Browser fingerprinting for web authentication, a large-scale empirical analysis

Nampoina Andriamilanto - Doctorant 2è année

RESSI - 19/05/2019

Gaëtan Le Guelvouit - Équipe C&S, IRT b<>com (Rennes)
Tristan Allard - Équipe DRUID, Univ Rennes, CNRS, IRISA

Prise d'empreinte de navigateur

Prise d'empreinte de navigateur : collecte d'attributs, appelés **vecteurs**, via un **navigateur web**.

Vecteurs : dépendent de l'**environnement web** (composants matériels et logiciels).

Empreinte de navigateur : aggrégat des valeurs des vecteurs.

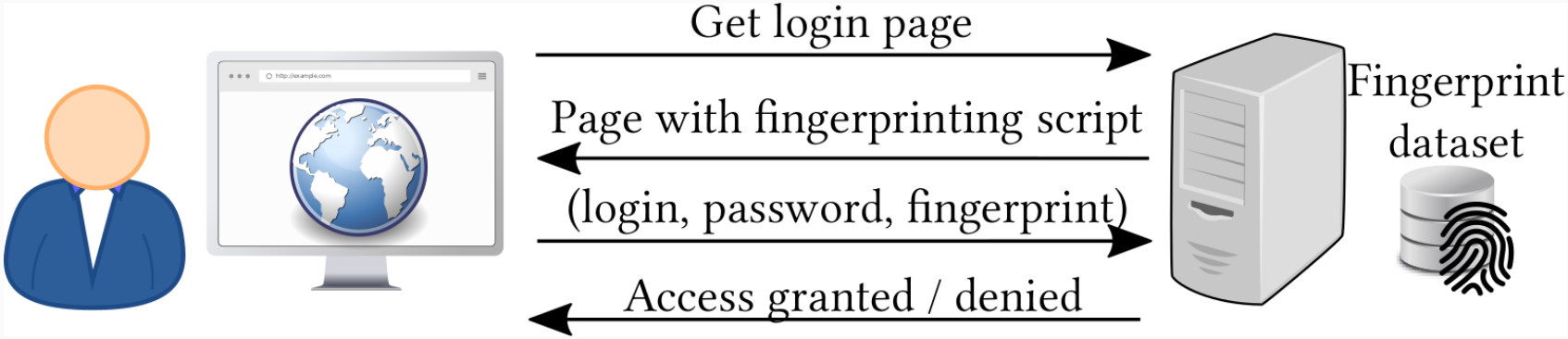

Figure 1 – Schéma du mécanisme d'authentification

Propriétés de facteur d'authentification

- Sécurité : distinguabilité et stabilité des empreintes
- Utilisabilité : accessibilité du facteur d'authentification [4, 3, 1]
- Déployabilité : consommation de ressources

Notation

F : Domaine des empreintes

Soit une sonde composée de n vecteurs, avec V_x le domaine du vecteur x.

$$F = \{(v_1, ..., v_n) \mid v_x \in V_x\} \tag{1}$$

$\mathcal{D}$: Jeu de données d'empreintes

Triplet : empreinte, navigateur dans B, moment de la collecte dans T

$$\mathcal{D} = \{(f, b, t) \mid f \in F, b \in B, t \in T\} \tag{2}$$

Sécurité

Distinguabilité : deux navigateurs différents peuvent être distingués.

$\mathcal{B}(f, \mathcal{D})$: les navigateurs partageant l'empreinte f dans $\mathcal{D}$.

$$\mathcal{B}(f, \mathcal{D}) = \{b \in B \mid (g, b, t) \in \mathcal{D}, f = g\} \tag{3}$$

$\mathcal{A}(\epsilon, \mathcal{D})$: les empreintes de $\mathcal{D}$ présents dans un ensemble d'anonymat de taille ϵ.

$$\mathcal{A}(\epsilon, \mathcal{D}) = \{f \in F \mid \mathrm{card}(\mathcal{B}(f, \mathcal{D})) = \epsilon\} \tag{4}$$

Sécurité

Stabilité : un même navigateur peut être reconnu au fil du temps.

