Université de Lille

CRIStAL

Inria

Leveraging browser fingerprinting to strengthen Web authentication

Antonin Durey

Inria, 14th January 2022

Supervisors
Romain ROUVOY, Univ. Lille - CRIStAL
Walter RUDAMETKIN, Univ. Lille - CRIStAL

Reviewers
Olivier BARAIS, Univ. Rennes 1 - IRISA
Sonia BEN MOKHTAR, CNRS - LIRIS

Examinators
Gunes ACAR, Radboud University Nijmegen
Isabelle CHRISMENT, TELECOM Nancy - LORIA
Marc TOMMASI, Univ. Lille - CRIStAL

Invited
Arnaud PÉRILLOUX, Ministère des Armées

Plan

Introduction

Contributions

I) Study fingerprinting uses for web authentication

II) Design and evaluate a fingerprint linking algorithm

III) Evaluate a web authentication system with fingerprinting

Conclusions & perspectives

Plan

Introduction

Contributions

I) Study fingerprinting uses for web authentication

II) Design and evaluate a fingerprint linking algorithm

III) Evaluate a web authentication system with fingerprinting

Conclusions & perspectives

Authentication

Informations commande

Nom de client : Antonin Durey

Commande N° : 330
Date d'ajout : 02/12/2021 19:18:01
Mode de paiement : Carte bancaire
Mode de livraison : Livraison

Courriel : imafake@email.com
Téléphone : 0600000000
Adresse IP : 127.0.0.1

Lundi 27 décembre 2021 10:10

CHU de Lille - Centre vaccination Covid - 19
Centre de vaccination COVID-19

Nom du vaccin
BioNTech/Pfizer

Nom du patient
John DOE

Numéro de téléphone
06 00 00 00 00

Identification proof

password collected via

Université de Lille

Service d'authentification

Username:

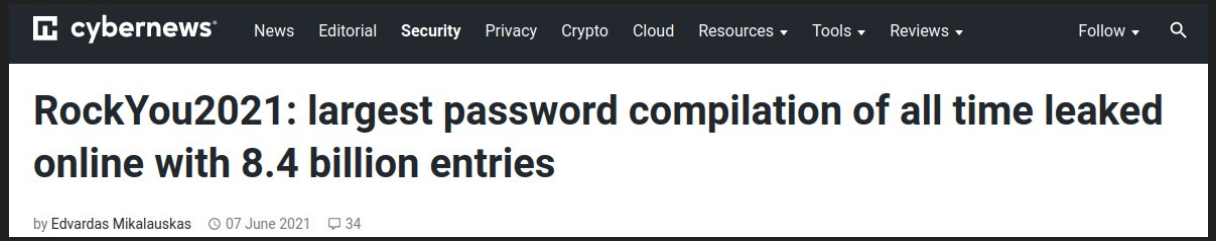
Password:

LOGIN

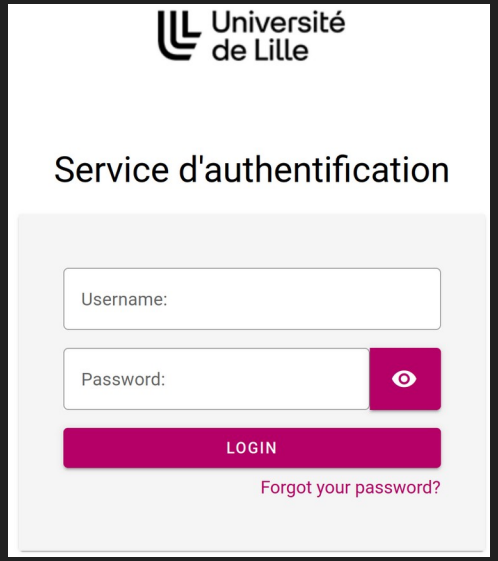
Forgot your password?

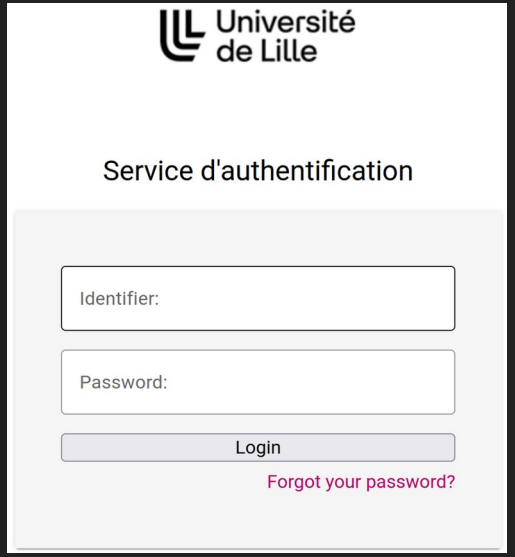
Threats from attacks

- Data leaks



- Phishing





User Experience

Strong requirement towards user acceptance

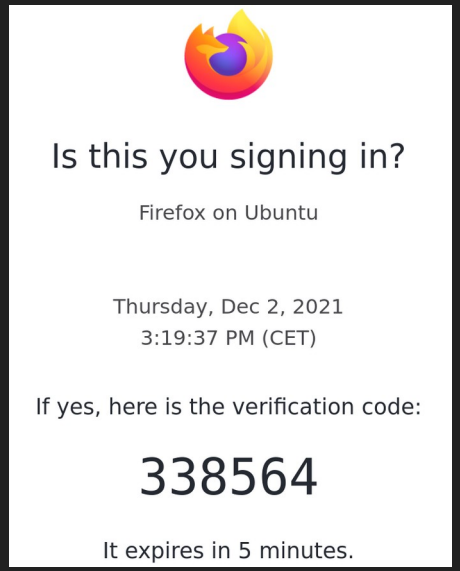
UX decreases:

- Too many passwords to remember
- Strict password-compositions policies

Komanrudi: "*Of passwords and people: measuring the effect of password-composition policies*", CHI'11
Wash: "*Understanding password choices: How frequently entered passwords are re-used across websites.*", SOUPS'16

Authentication system	Security	User experience
Password	✗	~
?	✓	✓

Multi-Factor Authentication



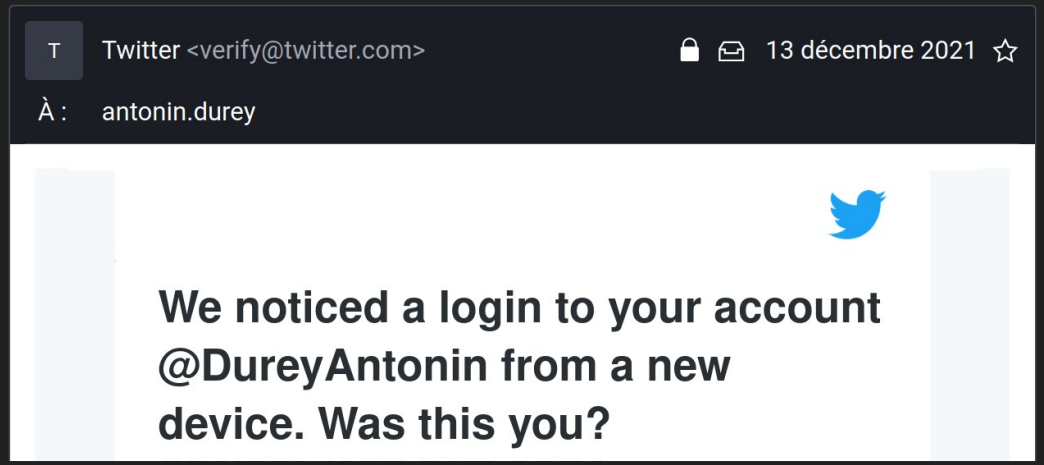
Additional identity proof

Authentication system	Security	User experience
Password	✗	~
Multi-factor	✓	✗

Wiefling: "*More than just good passwords? A study on usability and security perceptions of risk-based authentication.*", ACSAC'20

Risk-Based Authentication

Risk level computation



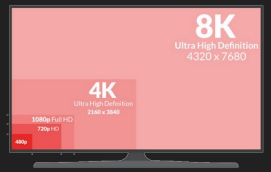
Cookies & IP address

Wiefling: "*Is this really you? an empirical study on risk-based authentication applied in the wild.*", IFIPSEC'19
Wiefling: "*More than just good passwords? A study on usability and security perceptions of risk-based authentication.*", ACSAC'20

Authentication system	Security	User experience
Password	✗	~
Multi-factor	✓	✗
Existing risk-based	~	~
?	✓	✓

Browser fingerprinting

Information about the user's device & browser



Cwm fjordbank glyphs vext quiz, 😃

Cwm fjordbank glyphs vext quiz, 😃

Lora Courier Pacifico New Economica Corsiva Caveat

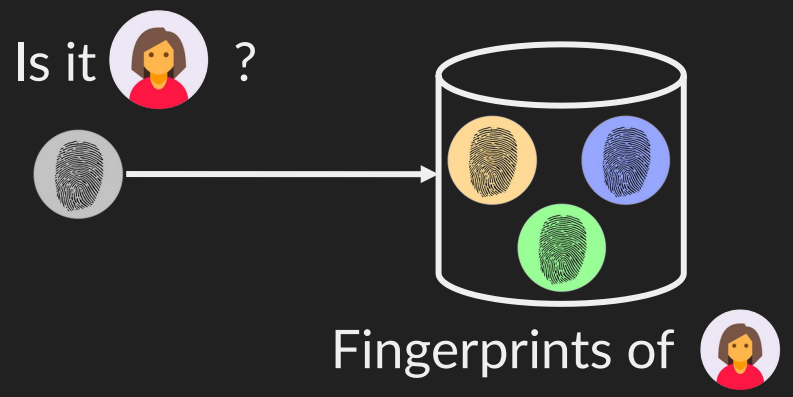
Diversity leads to unicity

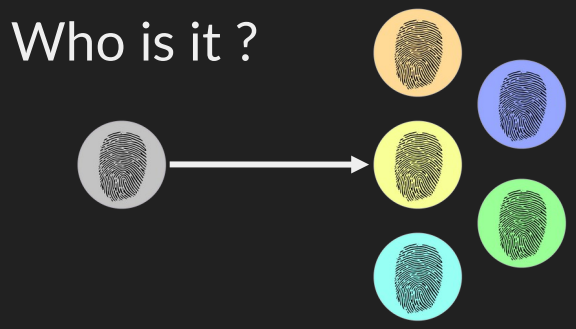
Eckersley: "*How Unique is your web browser?*", PETS'10

