AD FINGERPRINTING: CONCEPT, VIABILITY AND SOLUTIONS

Miguel A Bermejo-Agueda[1], Patricia Callejo[12], Rubén Cuevas[12], Angel Cuevas[12]

[1] Universidad Carlos III de Madrid, Leganés, Spain
[2] UC3M-Santander Big Data Institute, Getafe, Spain

Acknowledgements: This study has been supported by Plan de Recuperación, Transformación y Resiliencia - Financiado por laUnión Europea – NextGenerationEU.

Abstract

adF is a novel approach of web fingerprinting where devices are identifying via code embedded in ads. We deployed our adF system in multiple campaigns, yielding 2,78M ad impressions, enabling vulnerability assessments of mobile devices. Results show approximately 47% of mobile devices uniquely fingerprinted by adF. Notably, ad fingerprinting resilience varies widely across browsers and devices, with Android being most vulnerable configuration.

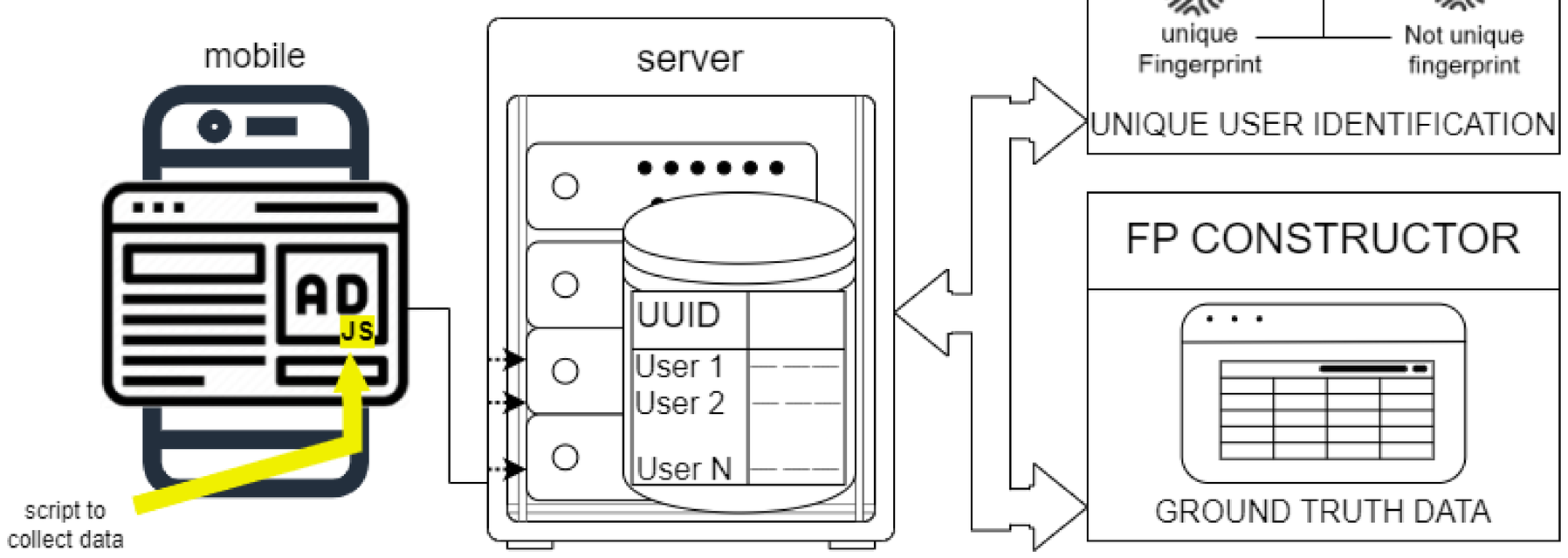
ShieldF, a simple solution, counters ad fingerprinting by blocking browser-reported attributes with significant discrimination power. It outperforms major browser-based anti-fingerprinting solutions, boosting resilience against ad fingerprinting by up to 55% for some devices. Available as a Chromium add-on, ShieldF is developer-friendly, promising enhanced protection across browsers and mobile apps.

Motivation

adF assesses the feasibility of ad fingerprinting in the current context, considering the imminent obsolescence of cookies and increasing restrictions on device identifiers. Our primary objective is to evaluate whether ad fingerprinting can serve as a viable means to uniquely identify devices through online advertisements, while addressing current challenges and future prospects in terms of privacy and regulation.

adF system

DEVICE FINGERPRINT	Device's fingerprint obtained from the Fingerprint Constructor.
DEVICE ADVERTISING ID	Device's advertising id obtained from the DSP.
ATTRIBUTES	List of attributes collected by the embedded script.
GROUND TRUTH UNIQUENESS	Binary variable indicating if the Advertising ID is unique in our dataset. It provides ground-truth information regarding the uniqueness of the device.
MESURABLE UNIQUENESS	Binary variable indicating if the adF system identifies the fingerprint as unique or not. This variable reports the result of the model used by the Fingerprint Classifier. (*)The classifier is trained using the ground truth uniqueness variable



An embedded script within an ad allows to collect numerous attributes from the device (browser version, OS, device type, fonts, screen size, graphics card...).

Removed samples without an associated advertising ID and with a fingerprint that appears only once.

