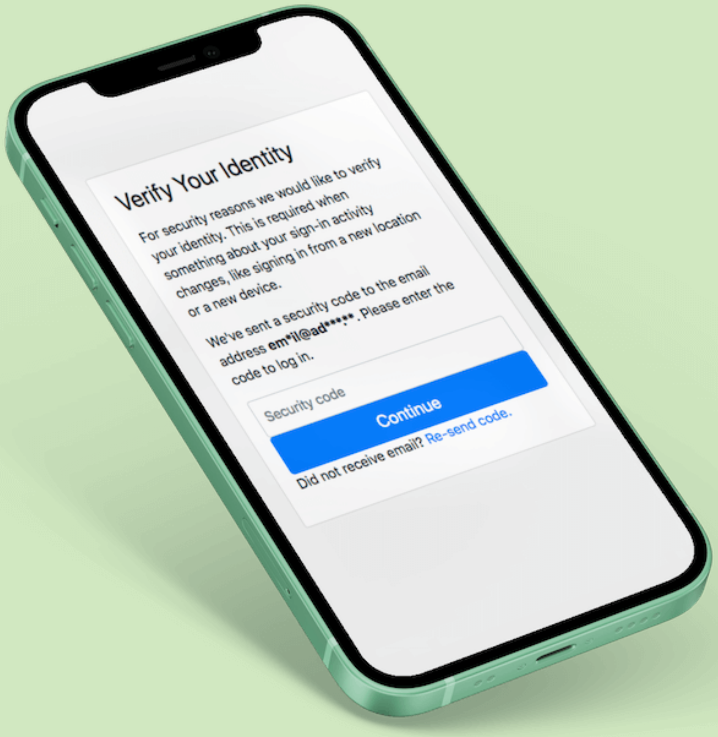
Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

RUHR
UNIVERSITÄT
BOCHUM
RUB



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

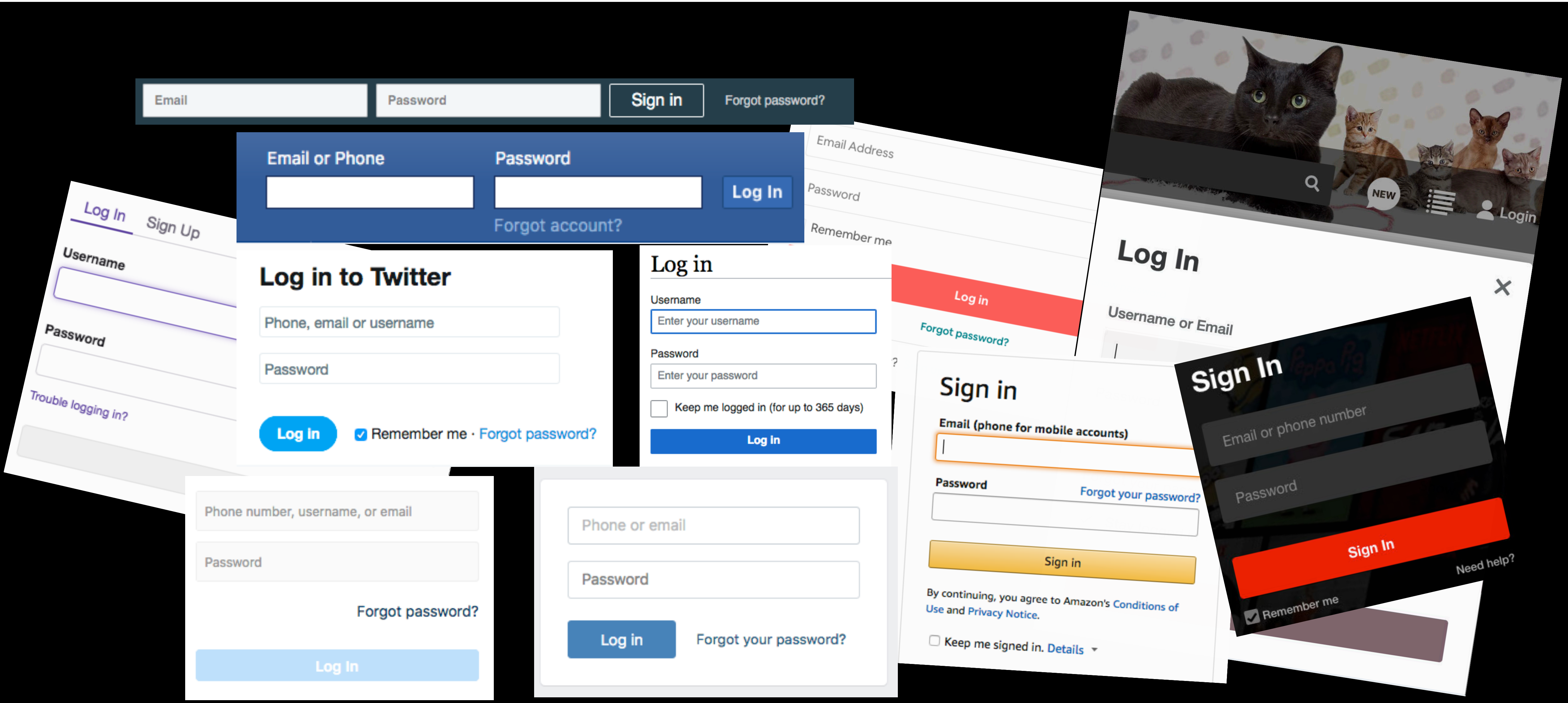
Did not receive email? Re-send code.

Privacy Considerations for Risk-Based Authentication Systems

Stephan Wiefling*, Jan Tolsdorf, Luigi Lo Iacono

H-BRS University of Applied Sciences

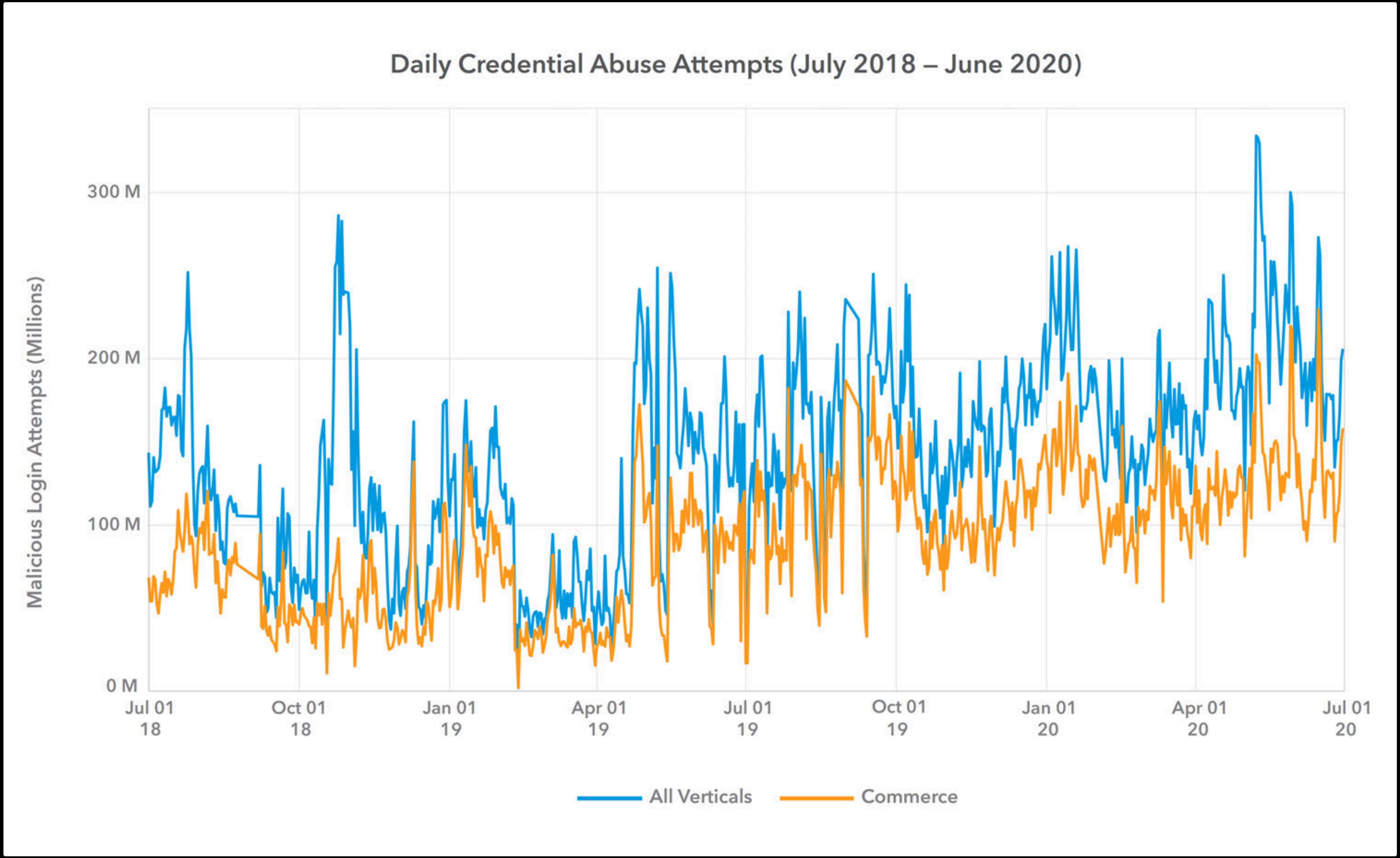
Ruhr University Bochum (*)


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
NEW
Log In
Username or Email
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
☑ Remember me
Need help?
Phone number, username, or email
Password
Forgot password?
Log In
Phone or email
Password
Log in
Forgot your password?