$\mathcal{C}(\Delta, \mathcal{D})$: les empreintes consécutives d'un même navigateur, observées après une fenêtre de temps comprise dans Δ.

$$\mathcal{C}(\Delta, \mathcal{D}) = \{(f_i, f_p) \mid ((f_i, b_j, t_k), (f_p, b_q, t_r)) \in \mathcal{D}^2, \\ b_j = b_q, t_k < t_r, (t_r - t_k) \in \Delta\} \tag{5}$$

$\mathrm{sim}(f, g)$: part de vecteurs à valeur identique, avec $f[x]$ la valeur du vecteur x de f.

$$\mathrm{sim}(f, g) = \frac{1}{n} \cdot \sum_{x=1}^{n} \mathrm{eq}(f[x], g[x]) \tag{6}$$

Jeu de données

Grand jeu de données utilisé

- Deux pages d'un site français populaire
- 3 578 197 empreintes distinctes, 1 989 366 navigateurs
- 6 mois (07/12/2016 - 07/06/2017)
- 216 vecteurs (et 46 extraits)

Distinguabilité

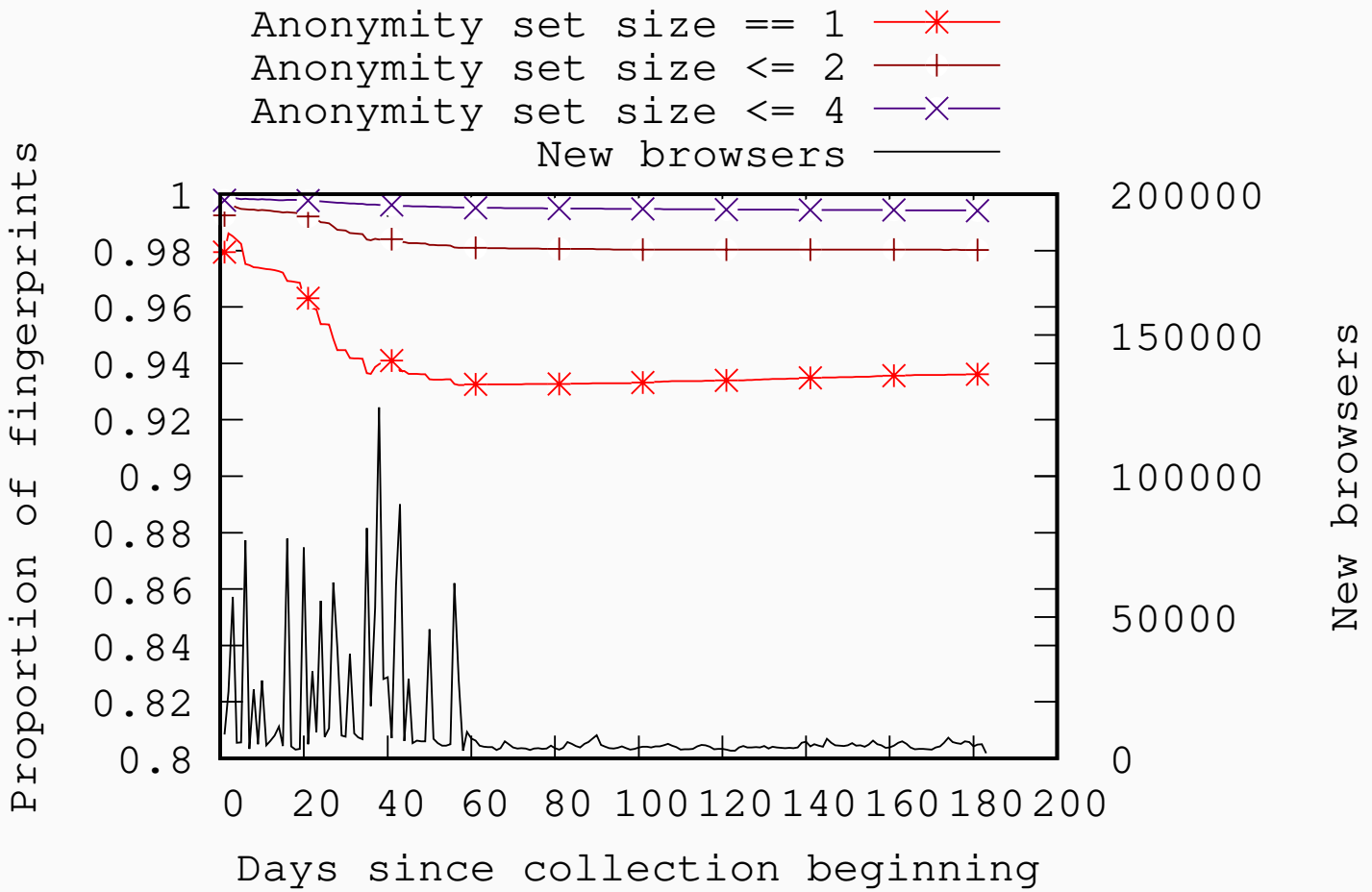

Figure 2 – Taille des ensembles d'anonymat selon un partitionnement temporel ne considérant que la dernière empreinte de chaque navigateur

