



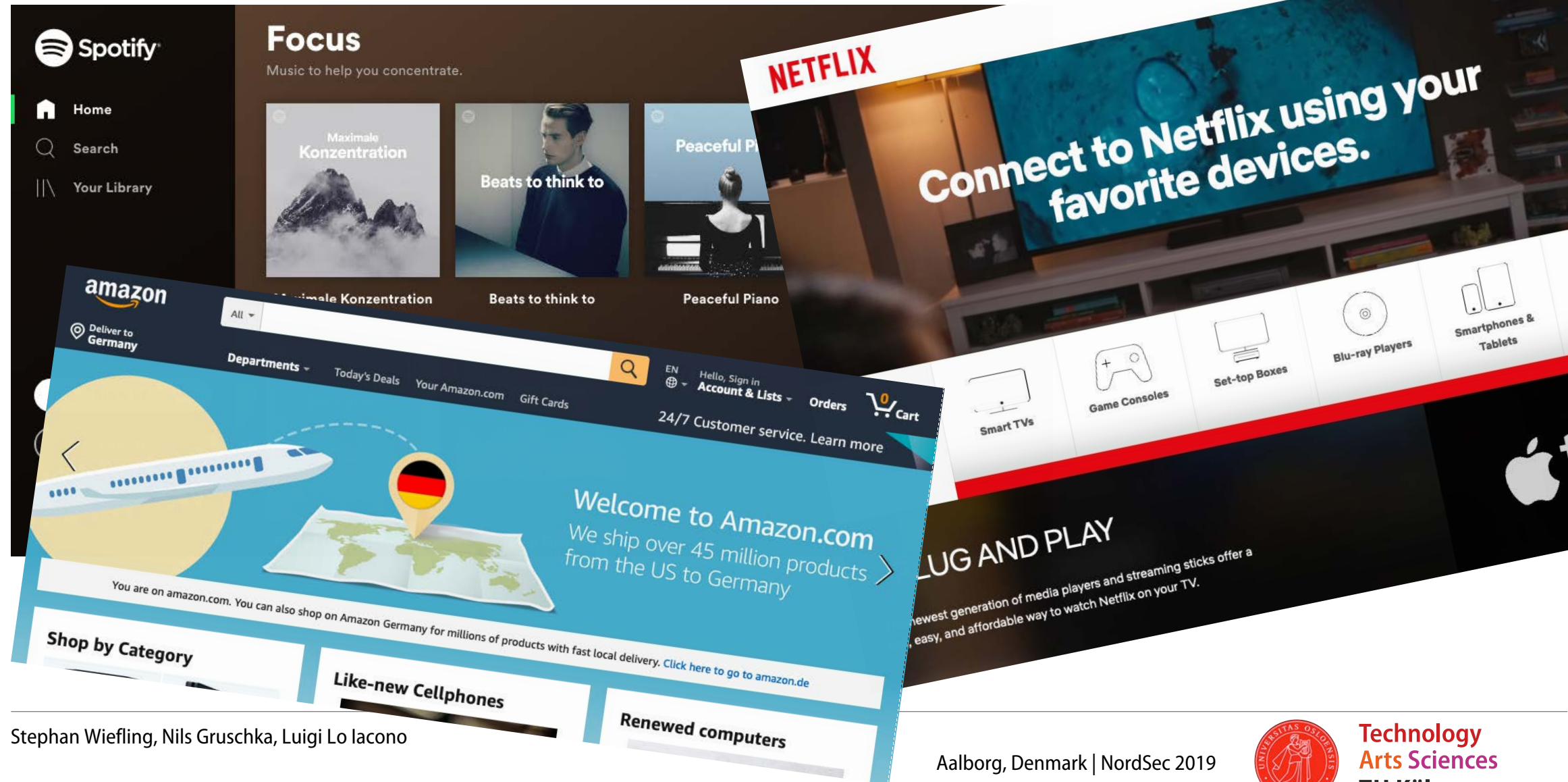
## Even Turing Should Sometimes Not Be Able To Tell: Mimicking Humanoid Usage Behavior for Exploratory Studies of Online Services

Stephan Wiefeling<sup>1</sup>, Nils Gruschka<sup>2</sup>, Luigi Lo Iacono<sup>1</sup>

<sup>1</sup> TH Köln – University of Applied Sciences

<sup>2</sup> University of Oslo

# Motivation



Stephan Wiefeling, Nils Gruschka, Luigi Lo Iacono

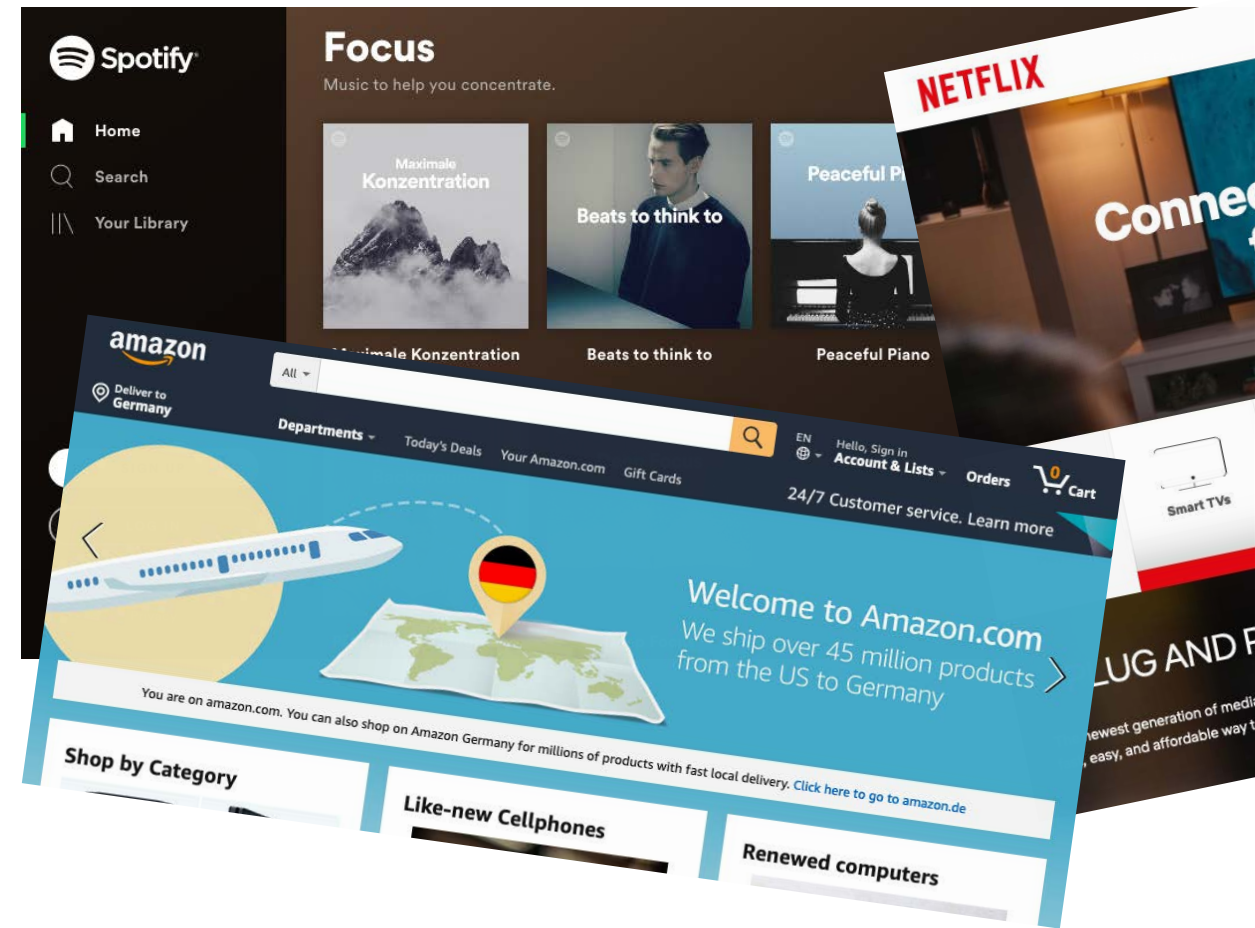
Aalborg, Denmark | NordSec 2019



Technology  
Arts Sciences  
TH Köln

# Motivation

- Algorithms impact our society
- Technical aspects hidden behind user interfaces
- Data availability needed for reliable research



# Motivation

- Most online services are black boxes
- Lack of transparency hinders research
- Reverse engineering needed



# Reverse engineering is complicated...

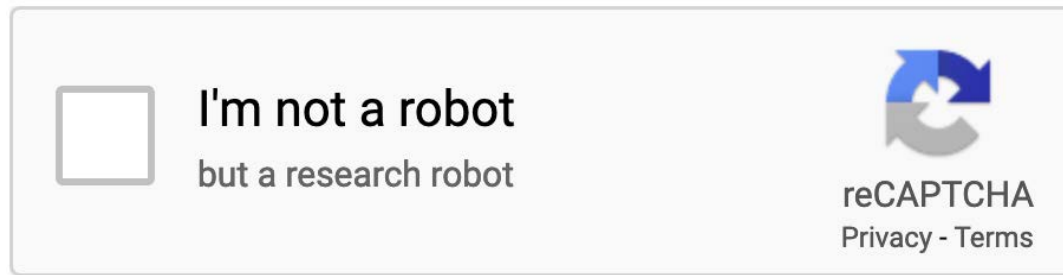


# Reverse engineering is complicated...

- No unique path to conduct such an analysis
- Services implement countermeasures

# Reverse engineering is complicated...

- No unique path to conduct such an analysis
  - Services implement countermeasures
- Camouflage measures needed





# HOSIT





# Humanoid Online Service Inspection Tool



# Overview

1. Tool



2. Proof of Concept



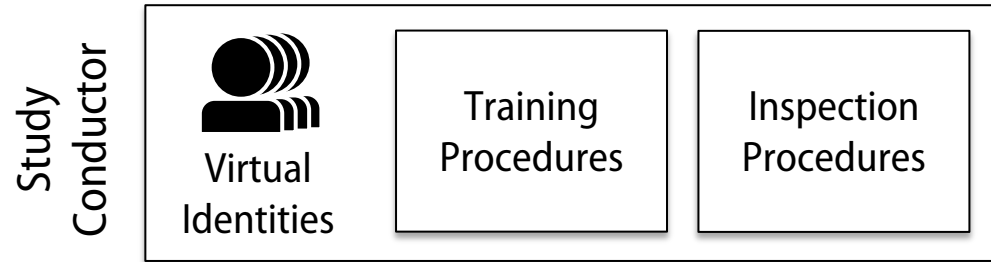
3. Conclusion

# Inspection Tool

- Simulates human-like browsing behavior on online services
- All actions have to be predefined by the researchers
  - Reliable and reproducible research
- Based on Puppeteer API



# Inspection Tool



# Virtual Identities

- Define properties
  - Typing, clicking behavior
  - Interests
  - ...