Credential Stuffing

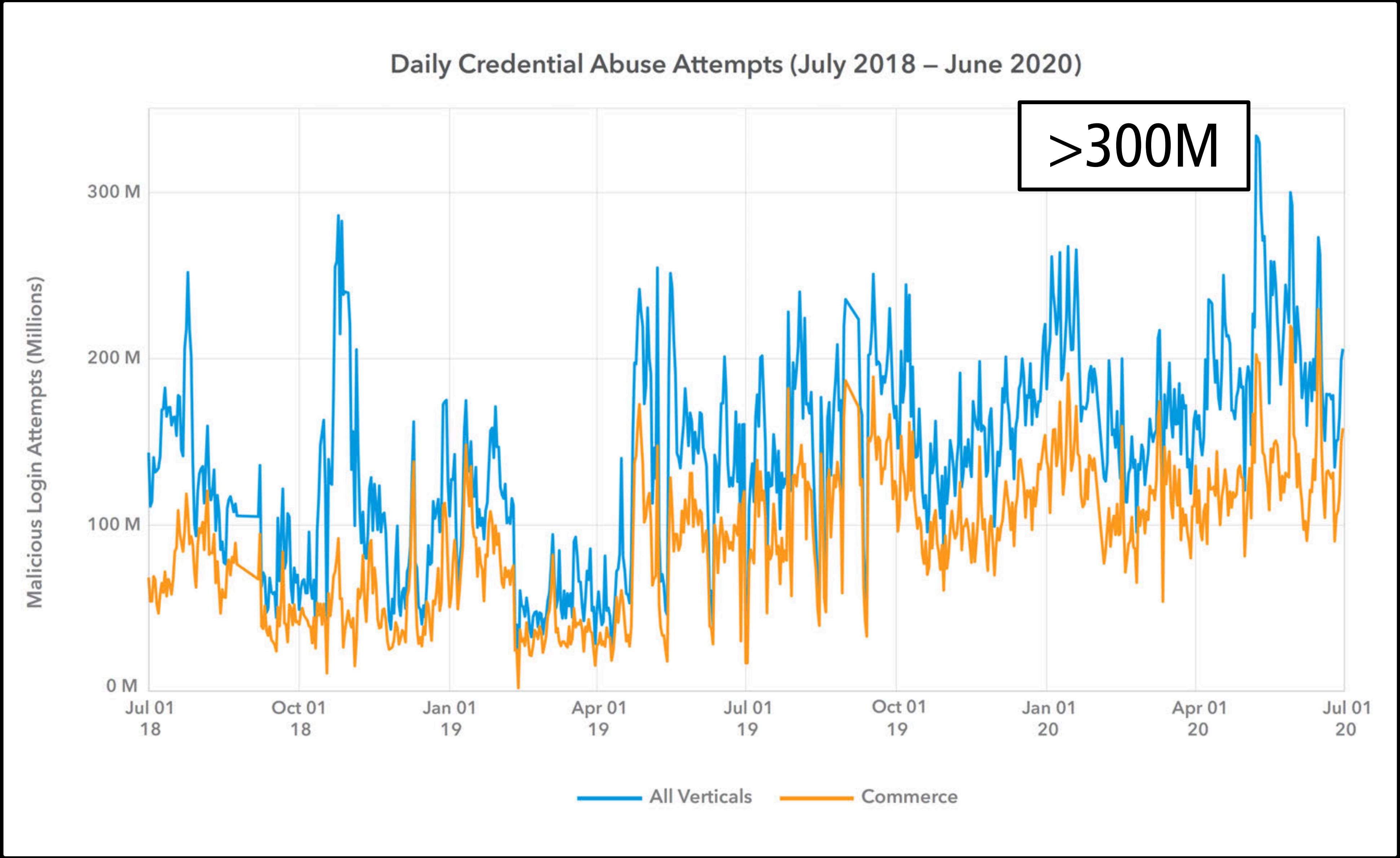
Daily Credential Abuse Attempts (July 2018 – June 2020)

Akamai: Loyalty for Sale – Retail and Hospitality Fraud. In: [state of the internet] / security (2020).



Daily Credential Abuse Attempts (July 2018 – June 2020)

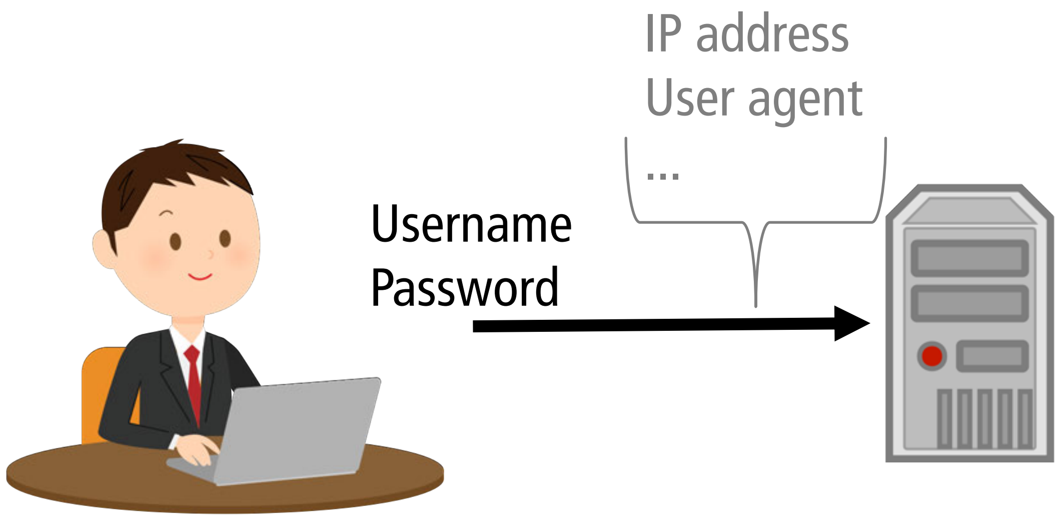
Akamai: Loyalty for Sale – Retail and Hospitality Fraud. In: [state of the internet] / security (2020).



>300M

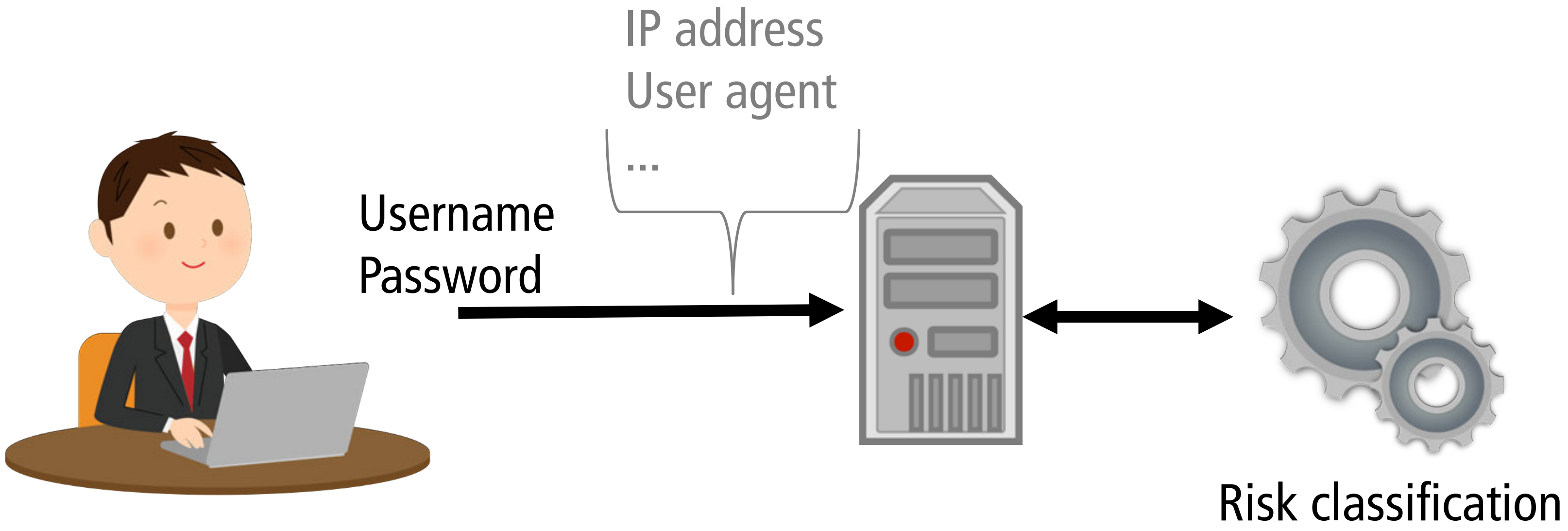
Akamai: Loyalty for Sale – Retail and Hospitality Fraud. In: [state of the internet] / security (2020).

Risk-based Authentication (RBA)



IP address
User agent
...

