



The image shows a screenshot of the OpenStack 'Verify Your Identity' interface. At the top is the OpenStack logo (a red square with a white 'O' inside) and the text 'openstack.'. Below this is the heading 'Verify Your Identity'. A pink message box contains the text: '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 your deposited contact address. Please enter the code to log in.' Below the message box is a label 'Security code' followed by a text input field. At the bottom left, there is a link 'Did not receive a message? Re-send code.' and at the bottom right, a blue 'Continue' button.

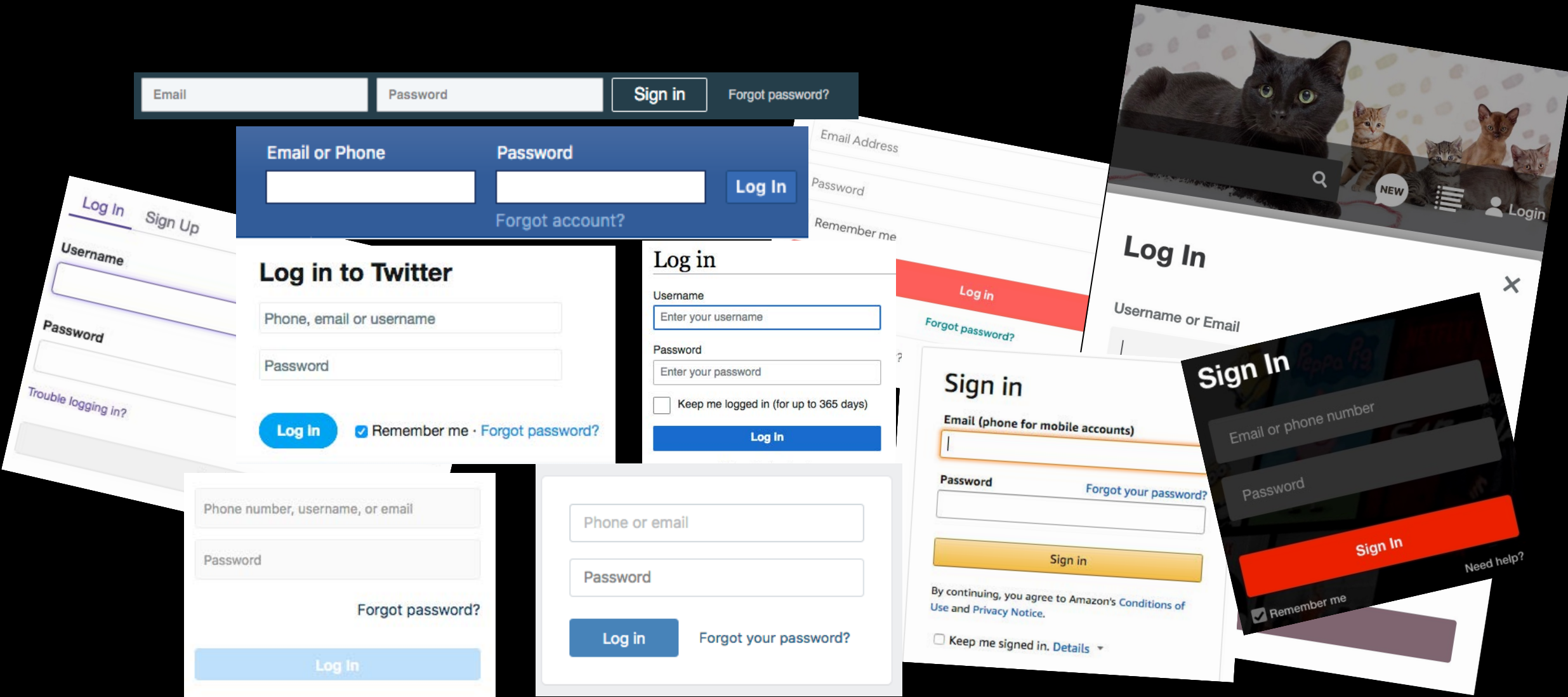
Risk-Based Authentication for OpenStack:

A Fully Functional Implementation and Guiding Example

Vincent Unsel, Stephan Wiefeling, Nils Gruschka*, Luigi Lo Iacono

H-BRS University of Applied Sciences, Germany

University of Oslo, Norway (*)



>50% Password Re-Use*

*Representative survey conducted by Bilendi & respondi in February 2022; n=1000 German Internet users >18 years old

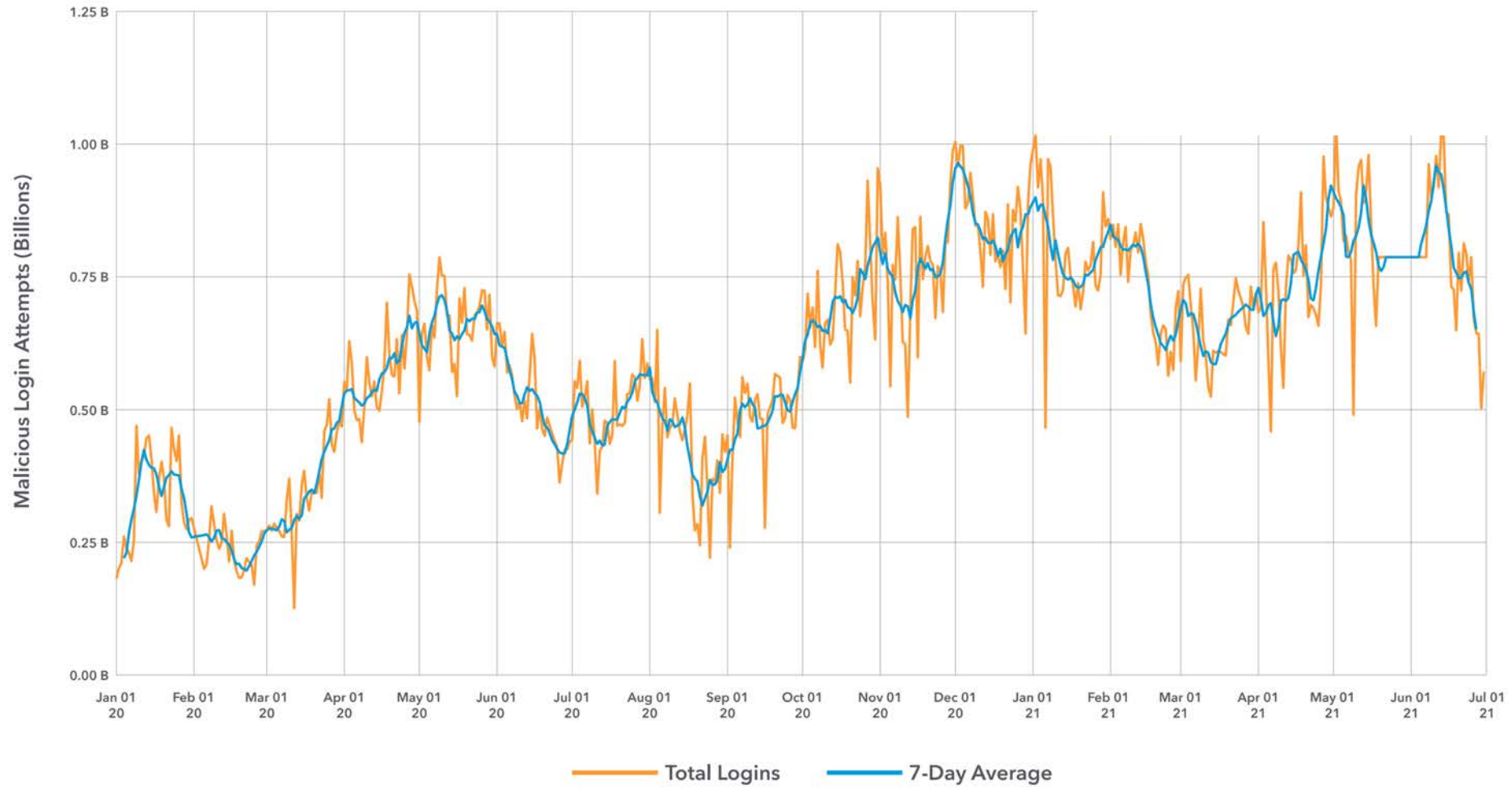
Credential Stuffing

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).

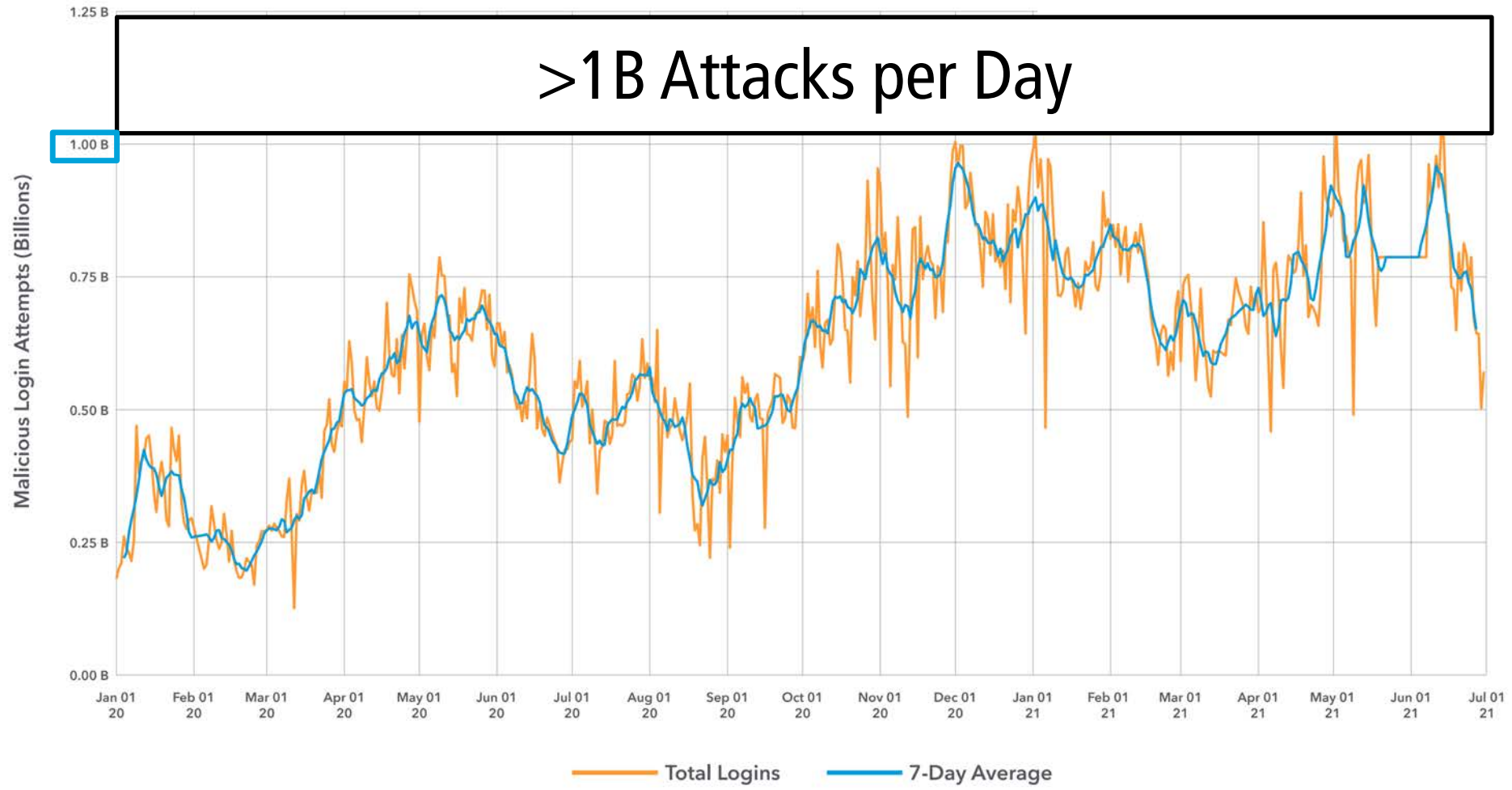
Daily Credential Abuse Attempts January 1, 2020 – June 30, 2021



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

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).

2FA



Low 2FA Adoption in Practice



<10%*

*In January 2018

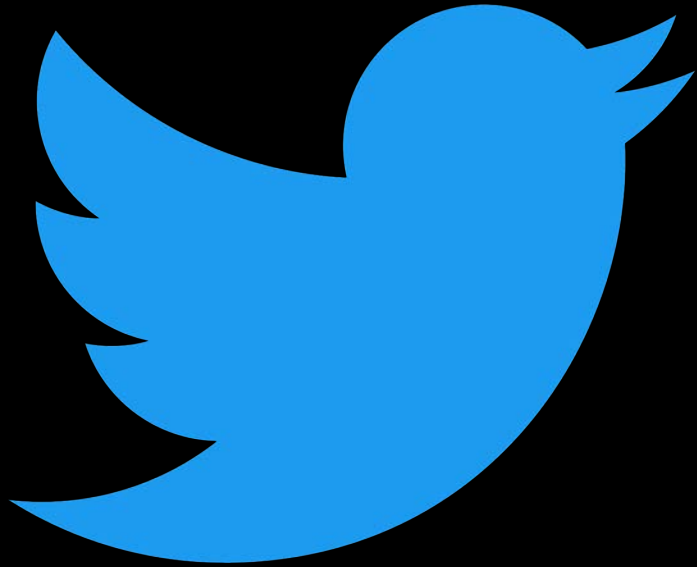
Milka, G.: Anatomy of Account Takeover. In: Enigma 2018. USENIX (Jan 2018)