# Training Procedures

- New accounts are considered suspicious
- Need to create valid behavior first
- Takes time



# Training Procedures

- Define activities to be performed on online service
  - and other online services (tracking)
- Executed multiple times





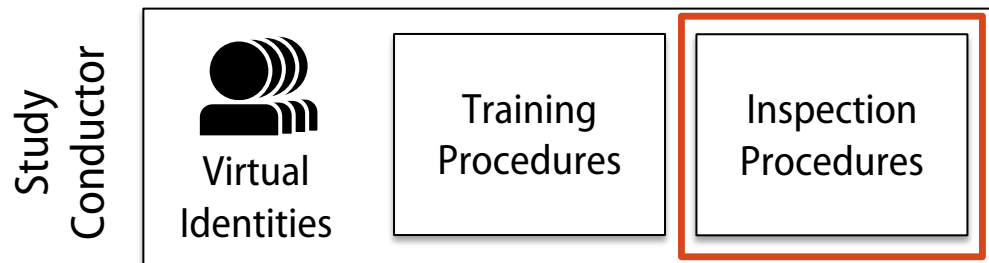
# Training Procedures

- Let the service learn “normal” behavior
- Get tracked on other websites by the service
- Desired result:
  - Get labeled as “normal” user

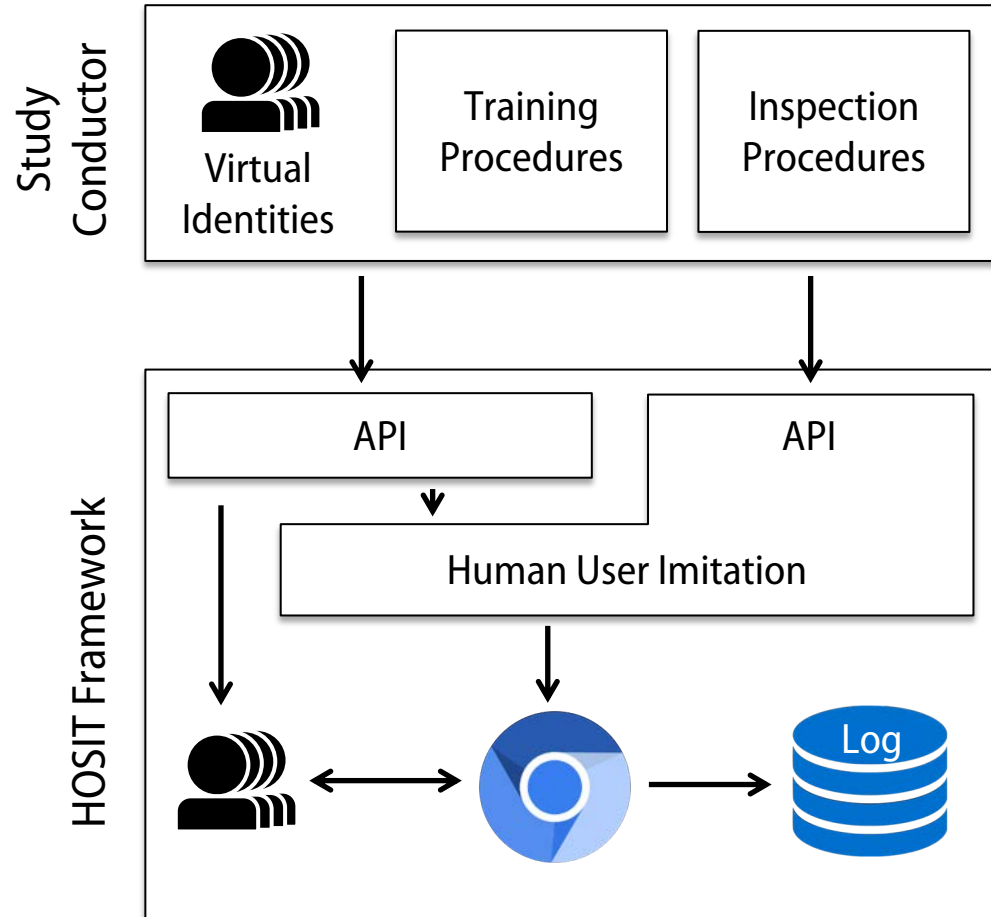


# Inspection Procedures

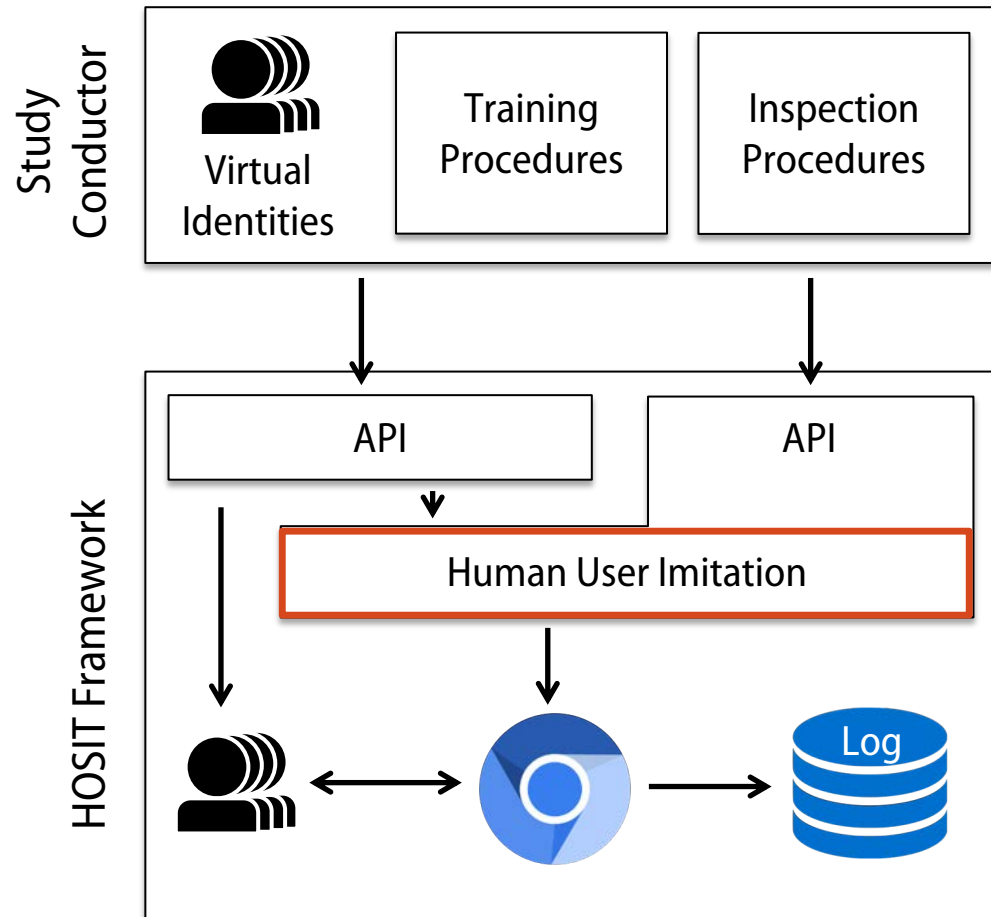
- Create unusual behavior at online service
- Analyze services' reaction to unusual behavior



