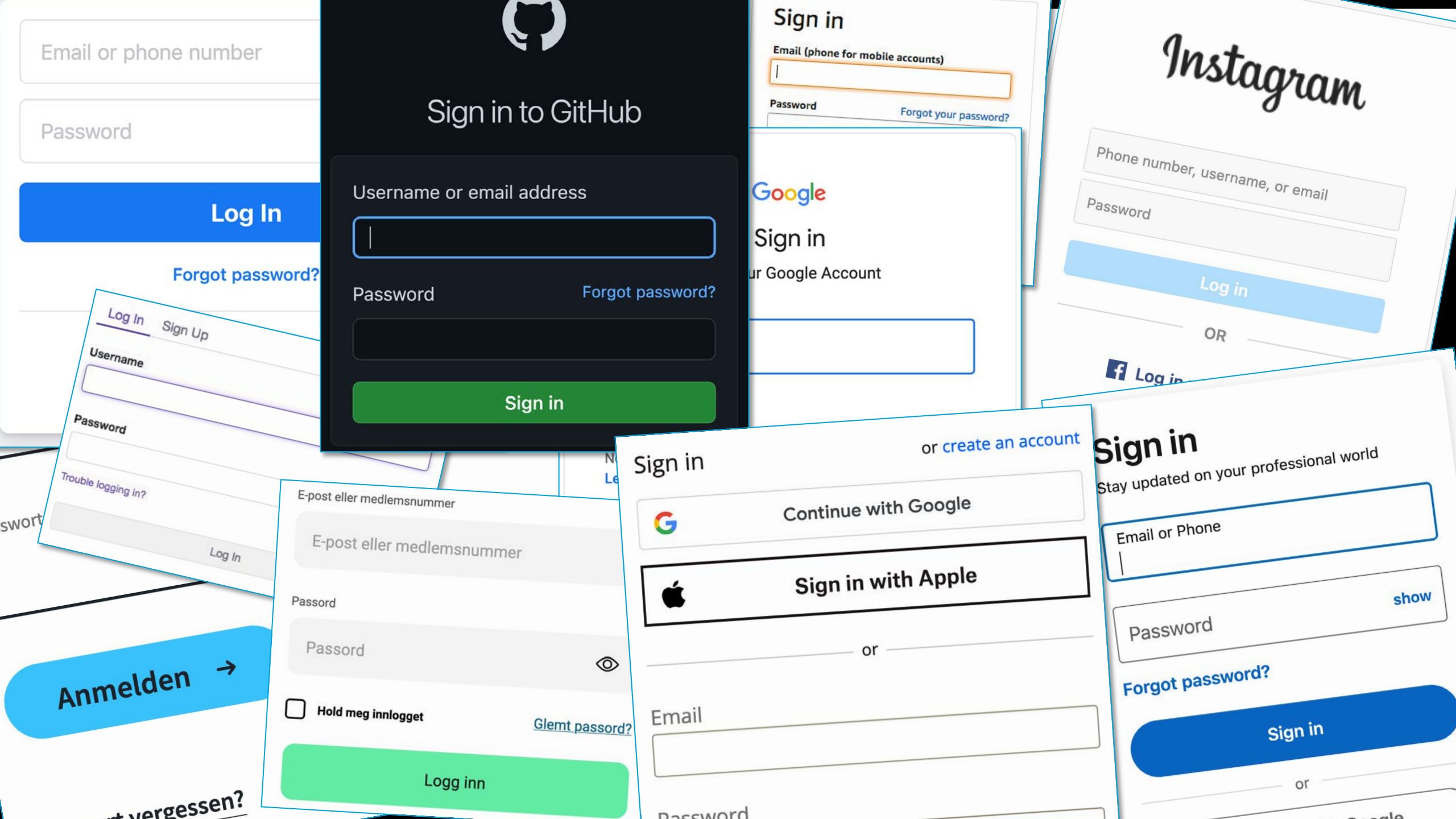
Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

Stephan Wiefling

Evaluating Risk-Based Authentication on a Large-Scale Online Service

PasswordsCon 2023
Bergen, Norway


Email or phone number
Password
Log In
Forgot password?
Sign in to GitHub
Username or email address
Password
Forgot password?
Sign in
Sign in
Email (phone for mobile accounts)
Password
Forgot your password?
Google
Sign in
ur Google Account
Instagram
Phone number, username, or email
Password
Log in
OR
Log In
Sign Up
Username
Password
Trouble logging in?
Log In
E-post eller medlemsnummer
E-post eller medlemsnummer
Passord
Passord
Hold meg innlogget
Glemt passord?
Logg inn
Anmelden
Sign in
or create an account
Continue with Google
Sign in with Apple
or
Email
Password
Sign in
Stay updated on your professional world
Email or Phone
Password
show
Forgot password?
Sign in
or

>50% Password Re-Use*

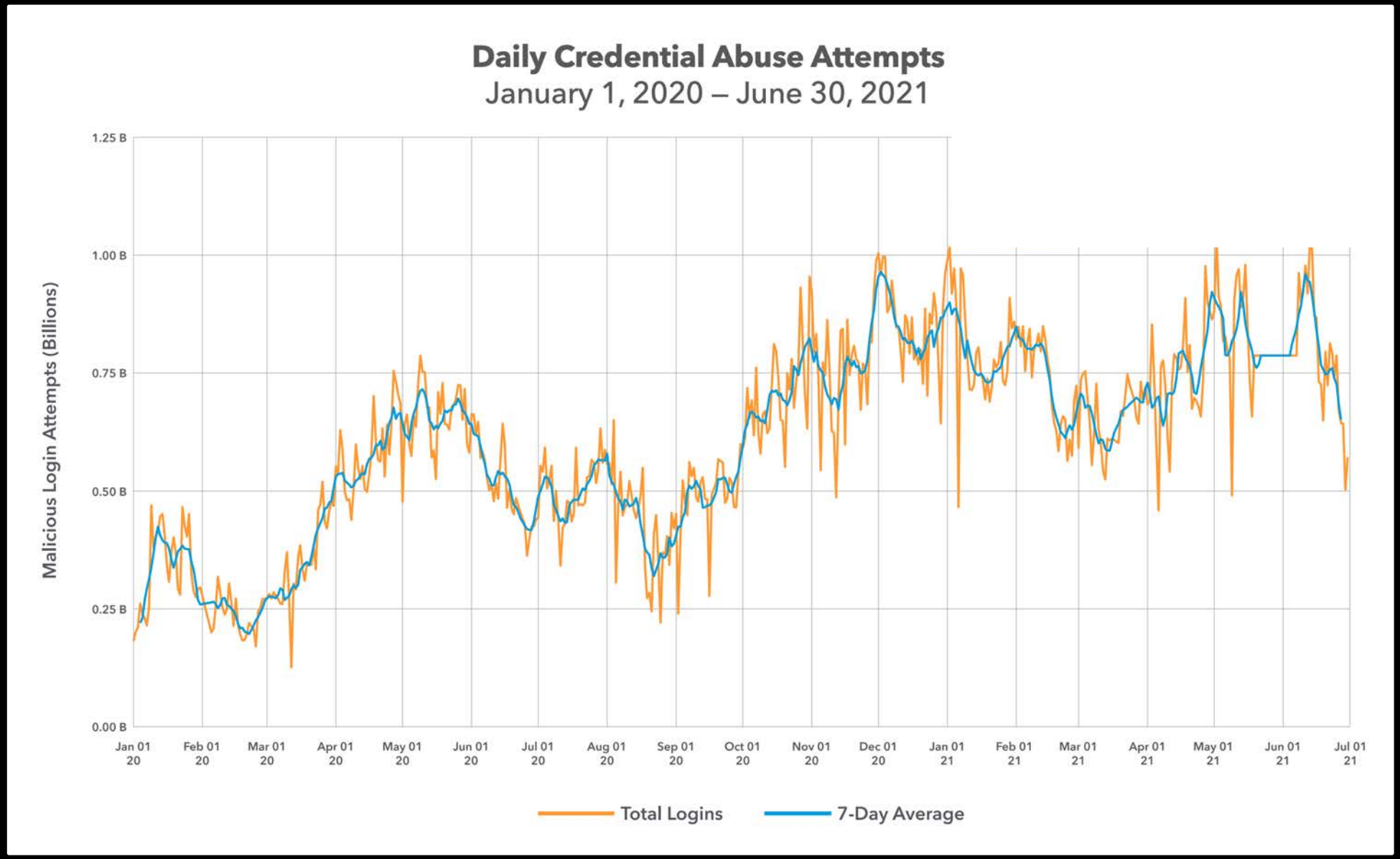
*Representative survey conducted by Bilendi & respondi in February 2022; n=1000 German Internet users >18 years old
Also:
Das et al.: The Tangled Web of Password Reuse. In: NDSS (2014)
Pearman et al.: Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat. In: CCS (2017)

Credential Stuffing

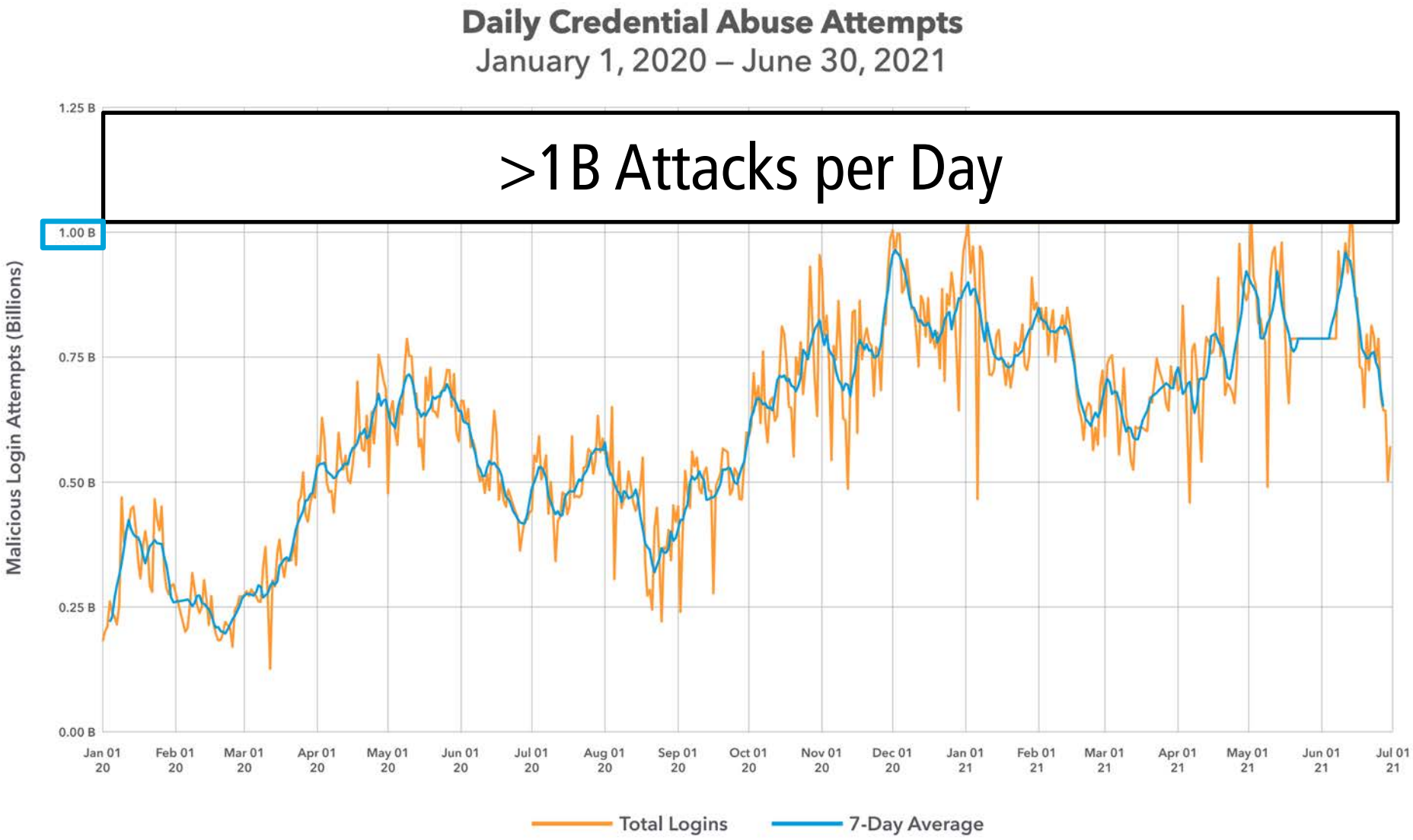
Daily Credential Abuse Attempts

January 1, 2020 – June 30, 2021

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



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



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

Phishing

2022 CRIME TYPES

By Victim Count			
Crime Type	*Victims*	*Crime Type*	*Victims*
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		

Federal Bureau of Investigation: Internet Crime Report 2022 (2023)


2FA

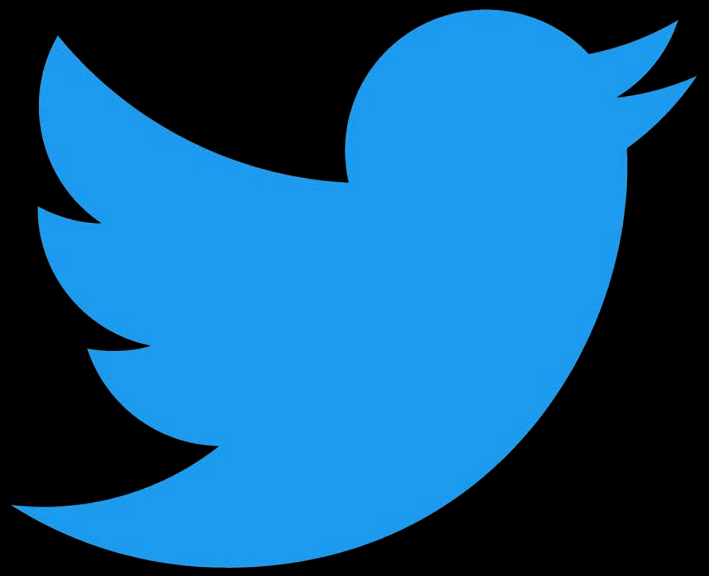
Low 2FA Adoption in Practice

<10%*

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

~4%*

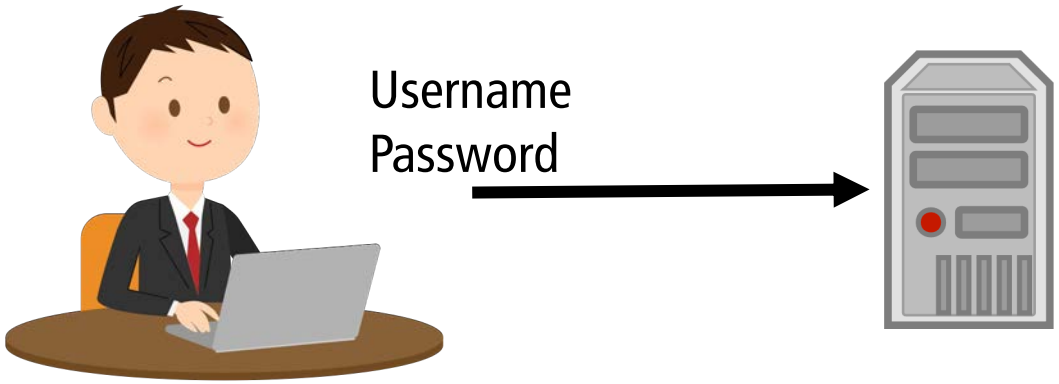
*In December 2021
Newman, L. H.: Facebook Will Force More At-Risk Accounts to Use Two-Factor. In: Wired (Dec 2021)

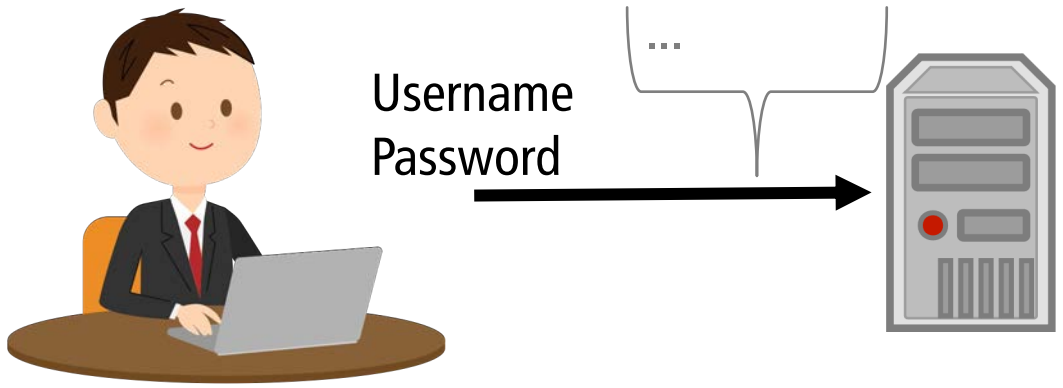


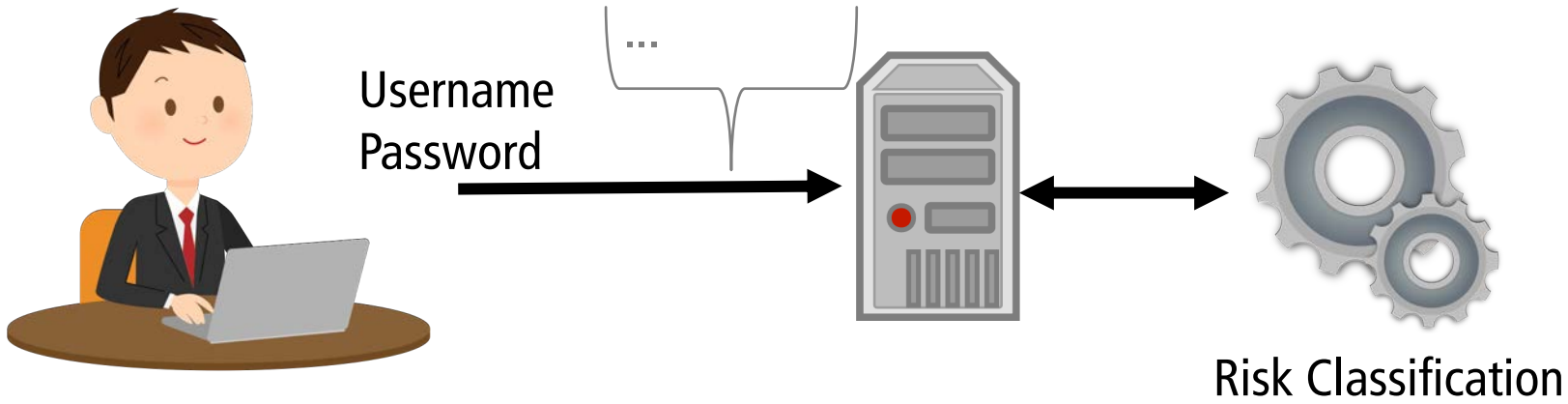
2.6%*

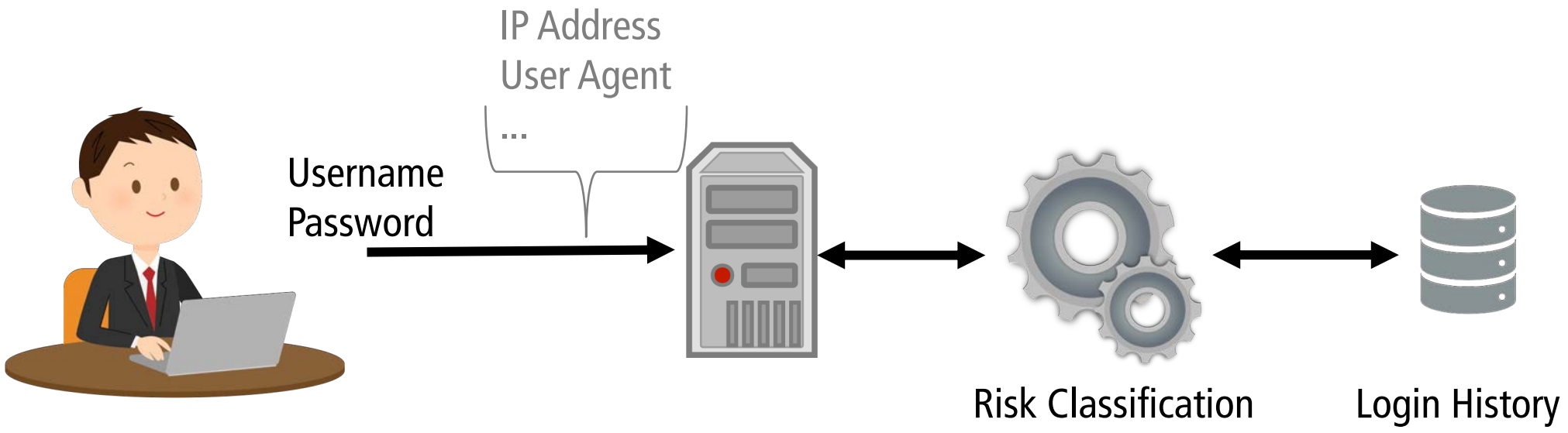
*In December 2021
Twitter: Account Security. In: Twitter Transparency Center (Jul 2022)

