UNIVERSITY OF OSLO

The 3rd International Conference on Ubiquitous Security 2023

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

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

* University of Oslo (Norway)

† H-BRS University of Applied Sciences (Germany)

2nd November 2023

# Motivation – Authentication

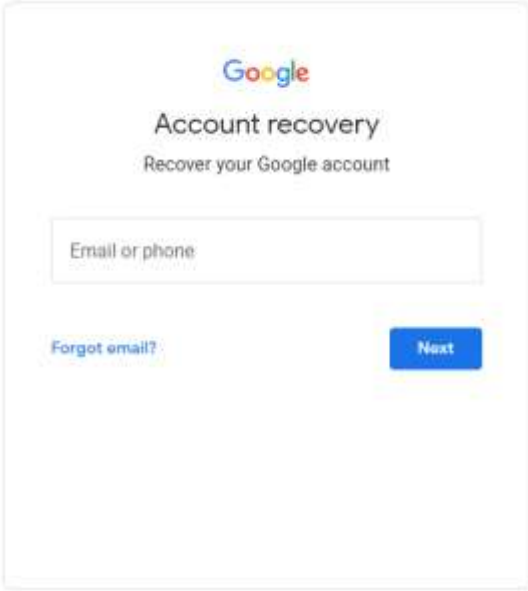
- Online accounts are usually protected by passwords[1]
  - Susceptible to account takeover attacks

- Multi-factor authentication (MFA) as countermeasure
  - Improves security
  - Usability issues

- Risk-based authentication (RBA)[2,3]
  - Risk assessment based on client features, e.g., (IP-)location, user agent, login times
  - Security ←→ Usability


[1] Quermann, Nils, Marian Harbach, and Markus Dürmuth. "The state of user authentication in the wild." *WAY* 18 (2018).
[2] Freeman, David, Sakshi Jain, Markus Dürmuth, Battista Biggio, and Giorgio Giacinto. "Who Are You? A Statistical Approach to Measuring User Authenticity." In *NDSS*, vol. 16, pp. 21-24. 2016.
[3] Wiefling, Stephan, Luigi Lo Iacono, and Markus Dürmuth. "Is this really you? An empirical study on risk-based authentication applied in the wild." *ICT Systems Security and Privacy Protection: 34th IFIP TC 11 International Conference, Proceedings 34*. Springer International Publishing, 2019.

# Motivation – Account Recovery




Account Recovery:

