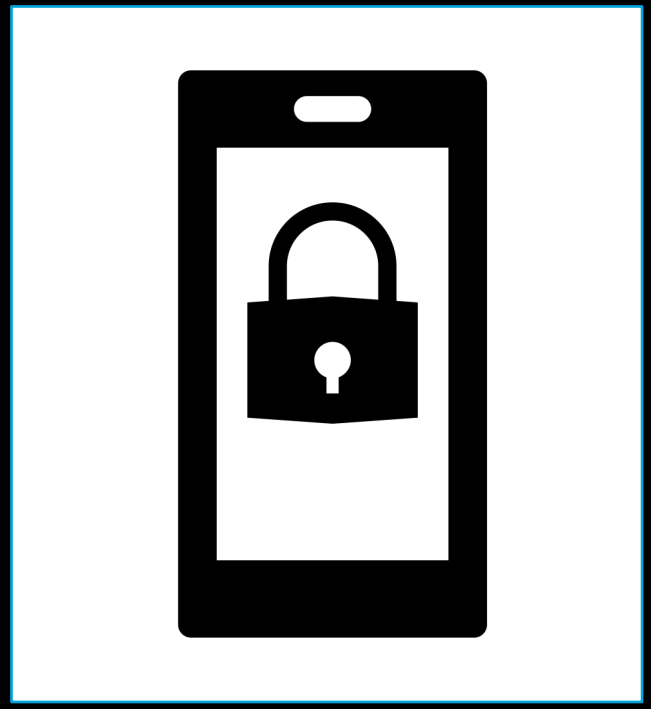
# Perceived Security of RBA comparable to 2FA




Wiefling et al.: More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. In: ACSAC (2020). ACM

# But: It depends on the use case

- RBA accepted for use cases involving sensitive data
  - e.g., online shopping, social media
- For online banking: 2FA preferable



Wiefling et al.: More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. In: ACSAC (2020). ACM

# But: It depends on the use case

- Re-authentication via email accepted in most use cases
- Phone number mostly not accepted
  - Exception: Online service involves sensitive financial data
    - E.g., online banking

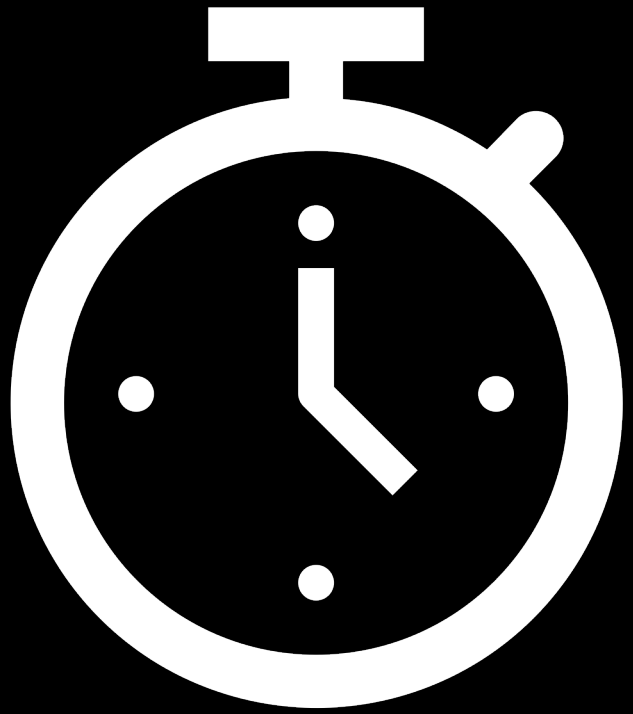
Wiefling et al.: More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. In: ACSAC (2020). ACM

## RQ3

"How can RBA's re-authentication state of practice [using email] be improved regarding usability [...]?"

