Complex Device Fingerprinting to Protect Against Account Takeover

Device detection with **unparalleled accuracy** that meets PSD2 and FFIEC standards for device-based authentication.

Distinguishing trusted devices from malicious ones requires persistent, accurate device fingerprinting — even when fraudsters use evasive tactics, browser vendors release new updates, and users uninstall and reinstall applications.

Challenge

Modern browsers eliminate many device identifiers

New regulations and increased demand for consumer data privacy have caused browser providers and device manufacturers to block third-party cookies and restrict the information that's returned by JavaScript engines, the main interface through which device fingerprinting is done.

Constant updates degrade fingerprints over time

Browser vendors make constant, frequent updates to their JavaScript engines, making it difficult to maintain accurate fingerprint over time, especially when considering the range of devices and browsers on the market.

Device spoofing and other evasion tactics manipulate attributes

Device emulators can be used to spoof a type of device used by a specific user while automation frameworks enable attackers to manipulate headers and cookies, making it harder to detect fraudulent devices.

Solution

Sophisticated calculations based on robust telemetry

Transmit Security's Detection and Response Service combines multiple device attributes using an advanced statistical proprietary framework to balance the tradeoff between consistency and uniqueness.

- **Complex fingerprints** are based on multiple identifiers and tested by data scientists on large device data sets in our in-house research labs, resulting in a **97% true acceptance rate** and a **99.97% true rejection rate**.
- **GPU sampling** uses unique properties of a device's GPU stack to help distinguish between devices with identical hardware and software configurations.

Key Use Cases

Verifies trusted user devices

Links trusted devices to individual user profiles to reduce friction for customers who establish a high level of trust.

Recognizes fraudulent devices

Identifies devices that have previously been used by attackers for ATO and new account fraud (NAF).

Discovers anomaly patterns

Finds anomalies in device usage to challenge unexpected scenarios that indicate activity from bots or automation frameworks.

Identifies high-velocity account opening

Detects fraudulent new accounts created at high rates or velocities by device farms or evasive bots using synthetic or stolen identities.

Detects credential stuffing

Identifies repeated login attempts from attackers using automation frameworks or bots to inject stolen credential lists into login forms.

Spots session hijacking

Detects fingerprint mismatches and verifies the authenticity of a device throughout the user session to prevent session and cookie hijacking.

Cloud-Native Fingerprinting with Risk, Trust, Fraud, Bots & Behavior Analysis

Device fingerprinting is part of our Detection and Response service, a fraud prevention SaaS that uses multiple detection methods to deliver transparent, contextual recommendations on risk and trust for each user, at each moment, across the entire user journey. Device fingerprints are calculated in real-time to match trusted devices with users' historical profiles, enabling less friction for trusted users and better detection of ATO and NAF.

- **Multiple identifiers and unique detection techniques,** such as GPU sampling, enable more robust and reliable calculations.
- **Dynamic adaptation to browser and device changes** leverages cloud-native, microservice architecture to deploy frequent, ongoing updates to our risk engine that adapt to rapid changes in the market that impact fingerprint accuracy.
- **Advanced statistical frameworks** are tested and optimized by in-house data scientists to continuously improve true acceptance and rejection rates.

Backed by the Transmit Security Research Lab

Benefit from the expertise of our security researchers, who constantly research changes in JavaScript engines that impact fingerprinting accuracy and use applied data science based on large data sets to continually optimize our algorithms. They apply their findings to choose the best features for calculating persistent, unique device fingerprints and create tools that can be used for detecting new trends in raw data.

kuppingercole ANALYSTS

Transmit Security Named 'Overall Leader'
in three ranking reports: Fraud Reduction Intelligence, Passwordless Authentication and CIAM Platforms.

Device Fingerprint Data Points

Hardware
- Screen properties
- Graphics card
- RAM
- Battery
- CPU
- Multimedia devices

Graphics
- Supported video codecs
- Canvas properties and sampling
- Rendering information

Audio
- Audio codecs
- Audio properties
- Sampling

Environment
- OS
- Connectivity
- Storage
- Supported fonts
- Plug-ins

GPU
- Sampling

FFIEC & PSD2 Compliance

- Meets complex fingerprint guidelines for FFIEC
- Meets PSD2 standards for low probability of unauthorized payments
- No data stored locally
- No data stored in cookies

About Transmit Security

Transmit Security gives businesses the modern tools they need to build secure, trusted and end-to-end digital identity journeys to innovate and grow. CX-focused, cybersecurity-conscious leaders rely on Transmit Security's CIAM platform to provide their customers with smooth experiences protected from fraud across all channels and devices. Transmit Security serves many of the world's largest banks, insurers, retailers, and other leading brands, collectively responsible for more than $1.3 trillion in annual commerce. For more information, please visit **www.transmitsecurity.com**.