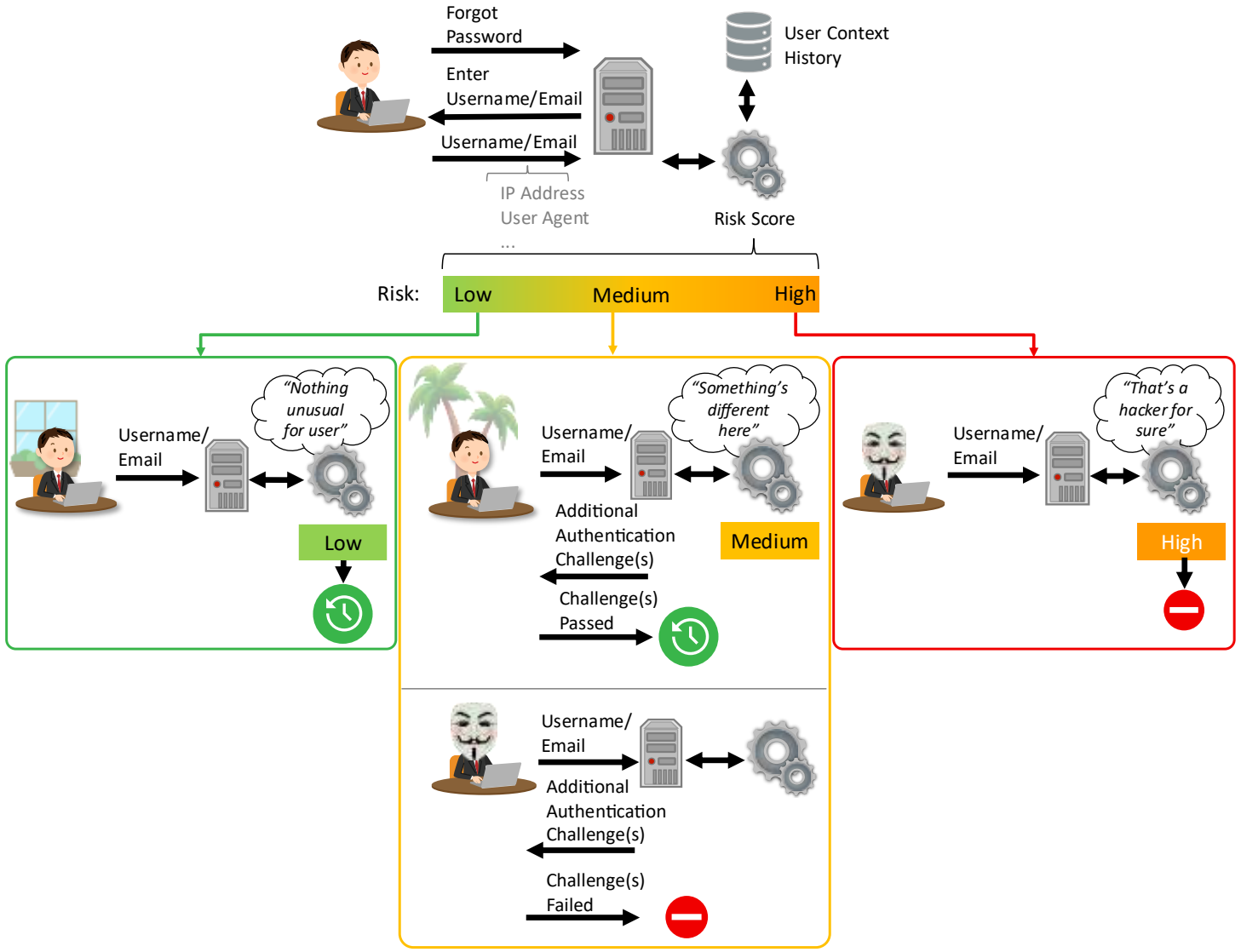
- Should meet the same security requirements as main authentication
- Can also benefit from risk-based decision making
  - Risk of account lockout ←→ Exploitation of recovery

Risk-Based Account Recovery (RBAR):

➔ A dynamic account recovery process on online services

- Uses similar features as RBA to detect suspicious users
- Different levels of difficulty to perform account recovery based on the risk
- Can lead to complete denial of account recovery for a highly suspicious client

# RBAR


Forgot Password
Enter Username/Email
Username/Email
IP Address
User Agent
...
User Context History
Risk Score
Risk:
Low
Medium
High
Username/ Email
"Nothing unusual for user"
Low
Username/ Email
"Something's different here"
Additional Authentication Challenge(s)
Challenge(s) Passed
Medium
Username/ Email
"That's a hacker for sure"
High
Username/ Email
Additional Authentication Challenge(s)
Challenge(s) Failed

# Research Questions

- RQ1: Do RBA-instrumented online services also use RBAR mechanisms?
- RQ2: What RBAR challenges are used in practice?
- RQ3: Are different RBAR challenges required when setting up MFA?

# Methodology

1. Exploratory experiment on Google
   - Confirm use of RBAR on Google[1]
   - Compare different account setups

2. Follow-up experiment on four other online services
   - Testing the use of RBAR on the following services*
     - Amazon (amazon.com)
     - GOG (gog.com)
     - Dropbox (dropbox.com)
     - LinkedIn (linkedin.com)

* These services have previously been confirmed to use RBA[2]

[1] Bonneau, Joseph, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike Williamson. "Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google." In *Proceedings of the 24th international conference on world wide web*. 2015.
[2] Wiefling, Stephan, Luigi Lo Iacono, and Markus Dürmuth. "Is this really you? An empirical study on risk-based authentication applied in the wild." *ICT Systems Security and Privacy Protection: 34th IFIP TC 11 International Conference, Proceedings 34*. Springer International Publishing, 2019.