Laperdrix: "*Beauty and the Beast: Diverting modern web browsers to build unique browser fingerprints*", S&P'16

Need to link fingerprints

Authentication versus Tracking

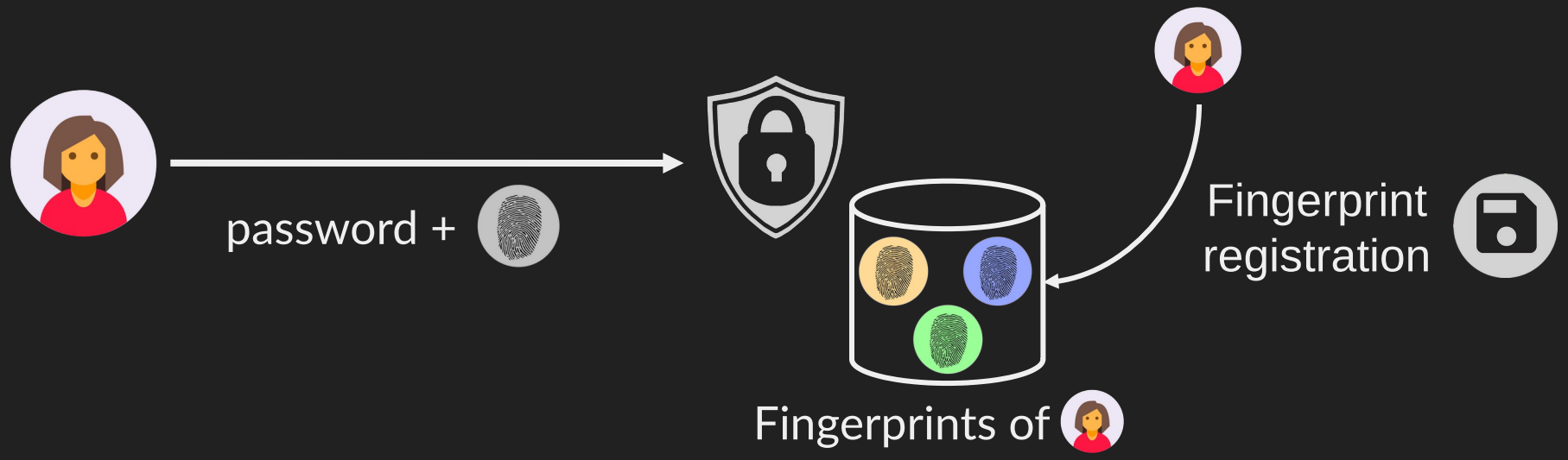




No algorithms for fingerprint-based authentication

Vastel: "*FP-STALKER: tracking browser fingerprint evolutions.*", S&P'18
Li: "*Who touched my browser fingerprint?*", IMC'20

Fingerprint-based authentication



No evaluation

Unger: "*SHPF: enhancing HTTP(S) session security with browser fingerprinting.*", ARES'13

Alaca: "*Device fingerprinting for augmenting web authentication: classification and analysis of methods.*", ACSAC'16

Authentication system	Security	User experience
Password	✗	~
Multi-factor	✓	✗
Existing risk-based	~	~
Fingerprint-based	✓	✓

More secure with low UX impact

Contributions - key findings

We show that:

- Fingerprinting is not being used for authentication
- Fingerprints are linkable for authentication
- Fingerprint-based authentication is reliable

Plan

Introduction

Contributions

I) Study fingerprinting uses for web authentication

"FP-Redemption: Studying Browser Fingerprinting Adoption for the Sake of Web Security", *DIMVA'21*

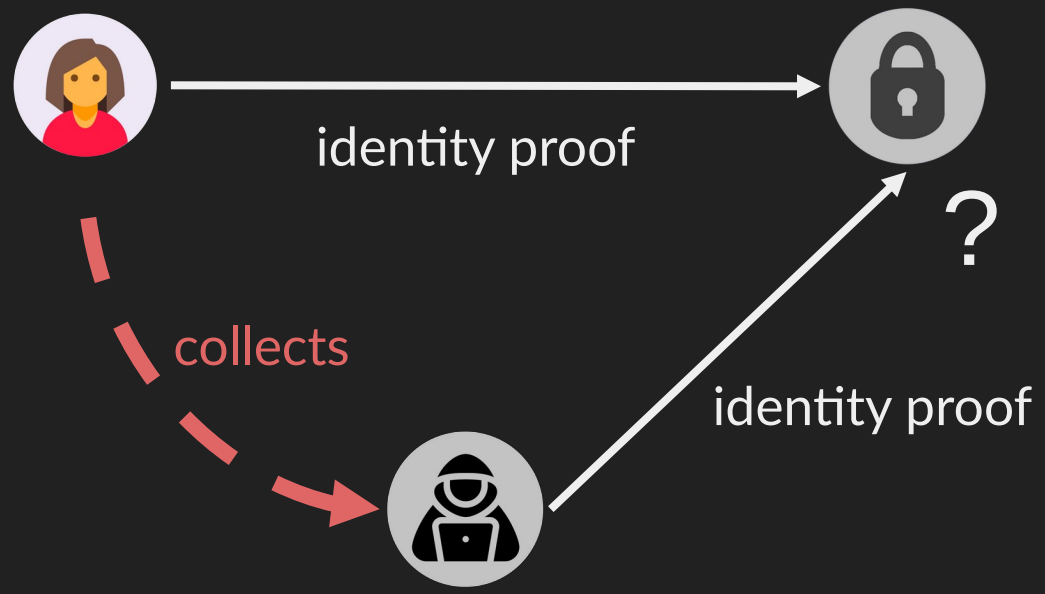
II) Design and evaluate a fingerprint linking algorithm

III) Evaluate a web authentication system with fingerprinting

Conclusions & perspectives

Hypothesis

Attacks target sensitive pages



Password & cookie 

Threat model: authentication & session attacks

- Stolen password

  sign-in pages 

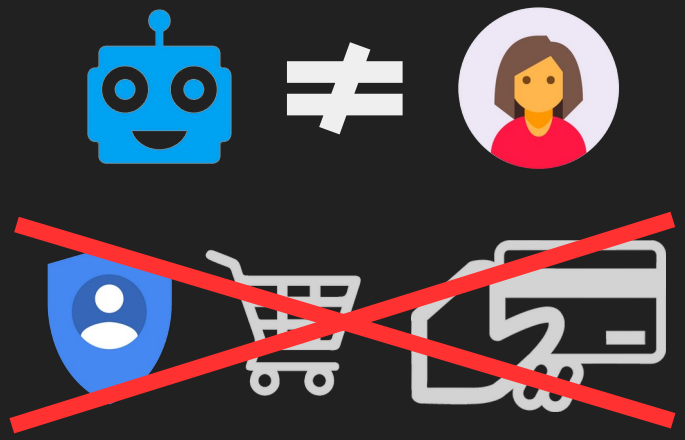
- Cookie hijacking 

  basket & payment pages 

Do websites use fingerprinting to strengthen security?

Existing datasets

- biases in the dataset
- no sensitive pages
- crawls lack depth



Need for a tailored dataset

Acar: "*The Web Never Forgets: Persistent Tracking Mechanisms in the Wild.*", CCS'14
Englehardt: "*Online Tracking: A 1-million-site Measurement and Analysis.*", CCS'16

Dataset of sensitive pages

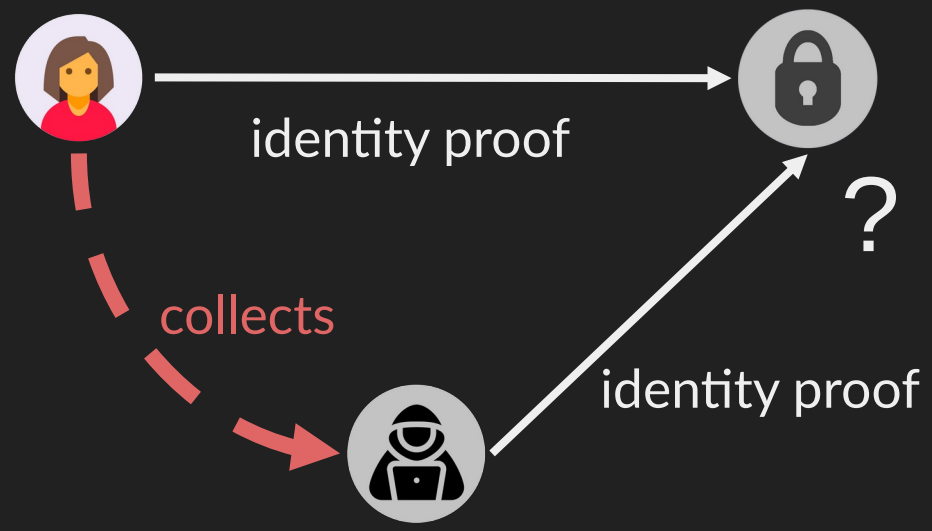
- 1 485 pages from 446 websites
  - 42 accounts created
  - 84 payments actions

Resulting fingerprinting dataset

- **Collected on**   
- By security-centered organizations
- Besides security mechanisms 

Are fingerprints used for security?

