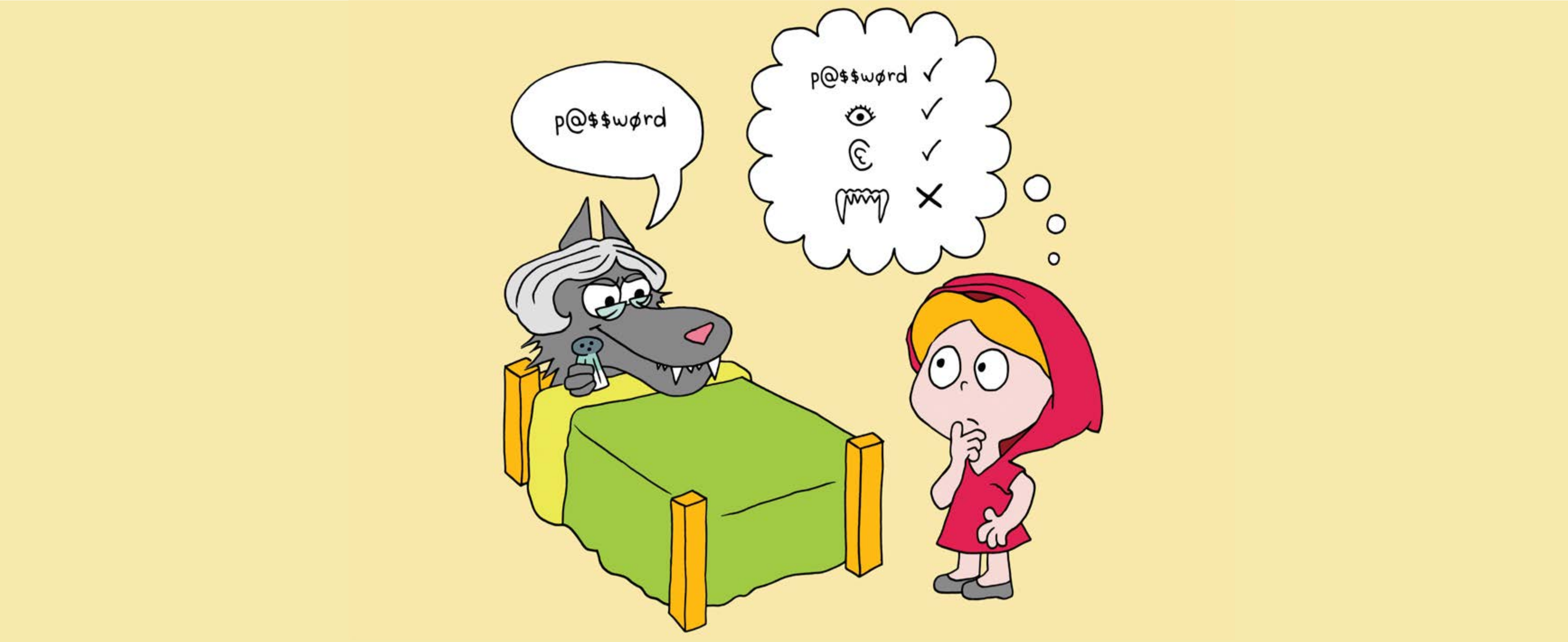
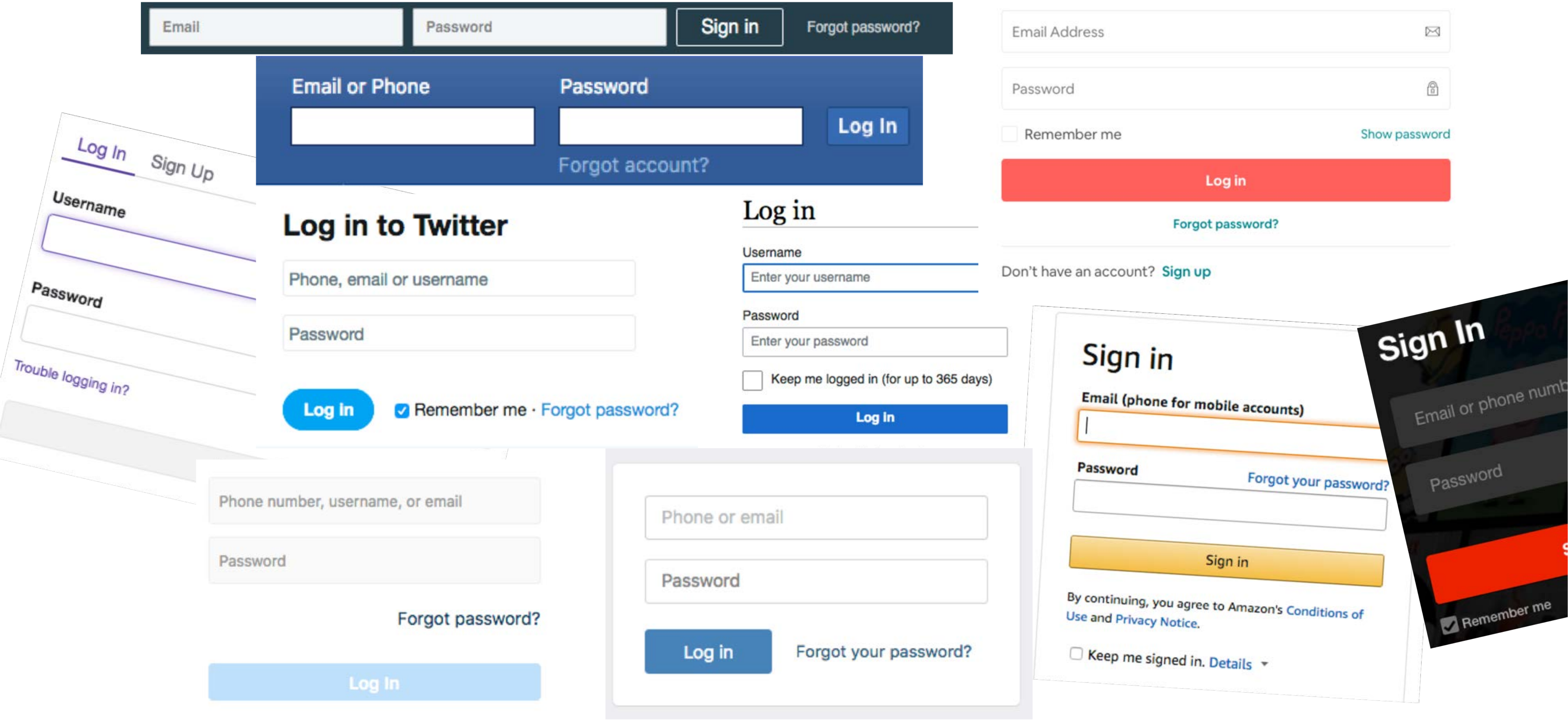


Image: Iwona Usakiewicz / Andrij Borys Associates
Bonneau et al.: Passwords and the evolution of imperfect authentication. Comm. ACM 58(7) (Jun 2015)

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

Stephan Wiefling, Luigi Lo Iacono – TH Köln – University of Applied Sciences
Markus Dürmuth – Ruhr University Bochum

Lisbon, Portugal | IFIPSEC 2019


Email
Password
Sign in
Forgot password?
Email or Phone
Password
Log In
Forgot account?
Email Address
Password
Remember me
Show password
Log in
Forgot password?
Don't have an account? Sign up
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
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 numb
Password
☑ Remember me
Phone number, username, or email
Password
Forgot password?
Log In
Phone or email
Password
Log in
Forgot your password?

Motivation

- Weaknesses in password-based authentication increase
  - Large-scale password database leaks
    - Credential Stuffing
  - Intelligent password guessing*
  - Phishing

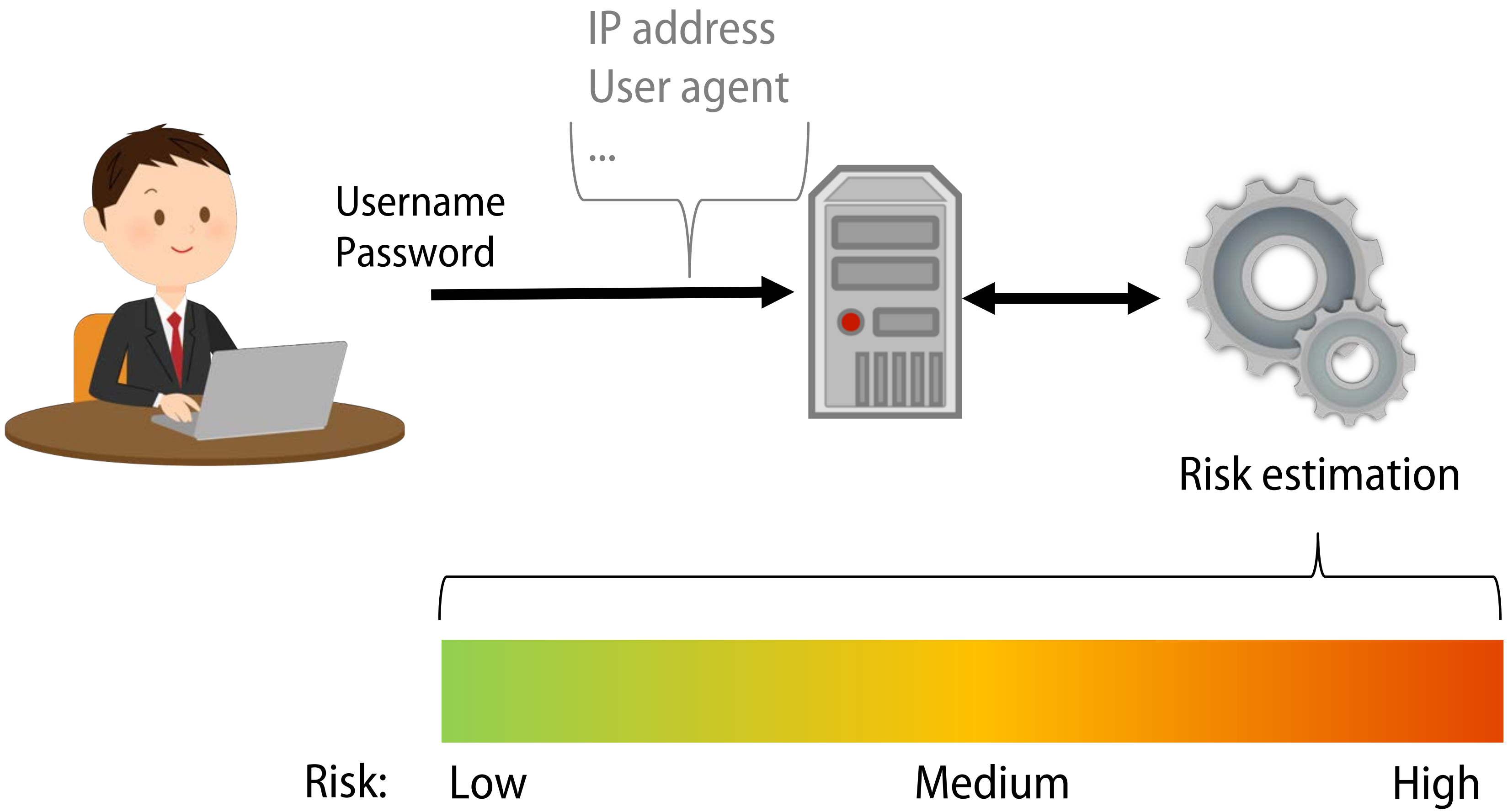
*Wang et al.: Targeted online password guessing: An underestimated threat. In CCS ’16. ACM (2016)