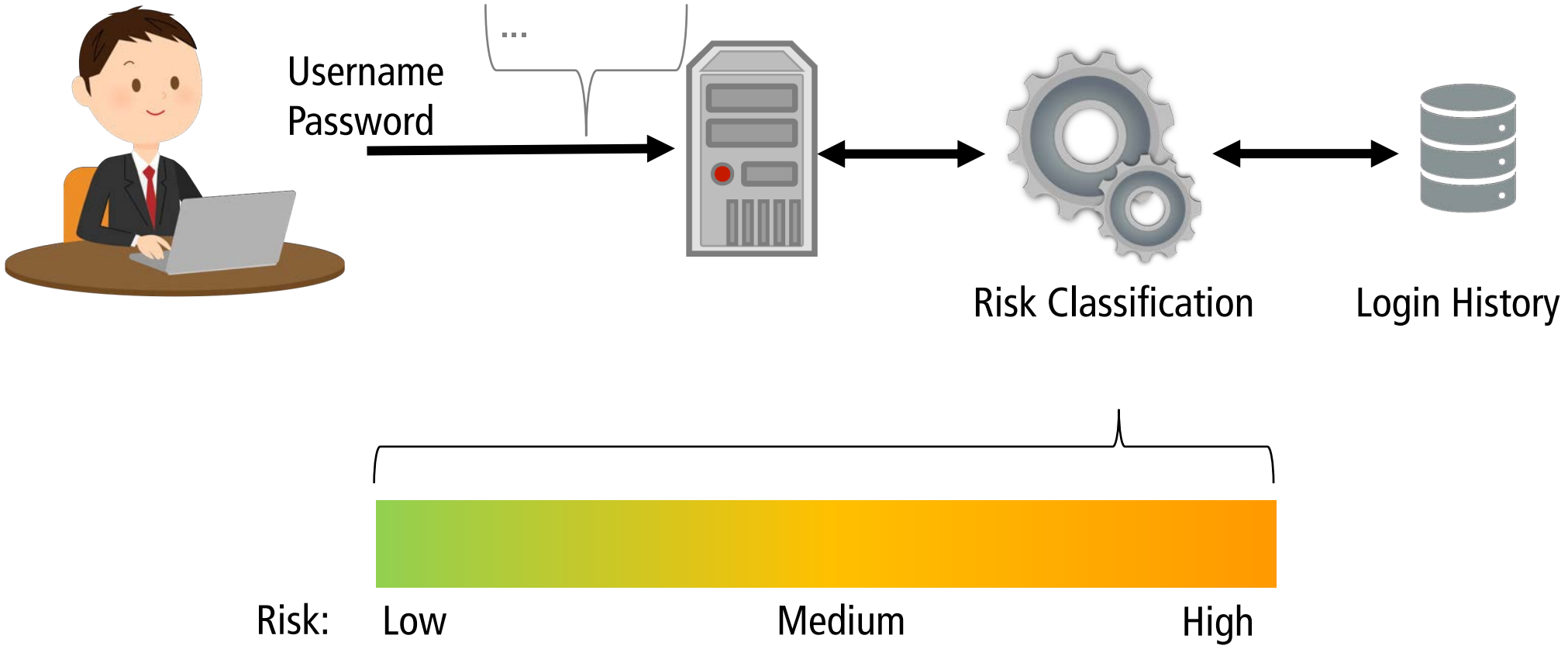
Risk-Based Authentication (RBA)

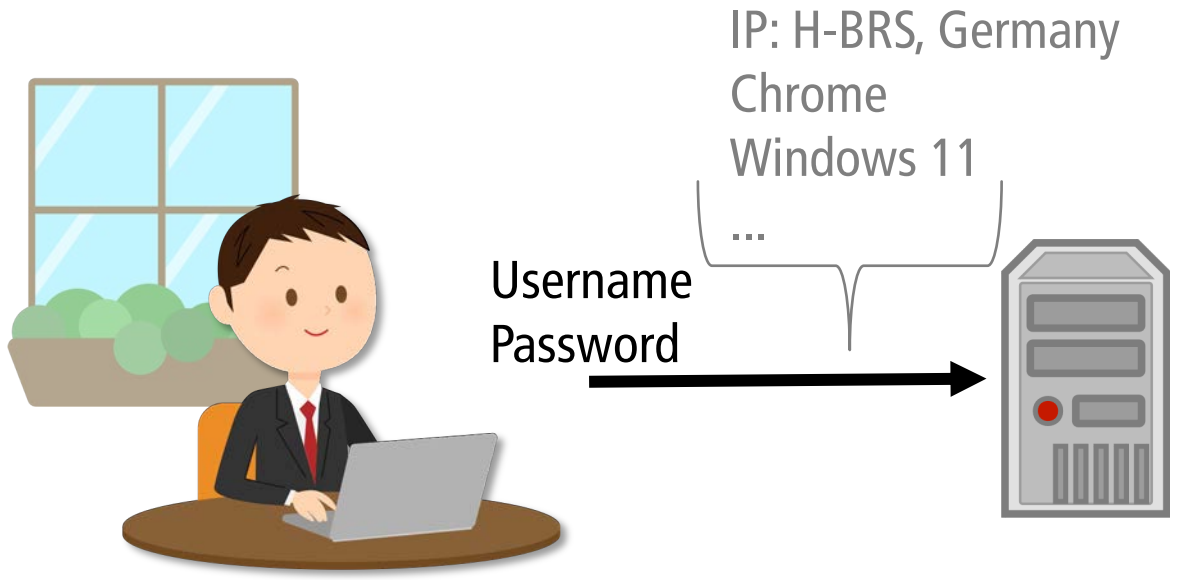

Username
Password

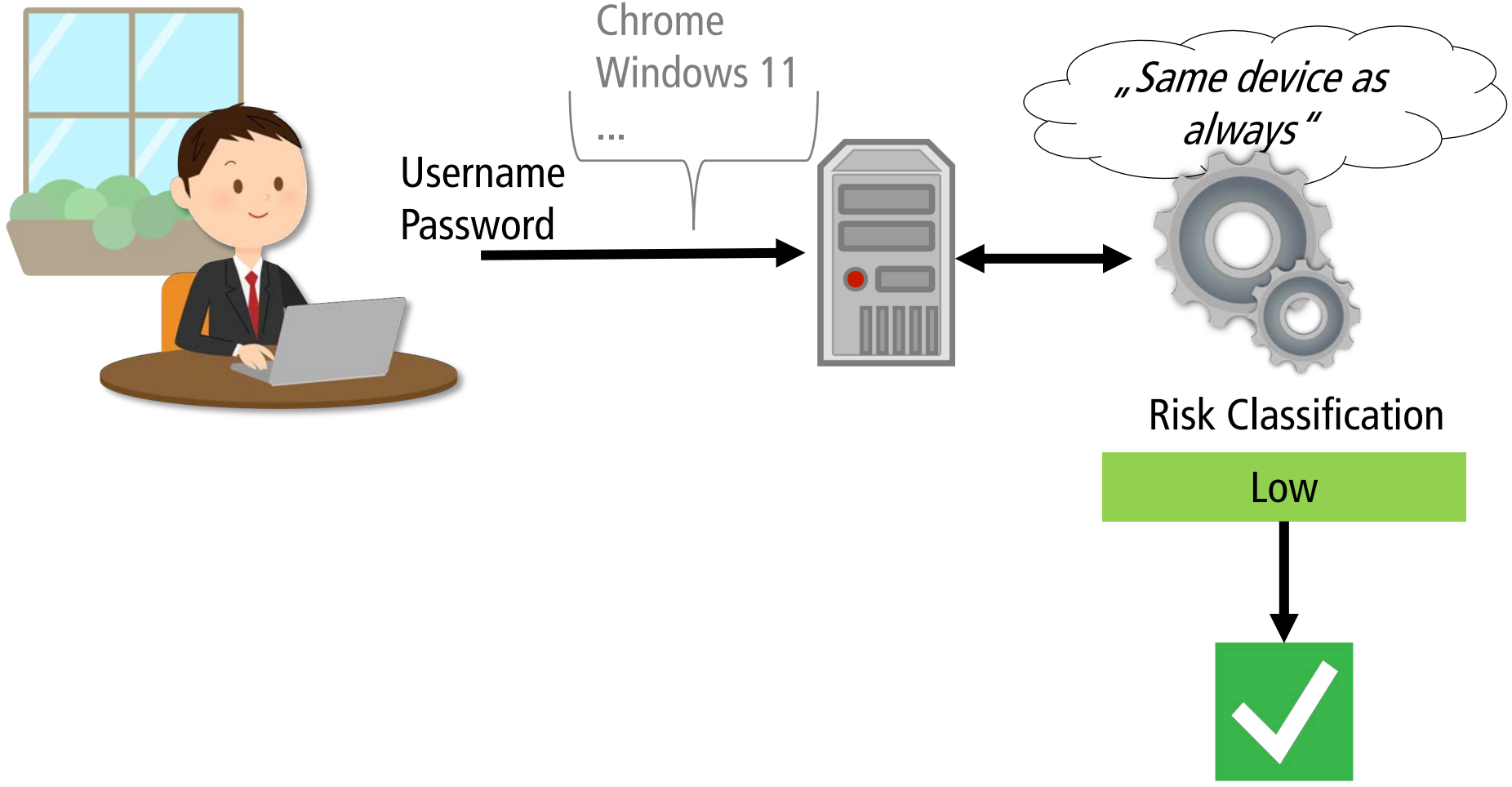

IP Address
User Agent
...
Username
Password

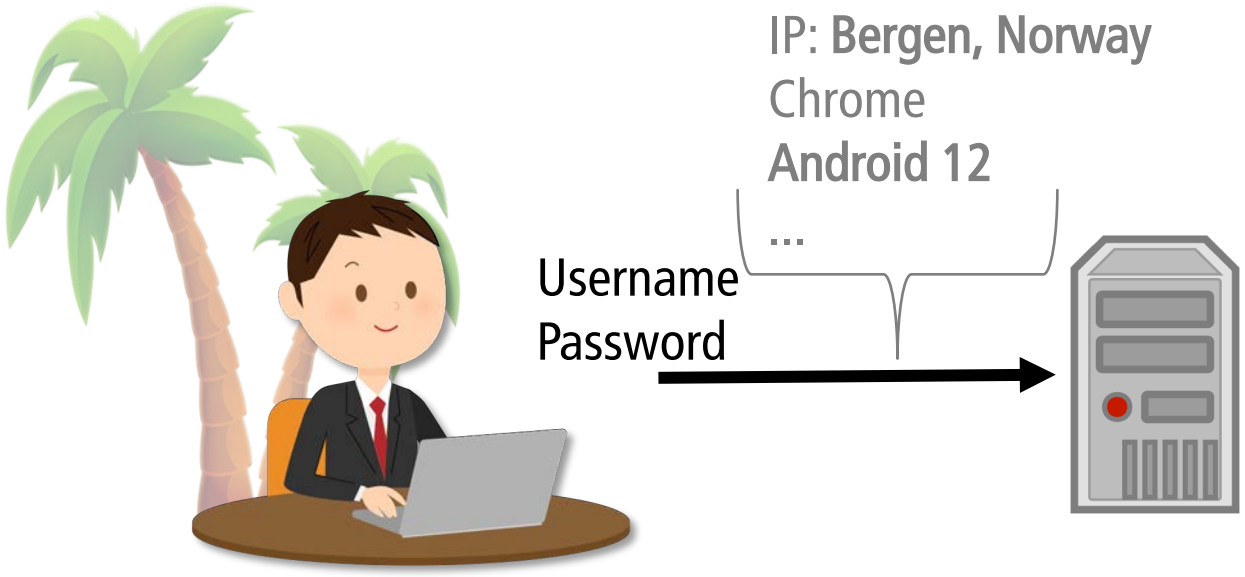

IP Address
User Agent
...
Username
Password
Risk Classification


IP Address
User Agent
...
Username
Password
Risk Classification
Login History


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

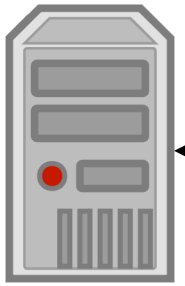

IP: H-BRS, Germany
Chrome
Windows 11
...
Username
Password

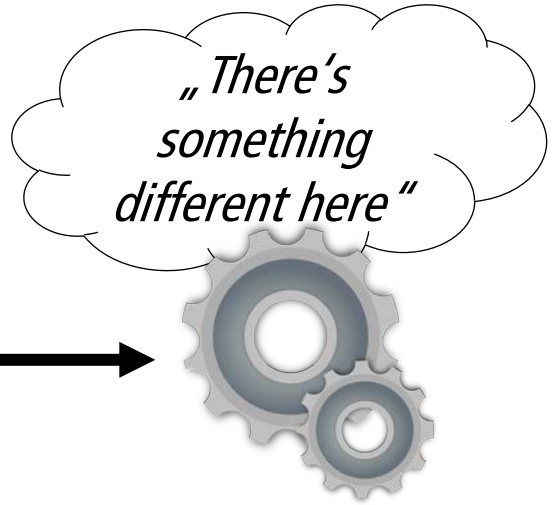

IP: H-BRS, Germany
Chrome
Windows 11
...
Username
Password
„Same device as always“
Risk Classification
Low


IP: Bergen, Norway
Chrome
Android 12
...
Username
Password

IP: **Bergen, Norway**
Chrome
Android 12
...

Username
Password





Risk Classification

Medium

Additional
Authentication

Verify Your Identity

For security reasons we would like to verify your identity. This is required when something about your sign-in activity changes, like signing in from a new location or a new device.

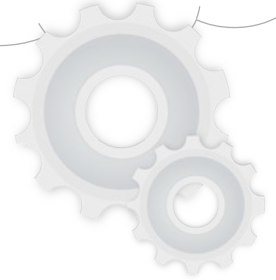
We've sent a security code to the email address **em*il@ad***.**. Please enter the code to log in.

Security code

Continue

Did not receive email? Re-send code.

„There's something different here"

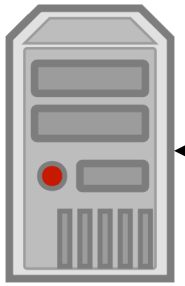


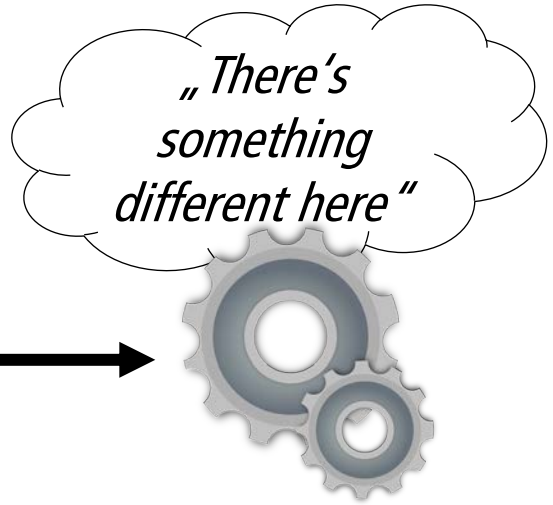
Risk Classification

Medium

IP: **Bergen, Norway**
Chrome
Android 12
...

Username
Password





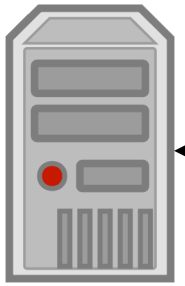
Risk Classification

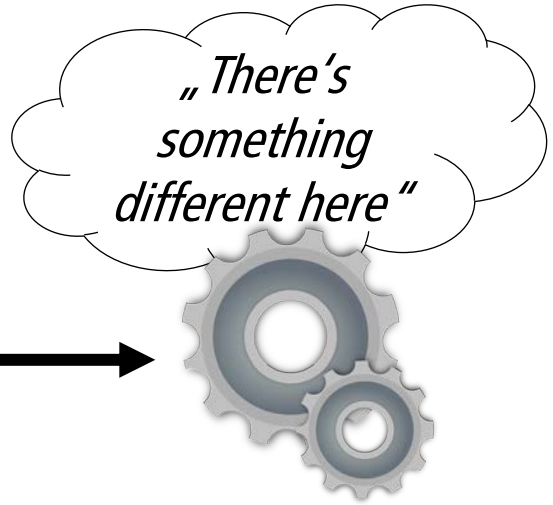
Medium

Additional
Authentication

IP: **Bergen, Norway**
Chrome
Android 12
...

Username
Password





Risk Classification

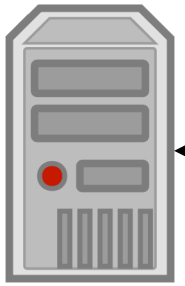
Medium

Additional Authentication

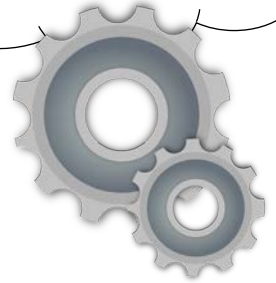
Proof for Additional Authentication

IP: **Bergen, Norway**
Chrome
Android 12
...