# Show Verification Code in Email Subject Line and Body

- Speeds up authentication time
  - Compared to code in email body only (state of practice)
  - ~5 seconds faster on desktop devices



Wiefling et al.: Evaluation of Risk-based Re-Authentication Methods. In: IFIP SEC (2020). Springer

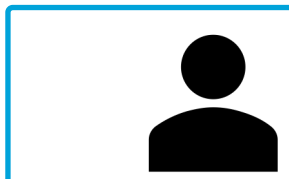
# Show Verification Code in Email Subject Line and Body

- Better user feelings while authenticating
  - Less nervous feelings reported (6%) than those having the code in the email body only (16%)
  - Also less anxious (7%) than those having to click link in the email to verify (15%)

Wiefling et al.: Evaluation of Risk-based Re-Authentication Methods. In: IFIP SEC (2020). Springer

State of Practice

IFIP SEC ‘19



Usability

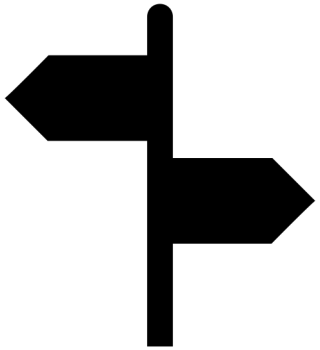
ACSAC ‘20
IFIP SEC ‘20
S&PM ‘21

Security and Privacy

FC ‘21
IWPE ‘21

Large-Scale Online Service

TOPS ‘22



## RQ4

"How [...] does RBA have to be configured to achieve high usability and security [in a practical deployment]?"