Motivation

- 2FA is unpopular
  - <10% of all Google accounts used 2FA in January 2018*

→ Using Risk-based Authentication
to increase account security
with minimal impact on user interaction

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

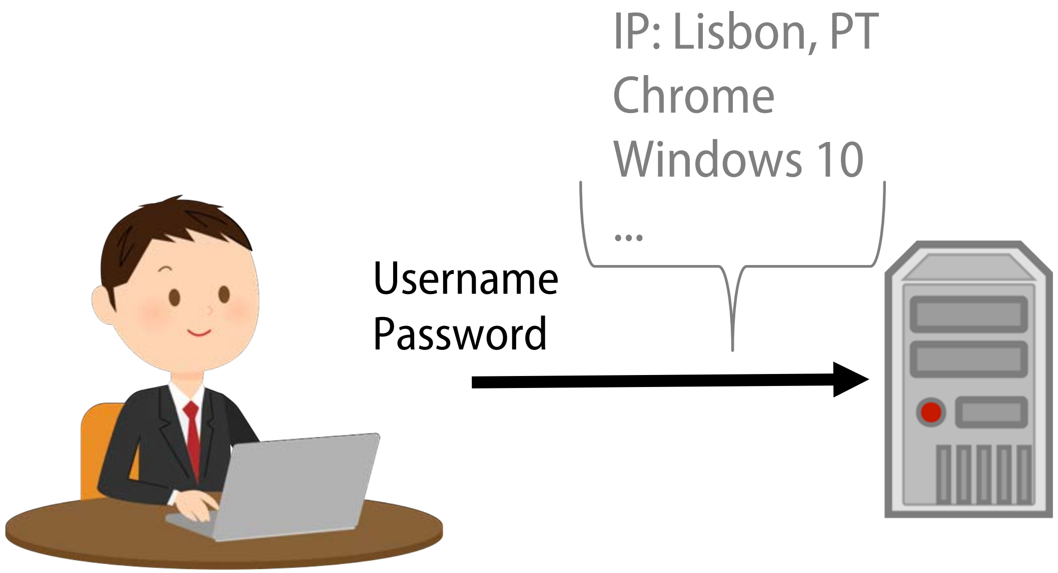


IP address
User agent
...

Username
Password

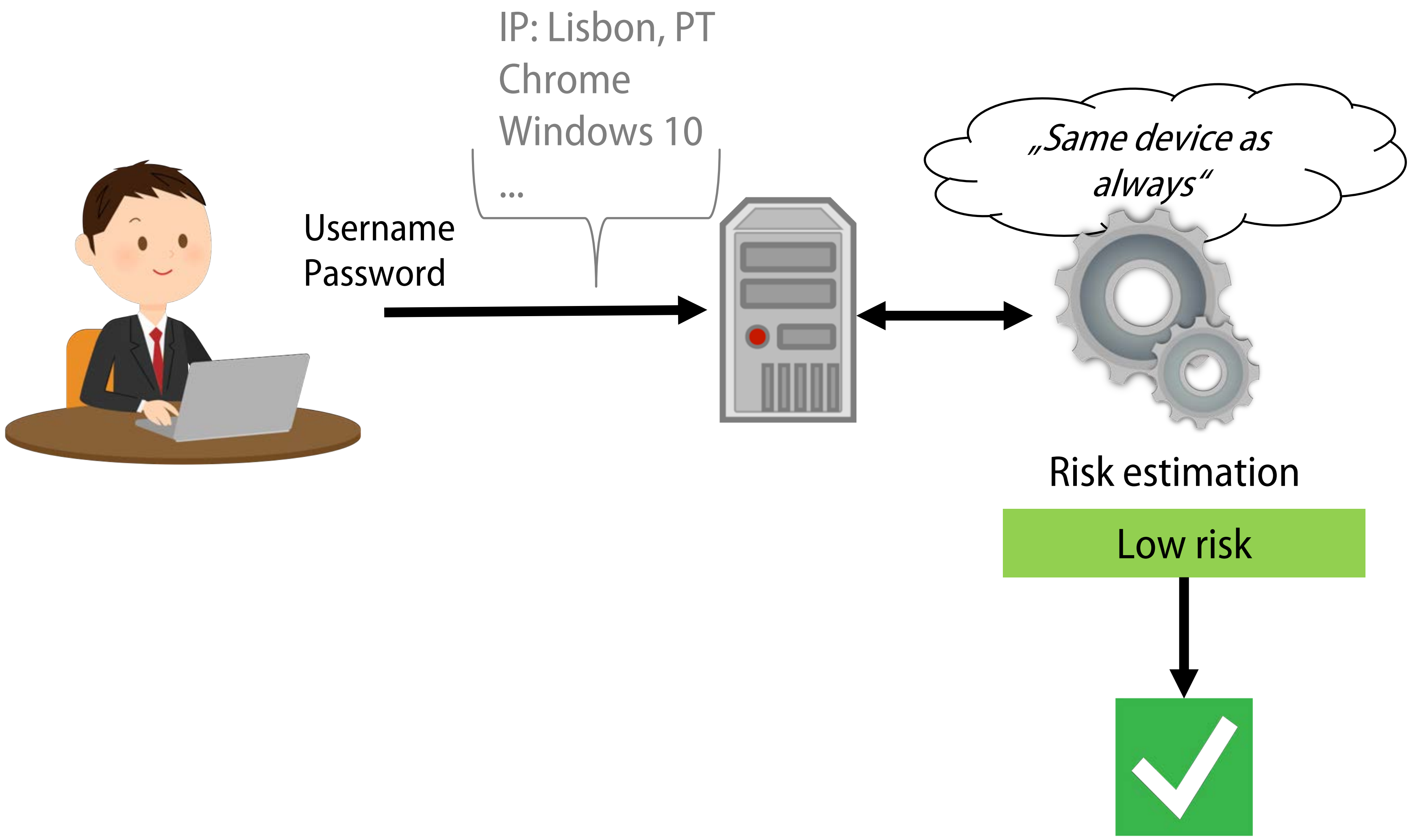
Risk estimation

Risk: Low Medium High



IP: Lisbon, PT
Chrome
Windows 10
...