# Experiment 1

Preparation:

- Four Google accounts were initially created with a certain time difference

Experimental procedure:

- Testing of account recovery with all possible single-factor and eight different MFA account setups
- Test variables
  - Known/unknown browser → using a private browser window
  - IP address → using a VPN

# Experiment 1 – Results

Example tests on Google without MFA enabled:

| Recovery factor | Phone signed in | Known browser | Known IP | Recovery procedure |
|---|---|---|---|---|
| None | ○ | ● | ● | Recovery not possible |
| None | ● | ● | ● | 1. Google prompt |
| None | ● | ○ | ○ | 1. Enter old password<br>2. Google prompt (two steps) |
| Email | ○ | ● | ● | 1. Verify account email |
| Email | ○ | ○ | ● | 1. Enter old password<br>2. Verify account email |

Example tests on Google with MFA phone enabled:

| Recovery factor | Known browser | Known IP | Recovery procedure |
|---|---|---|---|
| None | ● | ●/○ | 1. Verify MFA phone<br>~~2. Verify account email~~<br>3. Verify new email<br>→ Reset email after 48h |
| None | ○ | ● | 1. Verify MFA phone<br>~~2. Verify account email~~<br>→ Recovery not possible |
| None | ○ | ○ | 1. Enter MFA phone number<br>2. Verify MFA phone<br>~~3. Verify account email~~<br>→ Recovery not possible |

● = Feature present, ○ = Feature not present, ~~XXX~~ = Step omitted

# Experiment 2

Preparation:

- Four new accounts and at least one “old” account per online service
- Account training:
  - Sign into each service more than 20 times before the account recovery experiments
  - Use the same browser consistently for each account

Experimental procedure:

- Sign in once with a **suspicious** and once with a **normal** user context
  - **Normal user**: Login from same browser as during training
  - **Suspicious user**: Login from Tor browser

# Experiment 2 – Identifying RBAR Usage

| Online Service | Account | User Context | |
|---|---|---|---|
| | | Normal | Suspicious |
| Amazon | A1, A2, A4, A6* | EC | EC |
| | A3, A1† | CA→EC | CA→EC |
| | A5* | EC | <u>CA</u>→EC |
| Dropbox | D1-D4, D5* | EL | EL |
| GOG | G1-G4, G5* | CA→EL | CA→EL |
| LinkedIn | L1-L4, L5* | EC | <u>CA</u>→EC |

**Different behavior!**

EC = Email (Code), EL = Email (Link), CA = CAPTCHA, ∗ = Old account,
† = Experiment repeated, <u>XXX</u> = Additional step

# Experiment 2 – Further Testing

LinkedIn:

- MFA methods were always required for both suspicious and normal user
- We conclude that CAPTCHA is the only RBAR method used
- The number of CAPTCHA iterations seemed to vary depending on the IP location of the Tor exit node

Amazon:

- No further tests as we could not reproduce RBAR behavior consistently
- We conclude that CAPTCHA is possibly used in connection with a risk assessment

# RBAR Maturity Model

**Maturity level**


| RBAR challenge | Identified on | Possible attacks |
|---|---|---|
| Pre-configured MFA | Google | Physical attack, malware |
| Background knowledge | Google | OSINT, leaked passwords, phishing |
| CAPTCHA | LinkedIn, Amazon | Manual recovery, CAPTCHA bypass algorithm |
| None | Dropbox, GOG | n/a |

# Conclusion

- Account recovery is a relevant entry point for account takeover attacks
- There are online services that use RBAR to a different degree
  - **Google** uses several different methods
  - **Amazon** and **LinkedIn** only requested a CAPTCHA
  - **Dropbox** and **GOG** did not differ between suspicious and benign users
- The proposed maturity model can be used:
  - To evaluate RBAR implementations
  - As a guideline for implementing RBAR
- Future work:
  - Extending the RBAR model
  - Detailed analysis of RBAR client features
  - Comparison of RBA and RBAR

UNIVERSITY OF OSLO

The 3rd International Conference on Ubiquitous Security 2023

# Thank you!
# Any questions?

**Contact**
Andre Büttner
University of Oslo
Email: andrbut@ifi.uio.no
Web: https://www.mn.uio.no/ifi/english/people/aca/andrbut/index.html

Also at: