Extending Browser Extension Fingerprinting to Mobile Devices

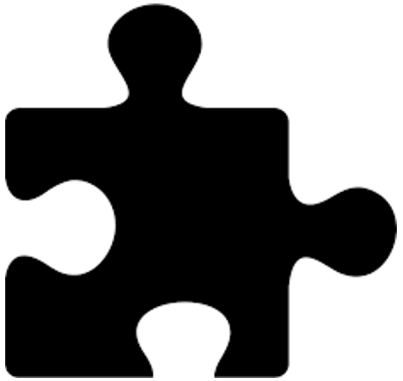
Brian Hyeongseok Kim, Shujaat Mirza, Christina Pöpper

WPES ’23: November 26, 2023

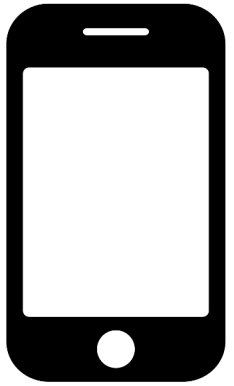
Introduction

Browser Fingerprinting

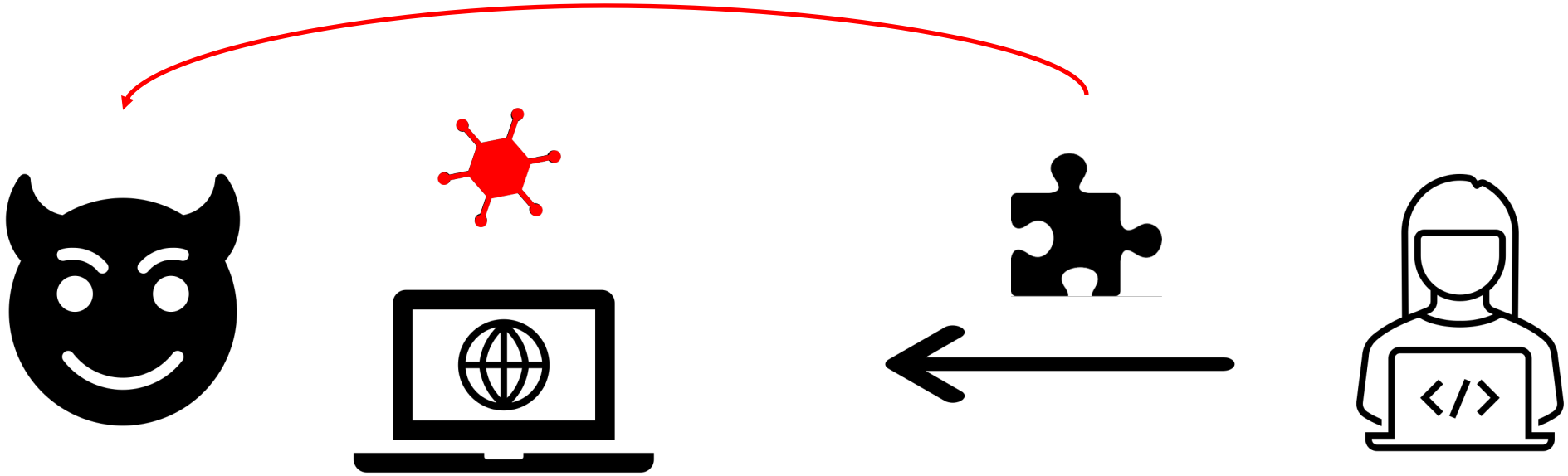
Extension Fingerprinting



Mobile Devices



Attacker Model



Malicious Webpage with Attack Script

Victim Access Webpage with Extensions

Assumptions

- Extensions have access to modify elements on the webpage
- A simple page visit launches the attack

Behavioral Techniques

Document Object Model (DOM)[1]

Dynamic honey pages

- Create DOM elements queried by extensions
- Monitor their modifications

For our attacker model

- No dynamic insertion of DOM elements
  → monitor any modifications to our static page

Cascading Style Sheet (CSS)[2]

Identify triggering HTML elements to be styled

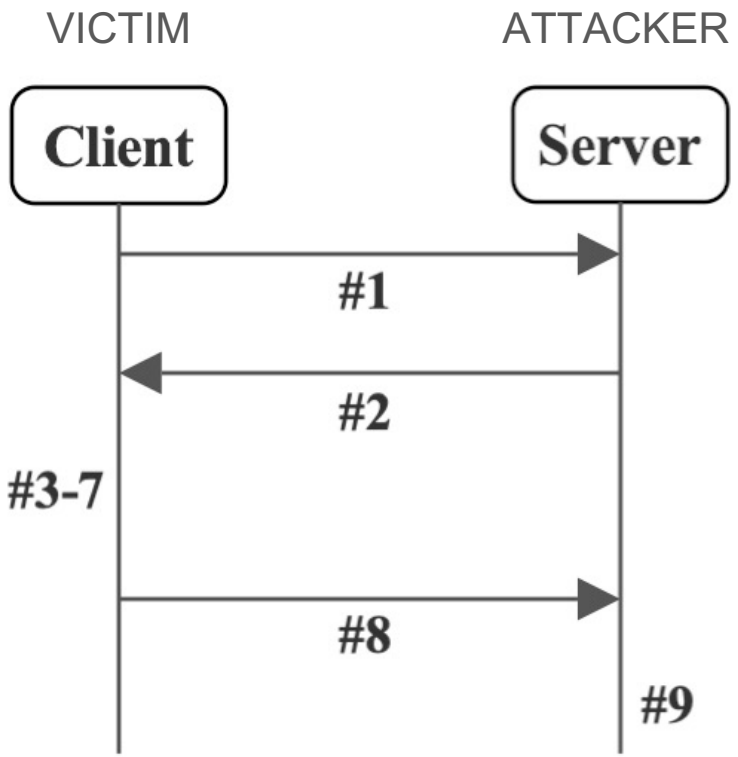
- Map unique id & class names to specific extensions
- Populate pages with two copies of such elements