Username
Password



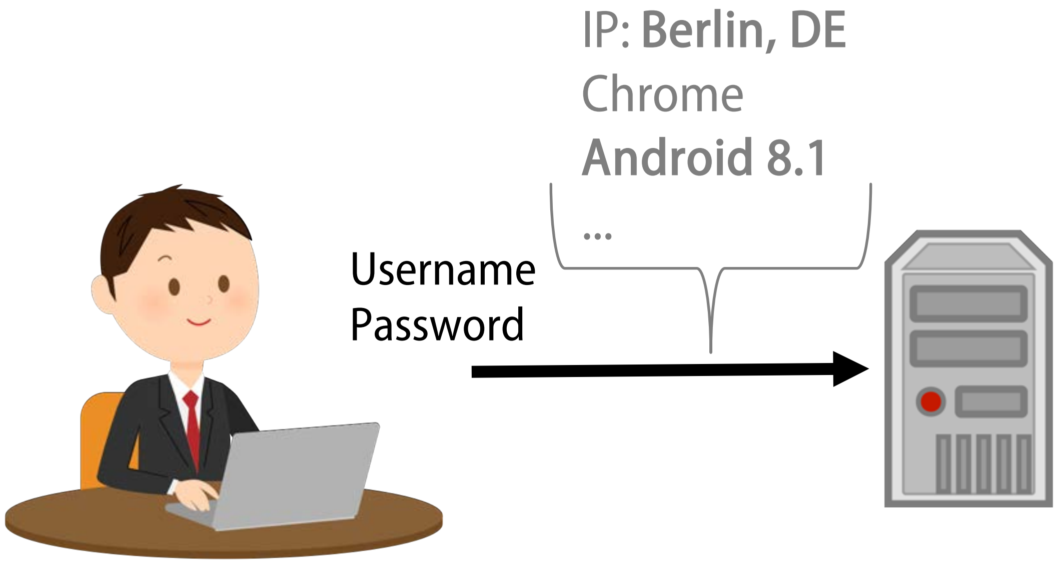
Username
Password

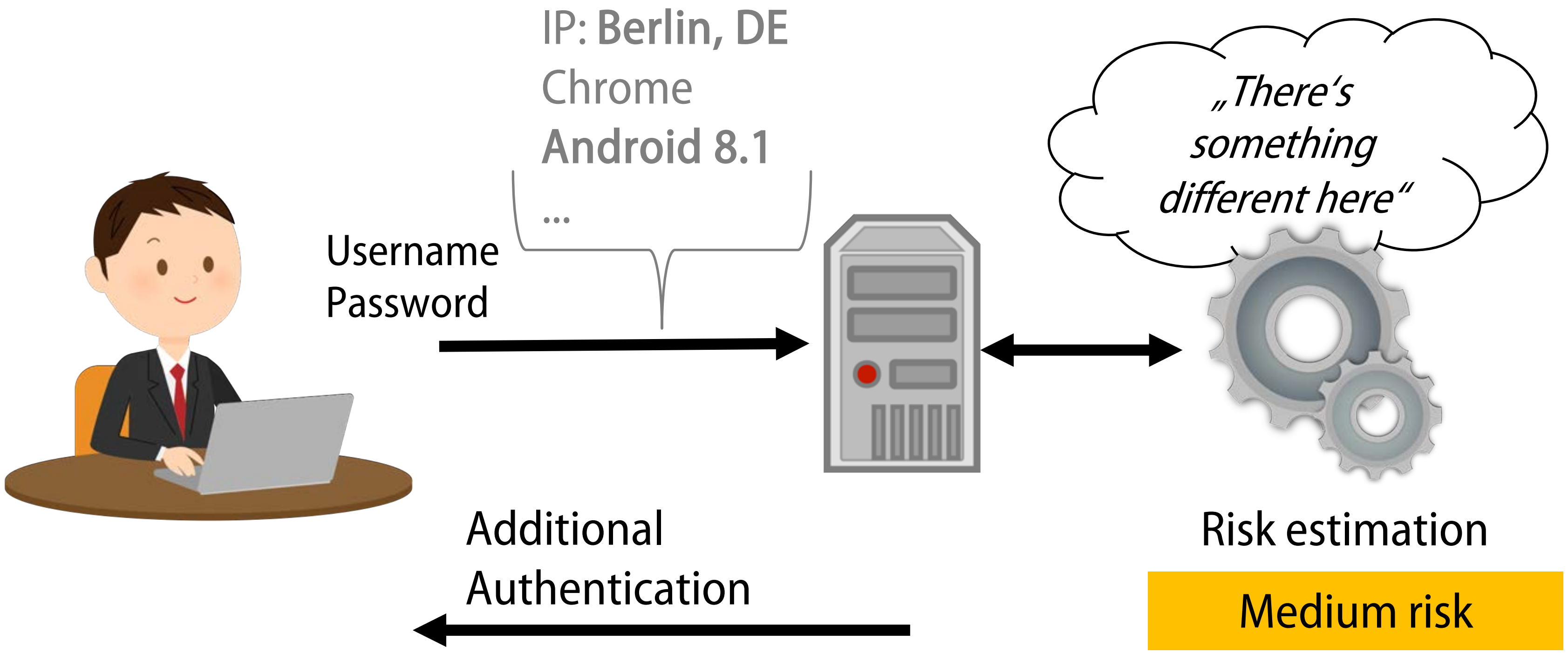
IP: Lisbon, PT
Chrome
Windows 10
...

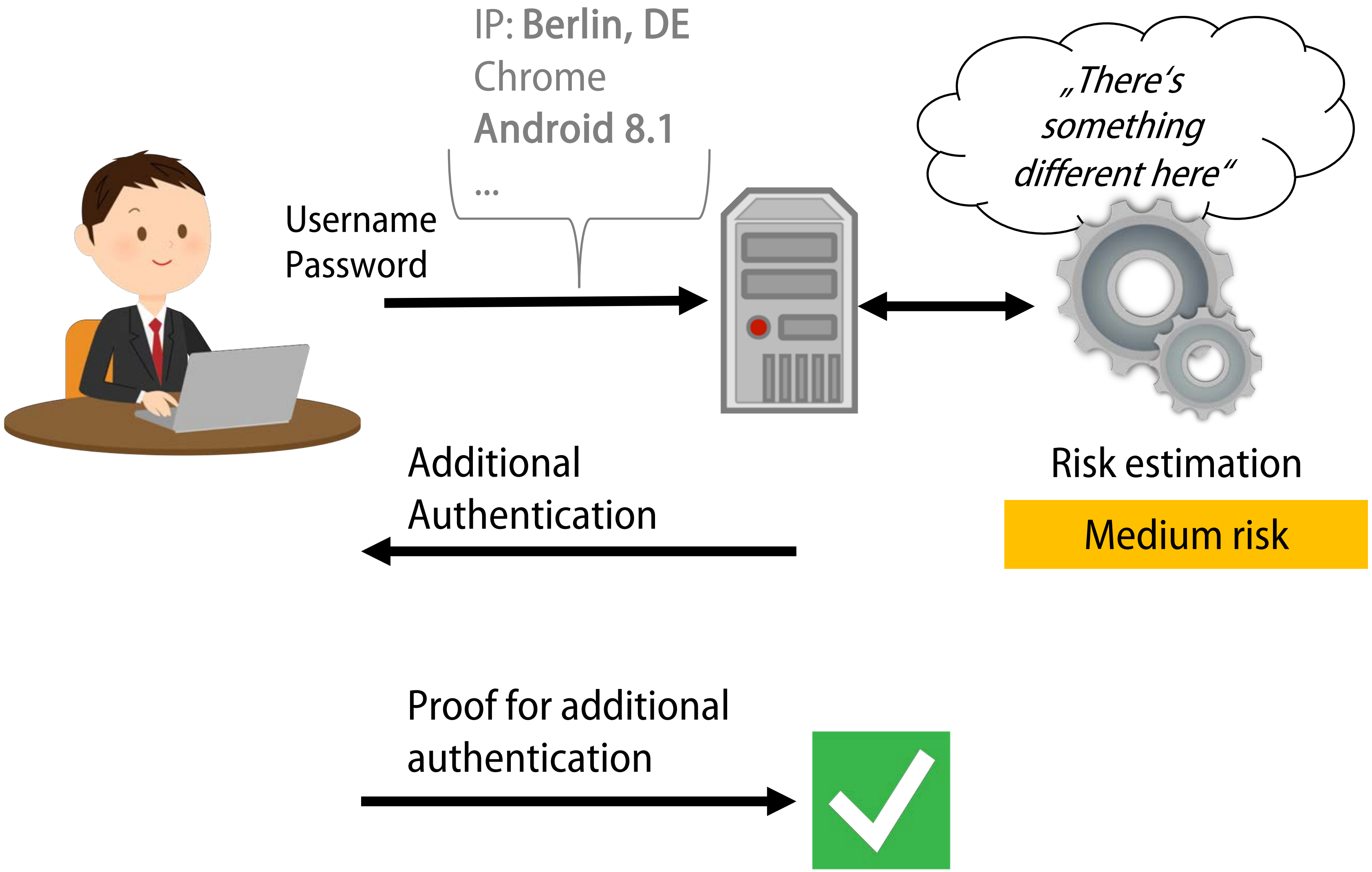
„Same device as always“

Risk estimation

Low risk


IP: **Berlin, DE**
Chrome
Android 8.1
...
Username
Password


IP: **Berlin, DE**
Chrome
Android 8.1
...
Username
Password
„There's something different here"
Risk estimation
Medium risk
Additional Authentication



IP: **Berlin, DE**

Chrome

Android 8.1

…

Username
Password

„There's something different here"