# Inspection Tool

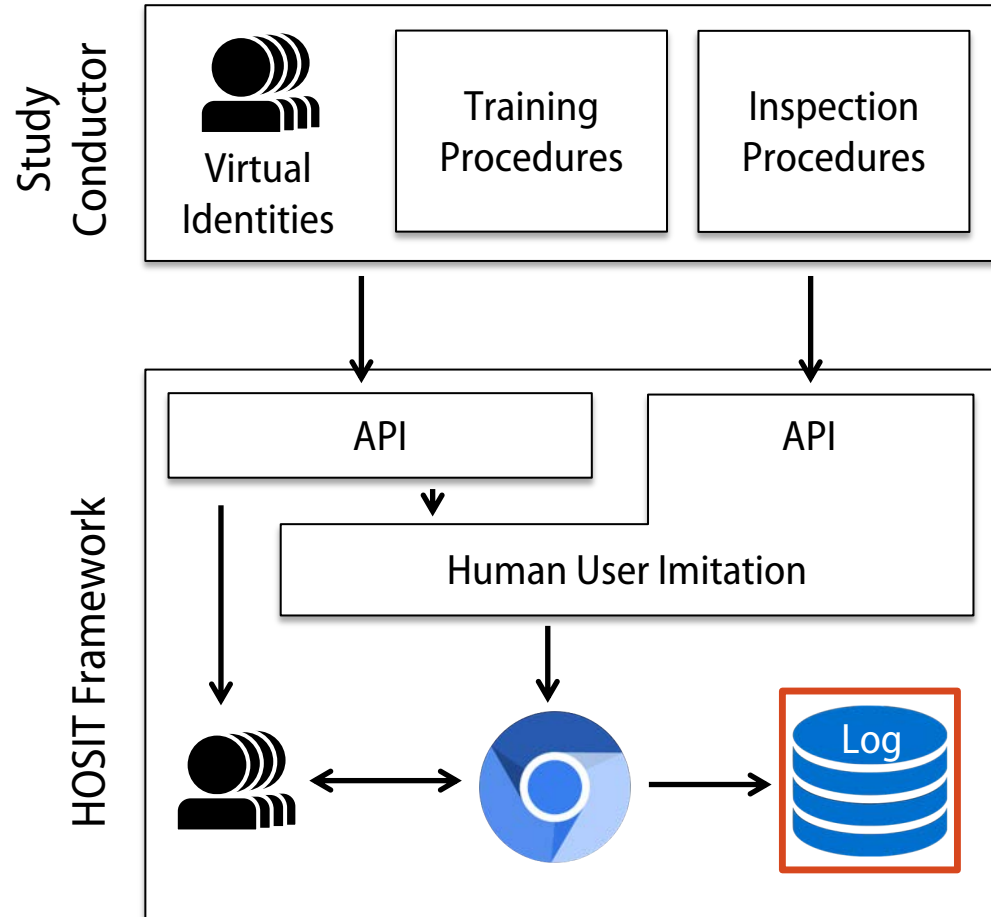


# Inspection Tool



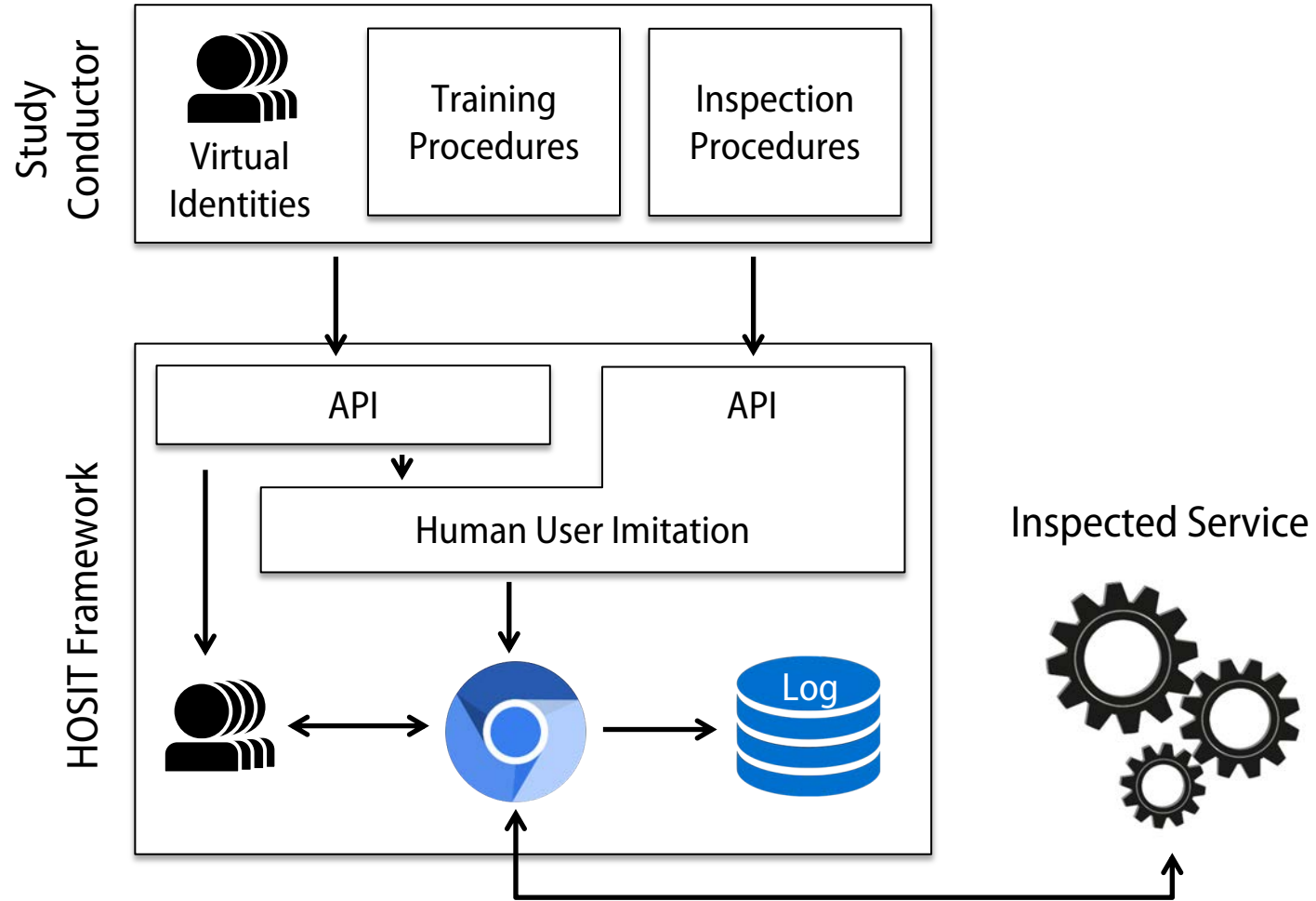
- Executes the actions
- Adds human-imitating behavior to function calls
- Properties of virtual identity

# Inspection Tool



- Logs all actions with screenshots
- Reproducibility

# Inspection Tool



# Why do we need another browser automation tool?



# Click Behavior



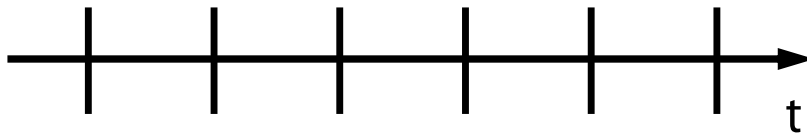
**Puppeteer 0.13.0**



**HOSIT**

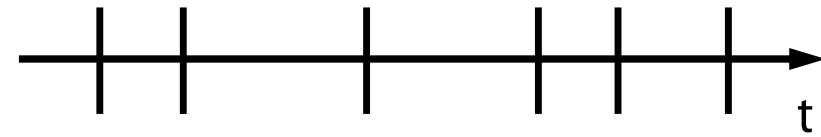
\* Komandur et al.: Relation between mouse button click duration and muscle contraction time. In: EMBC '08. (Aug 2008)

# Typing Speed



Constant delay

**Puppeteer 0.13.0**

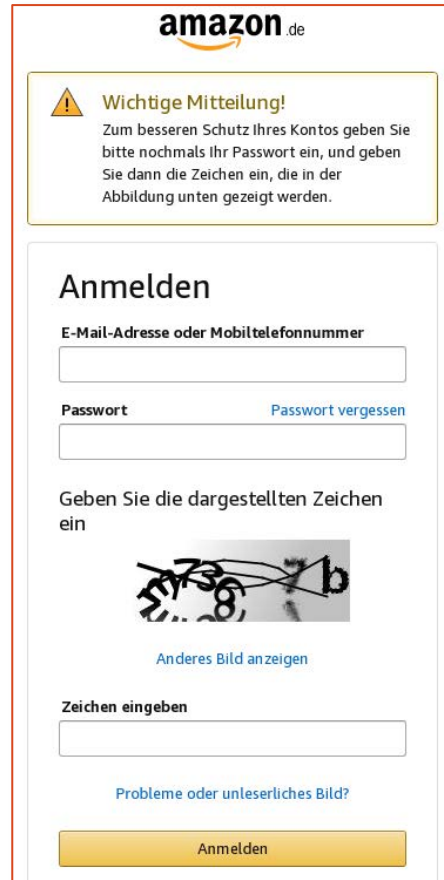


Randomized variations\*

**HOSIT**

\* Drury, C.G., Hoffmann, E.R.: A model for movement time on data-entry keyboards. *Ergonomics* 35(2) (Feb 1992)

# Bot Detection Protection



amazon.de


**Wichtige Mitteilung!**  
Zum besseren Schutz Ihres Kontos geben Sie bitte nochmals Ihr Passwort ein, und geben Sie dann die Zeichen ein, die in der Abbildung unten gezeigt werden.

**Anmelden**

E-Mail-Adresse oder Mobiltelefonnummer

Passwort [Passwort vergessen](#)

Geben Sie die dargestellten Zeichen ein

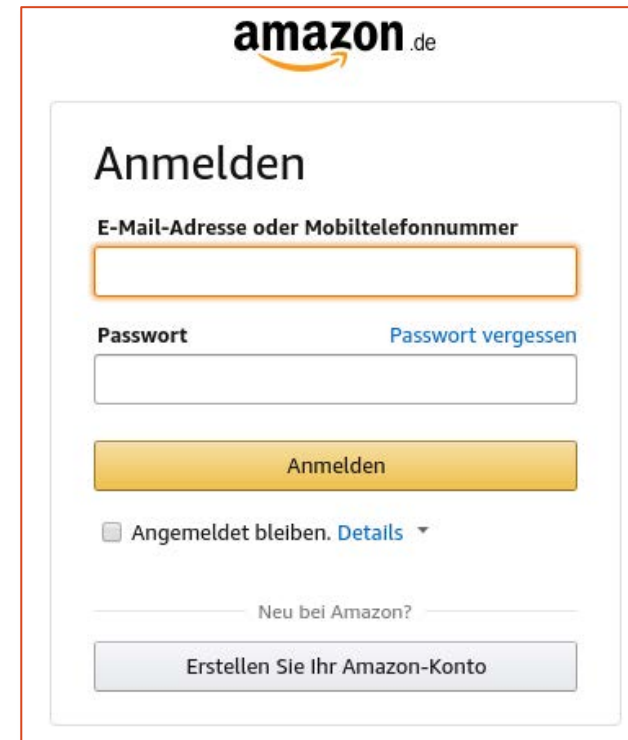


[Anderes Bild anzeigen](#)

Zeichen eingeben

[Probleme oder unleserliches Bild?](#)

Puppeteer 0.13.0



amazon.de

**Anmelden**

E-Mail-Adresse oder Mobiltelefonnummer

Passwort [Passwort vergessen](#)

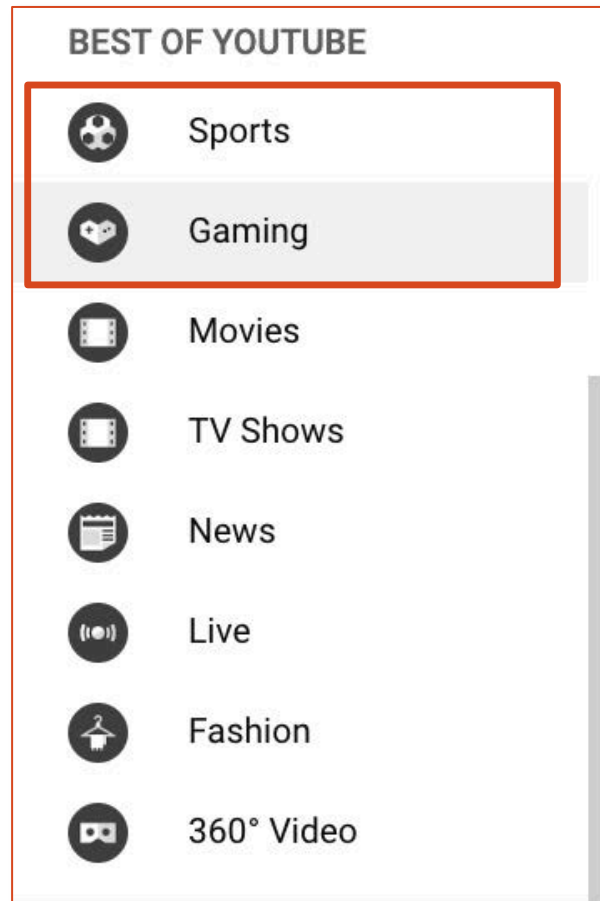
☐ Angemeldet bleiben. [Details](#)

Neu bei Amazon?