# Only Few Features Useful

- 8 Server-Originated
- 27 Client-Originated

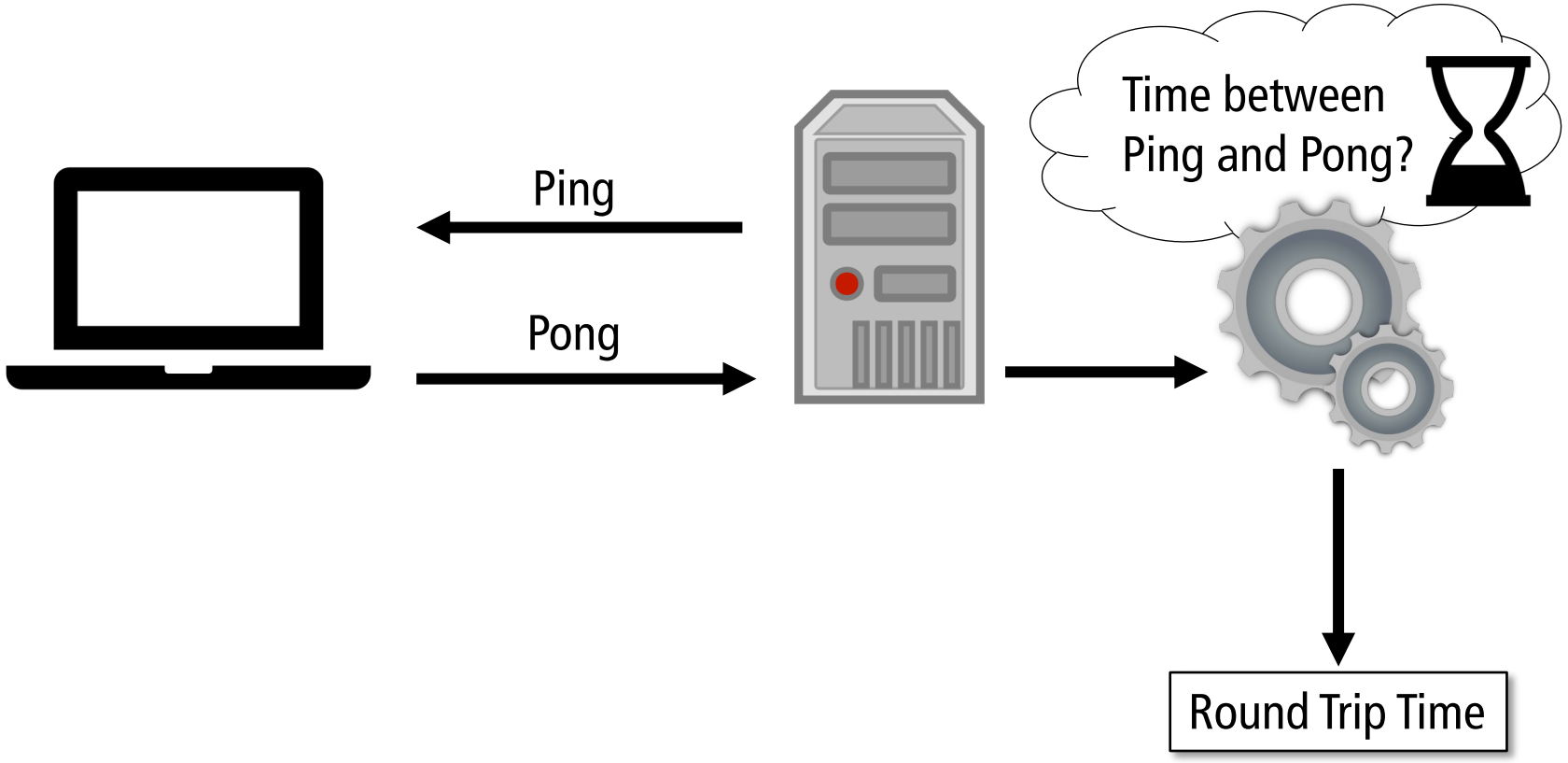
# Server-Originated

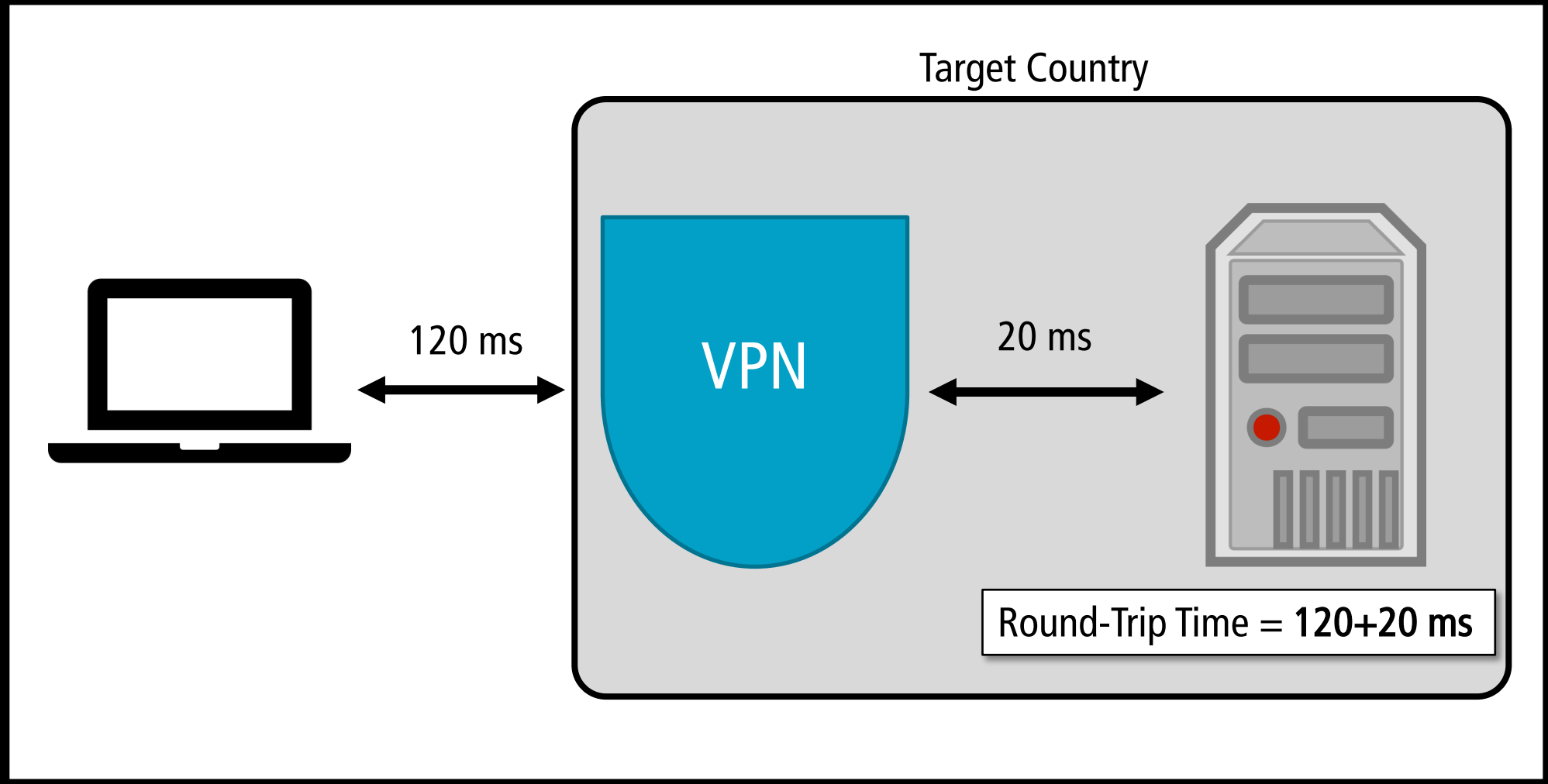
- IP Address
- Round-Trip Time (new)
- Autonomous System Number
- Weekday and Hour of Login