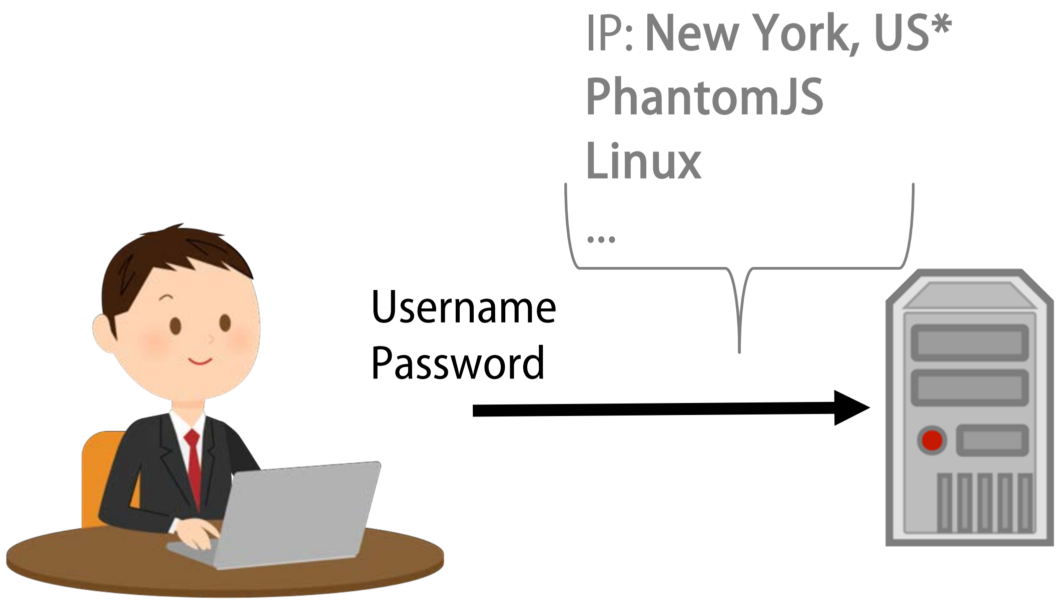
Additional Authentication

Risk estimation

Medium risk

Proof for additional authentication

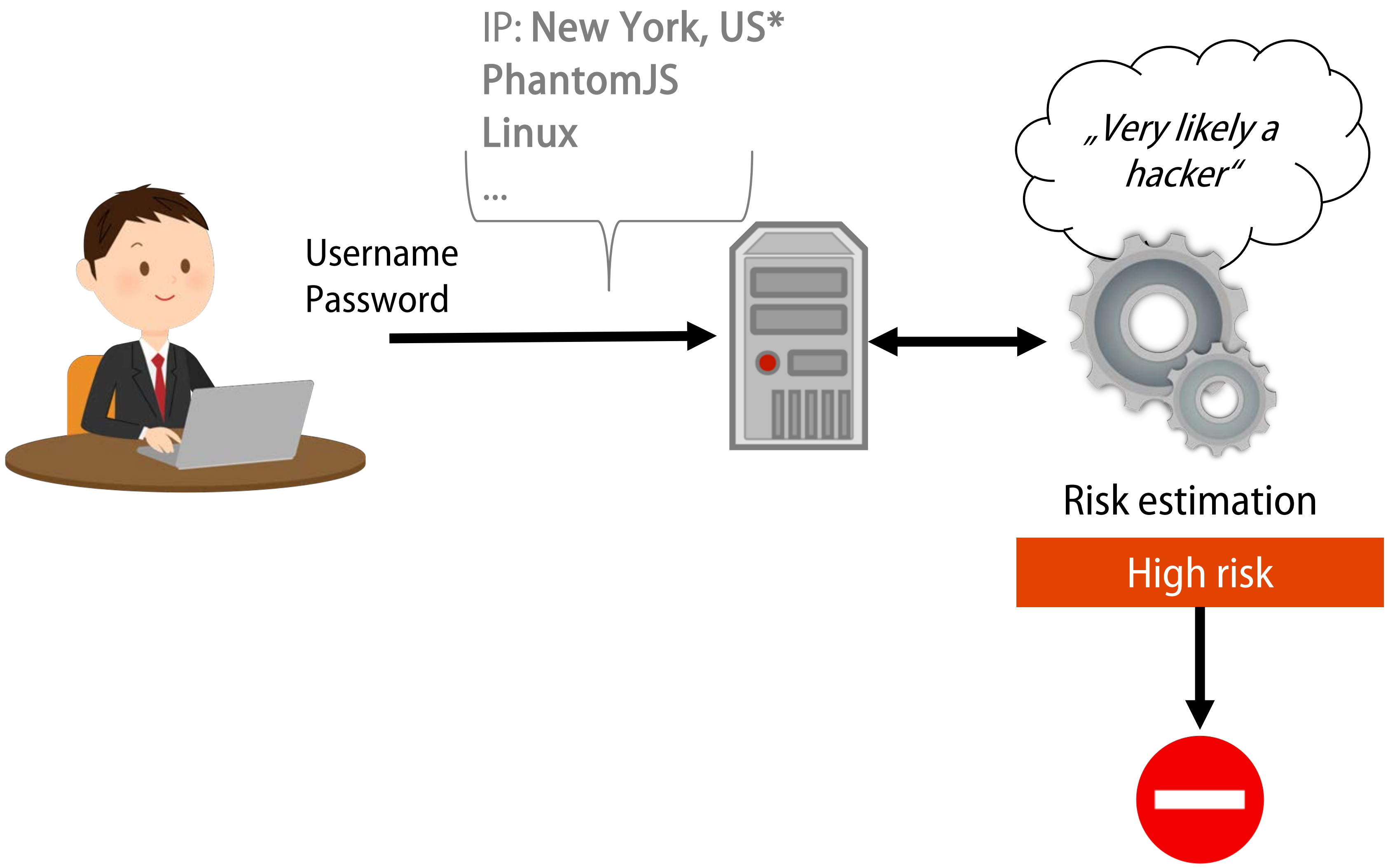
✓



IP: New York, US*
PhantomJS
Linux
...

Username
Password

*Known spam IP address



IP: New York, US*
PhantomJS
Linux
...

Username
Password

„Very likely a hacker“

Risk estimation

High risk

*Known spam IP address

Risk-based Authentication

- Recommended by NIST digital identity guidelines*
- Used by large online services
- However: Procedures not disclosed

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

Risk-based Authentication

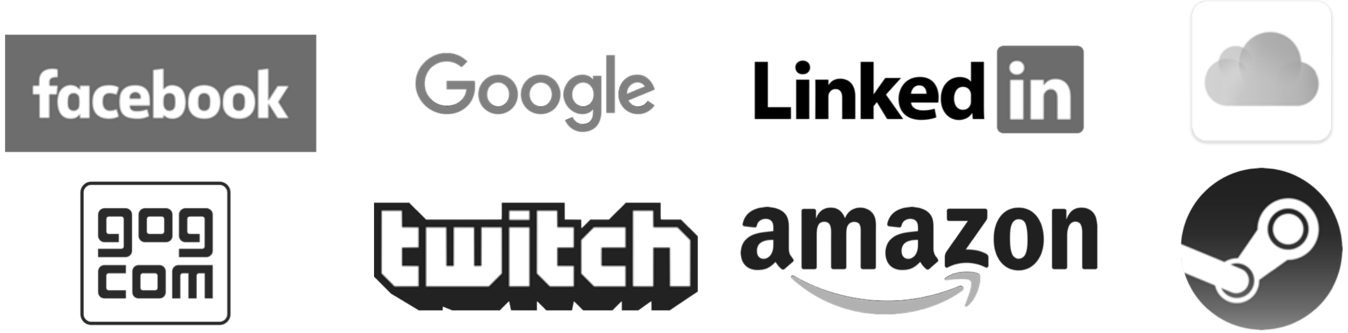
- Recommended by NIST digital identity guidelines*
- Used by large online services
- However: Procedures not disclosed
  - Prevents widespread adoption

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

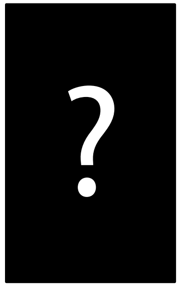
Risk-based Authentication

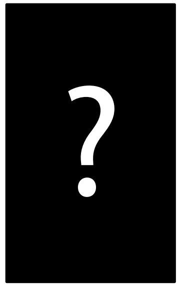
- Recommended by NIST digital identity guidelines*
- Used by large online services
- However: Procedures not disclosed

→ Black-box testing eight popular online services

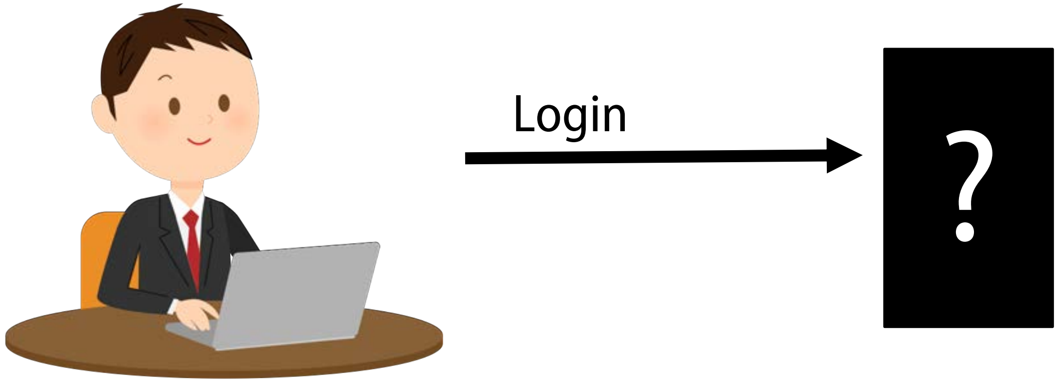


*Grassi et al.: Digital identity guidelines. Tech. Rep. NIST SP 800-63b (2017)

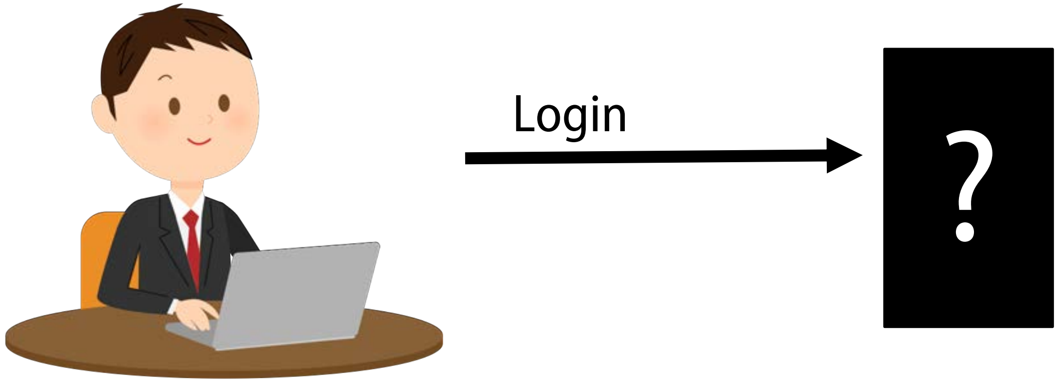




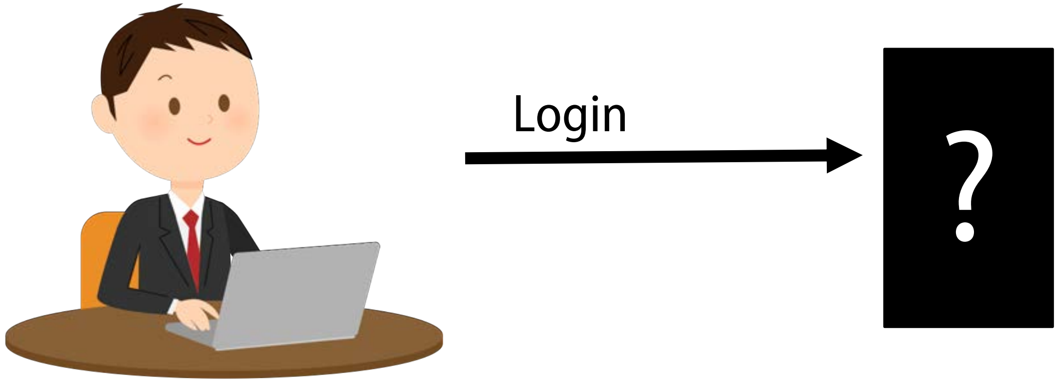
Login	IP address	User Agent	...



