threat | METRIX

Device Fingerprinting and Fraud Protection Whitepaper

Table Of Contents

1 Overview

Device Fingerprinting is a new way of differentiating between a valuable customer and a professional fraudster online.

Today, the prevalence of identity theft and hackers has meant that it is much harder to verify that the person you are doing business with is who they say they are. That new customer could be a compromised computer transacting on behalf of a sophisticated eastern European crime gang or an opportunistic thief that has lifted personal details from Facebook. It's clear that online identity verification is a significant challenge and concern to all business owners.

2 What is Device Fingerprinting?

Device Fingerprinting (sometimes called PC Fingerprinting) is part of a broader class of technologies called Device Intelligence used to determine whether the computer you are doing business with should be trusted or not. Device Fingerprinting is the measurement of anonymous browser, operating system and connection attributes in order to generate a risk profile of a device in real-time.

3 Why is Device fingerprinting necessary?

With personal identity information such as credit cards and login passwords now a commodity on the black market, companies need to look to alternative methods for verifying identities and transactions online. This problem is compounded by the fact that fraudsters now routinely evade IP Address Blacklisting and IP Address Geolocation tools using proxies. Proxies can be special purpose servers used to masquerade a fraudsters real IP Address, but are now increasingly likely to be one of the millions of compromised computers, also called botnets, that are under the control of criminal gangs. Device Fingerprinting is a powerful tool for recognizing a returning fraudster even if they change their name, IP Address or cookies.

4 How can Device Fingerprinting be used to prevent online fraud?

Device Fingerprinting is a valuable tool because it enables a fraudster's device to be recognized even when they change their identity through the use of proxies and stolen credit card or account password information.

Depending on the business, typically four main strategies are used to leverage Device Fingerprinting to combat fraud.

1. Anomaly Detection – detecting anomalies related to the device fingerprint is a powerful way of providing first time fraud detection. An example of anomaly detection would be determining that a device was connecting through a proxy to hide its real location, or determining that a device is currently under the control of a botnet.
2. Device Velocity – when fraudsters find a hole in your defenses they will try to extract the maximum value as fast as they can. Creating velocity filters based on a Device Fingerprint will enable you to minimize fraud costs even when names, credit card details and IP Addresses are changed.
3. Transaction linking – a Device Fingerprint is a powerful tool for finding related transactions either as an identifier in itself or as a means of finding transactions with related characteristics e.g. finding related transactions performed from the same ISP and location.
4. Account linking - a Device Fingerprint is a valuable tool to be able to detect when accounts or subscriptions are being accessed or shared illegally.

5. Device Reputation – if a device has been involved with fraud, adding that device to a a blacklist will enable you to protect customers that share the same device reputation network.

5 What are the trade-offs in Device Fingerprinting technologies?

The tradeoffs that need to be considered are the uniqueness, persistence, resistance and fit of the Device Fingerprinting approach.

1. Uniqueness is the measure of how accurately and confidently you can identify a return computer and differentiate it from other computers on the internet. It depends on the amount of entropy, or information, that is contained in the fingerprint. For example, screen-resolution by itself is does not represent a unique fingerprint while the MAC address of a computer is generally considered unique.
2. Persistence is the measure of how long you can expect to uniquely identify a device based on the fingerprint technique used. For example, the operating system would be a persistent fingerprint attribute, while javascript version used by the browser would change more frequently.
3. Resistance is a measure of how well the Device Fingerprinting technique stands up to tampering by a hacker or fraudster. For example, a browser cookie may be unique, but it is easy to delete or copy.
4. Fit is the measure of how seamlessly the Device Fingerprinting technology integrates with your business and technology requirements. For example, requiring a user to have a hardware token or to download software in order to uniquely identify them is inconvenience and not practical for most online businesses. Ideally the Device Fingerprinting method should be transparent to the end user.

Look for a Device Fingerprinting solution that strikes an optimal balance for your business.

6 What are the major types of Device Fingerprinting methods?

The two major types of Device Fingerprinting methods are client-based and server-based transparent profiling solutions.

6.1 Client-based methods

Client-based methods require installing a software executable on an end computer. The advantage of client-based methods is that they have access to otherwise hidden operating system information such as the hard drive serial number and MAC address of the network card. This information is highly unique, persistent and harder to tamper with. The major disadvantage of this method that excludes it from practical use in most ecommerce transactions is that the process requires some action or permission on behalf of the user. This may be ok if you are a bank, but definitely not if you are an ecommerce, media or retail financial services business. The other issue is of course that most corporate computers won't allow anything to be installed from an external website.