If a sufficient number of attributes with enough discrimination power are collected, the fingerprint may become unique even within a large pool of devices.

High value for advertisers once cookies are fully deprecated.

Vulnerability of devices to adF

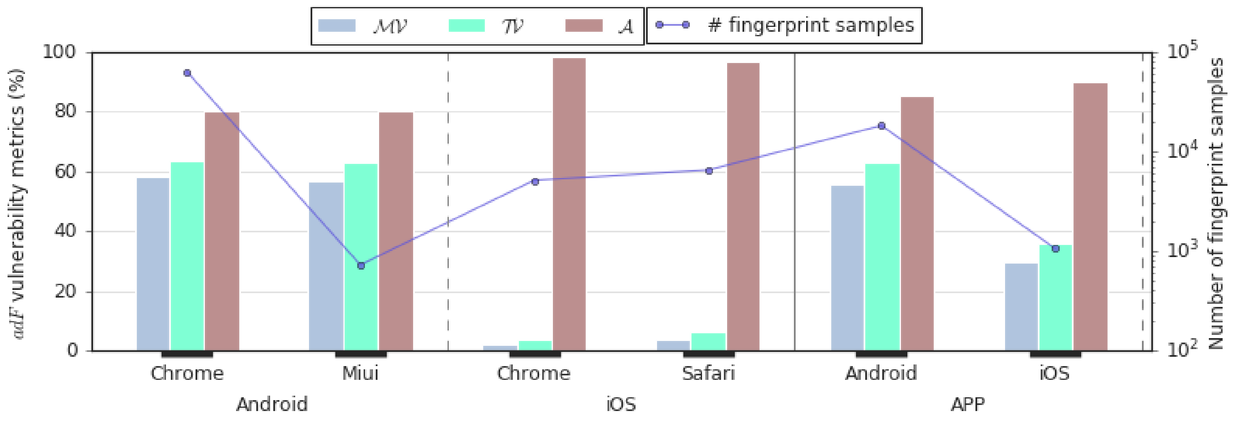
Extrapolated the results to current market share (as of August 2023):

- **At least 47% of mobile devices are vulnerable through mobile apps, and 40% through mobile browsers.**

Reasons behind vulnerability:

1. Number of reported attributes.
2. Cardinality: attribute value count, |S|.
3. Entropy: frequency of attribute values, |Hn|.

} Discrimination power



THEORETICAL VULNERABILITY $\mathcal{TV} = \frac{N_{tf}}{N_f}$

MEASURABLE VULNERABILITY $\mathcal{MV} = \frac{N_{mf}}{N_f}$

N_f : total number of fingerprints

N_{tf} : total number of fingerprints with ground-truth uniqueness equal to 1

N_{mf} : total number of fingerprints with measurable uniqueness equal to 1

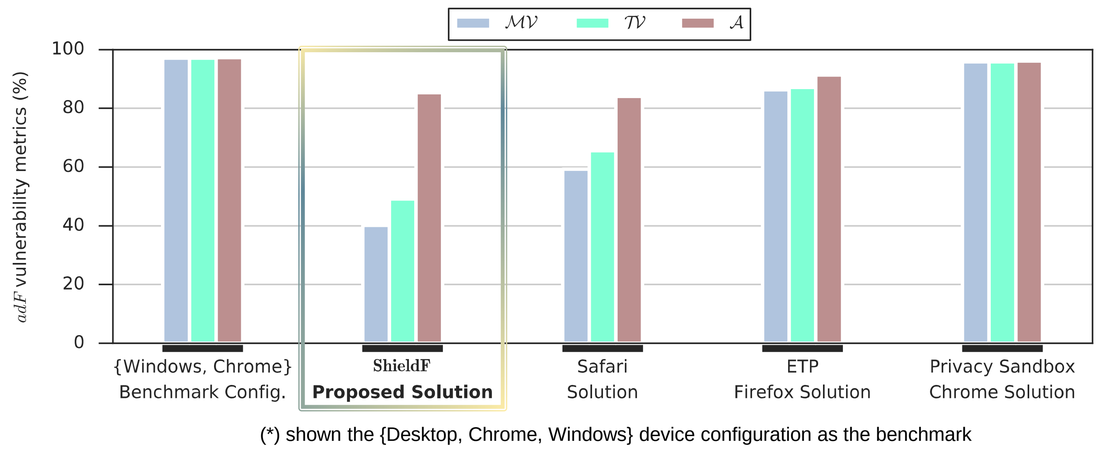
We also measure the accuracy of the adF system, $\mathcal{A}$

ShieldF: countering adF

ShieldF may substantially improve resilience against ad fingerprinting by easy-to-adopt solution blocking attributes with the largest discrimination power, **reducing vulnerability of devices by up to 55%.**

ShieldF is based on a simple heuristic selection of attributes:

- High discrimination power. { |S| > 25 ; |Hn| > 0,1 }
- Don't affect the user experience.



(*) shown the {Desktop, Chrome, Windows} device configuration as the benchmark

SCAN ME

ShieldF is available as an extension for any Chromium-based browser (Chrome, Edge, Opera), offering widespread adoption and enhanced protection against ad and other forms of fingerprinting.