Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

# A Privacy Measure Turned Upside Down?

## Investigating the Use of HTTP Client Hints on the Web

Stephan Wiefling*, Marian Hönscheid, Luigi Lo Iacono

H-BRS University of Applied Sciences, Germany

swiefling.de & H-BRS University of Applied Sciences, Germany (*)

ARES | Homepage

ares-conference.eu

Incognito

ARES

Vienna | Austria
July 30 - August 02, 2024

Conference | Venue and Location | Authors Area | Co-located Conferences | Archive | Registration & Visa

# The International Conference on Availability, Reliability and Security

focuses since 2006 on rigorous and novel research in the field of dependability, computer and information security. In cooperation with the conference several workshops are held covering a huge variety of security topics.

Co-located Conferences DOD 2024 and ICS-CSR 2024.

← 1 | 4 →

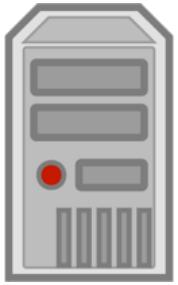
Submit Now! →

24

WORKSHOP SUBMISSION - This link will guide you to the ARES Easychair Submission.

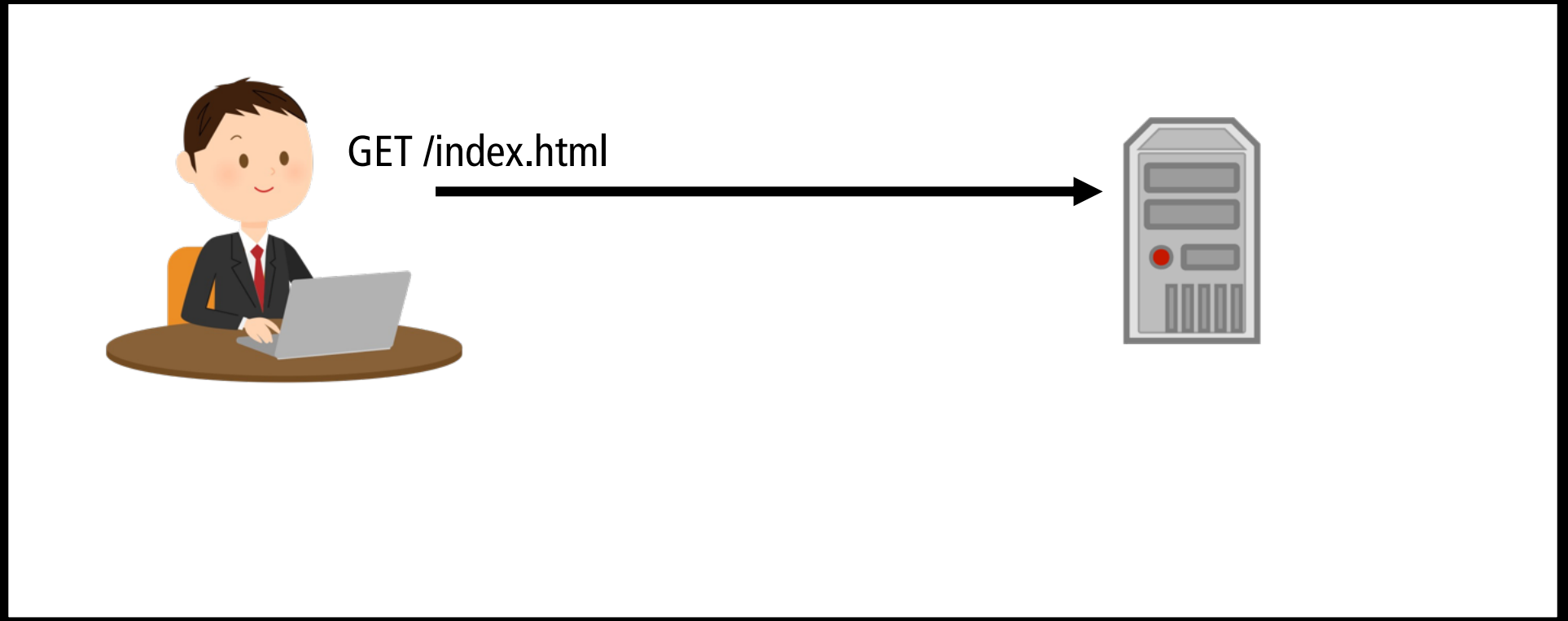
MORE ↓

# User Agent String



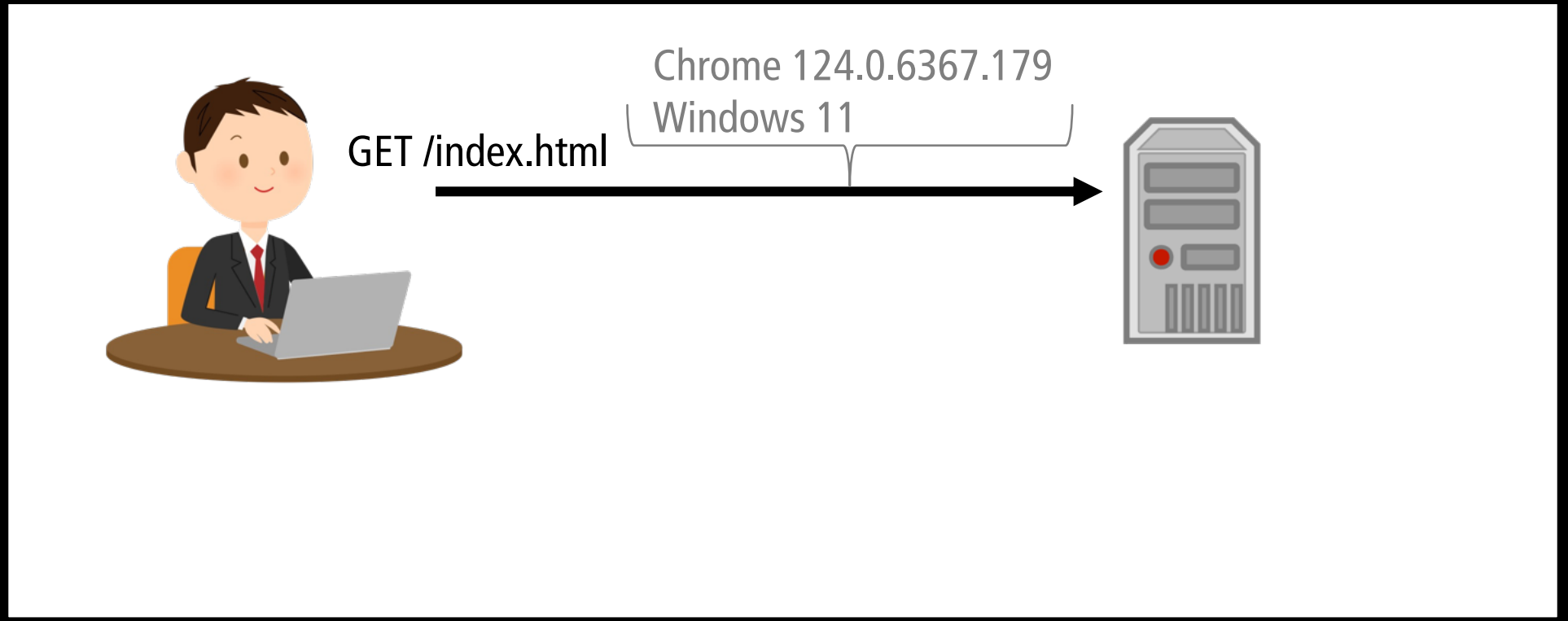
Nielsen et al. 1996. Hypertext Transfer Protocol – HTTP/1.0

# User Agent String



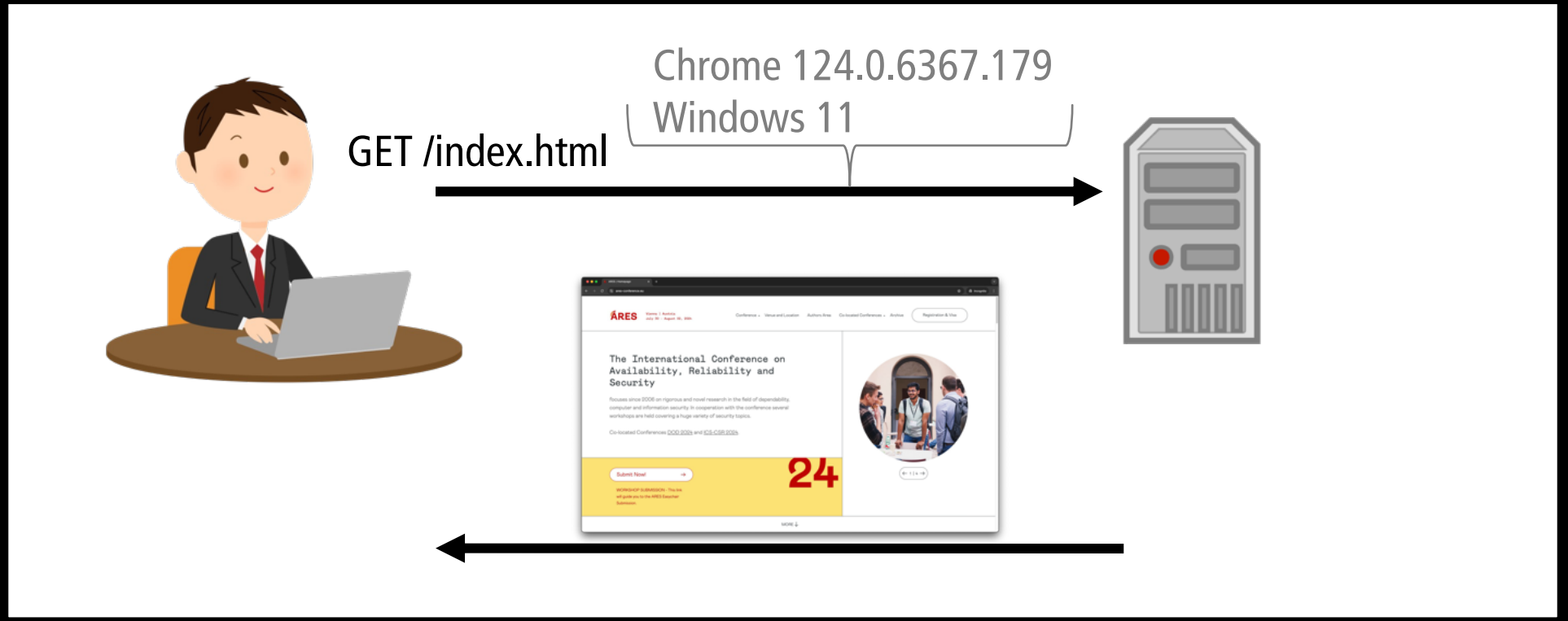

Nielsen et al. 1996. Hypertext Transfer Protocol – HTTP/1.0

# User Agent String



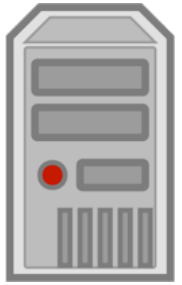

Nielsen et al. 1996. Hypertext Transfer Protocol – HTTP/1.0

# User Agent String




Nielsen et al. 1996. Hypertext Transfer Protocol – HTTP/1.0

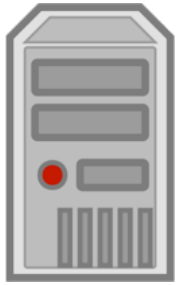
# HTTP Client Hints (HTTP CHs)



Grigorik and Weiss. 2021. HTTP Client Hints. RFC 8942, RFC8942
Weiss. 2023. Client Hints Infrastructure. W3C Draft Community Group Report

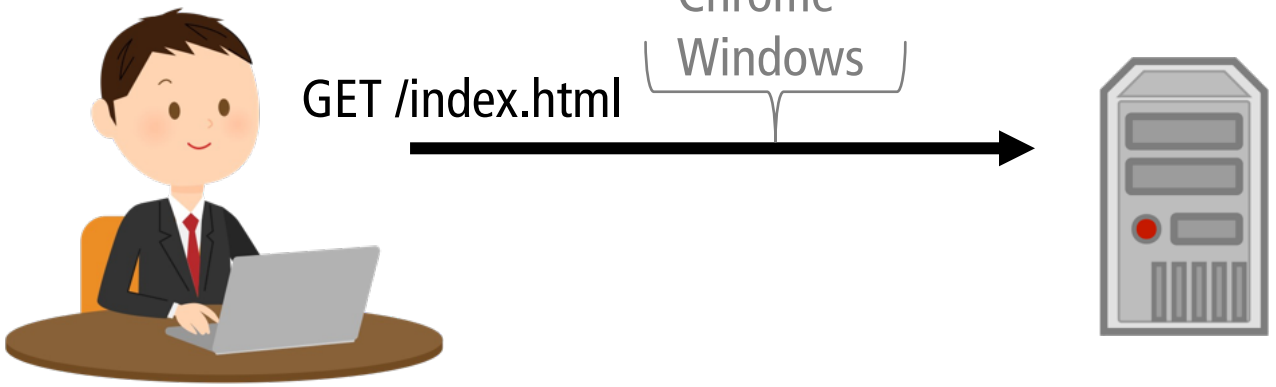
# HTTP Client Hints (HTTP CHs)

GET /index.html



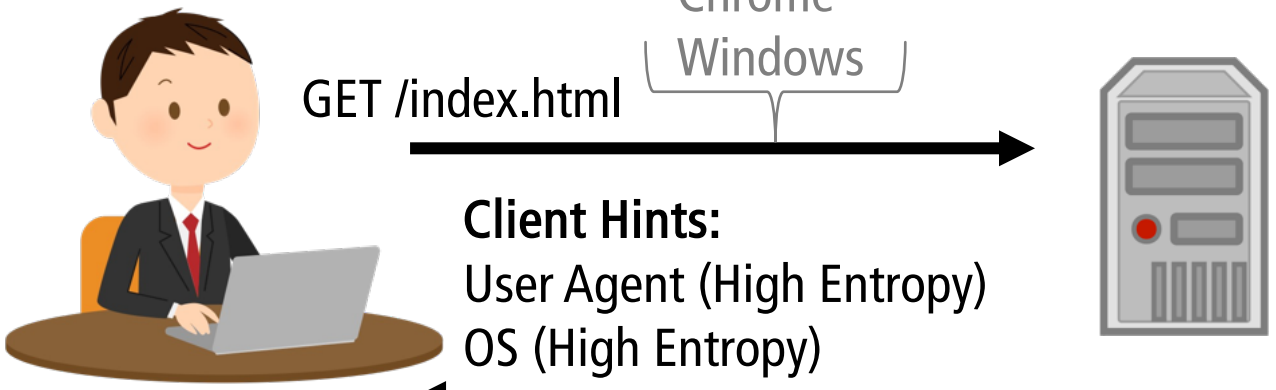
Grigorik and Weiss. 2021. HTTP Client Hints. RFC 8942, RFC8942
Weiss. 2023. Client Hints Infrastructure. W3C Draft Community Group Report

# HTTP Client Hints (HTTP CHs)




Grigorik and Weiss. 2021. HTTP Client Hints. RFC 8942, RFC8942
Weiss. 2023. Client Hints Infrastructure. W3C Draft Community Group Report

# HTTP Client Hints (HTTP CHs)

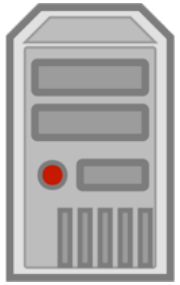



Grigorik and Weiss. 2021. HTTP Client Hints. RFC 8942, RFC8942
Weiss. 2023. Client Hints Infrastructure. W3C Draft Community Group Report