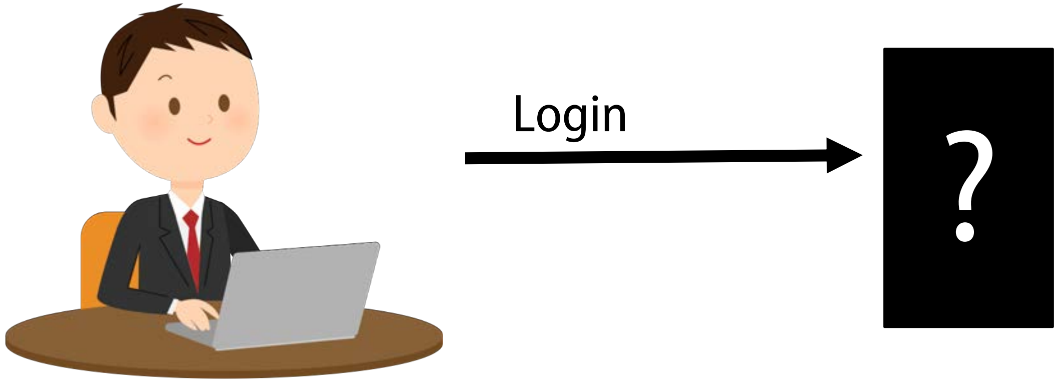
Login	IP address	User Agent	...
1	TH Köln	Chrome	...



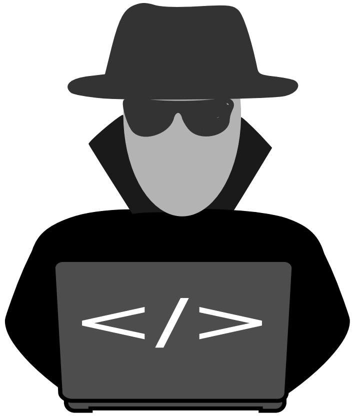
Login	IP address	User Agent	...
1	TH Köln	Chrome	...
2	TH Köln	Chrome	...

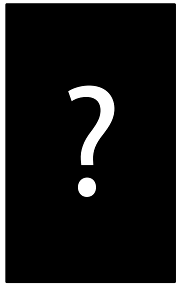


Login	IP address	User Agent	...
1	TH Köln	Chrome	...
2	TH Köln	Chrome	...
3	TH Köln	Chrome	...

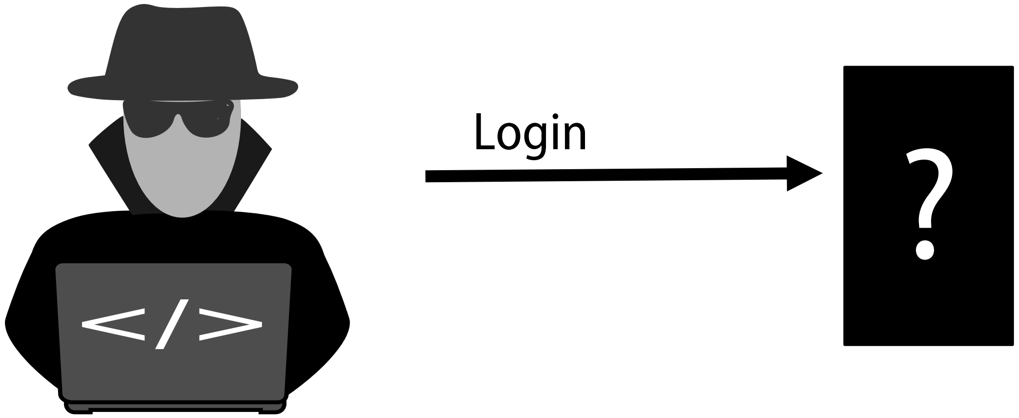


Login	IP address	User Agent	...
1	TH Köln	Chrome	...
2	TH Köln	Chrome	...
3	TH Köln	Chrome	...
...	...	...	....
20	TH Köln	Chrome	...

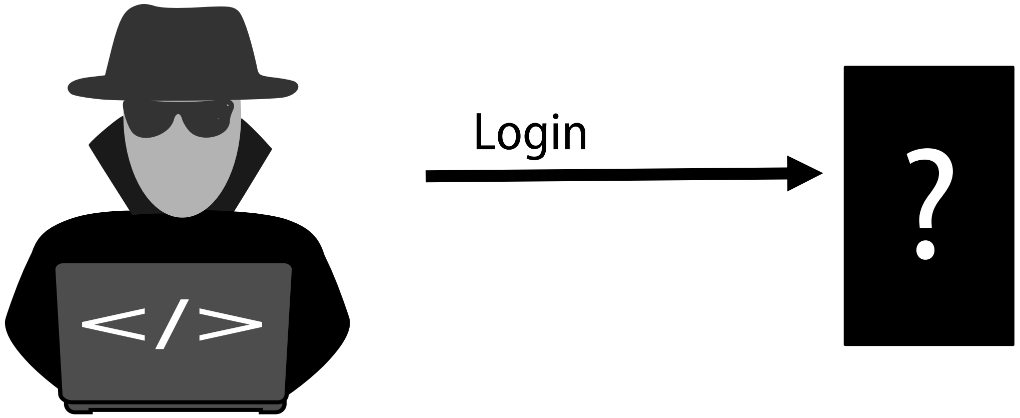




Login	IP address	User Agent	...
1	TH Köln	Chrome	...
2	TH Köln	Chrome	...
3	TH Köln	Chrome	...
...	...	...	....
20	TH Köln	Chrome	...



Login	IP address	User Agent	...
1	TH Köln	Chrome	...
2	TH Köln	Chrome	...
3	TH Köln	Chrome	...
...	...	...	....
20	TH Köln	Chrome	...
21	**Other Country**	Chrome	...



✅, 🟨 or ⛔?

Login	IP address	User Agent	...
1	TH Köln	Chrome	...
2	TH Köln	Chrome	...
3	TH Köln	Chrome	...
...	...	...	....
20	TH Köln	Chrome	...
21	**Other Country**	Chrome	...

It‘s not that easy…

Login history influences risk score

It‘s not that easy...

Login history influences risk score

Solution: Create many user accounts

It‘s not that easy...

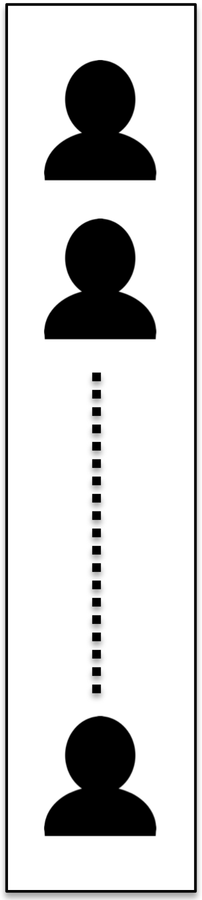
Automated testing influences result

It‘s not that easy...