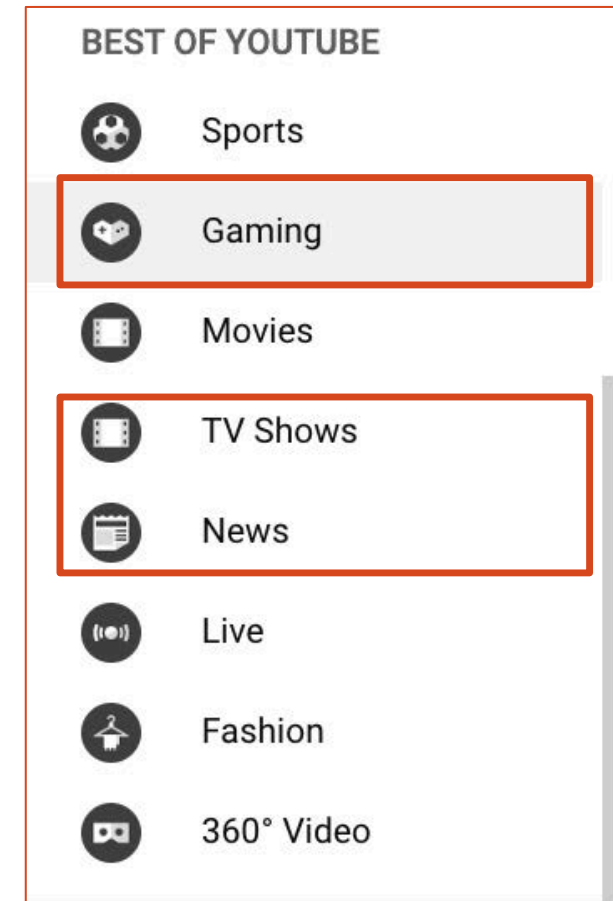
HOSIT

# Browsing Behavior Changes

Persona A



Persona B



# More Functions

- Common workflows integrated
- Search query generator
- CAPTCHA solving
- Scrolling
- Select tabs

# Example Script

- Opens a search engine
- Clicks on image search
- Types random search query covered in the media
- Scrolls to bottom of results

```
// Open new page tab
await controller.newPage("https://www.startpage.com/");

// Wait a random time period
await controller.randomWait();

// Click on the "Images"-Link
await controller.click("a[href='https://www.startpage.com/en/pics.html']");

// Wait until the text field is loaded
await controller.waitForSelector("input[type='text']");

// Generate and enter search query based on
// current events in media
await controller.typeSearchQuery("input[type='text']");

// Scroll to the bottom of the page
await controller.scrollToBottom();
```

# Example Script

- Video recorded at October 22<sup>nd</sup>, 2019

```
// Open new page tab
await controller.newPage("https://www.startpage.com/");

// Wait a random time period
await controller.randomWait();

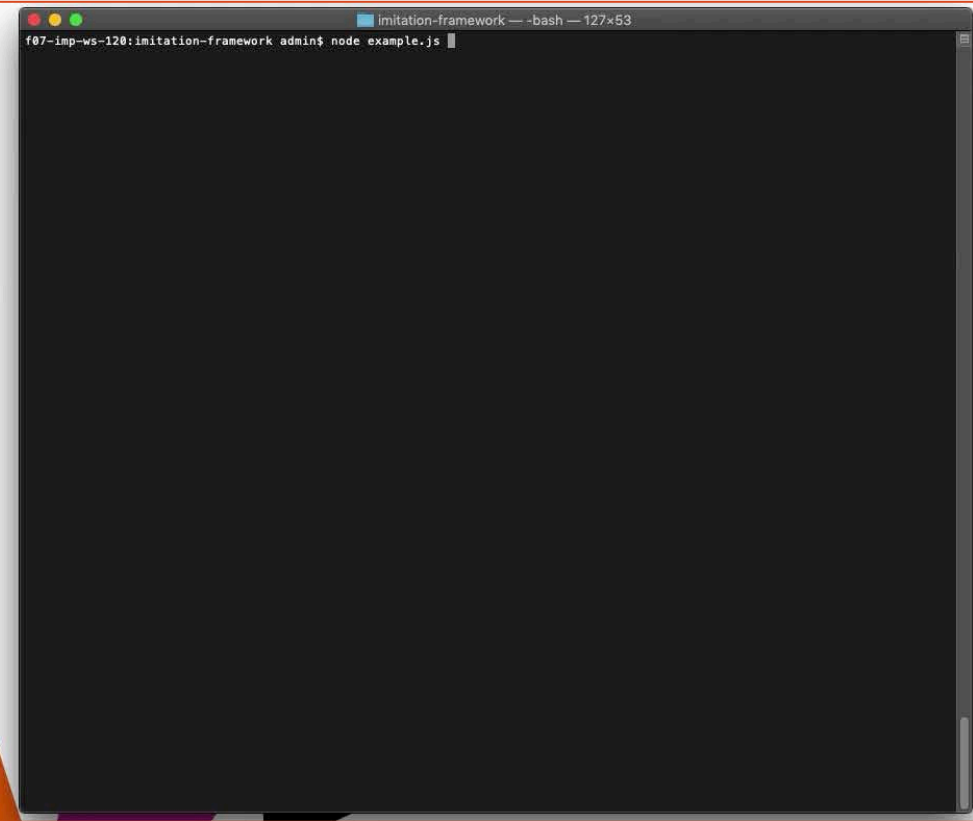
// Click on the "Images"-Link
await controller.click("a[href='https://www.startpage.com/en/pics.html']");

// Wait until the text field is loaded
await controller.waitForSelector("input[type='text']");

// Generate and enter search query based on
// current events in media
await controller.typeSearchQuery("input[type='text']");

// Scroll to the bottom of the page
await controller.scrollToBottom();
```

/IDA





# Overview

1. Tool



2. Proof of Concept



3. Conclusion

# Proof of Concept

- Study on Risk-based Authentication\*
- Required human-like behavior from clients



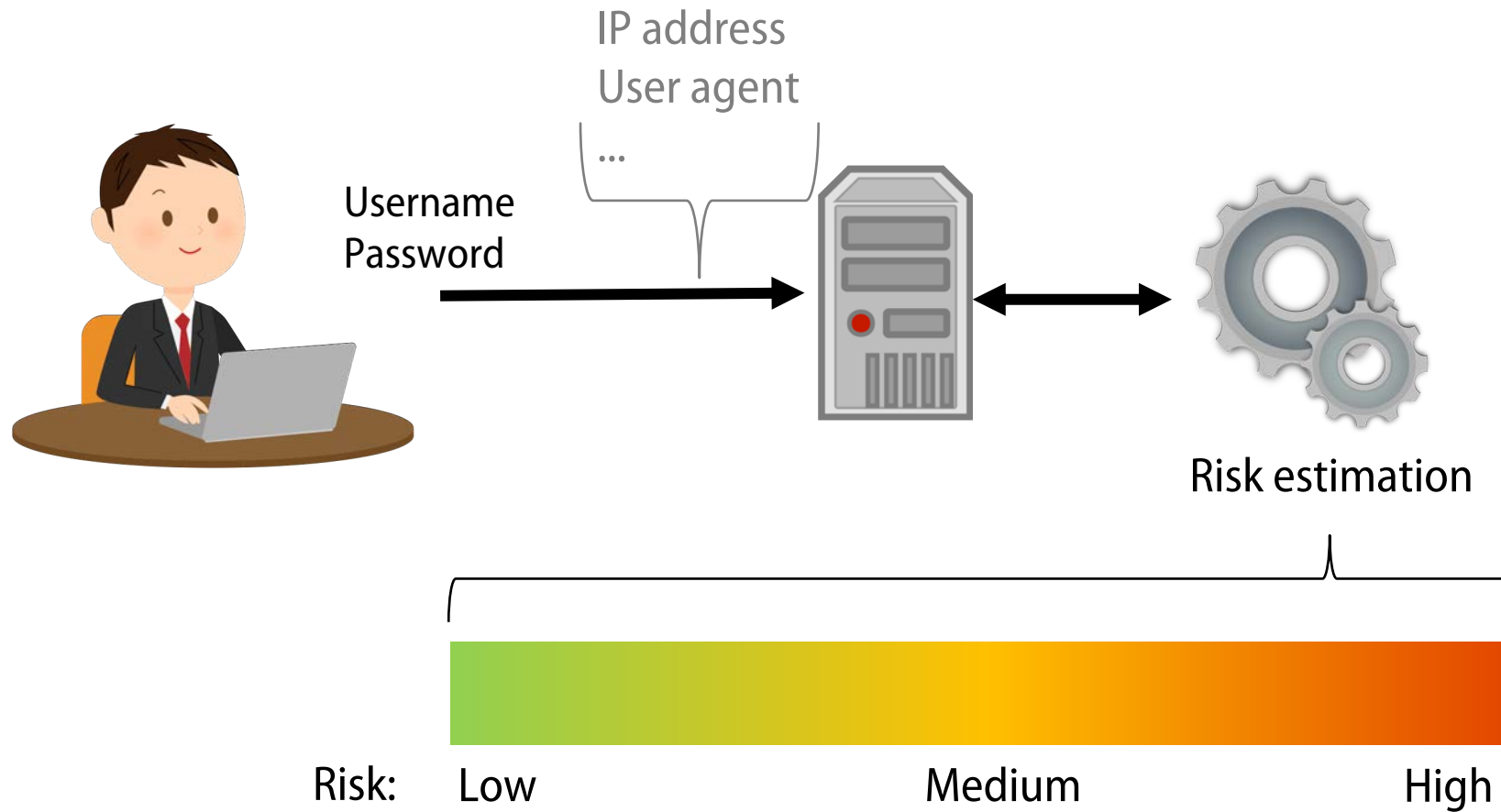
\* Wiefeling et al.: Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild. In: IFIP SEC '19. (Jun 2019)