# HTTP Client Hints (HTTP CHs)

Chrome
Windows

GET /index.html

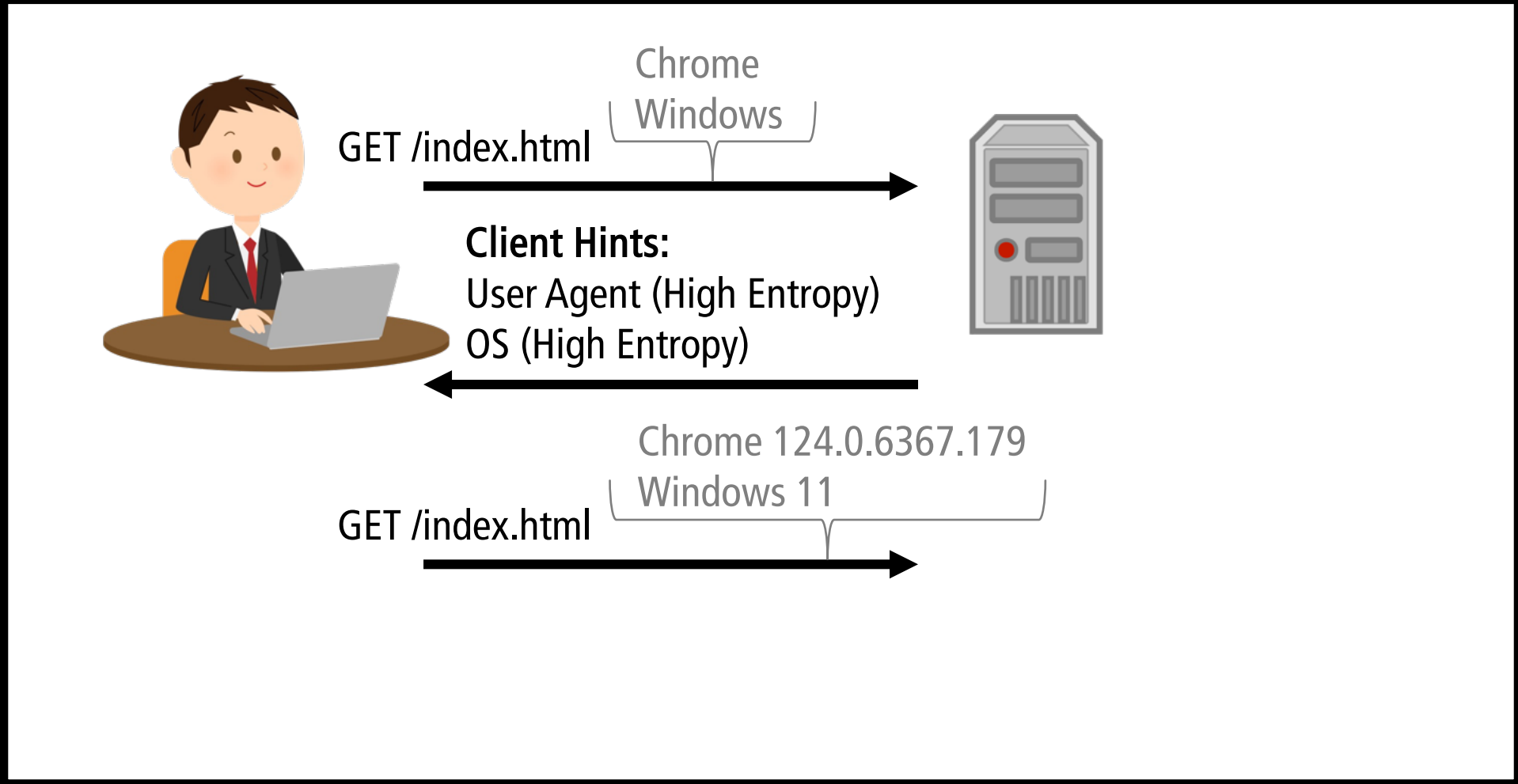


**Client Hints:**
User Agent (High Entropy)
OS (High Entropy)

GET /index.html

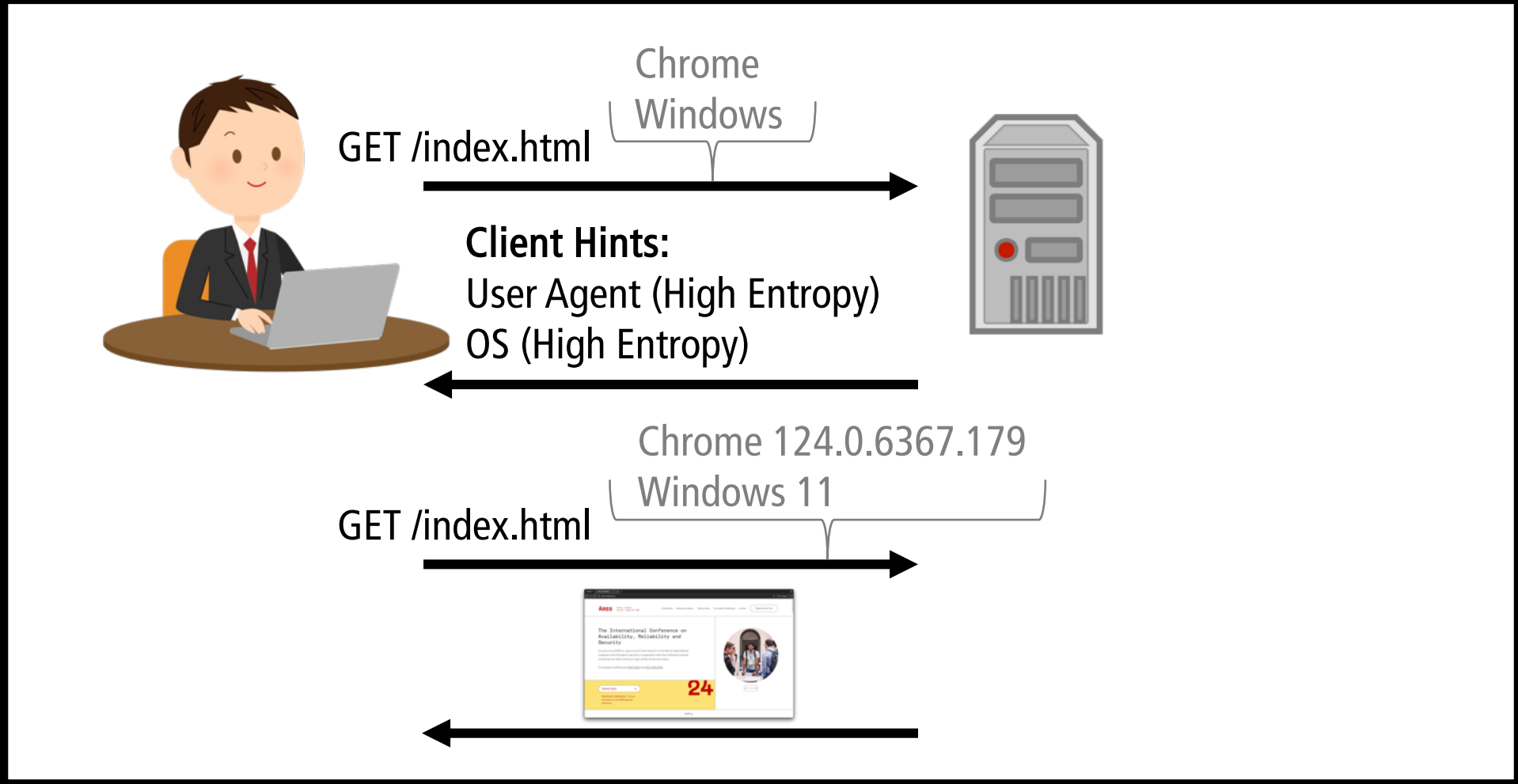
Grigorik and Weiss. 2021. HTTP Client Hints. RFC 8942, RFC8942
Weiss. 2023. Client Hints Infrastructure. W3C Draft Community Group Report

# HTTP Client Hints (HTTP CHs)




Grigorik and Weiss. 2021. HTTP Client Hints. RFC 8942, RFC8942
Weiss. 2023. Client Hints Infrastructure. W3C Draft Community Group Report

# HTTP Client Hints (HTTP CHs)




Grigorik and Weiss. 2021. HTTP Client Hints. RFC 8942, RFC8942
Weiss. 2023. Client Hints Infrastructure. W3C Draft Community Group Report

| User Agent | Level of Detail |
| --- | --- |
| User Agent (High Entropy) | High |
| User Agent Brand List | |
| OS (High Entropy) | |
| Device Model | Medium |
| OS (Low Entropy) | |
| User Agent (Low Entropy) | |
| CPU Bitness | |
| Device Form Factor | |
| Is Windows64 | |
| Platform Architecture | |
| Prefers Mobile UX | Low |

| User Agent | Level of Detail |
| --- | --- |
| User Agent (High Entropy) | High |
| User Agent Brand List | |
| OS (High Entropy) | |
| Device Model | Medium |
| OS (Low Entropy) | |
| User Agent (Low Entropy) | |
| CPU Bitness | |
| Device Form Factor | |
| Is Windows64 | |
| Platform Architecture | |
| Prefers Mobile UX | Low |

## User Preference Media

Contrast Preference
Forced Colors
Light/Dark Mode
Prefers Reduced Motion
Reduced Transparency

## Level of Detail

Low

| Device Information | Level of Detail |
| --- | --- |
| Viewport Width | High |
| Width | |
| Client Device Pixel Ratio | |
| Client's RAM | |
| Image Device Pixel Ratio | Low |

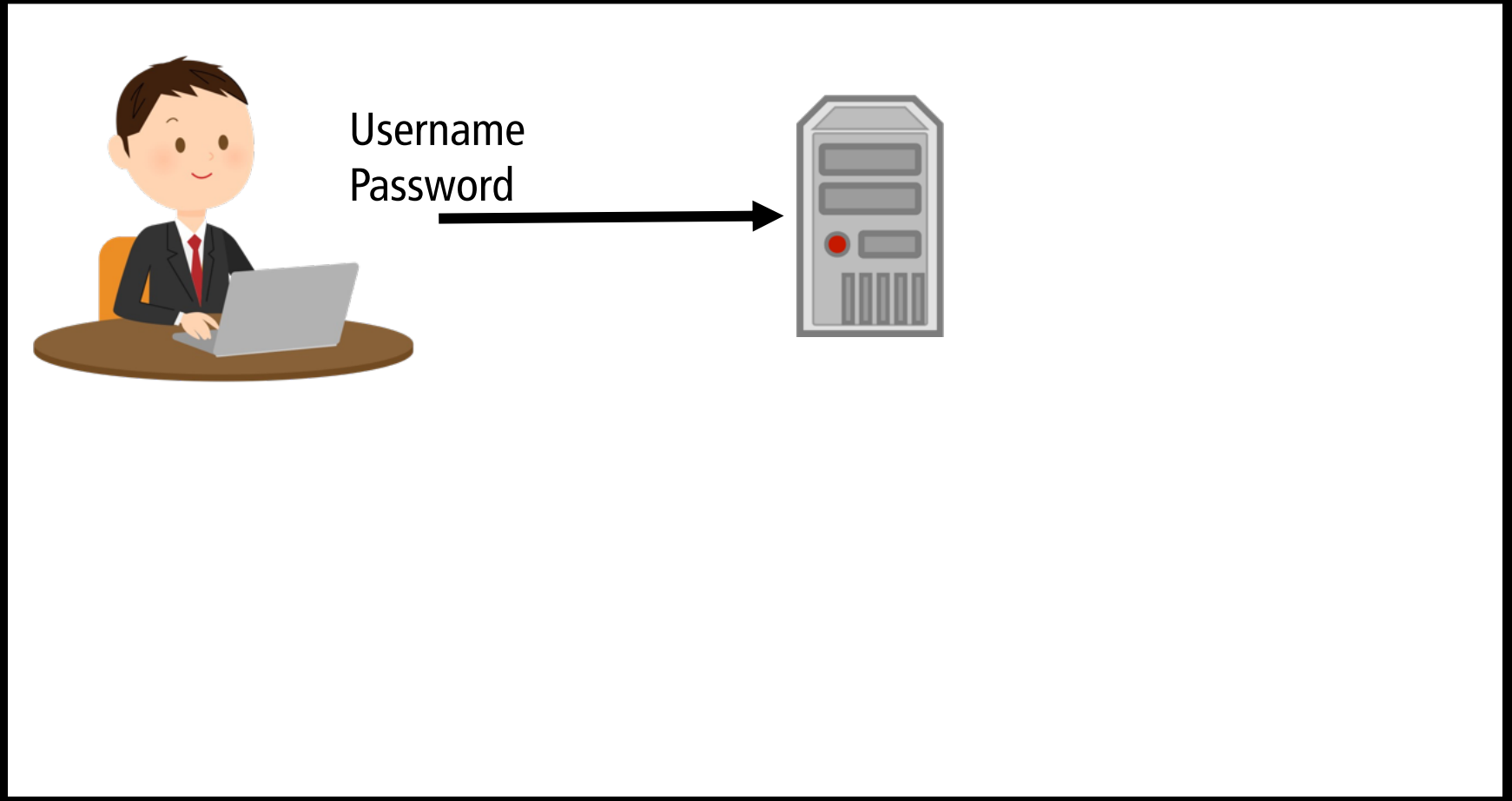
| Network | Level of Detail |
| --- | --- |
| Bandwidth | High |
| Network Profile | |
| Round-Trip Time | |
| Prefers Reduced Data | Low |

# Affects 78% desktop and 69% mobile users*

* Statscounter. 2024. Browser Market Share Worldwide.

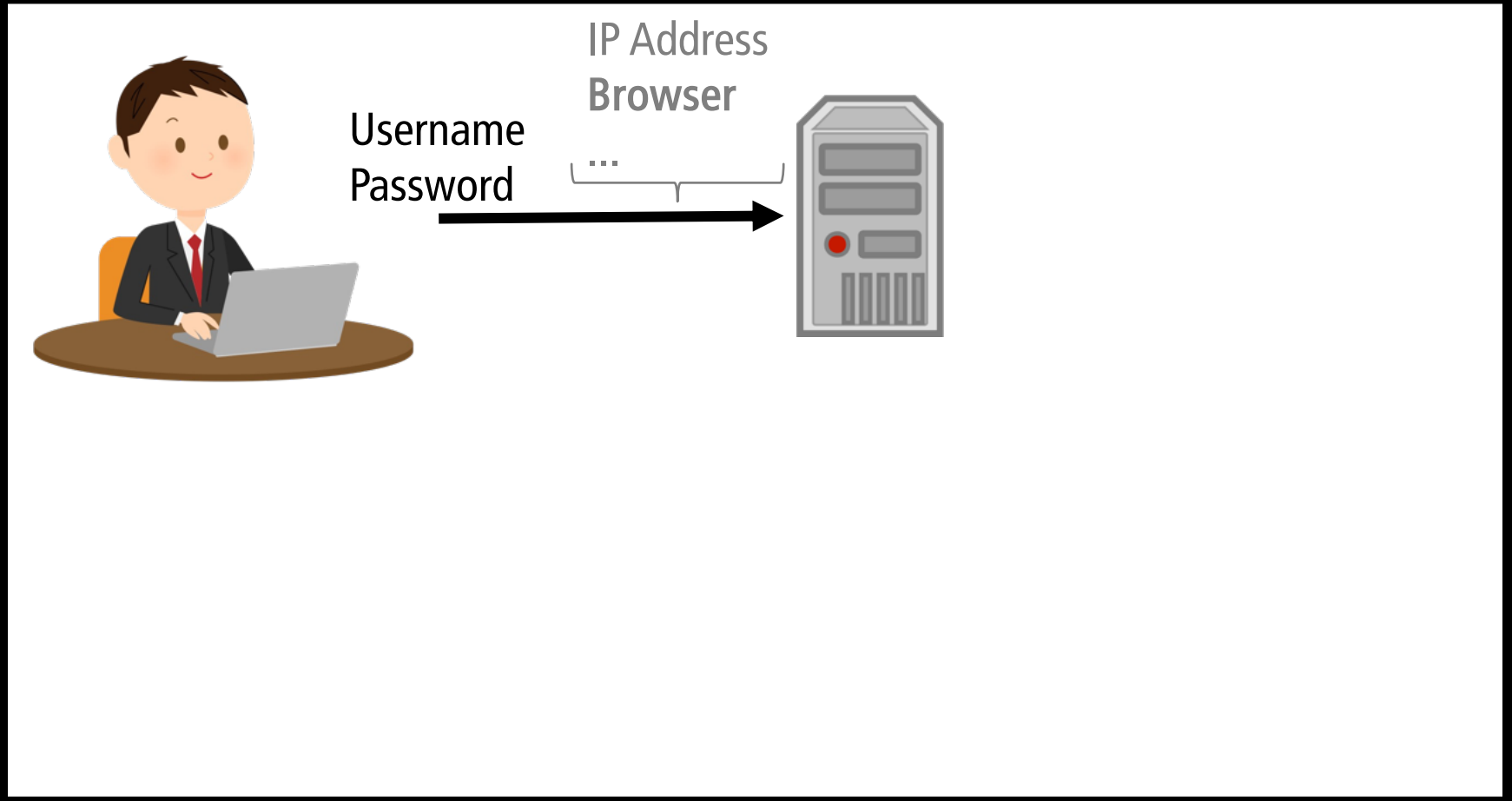
# Some Websites Depend on Browser Information

# Risk-Based Authentication (RBA)

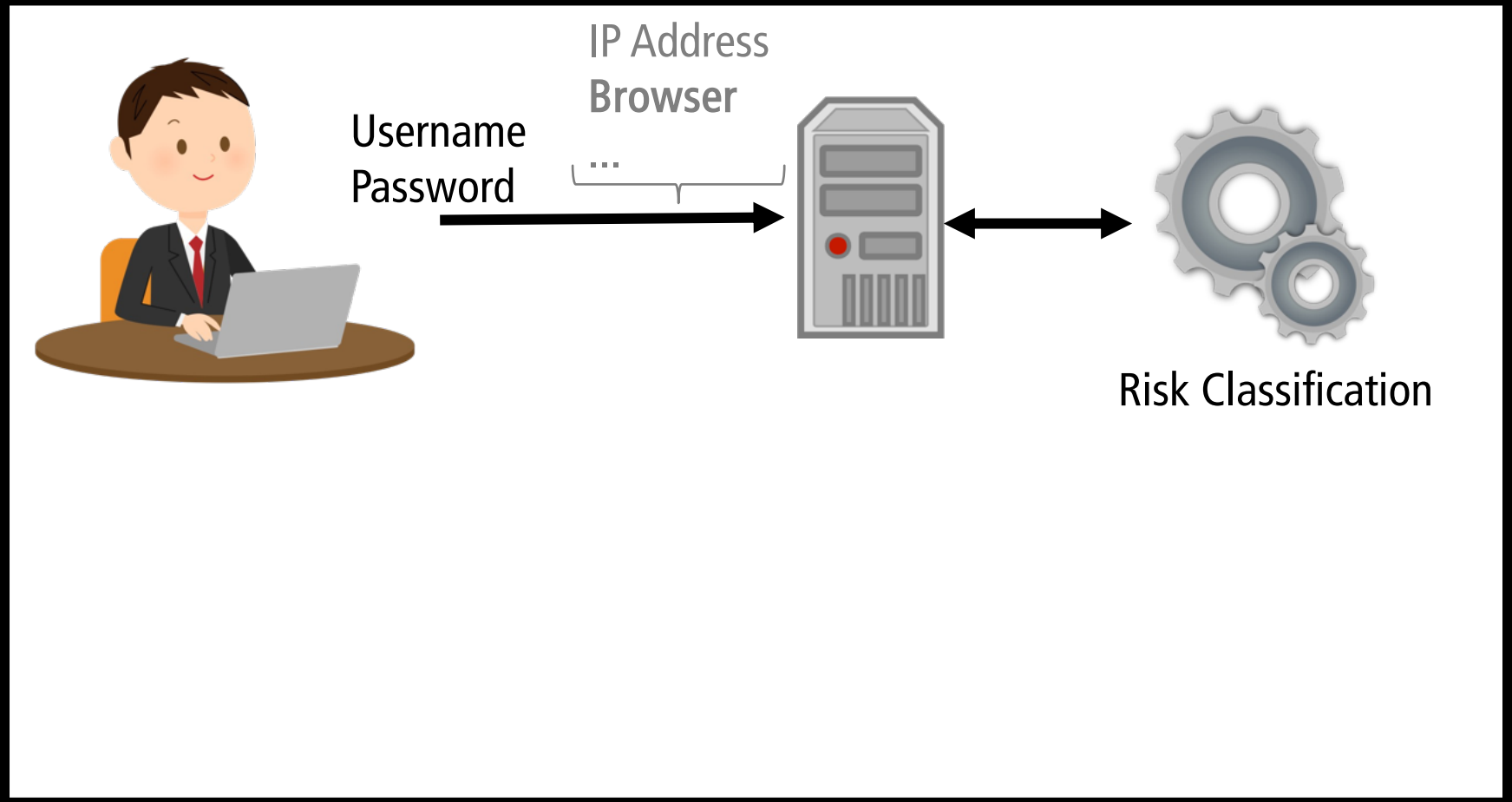



Wiefling et al.: Verify It's You: How Users Perceive Risk-Based Authentication. In: IEEE Security & Privacy (2021). IEEE

# Risk-Based Authentication (RBA)

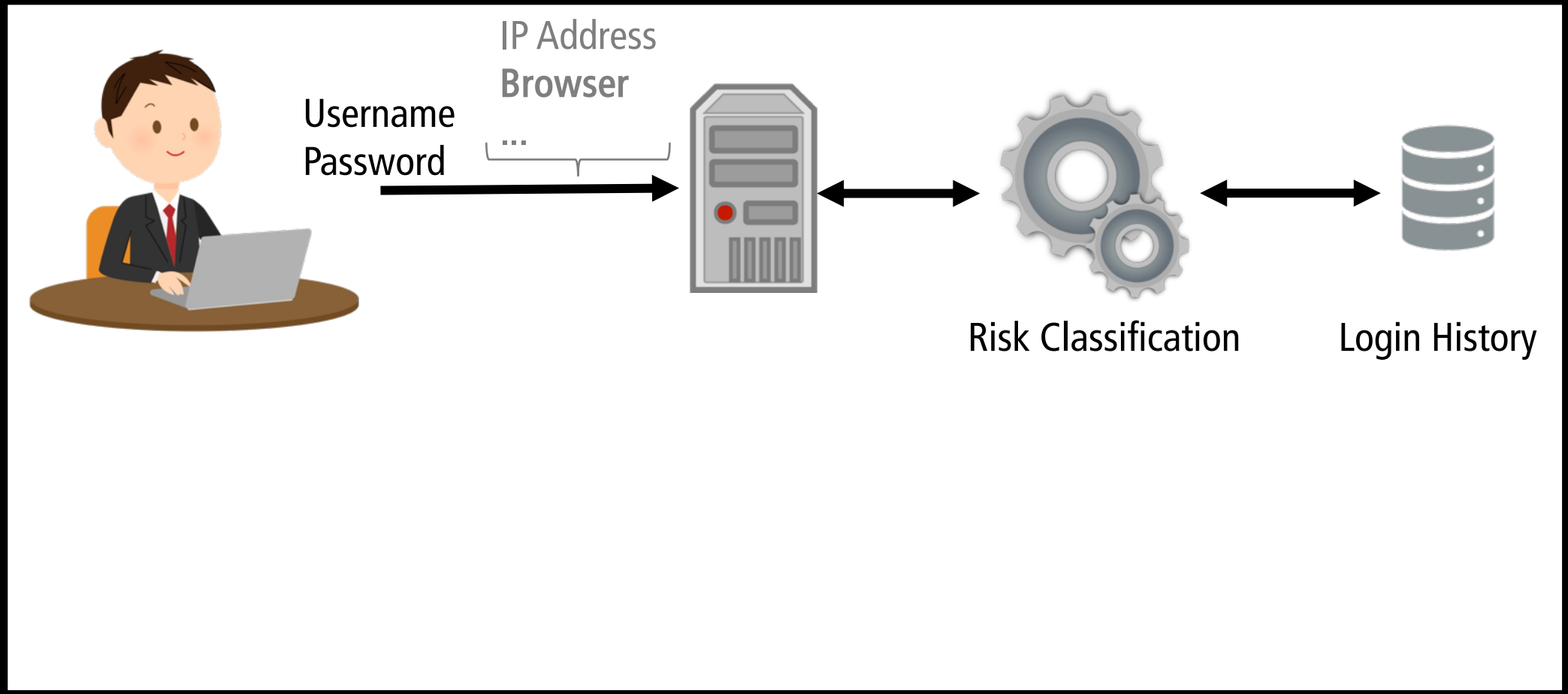


# Risk-Based Authentication (RBA)

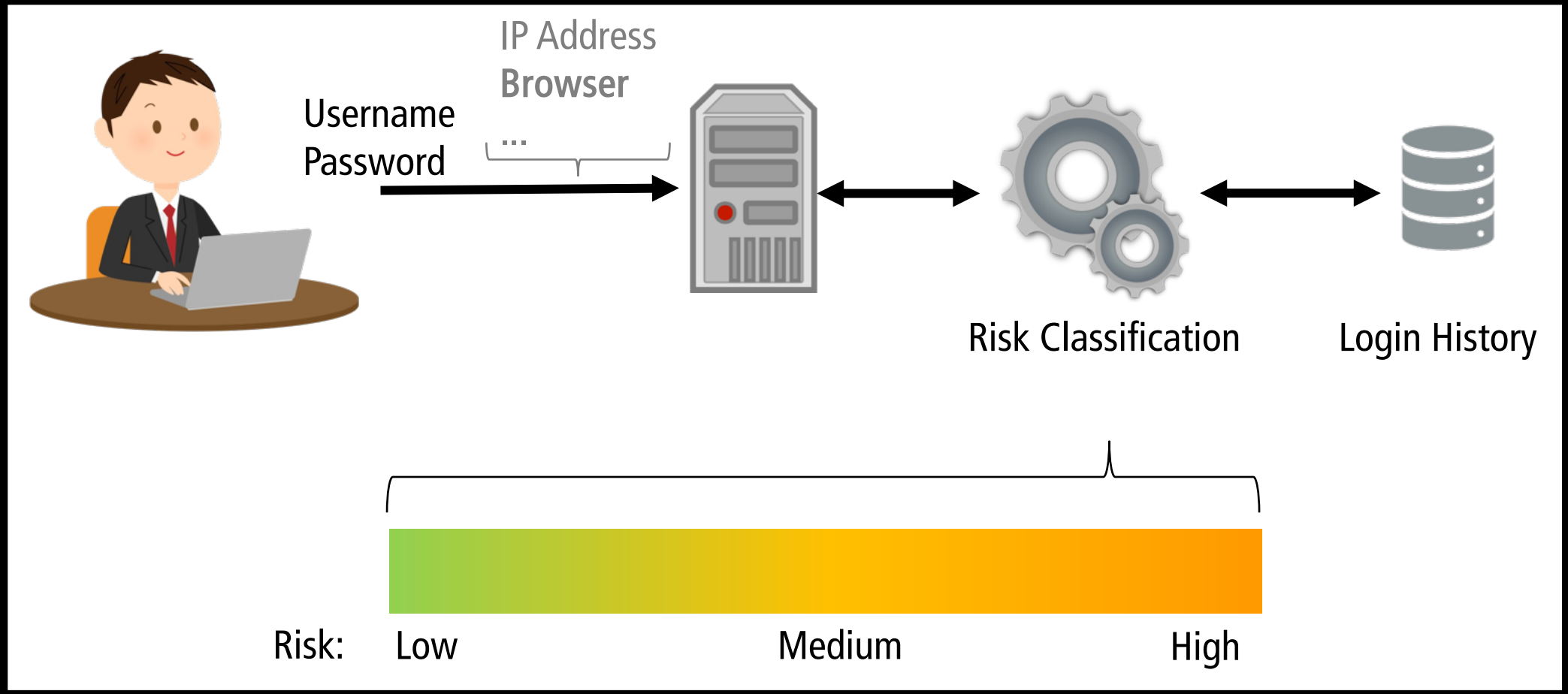



Wiefling et al.: Verify It's You: How Users Perceive Risk-Based Authentication. In: IEEE Security & Privacy (2021). IEEE

# Risk-Based Authentication (RBA)

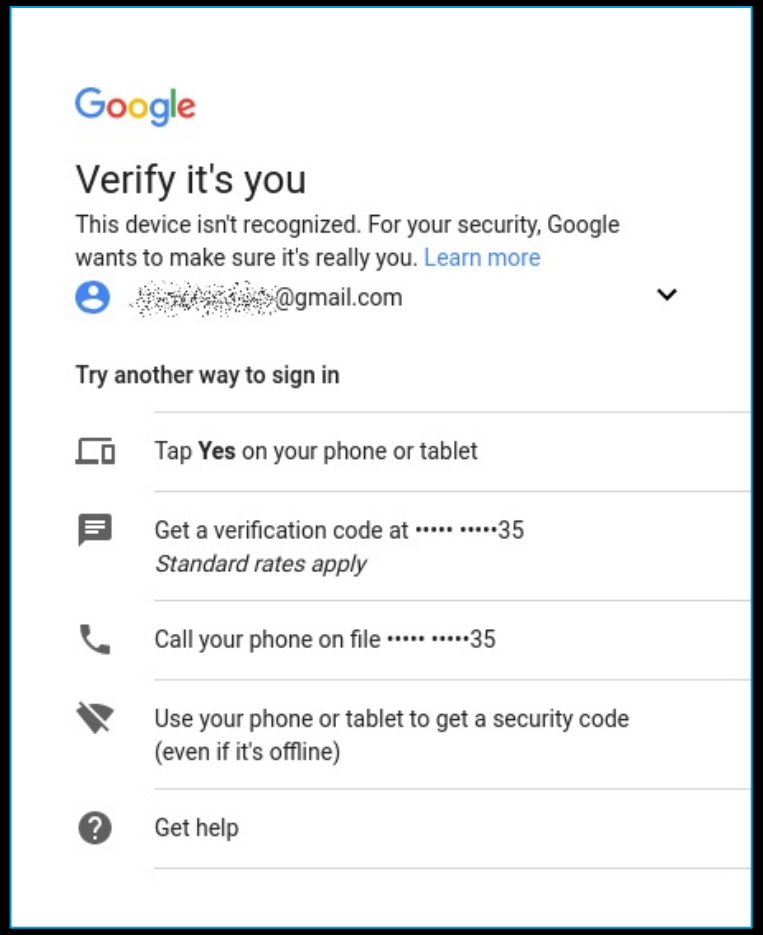


# Risk-Based Authentication (RBA)




Wiefling et al.: Verify It's You: How Users Perceive Risk-Based Authentication. In: IEEE Security & Privacy (2021). IEEE

# Risk-Based Authentication




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

# User Tracking

# How do Websites use HTTP CHs in Practice?

# Overview


Study


Results


Conclusion

# Overview



# Two Data Sources

# Two Data Sources

- Website Start Pages (~12M Websites*)

*12M websites from on Chrome UX Report

# Two Data Sources

- Website Start Pages (~12M Websites*)
  - Taken from The HTTP Archive
  - November 2010 - December 2023

*12M websites from on Chrome UX Report

# Two Data Sources

- Website Start Pages (~12M Websites*)
  - Taken from The HTTP Archive
  - November 2010 - December 2023
- Login Pages from Tranco 8M#

*12M websites from on Chrome UX Report

# 8M most popular websites based on the Tranco List
Le Pochat et al.: Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In: NDSS (2019). Internet Society

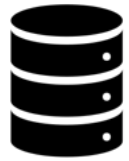
# Two Data Sources

- Website Start Pages (~12M Websites*)
  - Taken from The HTTP Archive
  - November 2010 - December 2023
- Login Pages from Tranco 8M#
  - Own Crawling Data
  - August 2022 – December 2023

*12M websites from on Chrome UX Report

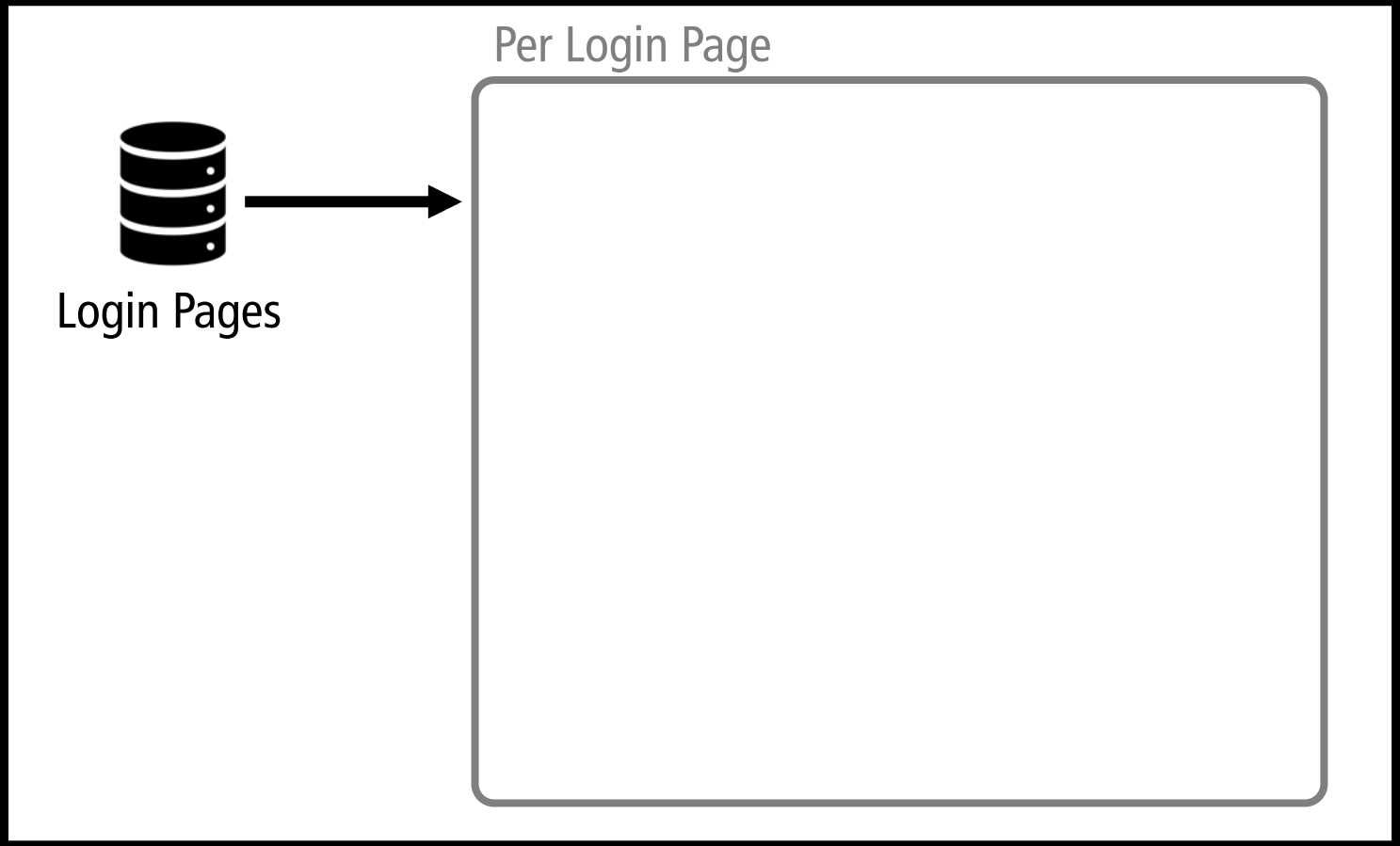
# 8M most popular websites based on the Tranco List
Le Pochat et al.: Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In: NDSS (2019). Internet Society

# Login Pages Crawling

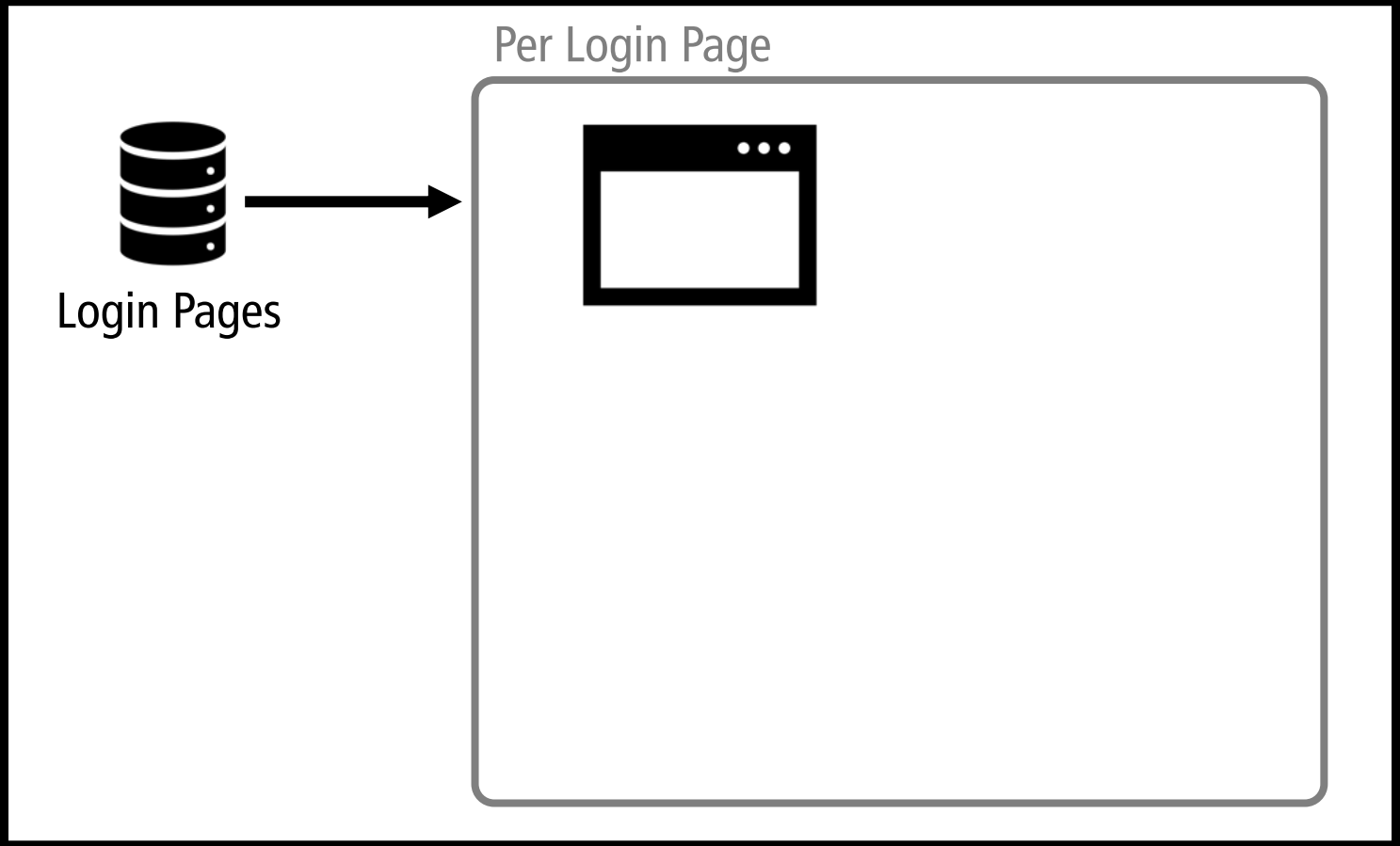


Login Pages

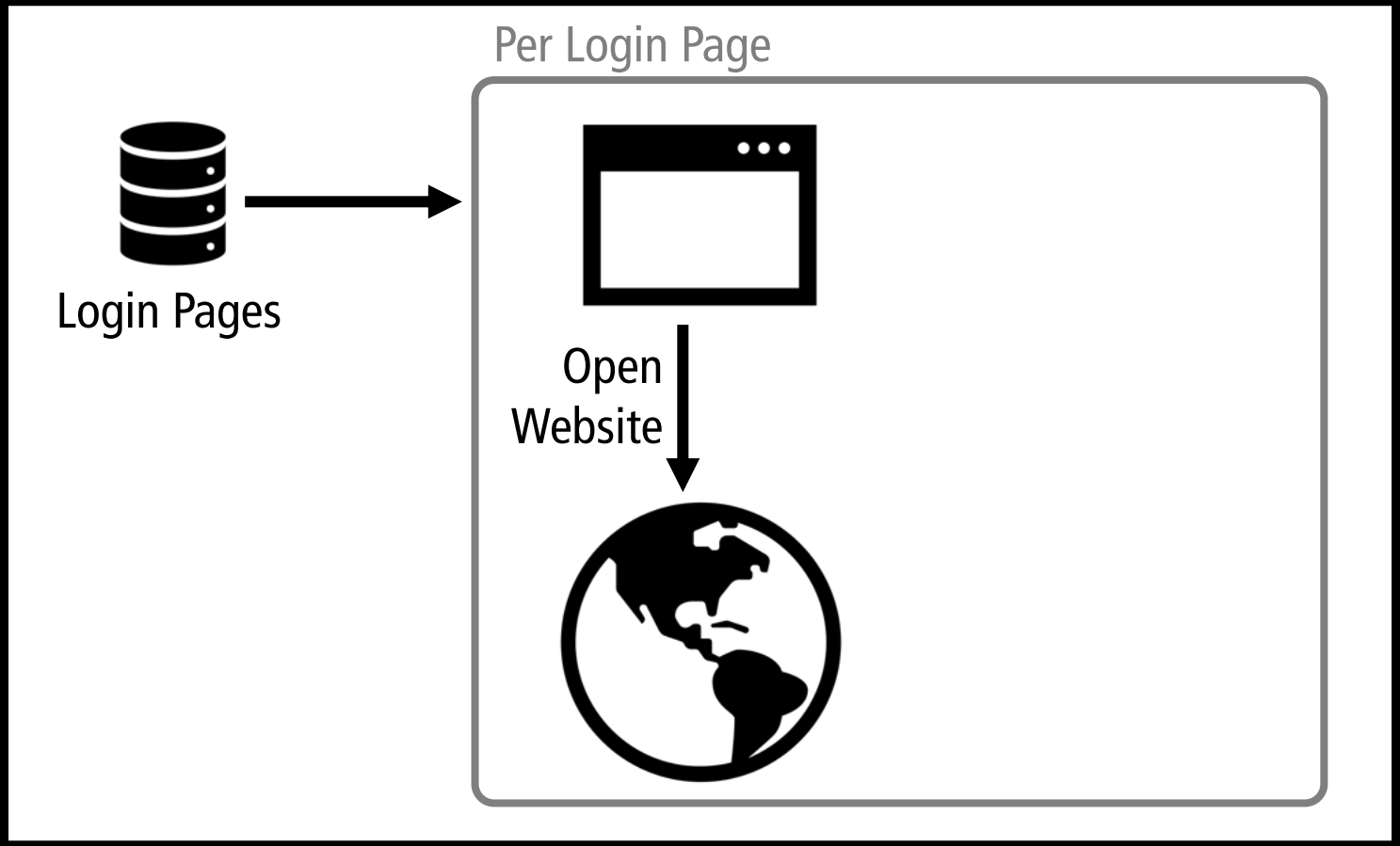
# Login Pages Crawling



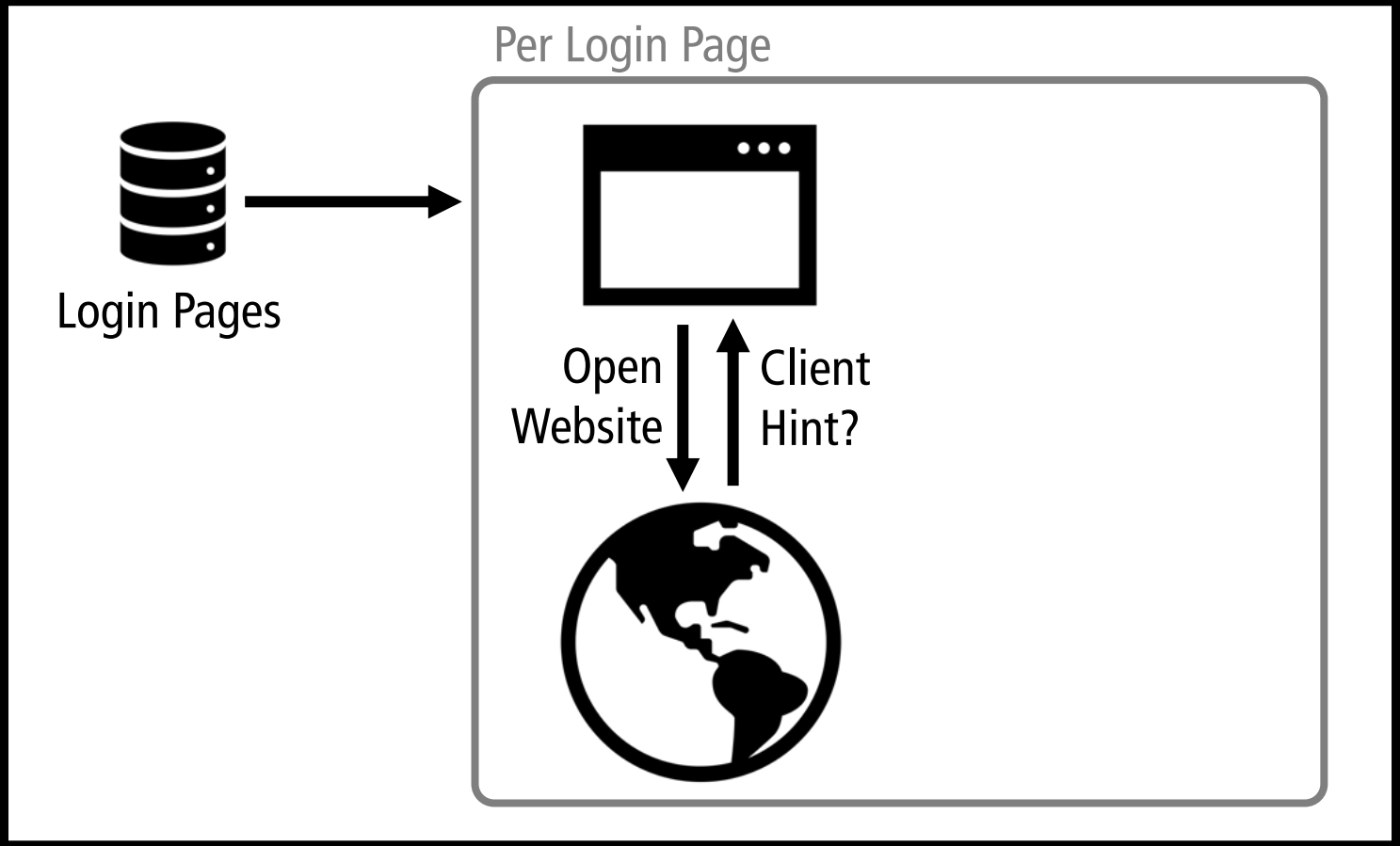
# Login Pages Crawling



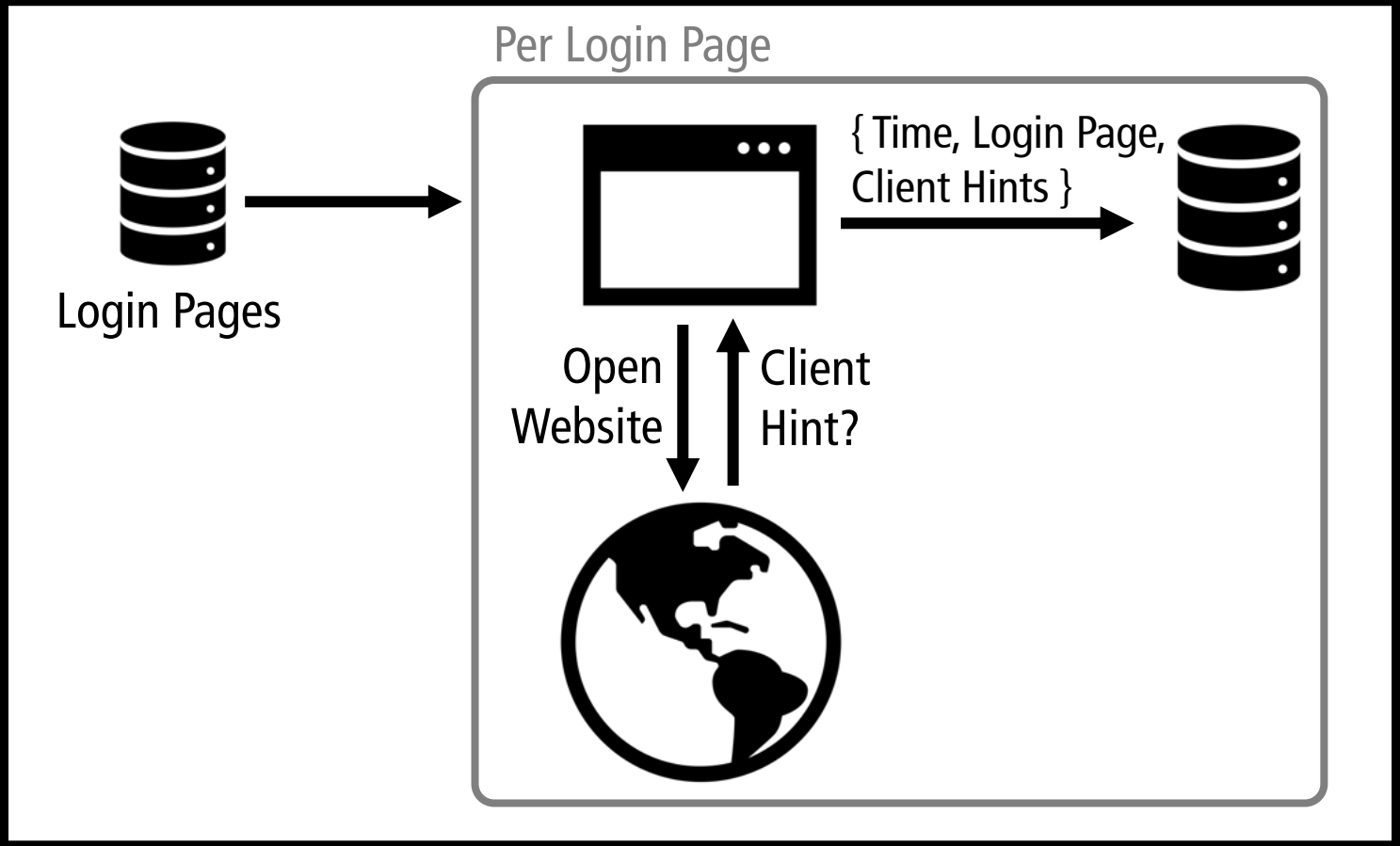
# Login Pages Crawling



# Login Pages Crawling



# Login Pages Crawling



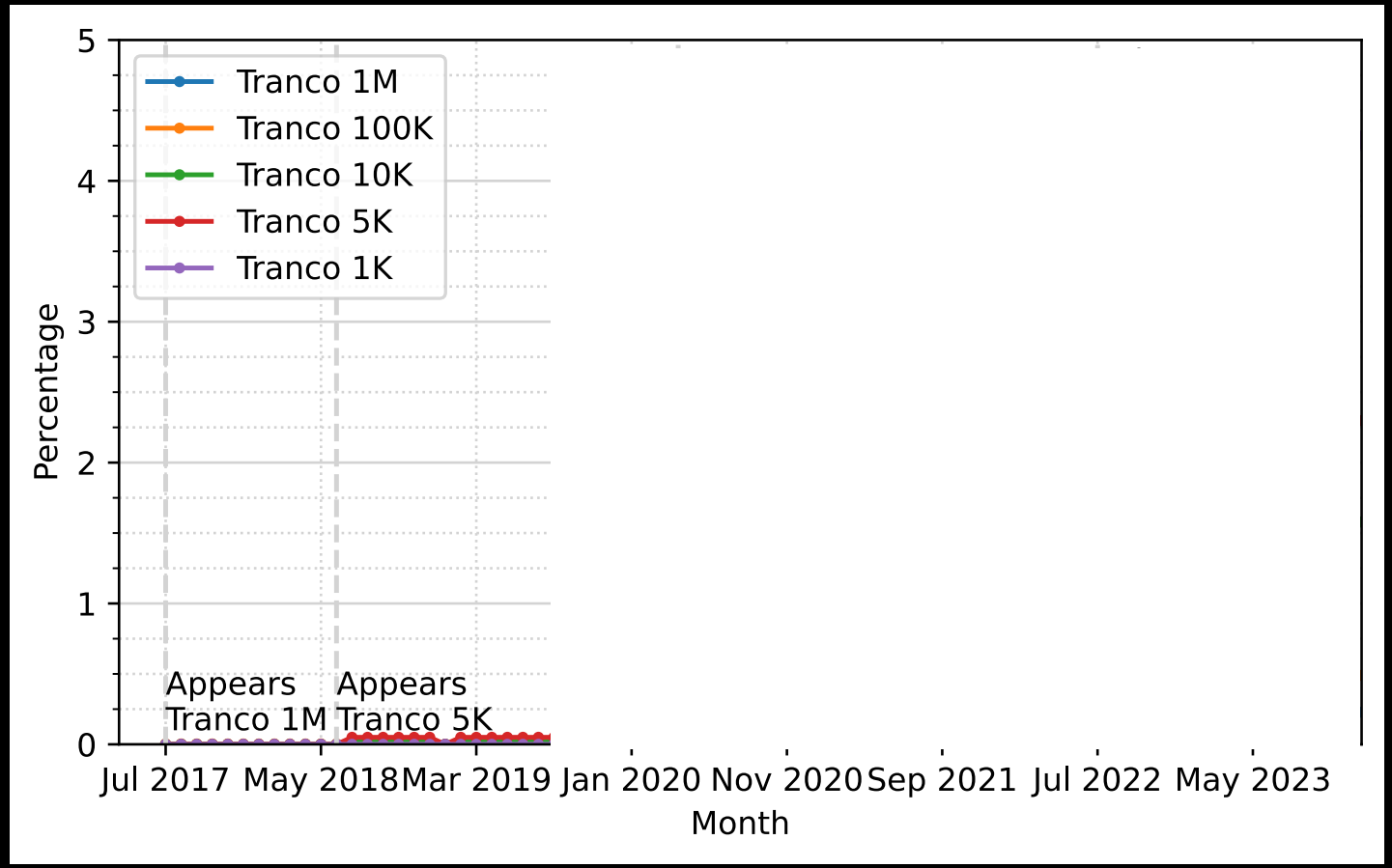
# Overview


Study

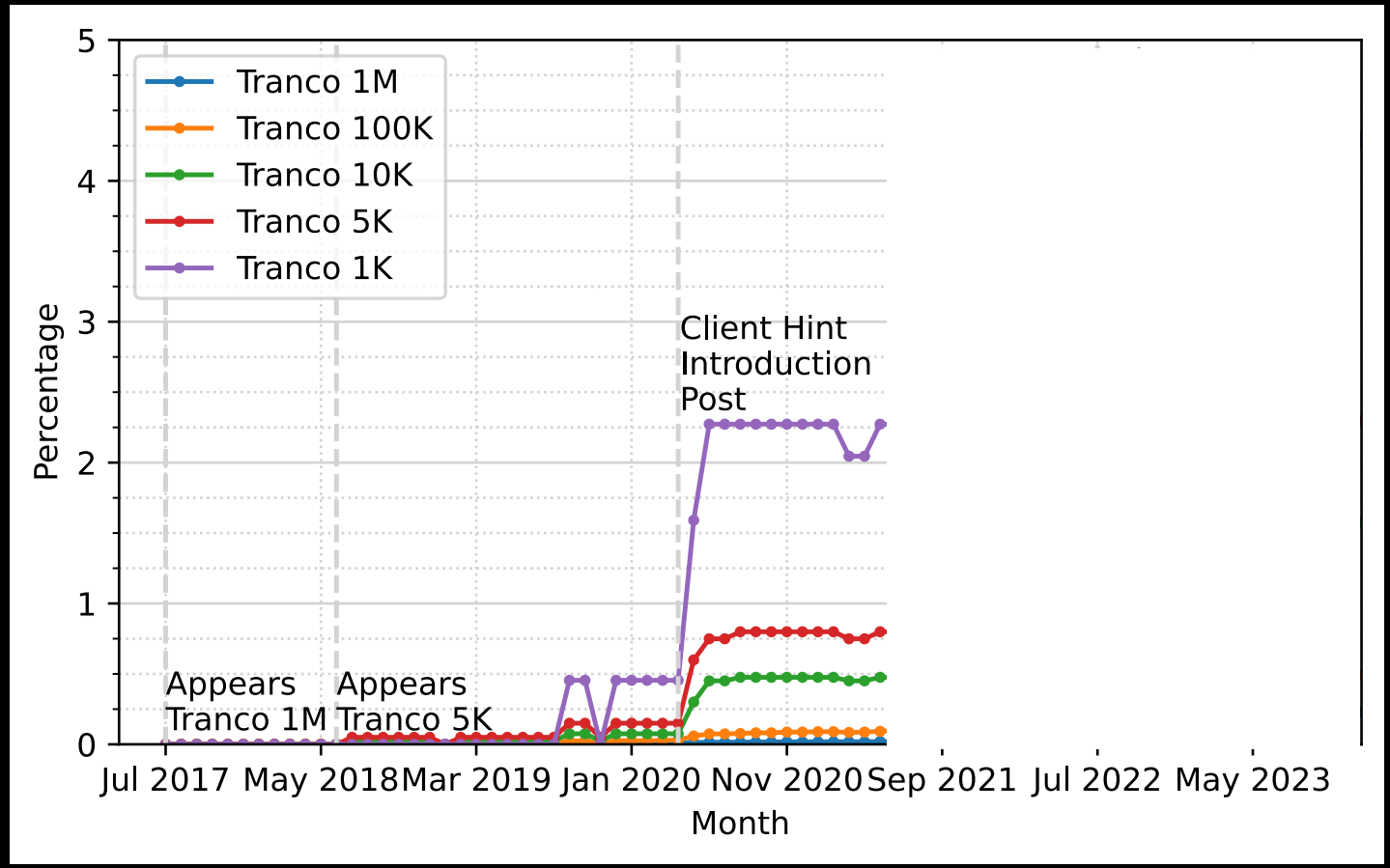

Results


Conclusion

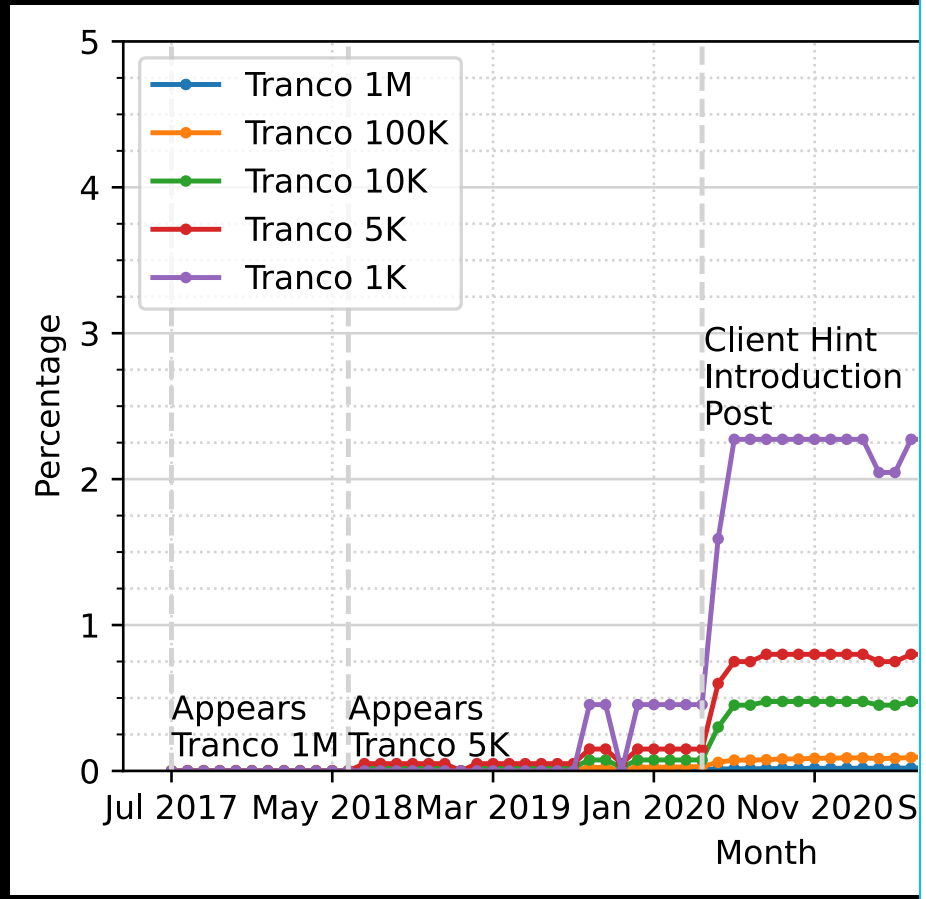
# HTTP CHs Get More Popular

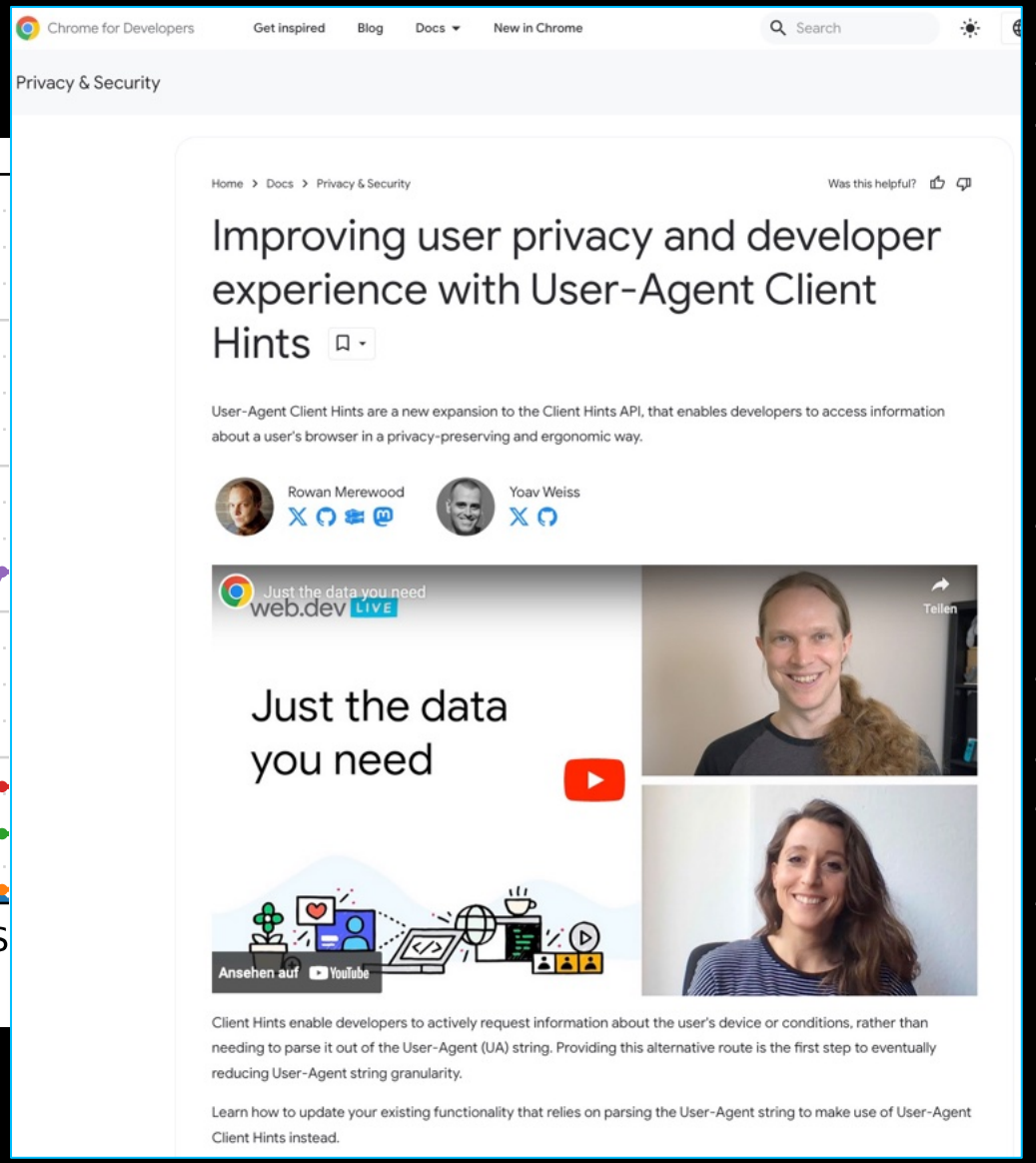


# HTTP CHs Get More Popular



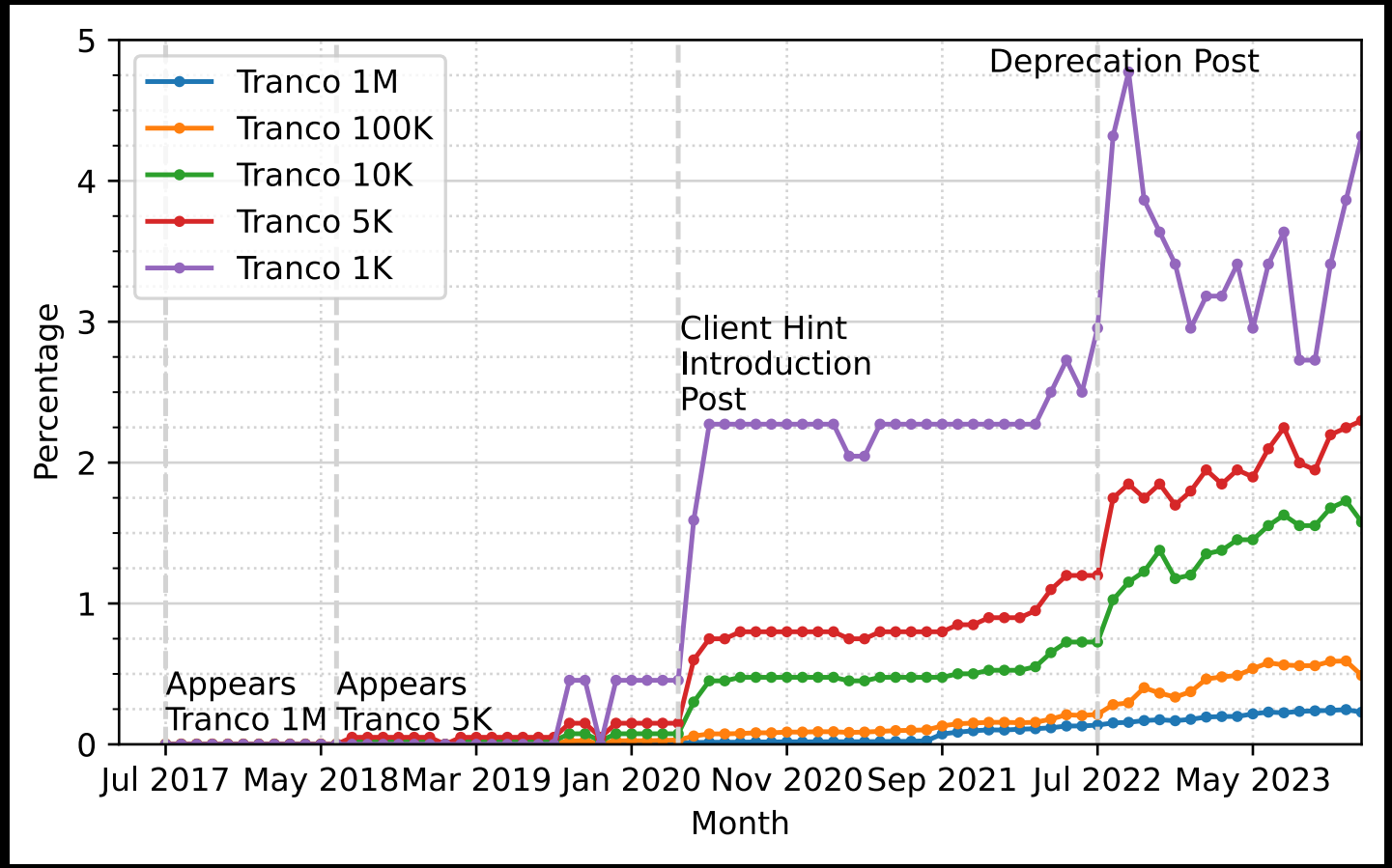
# HTTP CHs Get More Popular



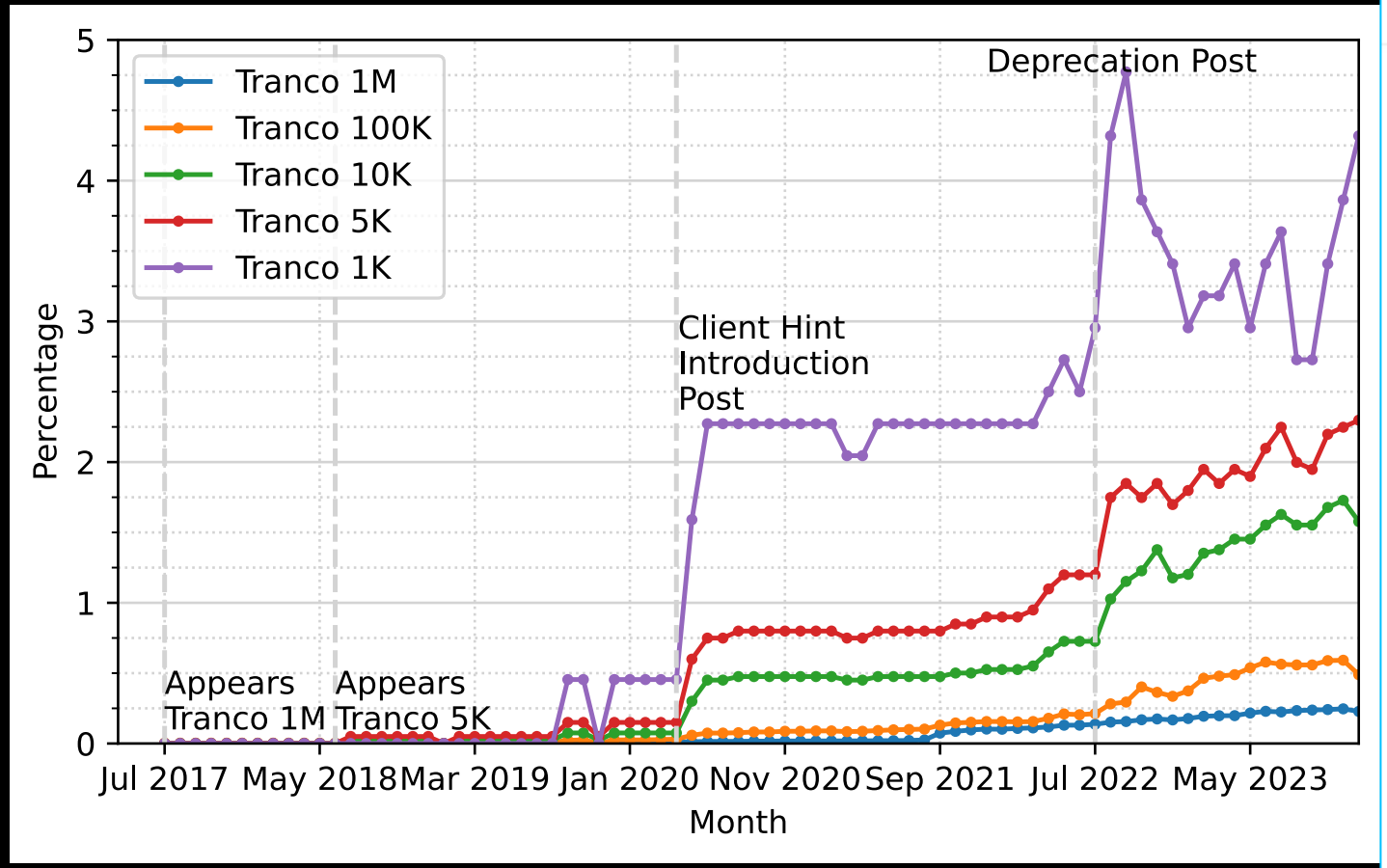



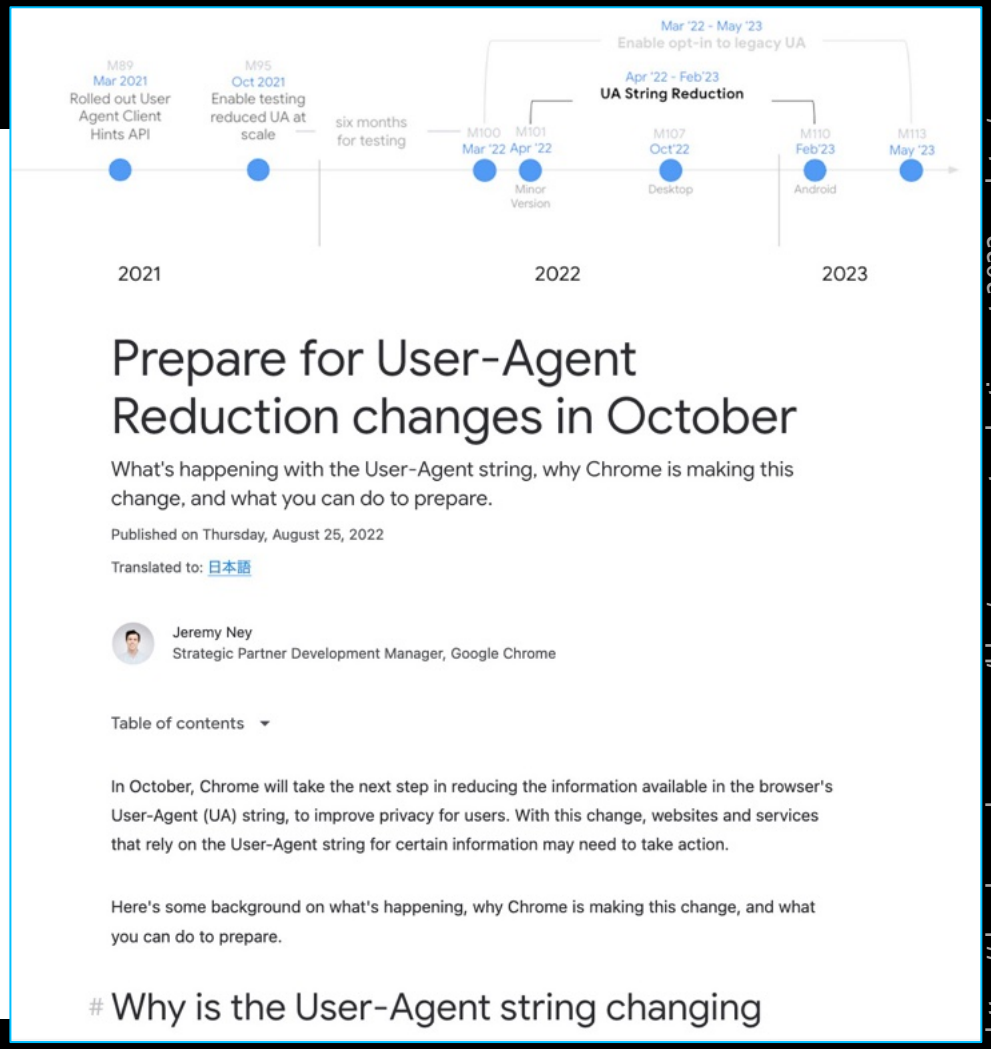

https://developer.chrome.com/docs/privacy-security/user-agent-client-hints

# HTTP CHs Get More Popular



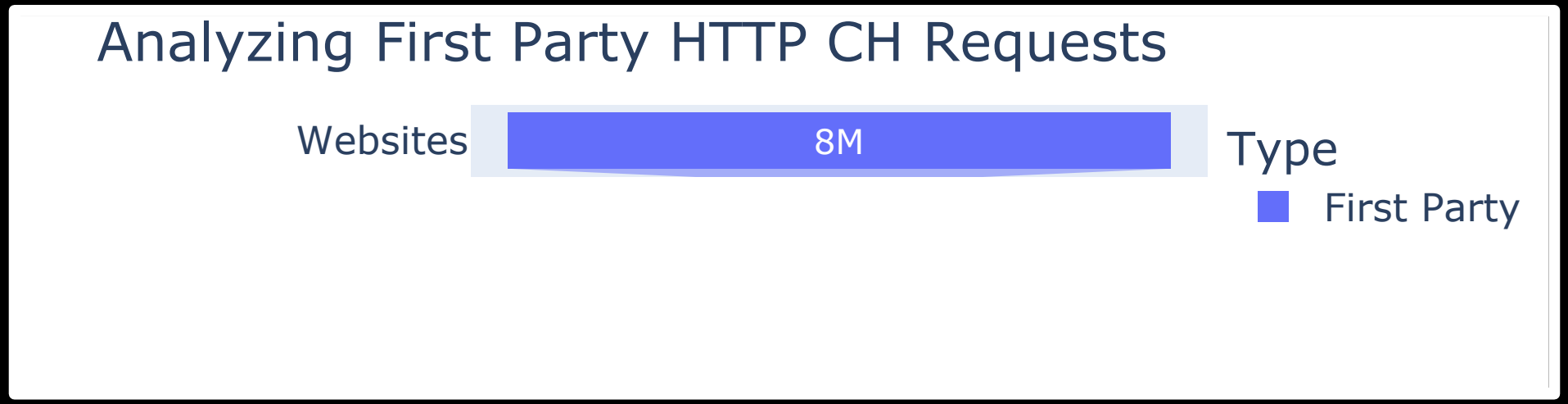
# HTTP CHs Get More Popular



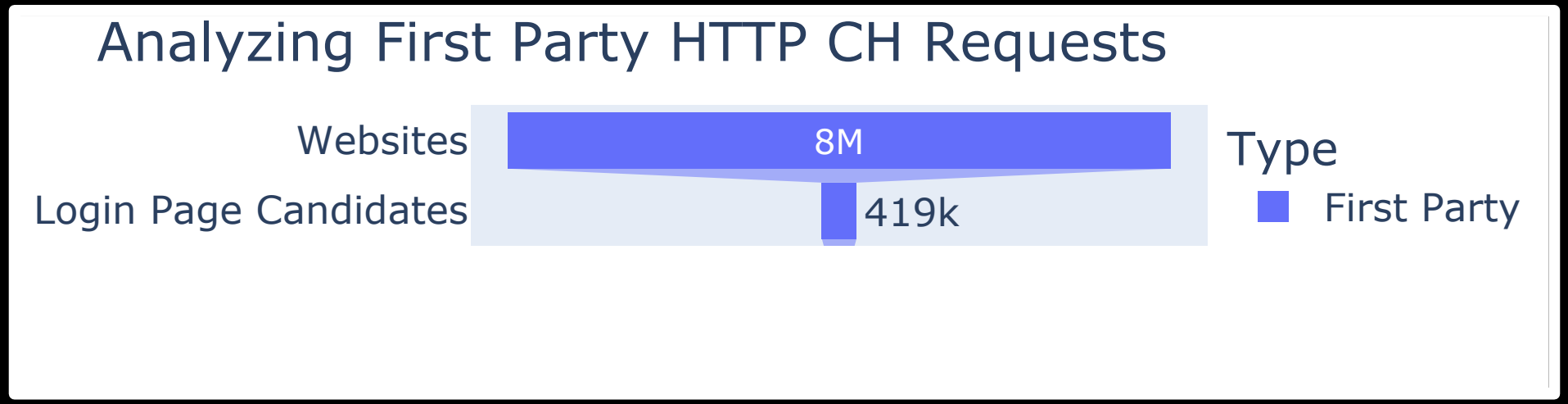




https://developer.chrome.com/blog/user-agent-reduction-oct-2022-updates/

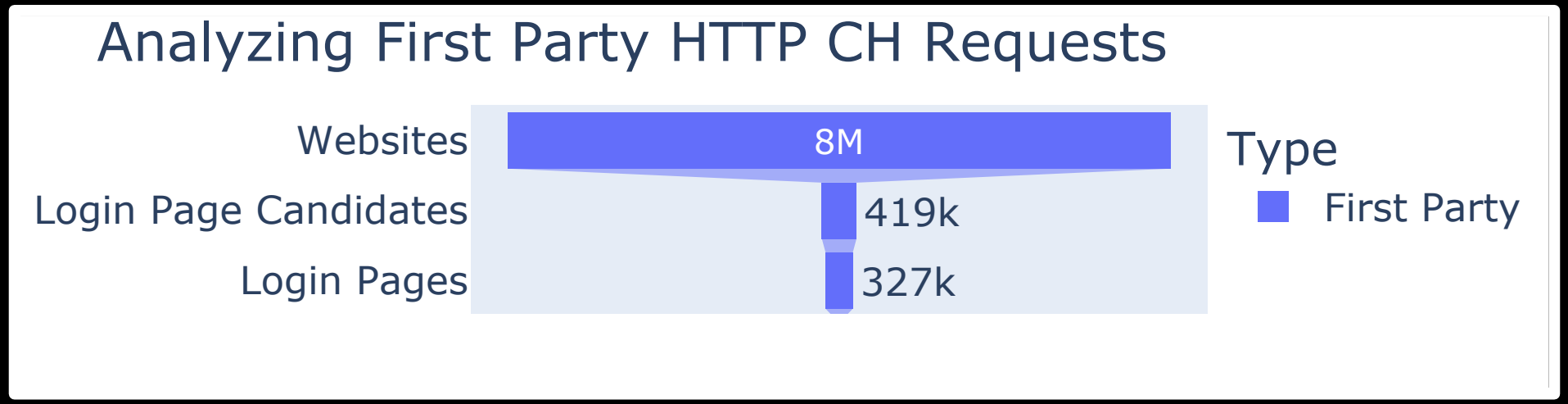
# But Only Few Websites Use Them



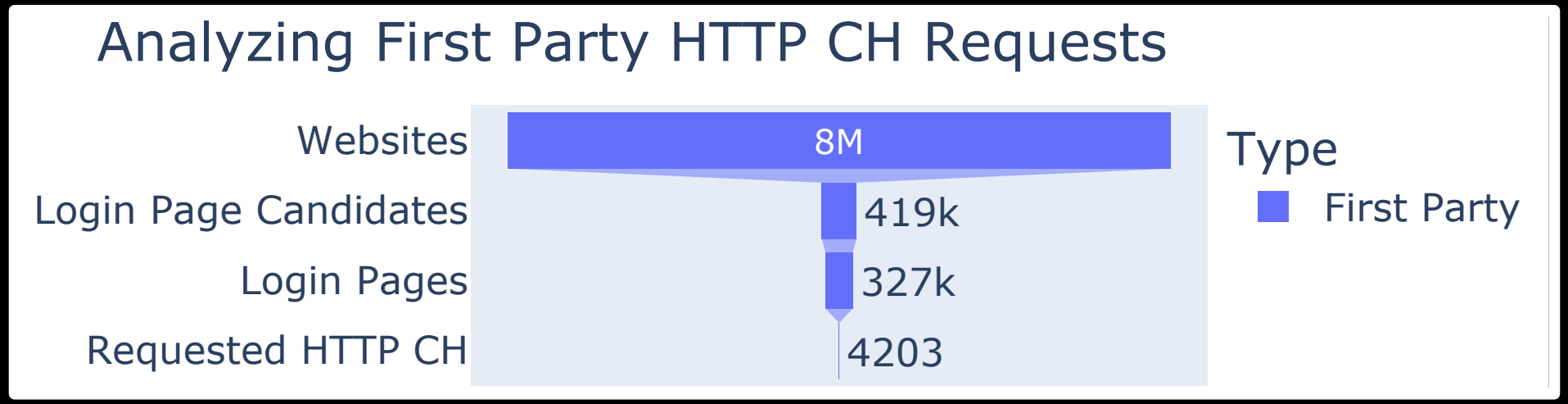
# But Only Few Websites Use Them



# But Only Few Websites Use Them

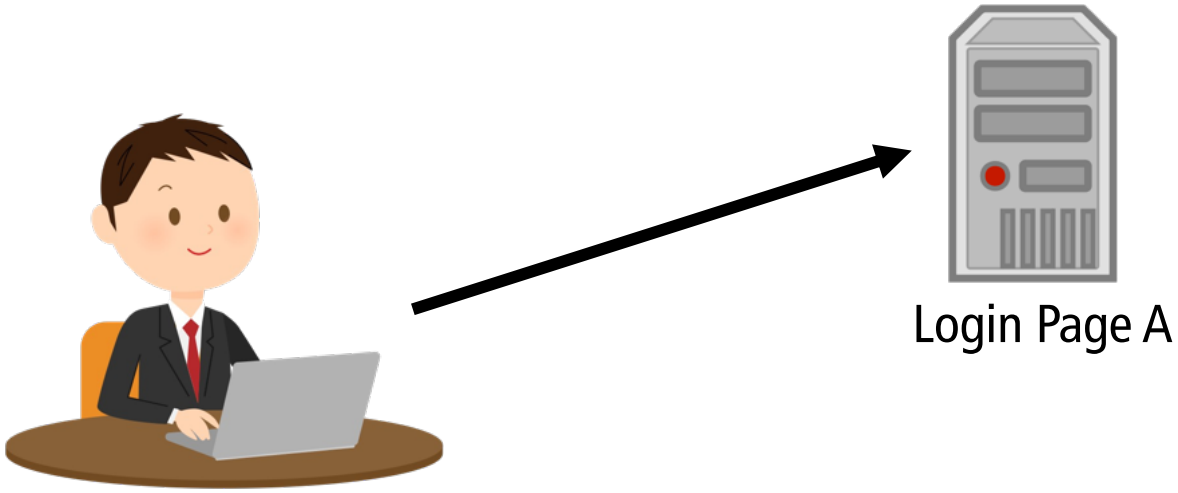


# But Only Few Websites Use Them

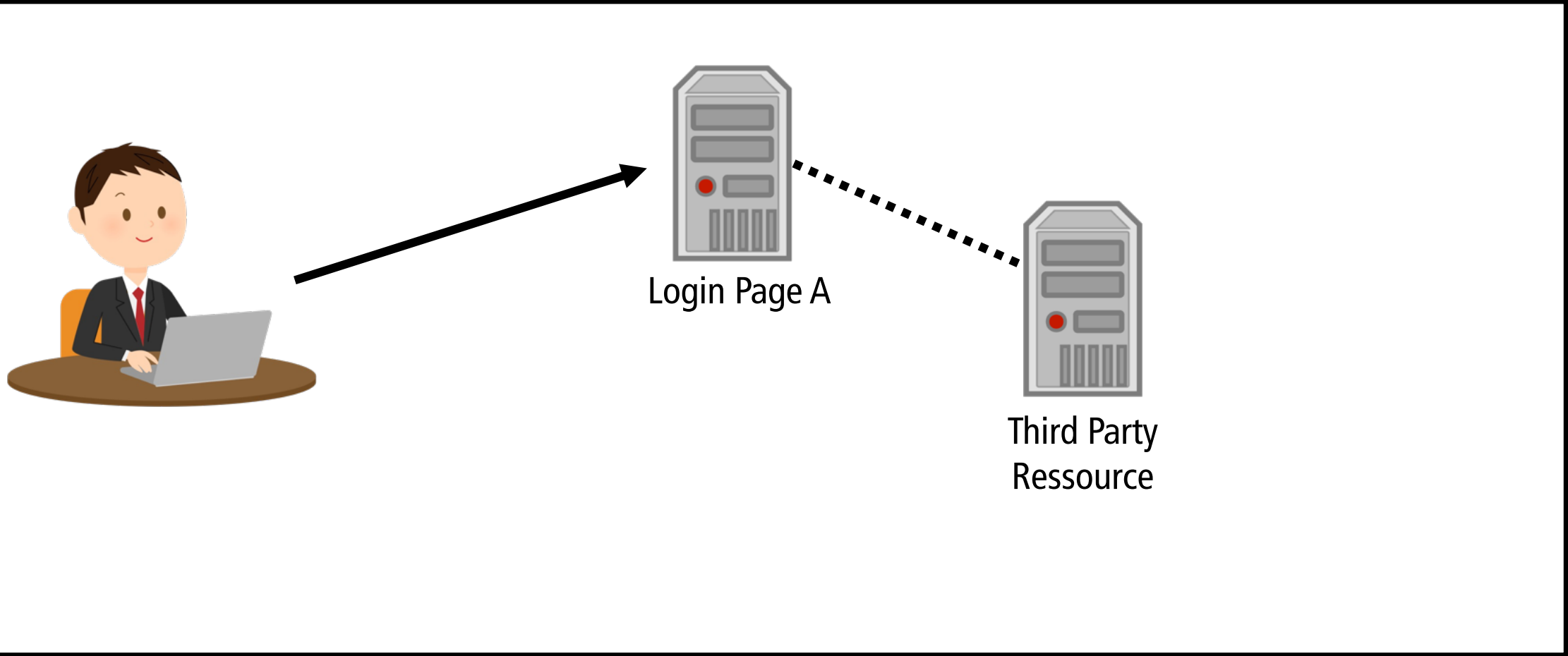


# Except for Embedded Third Parties

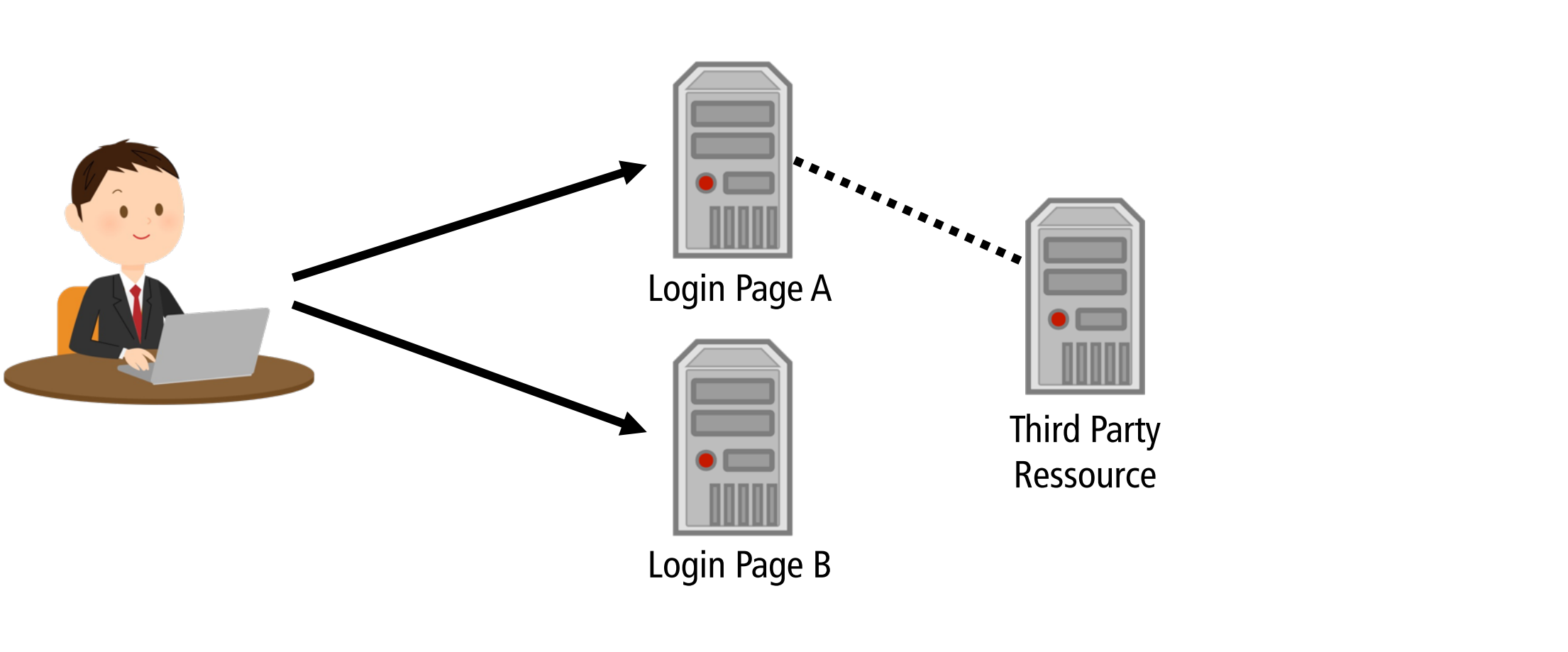
# Except for Embedded Third Parties



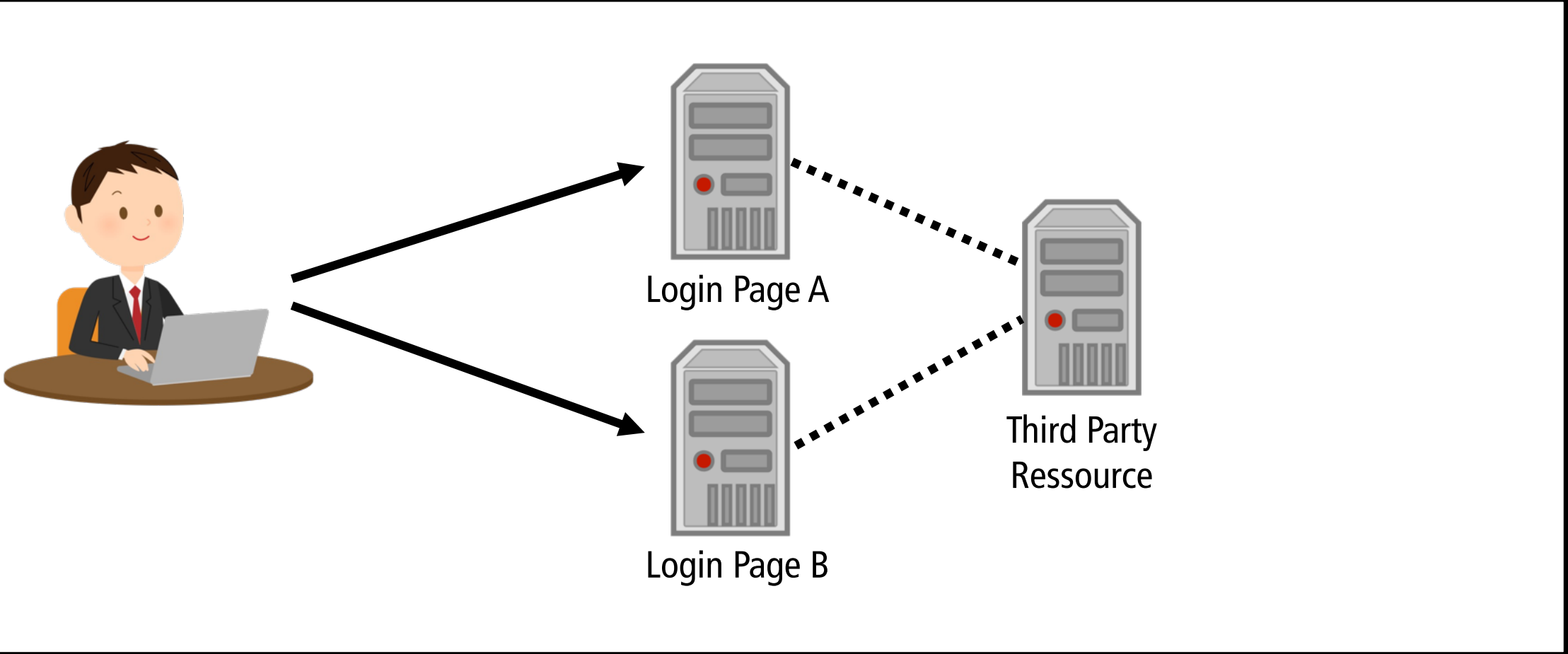
# Except for Embedded Third Parties



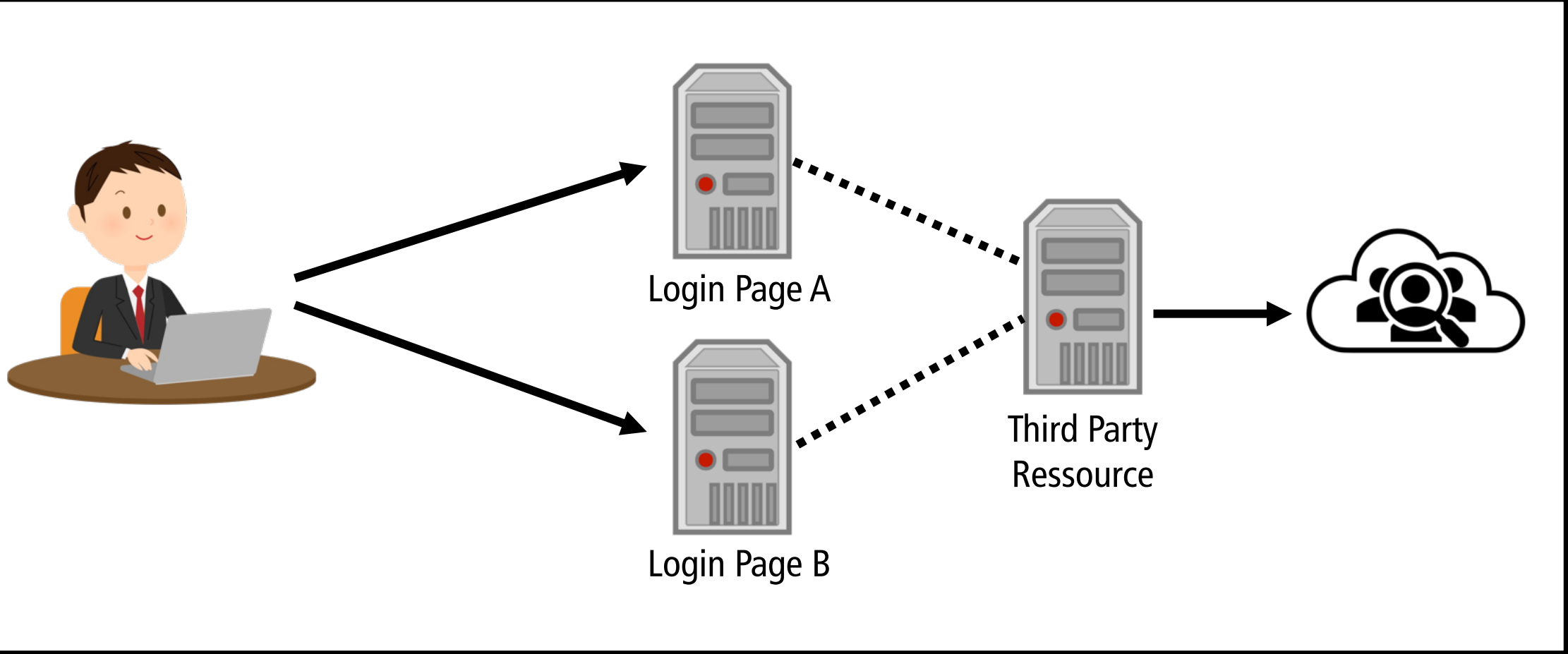
# Except for Embedded Third Parties



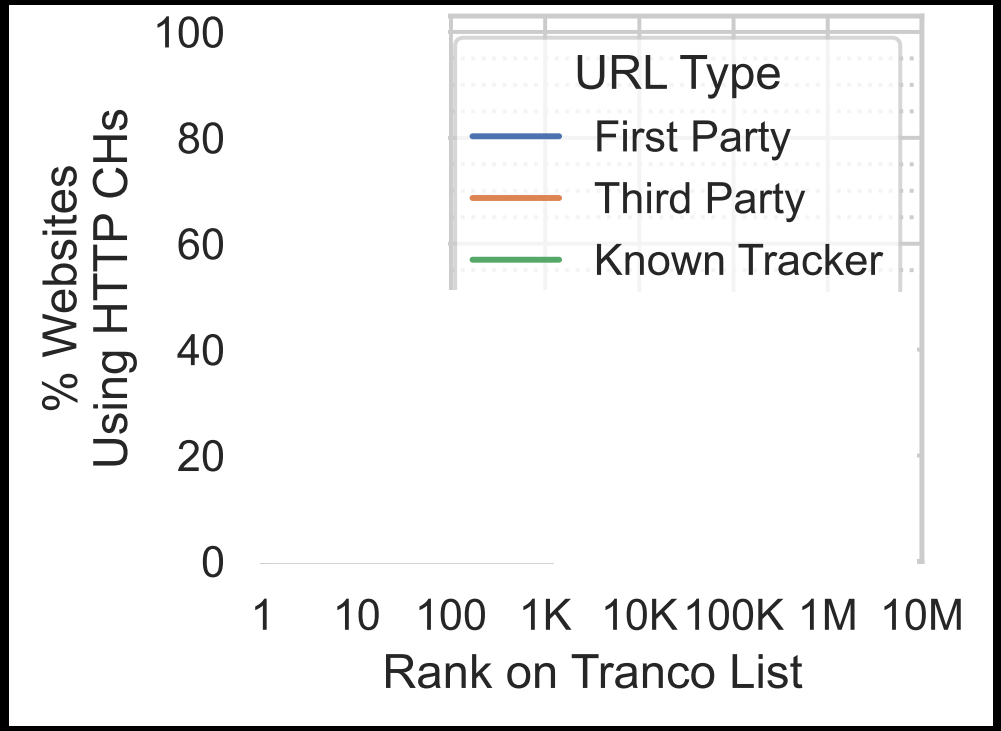
# Except for Embedded Third Parties



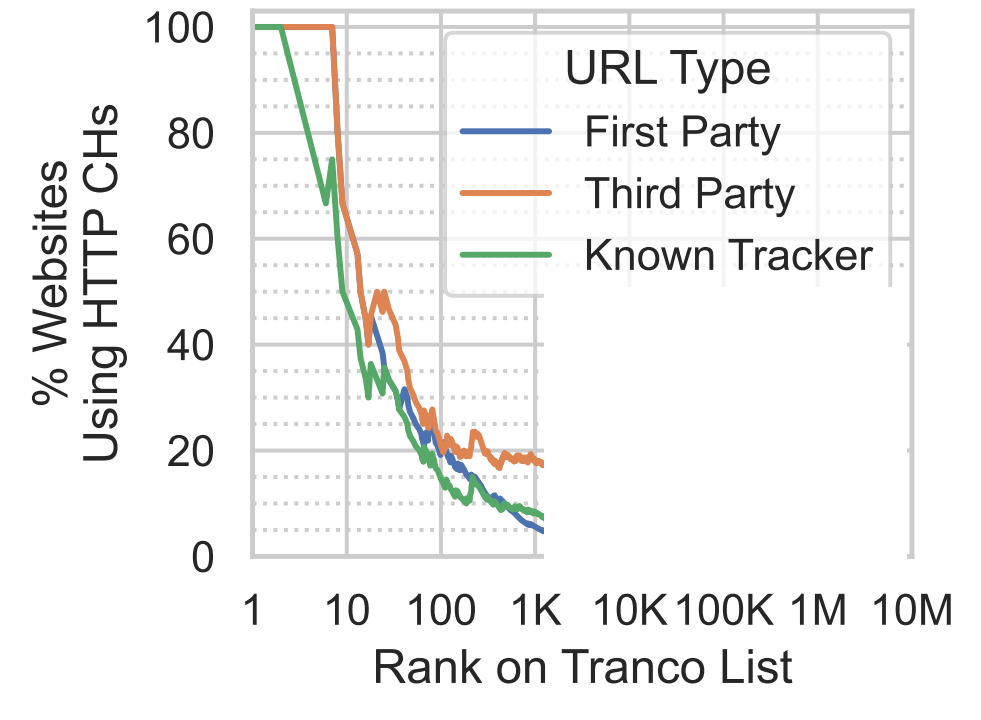
# Except for Embedded Third Parties



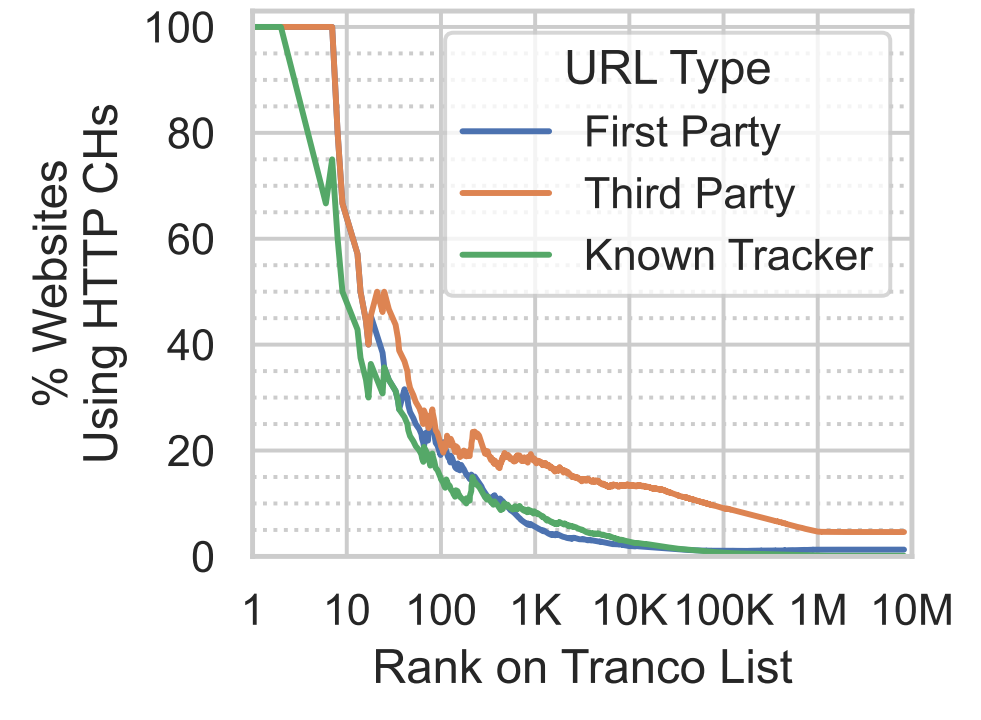
# Except for Embedded Third Parties



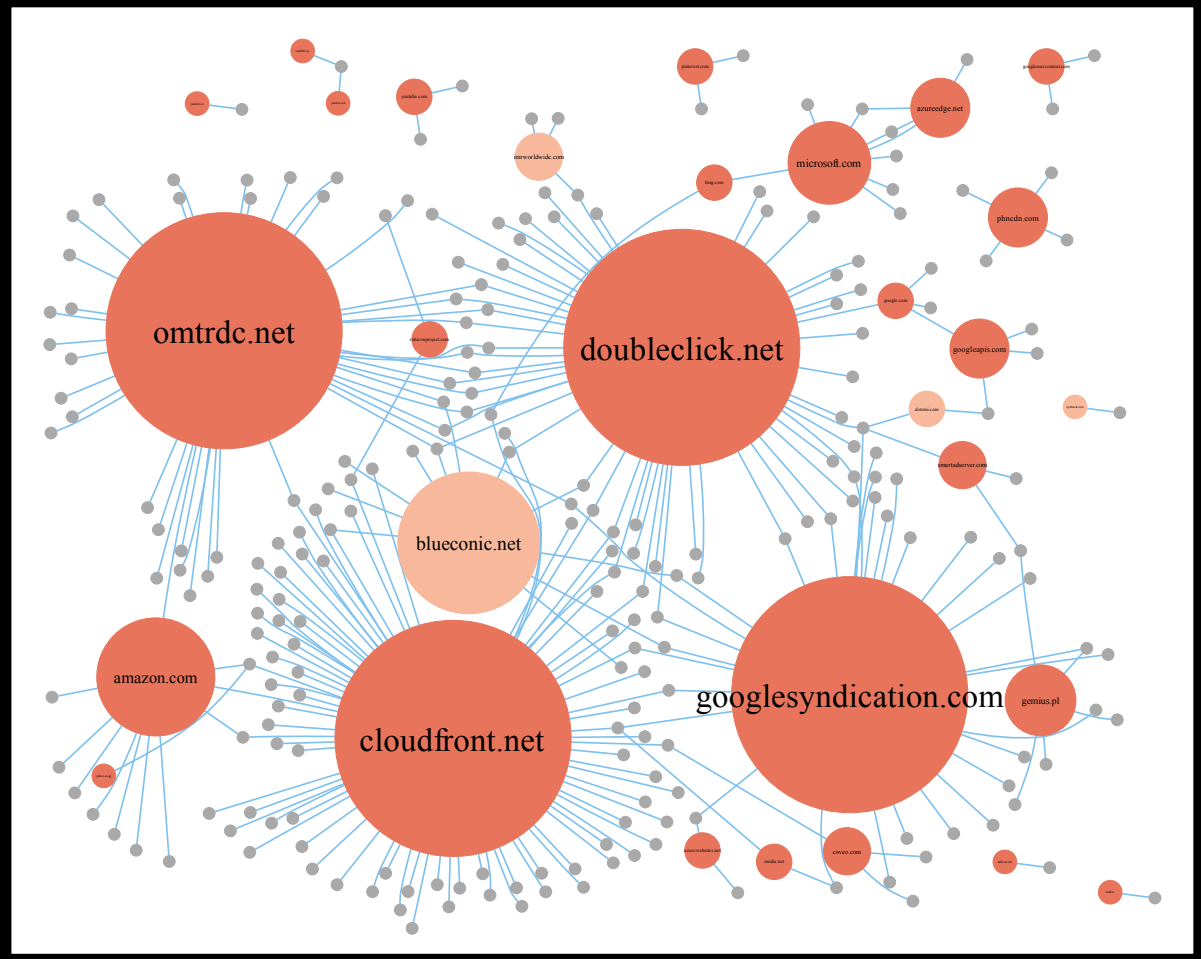
# Except for Embedded Third Parties



# Except for Embedded Third Parties

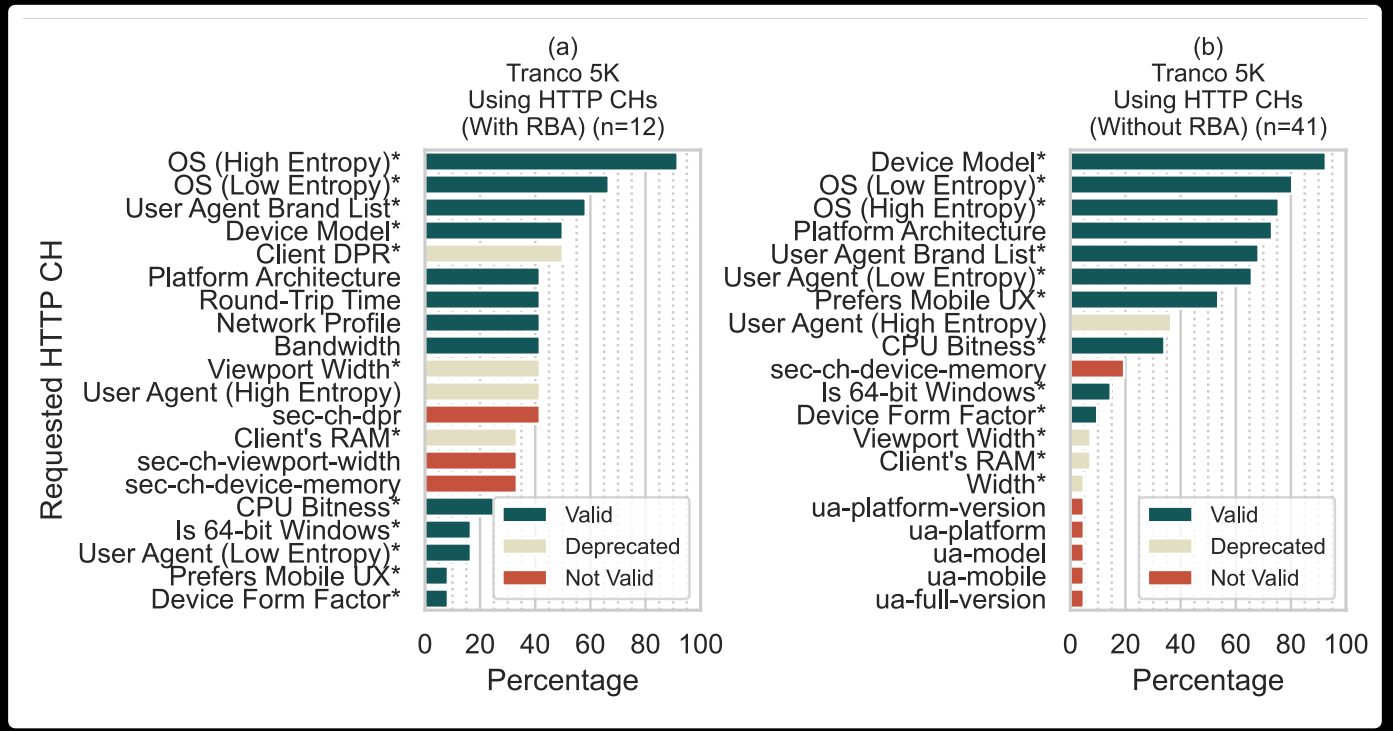


# Except for Embedded Third Parties



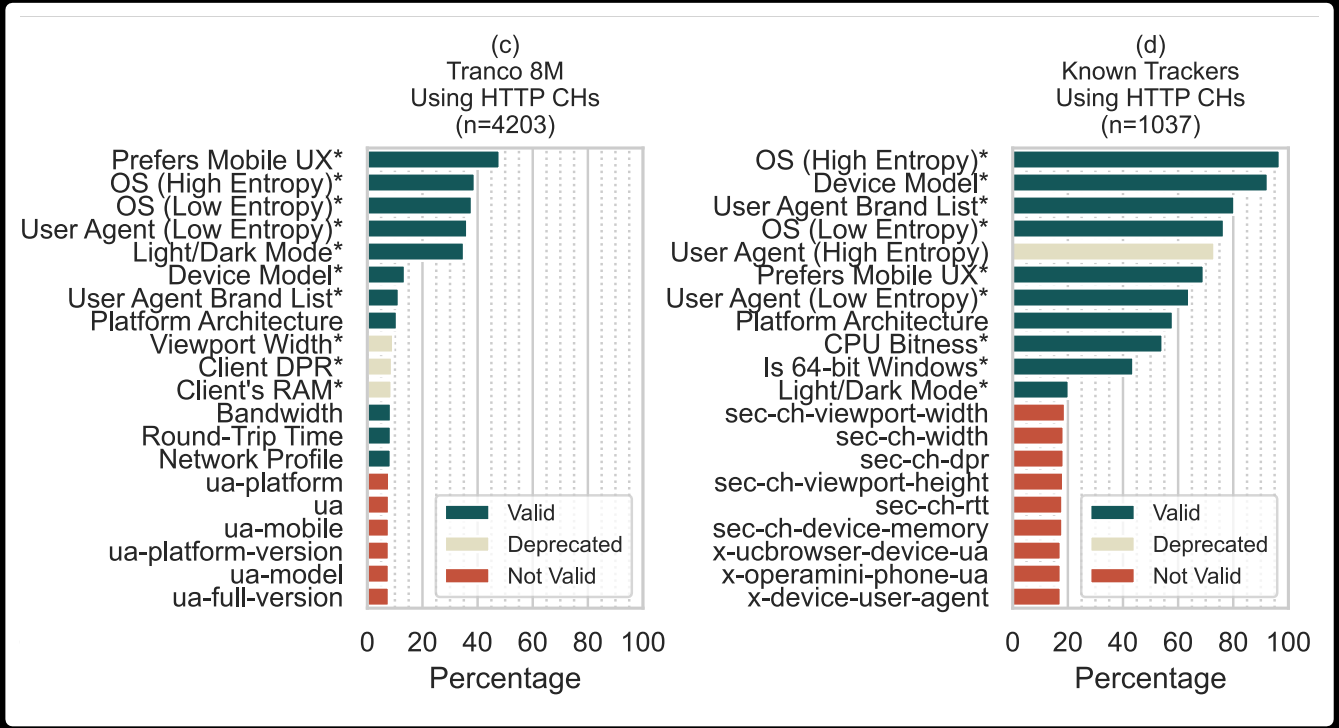
# Collected Data Differs on Use Case

- Websites with risk-based authentication (RBA) request higher entropy data than those without

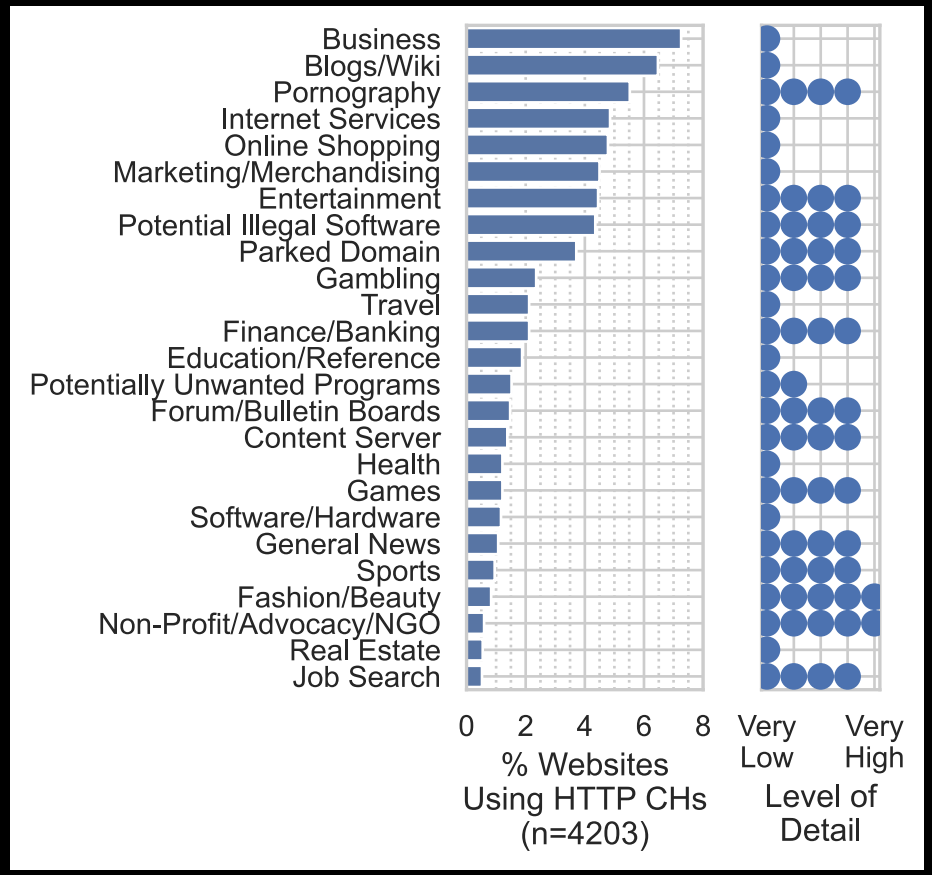


# Collected Data Differs on Use Case

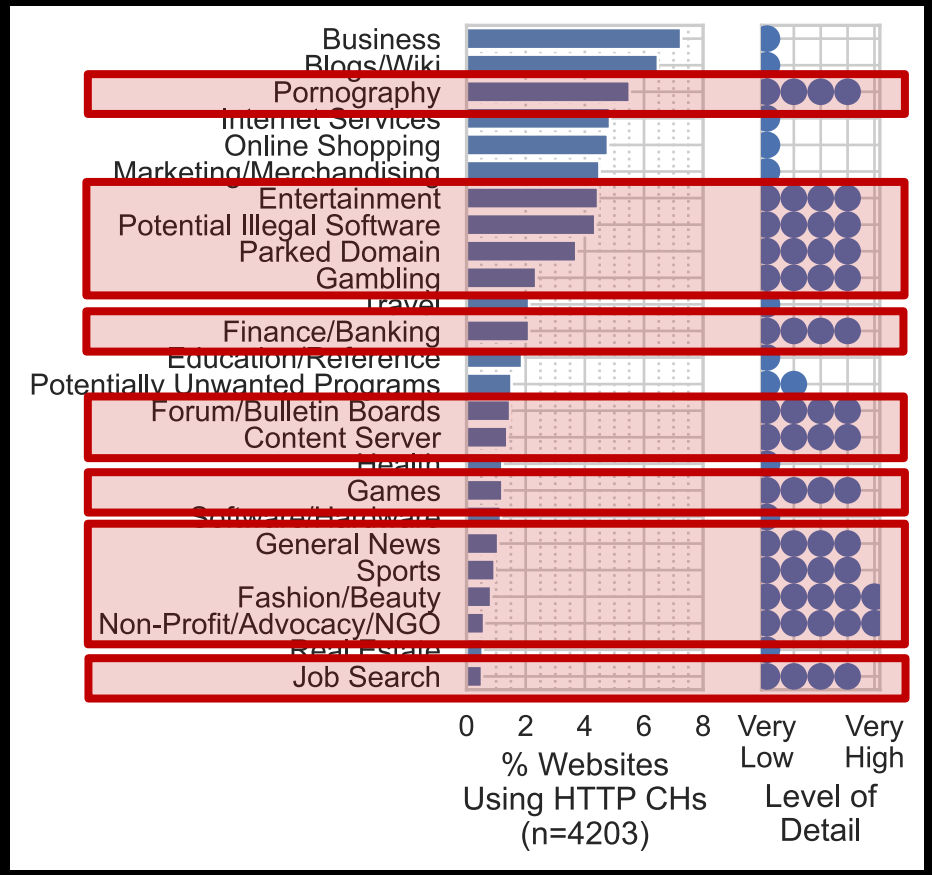
- Known trackers collect more high entropy data than general websites



# Website Type Matters, Too



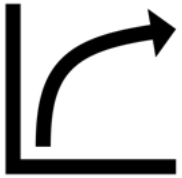
# Website Type Matters, Too



# Summary

*rbainfo.org/clienthints

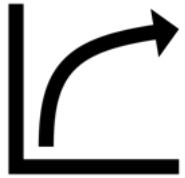
# Summary



- HTTP CHs are not widespread on 8M top websites

*rbainfo.org/clienthints

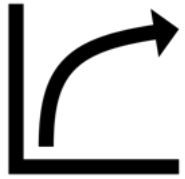
# Summary



- HTTP CHs are not widespread on 8M top websites
- But: Highly adopted by third-party trackers

*rbainfo.org/clienthints

# Summary

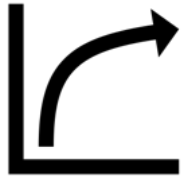


- HTTP CHs are not widespread on 8M top websites
- But: Highly adopted by third-party trackers

- Privacy issue: HTTP CHs collect more data than the classical user agent string

*rbainfo.org/clienthints

# Summary

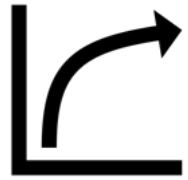


- HTTP CHs are not widespread on 8M top websites
- But: Highly adopted by third-party trackers

- Privacy issue: HTTP CHs collect more data than the classical user agent string
- Browsers should implement countermeasures

*rbainfo.org/clienthints

# Summary



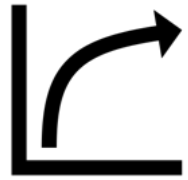
- HTTP CHs are not widespread on 8M top websites
- But: Highly adopted by third-party trackers

- Privacy issue: HTTP CHs collect more data than the classical user agent string
- Browsers should implement countermeasures

- Crawling data provided as open data*

*rbainfo.org/clienthints

# Summary



- HTTP CHs are not widespread on 8M top websites
- But: Highly adopted by third-party trackers

- Privacy issue: HTTP CHs collect more data than the classical user agent string
- Browsers should implement countermeasures

- Crawling data provided as open data*
- Login URLs provided to ethical researchers on request

*rbainfo.org/clienthints

# Thank you

rbainfo.org/clienthints
das.h-brs.de

clienthints@swiefling.de
luigi.lo_iacono@h-brs.de

@swiefling@hci.social