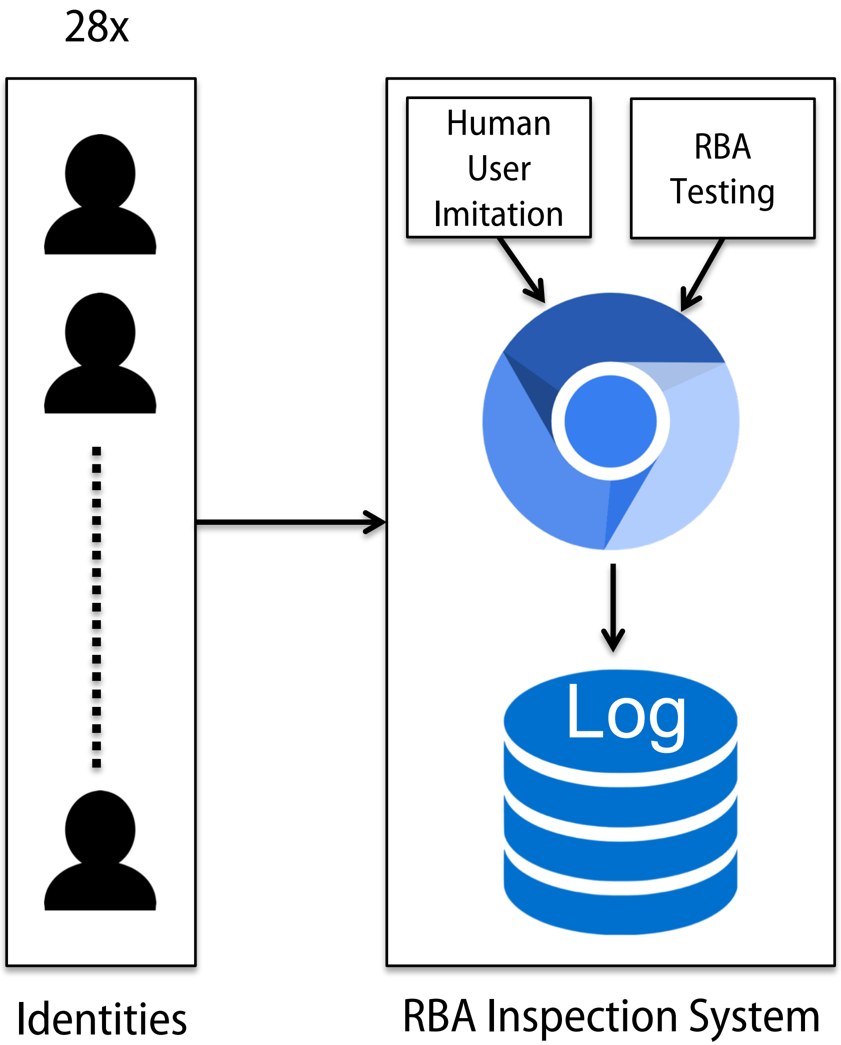
Automated testing influences result

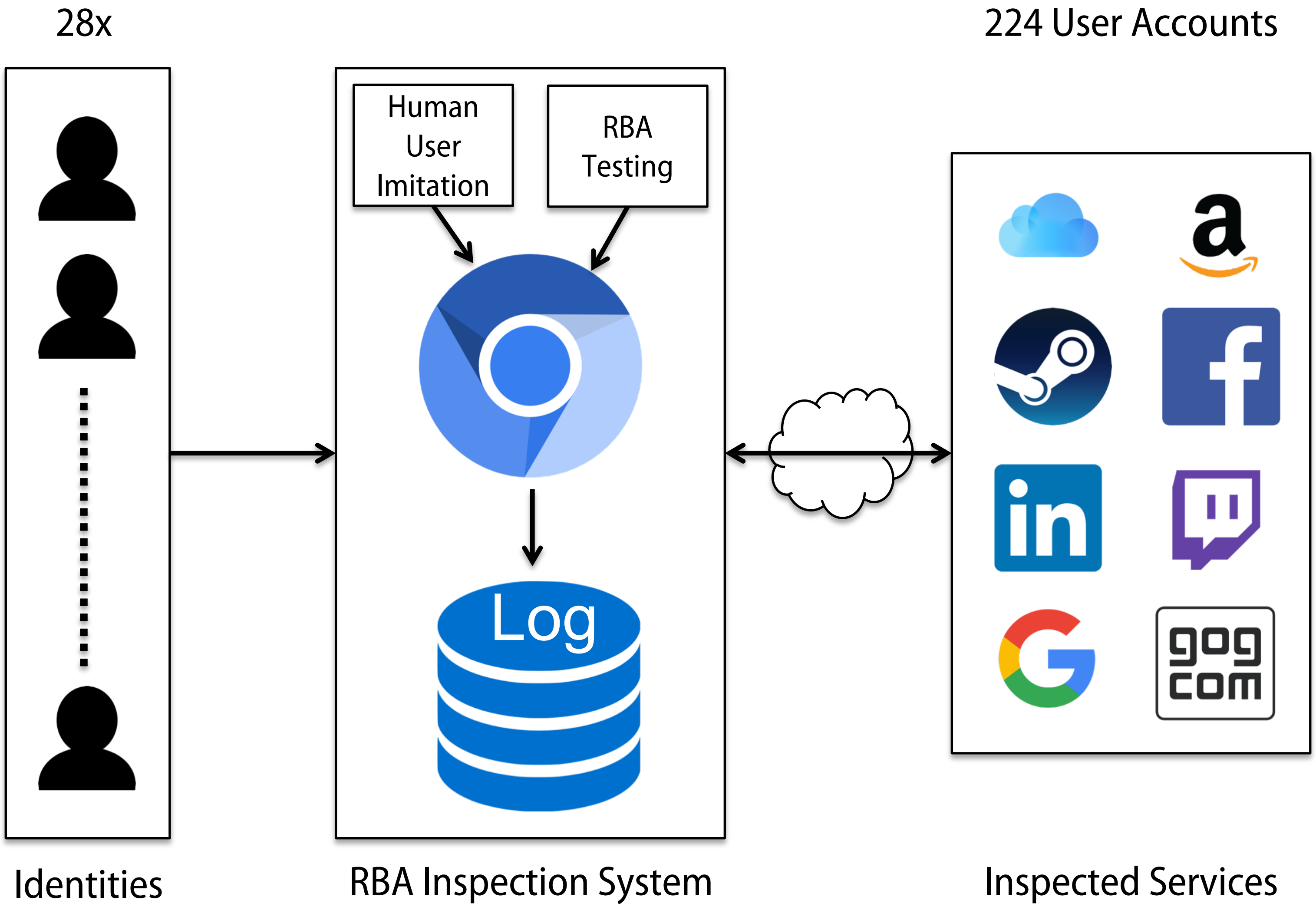
Solution: Create human-like browsing behavior

28x



Identities


28x
Human User Imitation
RBA Testing
Log
Identities
RBA Inspection System



28x

224 User Accounts

Human User Imitation

RBA Testing

Identities

RBA Inspection System

Inspected Services

It‘s still not that easy…

List of potential features is huge

It‘s still not that easy...

List of potential features is huge

Solution: Test most relevant* features

*Citations in literature, Highest distinguishing info in Alaca and van Oorschot

Alaca, F., van Oorschot, P.C.: Device Fingerprinting for augmenting web authentication. In: Proc. ACSAC '16. pp. 289-301. ACM (2016)

It‘s still not that easy...

Feature	RBA references count (except *)	Distinguishing info*
IP address	■■■■■■	●●●●○
User agent string	■■■	●●●●○
Language	■■■	●●●●○
Display resolution	■■	●●●●○
Login time	■■■■■	●●●○○
Evercookies	■	●●●●●
Canvas fingerprinting	■■■	●●●○○
Mouse and keystroke dynamics	■	-
Failed login attempts	■■	-
WebRTC	-	●●●○○
Counting hosts behind NAT	-	●●○○○
Ad blocker detection	-	●○○○○

*Alaca, F., van Oorschot, P.C.: Device Fingerprinting for augmenting web authentication. In: Proc. ACSAC '16. pp. 289-301. ACM (2016)

It‘s still not that easy...

List of potential features is huge

Solution: Test most relevant features

- IP address
- User agent string
- Language
- Display resolution
- Login time

It‘s still not that easy…

IP address feature has wide range of values

It‘s still not that easy...

IP address feature has wide range of values

Solution: Conduct a two part study

It‘s still not that easy...

IP address feature has wide range of values

Solution: Conduct a two part study

1. Find IP feature thresholds
2. Test all features with the IP threshold

It‘s still not that easy...

Study one

Find IP feature thresholds

Results

IP variation	Facebook	Google	Amazon	LinkedIn	GOG.com	Steam	Twitch	iCloud
#0 (TH Köln, fixed)	-	-	-	-	-	-	-	-
#1 (TH Köln, fresh)	-	-	-	-	A	-	-	-
#2 (same city, different ISP)	-	S	-	-	A	-	-	-
#3 (Frankfurt, DE)	-	S	-	-	A	-	-	-
#4 (Paris, FR)	-	A	A	A	A	-	-	-
#5 (Oregon, US)	-	A	A	A	A	-	-	-
#6 (Tor)	-	A	A	A	A	-	-	-

A: Additional authentication factors requested
S: Security alert submitted

It‘s still not that easy...

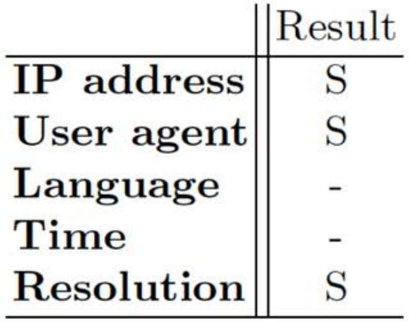
Study two

Test all features with the IP threshold*

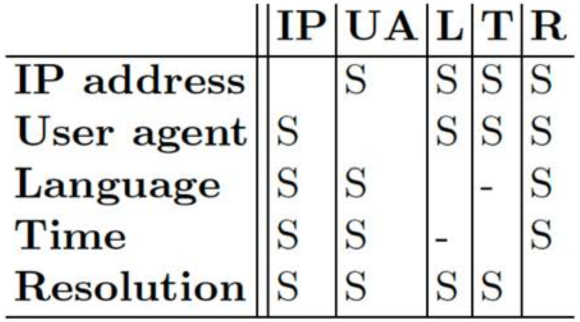
*Set IP one step below RBA threshold, set other features as “suspicious“ as possible

Results

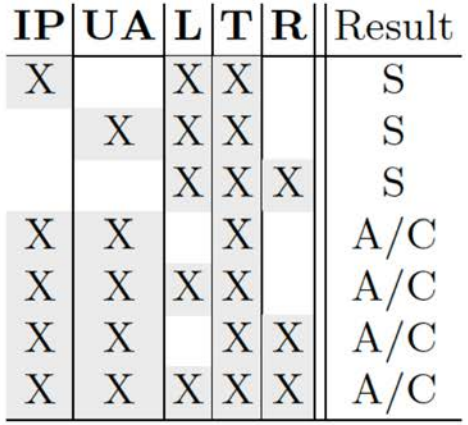
Google



	Result
IP address	S
User agent	S
Language	-
Time	-
Resolution	S



	IP	UA	L	T	R
IP address		S	S	S	S
User agent	S		S	S	S
Language	S	S		-	S
Time	S	S	-		S
Resolution	S	S	S	S	

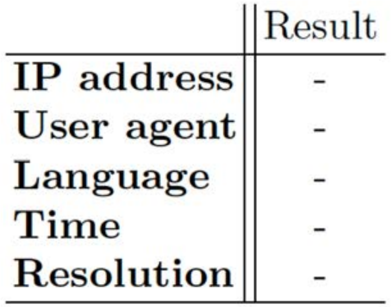


IP	UA	L	T	R	Result
X		X	X		S
	X	X	X		S
		X	X	X	S
X	X		X		A/C
X	X	X	X		A/C
X	X		X	X	A/C
X	X	X	X	X	A/C

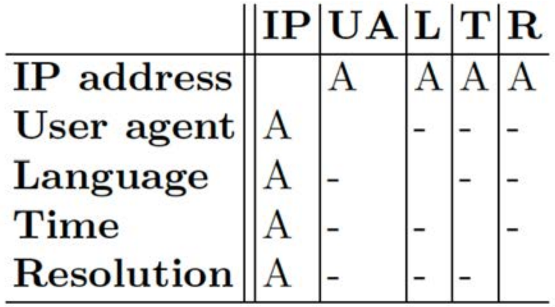
A: Additional authentication factors requested
S: Security alert submitted
C: Critical security alert submitted