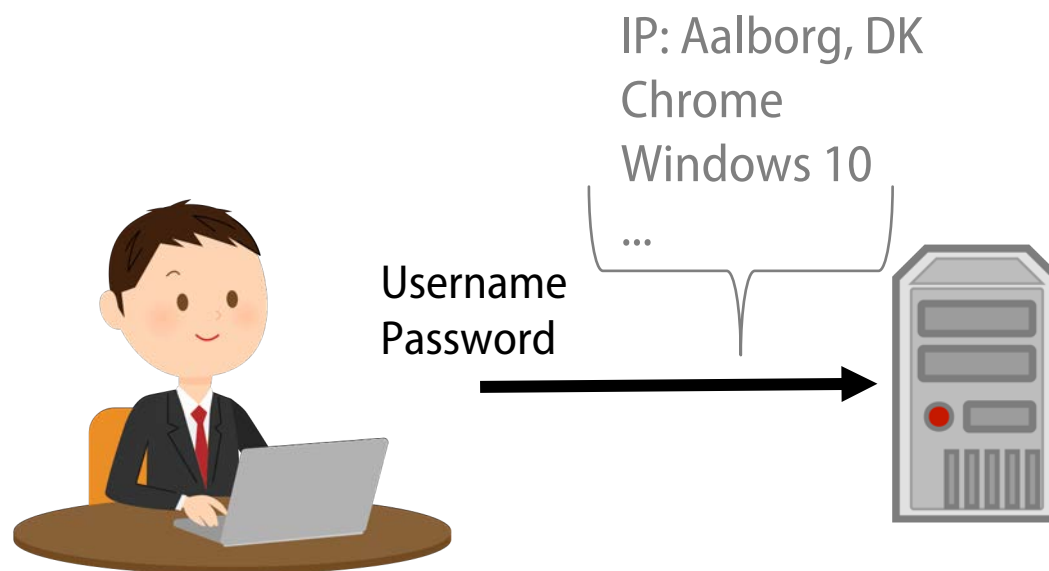
Stephan Wiefeling, Nils Gruschka, Luigi Lo Iacono