Username
Password



„There's something different here"



Risk Classification

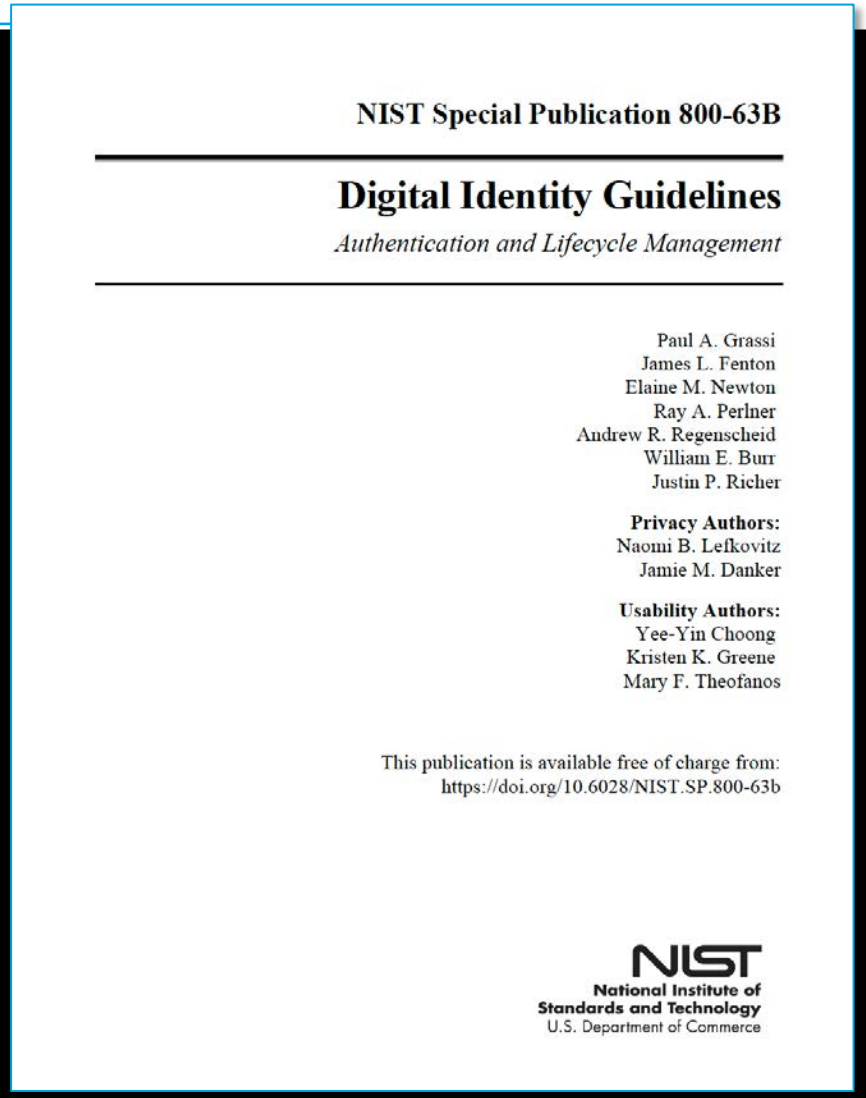
Medium

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

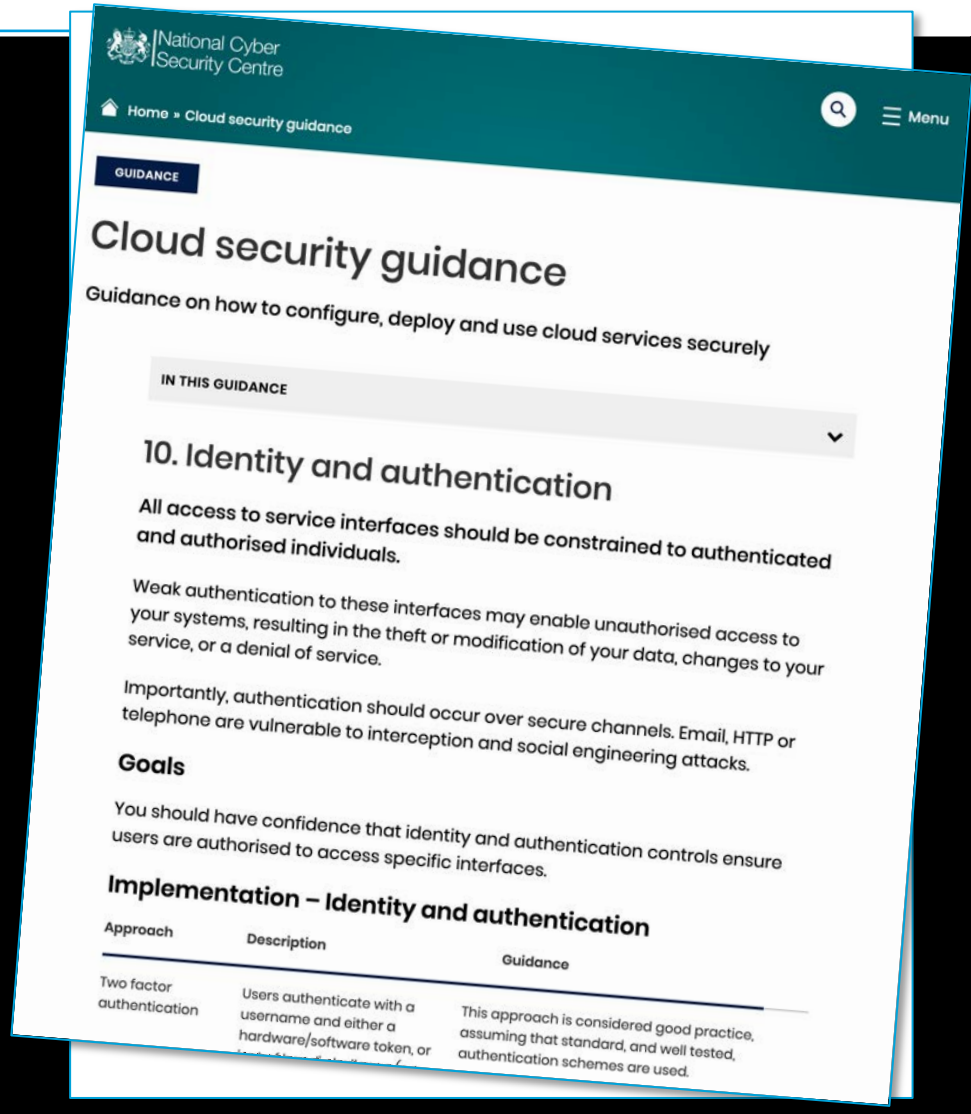
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63b

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.

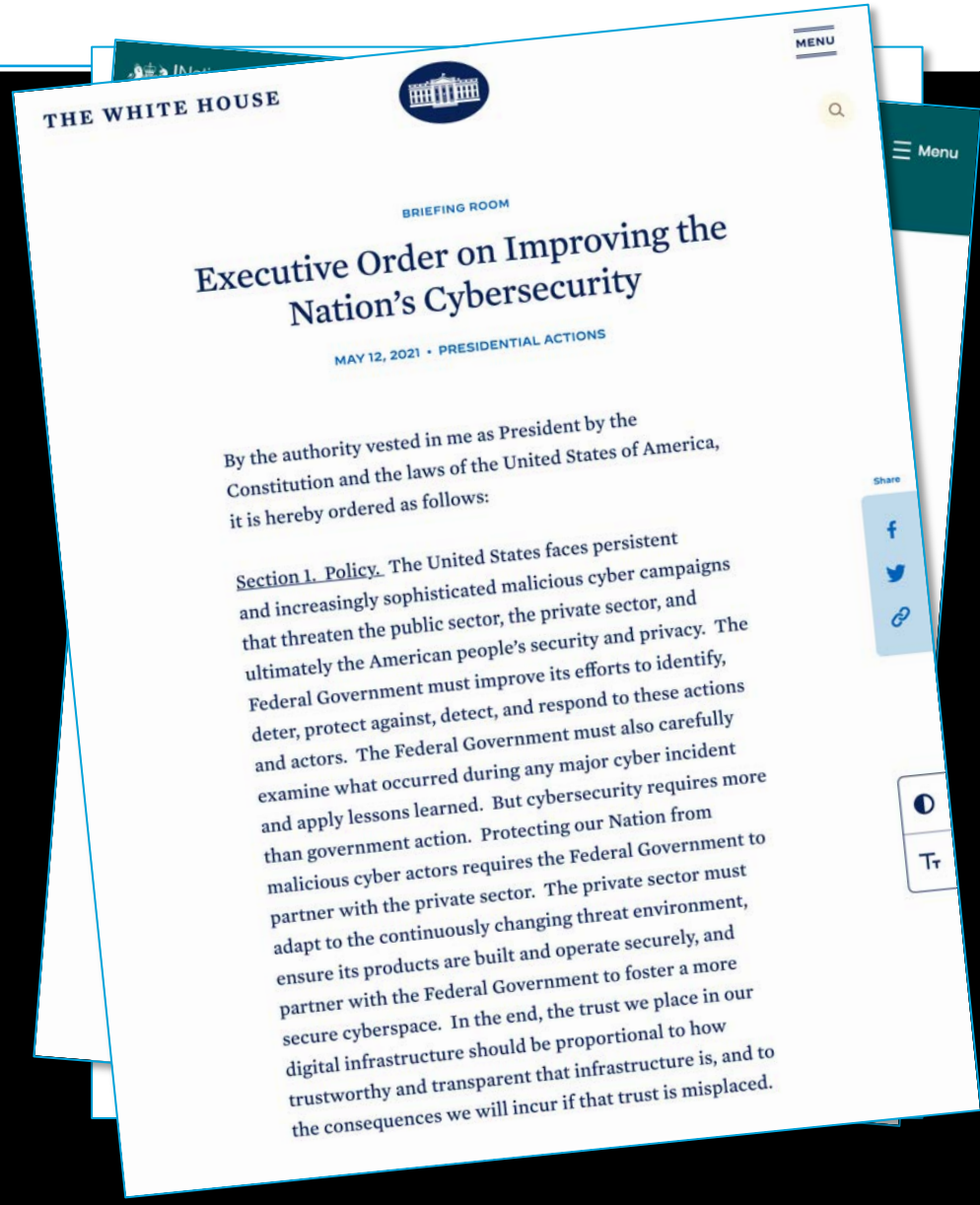
Implementation – Identity and authentication

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]



THE WHITE HOUSE

MENU

Menu

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

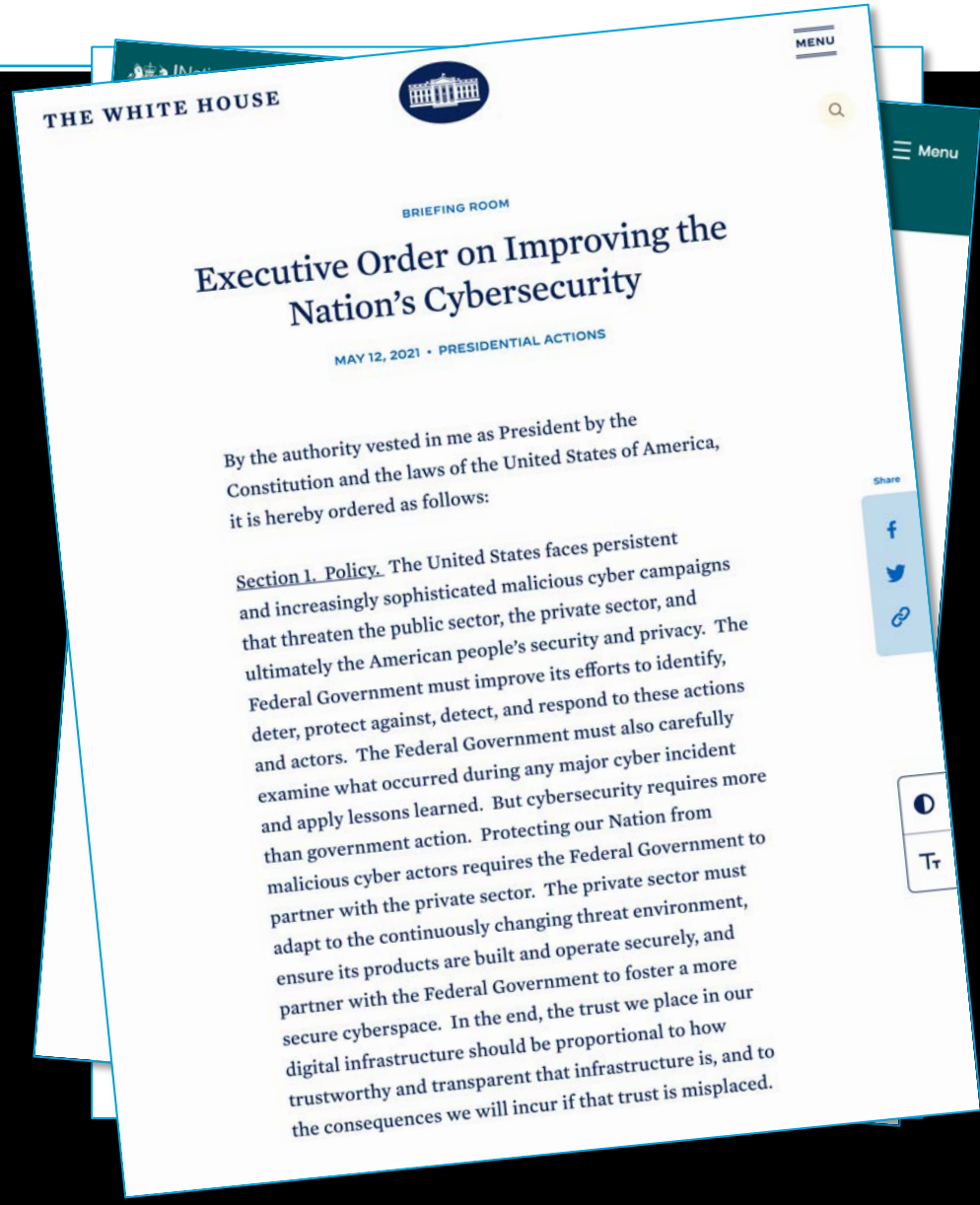
Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Share

[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)

Risk-Based Authentication

- Recommended by NIST[1], NCSC[2] and others
- Required in the US by Presidential Order[3]
- More usable than comparable 2FA methods[4]



THE WHITE HOUSE

MENU

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

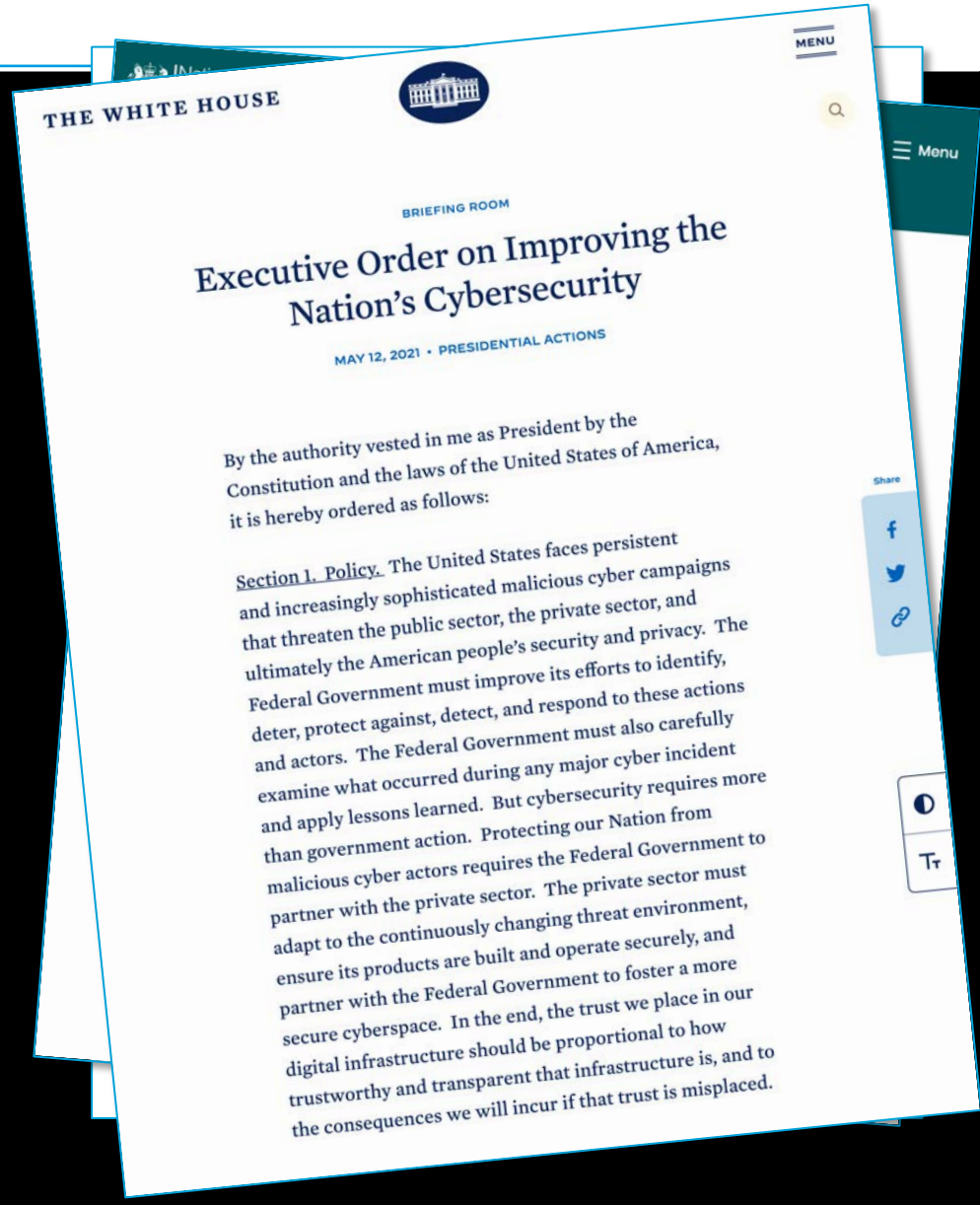
By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

[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)
[4] Wiefling et al.: More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. In: ACSAC '20. ACM (2020)

Risk-Based Authentication

- Recommended by NIST[1], NCSC[2] and others
- Required in the US by Presidential Order[3]
- More usable than comparable 2FA methods[4]
- But: Limited research on large online services



THE WHITE HOUSE

MENU

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

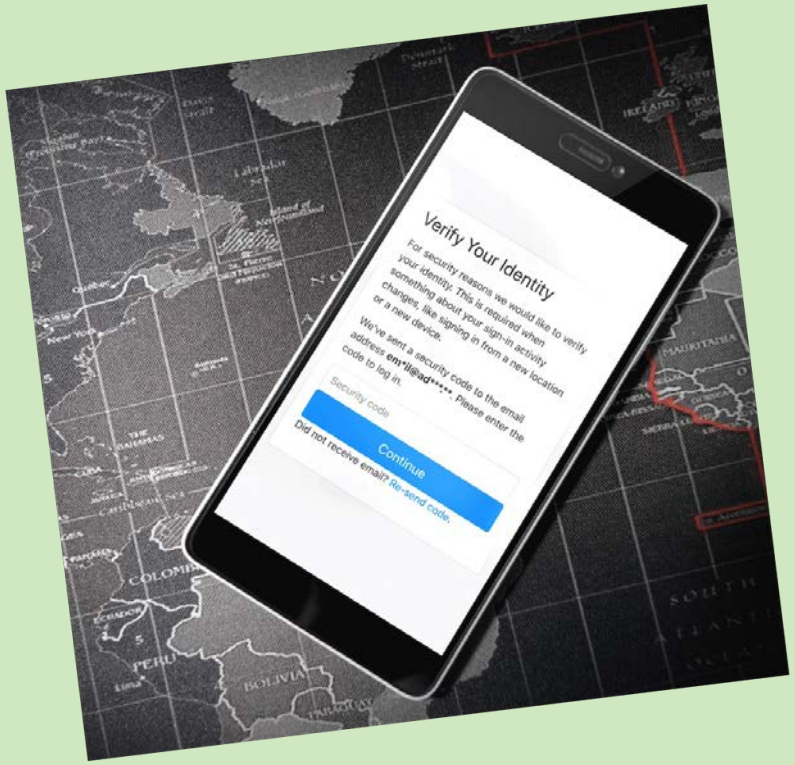
MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

[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)
[4] Wiefling et al.: More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. In: ACSAC '20. ACM (2020)

Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences



Pump Up Password Security!

Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service

Stephan Wiefling, Paul René Jørgensen*, Sigurd Thunem*, Luigi Lo Iacono

H-BRS University of Applied Sciences, Germany

Telenor Digital, Norway (*)

Published in ACM TOPS ‘23

Overview

Study

Results

Open Source

Overview

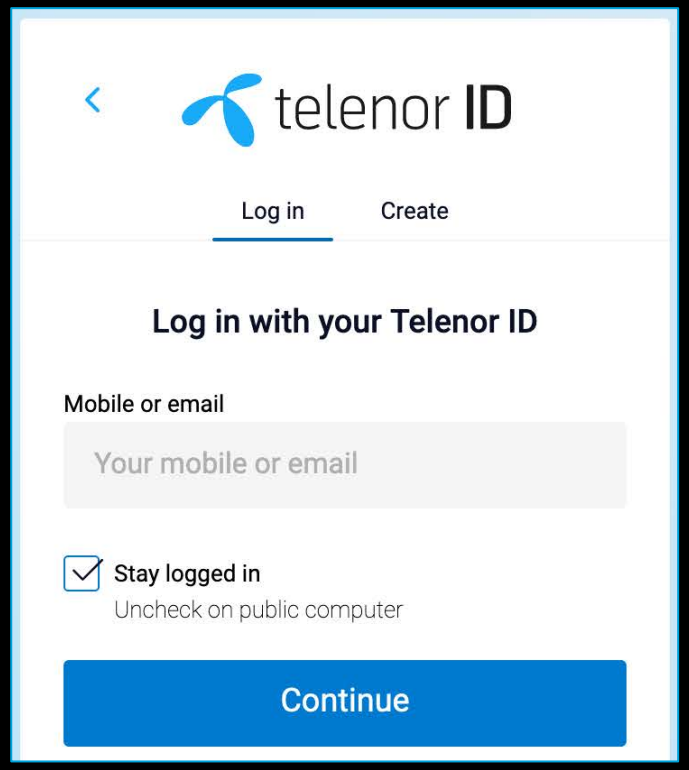
Study

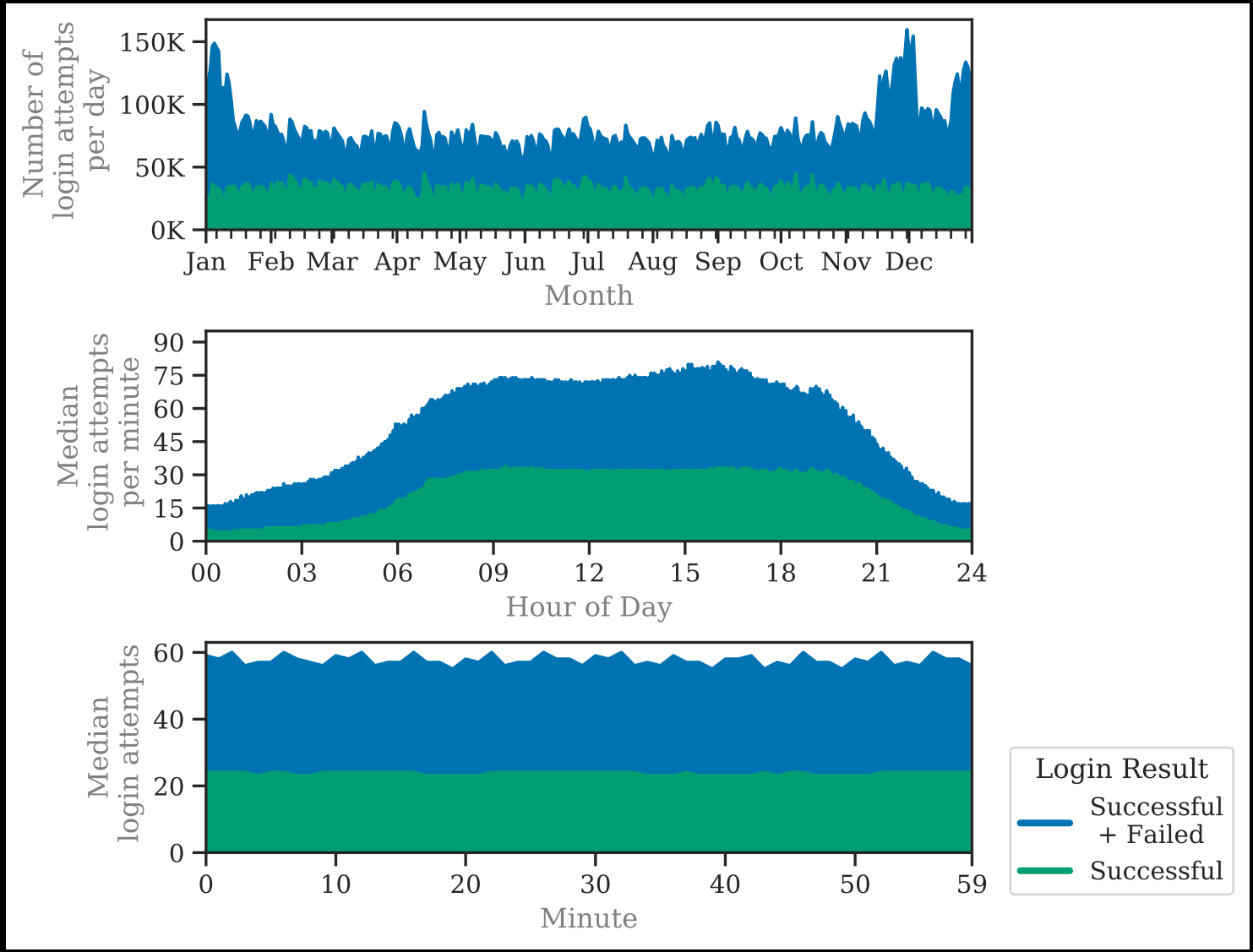
Results

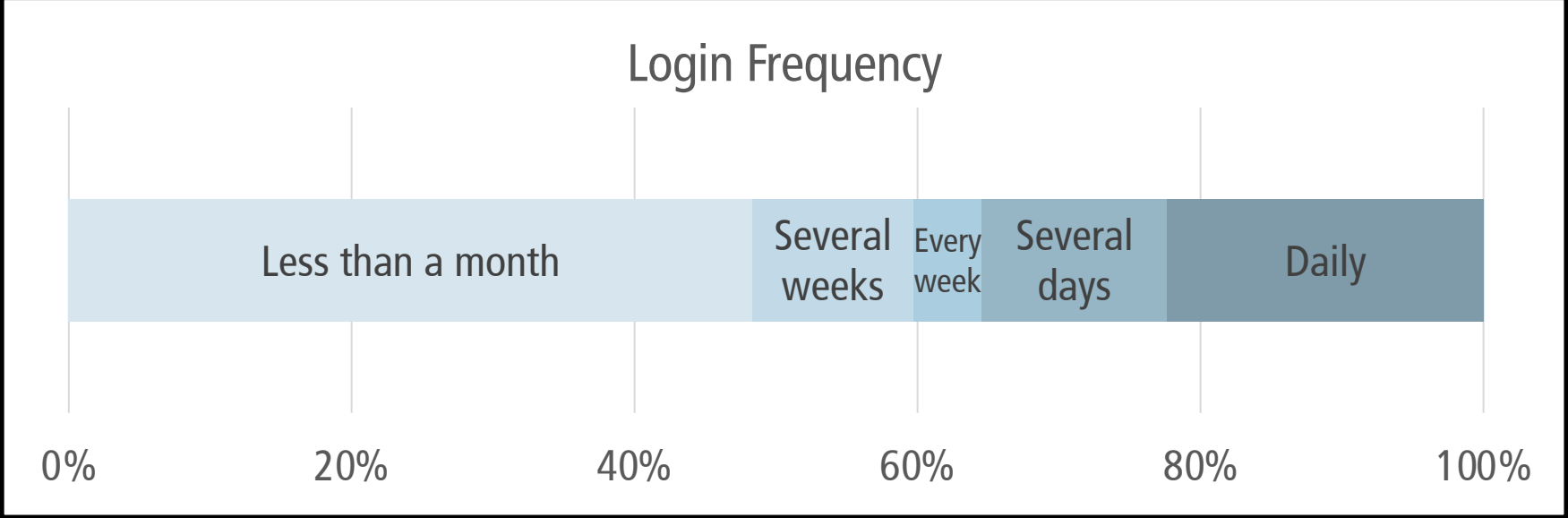
Open Source

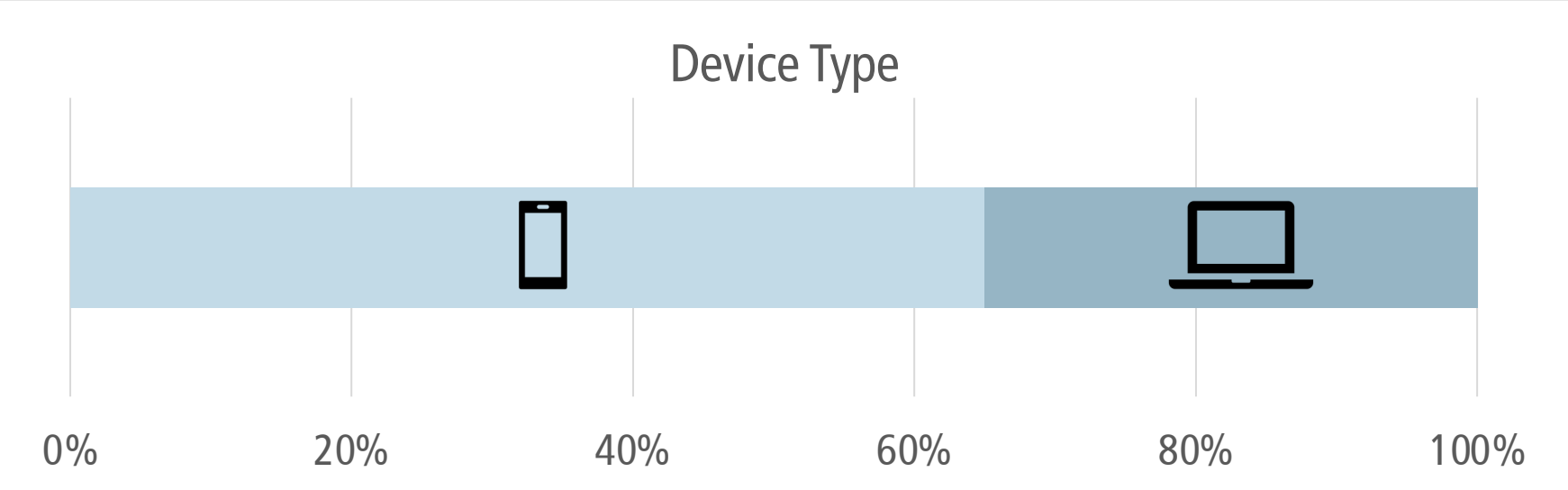
Large-Scale Study

- 3.3M Users
- >31M Login Attempts
- Collected over one Year




Number of login attempts per day
150K
100K
50K
0K
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Month
Median login attempts per minute
90
75
60
45
30
15
0
00 03 06 09 12 15 18 21 24
Hour of Day
Median login attempts
60
40
20
0
0 10 20 30 40 50 59
Minute
Login Result
Successful + Failed
Successful


Login Frequency
Less than a month
Several weeks
Every week
Several days
Daily
0%
20%
40%
60%
80%
100%


Device Type
0%
20%
40%
60%
80%
100%

Freeman et al. Algorithm

- Comparable to models apparently used by Google, Amazon, and LinkedIn

Freeman et al.: Who Are You? A Statistical Approach to Measuring User Authenticity. NDSS (2016)

$$Score_{user}(FeatureValues) =$$

$$Score_{user}(FV) = \left(\prod_{k=1}^{d} \frac{p(FV_k)}{} \right)$$

$$Score_{user}(FV) = \left(\prod_{k=1}^{d} \frac{p(FV_k)}{p(FV_k | user, legitimate)} \right)$$

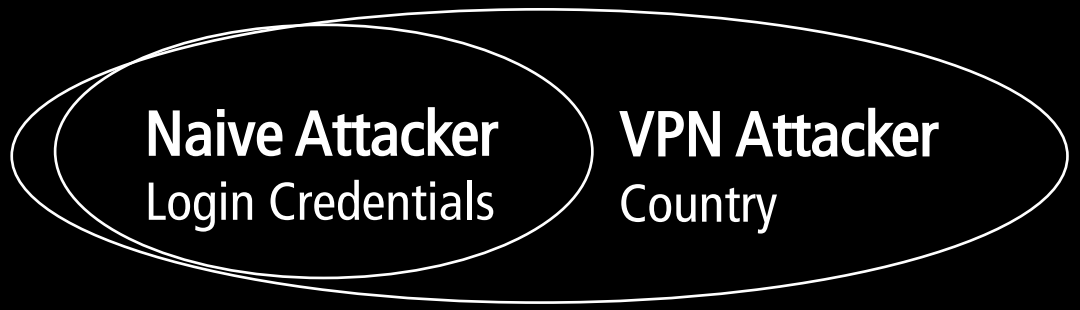
$$S_{user}(FV) = \left(\prod_{k=1}^{d} \frac{p(FV_k)}{p(FV_k | user, legitimate)} \right)$$

$$S_{user}(FV) = \left(\prod_{k=1}^{d} \frac{p(FV_k)}{p(FV_k | user, legitimate)} \right) \frac{p(user|attack)}{}$$

$$S_{user}(FV) = \left(\prod_{k=1}^{d} \frac{p(FV_k)}{p(FV_k | user, legitimate)} \right) \frac{p(user | attack)}{p(user | legitimate)}$$

Attacker Models

Naive Attacker
Login Credentials


Naive Attacker
Login Credentials
VPN Attacker
Country


Naive Attacker
Login Credentials
VPN Attacker
Country
Targeted Attacker
City, Browser, Device


Naive Attacker
Login Credentials
VPN Attacker
Country
Targeted Attacker
City, Browser, Device
Very Targeted Attacker
Verified Breaches

Naive Attacker	VPN Attacker	Targeted Attacker	Very Targeted Attacker
2.2M		58k	87
97%		3%	<0.0001%

Overview

Study

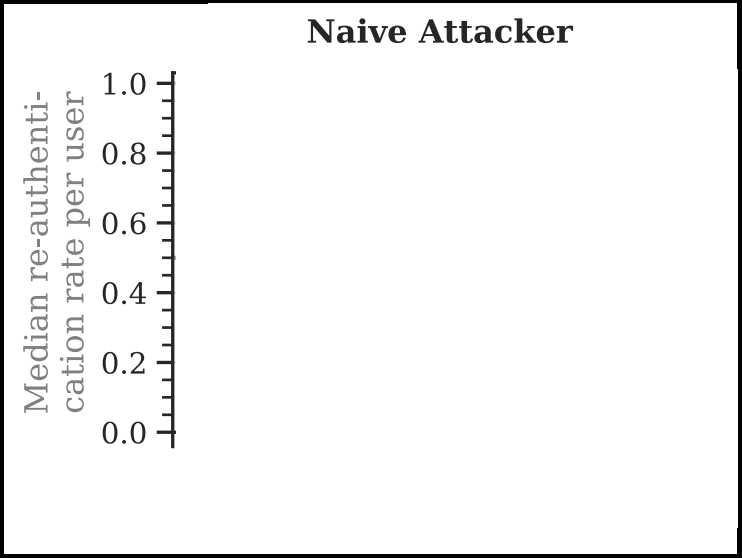
Results

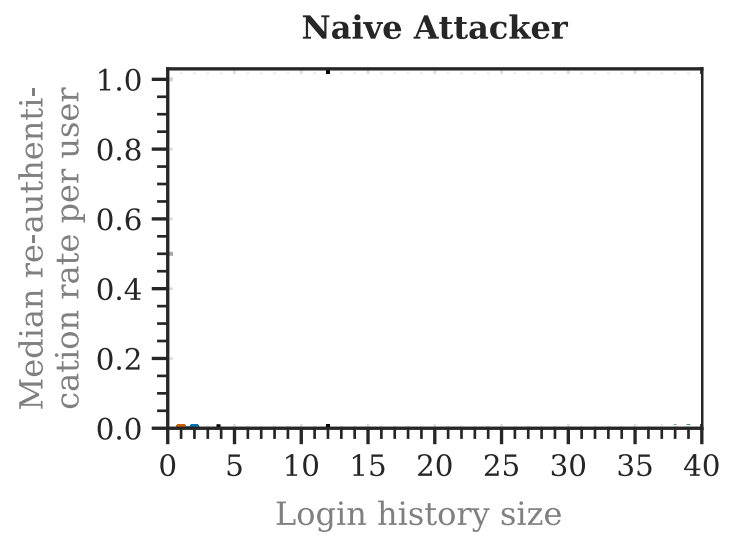
Open Source

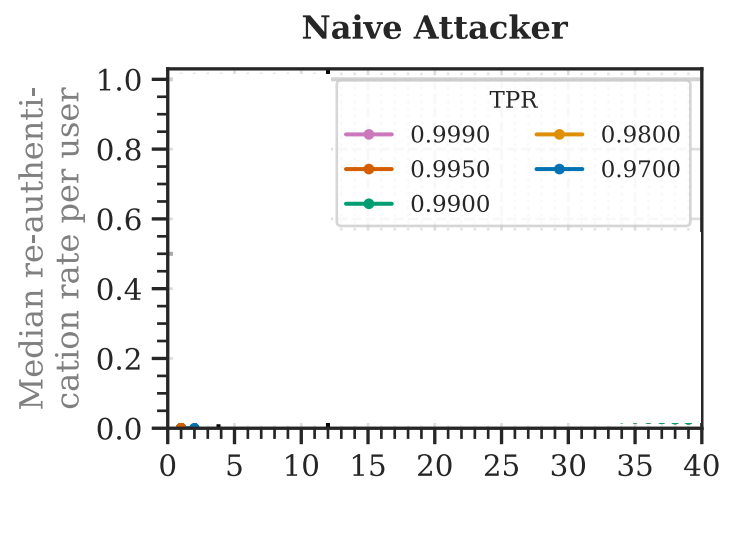
Low Re-Authentication Rates in Practice

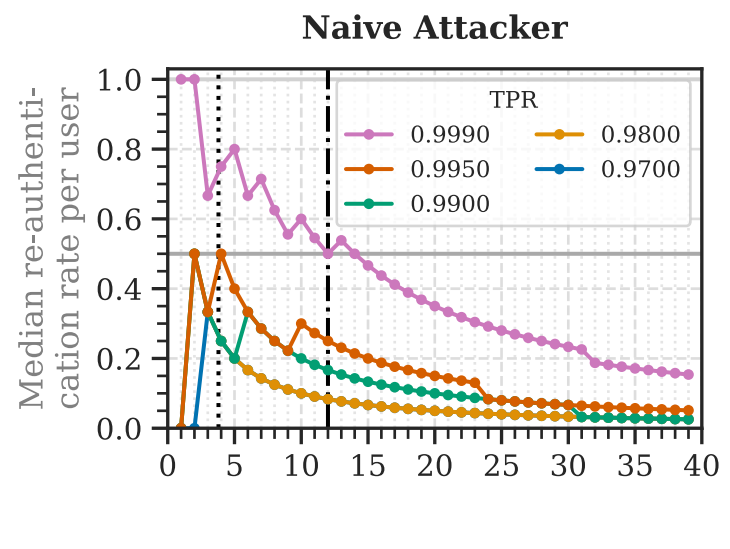
Low Re-Authentication Rates in Practice

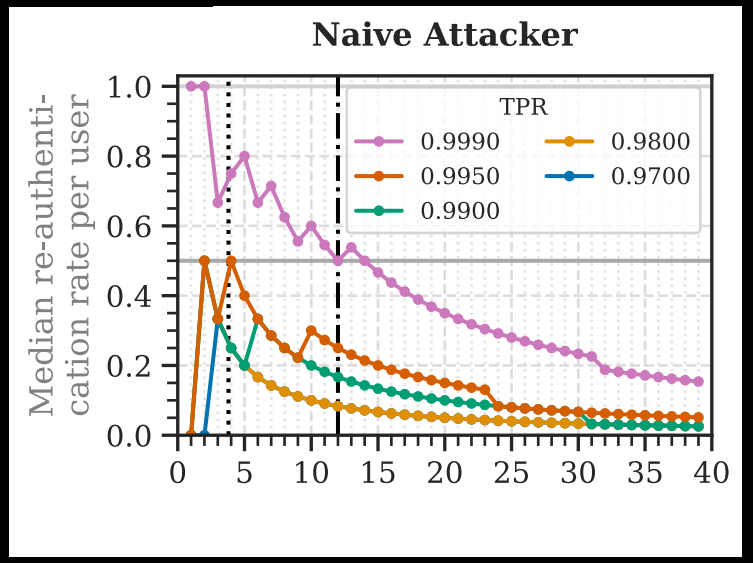
- Even when blocking >99% of targeted attackers


Naive Attacker
Median re-authenti-
cation rate per user
1.0
0.8
0.6
0.4
0.2
0.0

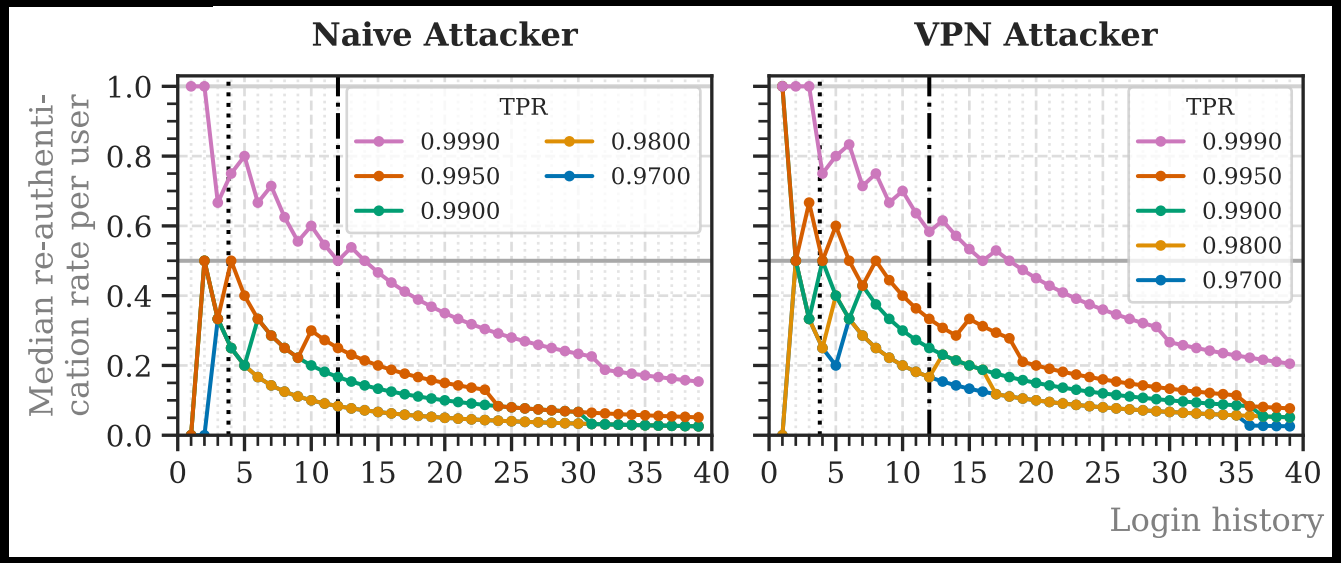

Naive Attacker
Median re-authenti-
cation rate per user
1.0
0.8
0.6
0.4
0.2
0.0
0
5
10
15
20
25
30
35
40
Login history size


Naive Attacker
Median re-authenti-
cation rate per user
1.0
0.8
0.6
0.4
0.2
0.0
0
5
10
15
20
25
30
35
40
TPR
0.9990
0.9950
0.9900
0.9800
0.9700

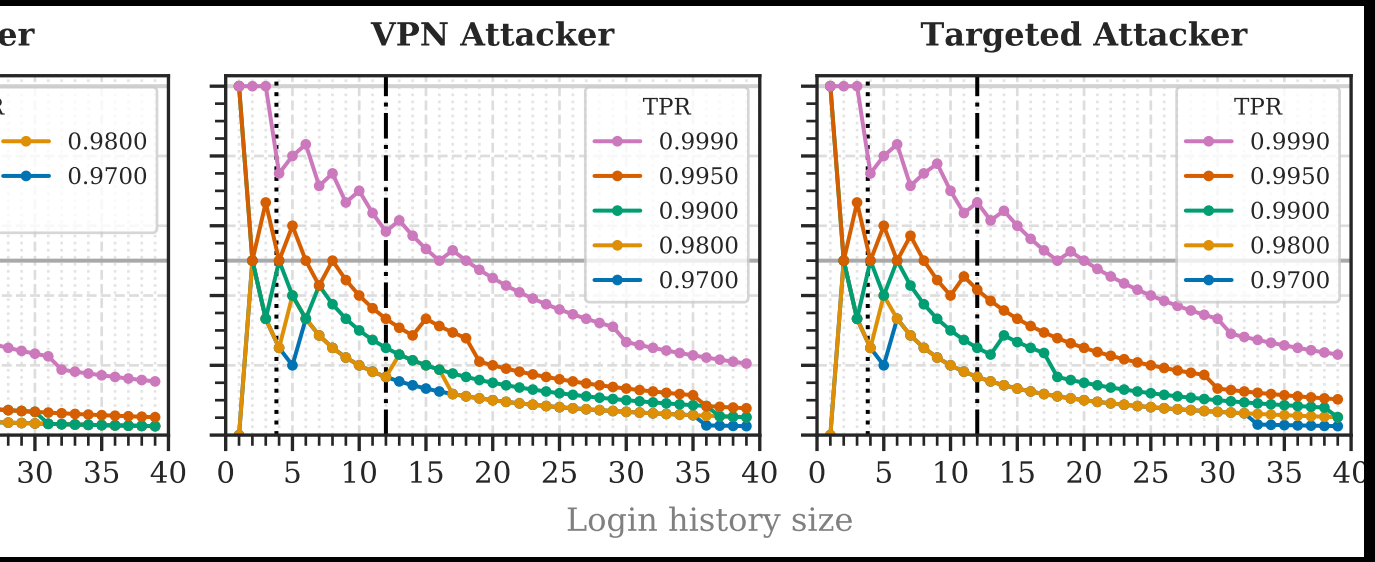

Naive Attacker
Median re-authenti-
cation rate per user
1.0
0.8
0.6
0.4
0.2
0.0
0
5
10
15
20
25
30
35
40
TPR
0.9990
0.9950
0.9900
0.9800
0.9700



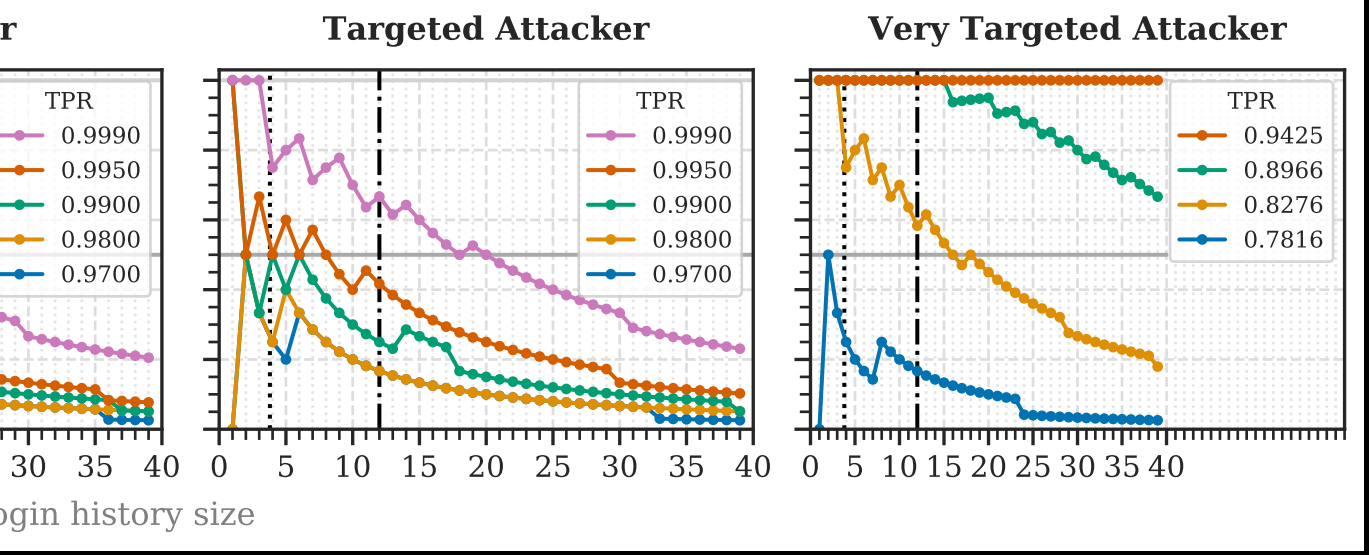
Re-Authentication Decreases With More Logins



Re-Authentication Increases With Stronger Attackers

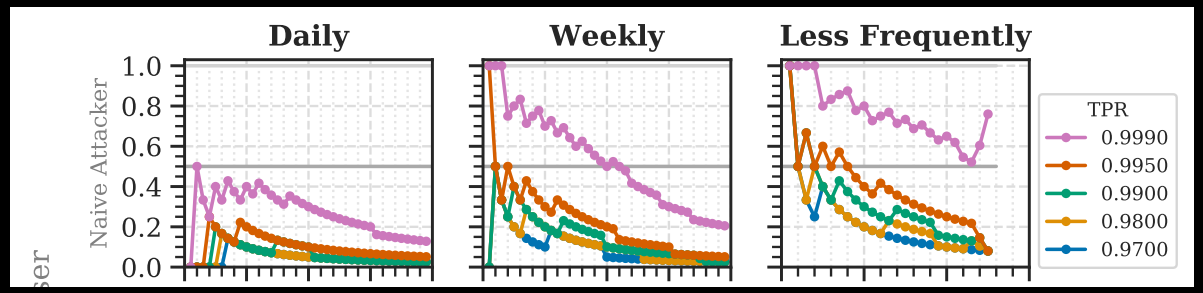


Re-Authentication Increases With Stronger Attackers

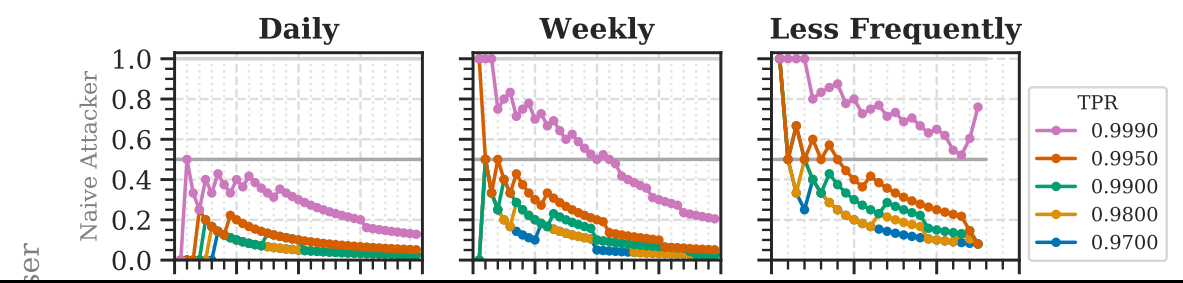


Re-Authentication Increases With Stronger Attackers

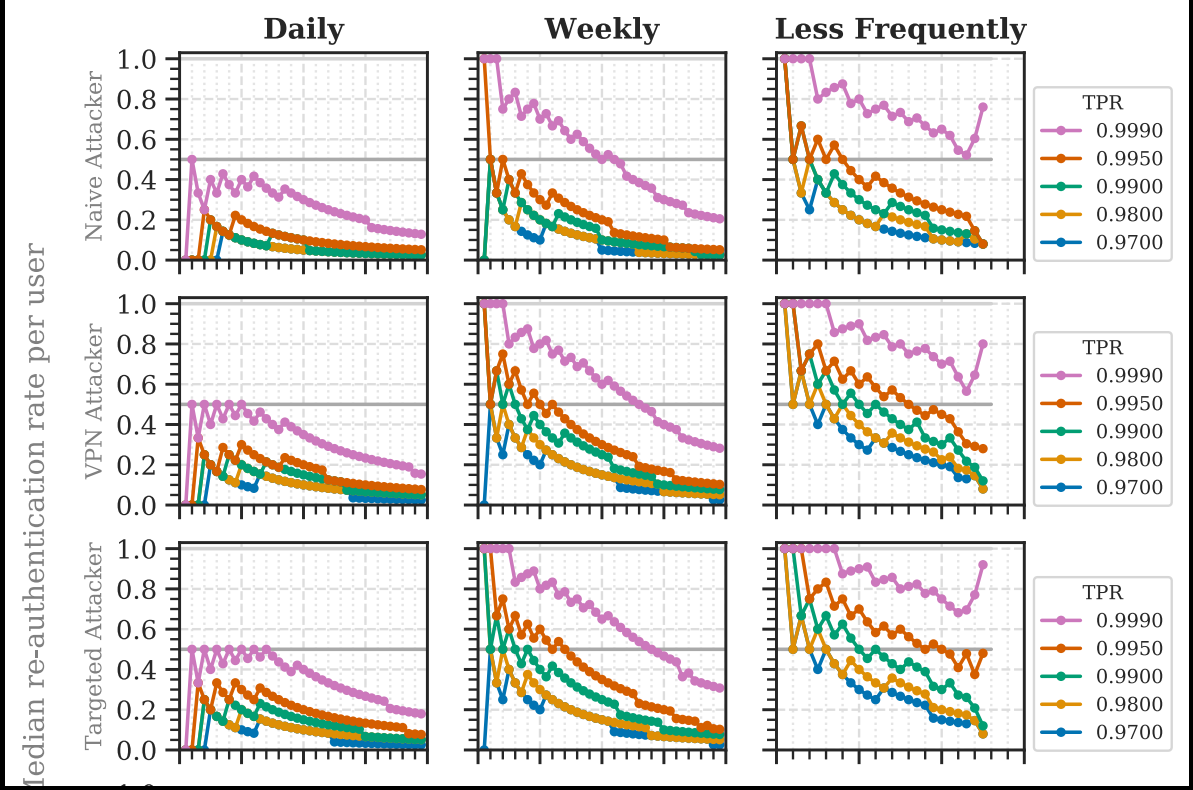
RBA Behavior Changes With Login Frequency



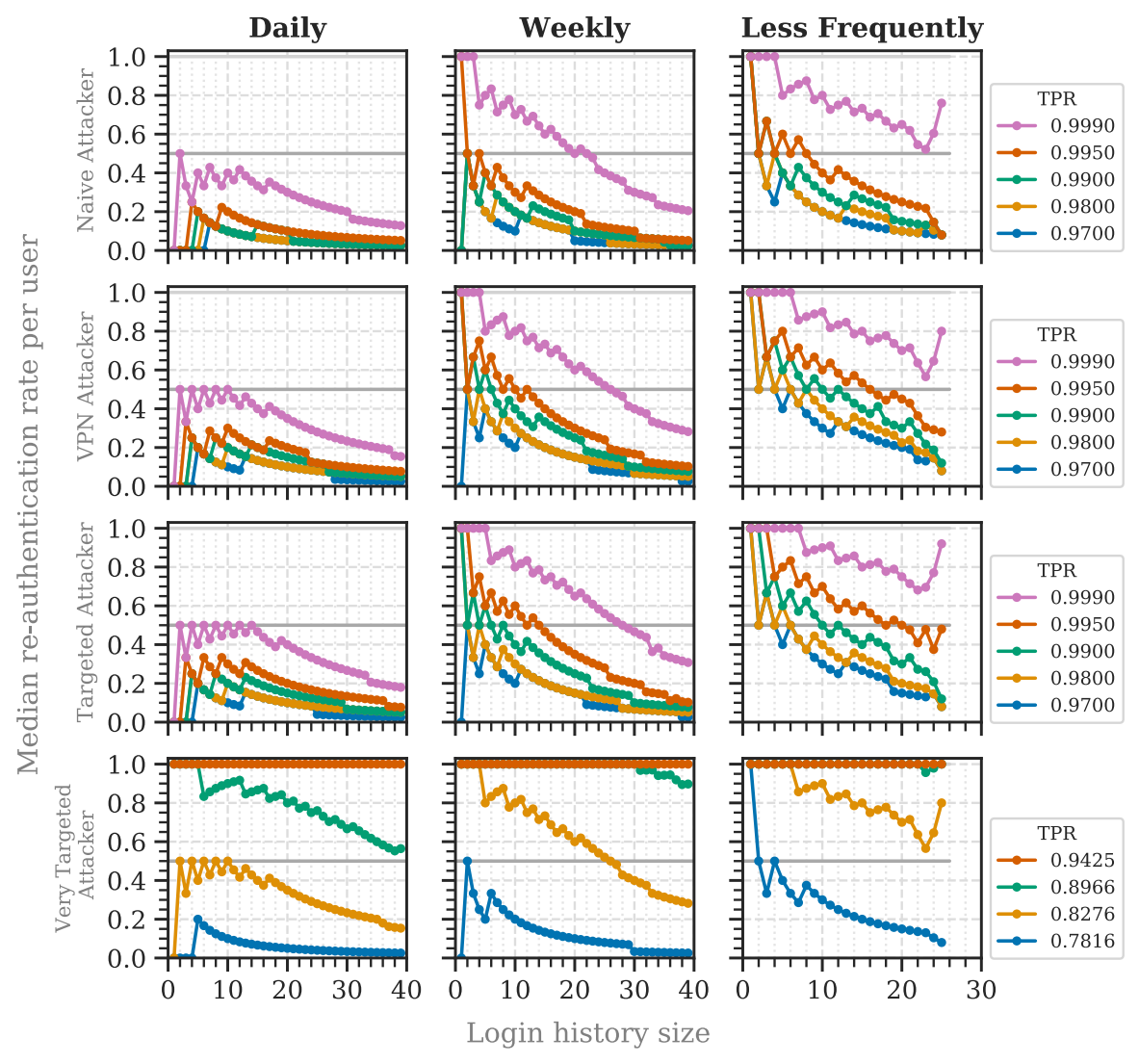
Re-Authentication Rates



Less Re-Authentication for Daily Logins

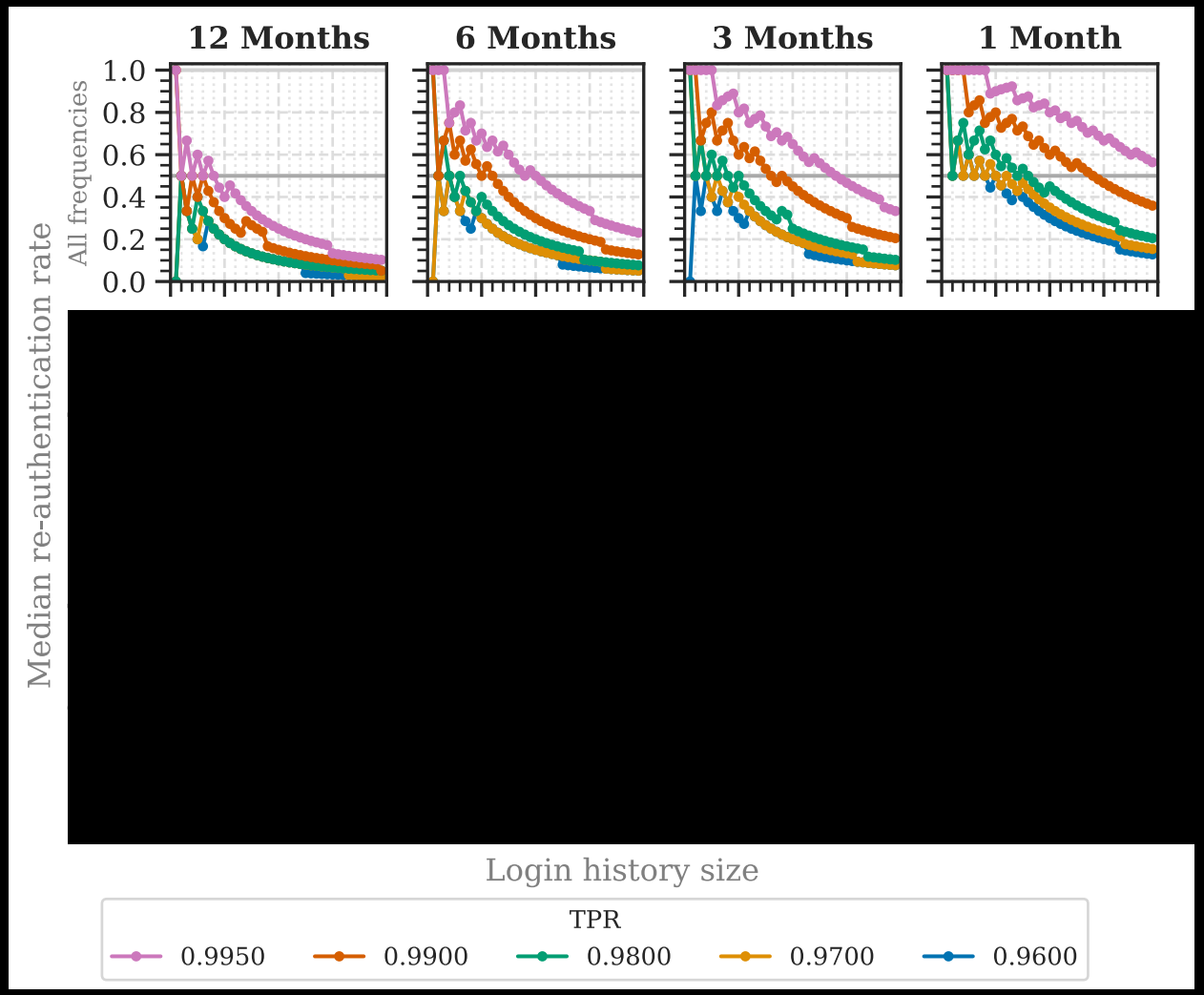


Same Tendency for All Attacker Models

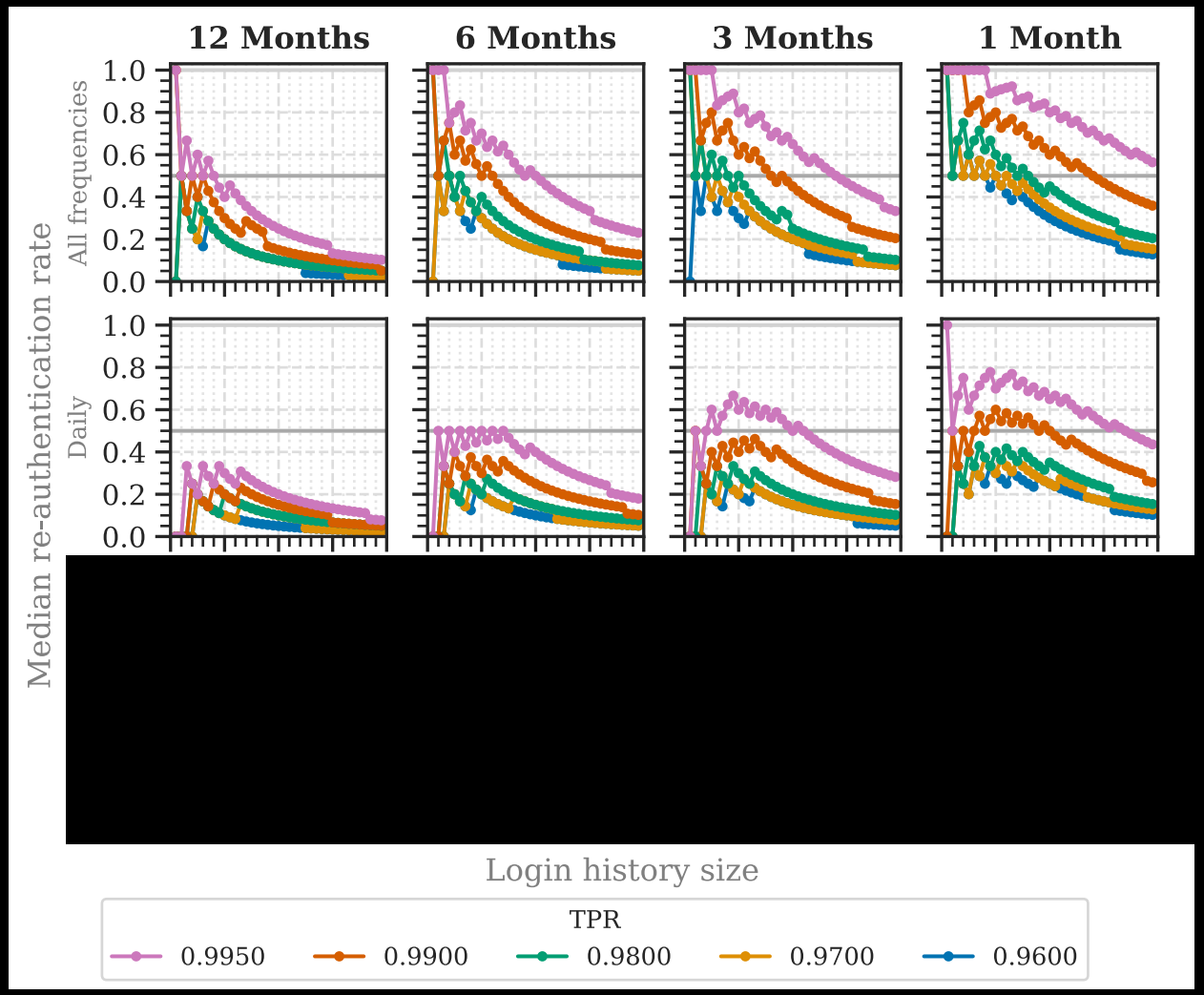

Daily
Weekly
Less Frequently
Median re-authentication rate per user
Naive Attacker
VPN Attacker
Targeted Attacker
Very Targeted Attacker
TPR
0.9990
0.9950
0.9900
0.9800
0.9700
0.9425
0.8966
0.8276
0.7816
Login history size

Login History Minimization

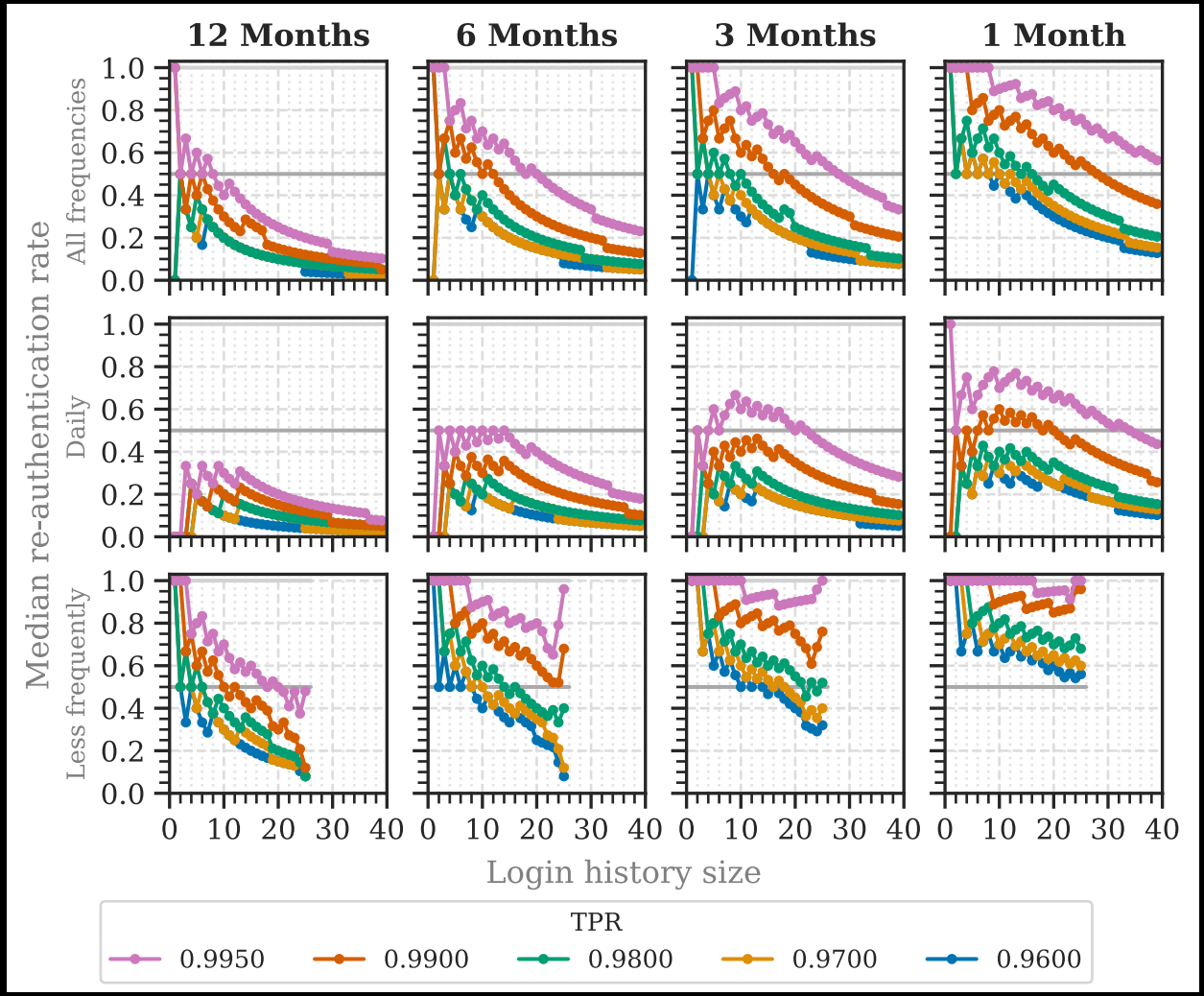
Remove Global Login History After n Months



Increases overall re-authentication rate



But: Not as high for daily users

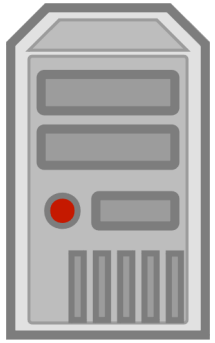

12 Months
6 Months
3 Months
1 Month
Median re-authentication rate
All frequencies
Daily
Less frequently
1.0
0.8
0.6
0.4
0.2
0.0
0
10
20
30
40
Login history size
TPR
0.9950
0.9900
0.9800
0.9700
0.9600