~4%*

*In December 2021

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

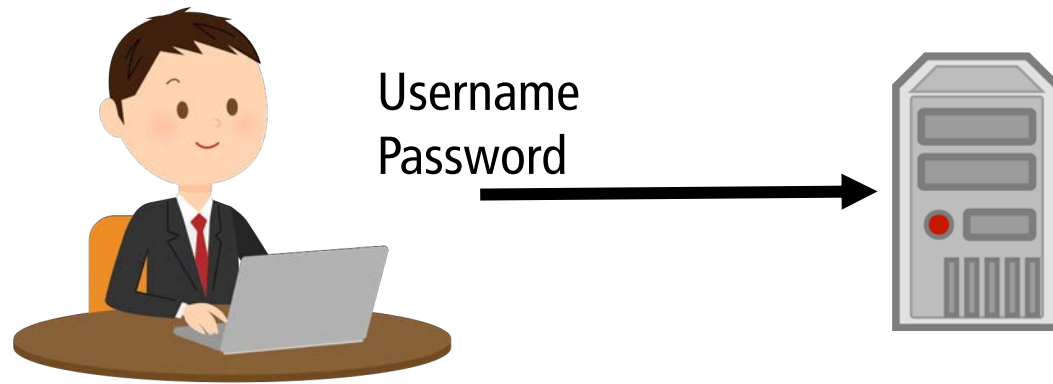


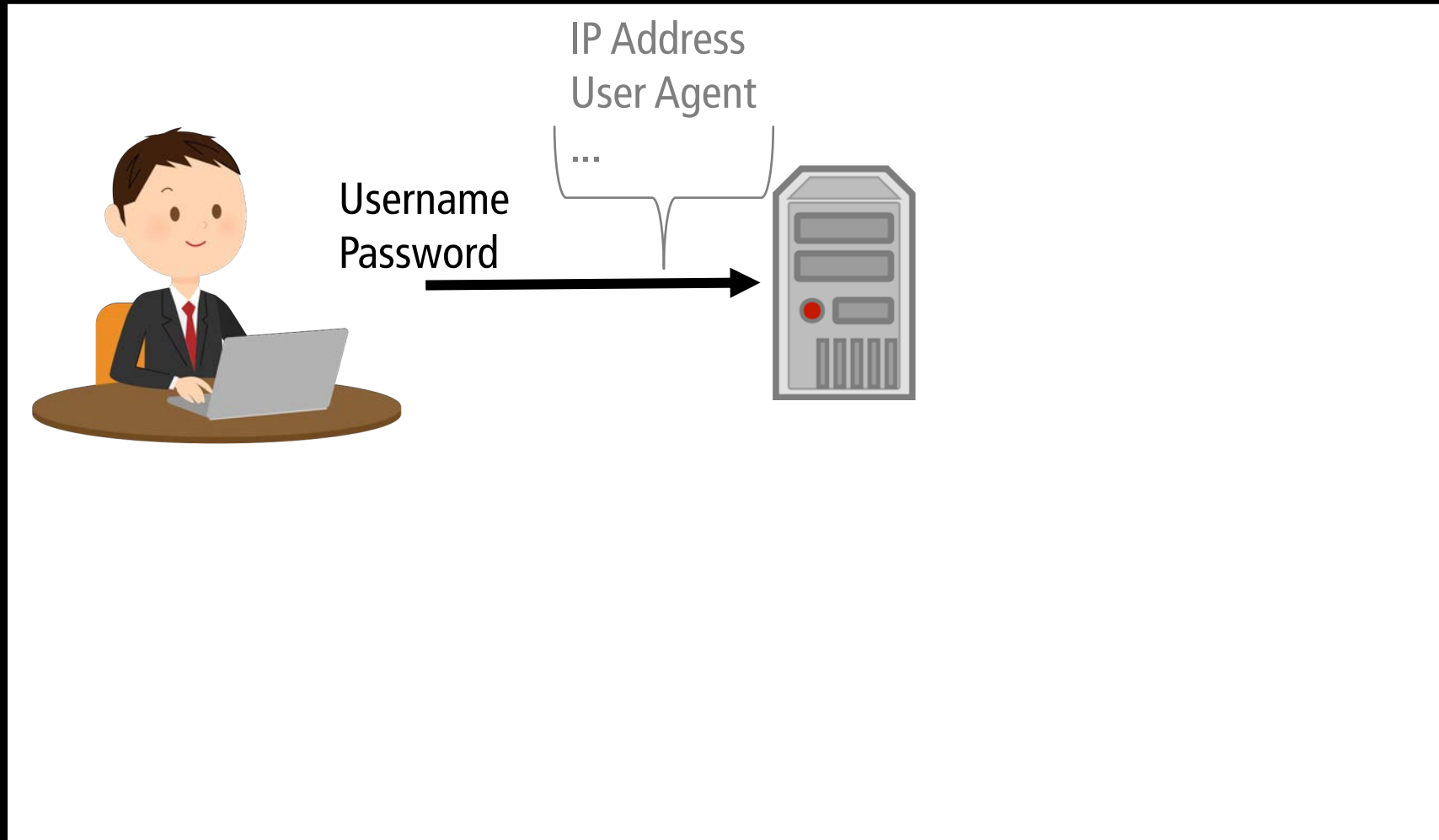
2.6% *

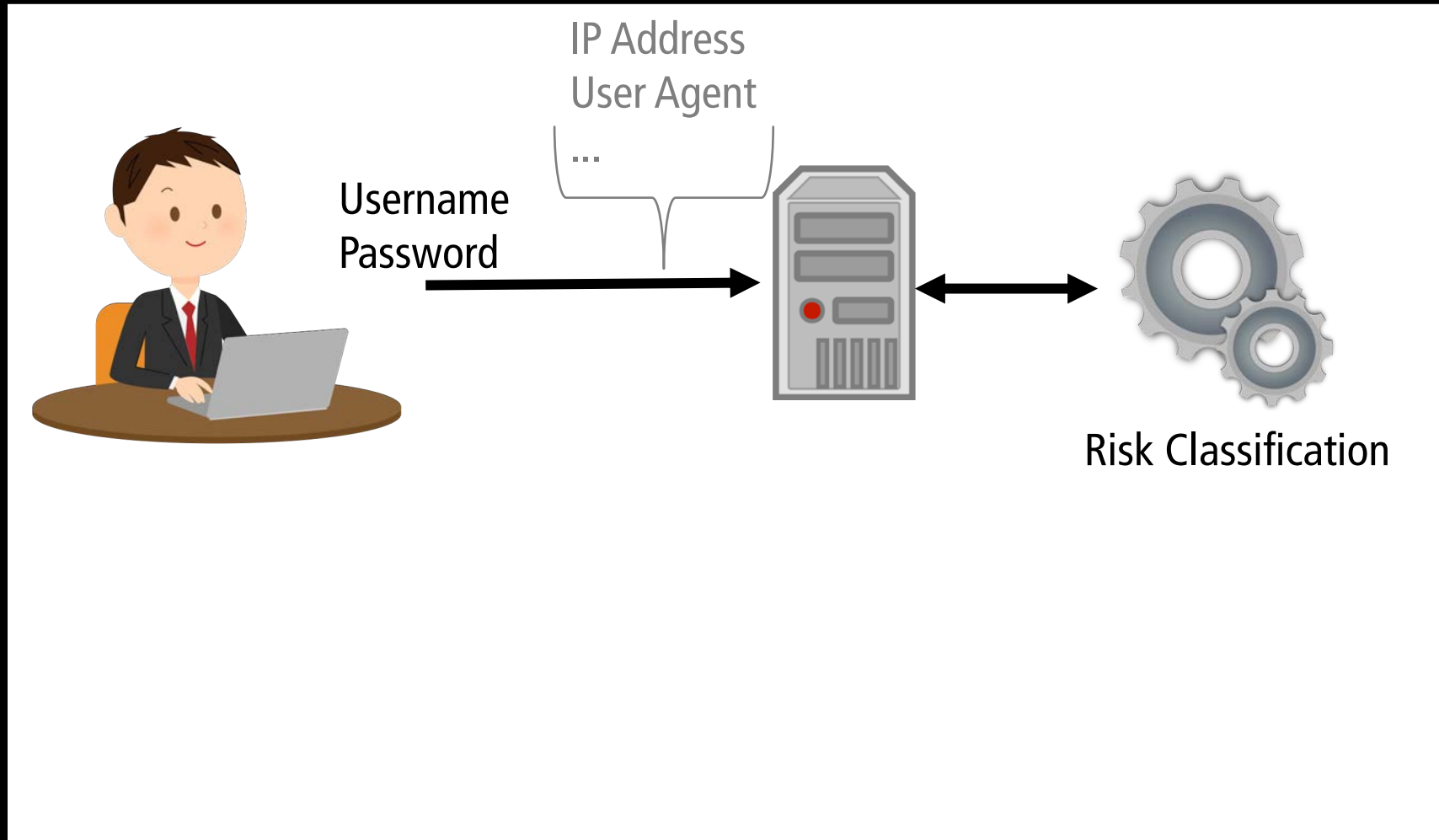
*In December 2021

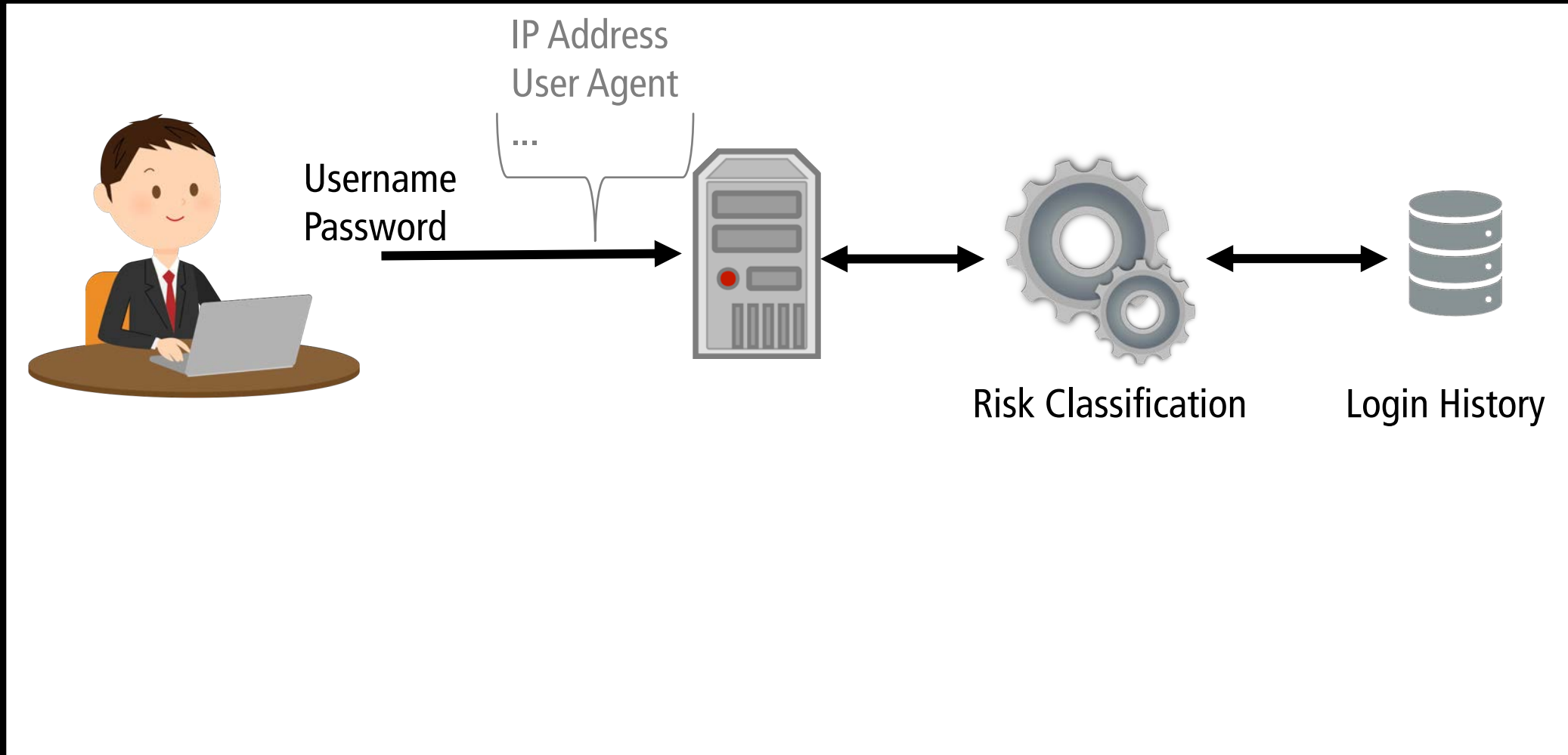
Twitter: Account Security. In: Twitter Transparency Center (Jul 2022)

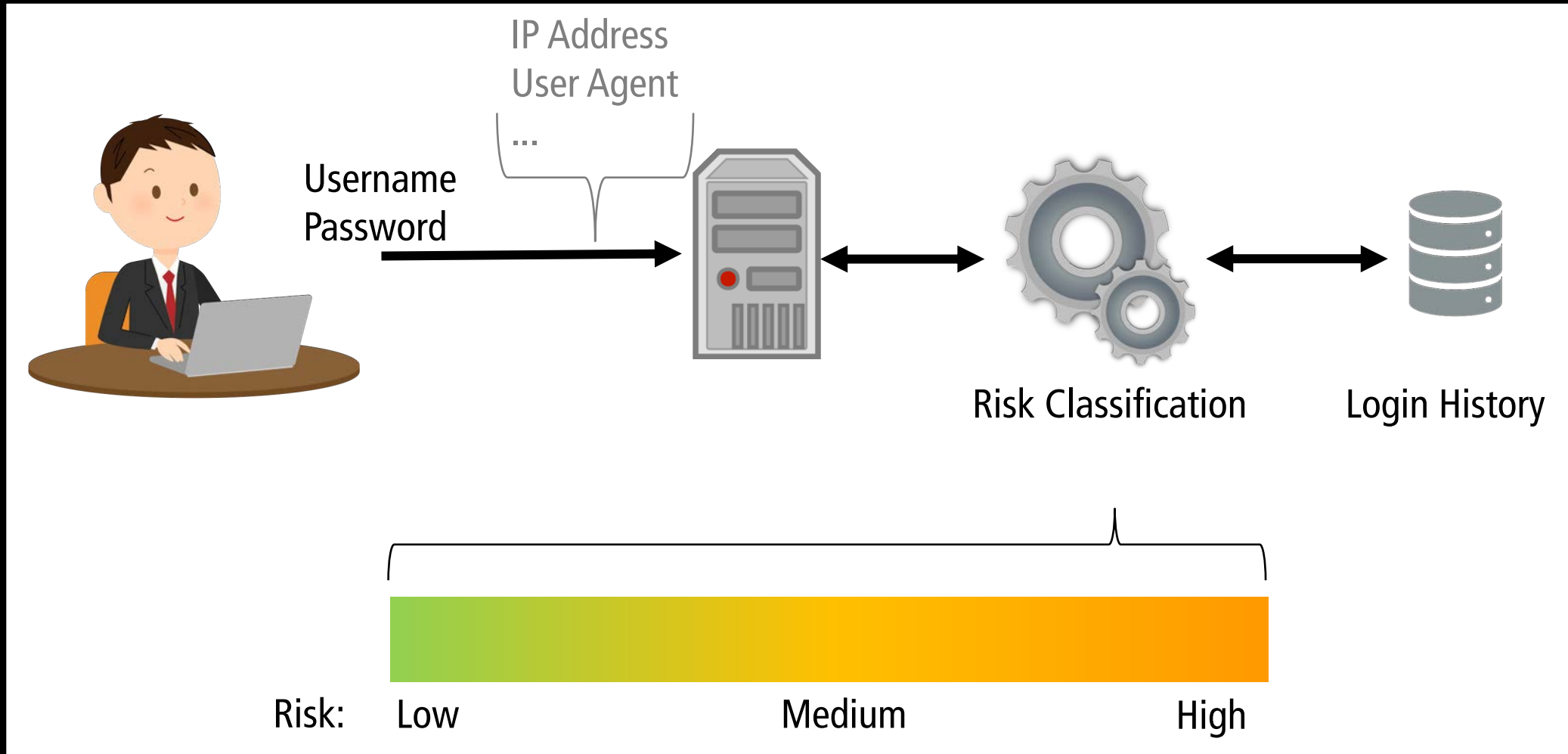
Risk-Based Authentication (RBA)