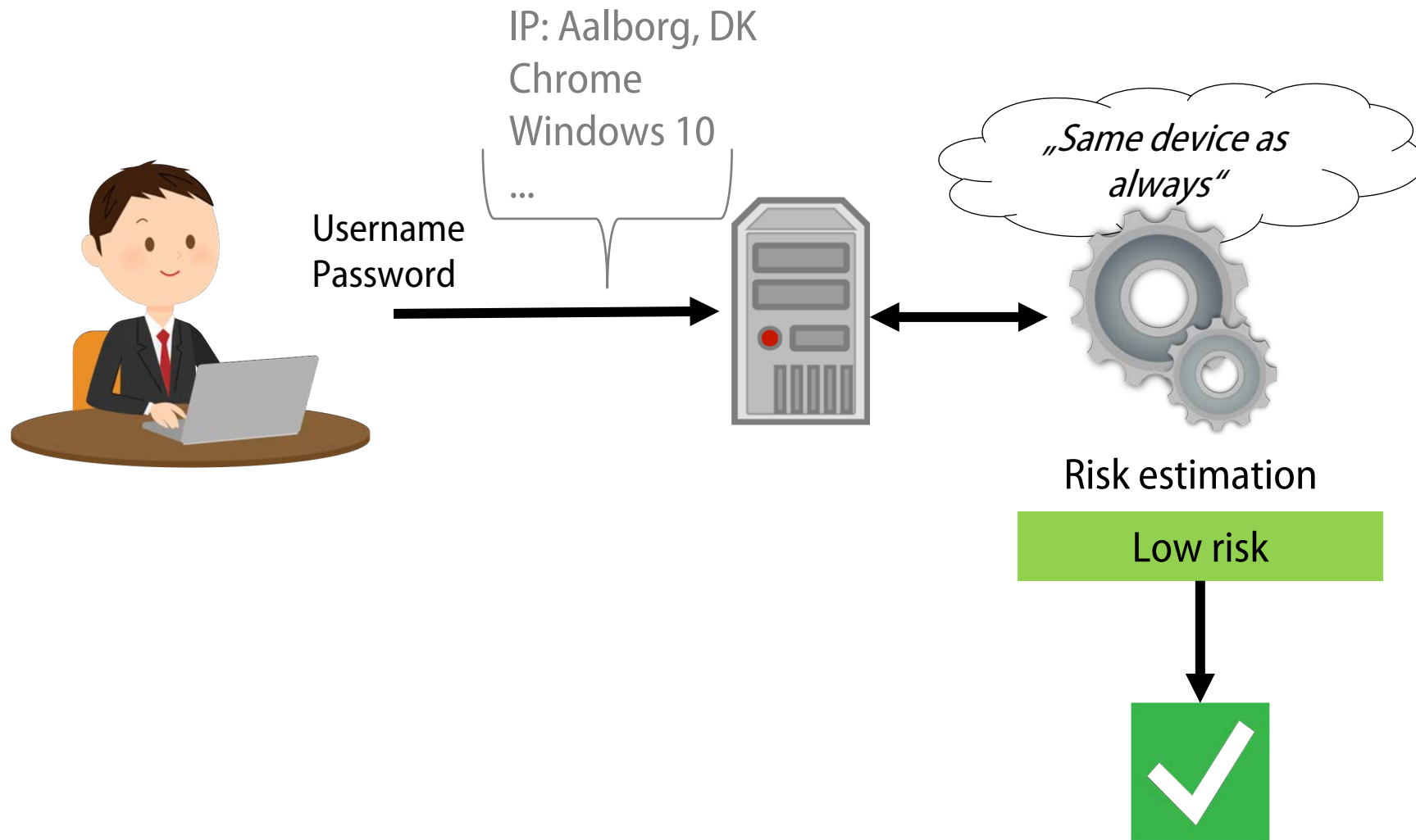
Aalborg, Denmark | NordSec 2019

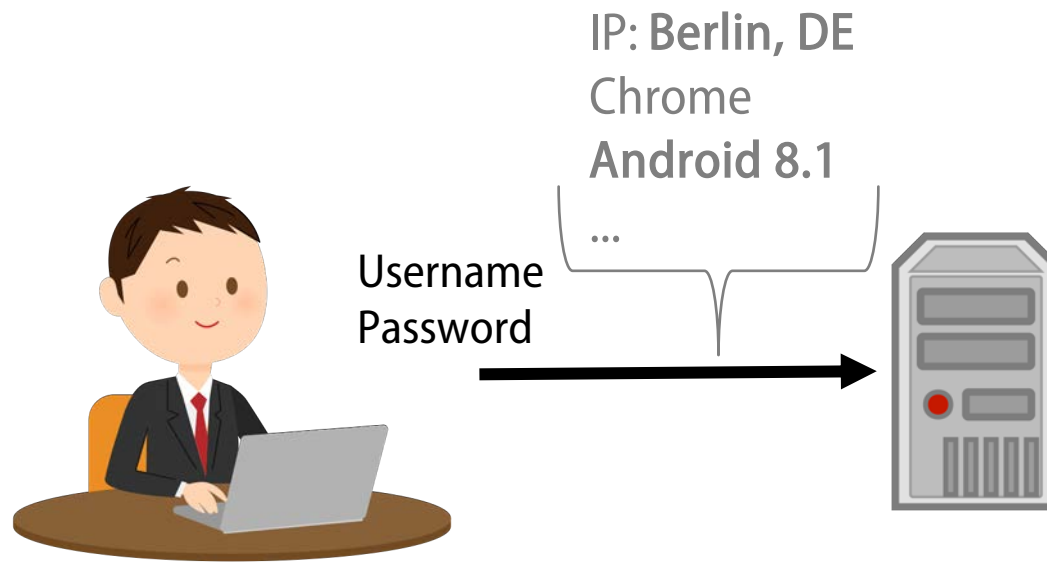


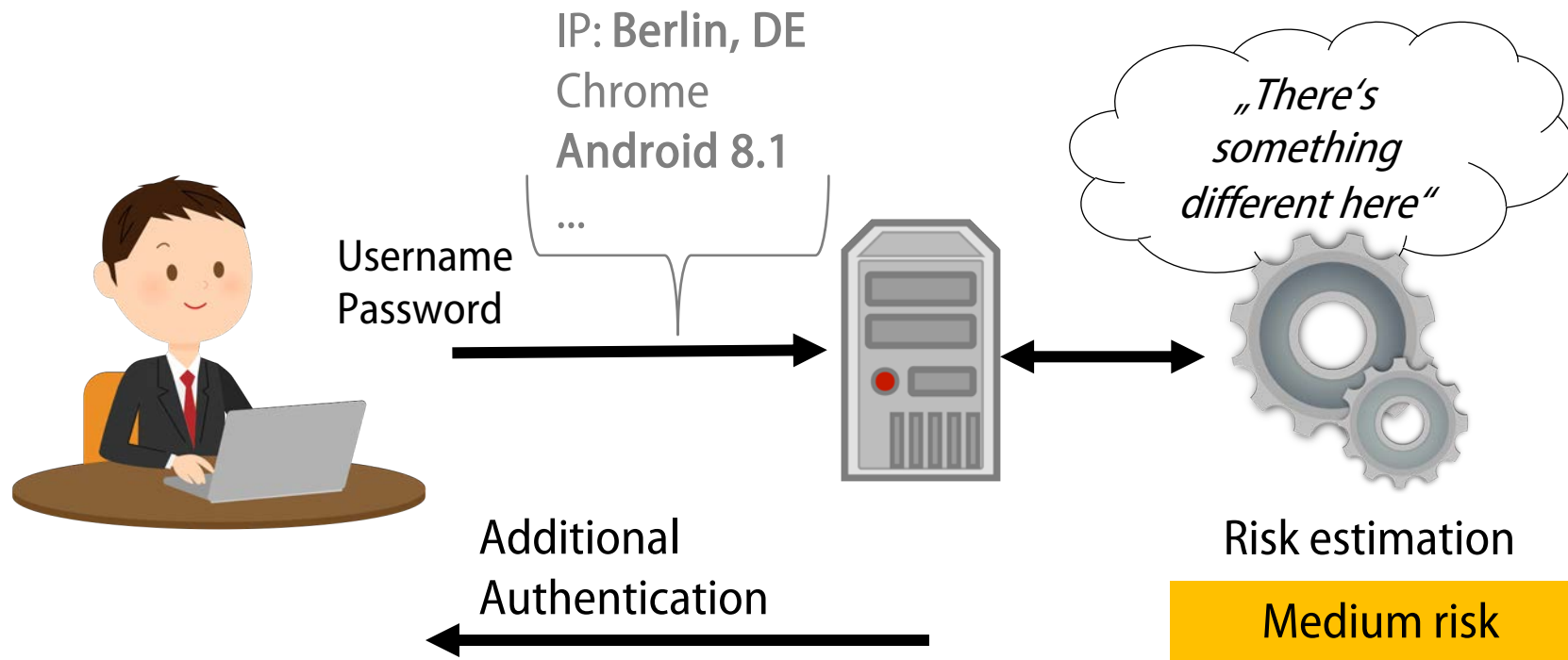
Technology  
Arts Sciences  
TH Köln



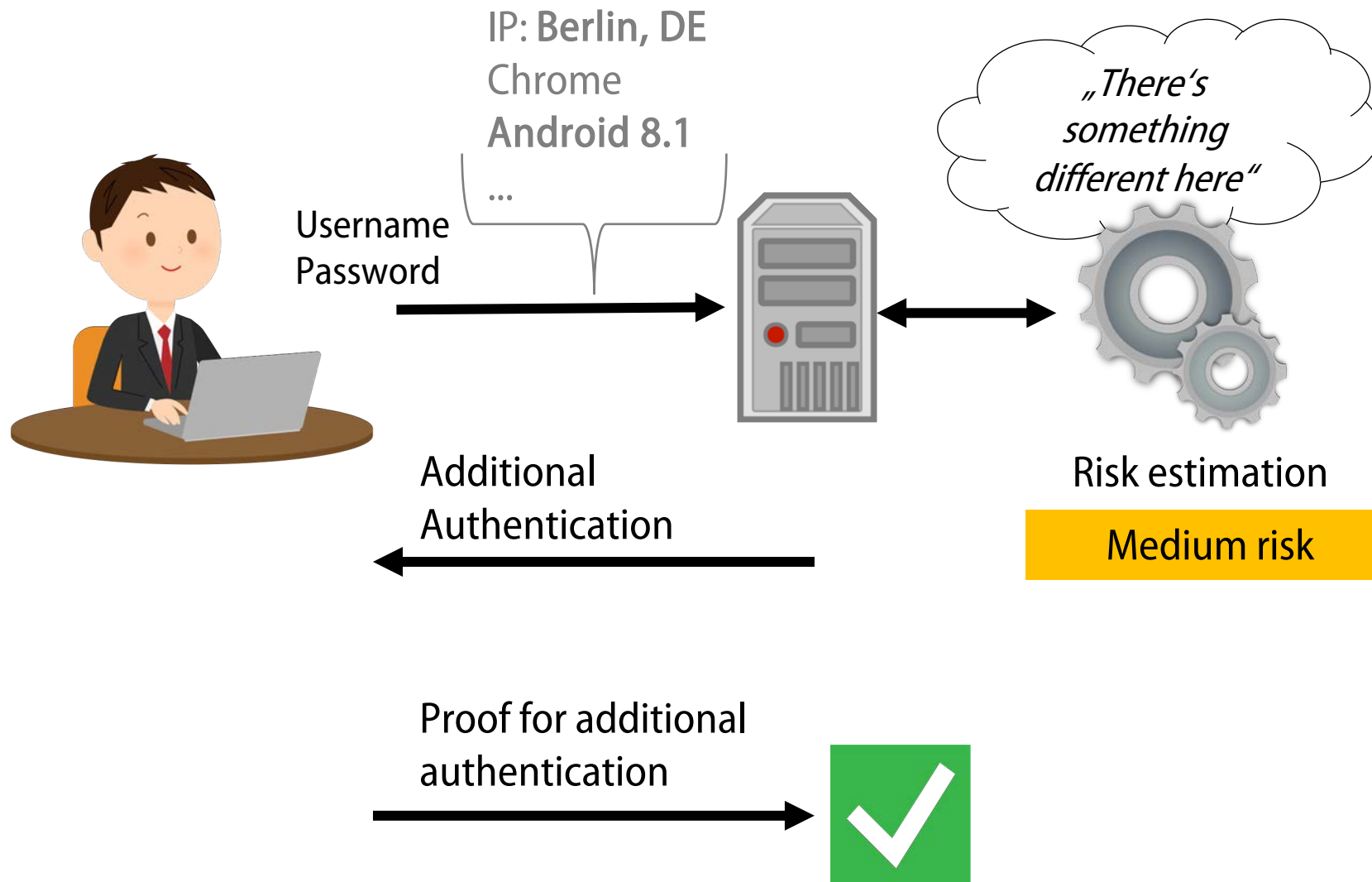


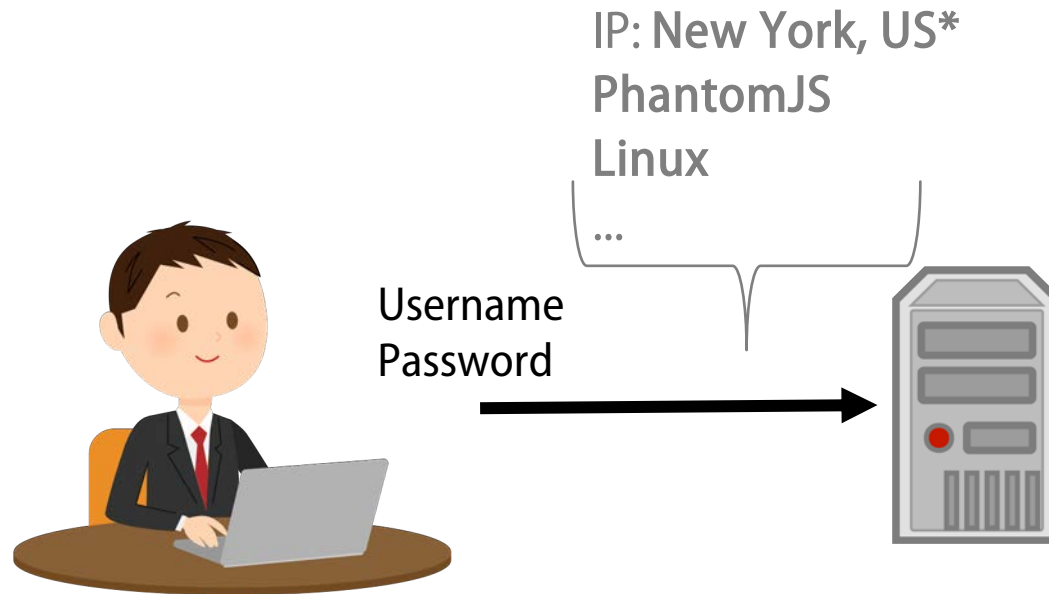












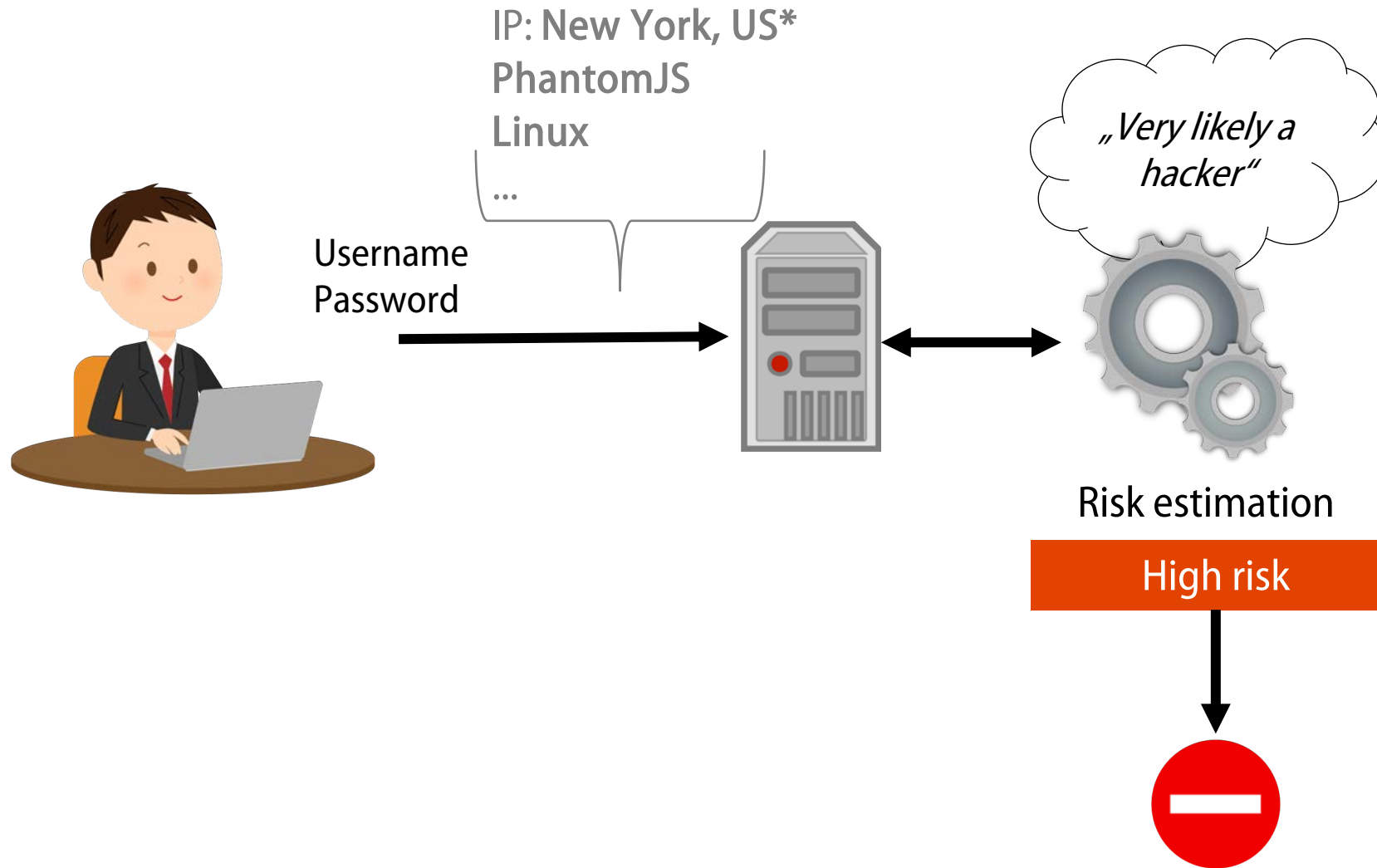
\* Known spam IP address

Stephan Wiefeling, Nils Gruschka, Luigi Lo Iacono

Aalborg, Denmark | NordSec 2019



Technology  
Arts Sciences  
TH Köln

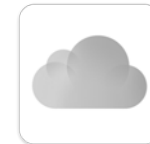


\* Known spam IP address

# Risk-based Authentication

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

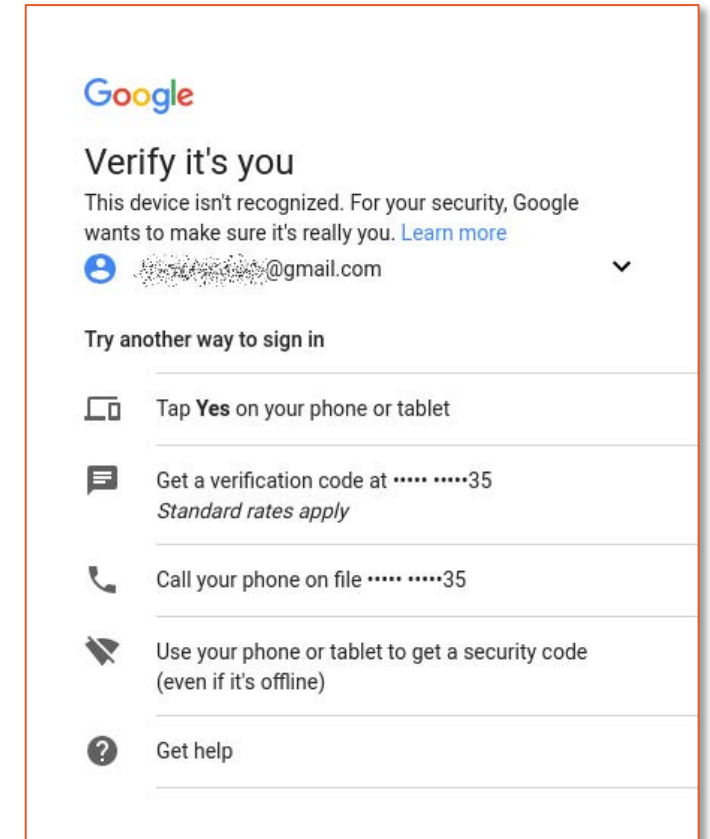
→ Black-box testing eight popular online services



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

# Proof of Concept\*

- Trained services with human-like behavior
- Triggered RBA with behavior



\* Wiefeling et al.: Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild. In: IFIP SEC '19. (Jun 2019)

Stephan Wiefeling, Nils Gruschka, Luigi Lo Iacono

