Technical analysis of browser fingerprinting techniques based on FingerprintJS

James Bergfeld
Technical University Munich
Munich, Germany
j.bergfeld@tum.de

Samuel Scheit
Technical University Munich
Munich, Germany
tum@samuelscheit.com

I. Introduction

- “How does modern browser fingerprinting work (in practice)?”

A. Browser Fingerprinting

a) General

b) Advantages

c) Disadvantages

d) Relevance

B. Technical implementation

II. Background

III. Methodology

IV. Results

A. Parameters

a) Browser Properties

- window.navigator.onLine
- window.devicePixelRatio
- navigator.storage.estimate()
- window.screen
- window.indexedDB
- window.webkitRequestFileSystem
-
-
-
-
-
-
-
-

b) TLS

c) Audio

d) Canvas

1. Fonts

e) WebRTC

1. ICE Candidates
2. Media Devices

f) Speech synthesis

SpeechSynthesis is part of the Web Speech Browser API that allows websites to convert text to audio data (TTS). For this the browser exposes the function SpeechSynthesis.getVoices() that lists all locally and remotely available voices that can be used for TTS.
Each voice contains the following properties:

- `voiceURI` (unique voice identifier)
- `name` (human-readable name of the voice)
- `lang` (ISO language code of the voice)
- `localService` (boolean indicating if the voice is locally available or a remote service)
- `default` (boolean indicating if the voice is set as default)

B. Comparison to open-source FingerprintJS

V. Discussion

VI. Conclusion

References