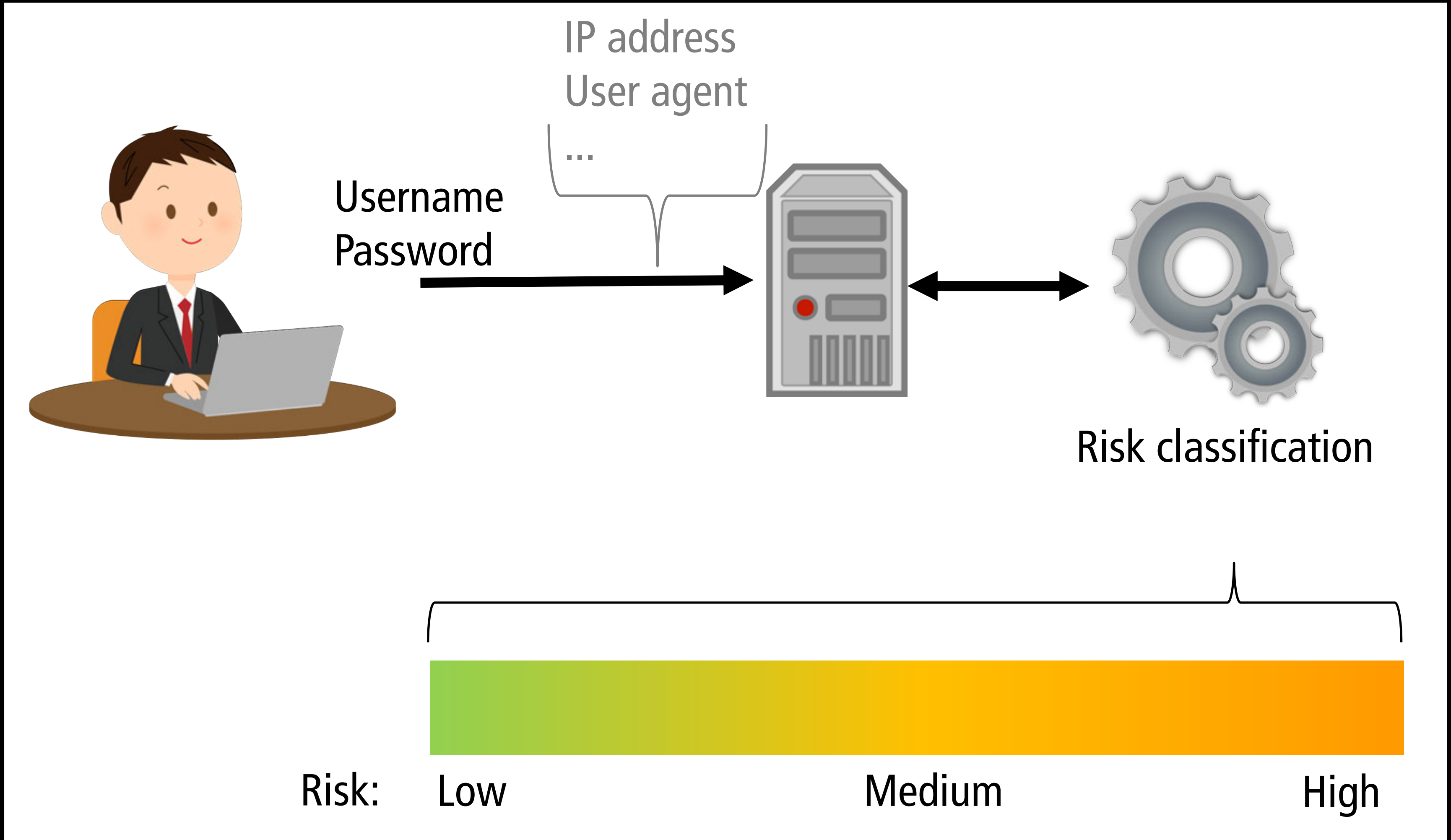
Username
Password



IP address
User agent
...

Username
Password

Risk classification

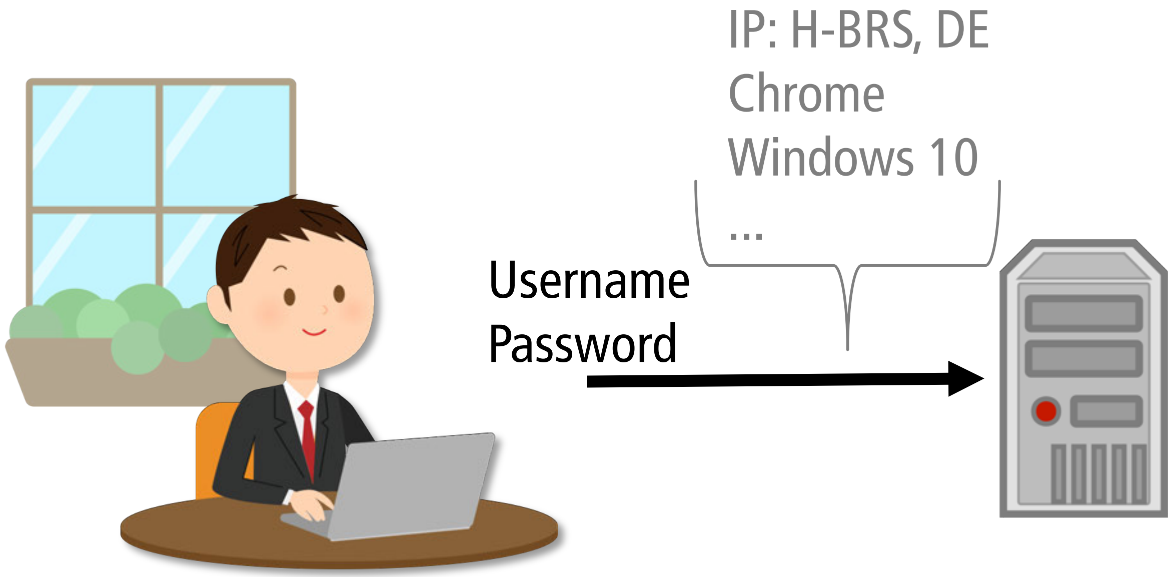


IP address
User agent
...

Username
Password

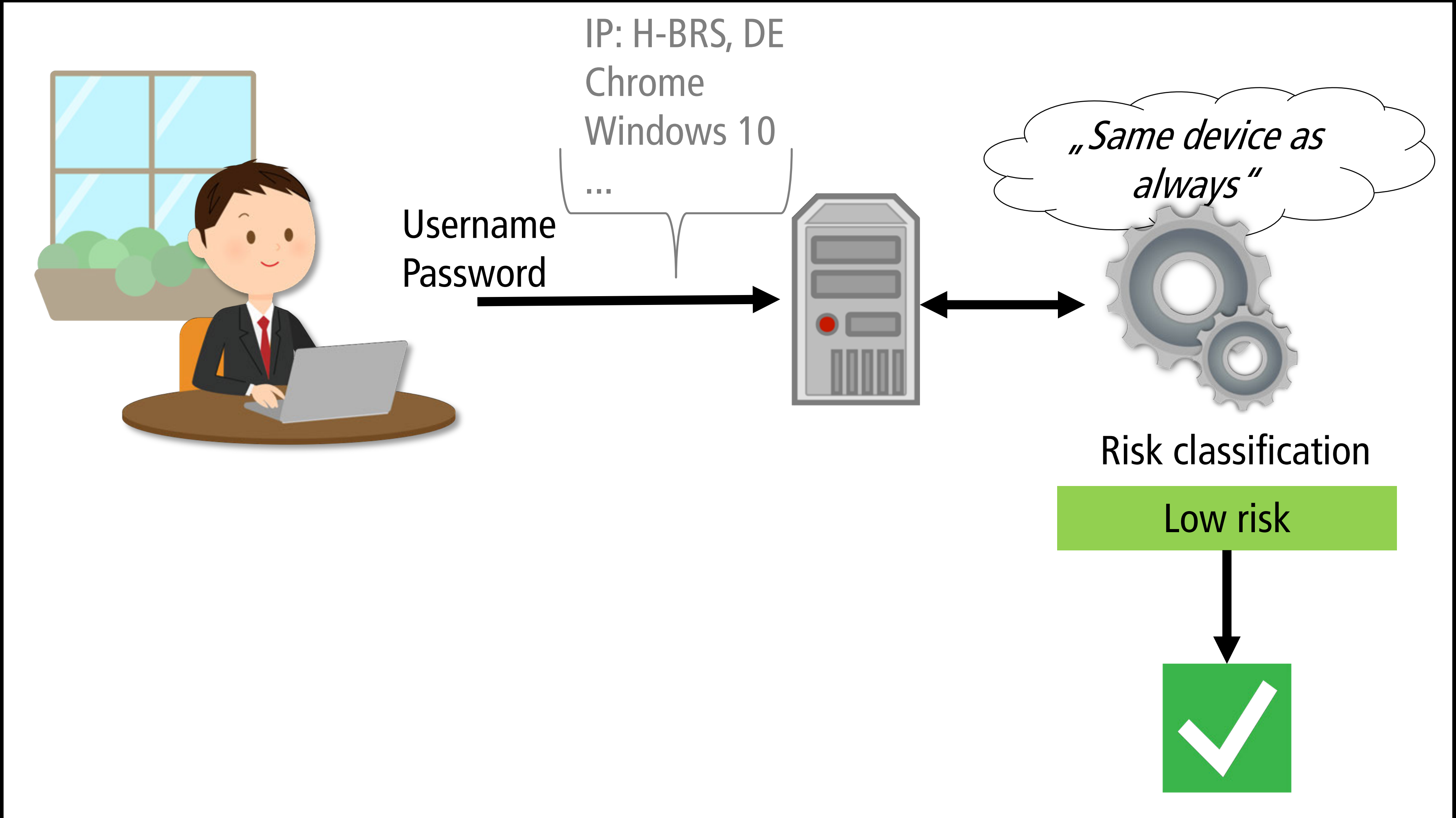
Risk classification

Risk: Low Medium High



IP: H-BRS, DE
Chrome
Windows 10
...

Username
Password

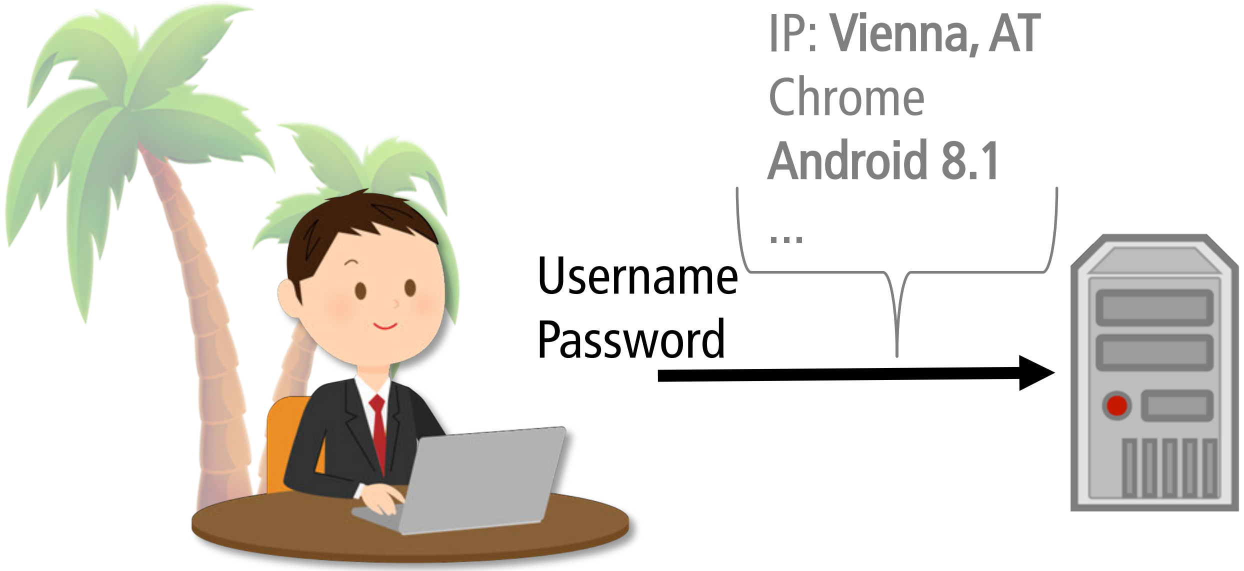

IP: H-BRS, DE
Chrome
Windows 10
...