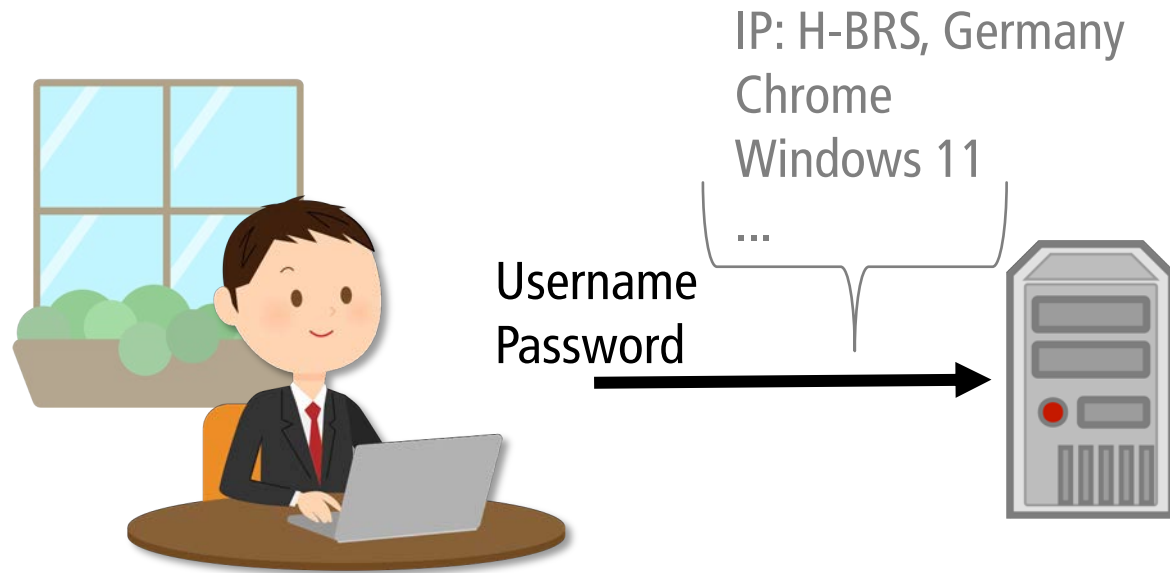


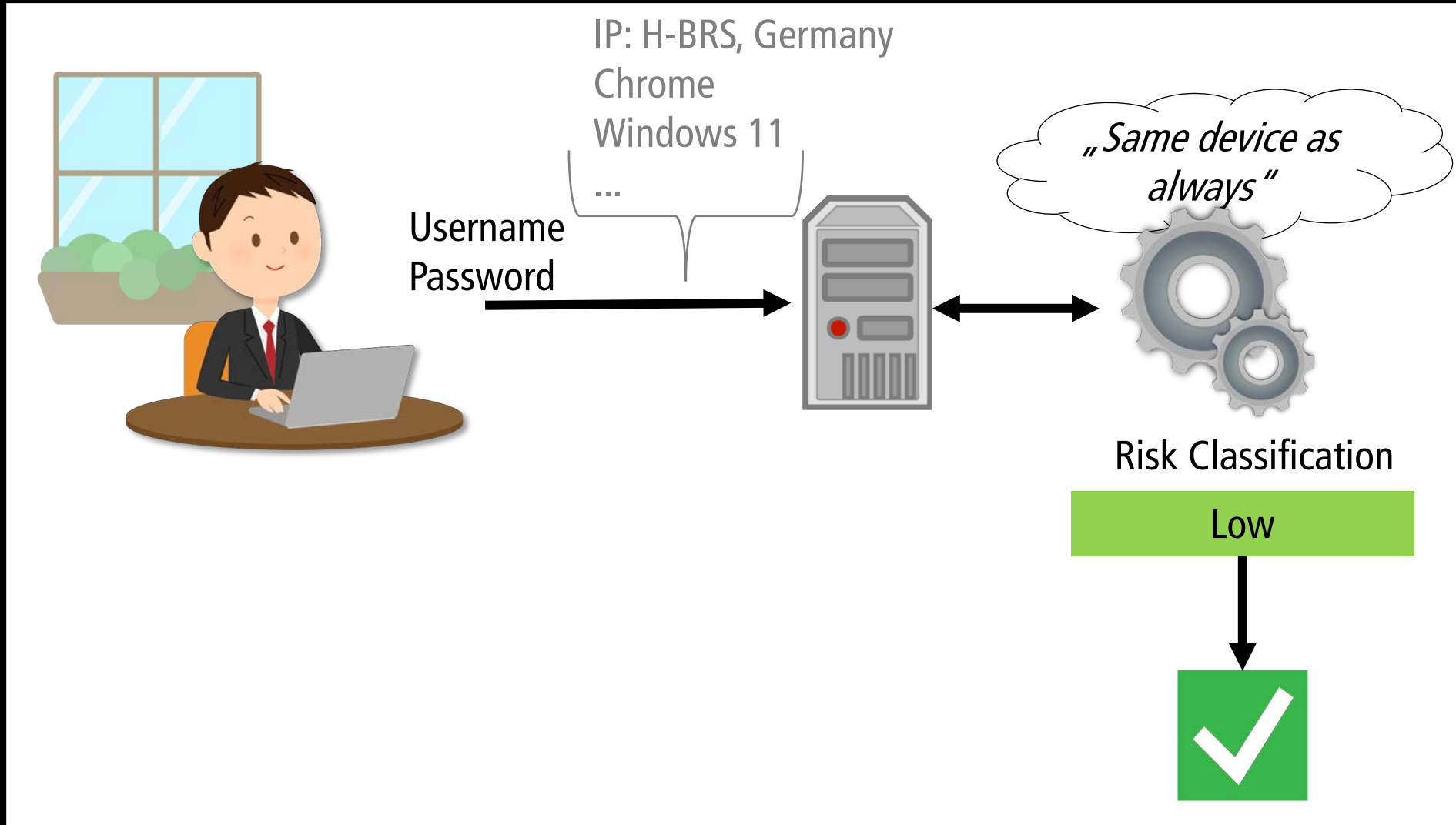


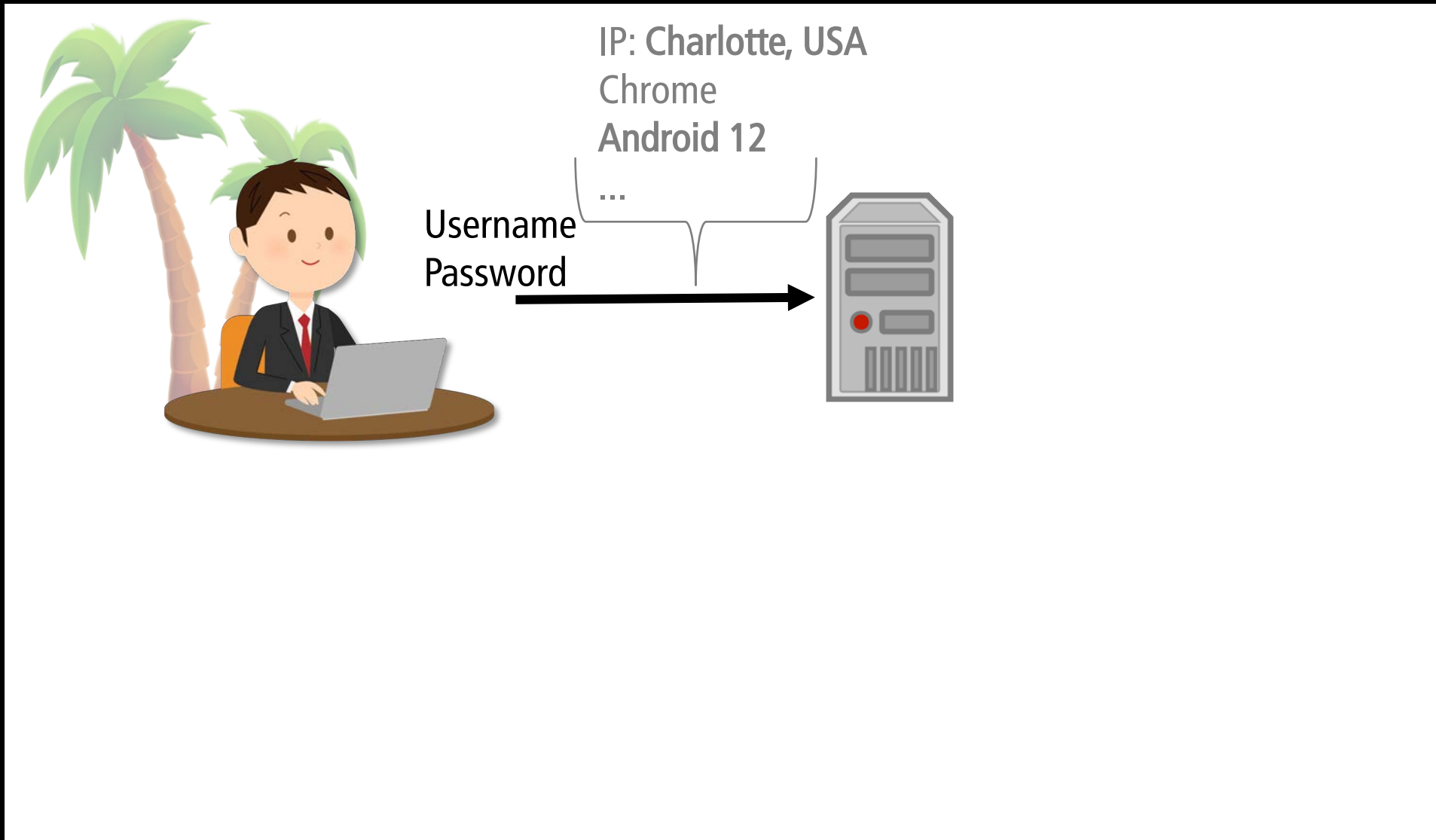


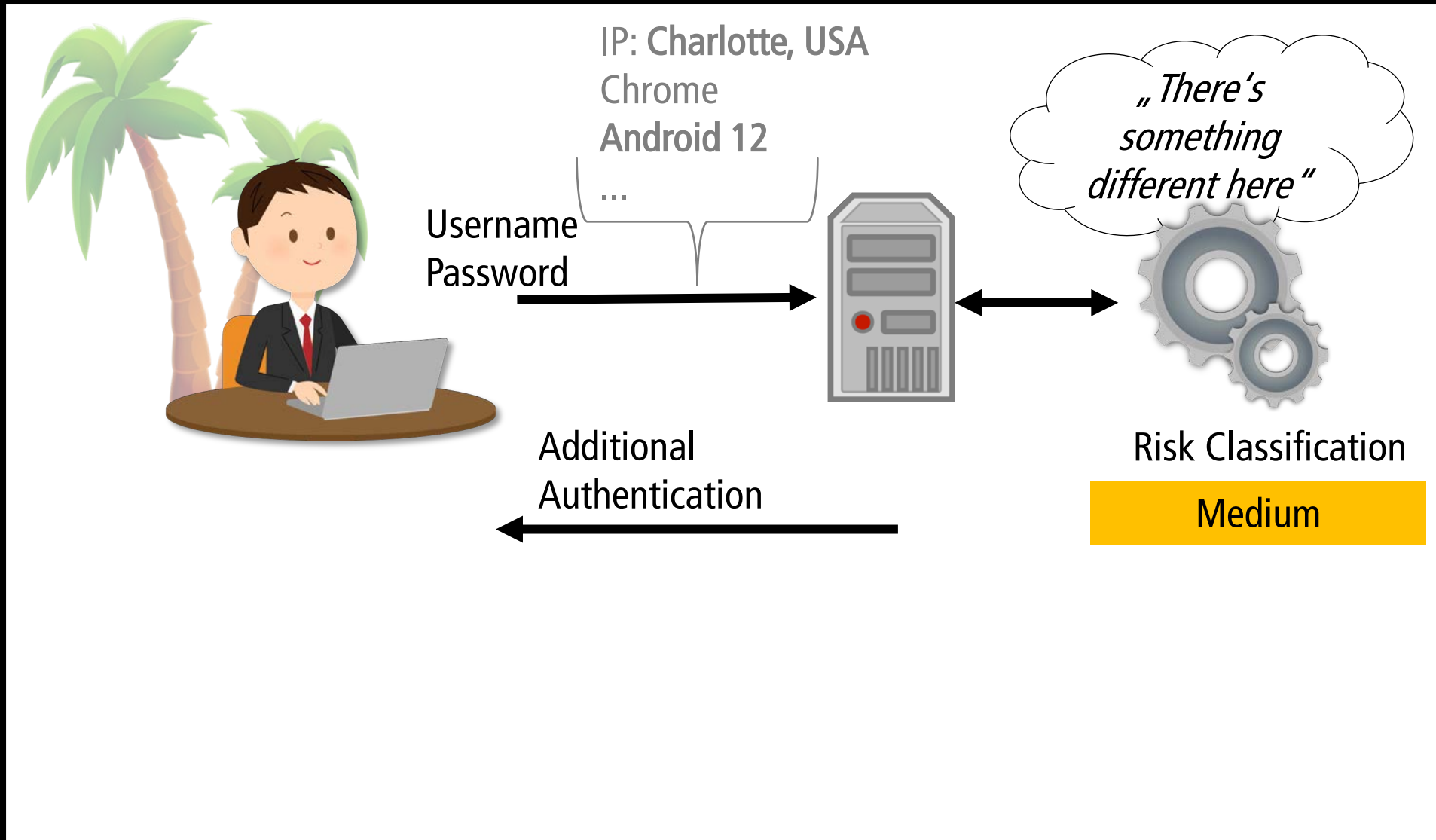















Verify Your Identity

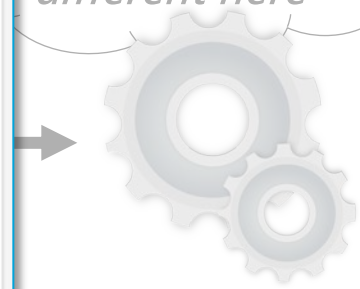
For security reasons we would like to verify your identity. This is required when something about your sign-in activity changes, like signing in from a new location or a new device.