Hypothesis

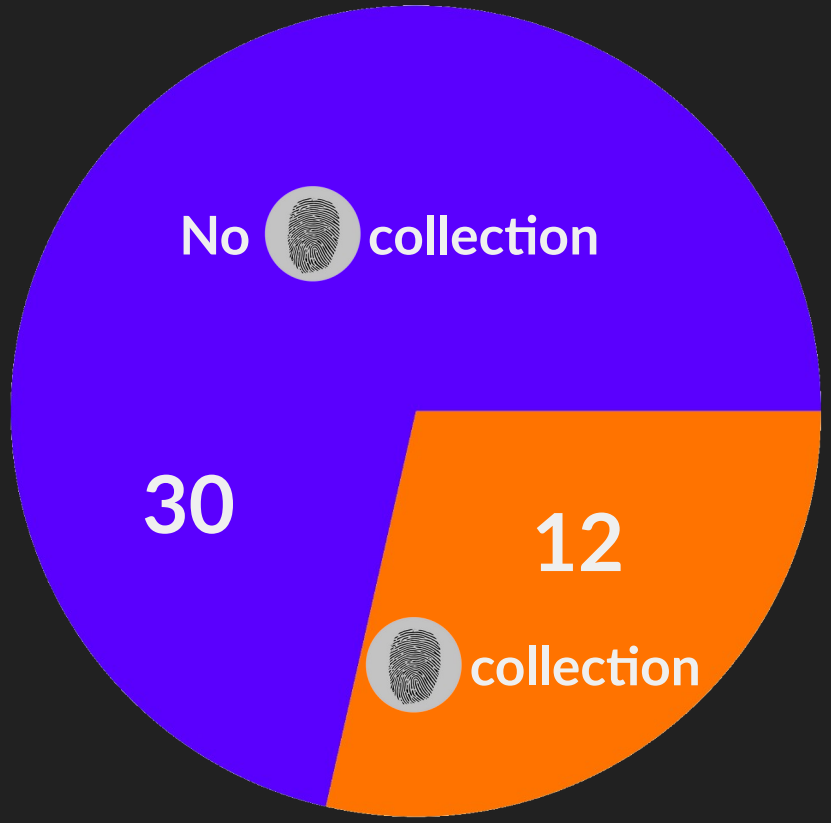


Evaluate fingerprinting for security

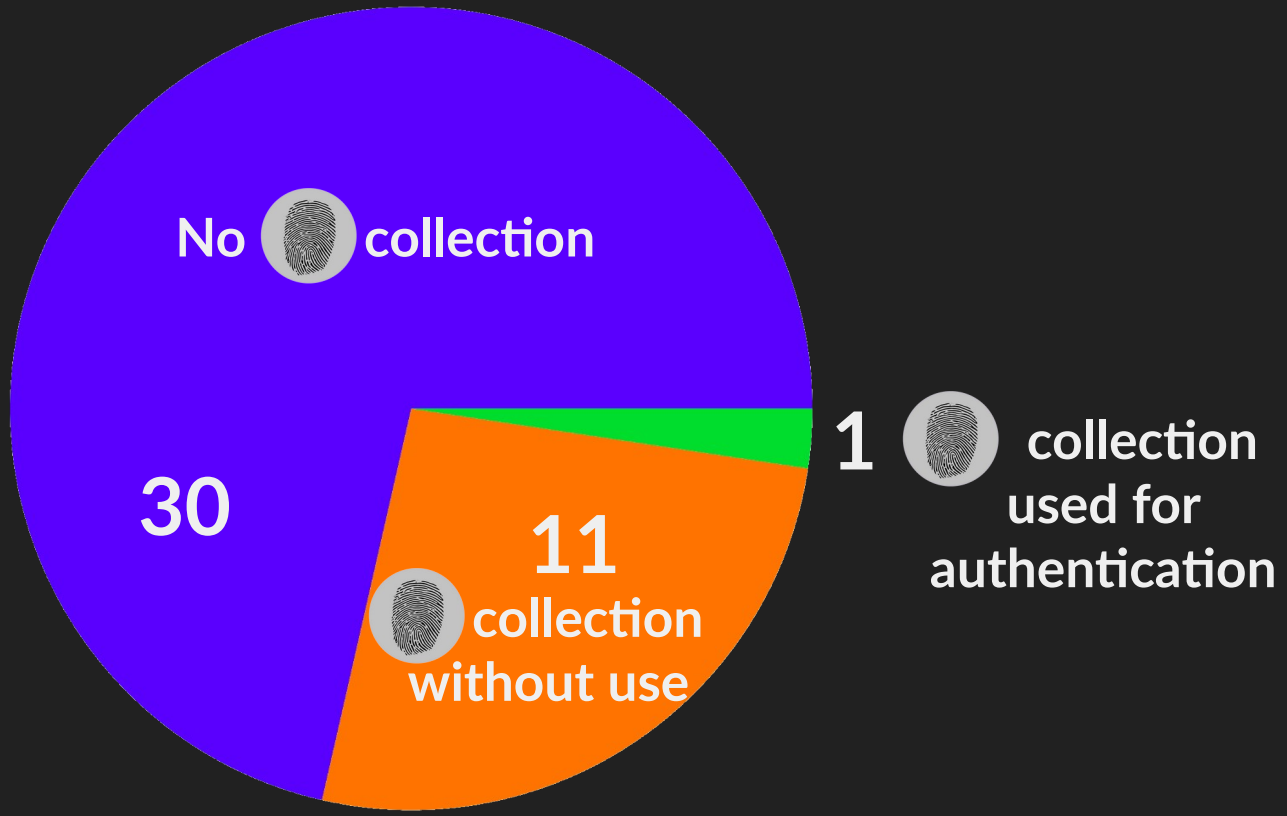
Simulated attacks:

- Stolen password - 42 accounts
- Cookie hijacking - 84 payments

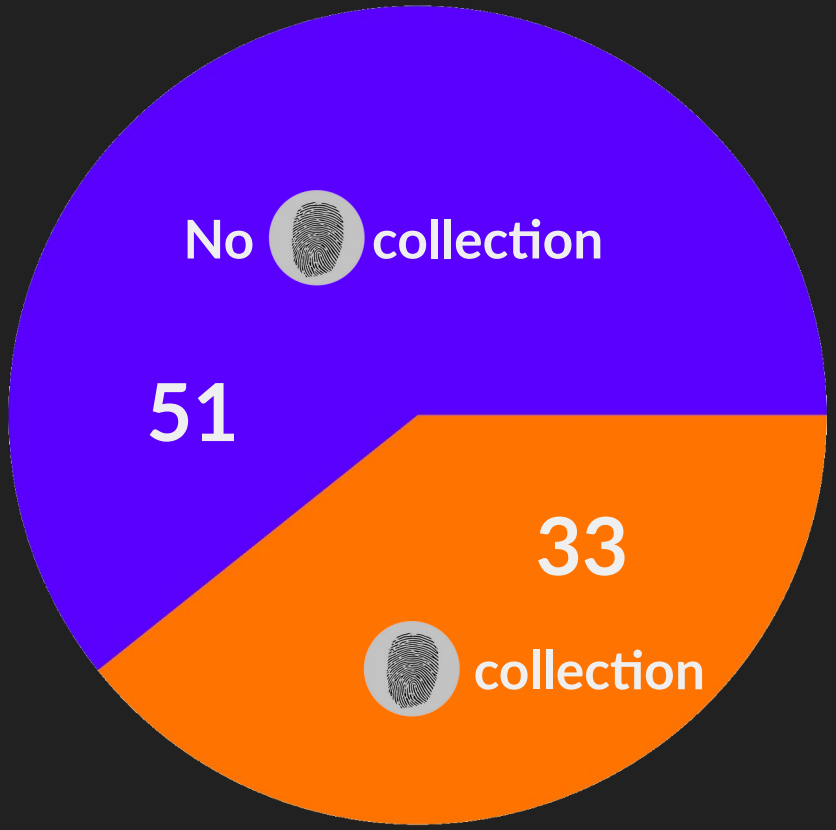
Stolen password evaluation



Stolen password evaluation



Cookie hijacking evaluation



Zero sites use

for cookie protection

Reasons behind low adoption

- Cookie hijacking 

  Modern browsers include more cookies protection

- Stolen password
  - No linking algorithm
  - Fingerprint registration  ?
  - Impact on 

?

Takeaways

Does fingerprinting protect against attacks?

- Manual data collection
- Experimental validation

Fingerprinting is barely used for web authentication

Plan

Introduction

Contributions

I) Study fingerprinting uses for web authentication

II) Design and evaluate a fingerprint linking algorithm

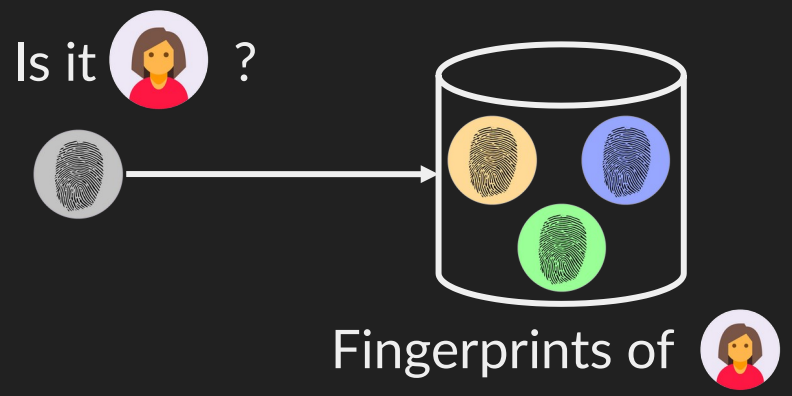
"FP-Controlink: Improving Browser Fingerprint Linking Algorithms through in vitro Analysis", *PETS'22 - under submission*

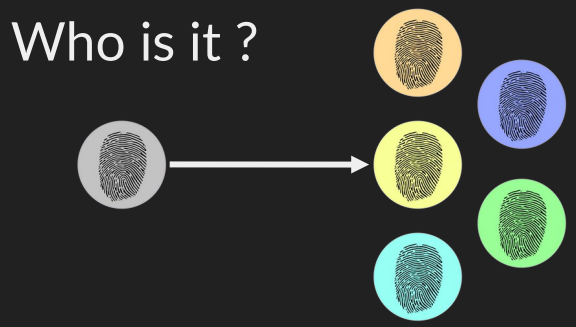
III) Evaluate a web authentication system with fingerprinting

Conclusions & perspectives

Problem statement

Authentication versus Tracking





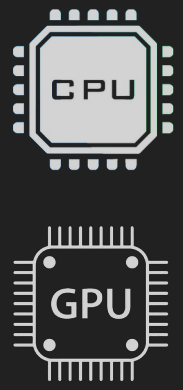
No algorithms for fingerprint-based authentication

Vastel: "*FP-STALKER: tracking browser fingerprint evolutions*", S&P'18
Li: "*Who touched my browser fingerprint?*", IMC'20

Objectives

- Collect fingerprints & understand properties
- Design the algorithm
- Evaluate 2 properties
  - Linking duration
  - Resilience to attackers

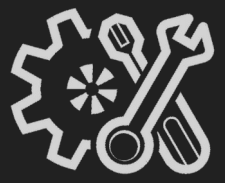
Collection on controlled environment



Hardware

OS

Browser



User configuration

1 160 fingerprints on 4 desktop & 23 mobile devices

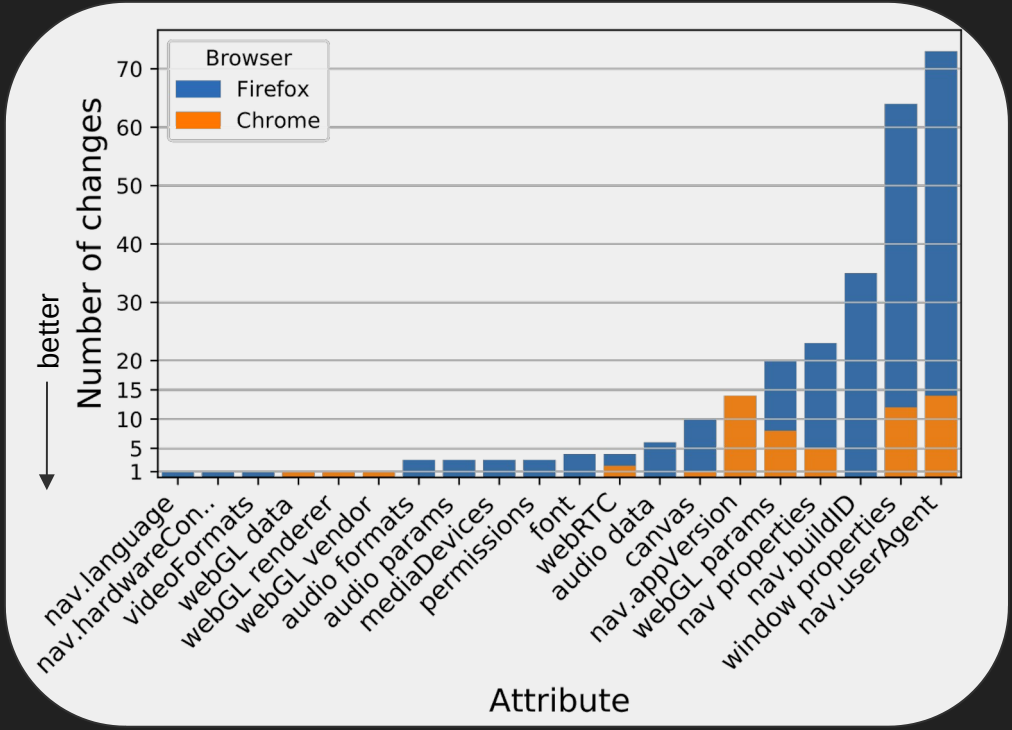
Property evaluation

Uniqueness

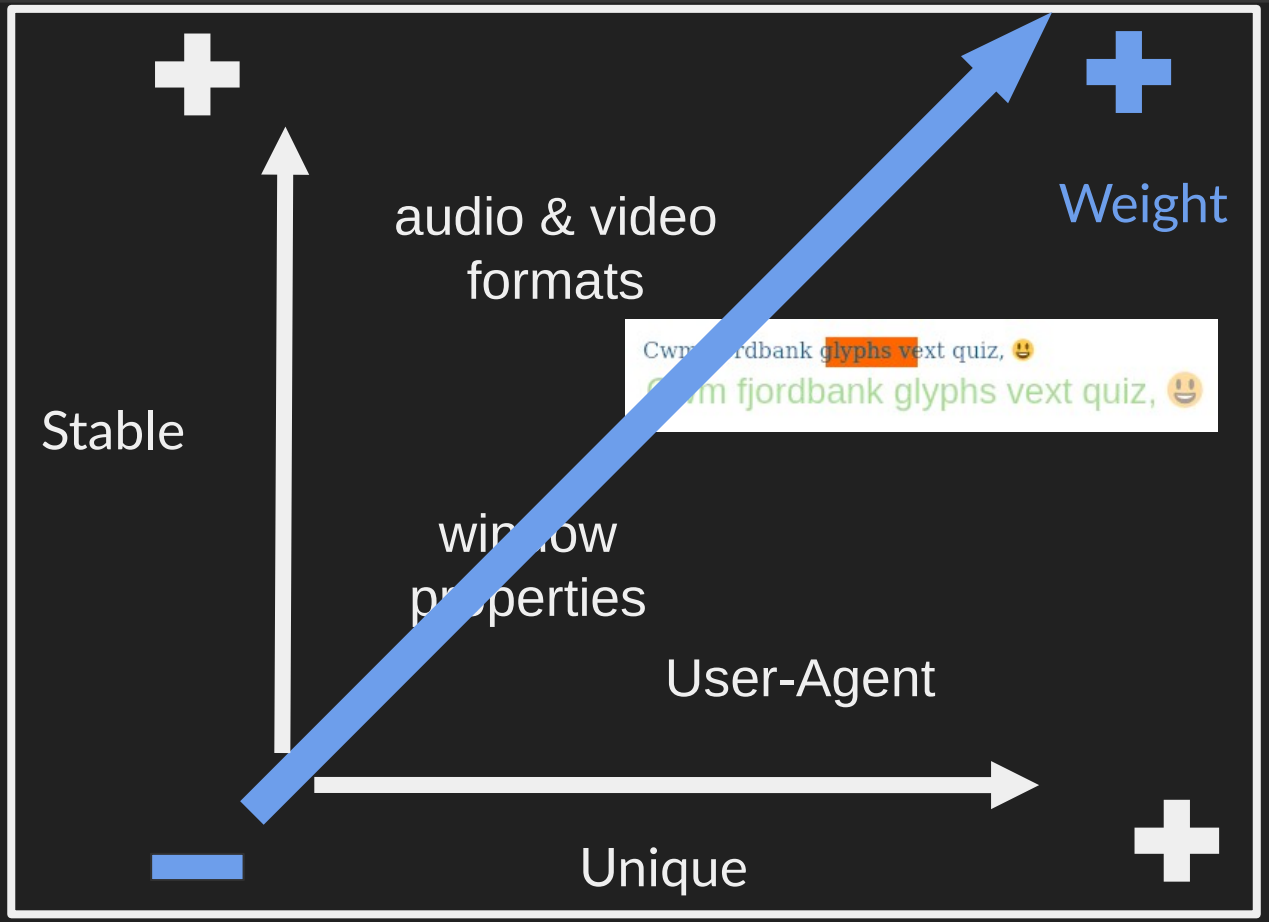
Understand fingerprint differences

Measure attributes entropy

Stability



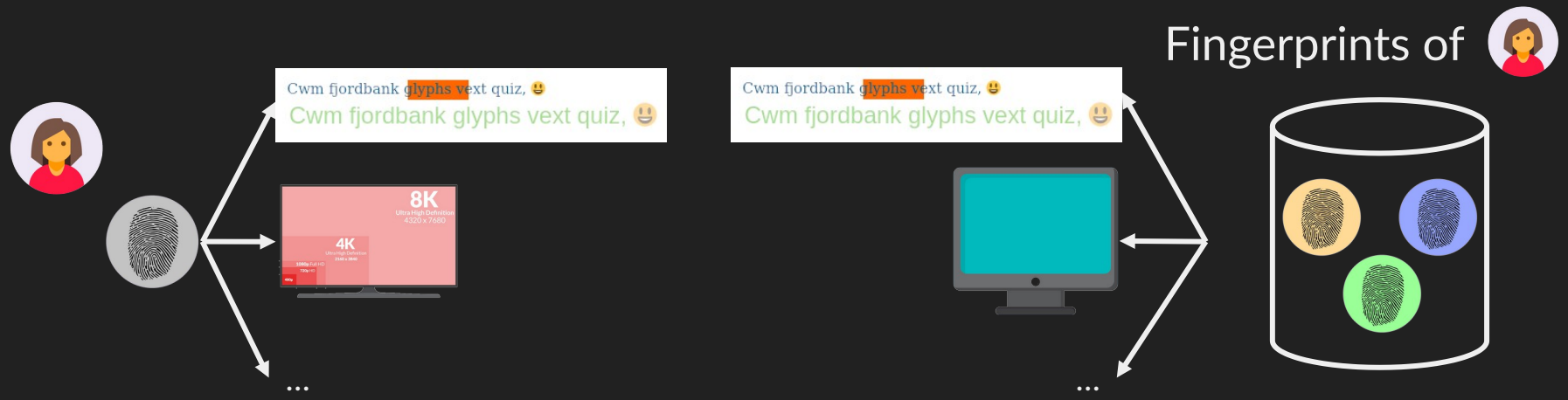
Constraint weights



Define weight constraints

Evaluate different weight variations

Design



Similarity > threshold ⟶ link

Evaluation

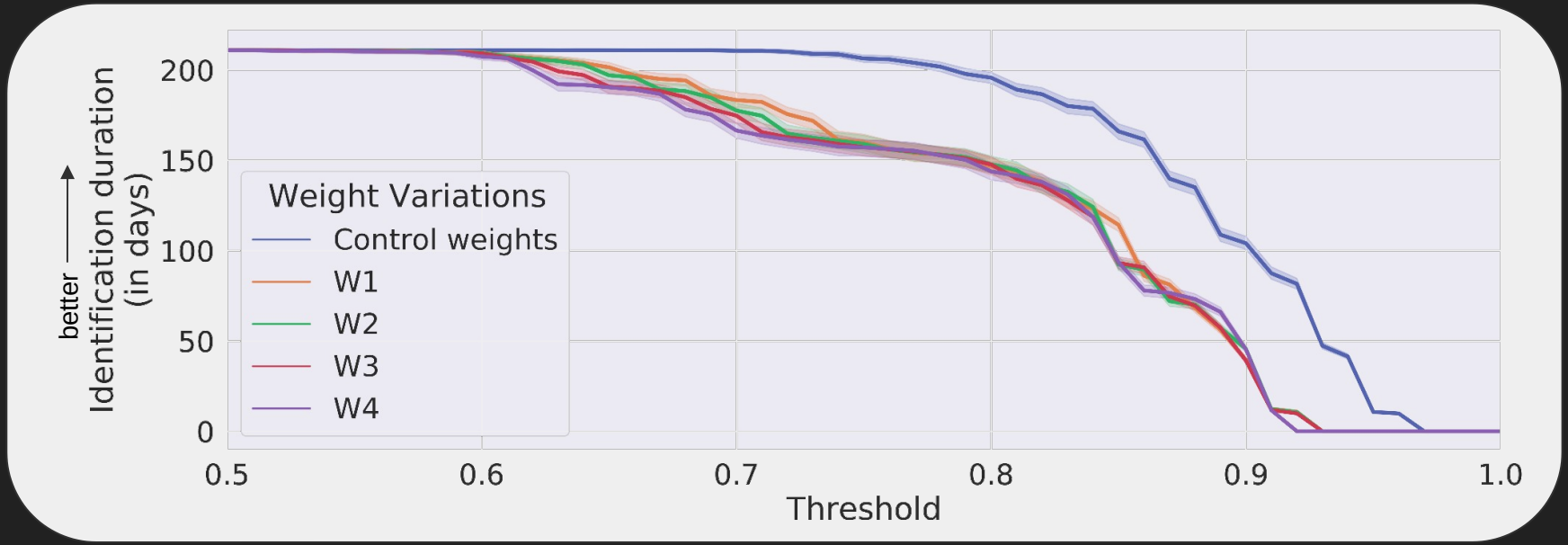
AmIUnique dataset: and extension

- 420K fingerprints
- 728 browser instances
- 7 months

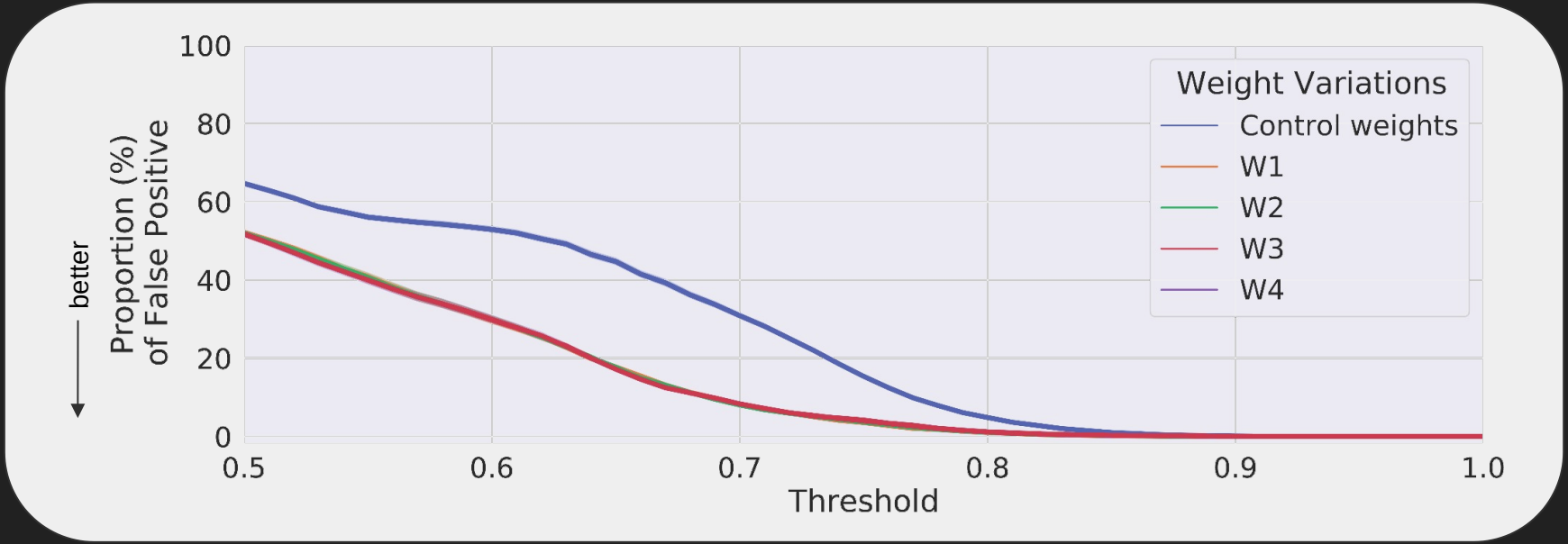
- Linking duration
- Resilience to attackers: proportion of incorrect links

Vary the weights and threshold

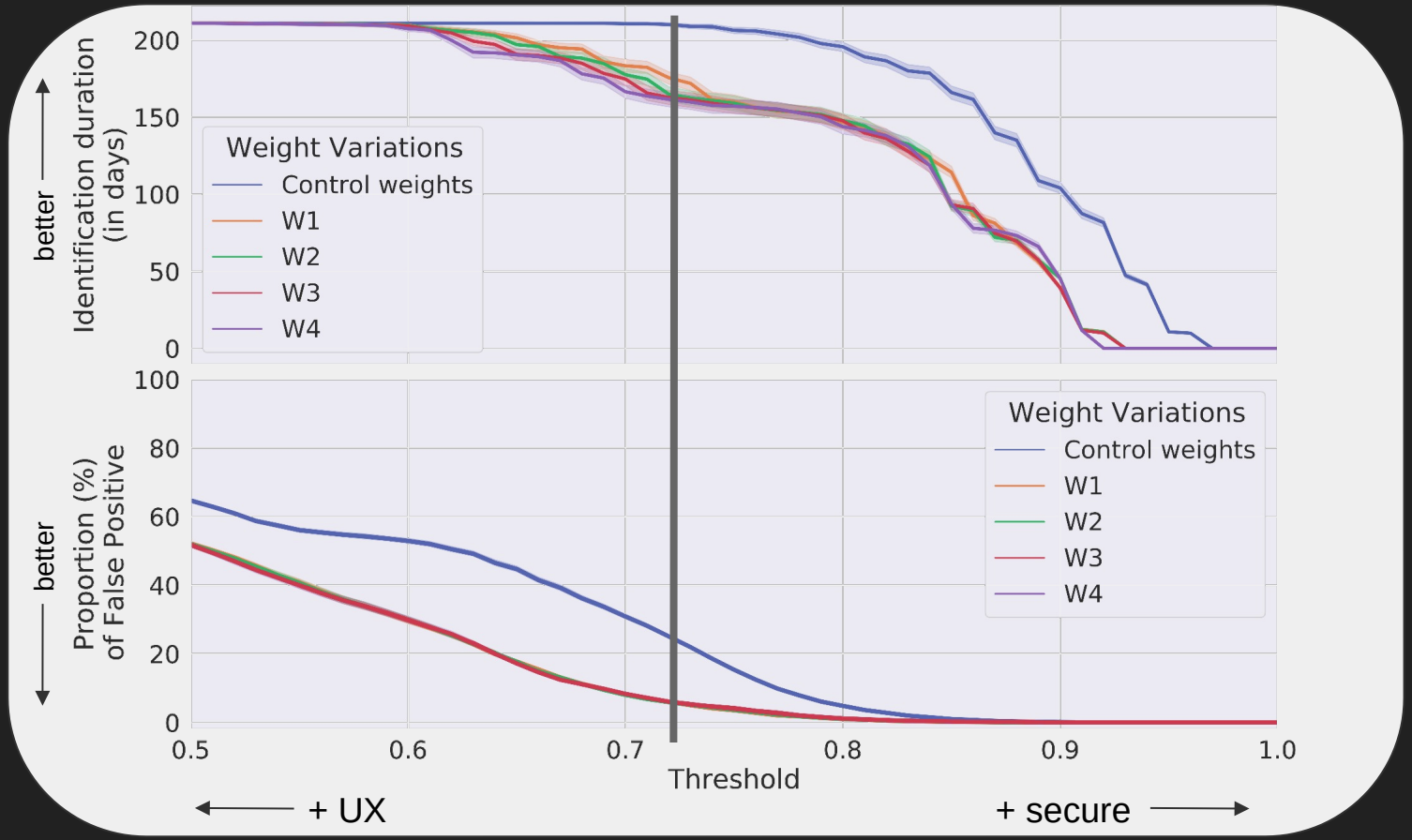
Linking duration evaluation



Resilience evaluation



Reliable and flexible solution



Takeaways

New fingerprint linking algorithm for authentication

- *In vitro* data collection
- Algorithm design
- Experimental validation

Reliable & flexible

Durey: “FP-Controlink: Improving Browser Fingerprint Linking Algorithms through in vitro Analysis”, *PETS’22 - under submission*

Plan

Introduction

Contributions

I) Study fingerprinting uses for web authentication

II) Design and evaluate a fingerprint linking algorithm

III) Evaluate a web authentication system with fingerprinting

Conclusions & perspectives

Remaining obstacles

- Linking algorithm: tackled in 2nd contribution
- Fingerprint registration ?
- Impact on UX ?

Inria's authentication system

Single Sign-On

em@il

Several constraints:

- Easy fingerprint registration
- Minimal UX impact

Implementation

Use of **trusted networks** to register fingerprints

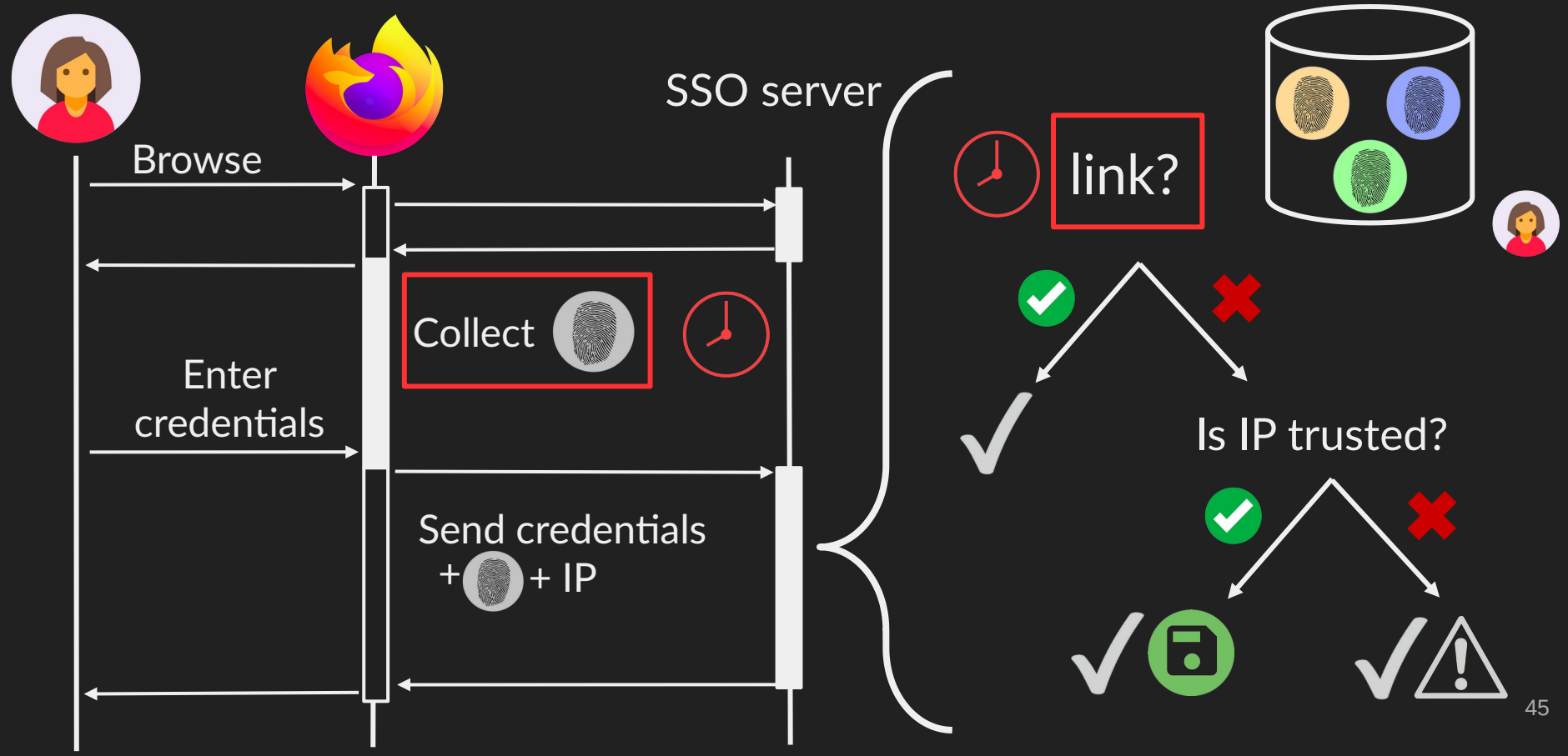
WiFi & ethernet networks + VPN

Inria's Risk-Based model with 2 features

or network feature → low risk

+ password

Authentication flow



Evaluation goals & dataset

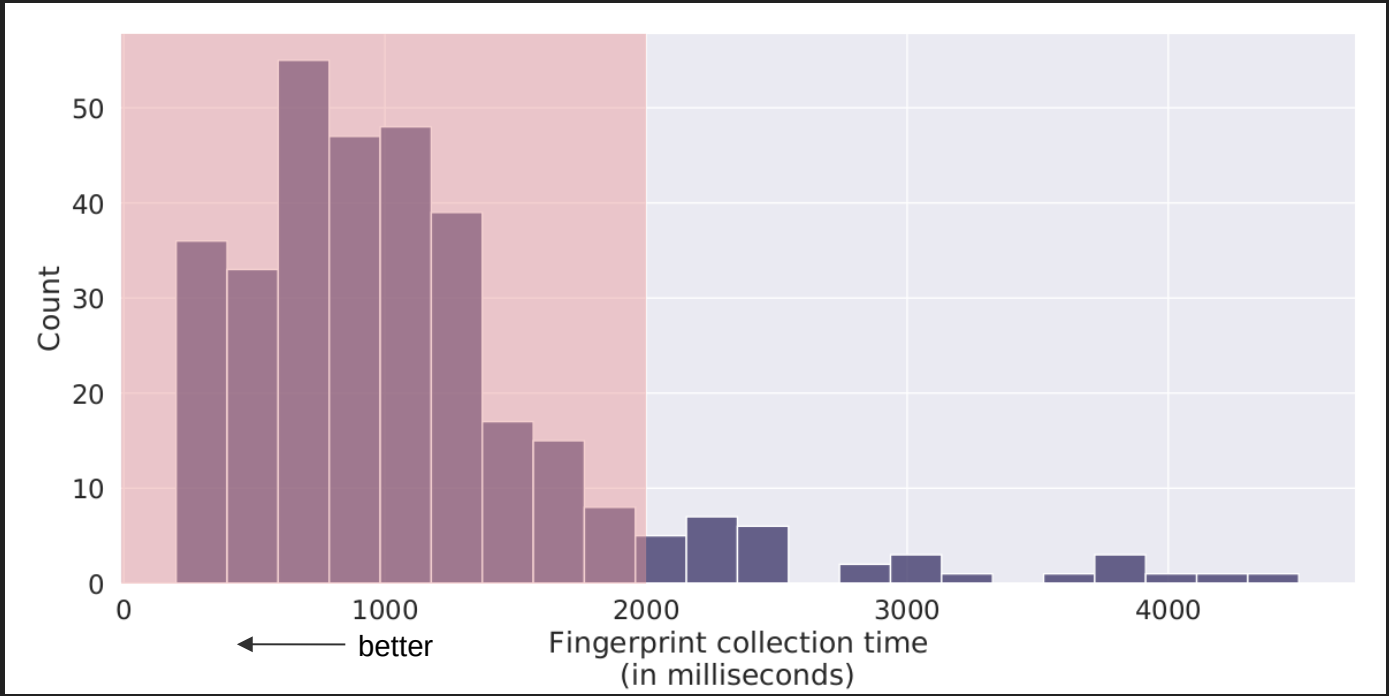
Measure UX impact

- Collection time
- Linking time

Data from test environment:

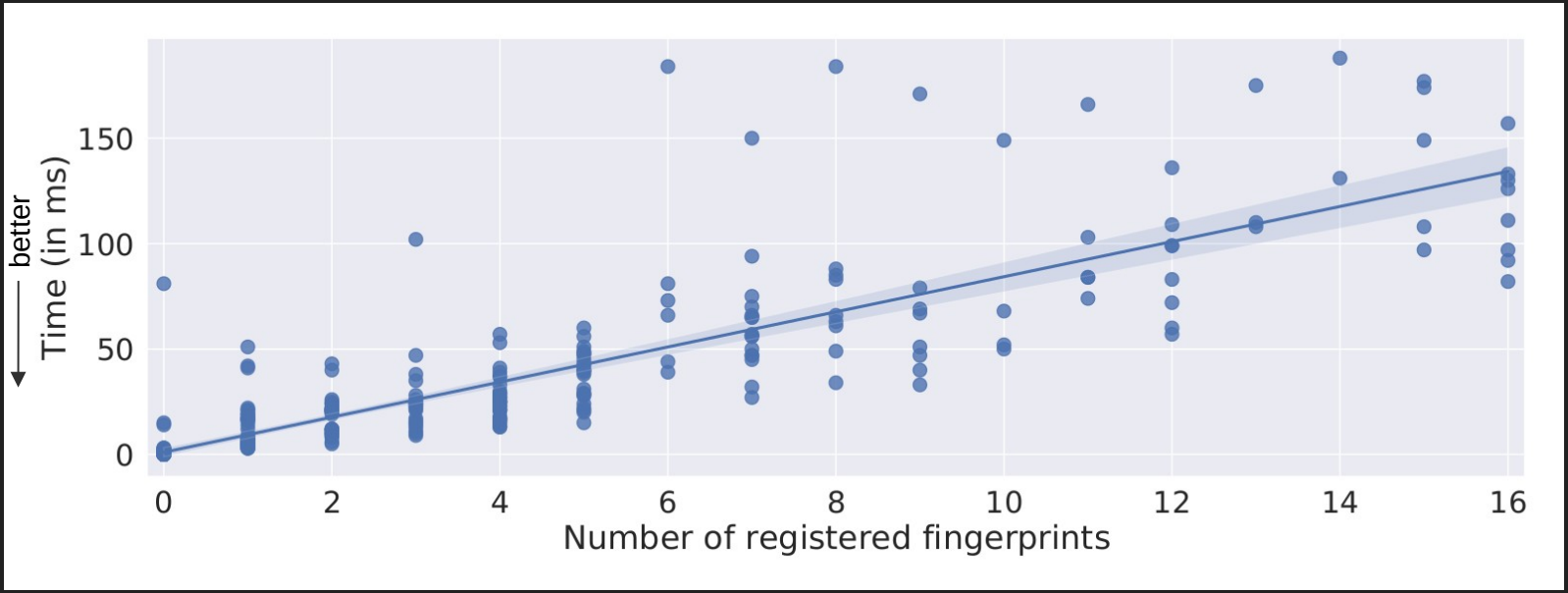
- 82 users
- 331 authentication attempts
- May to September 2021

Collection time



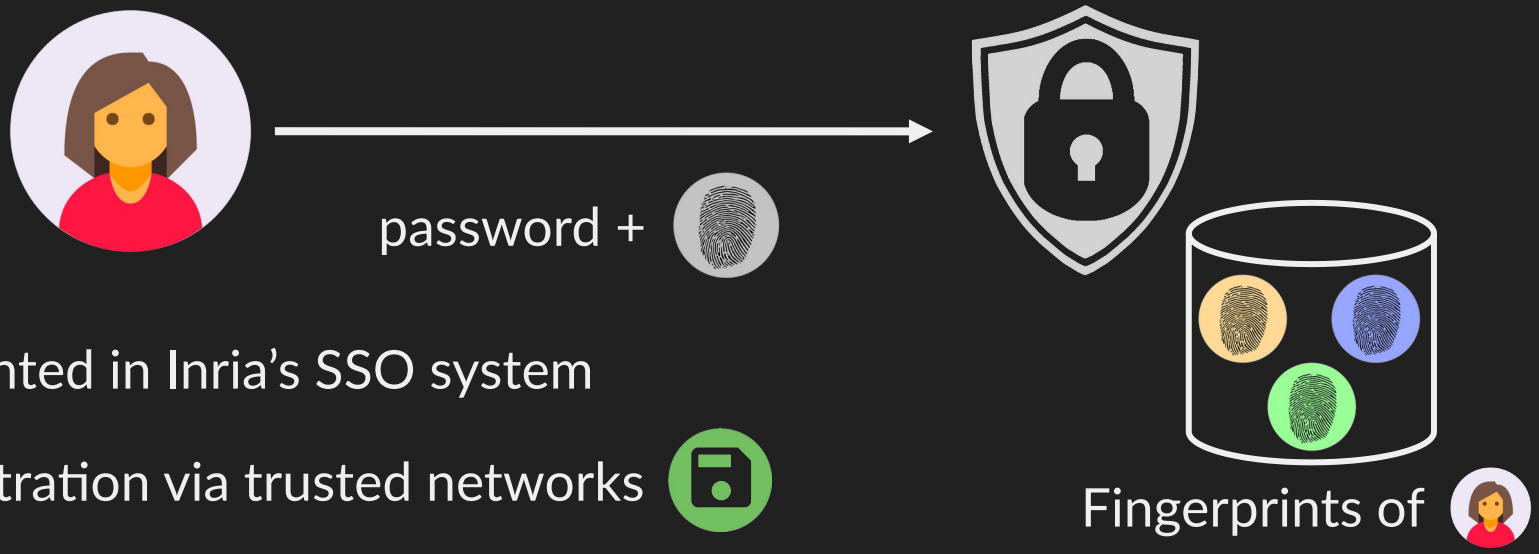
Collection time is acceptable

Linking time



Linking time is acceptable

Takeaways



- Implemented in Inria's SSO system

  registration via trusted networks

- Evaluated on real users

  Impact on UX negligible

Plan

Introduction

Contributions

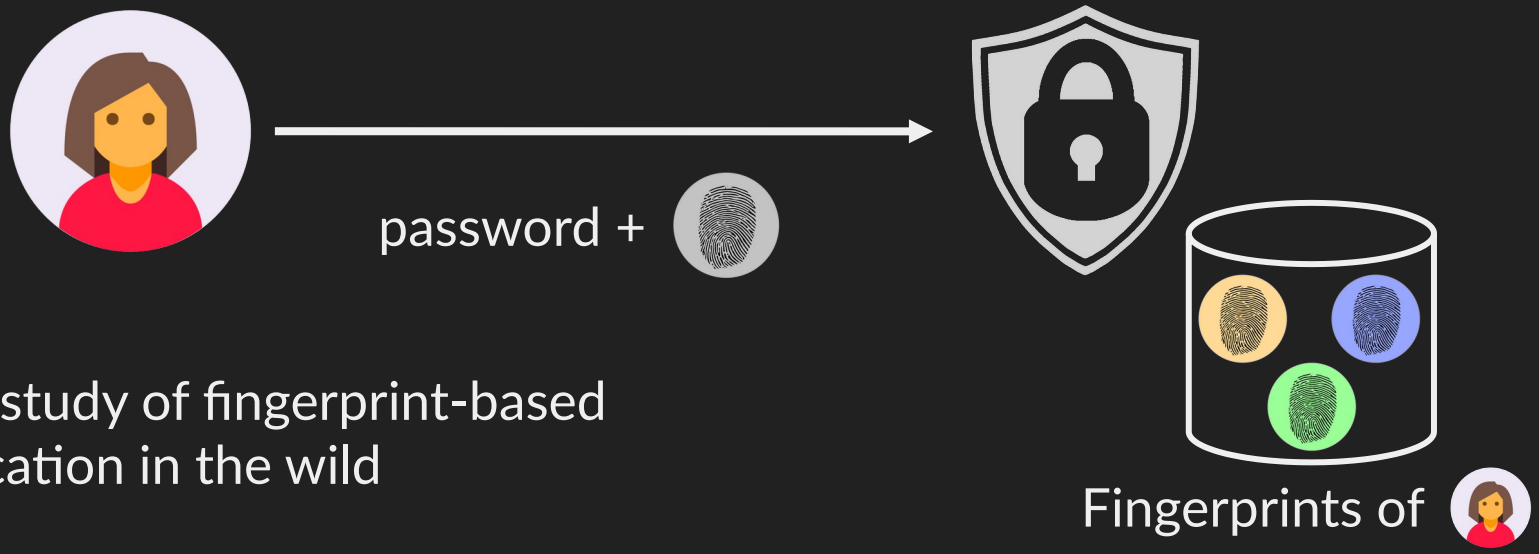
I) Study fingerprinting uses for web authentication

II) Design and evaluate a fingerprint linking algorithm

III) Evaluate a web authentication system with fingerprinting

Conclusions & perspectives

Key contributions



- In-depth study of fingerprint-based authentication in the wild
- Linking algorithm for authentication
- Evaluation in a real system

Authentication system	Security	User experience
Password	✗	~
Multifactor	✓	✗
Existing Risk-based	~	~
Fingerprint-based	✓	✓

Impact of new technologies

- New APIs
  - Network information
  - KeyboardLayout
  - WebVR
- New technologies

WebGPU

Web Assembly

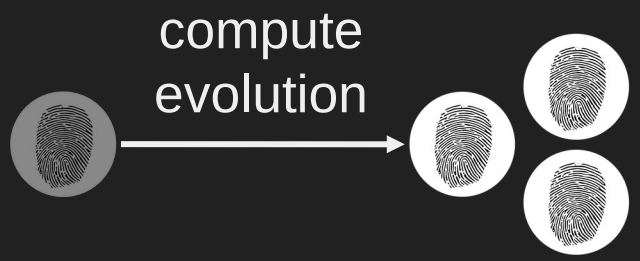
Laor: "*DRAWN APART : A Device Identification Technique based on Remote GPU Fingerprinting*", NDSS'22

Replay attacks targeting fingerprints

- Client-side identity proof

Design dynamic fingerprints

- Limited fingerprint lifetime



- Recover full fingerprint from partial information

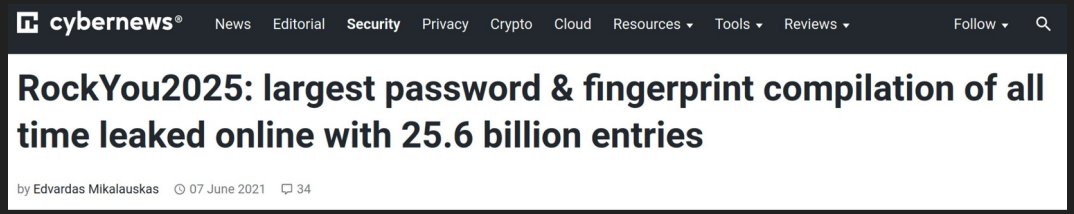
Bursztein: "*Picasso: Lightweight Device Class Fingerprinting for Web Clients*." CCS'16

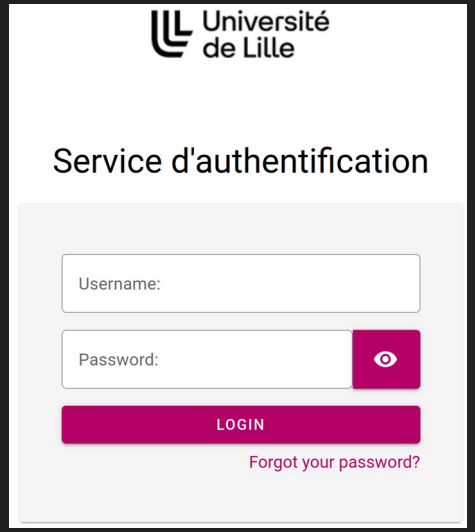
Laperdrix: "*Morellian Analysis for Browsers: Making Web Authentication Stronger With Canvas Fingerprinting.*", DIMVA'19

Fraudulent fingerprint collection

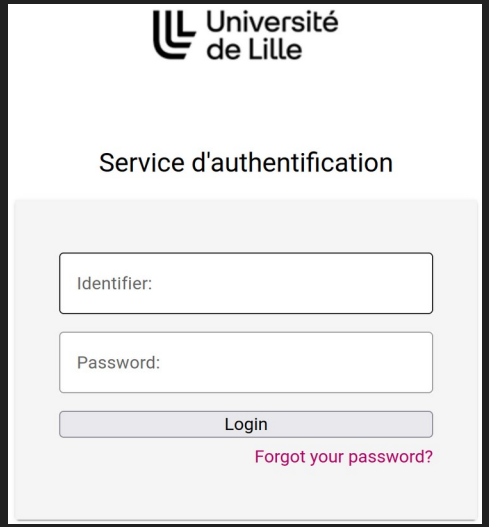
- Password + fingerprint leaks

- Phishing





password +



password +

Leveraging browser fingerprinting to strengthen Web authentication

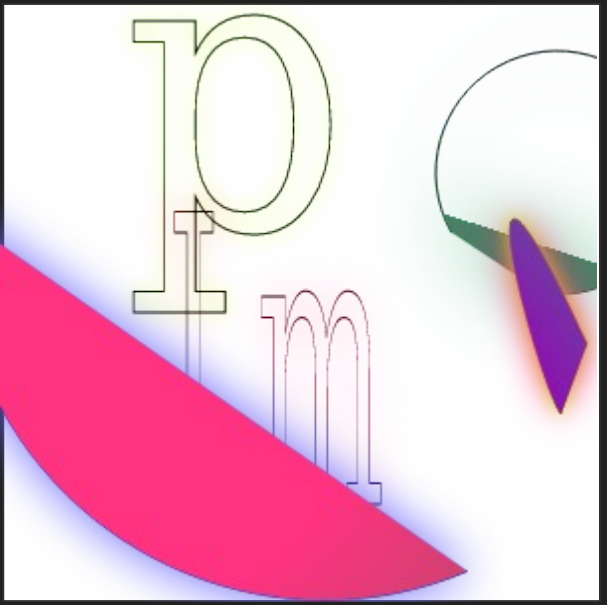
"FP-Redemption: Studying Browser Fingerprinting Adoption for the Sake of Web Security", *DIMVA'21*

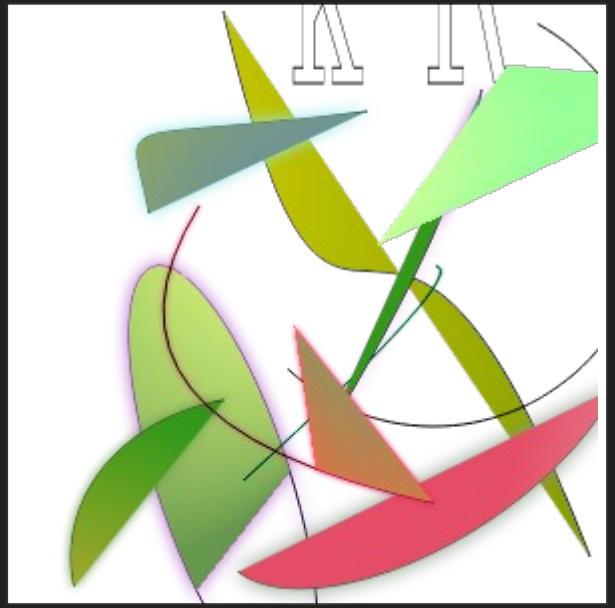
"DRAWN APART : A Device Identification Technique based on Remote GPU Fingerprinting", *NDSS'22*

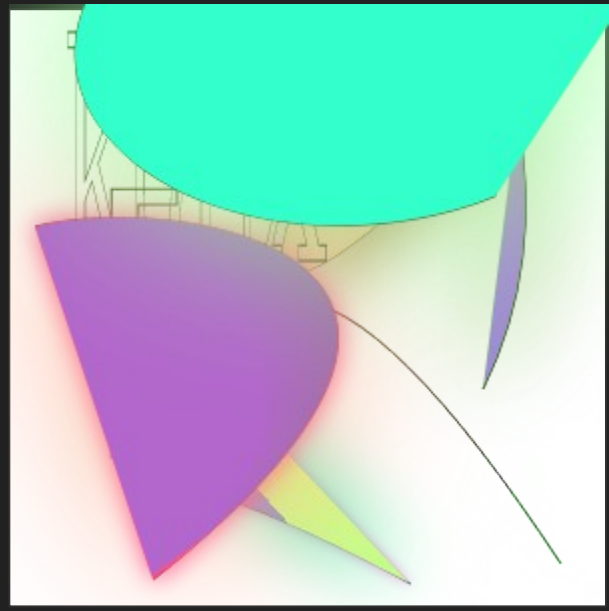
"The Price to Play: a Privacy Analysis of Free and Paid Games in the Android Ecosystem", *WWW'22*

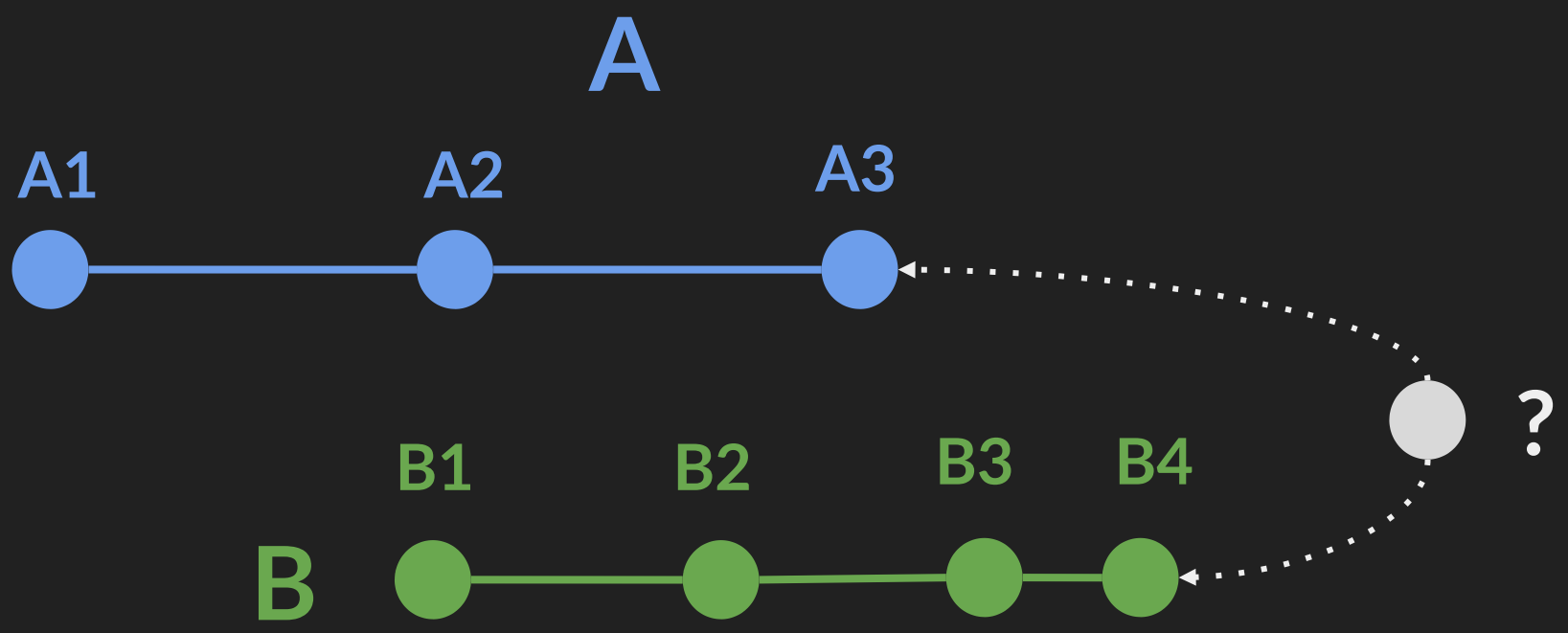
"FP-Controlink: Improving Browser Fingerprint Linking Algorithms through in vitro Analysis", *PETS'22 - under submission*

https://gitlab.com/adurey








A
A1
A2
A3
?
B1
B2
B3
B4
B