Username
Password

„Same device as always"

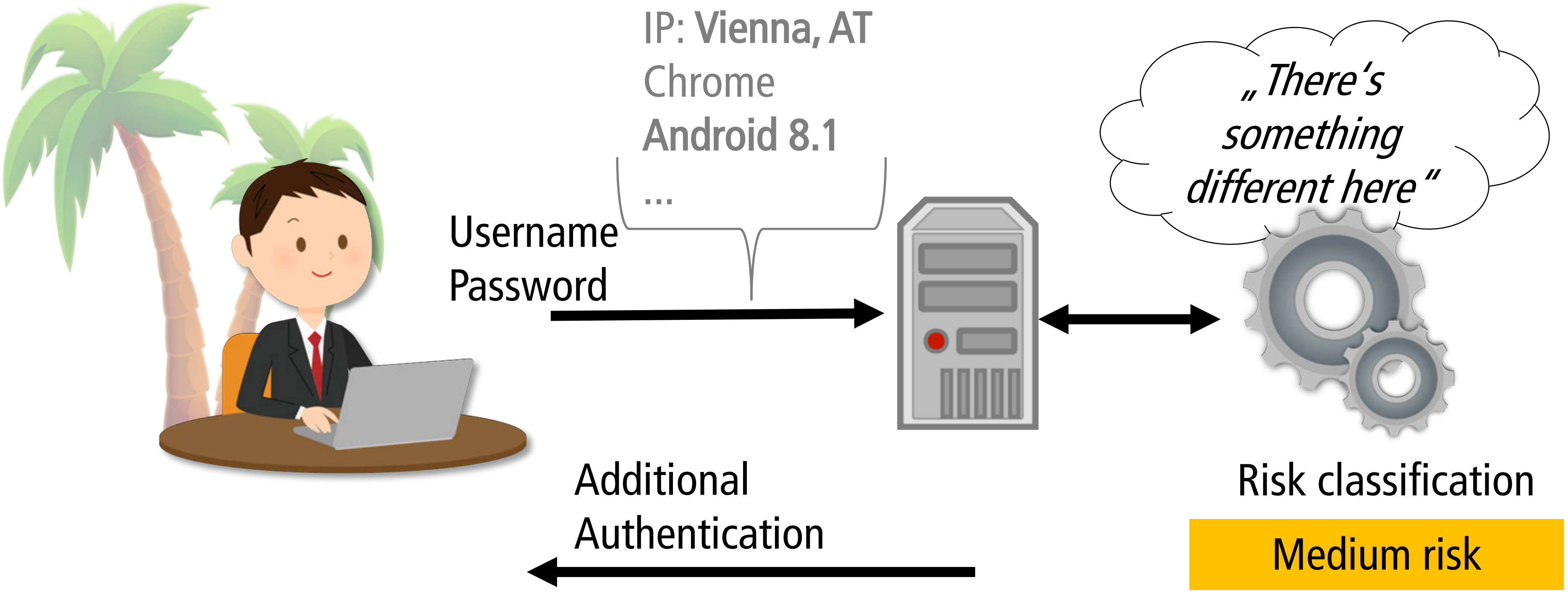
Risk classification

Low risk



IP: **Vienna, AT**
Chrome
Android 8.1
…

Username
Password



IP: **Vienna, AT**
Chrome
Android 8.1
…

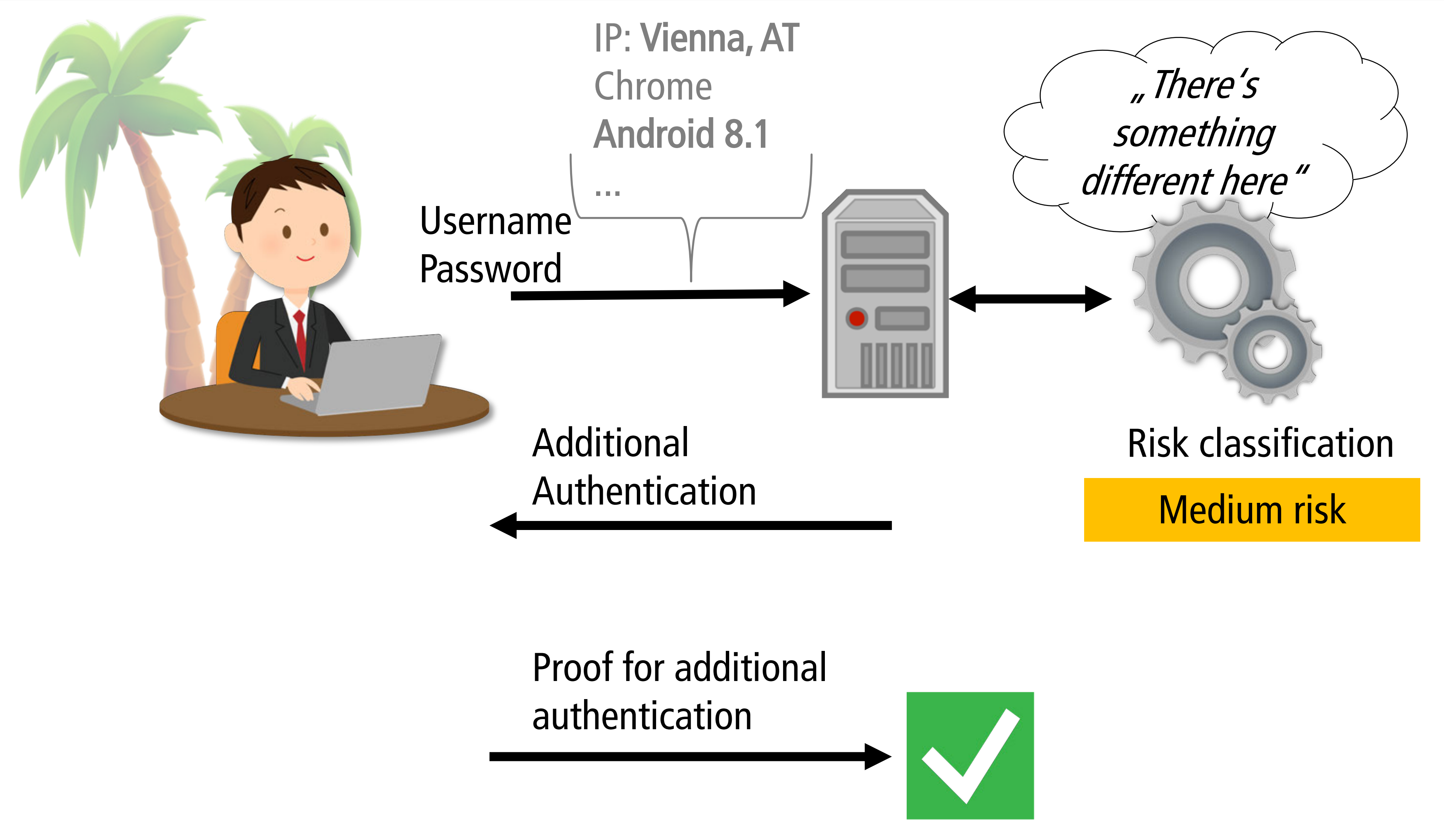
Username
Password

„There's something different here"

Risk classification

Medium risk

Additional Authentication



IP: **Vienna, AT**
Chrome
Android 8.1
…

Username
Password

„There's something different here"