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

Continue

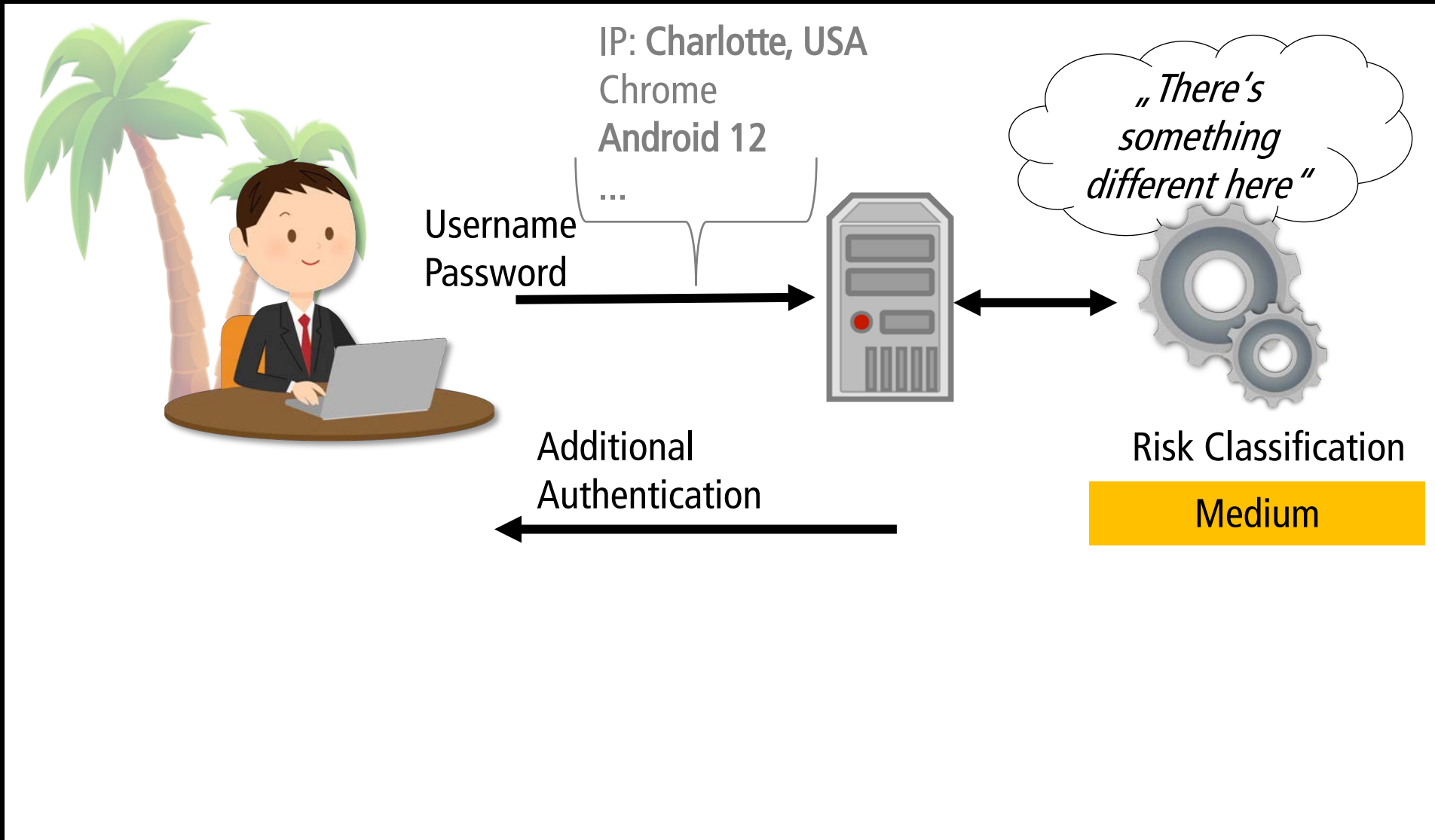
Did not receive email? [Re-send code.](#)

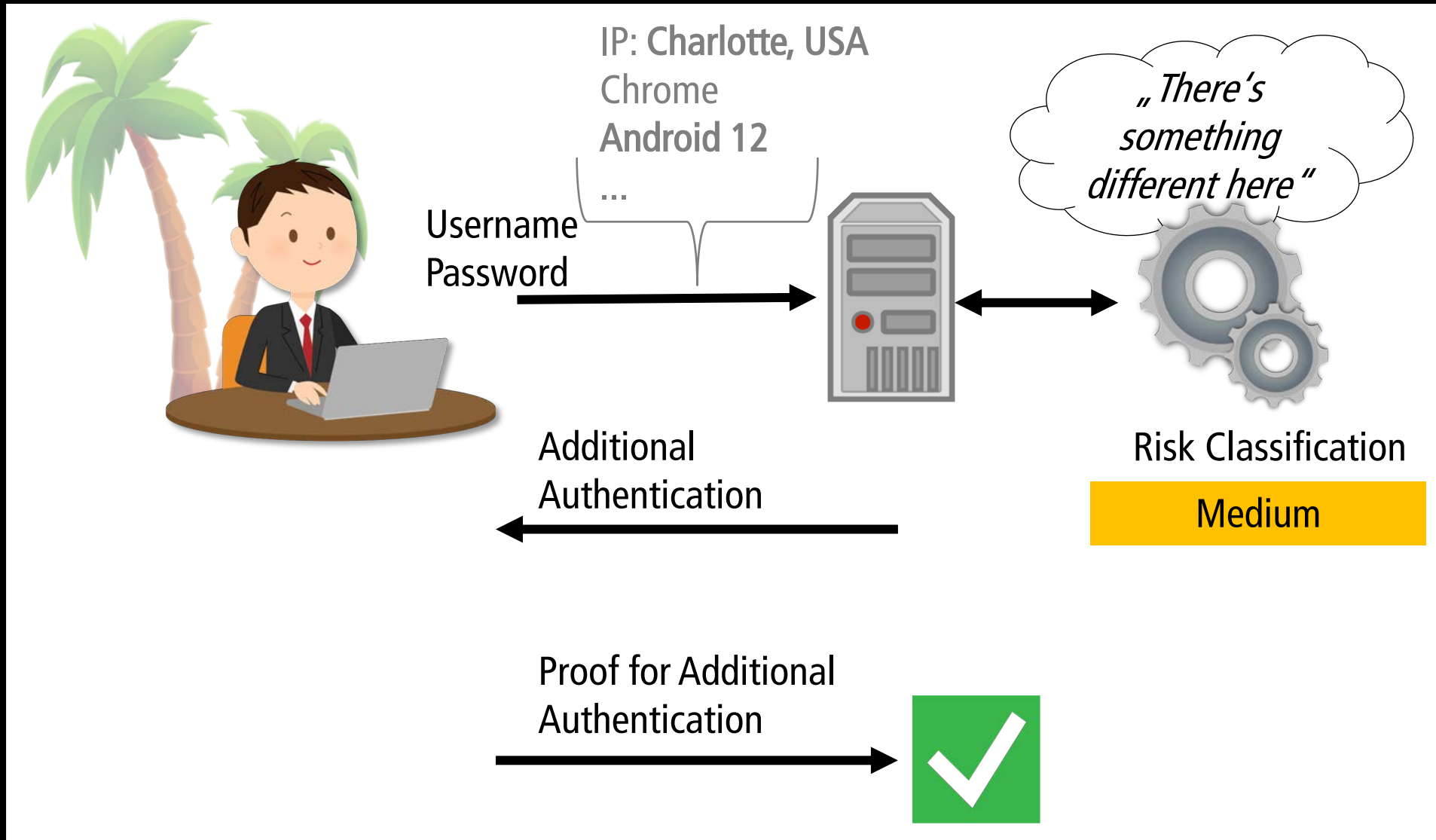
„There's something different here“

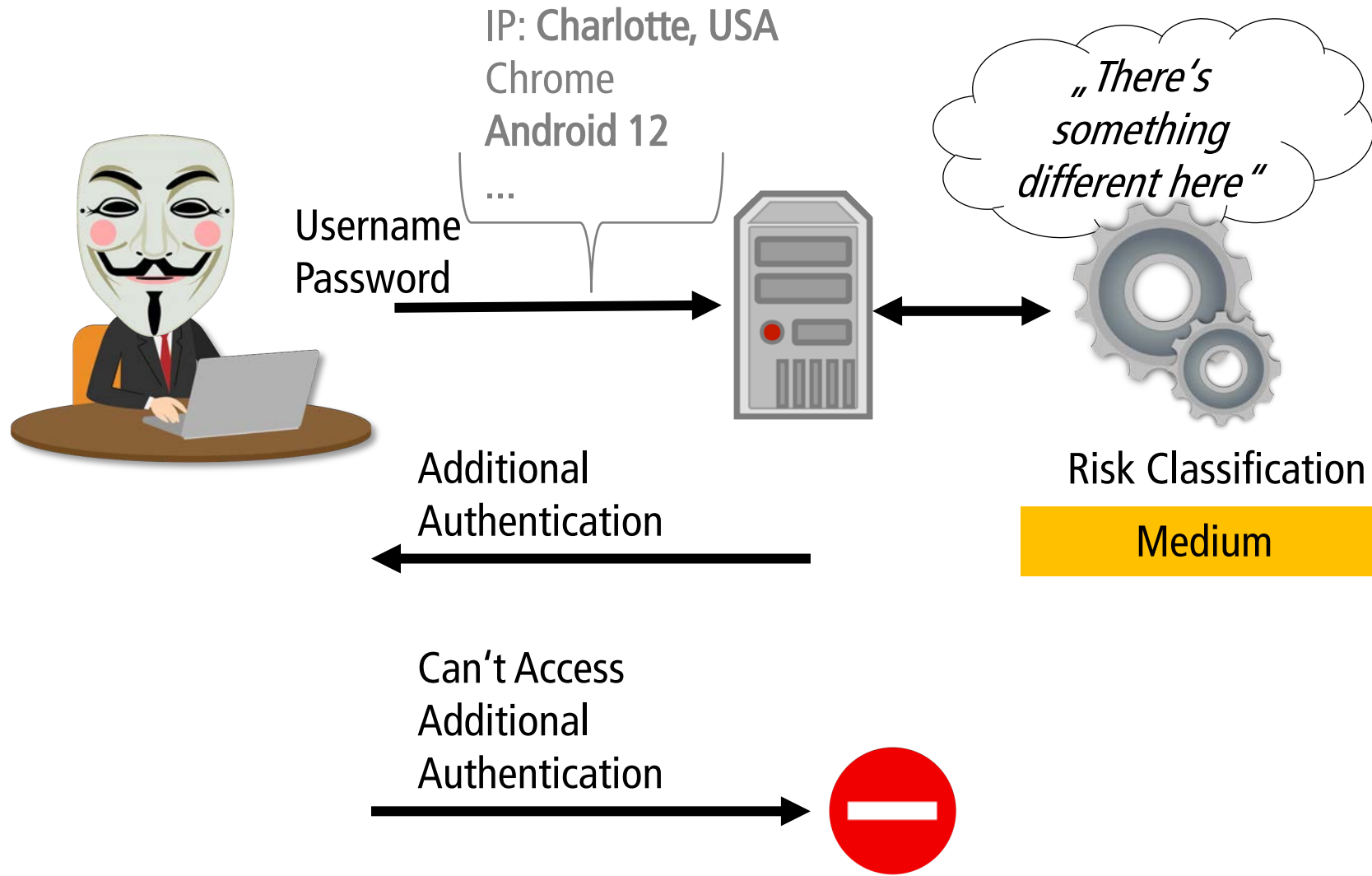


Risk Classification

Medium







Risk-Based Authentication

- Recommended by NIST^[1]

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

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. Lefkowitz
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>