Aalborg, Denmark | NordSec 2019



Technology  
Arts Sciences  
TH Köln

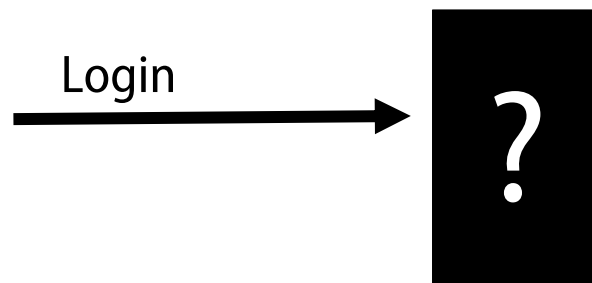




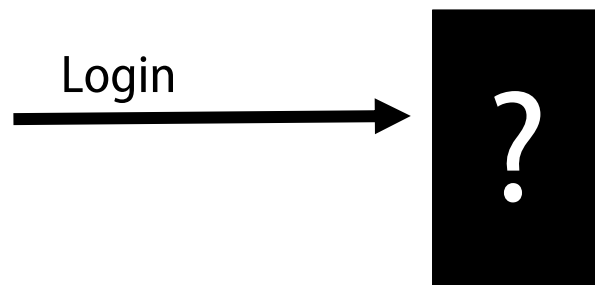


Login	IP address	User Agent	...

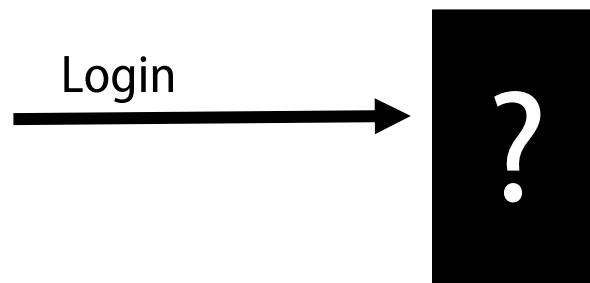




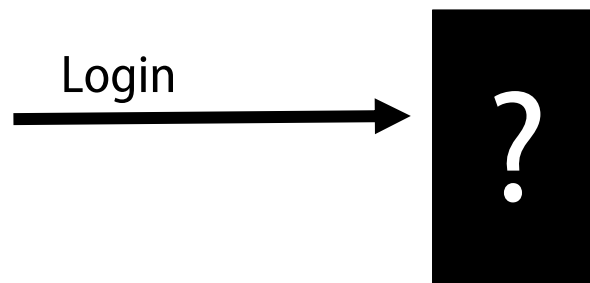
Login	IP address	User Agent	...
1	TH Köln	Chrome	...



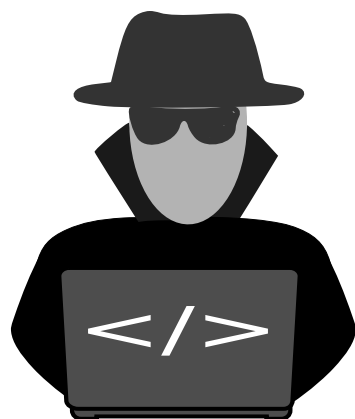
Login	IP address	User Agent	...
1	TH Köln	Chrome	...
2	TH Köln	Chrome	...



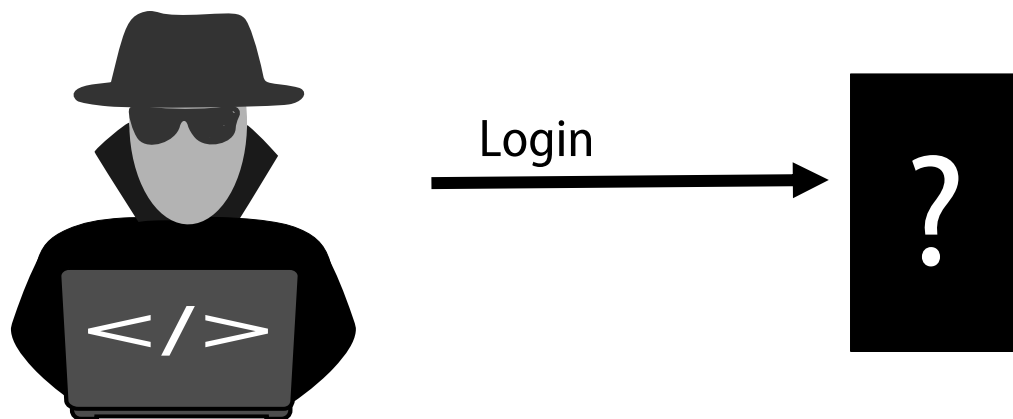
Login	IP address	User Agent	...
1	TH Köln	Chrome	...
2	TH Köln	Chrome	...
3	TH Köln	Chrome	...



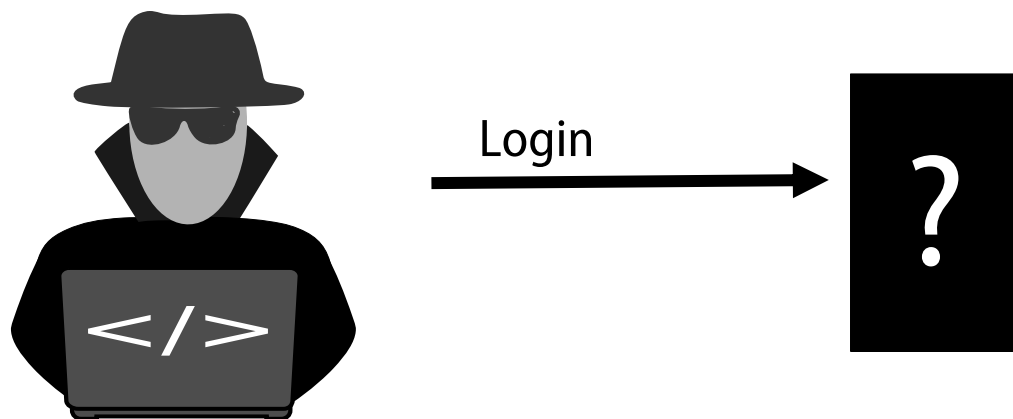
Login	IP address	User Agent	...
1	TH Köln	Chrome	...
2	TH Köln	Chrome	...
3	TH Köln	Chrome	...
...	...	...	...
20	TH Köln	Chrome	...



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



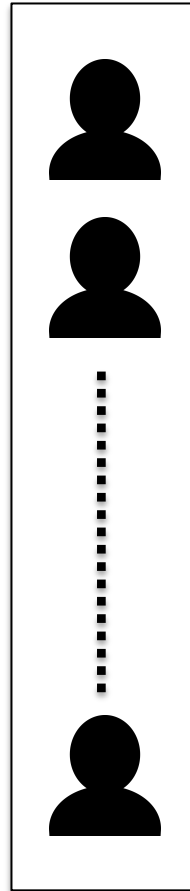
Login	IP address	User Agent	...
1	TH Köln	Chrome	...
2	TH Köln	Chrome	...
3	TH Köln	Chrome	...
...	...	...	...
20	TH Köln	Chrome	...
21	Other Country	Chrome	...



✓, ■ or ⚡?