Round-Trip Time

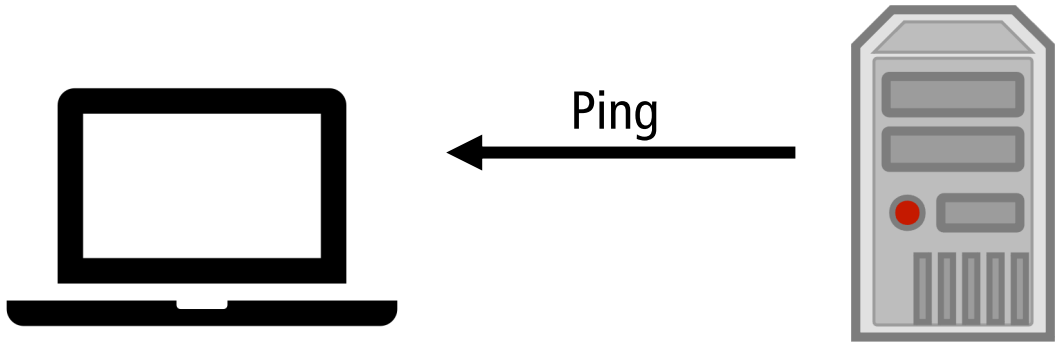
Round-Trip Time

- Based on WebSockets

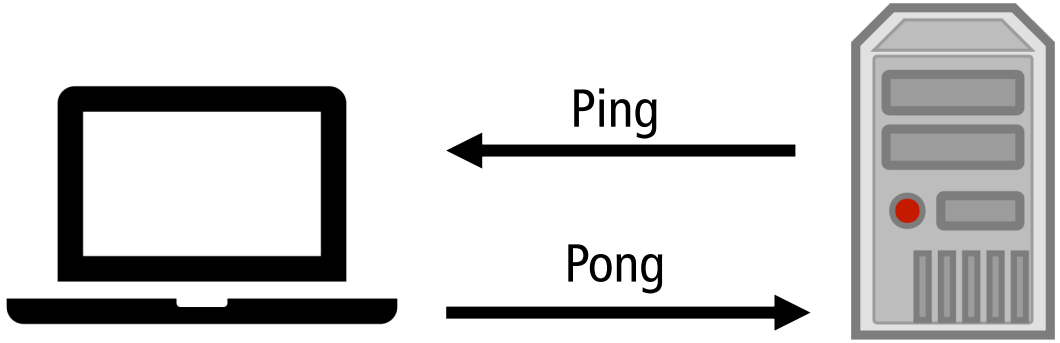
WebSocket Connection



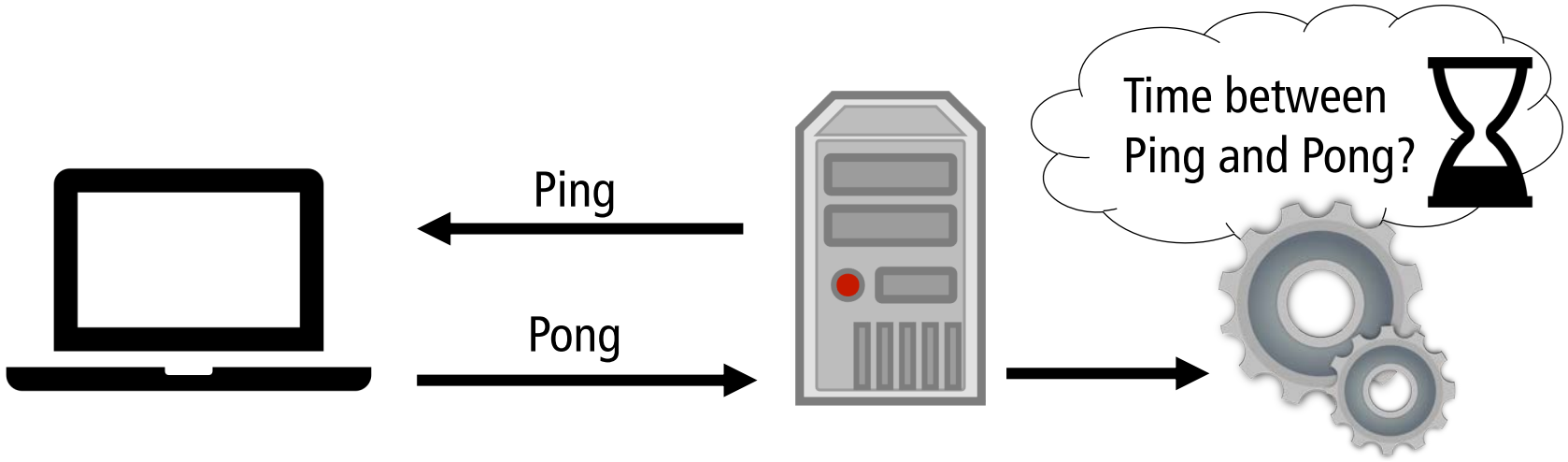
WebSocket Connection



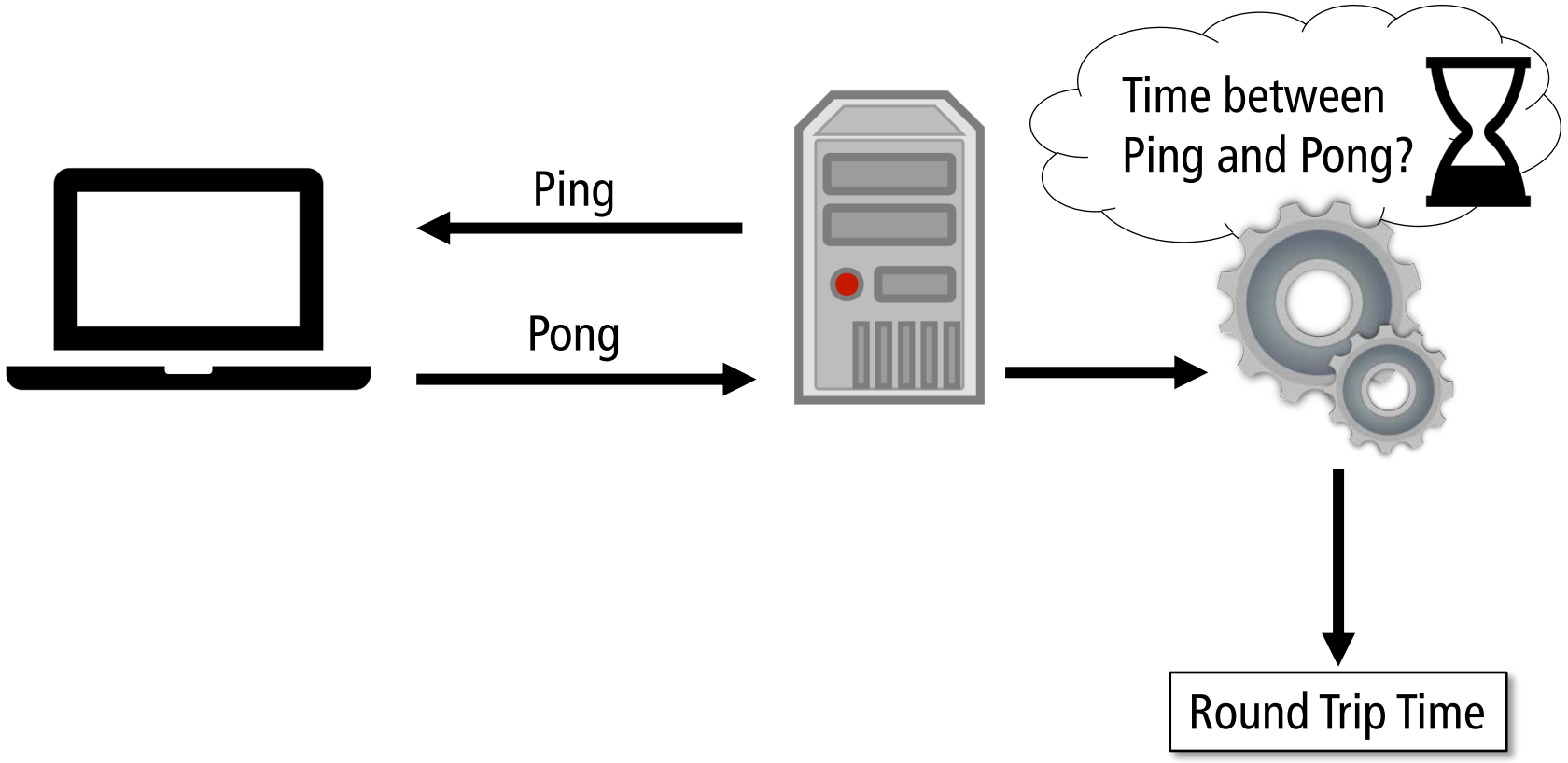
WebSocket Connection

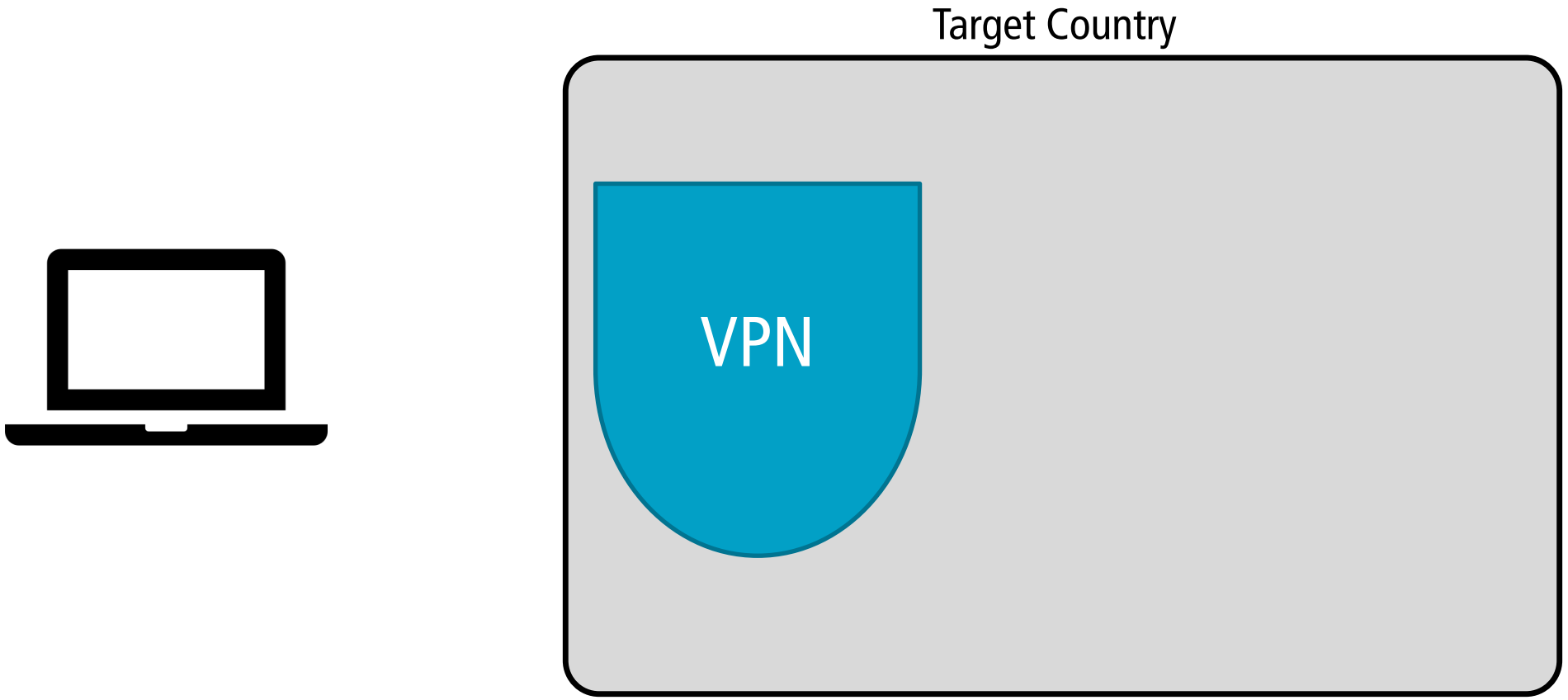


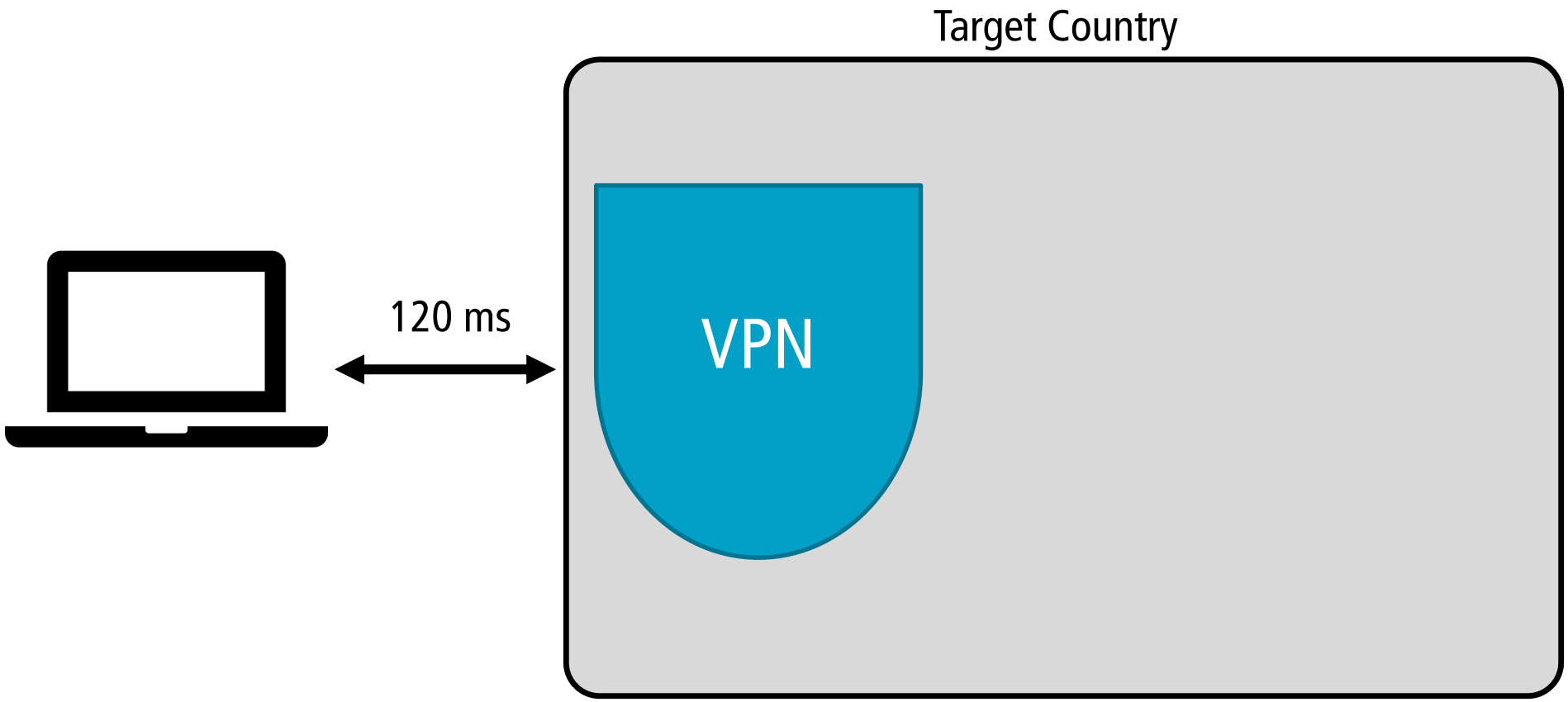
WebSocket Connection

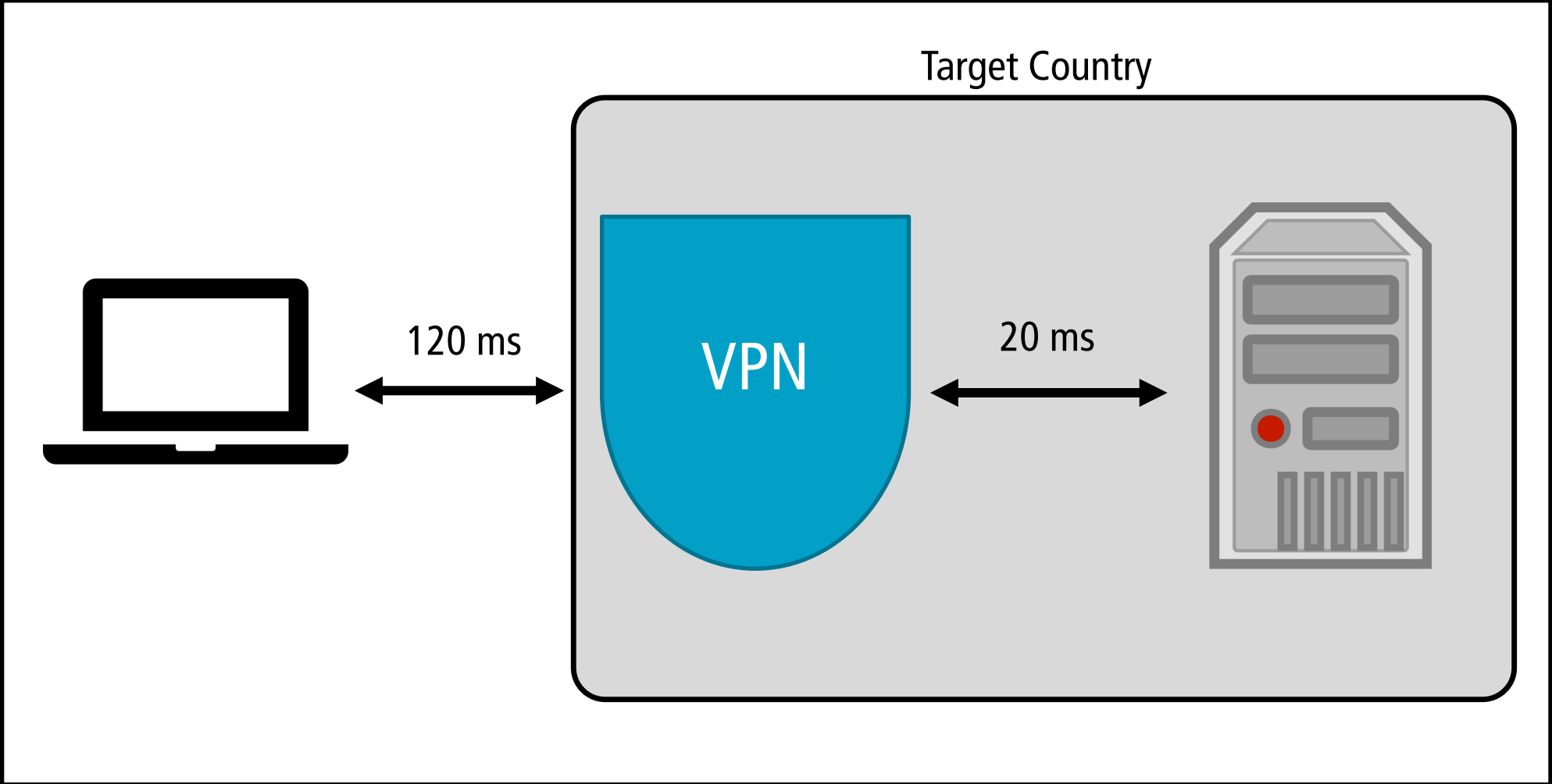


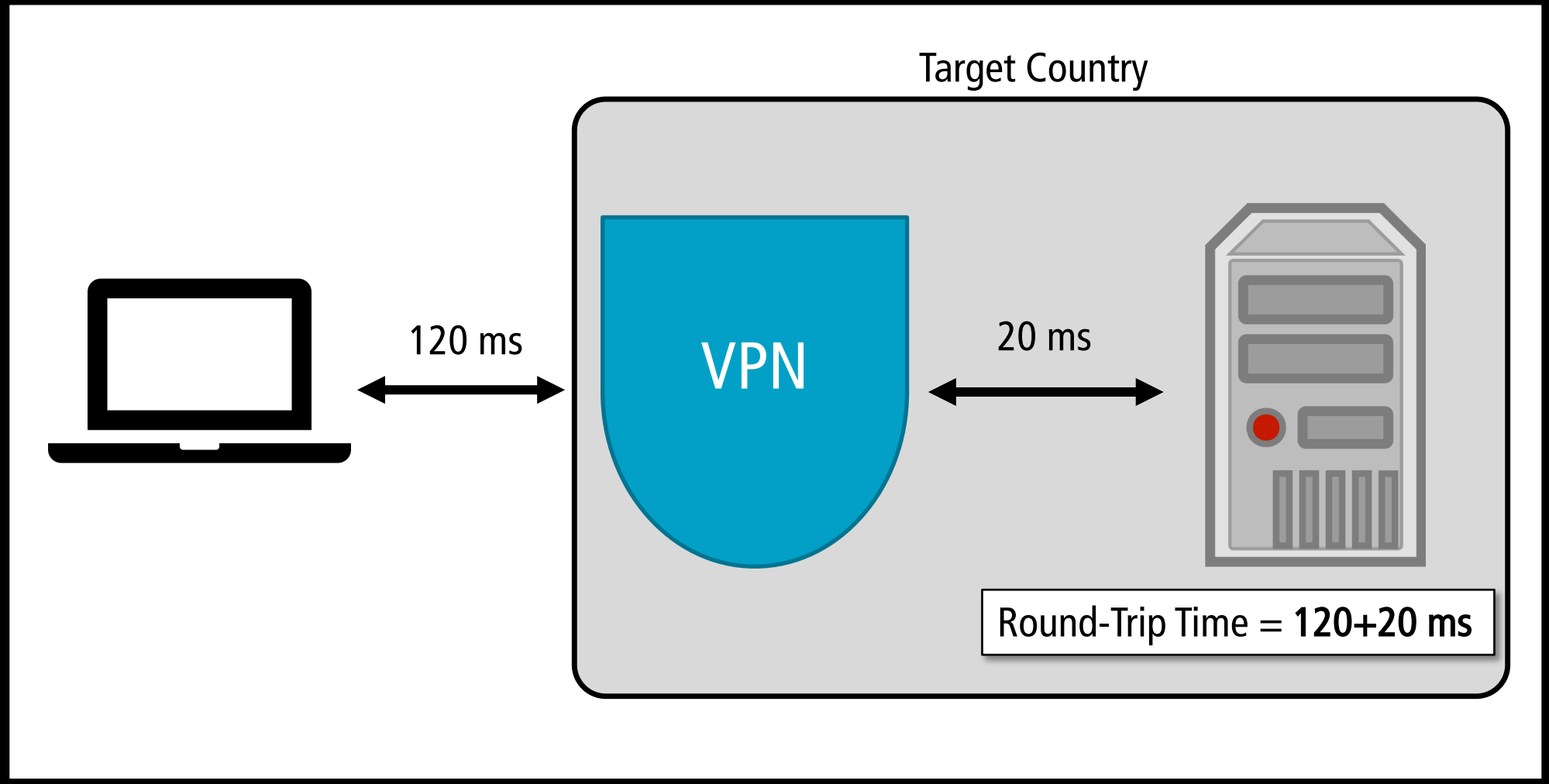
WebSocket Connection



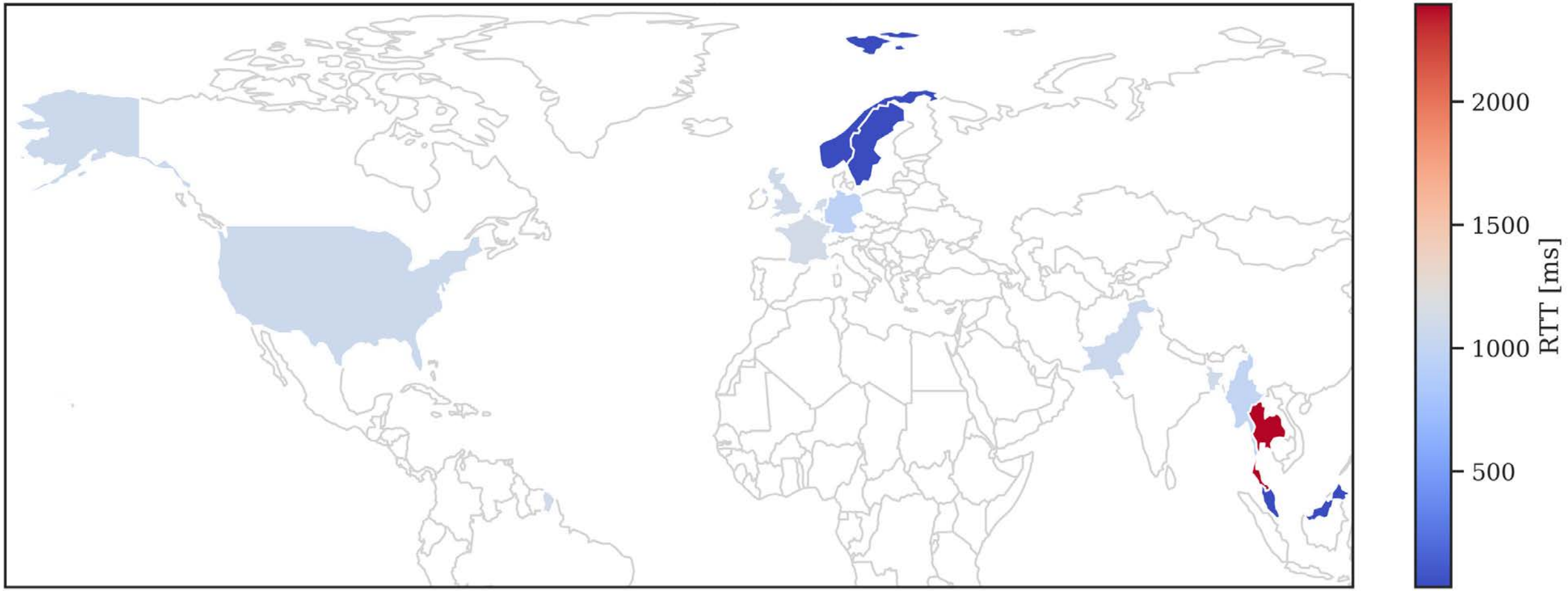

Target Country
VPN


Target Country
120 ms
VPN


Target Country
120 ms
VPN
20 ms


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

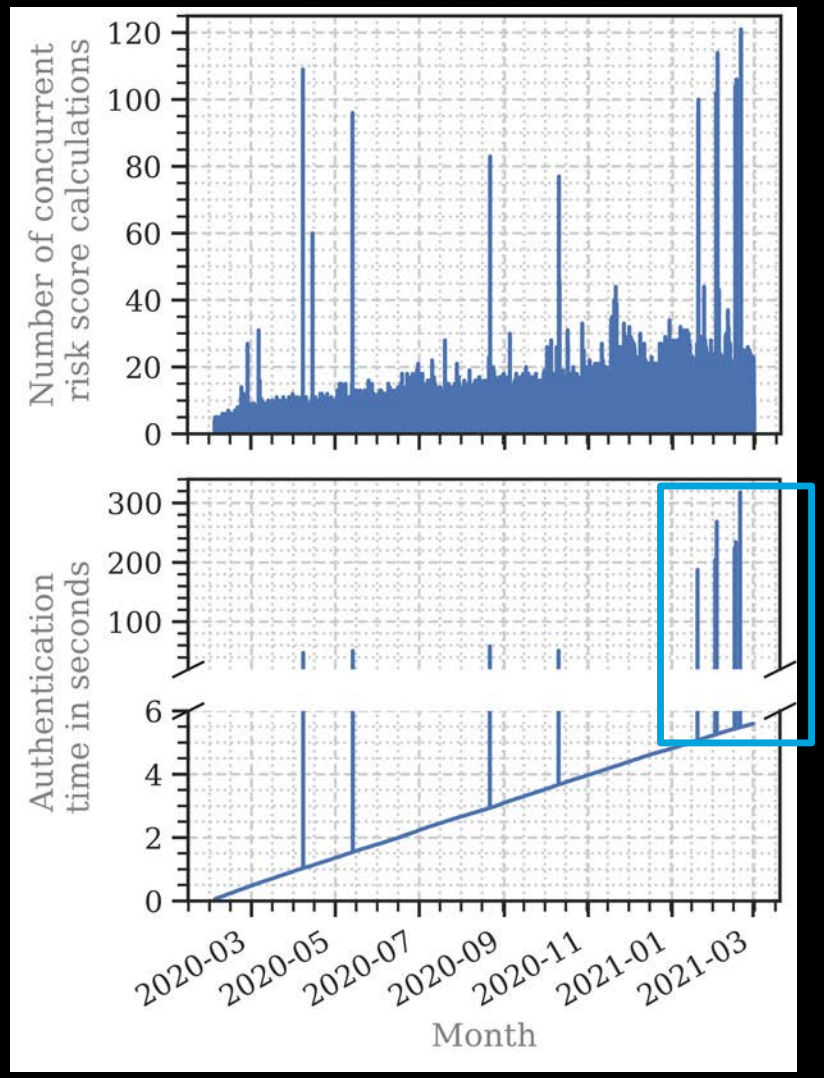
Round-Trip Time can Distinguish Countries, Regions, and Users