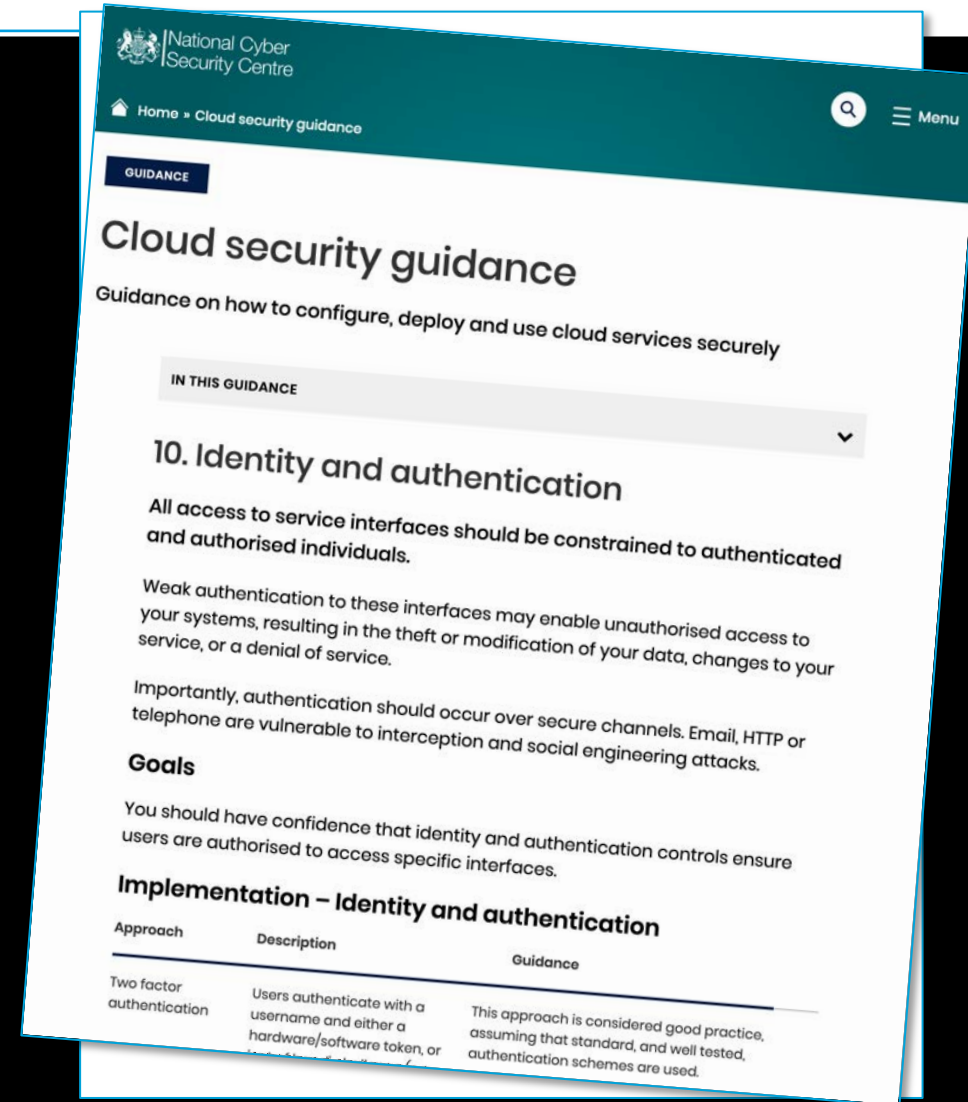
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Risk-Based Authentication

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

[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)



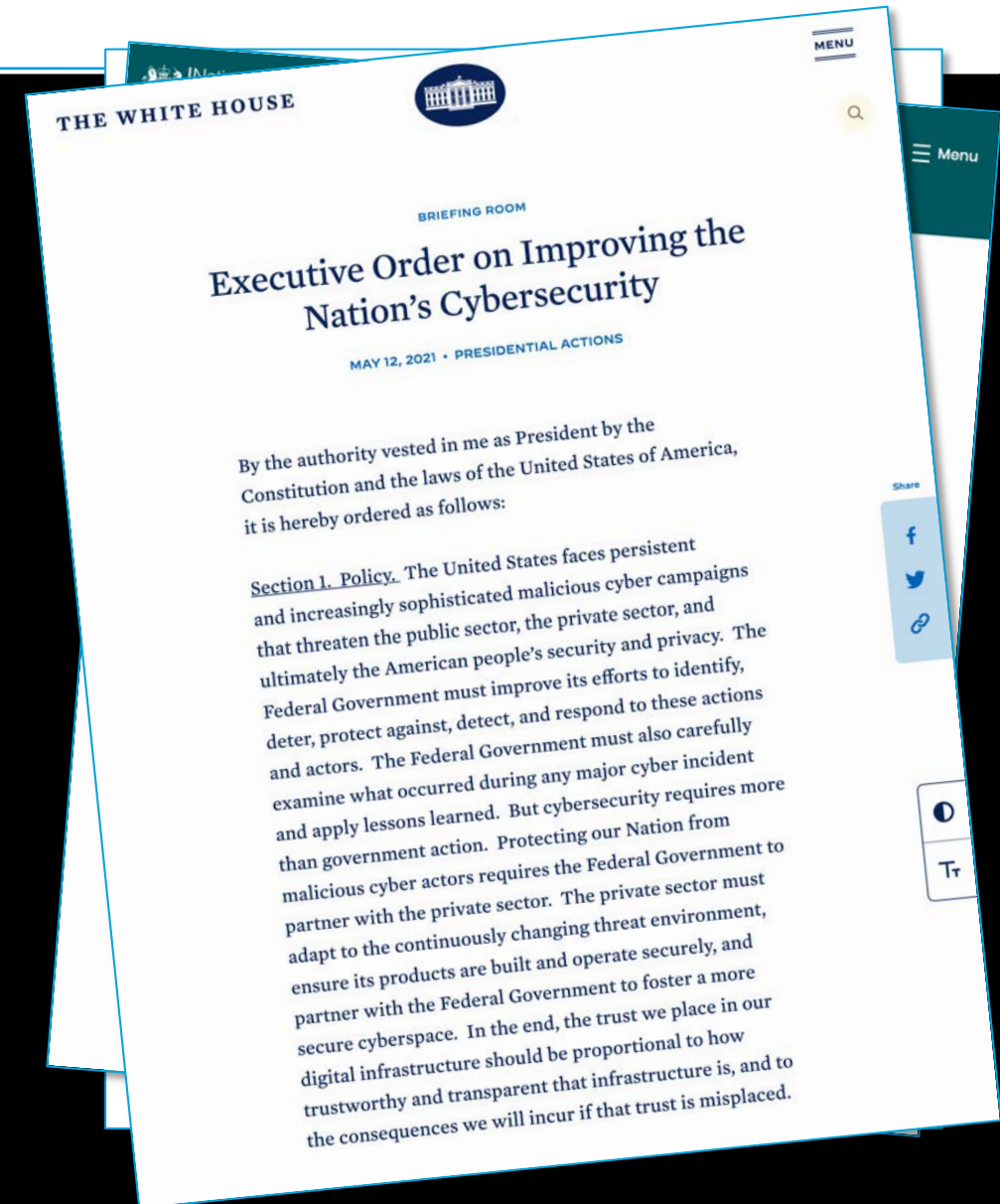
Risk-Based Authentication

- Recommended by NIST^[1], NCSC^[2] and others
- Required in the US by Presidential Order^[3]

[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

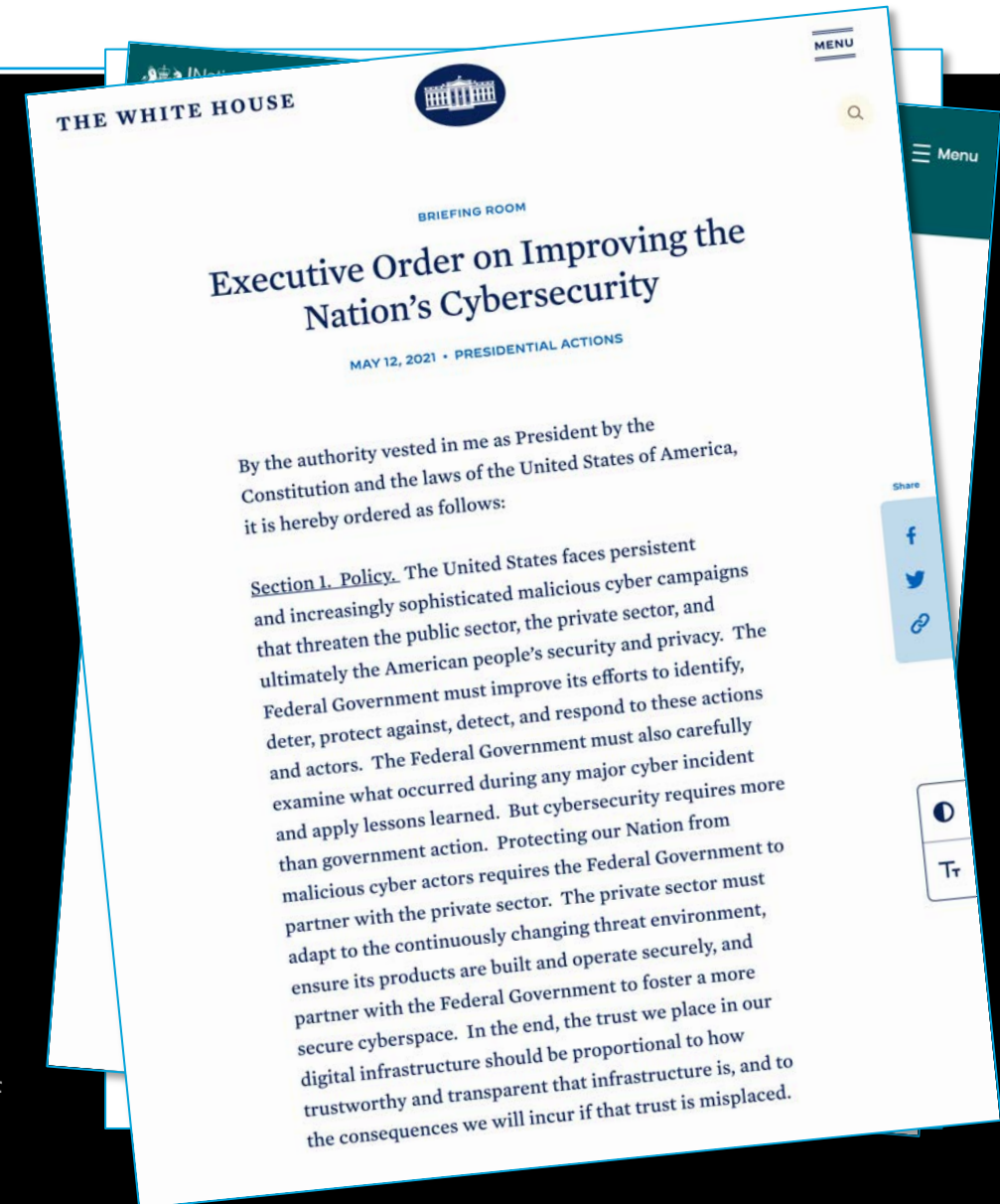
- Recommended by NIST^[1], NCSC^[2] and others
- Required in the US by Presidential Order^[3]
- More usable than comparable 2FA methods^[4]

[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] Wiefeling 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

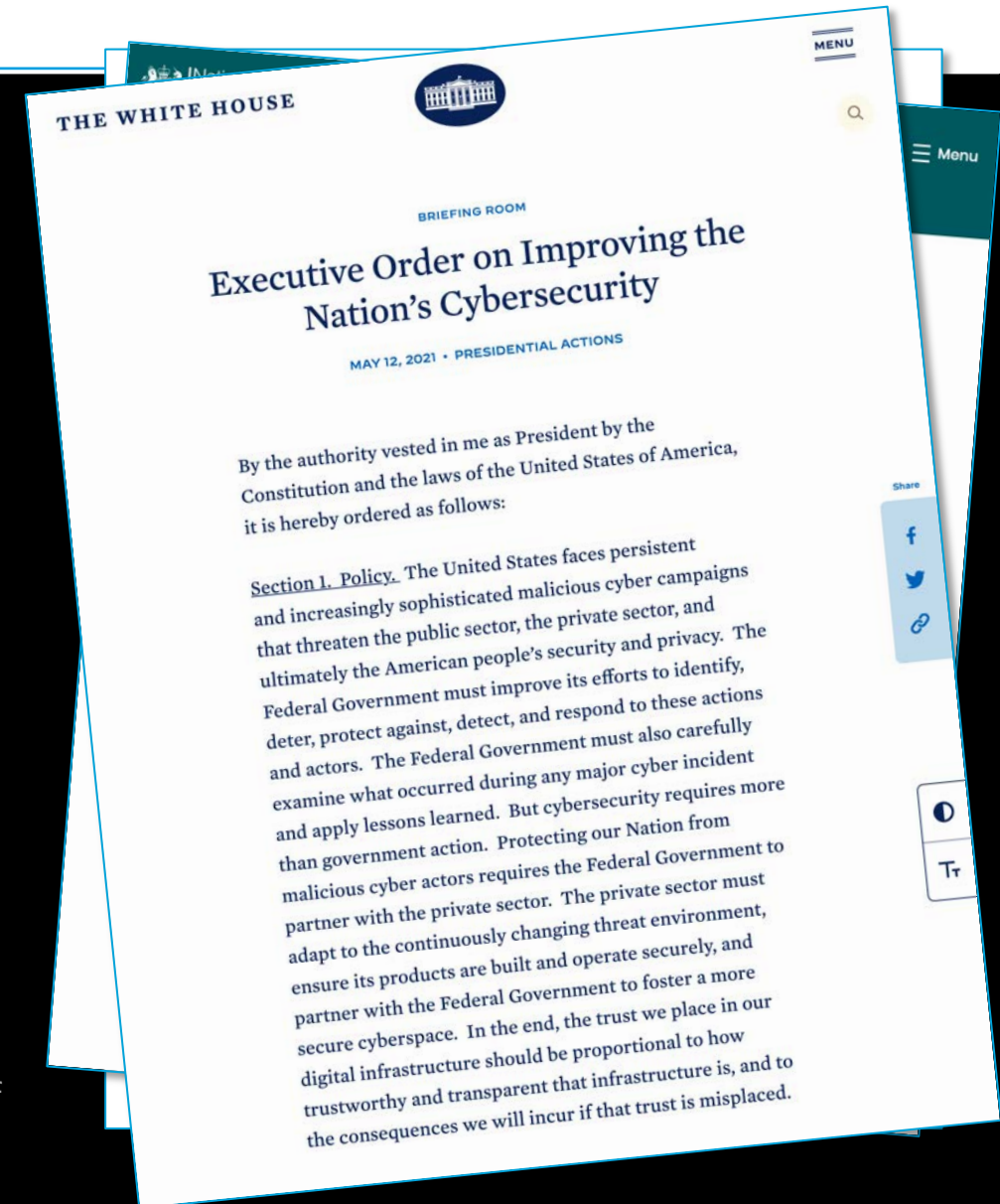
- Recommended by NIST^[1], NCSC^[2] and others
- Required in the US by Presidential Order^[3]
- More usable than comparable 2FA methods^[4]
- But: Lack of Open Source solutions

[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)

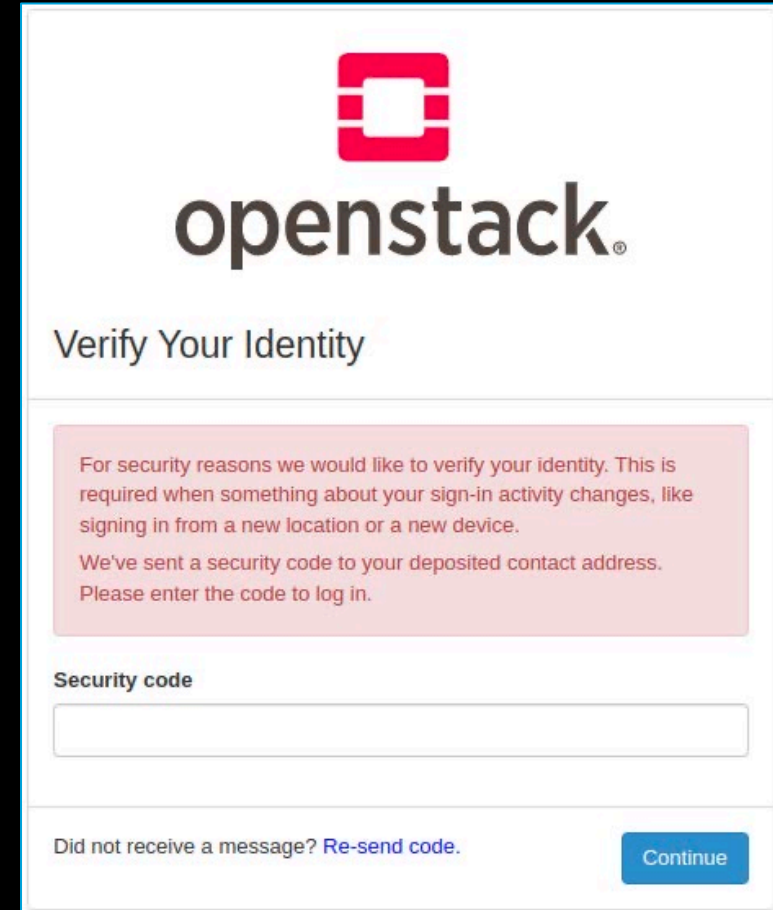
[3] Biden Jr., J.R.: Executive Order on Improving the Nation's Cybersecurity. The White House. (2021)

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



RBA Plugin

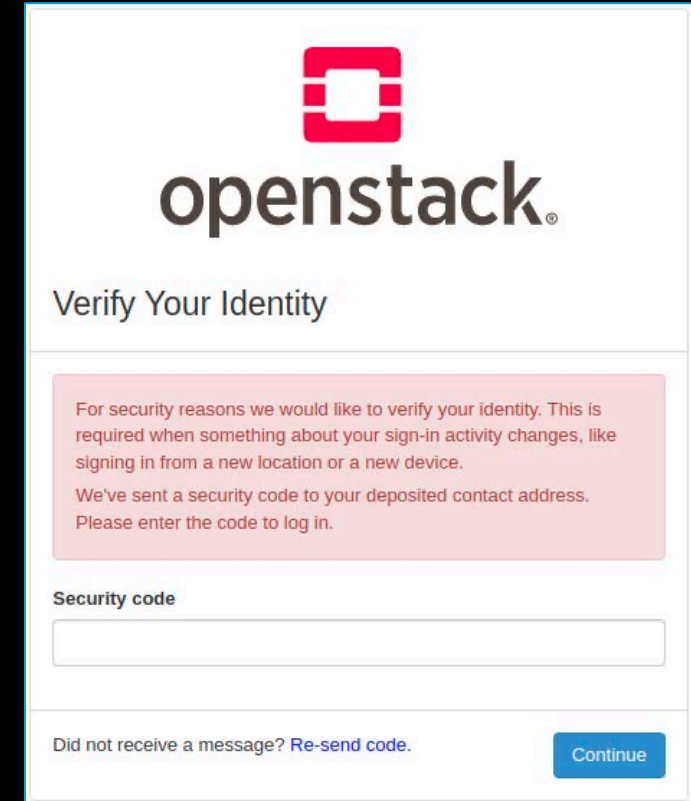
- First fully functional plugin for OpenStack cloud computing platform



The image shows a screenshot of the OpenStack 'Verify Your Identity' page. At the top is the OpenStack logo, which consists of a red square with a white 'O' inside, followed by the word 'openstack.' in a dark grey sans-serif font. Below the logo, the heading 'Verify Your Identity' is displayed in a dark grey font. A light red rectangular box contains the following text: '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 your deposited contact address. Please enter the code to log in.' Below this box, the label 'Security code' is positioned above a white text input field with a thin grey border. At the bottom of the page, there is a link that says 'Did not receive a message? [Re-send code.](#)' and a blue button with the text 'Continue'.

Frontend

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



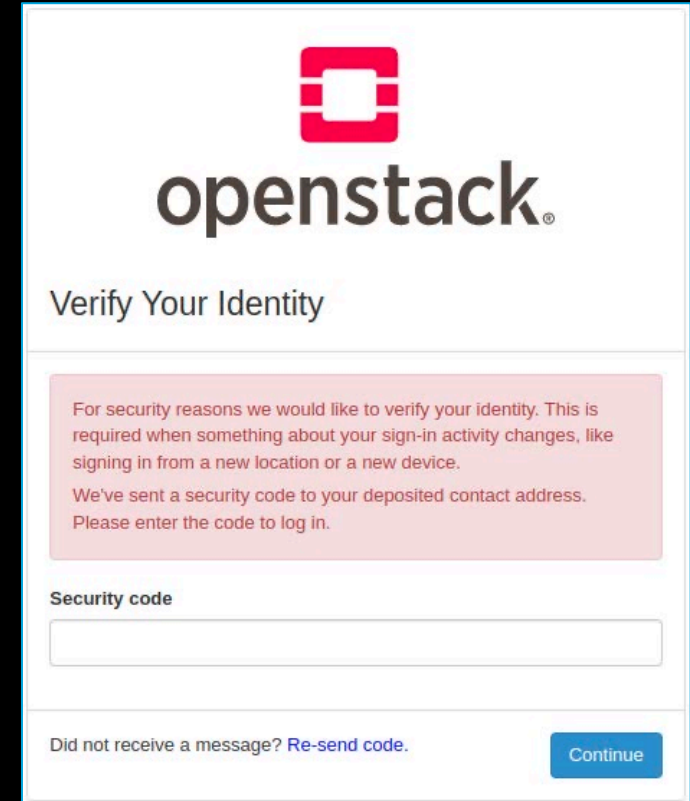
The image shows a screenshot of the OpenStack 'Verify Your Identity' page. At the top is the OpenStack logo (a red square with a white 'O' inside) and the text 'openstack®'. Below the logo is the heading 'Verify Your Identity'. A pink message box contains the text: 'For security reasons we would like 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 your deposited contact address. Please enter the code to log in.' Below this message box is a label 'Security code' and a text input field. At the bottom left, there is a link 'Did not receive a message? Re-send code.' and at the bottom right, a blue button labeled 'Continue'.


Wiefeling et al.: Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild. In: IFIP SEC (2019). Springer

Wiefeling 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




openstack®

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 your deposited contact address. Please enter the code to log in.

Security code

Did not receive a message? [Re-send code.](#) [Continue](#)

Wiefeling et al.: Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild. In: IFIP SEC (2019). Springer

Wiefeling 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

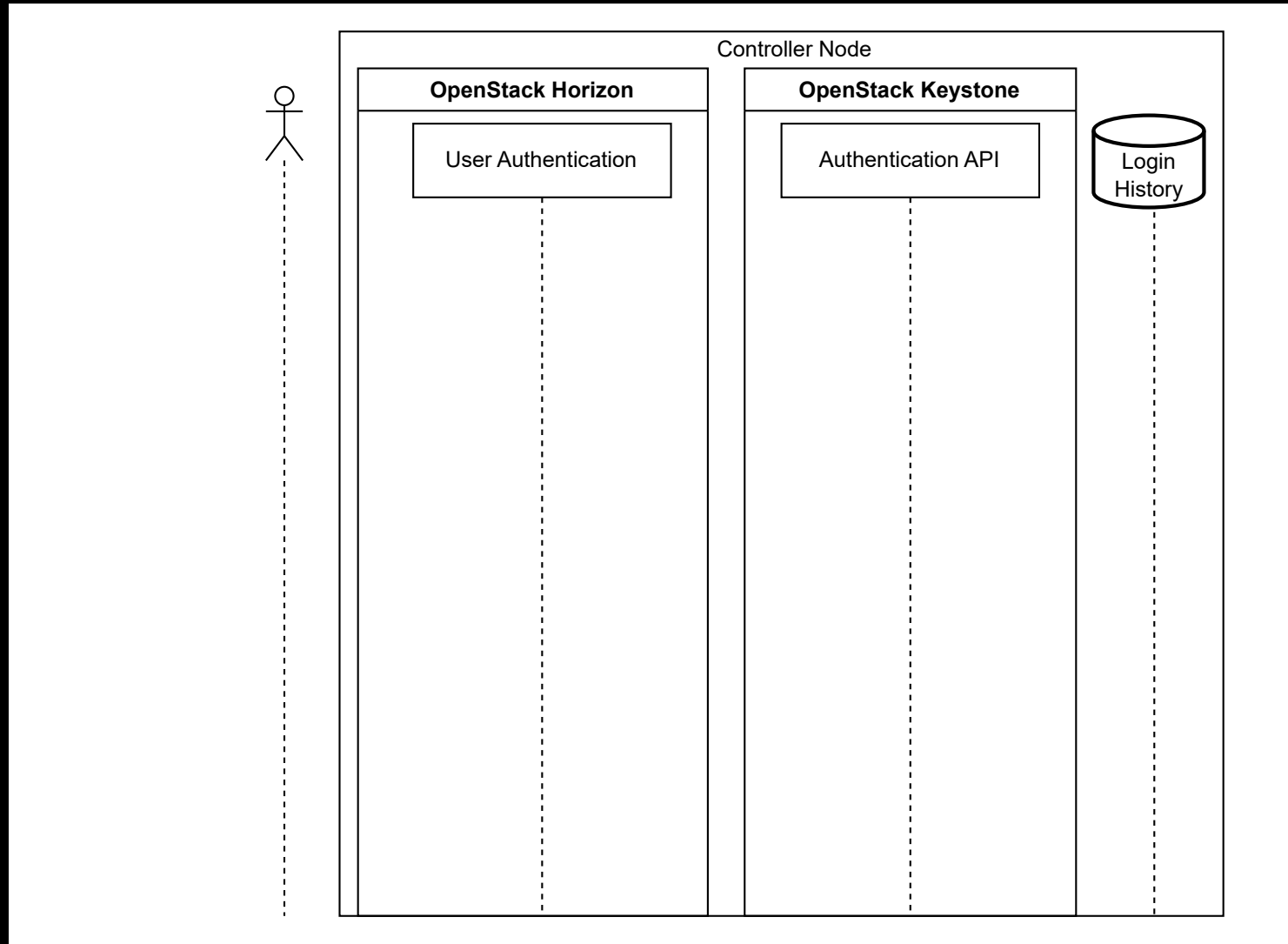
Wiefling et al.: Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service. In: TOPS (2023). ACM.

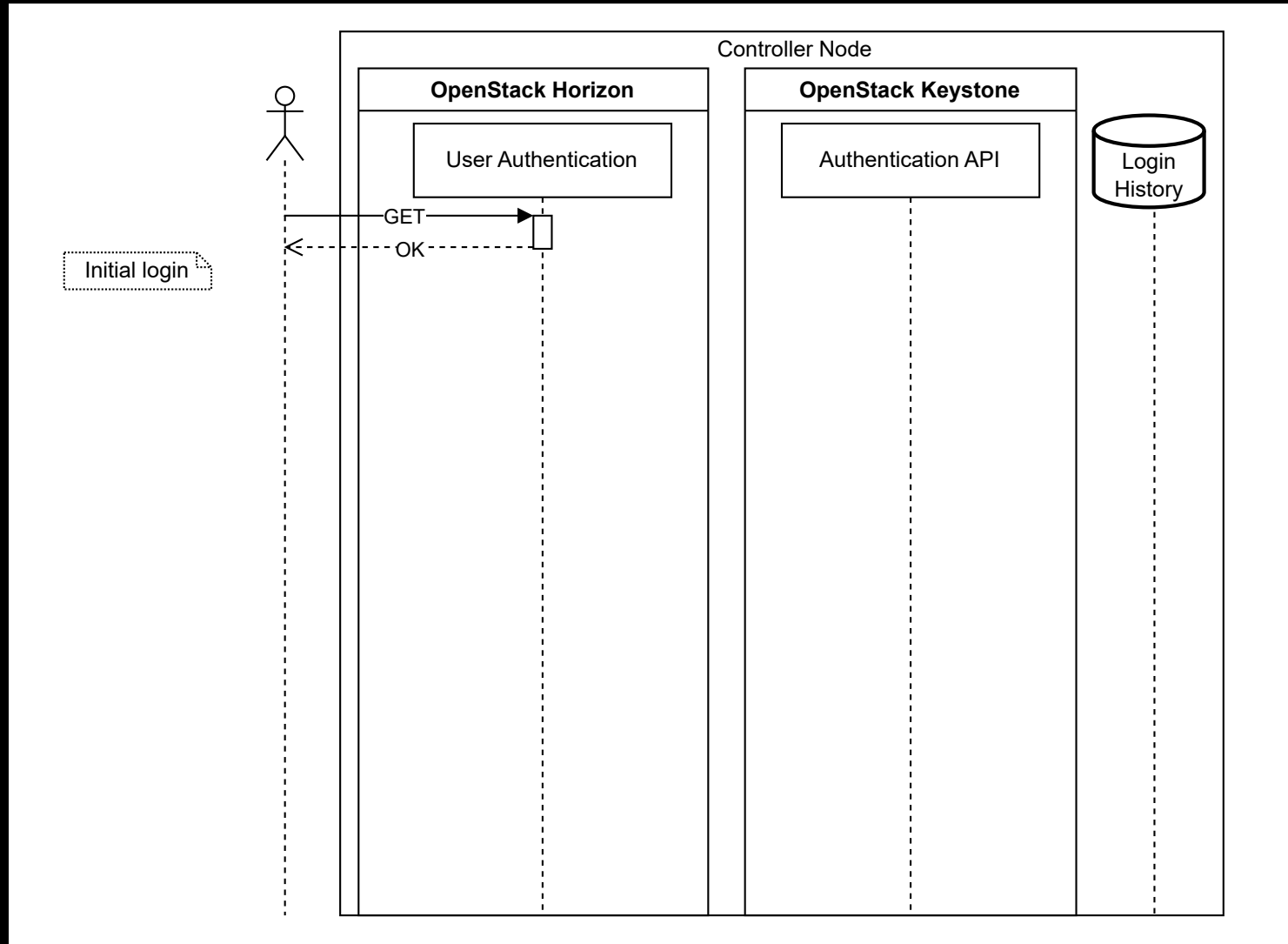
Freeman et al. Algorithm

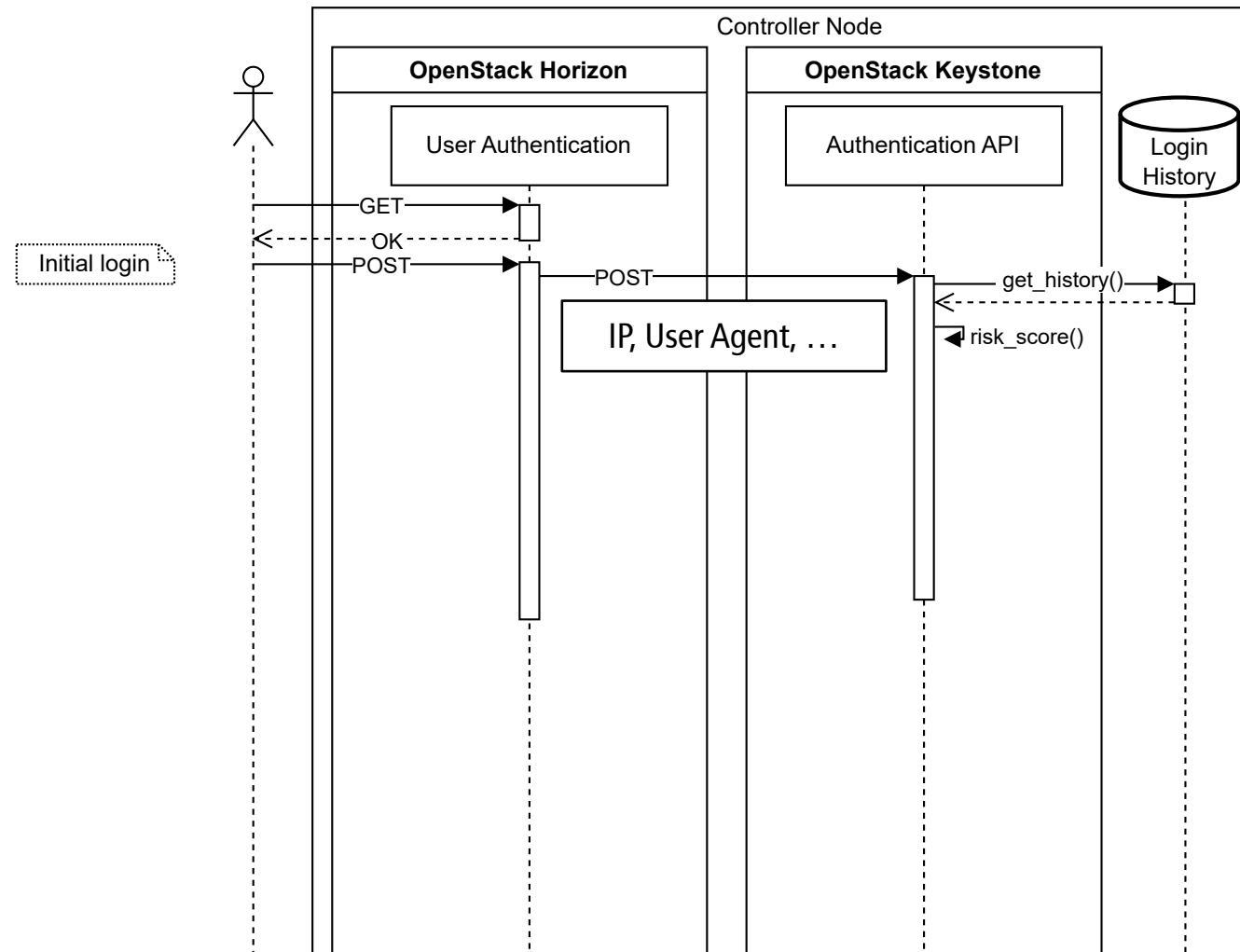
- Low Re-Authentication Rates in Practice
- Even when blocking 99% of targeted attackers*

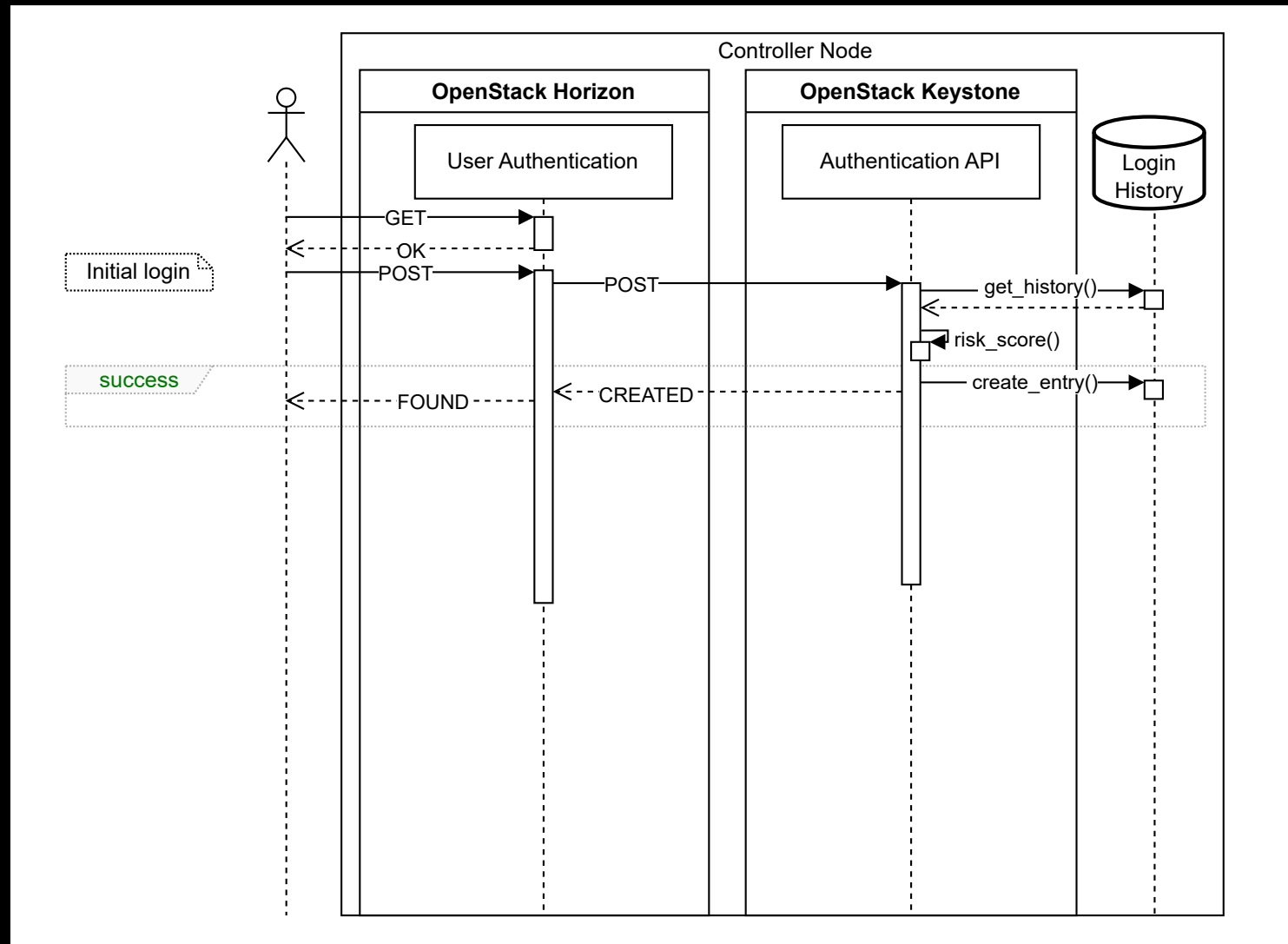
Freeman et al.: Who Are You? A Statistical Approach to Measuring User Authenticity. NDSS (2016)

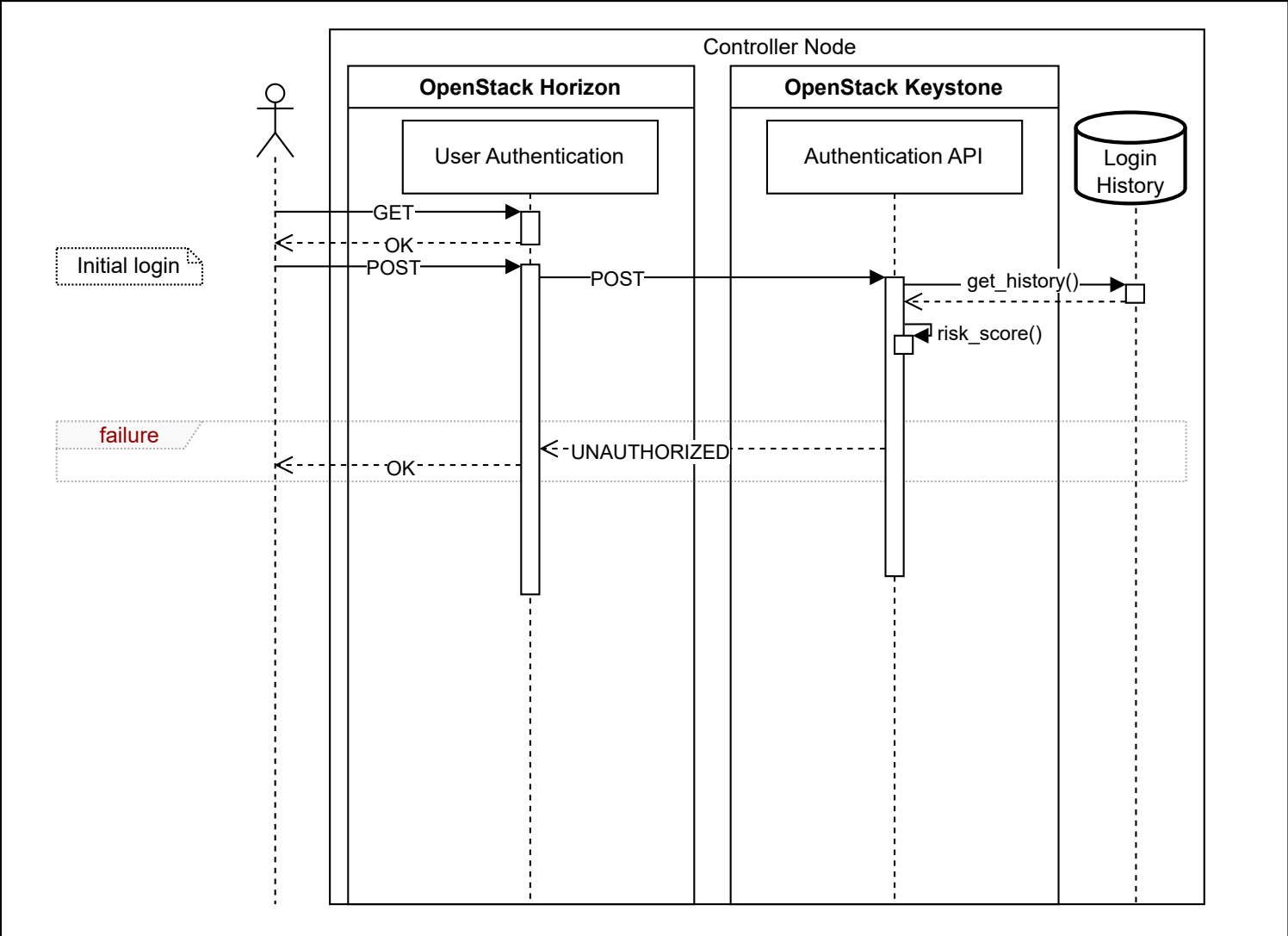
*Wiefling et al.: Pump Up Password Security! Evaluating and Enhancing Risk-Based Authentication on a Real-World Large-Scale Online Service. In: TOPS (2022) ACM