Distinguabilité ordinateurs / ordiphones

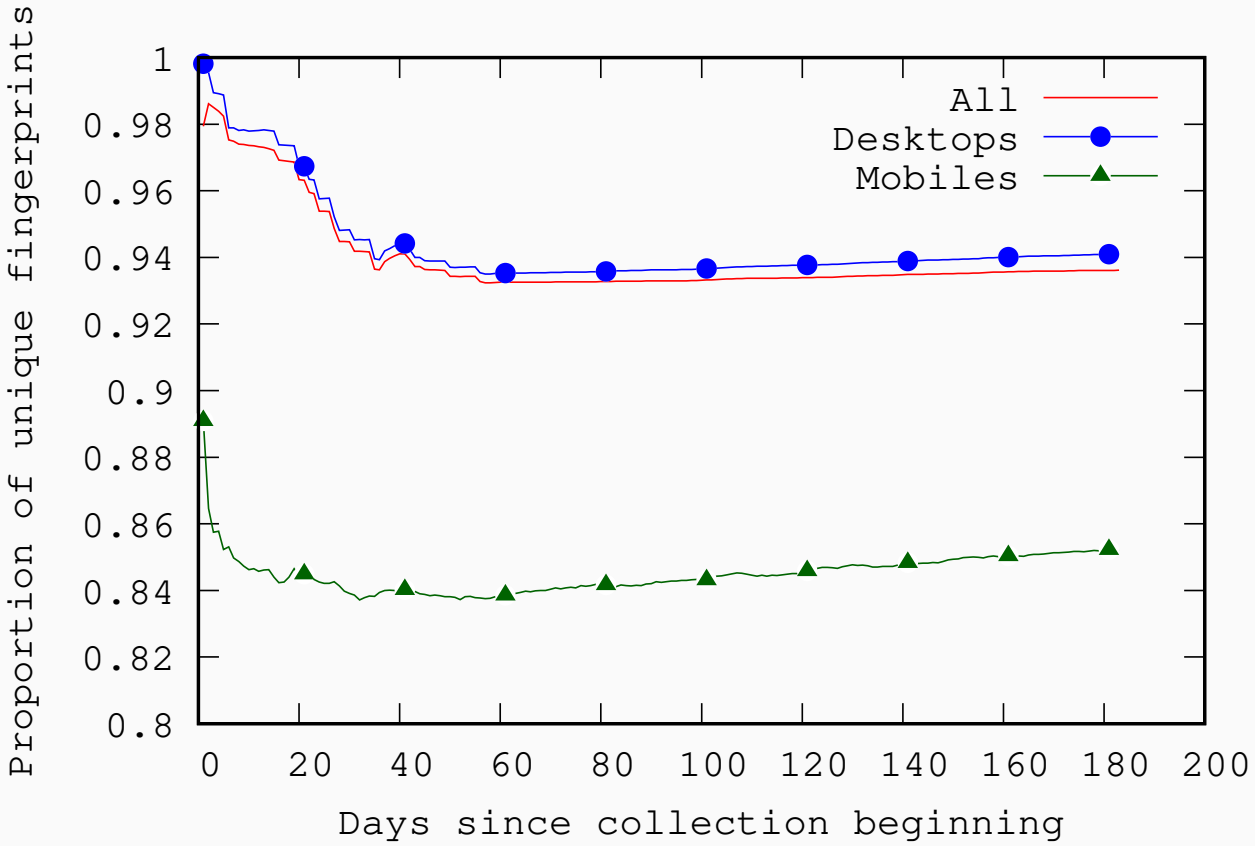

Figure 3 – Proportion d'empreintes uniques, selon un partitionnement temporel ne considérant que la dernière empreinte de chaque navigateur, en fonction du type d'appareil