Optimization Needed

Optimization Needed

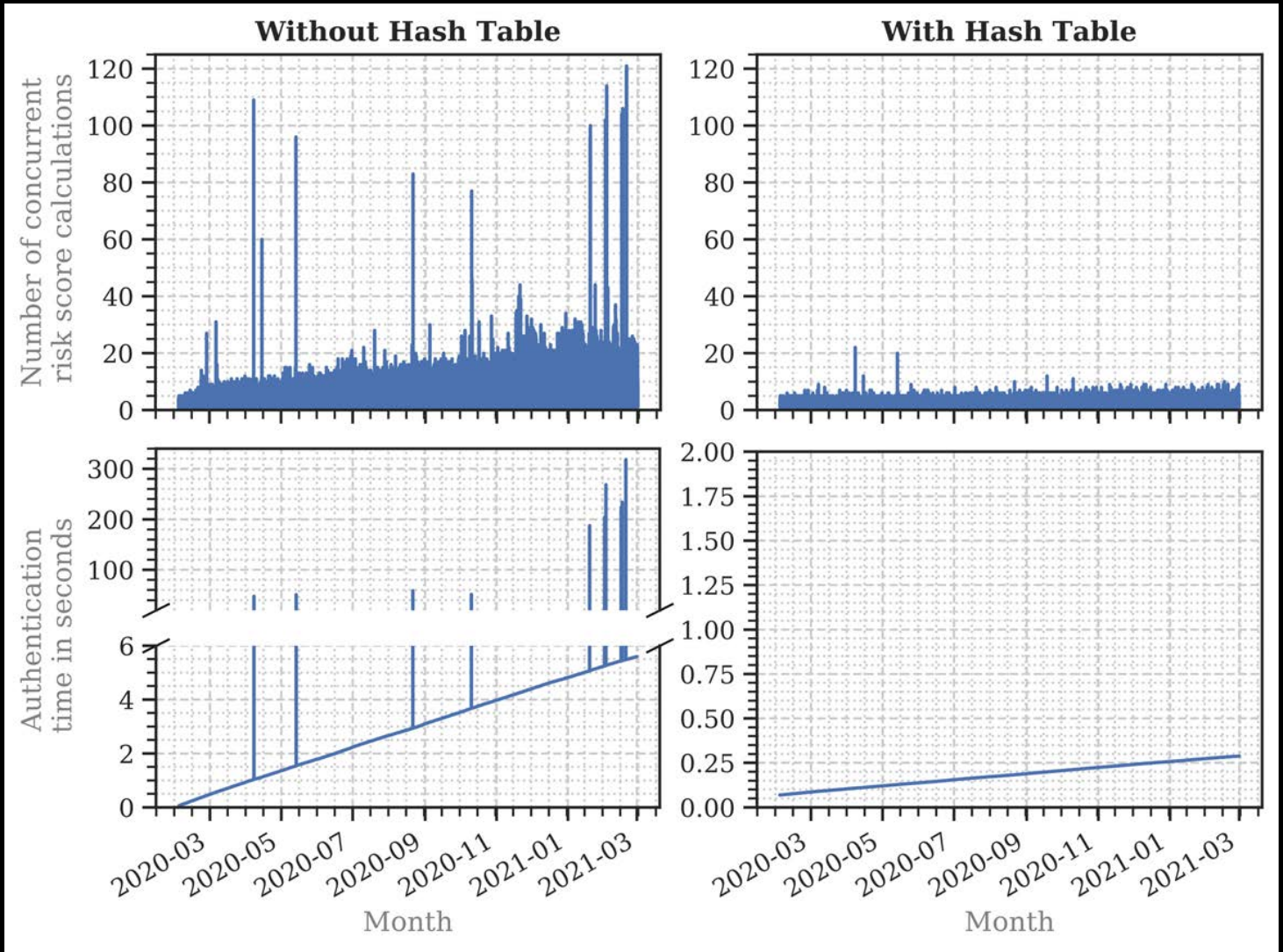
- Many queries per risk score calculation
- Risk of Denial of Service



Long Risk Score Calculation = Prone to Denial of Service

Use Hash Tables

- Reduced median authentication time from 3.2s to 0.2s


Without Hash Table
With Hash Table
Number of concurrent risk score calculations
Authentication time in seconds
Month
Month
2020-03
2020-05
2020-07
2020-09
2020-11
2021-01
2021-03

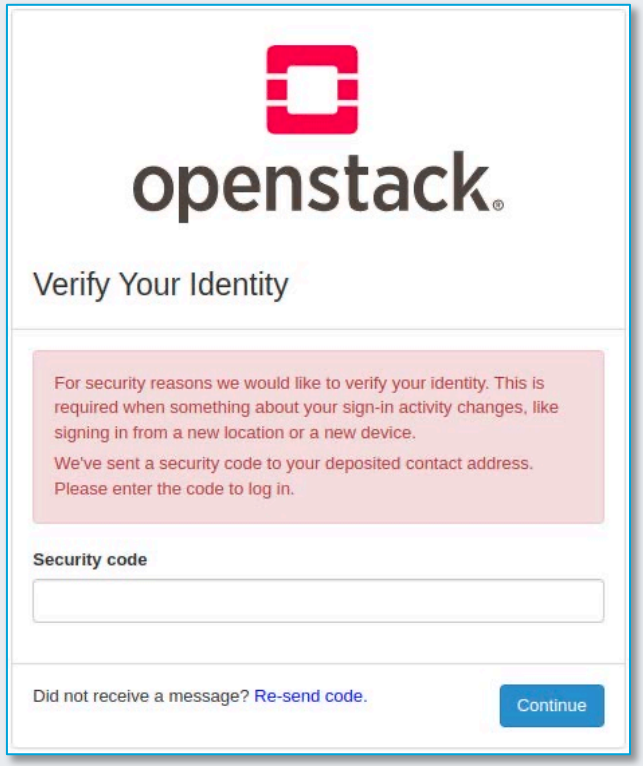
Overview

Results

Open Source

Conclusion

Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences



Risk-Based Authentication for OpenStack:

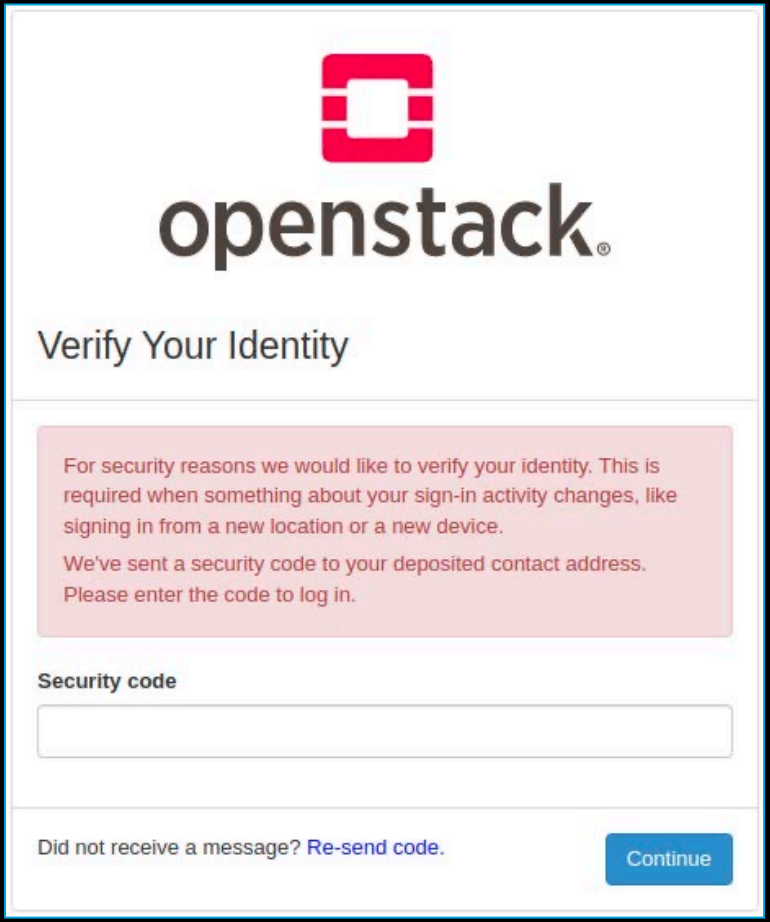
A Fully Functional Implementation and Guiding Example

Vincent Unsel, Stephan Wiefling, Nils Gruschka*, Luigi Lo Iacono
H-BRS University of Applied Sciences, Germany
University of Oslo, Norway (*)

Published at ACM CODASPY ‘23

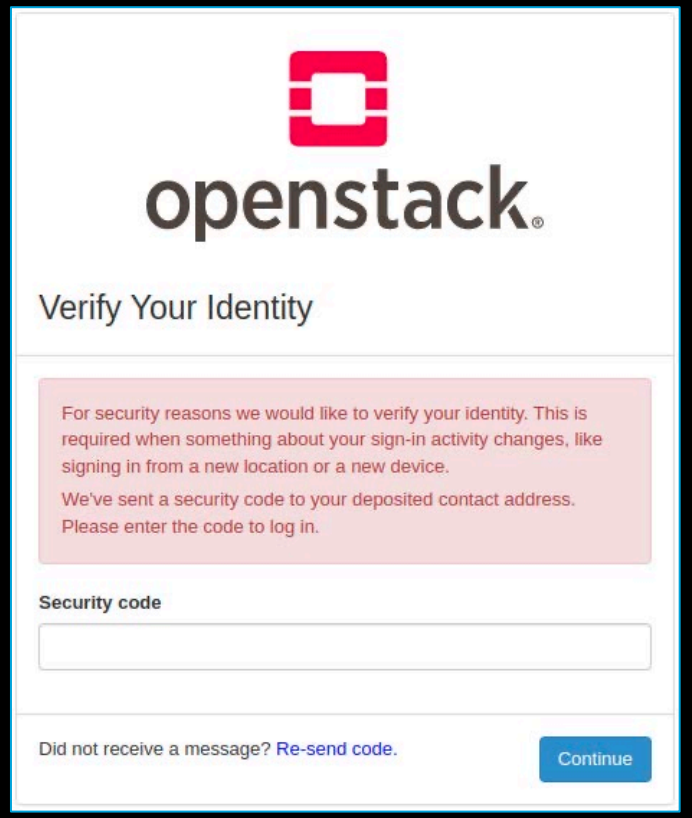
RBA Plugin

- First fully functional plugin for OpenStack cloud computing platform



Frontend

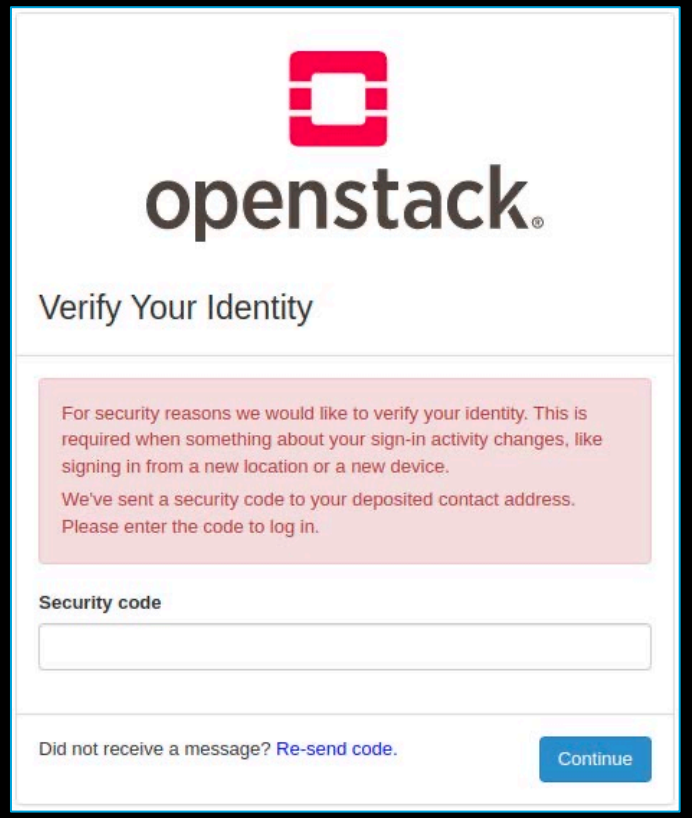
- Based on state of practice found in real-world solutions
  - Amazon, Facebook, GOG.com, Google, LinkedIn, and Microsoft



Wiefling et al.: Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild. In: IFIP SEC (2019). Springer
Wiefling et al: More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-Based Authentication. In ACSAC (2020). ACM

Frontend

- E-Mail verification via code
- Generic RBA dialog based on studied online services



Wiefling et al.: Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild. In: IFIP SEC (2019). Springer
Wiefling et al: More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-Based Authentication. In ACSAC (2020). ACM

Verification Method

- Designed by recommendations of usability studies

Wiefling et al: More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-Based Authentication. In ACSAC (2020). ACM
Wiefling et al.: Evaluation of Risk-Based Re-Authentication Methods. In: IFIP SEC (2020). Springer

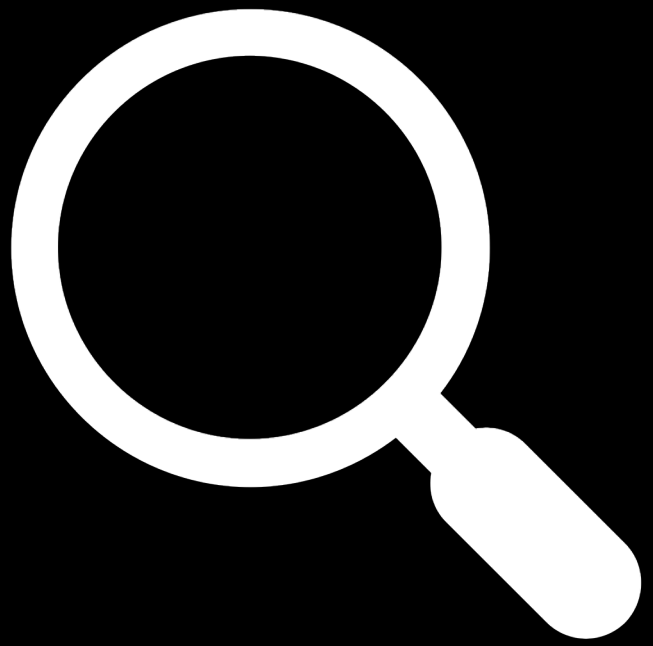
Verification Method

- E-Mail verification
  - Six digit code in email subject line and body
- Can be modified in plugin

Wiefling et al: More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-Based Authentication. In ACSAC (2020). ACM
Wiefling et al.: Evaluation of Risk-Based Re-Authentication Methods. In: IFIP SEC (2020). Springer

Feature Selection

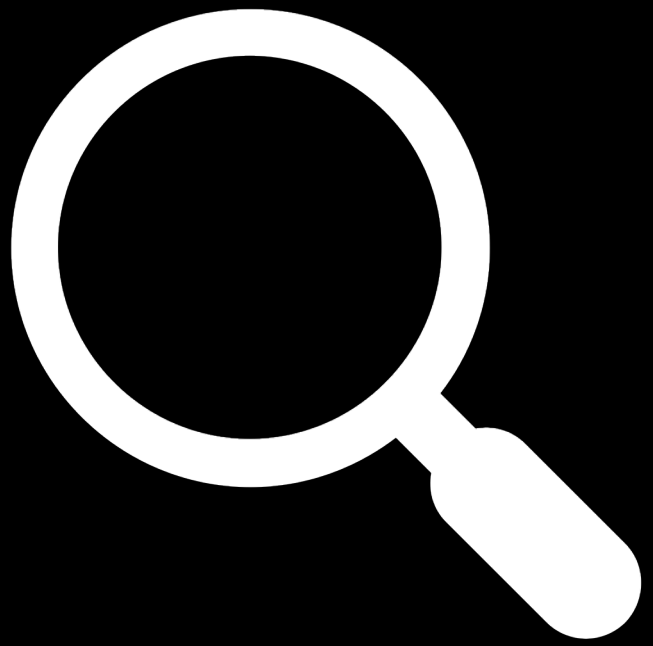
- Most effective ones to identify users
- Based on findings of multiple security and privacy analysis studies



Wiefling et al.: What's in Score for Website Users: A Data-Driven Long-Term Study on Risk-Based Authentication Characteristics. In: FC (2021). Springer
Wiefling et al.: Privacy Considerations for Risk-Based Authentication Systems. In: IWPE (2021). IEEE
Wiefling et al.: Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service. In: TOPS (2023). ACM.

Feature Selection

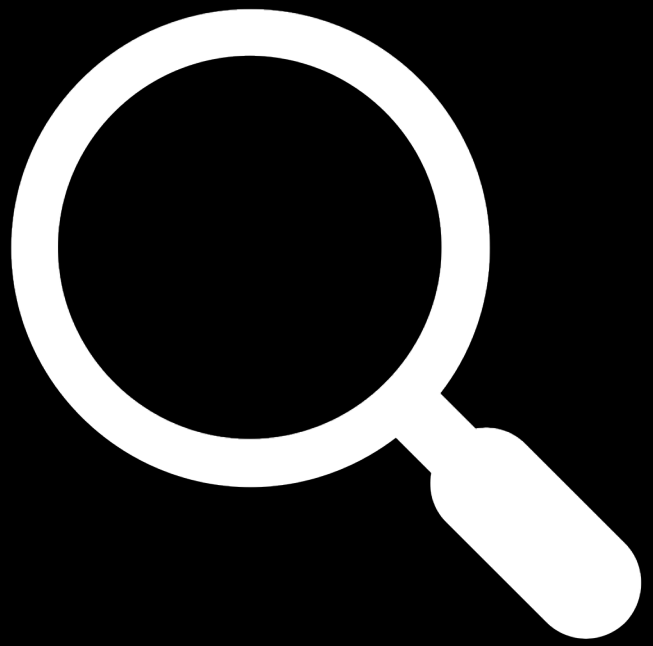
- IP Address
- User Agent String
- Round-Trip Time



Wiefling et al.: What's in Score for Website Users: A Data-Driven Long-Term Study on Risk-Based Authentication Characteristics. In: FC (2021). Springer
Wiefling et al.: Privacy Considerations for Risk-Based Authentication Systems. In: IWPE (2021). IEEE
Wiefling et al.: Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service. In: TOPS (2023). ACM.

Feature Selection

- Can be extended in plugin



Wiefling et al.: What's in Score for Website Users: A Data-Driven Long-Term Study on Risk-Based Authentication Characteristics. In: FC (2021). Springer
Wiefling et al.: Privacy Considerations for Risk-Based Authentication Systems. In: IWPE (2021). IEEE
Wiefling et al.: Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service. In: TOPS (2023). ACM.

Overview

Results

Open Source

Conclusion

Summary

- RBA* can achieve low re-authentication rates when blocking >99% targeted attackers
  - But it depends on the user base

- RTT is promising feature to replace IP address
- Optimization can bring performance gain

- Dataset Download available at riskbasedauthentication.org

*Using the Freeman et al. (2016) model

Summary

- Provide Open Source Plugin for OpenStack*
- Blueprint for Developers

- Guidance on how to test and strengthen RBA implementations in the paper*

- Outlook:
  - Putting RBA into more Open Source software
  - Continuous Authentication

*rbainfo.org/opensource

Thank you

riskbasedauthentication.org
das.h-brs.de

stephan.wiefling@h-brs.de

@swiefling@hci.social