Results

LinkedIn



	Result
IP address	-
User agent	-
Language	-
Time	-
Resolution	-



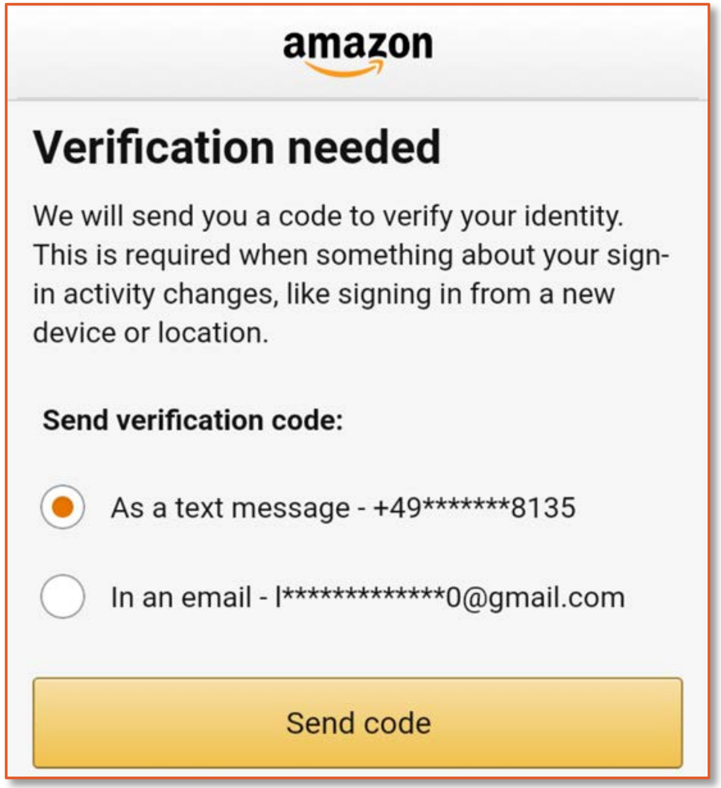
	IP	UA	L	T	R
IP address		A	A	A	A
User agent	A		-	-	-
Language	A	-		-	-
Time	A	-	-		-
Resolution	A	-	-	-	

A: Additional authentication factors requested

Results

Service	Used features and weightings
Amazon	IP address
GOG.com	IP address
Google	1. IP address 2. Time parameters 3. User agent string, display resolution
LinkedIn	1. IP address 2. User agent string, language, time parameters, display resolution

Results



amazon

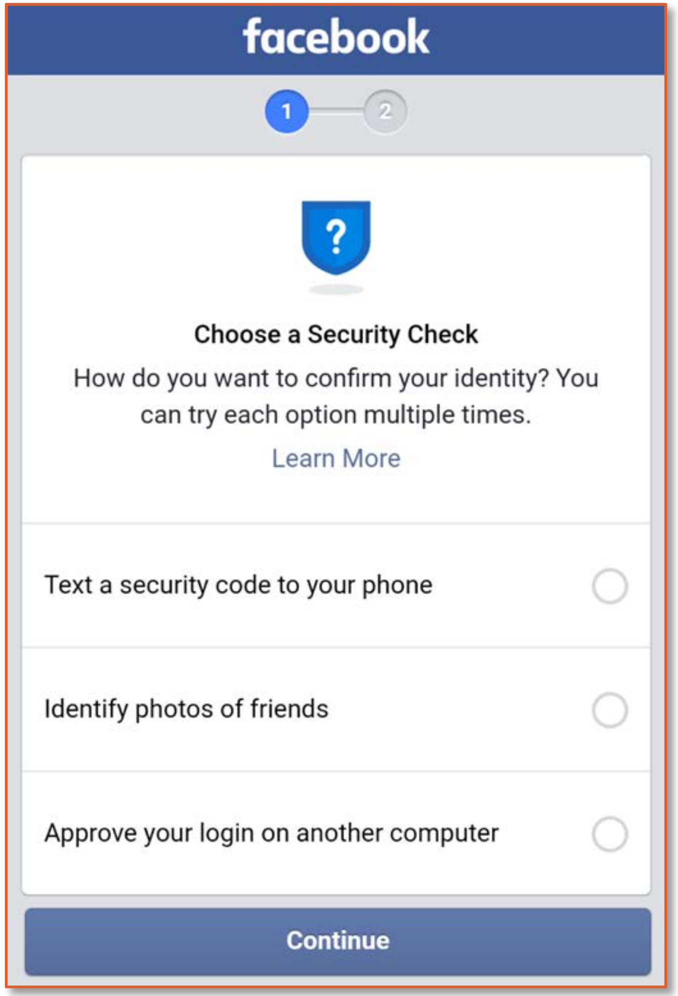
Verification needed

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



Choose a Security Check

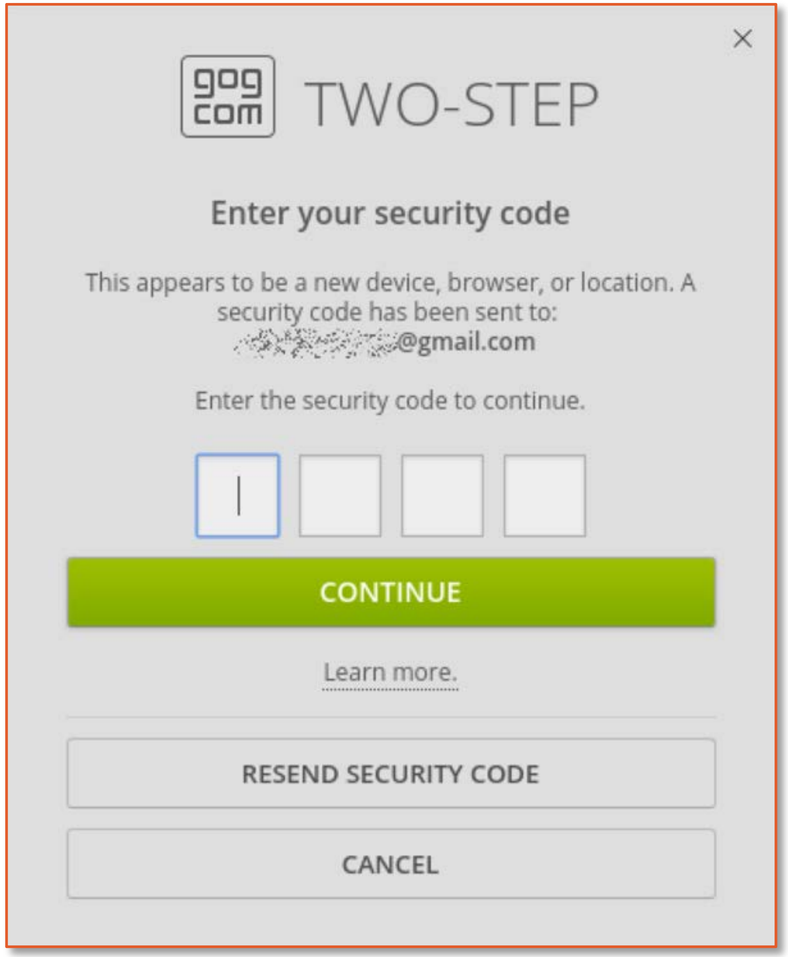
How do you want to confirm your identity? You can try each option multiple times.

Learn More

Text a security code to your phone ○

Identify photos of friends ○

Approve your login on another computer ○

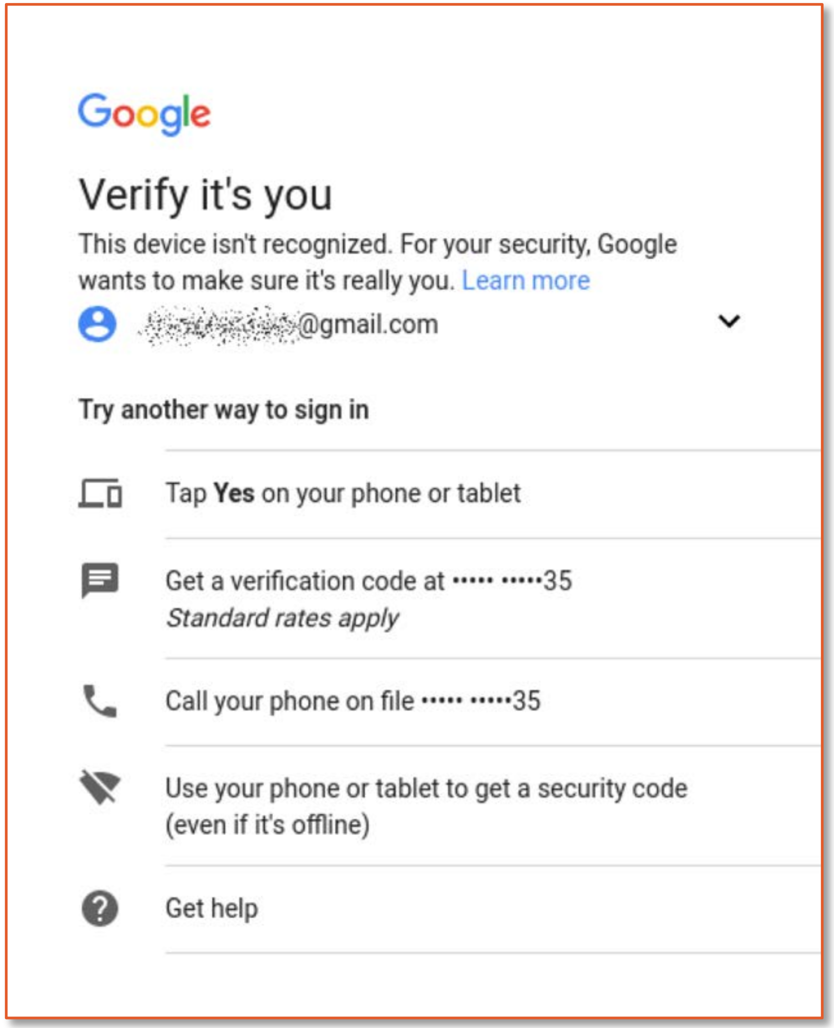


Enter your security code

This appears to be a new device, browser, or location. A security code has been sent to: [redacted]@gmail.com

Enter the security code to continue.

Results


Google

Verify it's you

This device isn't recognized. For your security, Google wants to make sure it's really you. Learn more

[redacted]@gmail.com

Try another way to sign in

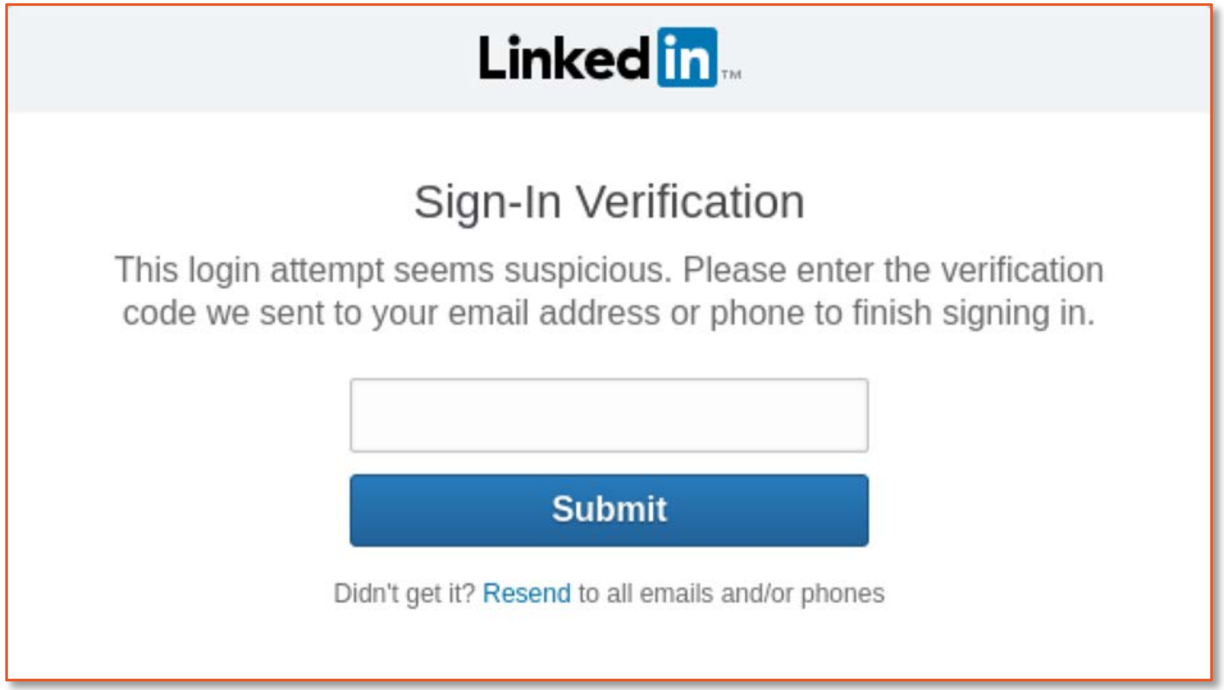
Tap **Yes** on your phone or tablet

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



Sign-In Verification

This login attempt seems suspicious. Please enter the verification code we sent to your email address or phone to finish signing in.

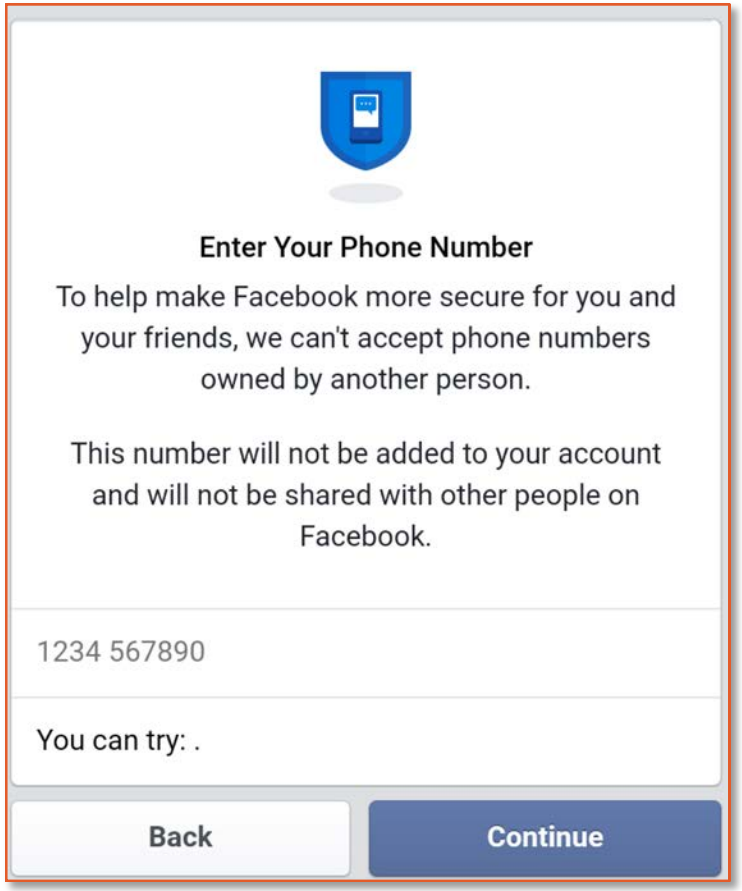
Didn't get it? Resend to all emails and/or phones

Results

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

*: Authentication factor was offered in all tested parameter variations

Privacy leak on Facebook



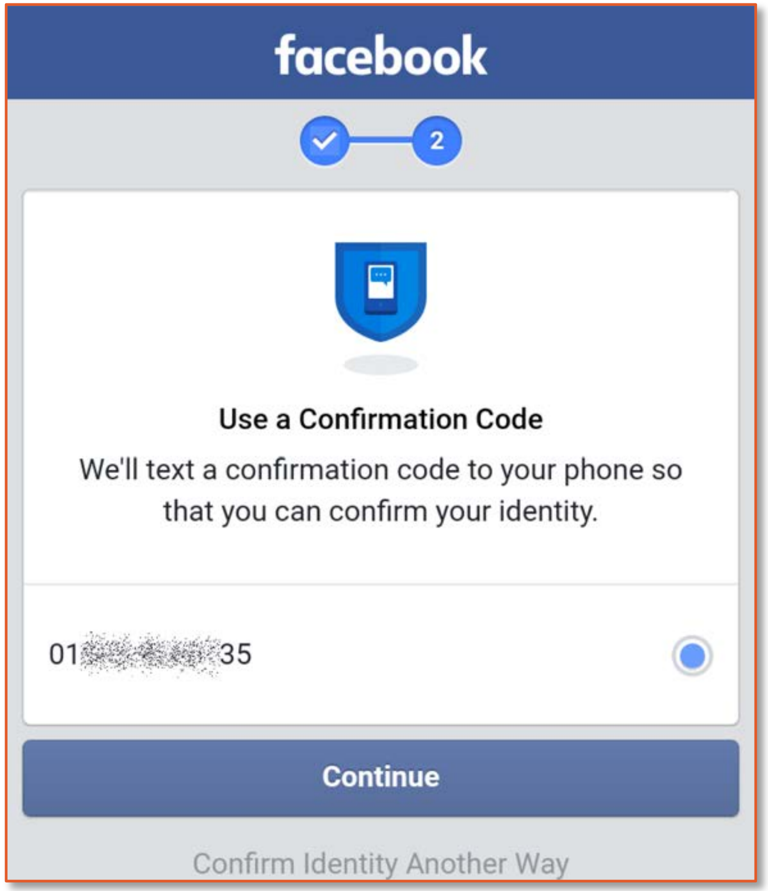
Enter Your Phone Number

To help make Facebook more secure for you and your friends, we can't accept phone numbers owned by another person.

This number will not be added to your account and will not be shared with other people on Facebook.

1234 567890

You can try: .



Use a Confirmation Code

We'll text a confirmation code to your phone so that you can confirm your identity.

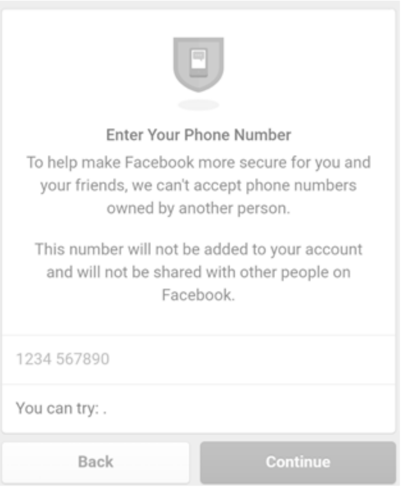
01[redacted]35 ●

Privacy leak on Facebook

Responsible disclosure

Reported: September 4th, 2018

Fixed: September 6th, 2018



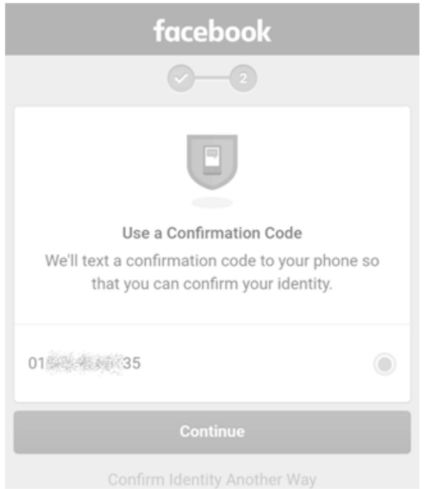
Enter Your Phone Number

To help make Facebook more secure for you and your friends, we can't accept phone numbers owned by another person.

This number will not be added to your account and will not be shared with other people on Facebook.

1234 567890

You can try: .



Use a Confirmation Code

We'll text a confirmation code to your phone so that you can confirm your identity.

01[redacted]35

Conclusion

- First insights into RBA practices of big online services
- Intended to support developers, administrators and researchers
- Testing tool available as open source software*
- Interactive results and RBA models on website#

*https://github.com/das-th-koeln/HOSIT

#https://riskbasedauthentication.org

Thank you

riskbasedauthentication.org
das.th-koeln.de

stephan.wiefling@th-koeln.de

@swiefling