# Round-Trip Time

- Based on WebSockets

# WebSocket Connection



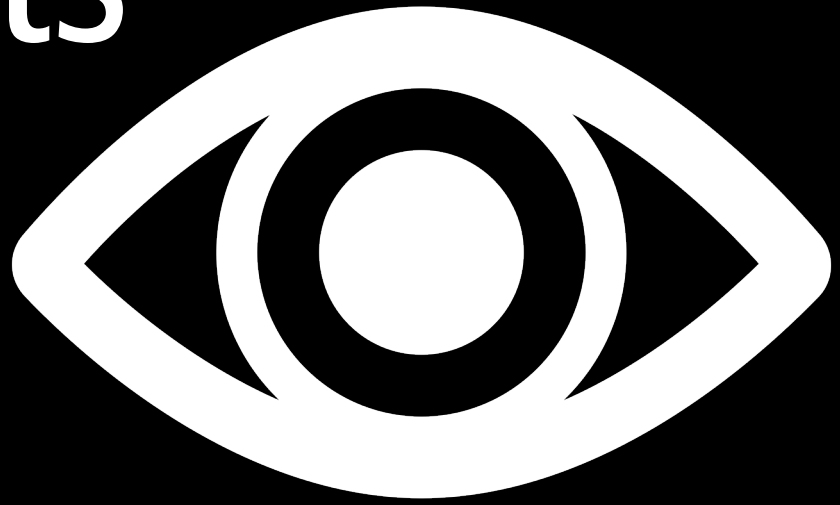

Target Country
120 ms
VPN
20 ms
Round-Trip Time = 120+20 ms

## RQ5

"What privacy challenges may arise with RBA use, and how can RBA systems be privacy enhanced while balancing security and usability in practice?"