6.2 Transparent Device Profiling

Transparent Device Profiling methods on the other hand rely on information that can be measured remotely via a profiling server. This information is based on anonymous attributes that can be measured or derived about the user's browser, operating system and connection. Because this method has zero impact to the user's customer experience and their privacy and does not require registration, this is often the only practical method available to ecommerce, online media and retail financial businesses. The trade-off with transparent profiling is that protected device attributes such as MAC address or hard-drive serial number are not available. However, recent advances in TCP protocol and Operating System profiling now enable a device to be uniquely identified beyond more obvious browser characteristics such as browser type and version. Look for a Transparent Device Fingerprinting solution that incorporates information across all levels of the web connection,

and understands how to interpret anomalies detected across each of these levels described below.

6.2.1 Browser Tagging

At its simplest level Browser Tagging involves the use of a cookie to positively identify a return user. For example, many authentication systems will use a cookie to identify whether a user has logged in or transacted from this device before.

6.2.2 Browser Fingerprinting

Browser Profiling is the use of HTML, Javascript, Flash or other methods available in the browser in order to profile a device. Information available through the browser includes, but is not limited to, screen resolution, browser type, clock time, time zone, languages and media supported.

6.2.3 HTTP Fingerprinting

HTTP Fingerprinting is a method of extracting additional risk information communicated during the HTTP connection between the client and the server. Such information includes, but is not limited to the types of compression supported, proxy support and language.

6.2.4 Operating System Fingerprinting

By profiling connection characteristics in real-time is it possible to accurately determine the operating system, and often version, being used to establish the internet connection.

6.2.5 TCP Fingerprinting

TCP Fingerprinting provides information about the type of connection being used, connection speeds, and for more sophisticated approaches, can be used to individually fingerprint devices based on the network protocol stack.

7 Preferred characteristics of a Device Fingerprinting solution

There are a number of factors you will need to consider when implementing a Device Fingerprinting technology.

7.1 Zero impact

Ideally your Device Fingerprinting solution should have zero impact on both your customer's experience as well as your IT infrastructure. Requiring a user to download software or use a hardware token will lead to dissatisfaction and abandonment, while requiring your operational staff, who are often incented on up-time and availability, to install additional software on your web servers will also be met with some pushback.

7.2 Installation flexibility

Preferably your device fingerprinting technology is able to be implemented as a web service to reduce installation and maintenance costs. A set of well defined web-API will enable easy and cost effective integration of Device Intelligence into your existing business rules engines, fraud systems or risk-based access control systems.

7.3 Real-time decision engine

Intelligence is only as valuable as it is timely. Look for Device Fingerprinting solution that is capable of calculating Device Risk in real-time rather than minutes, hours or days.

7.4 Fuzzy matching

One approach to generating a Device Fingerprinting is to perform a simple hash of measured attributes. The limitation of such an approach is that it takes only one parameter to change, for example swapping the browser used from Internet Explorer to Firefox, and an entirely new

Device Fingerprint is generated. Look for a Device Fingerprinting solution that uses a fuzzy matching technique to provide a more accurate and persistent Device Fingerprint.

7.5 Measurement Diversity

Today's browsers support technologies such as Flash and JavaScript that are capable of gathering extensive Device Fingerprinting information. However, such technologies are also able to be readily disabled by fraudsters and privacy conscious web surfers alike. To be able to differentiate between a fraudster and a valuable customer, look for a Device Fingerprinting technology that does not rely exclusively on either JavaScript or flash and can uniquely identify a device even when these technologies are disabled.

7.6 Device Fingerprint Depth

Just like an iceberg, what you can't see could sink you. All web servers and web analytics companies provide basic browser techno graphics such as browser type, browser language and the types of multimedia and languages that are supported. However, this information also very easy to manipulate by a knowledgeable fraudster and is also blind to warning signals that lie beneath what the browser is telling you. Look for a Device Fingerprinting approach that looks beyond the browser and is able to perform Operating System, Protocol and Connection Fingerprinting in real-time. The benefit of these technologies is that they are able to recognize a fraudster even when the browser attributes change or when cookies are deleted, and can more accurately alert to when a high risk proxy is being used.

7.7 First-time protection: Device Analytics and Anomaly Detection

For most ecommerce websites, the majority of their transactions and fraud attempts are from new customers. For these companies, recognizing a return fraudulent device is not as useful as being able to detect a fraud attempt the first-time, in real-time. Look for a Device Fingerprinting solution that is able to provide first-time fraud intelligence such as:

- Whether the Device is hiding behind a proxy and accurately determine the risk associated with the proxy.
- The True IP and not just the Proxy IP that the device is connection from.
- The True Geo that the connection originated from, and not just the location of the proxy used.
- Whether a device has been compromised by malware and belongs to a botnet

8 Conclusion

As ecommerce revenues grow, fraud inevitably follows. The absence of a physical customer at the time of the transaction or login combined with a new era of technology-driven identity theft means that there is a need for a new alternative to online identity verification. Device Fingerprinting, while not a panacea, is a valuable Device Intelligence tool capable of detecting and stopping fraud that currently flies under the radar of outdated and outmatched fraud detection systems. Lastly, understanding the different approaches, and choosing a Device Fingerprinting solution that fits within your business and technology requirements will yield the best results.