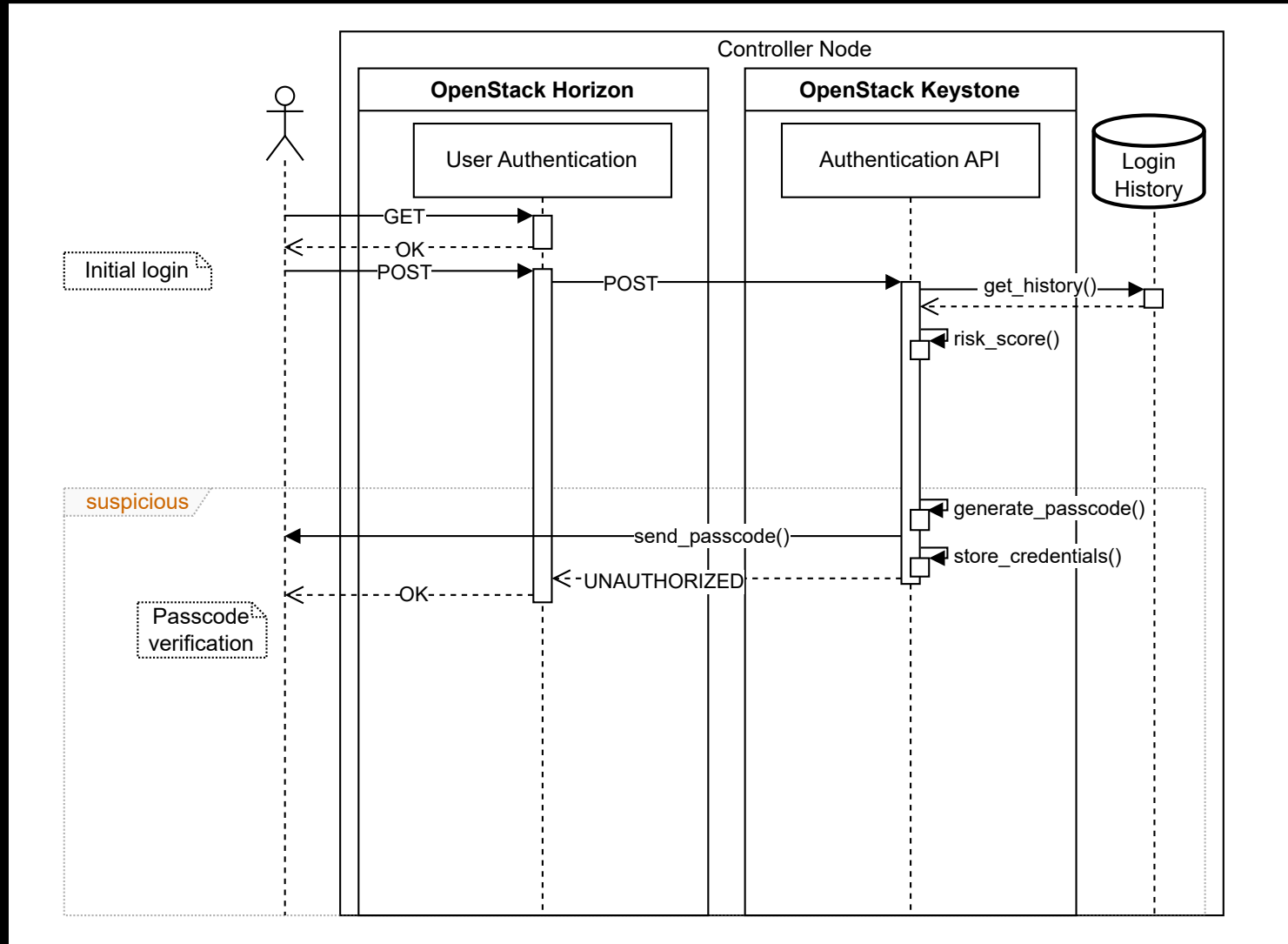


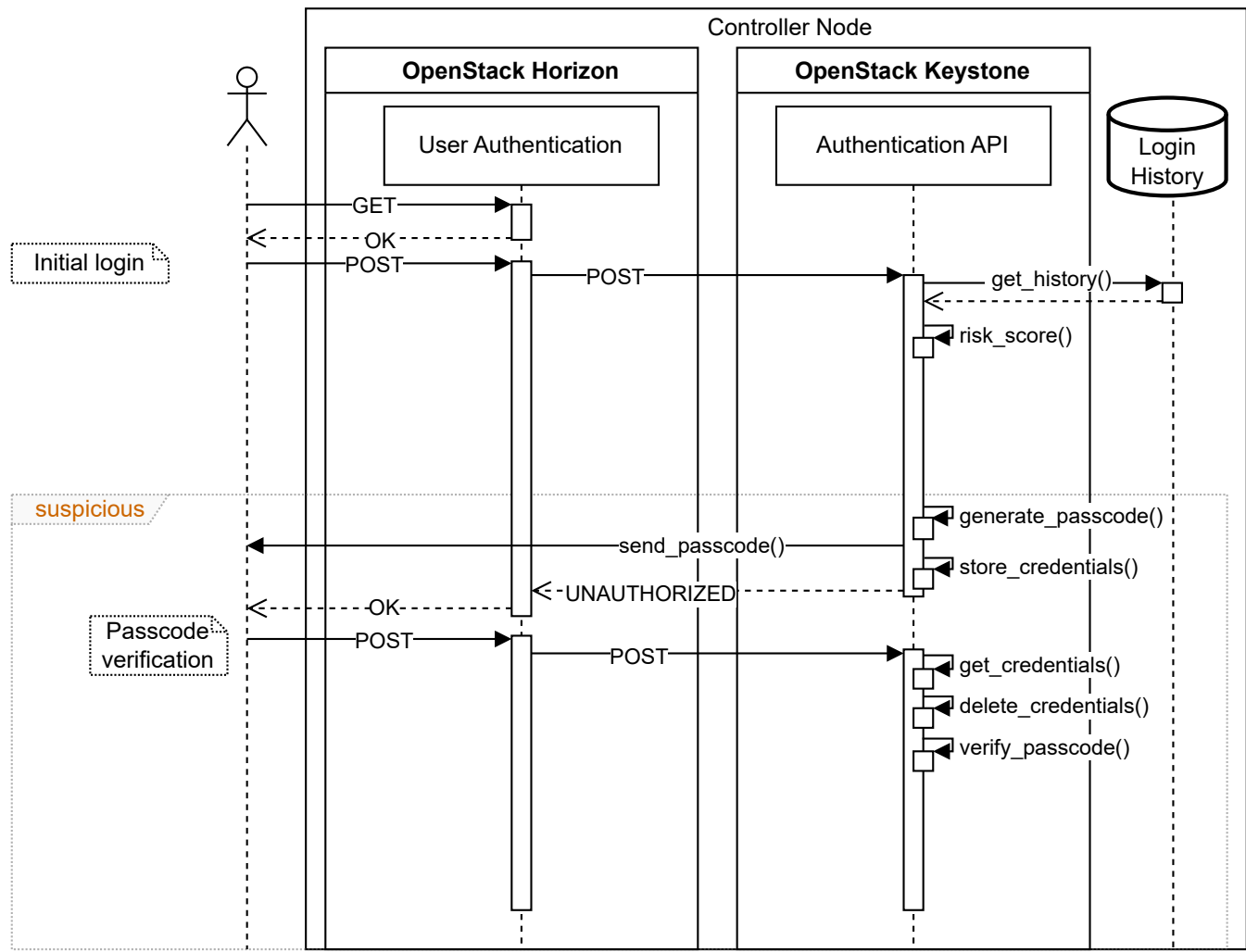


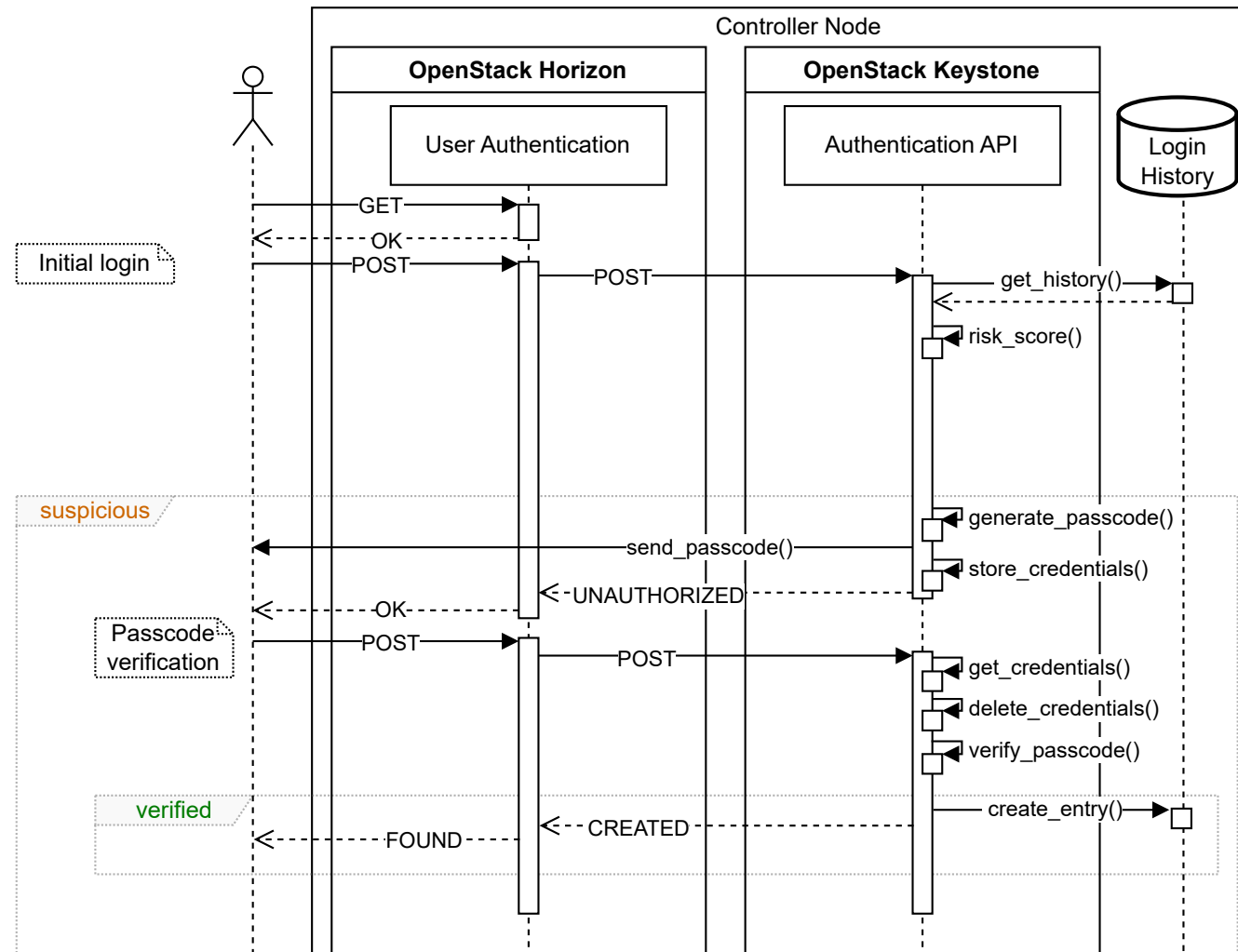


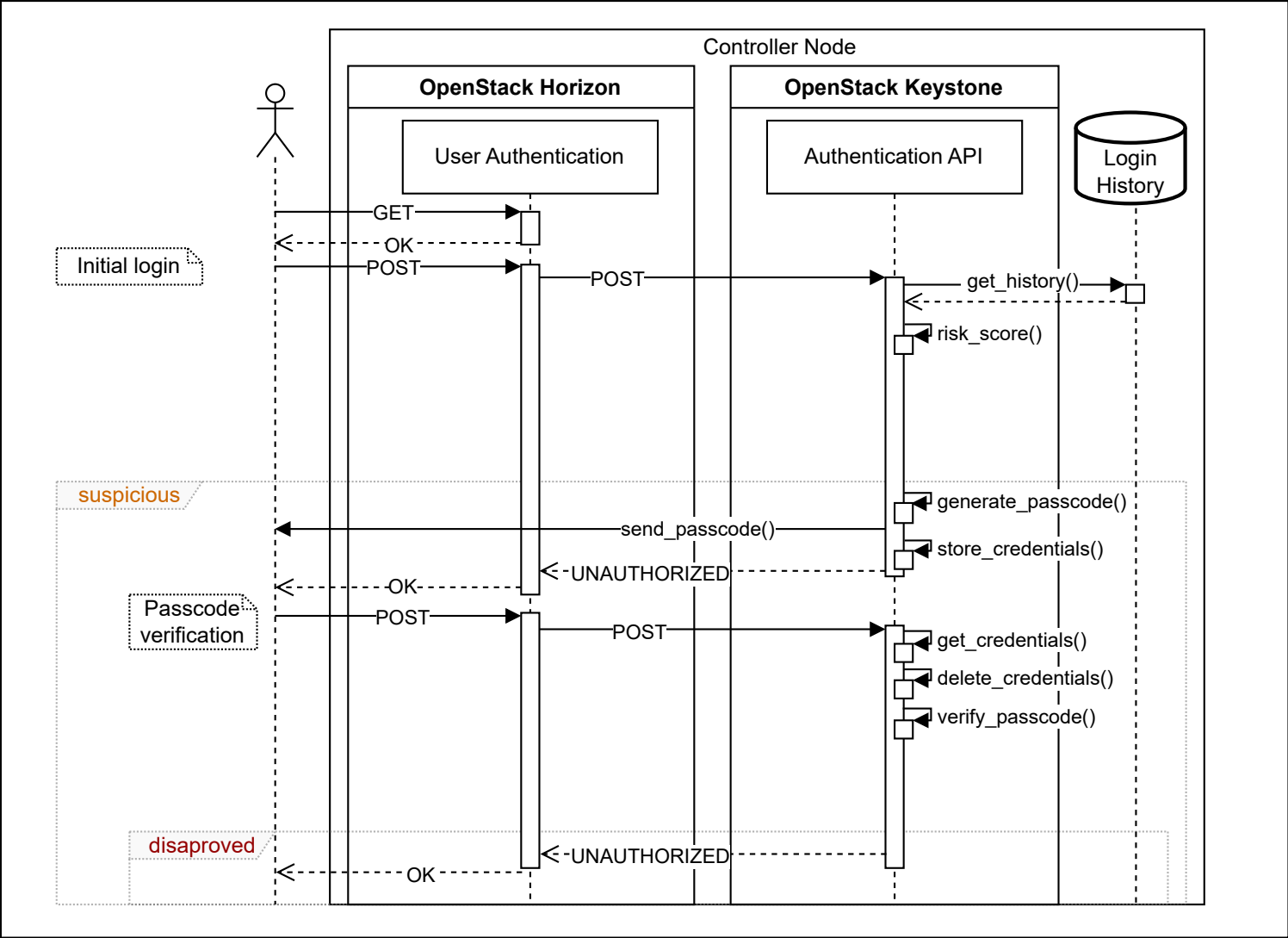




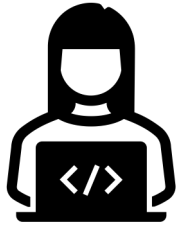








Summary



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



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



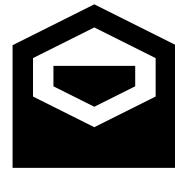
- Outlook:
 - Putting RBA into more Open Source software
 - Continuous Authentication

*rbainfo.org/opensource

Thank you



riskbasedauthentication.org
das.h-brs.de



stephan.wiefling@h-brs.de



[@swiefling@hci.social](https://mstdn.social/@swiefling)