# Privacy Threats

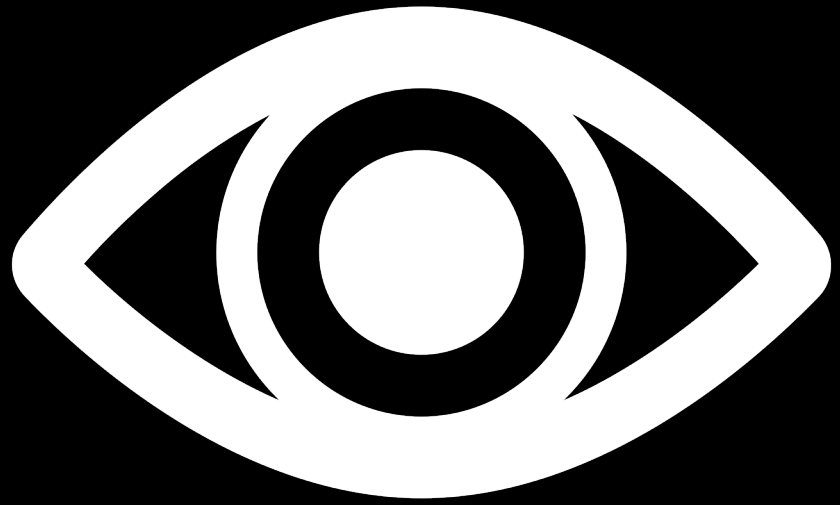
- Data Misuse
- Data Forwarding
- Data Breach



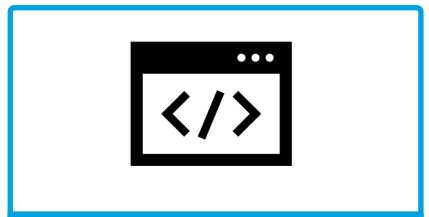
Wiefling et al.: Privacy Considerations for Risk-Based Authentication Systems. In: IWPE (2021). IEEE

# Privacy Enhancements

- Aggregating
- Hashing
- Truncation
- k-Anonymity
- Login History Minimization



Wiefling et al.: Privacy Considerations for Risk-Based Authentication Systems. In: IWPE (2021). IEEE