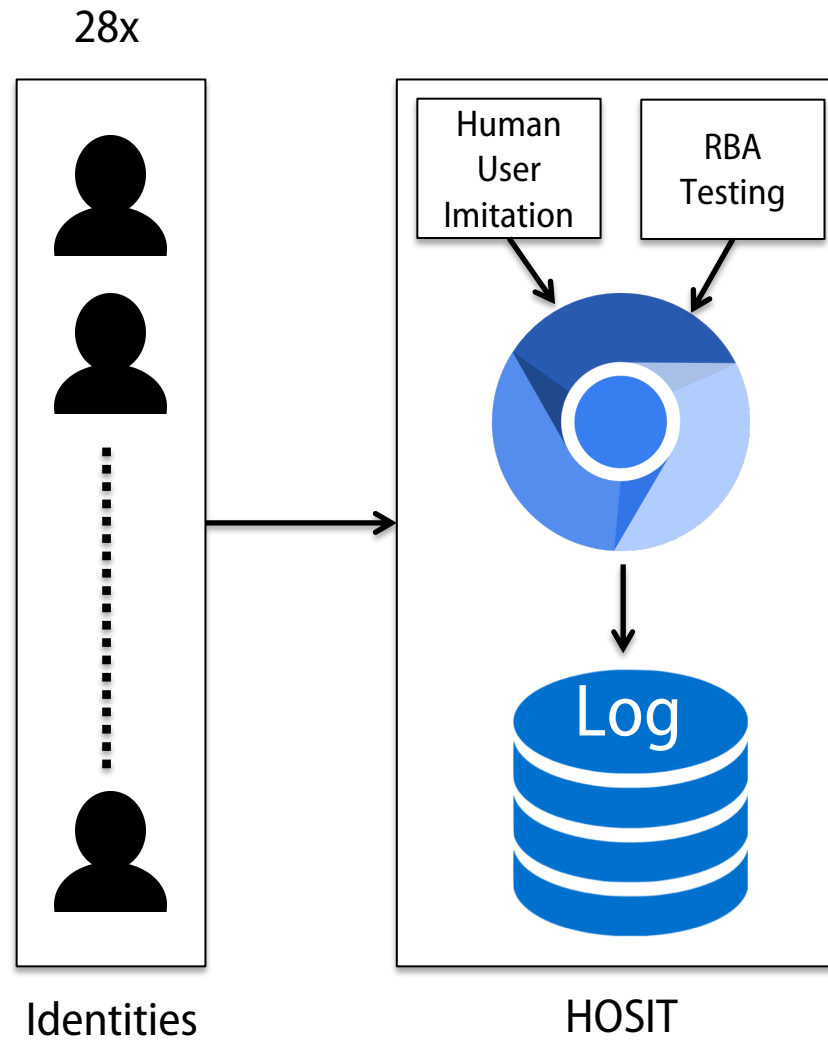
Login	IP address	User Agent	...
1	TH Köln	Chrome	...
2	TH Köln	Chrome	...
3	TH Köln	Chrome	...
...	...	...	...
20	TH Köln	Chrome	...
21	Other Country	Chrome	...

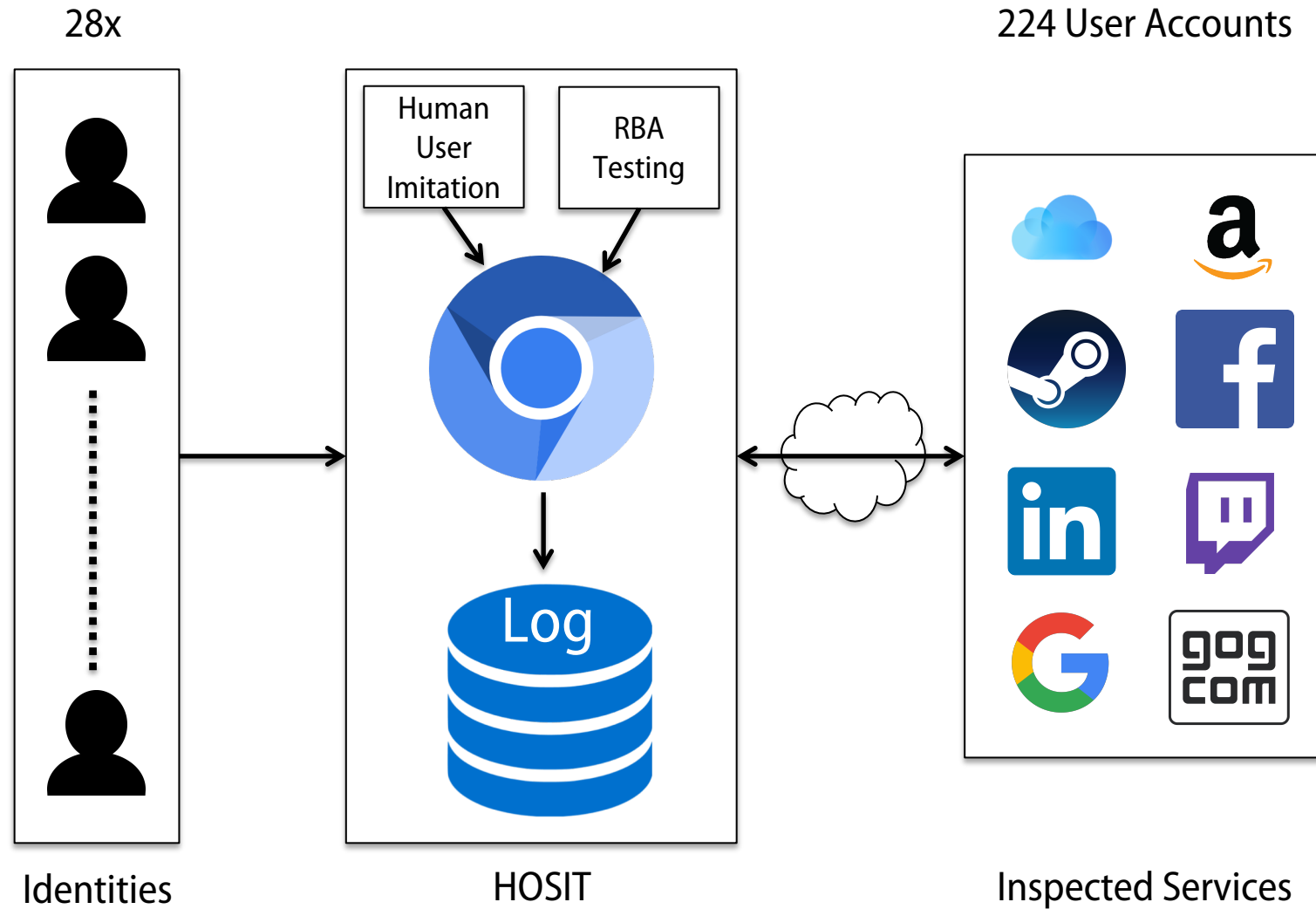
28x



Identities

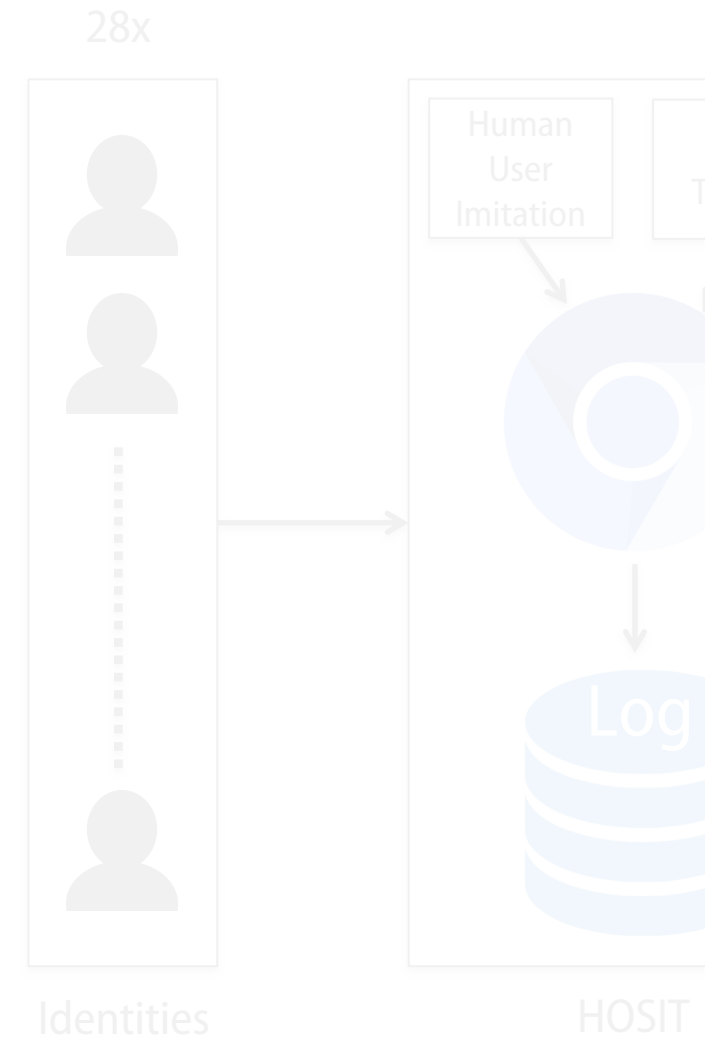






# Proof of Concept\*

- Results:
  - Internal features used for RBA
  - Estimation of services' RBA procedures
- Would not have been possible without HOSIT



\* Wiefeling et al.: Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild. In: IFIP SEC '19. (Jun 2019)

Stephan Wiefeling, Nils Gruschka, Luigi Lo Iacono

Aalborg, Denmark | NordSec 2019



Technology  
Arts Sciences  
TH Köln

# Overview

1. Tool



2. Proof of Concept



3. Conclusion

# Conclusion

- HOSIT available as open source software\*
- Can be used for own studies of online services
- Responsible service access for researchers?



\* <https://git.io/hosit>

Stephan Wiefling, Nils Gruschka, Luigi Lo Iacono

# Thank you



[riskbasedauthentication.org/hosit](https://riskbasedauthentication.org/hosit)  
[das.th-koeln.de](mailto:das.th-koeln.de)



[stephan.wiefling@th-koeln.de](mailto:stephan.wiefling@th-koeln.de)



[@swiefling](https://twitter.com/swiefling)