Risk classification

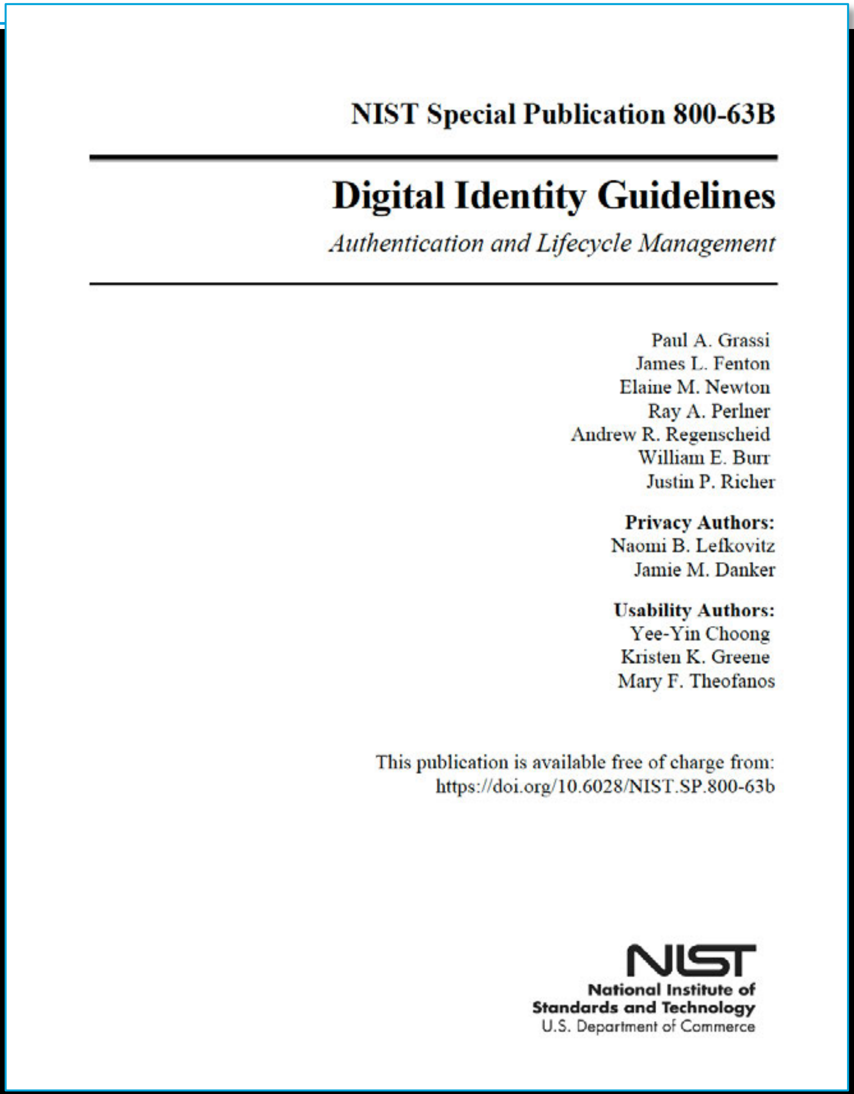
Medium risk

Additional Authentication

Proof for additional authentication

Risk-based Authentication

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



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

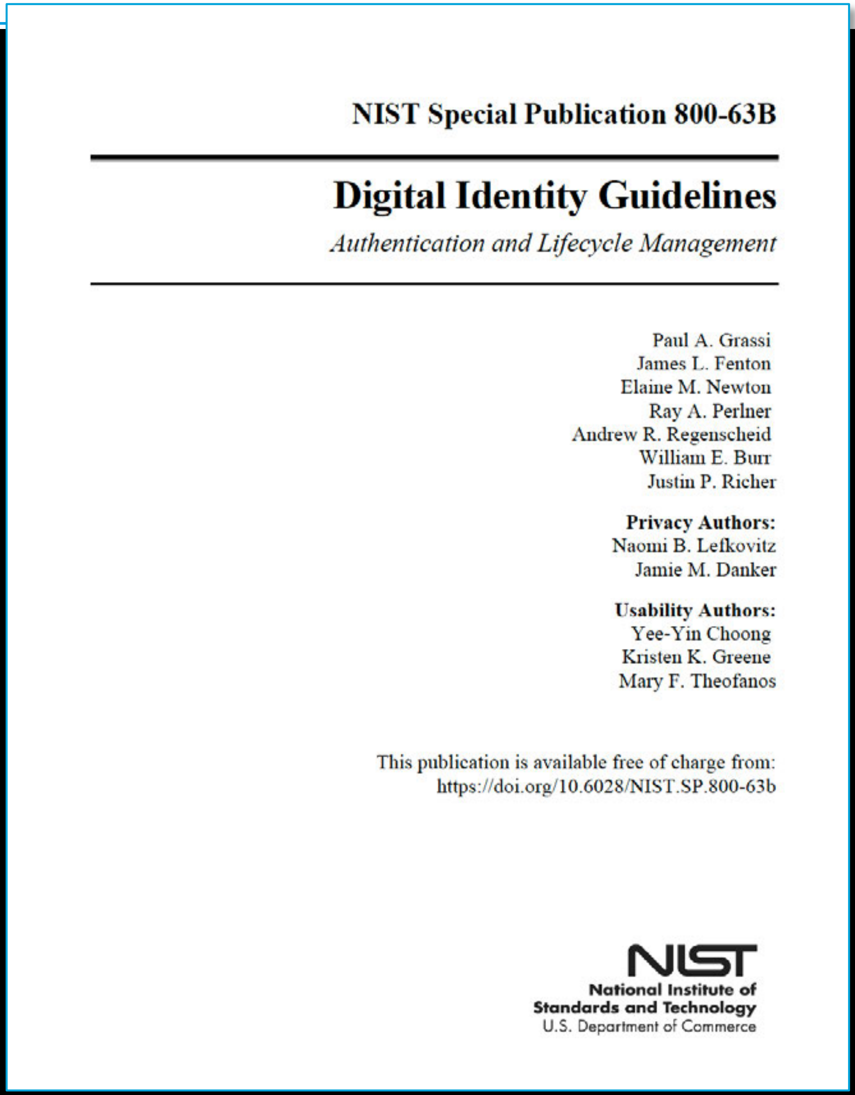
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63b

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)
[2| NCSC: Cloud security guidance: 10, Identity and authentication (2018)

Risk-based Authentication

- Recommended by NIST[1] and NCSC[2]
- More usable than comparable 2FA methods with high security[3,4]



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

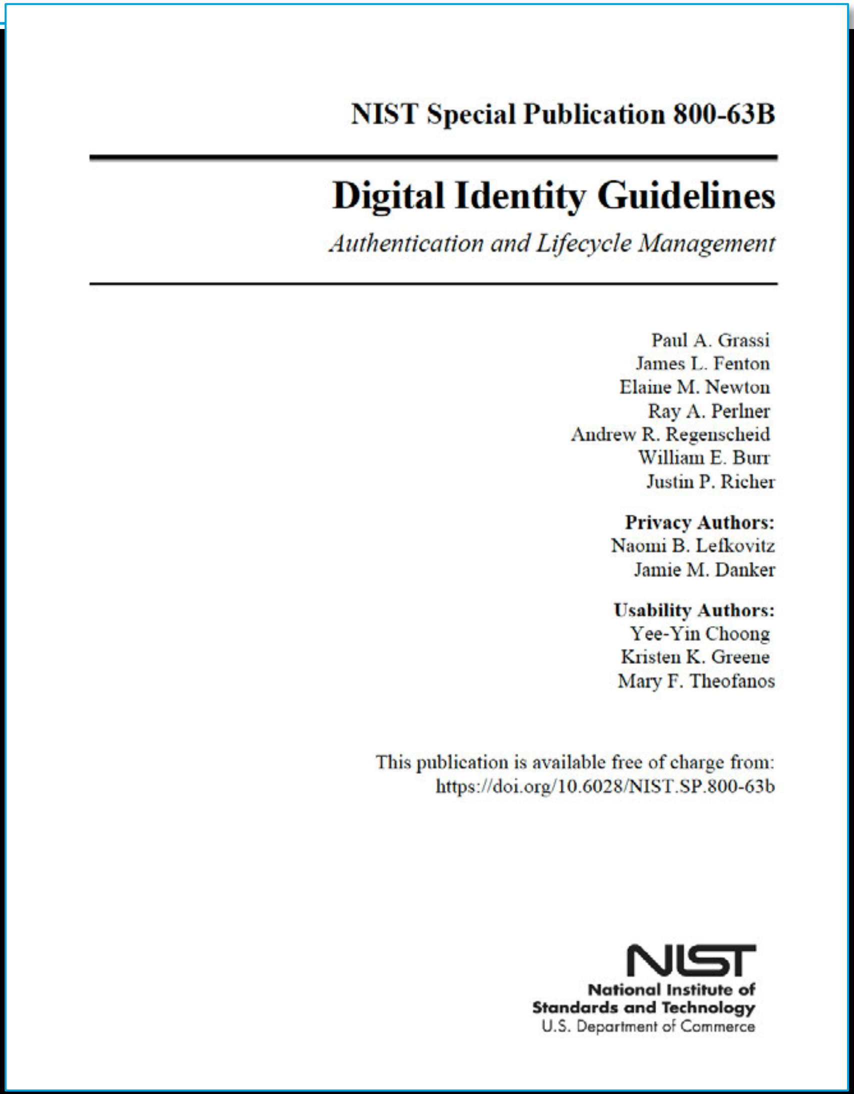
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

[1] Grassi et al.: Digital identity guidelines. Tech. Rep. NIST SP 800-63b (2017)
[2] NCSC: Cloud security guidance: 10, Identity and authentication (2018)
[3] Wiefling et al.: More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. In: ACSAC ’20. ACM (2020)
[4] Wiefling et al.: What’s in Score for Website Users: A Data-driven Long-term Study on Risk-based Authentication Characteristics. In: FC ’21. Springer (2021)

Risk-based Authentication

- Recommended by NIST[1] and NCSC[2]
- More usable than comparable 2FA methods with high security[3,4]
- But: Privacy Challenge

[1] Grassi et al.: Digital identity guidelines. Tech. Rep. NIST SP 800-63b (2017)
[2] NCSC: Cloud security guidance: 10, Identity and authentication (2018)
[3] Wiefling et al.: More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. In: ACSAC '20. ACM (2020)
[4] Wiefling et al.: What's in Score for Website Users: A Data-driven Long-term Study on Risk-based Authentication Characteristics. In: FC '21. Springer (2021)



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

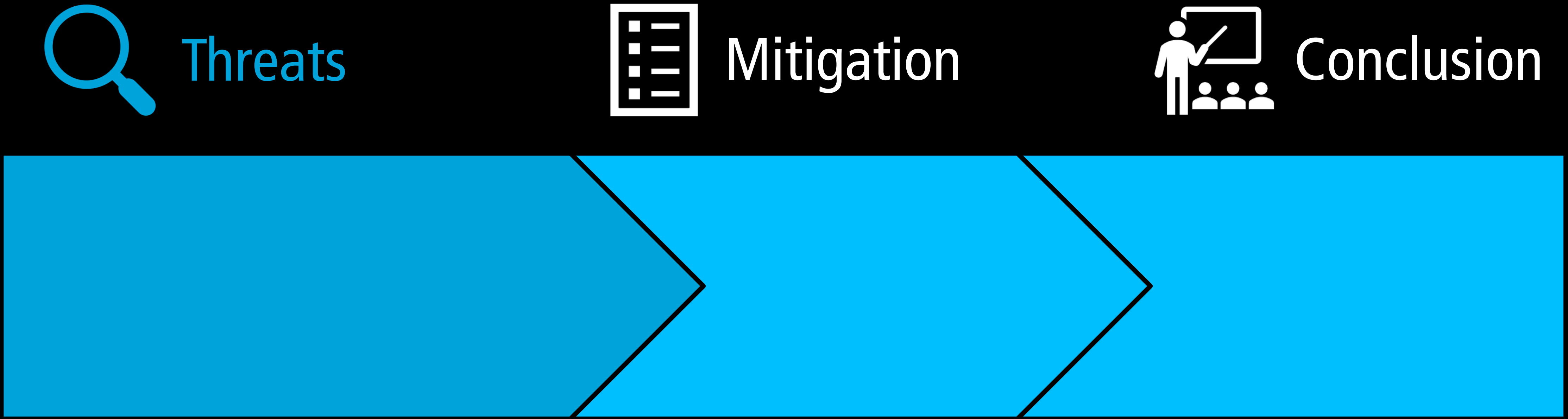
Overview

Threats

Mitigation

Conclusion

Overview

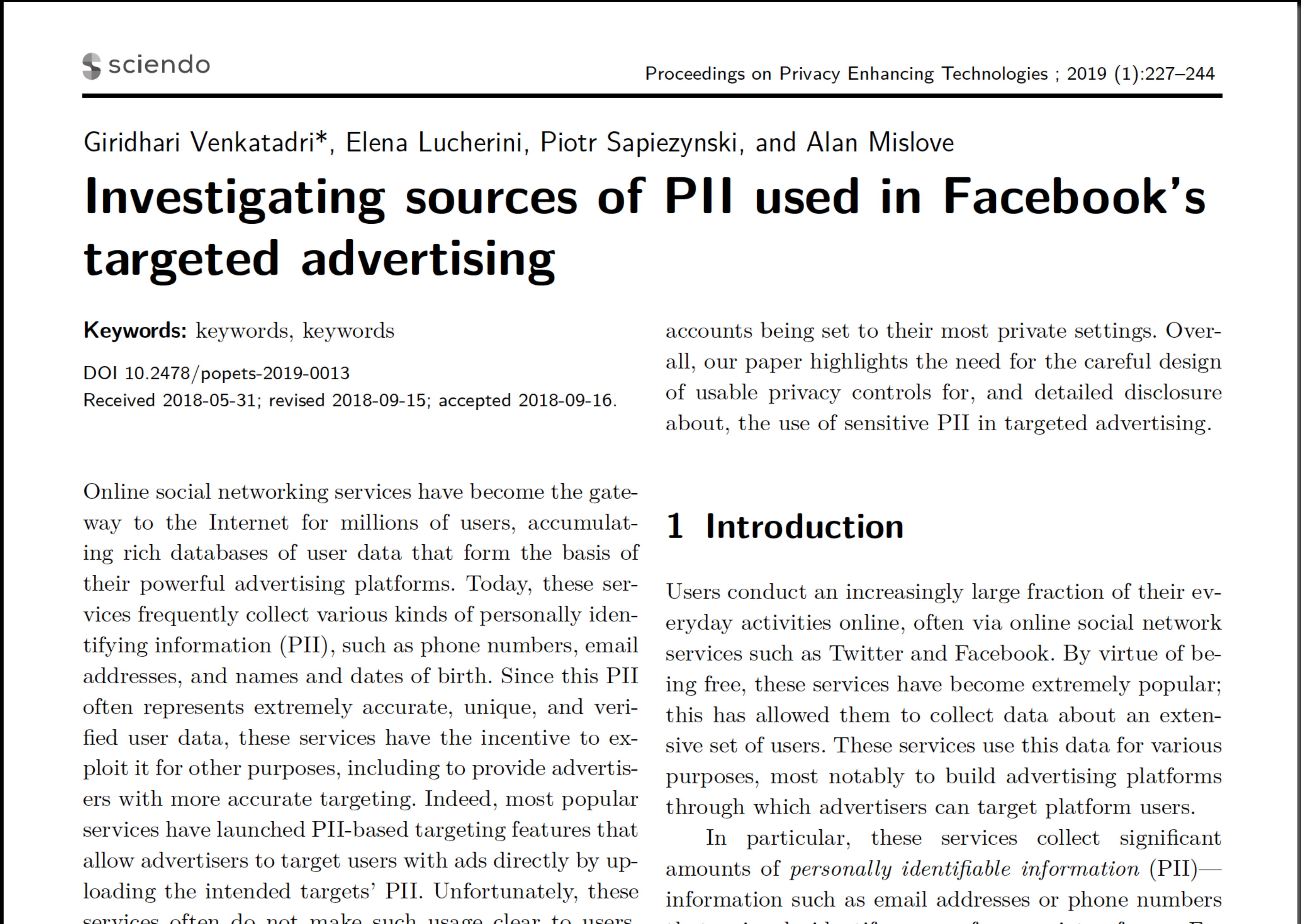


Threats

Mitigation

Conclusion

Data Misuse



sciendo Proceedings on Privacy Enhancing Technologies ; 2019 (1):227–244

Giridhari Venkatadri*, Elena Lucherini, Piotr Sapiezynski, and Alan Mislove

Investigating sources of PII used in Facebook's targeted advertising

Keywords: keywords, keywords

DOI 10.2478/popets-2019-0013
Received 2018-05-31; revised 2018-09-15; accepted 2018-09-16.

Online social networking services have become the gateway to the Internet for millions of users, accumulating rich databases of user data that form the basis of their powerful advertising platforms. Today, these services frequently collect various kinds of personally identifying information (PII), such as phone numbers, email addresses, and names and dates of birth. Since this PII often represents extremely accurate, unique, and verified user data, these services have the incentive to exploit it for other purposes, including to provide advertisers with more accurate targeting. Indeed, most popular services have launched PII-based targeting features that allow advertisers to target users with ads directly by uploading the intended targets' PII. Unfortunately, these services often do not make such usage clear to users

accounts being set to their most private settings. Overall, our paper highlights the need for the careful design of usable privacy controls for, and detailed disclosure about, the use of sensitive PII in targeted advertising.

1 Introduction

Users conduct an increasingly large fraction of their everyday activities online, often via online social network services such as Twitter and Facebook. By virtue of being free, these services have become extremely popular; this has allowed them to collect data about an extensive set of users. These services use this data for various purposes, most notably to build advertising platforms through which advertisers can target platform users.

In particular, these services collect significant amounts of *personally identifiable information* (PII)—information such as email addresses or phone numbers

Veenkatadri et al.: Investigating sources of PII used in Facebook's targeted advertising. PoPETS. 2019, 227–244 (2019).

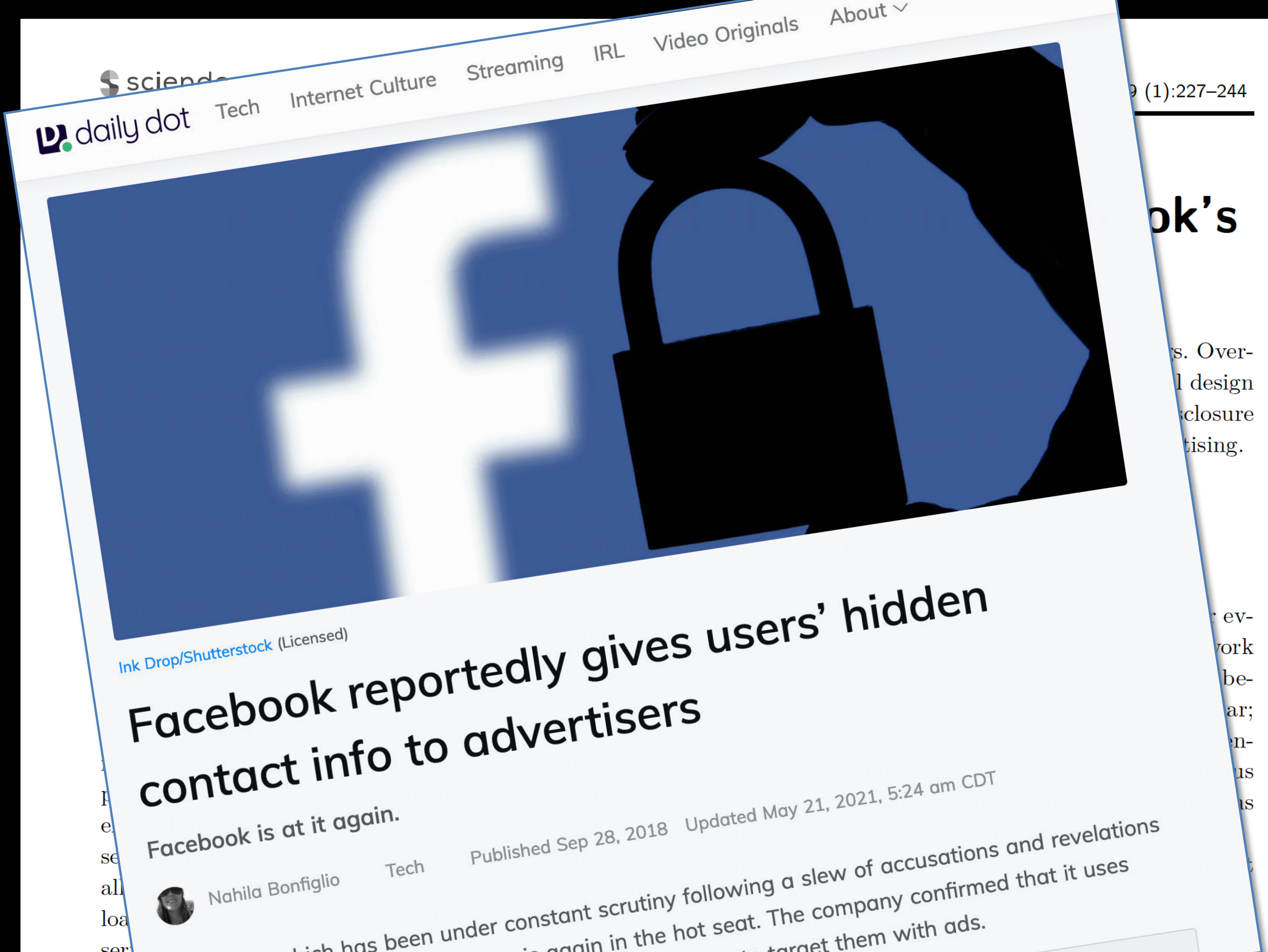
sciendo

9 (1):227–244

ok's

s. Over-
l design
sclosure
tising.

ev-
ork
be-
ar;
en-
us
us



Ink Drop/Shutterstock (Licensed)

Facebook reportedly gives users' hidden contact info to advertisers

Facebook is at it again.

Nahila Bonfiglio   Tech   Published Sep 28, 2018   Updated May 21, 2021, 5:24 am CDT

hich has been under constant scrutiny following a slew of accusations and revelations
is again in the hot seat. The company confirmed that it uses
target them with ads.

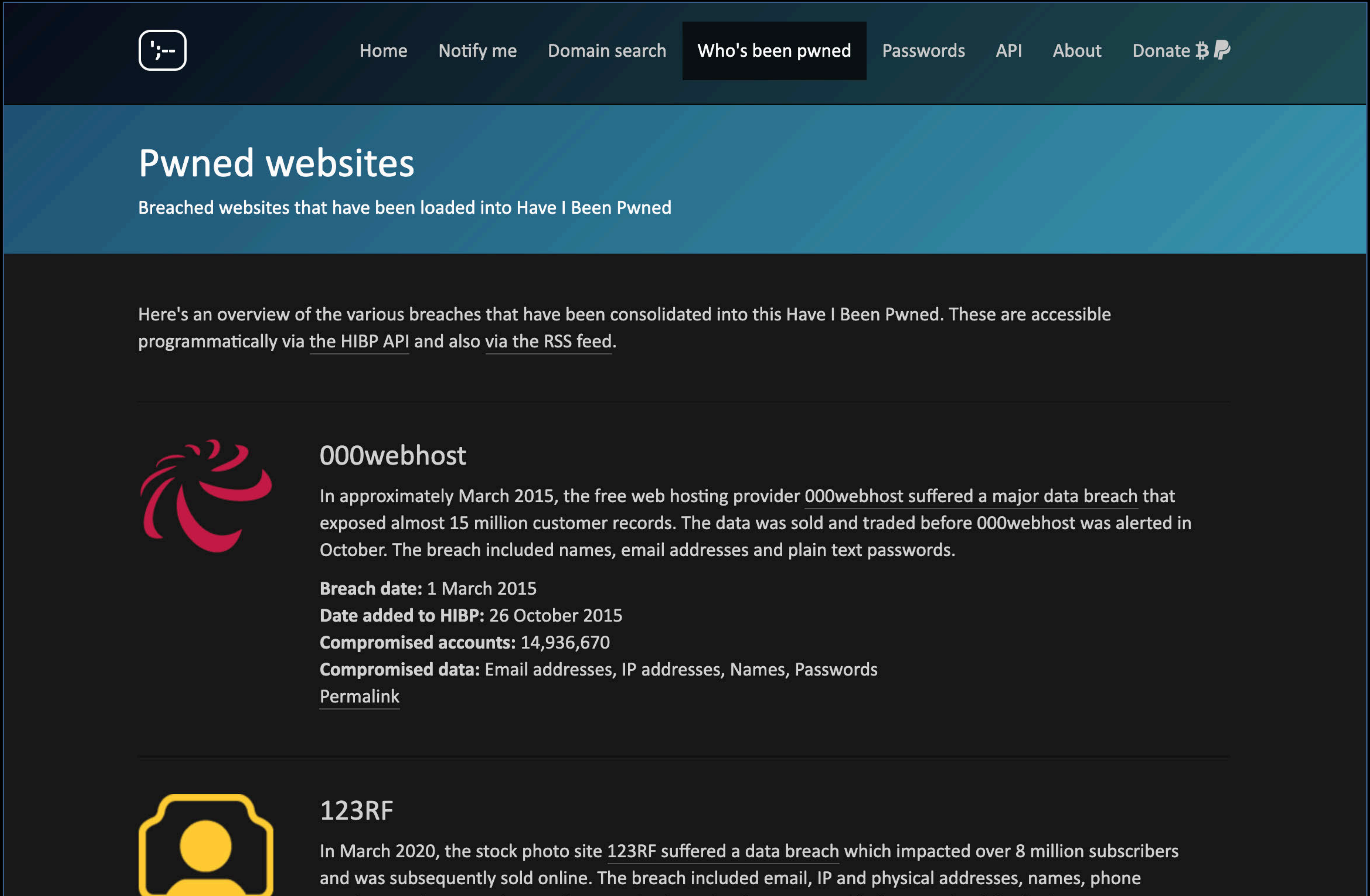
https://www.dailydot.com/debug/facebook-two-factor-authentication-ads/

Data Forwarding

Data Forwarding

e.g., to state actors,
advertising networks

Data Breach



Pwned websites

Breached websites that have been loaded into Have I Been Pwned

Here's an overview of the various breaches that have been consolidated into this Have I Been Pwned. These are accessible programmatically via the HIBP API and also via the RSS feed.

000webhost

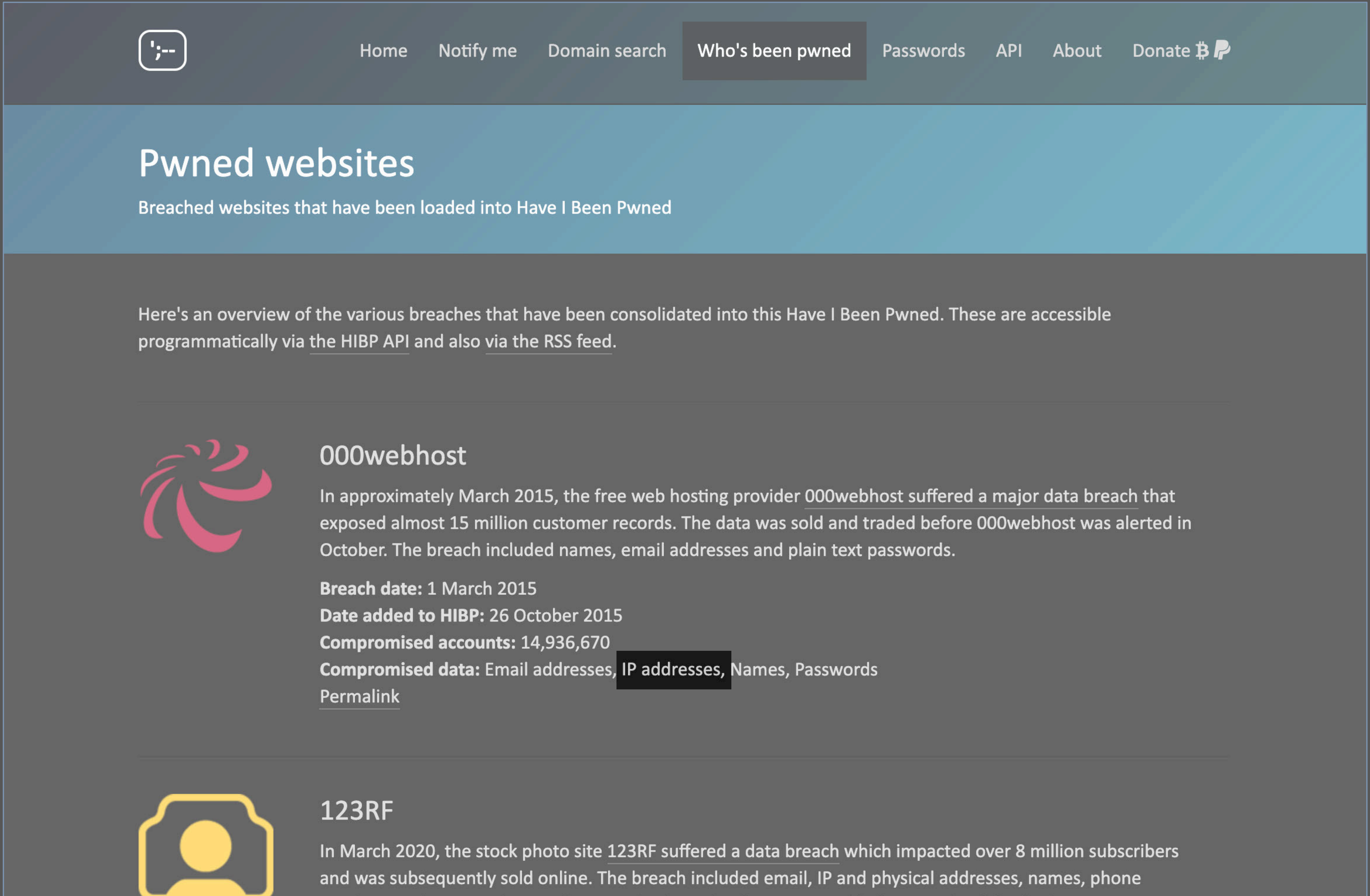
In approximately March 2015, the free web hosting provider 000webhost suffered a major data breach that exposed almost 15 million customer records. The data was sold and traded before 000webhost was alerted in October. The breach included names, email addresses and plain text passwords.

Breach date: 1 March 2015
Date added to HIBP: 26 October 2015
Compromised accounts: 14,936,670
Compromised data: Email addresses, IP addresses, Names, Passwords
Permalink

123RF

In March 2020, the stock photo site 123RF suffered a data breach which impacted over 8 million subscribers and was subsequently sold online. The breach included email, IP and physical addresses, names, phone

https://haveibeenpwned.com/PwnedWebsites



Pwned websites

Breached websites that have been loaded into Have I Been Pwned

Here's an overview of the various breaches that have been consolidated into this Have I Been Pwned. These are accessible programmatically via the HIBP API and also via the RSS feed.

000webhost

In approximately March 2015, the free web hosting provider 000webhost suffered a major data breach that exposed almost 15 million customer records. The data was sold and traded before 000webhost was alerted in October. The breach included names, email addresses and plain text passwords.