For our attacker model

- Use the existing mapping to populate our page

1. O. Starov and N. Nikiforakis. 2017. XHOUND: Quantifying the Fingerprintability of Browser Extensions. In 2017 IEEE Symposium on Security and Privacy (SP).
2. P. Laperdrix, O. Starov, Q. Chen, A. Kapravelos, and N. Nikiforakis. 2021. Fingerprinting in Style: Detecting Browser Extensions via Injected Style Sheets. In 30th USENIX Security Symposium.

Pipeline



1. Visit page
2. Send attack files
3. Insert CSS elements
4. Start recording DOM changes
5. Extensions modify page
6. Record CSS changes
7. Stop recording DOM changes
8. Send collected data
9. Save data

Experiment Setup

Device

1. Samsung Galaxy Note 10 5G
2. OnePlus Nord
3. OnePlus 6 (A6000)

Browser

1. Yandex
2. Kiwi
3. Firefox Nightly

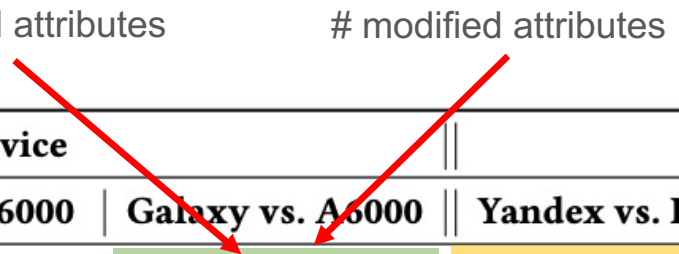
- Yandex and Kiwi instead of Chrome
- Firefox Nightly instead of Firefox

Extension

50 extensions → down to 16 → identified 6

1. 360 Internet Protection → CSS
2. AdBlocker Ultimate → CSS
3. Avast SafePrice → CSS & DOM
4. Dark Reader → DOM
5. DuckDuckGo → CSS
6. Touch VPN → CSS

Results: Cross Device & Cross Browser

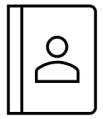


		Cross-Device			Cross-Browser		
Per		Nord vs. Galaxy	Nord vs. A6000	Galaxy vs. A6000	Yandex vs. Kiwi	Yandex vs. Firefox	Kiwi vs. Firefox
Extension	AdBlocker	0/114	0/114	0/114	0/105	0/98	0/105
	DuckDuckGo	0/6	0/6	0/6	0/6	0/6	0/6
	Avast SafePrice	48/8498 (0.56%)	48/8498 (0.56%)	0/8498	0/8298	219/8004 (2.74%)	219/8130 (2.69%)
	360 Internet	0/560	0/560	0/560	0/816	-	-
	Touch VPN	9/958 (0.93%)	9/958 (0.93%)	1/958 (0.1%)	0/942	25/924 (2.7%)	25/942 (2.65%)
	All	57/10136 (0.56%)	57/10136 (0.56%)	1/10136 (0.01%)	0/10167	244/9032 (2.7%)	244/9183 (2.66%)
Browser	Yandex	0/6892	0/6892	0/6892	-	-	-
	Kiwi	0/6896	0/6896	0/6896	-	-	-
	Firefox	114/6484 (1.76%)	114/6484 (1.76%)	2/6484 (0.03%)	-	-	-
Device	Nord	-	-	-	0/6778	88/6024 (1.46%)	88/6122 (1.44%)
	Galaxy	-	-	-	0/6778	200/6020 (3.32%)	200/6122 (3.27%)
	A6000	-	-	-	0/6778	200/6020 (3.32%)	200/6122 (3.27%)
	Total	114/20272 (0.56%)	114/20272 (0.56%)	2/20272 (0.01%)	0/20334	488/18064 (2.7%)	488/18366 (2.66%)

Conclusion

- We demonstrate the feasibility of extension fingerprinting in the new context of **mobile devices**.
- We shift attention from binary to **granular results** which can be used to discriminate users further.
- **Future Work**: 1) User study, 2) Countermeasures

Thank You!



Brian Hyeongseok Kim
brian.hs.kim@usc.edu

https://github.com/briankim113/WPES2023-Artifact