State of Practice

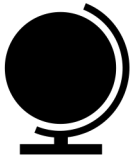
IFIP SEC ‘19

Usability

ACSAC ‘20
IFIP SEC ‘20
S&PM ‘21

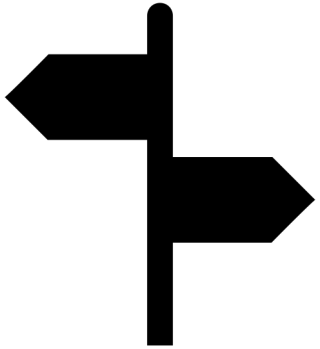
Security and Privacy

FC ‘21
IWPE ‘21



Large-Scale Online Service

TOPS ‘22



## RQ6

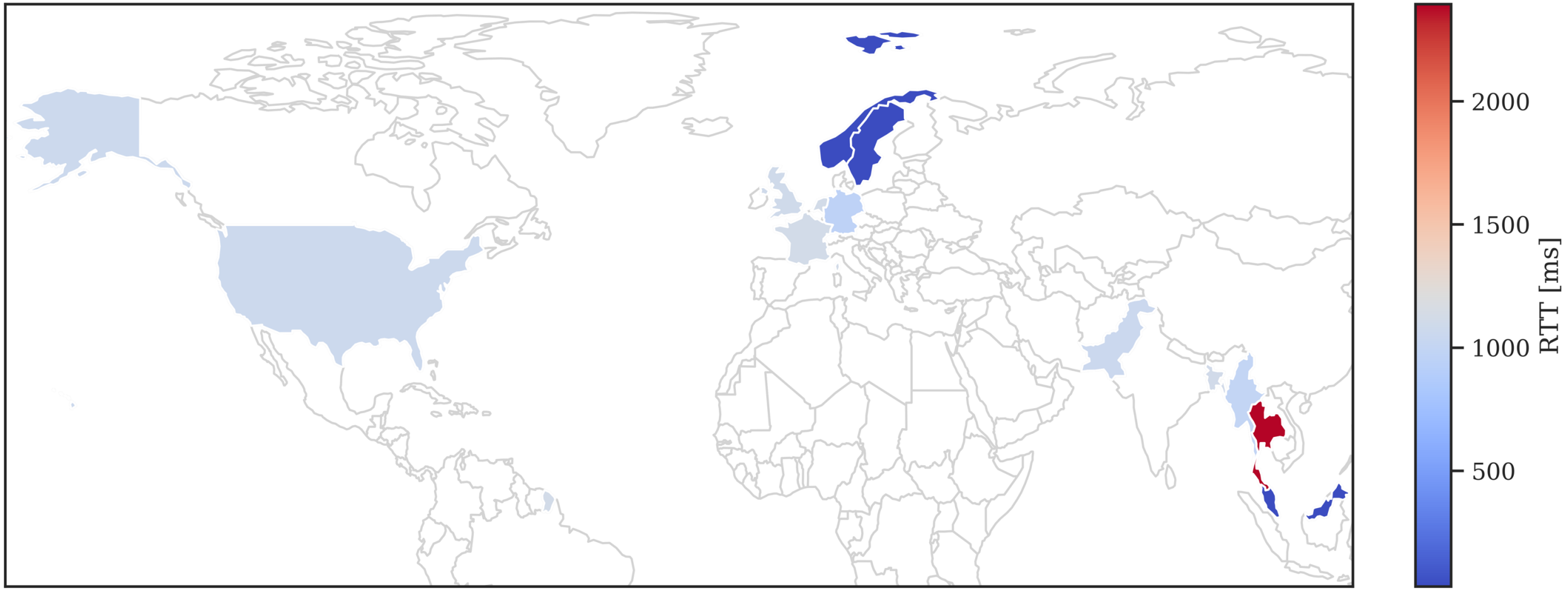
"How are RBA characteristics on a large-scale online service and how can RBA [...] be optimized to achieve high usability, security, and privacy?"

# Low Re-Authentication Rates in Practice

- Even when blocking >99% of targeted attackers

Wiefling et al.: Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service. In: TOPS (2022) ACM

# Round-Trip Time can Distinguish Countries, Regions, and Users



# Main Contributions

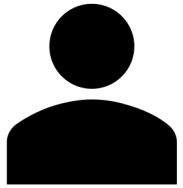
- Thesis substantially increased body of knowledge

- Uncovered RBA's state of practice

- Deep insights and advances in RBA's usability, security, and privacy

- Major improvements for RBA systems in practice

# Key Findings



- Users prefer RBA to 2FA*
- Perceived security comparable to 2FA

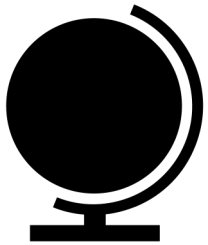
- RBA# rarely asks legitimate users for re-authentication, even when blocking >99% of targeted attackers

- Privacy-enhanced RBA is possible
- Only few features useful for risk estimation

*In use cases with sensitive data involved

# Using the Freeman et al. (2016) model

# Impact



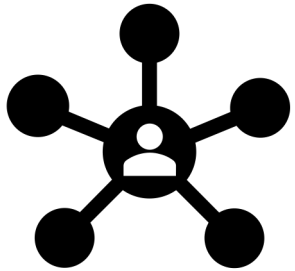
- Fostered RBA adoption worldwide
  - Roll-out Telenor (>185M users)
  - Open data, open source solution, Okta, MIT, TU Eindhoven

- Improved real-world RBA solutions
  - Responsible disclosure (>3B Facebook users)
  - RTT feature

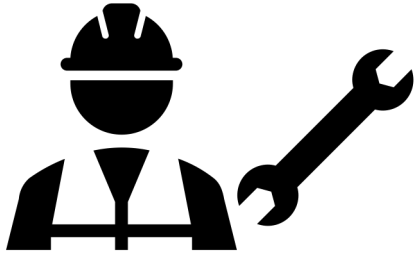
- Increased awareness
  - riskbasedauthentication.org (Google #1 when searching RBA)
  - Bruce Schneier, >125 citations (e.g., USENIX Security, CCS)

# Future Research Directions

- State of RBA today



- Influence of anti-tracking measures



- Usability for administrators