Breach date: 1 March 2015
Date added to HIBP: 26 October 2015
Compromised accounts: 14,936,670
Compromised data: Email addresses, IP addresses, Names, Passwords
Permalink

123RF

In March 2020, the stock photo site 123RF suffered a data breach which impacted over 8 million subscribers and was subsequently sold online. The breach included email, IP and physical addresses, names, phone

https://haveibeenpwned.com/PwnedWebsites

Overview

Threats

Mitigation

Conclusion

RBA Model*

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

RBA Model*

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

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

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

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

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

Aggregating

Feature Value
A
B
C
A
C
B

Feature Value
A
B
C
A
C
B

→

Feature Value
A
A
B
B
C
C

Feature Value
A
B
C
A
C
B

→

Feature Value
A
A
B
B
C
C

$$Score_{user}(FV) = 0.2$$

$$Score_{user}(FV) = 0.2$$

Hashing

$$H(192.168.1.166 \,||\, salt) = 243916 \ldots aad132$$

$$H(192.168.1.166\,||\,salt) = 243916\ldots aad132$$

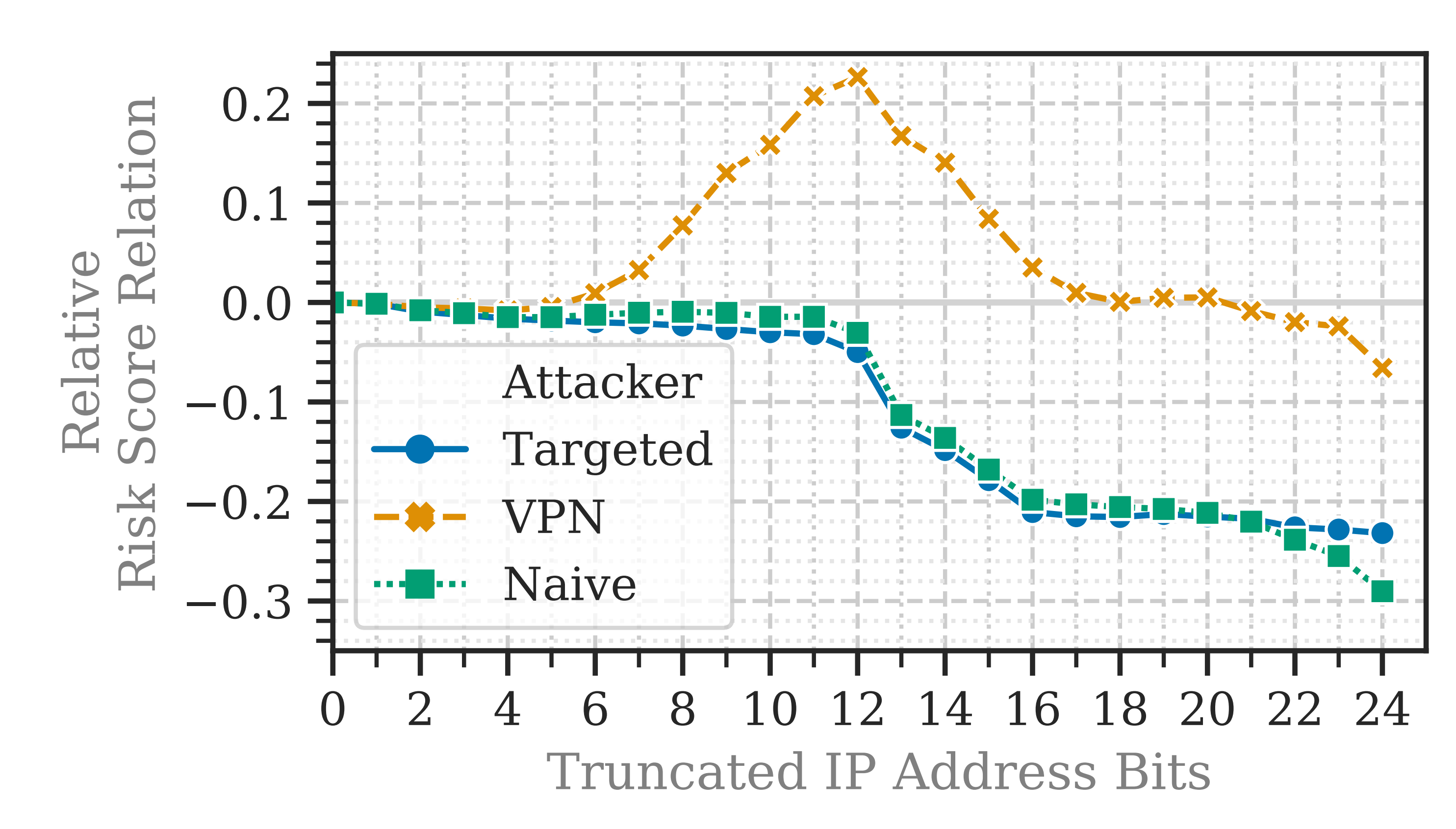
Identical risk score

Truncation

$$Truncate(192.168.1.166, 8\ Bit) = 192.168.1.0$$

$$Truncate(192.168.1.166, 8\,Bit) = 192.168.1.0$$

Different risk score!



Attackers and legitimate users harder to distinguish when truncating

k-Anonymity

User	Feature Value
1	A
2	B
3	B

User	Feature Value
1	A
2	B
3	B

User	Feature Value
1	A
2	B
3	B

→

User	Feature Value
1	A
2	B
3	B
4	A

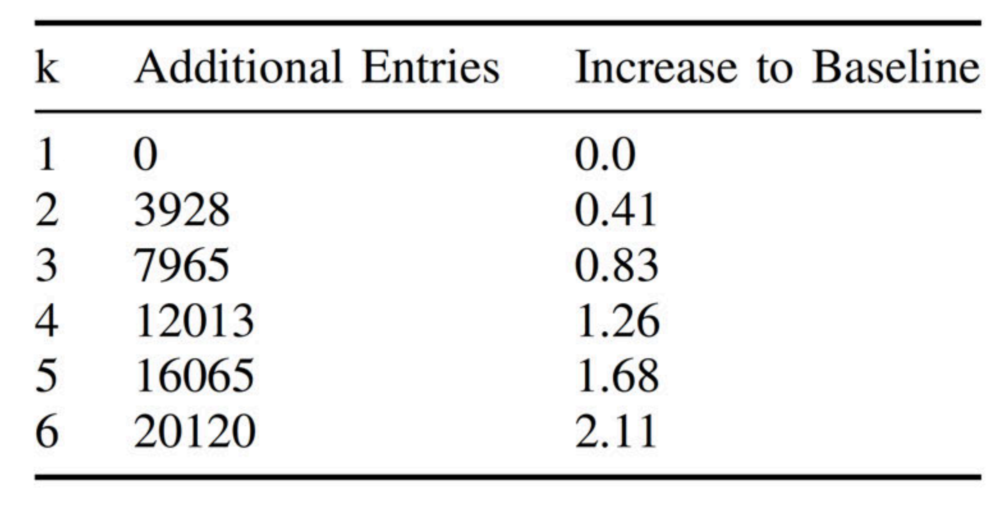
$$k = 2$$

User	Feature Value
1	A
2	B
3	B

User	Feature Value
1	A
2	B
3	B
4	A

Different risk score!

$$k = 2$$



k	Additional Entries	Increase to Baseline
1	0	0.0
2	3928	0.41
3	7965	0.83
4	12013	1.26
5	16065	1.68
6	20120	2.11

Produces overhead

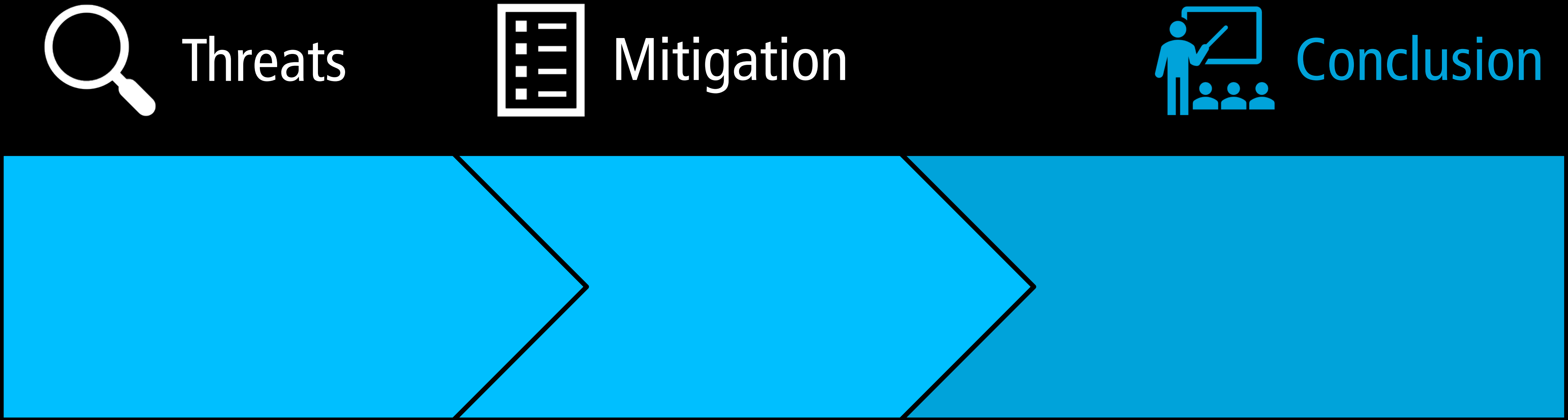
Login History Minimization

Remove entries after n months

Remove entries after n months

Different risk score?

Overview



Threats

Mitigation

Conclusion

Conclusion

Conclusion

- Indications that RBA implementations can be designed more privacy friendly

Conclusion

- Indications that RBA implementations can be designed more privacy friendly

- IP address is still sensitive feature. Replacing with server-originated Round-Trip Time* possible?

*Wiefling et al.: What's in Score for Website Users: A Data-driven Long-term Study on Risk-based Authentication Characteristics. In: FC '21. Springer (2021)

Conclusion

- Indications that RBA implementations can be designed more privacy friendly

- IP address is still sensitive feature. Replacing with server-originated Round-Trip Time* possible?

- Research Directions:
  More/Other features, Login History Minimization

*Wiefling et al.: What’s in Score for Website Users: A Data-driven Long-term Study on Risk-based Authentication Characteristics. In: FC ’21. Springer (2021)

Thank you

riskbasedauthentication.org
das.h-brs.de

stephan.wiefling@h-brs.de

@swiefling