Stabilité ordinateurs / ordiphones

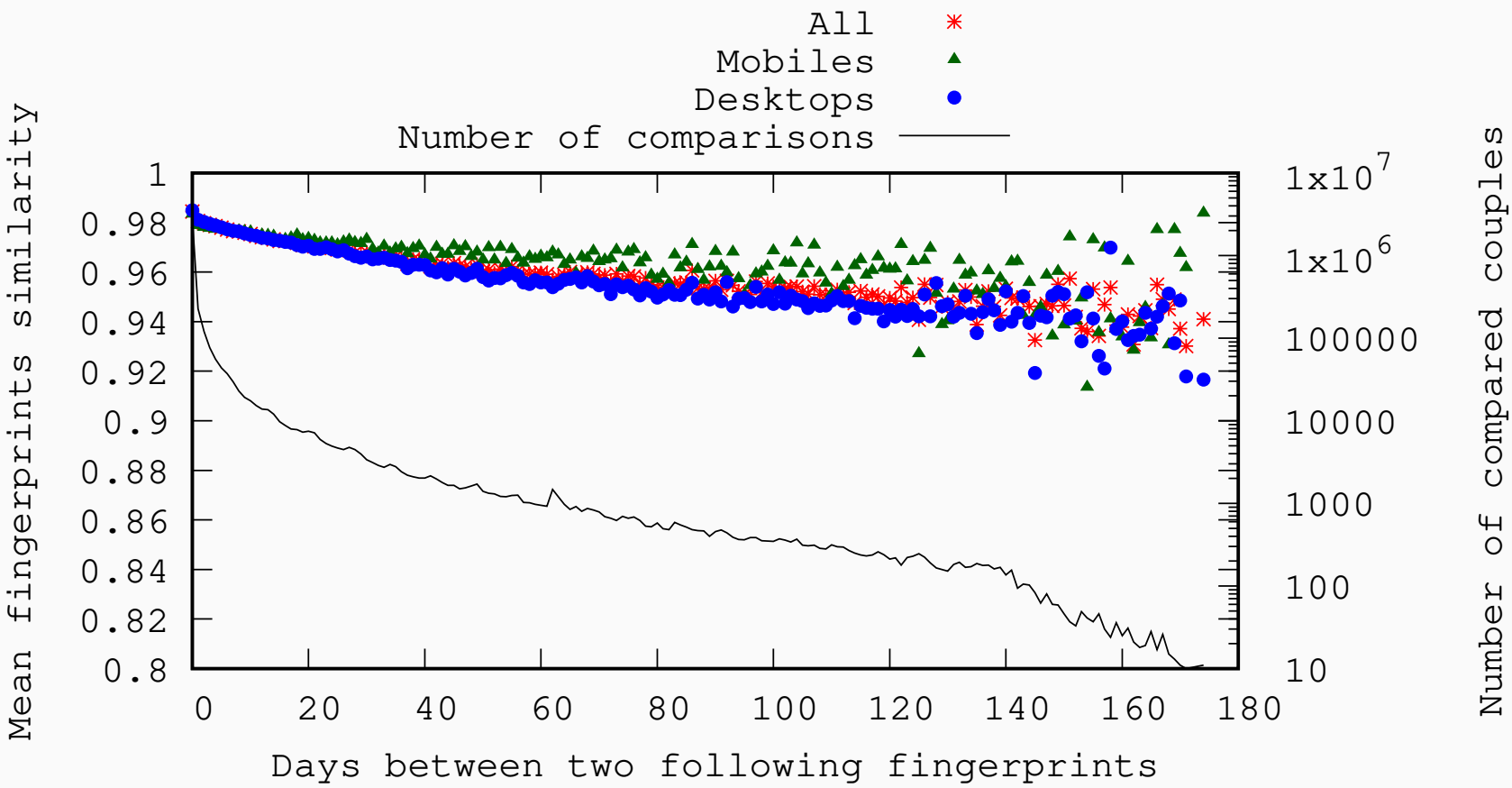

Figure 4 – Stabilité en fonction du temps passé entre deux empreintes appartenant à un même navigateur selon le type d'appareil

Attaques sur notre mécanisme

Forge : présentation d'une empreinte forgée

- Différentes stratégies et connaissances possibles

Rejeu : présentation d'une empreinte complète volée

- Proposition de défi-réponse [2]

Relais : proche d'un Homme-du-Milieu

- Se sert d'autres techniques, les contre-mesures aussi

Merci pour votre attention.

Présent à la session poster, n'hésitez pas à passer ! :-)

Bibliographie

Bibliographie i

Gómez-Boix, A., Laperdrix, P., and Baudry, B.
Hiding in the Crowd : an Analysis of the Effectiveness of Browser Fingerprinting at Large Scale.
In *The Web Conference* (2018).

Laperdrix, P.
***Browser Fingerprinting : Exploring Device Diversity to Augment Authentication and Build Client-Side Countermeasures*.**
PhD thesis, INSA Rennes, 2017.

Bibliographie ii

Laperdrix, P., Rudametkin, W., and Baudry, B.
Beauty and the Beast : Diverting modern web browsers to build unique browser fingerprints.
In *37th IEEE Symposium on Security and Privacy* (2016).

Spooren, J., Preuveneers, D., and Joosen, W.
Mobile Device Fingerprinting Considered Harmful for Risk-based Authentication.
In *Proceedings of the Eighth European Workshop on System Security* (2015).