Today, users gain access to private information from just about anywhere in a variety of situations. As such, organizations continually face the dilemma of choosing between the risk pitfalls of remote access verses putting users through an arduous authentication process. Not so with strong authentication methods that provide greater flexibility in the way users are required to verify their identity.

This paper will provide an overview of what device fingerprinting is and how it works. It will also cover why it’s important and how NetIQ® enables you to best take advantage of it.
Smarter Authentication

With ever increasing cases of account hijacking and cybercrimes, it’s clear that passwords on their own are no longer enough to protect critical applications and services, including private or regulated information. In recent years, organizations have been bolstering user verification through the adoption of multi factor authentication. Multi factor authentication adds another layer of security by further validating the user’s claim. With multi factor authentication a user is asked to provide an additional piece(s) of information to prove his identity; typically related to what the user knows or possess. While this added step does strengthen security, requiring multiple inputs of identifying information adds friction to the whole authentication process, resulting in degraded user experience and possible user frustration.

This protracted experience is concerning to the business. There may be times when user access needs to be quick, yet secure. Businesses are also be concerned about users deferring a business process because access to an application or service may be too inconvenient. Often, users engineer around inconvenient tasks or processes.

Risk based or Adaptive authentication is being increasingly used to overcome these concerns. This technique tailors the level of the security to the risk factors or the threat level that the user presents at the time of login or access to a service. For example, location of access can be a risk factor. If the user access the service from her home or office location routinely, the risk factor can be considered low and the authentication process can be a basic identity verification. If the same user is found to be accessing from an unusual or suspicious location and is trying to access a sensitive information, the risk level can be considered higher. In order to securely identity and prove the identity of the user, she could be presented with an advanced authentication method (such as biometric or a challenge) at that stage.
Device Fingerprinting in the Enterprise

Device fingerprinting is a strong way for organizations to identify devices by obtaining characteristics from it by reading attributes that give information about its browser, platform, operating system and hardware. While it may be true that each attribute in isolation is not unique, adding them all together does provide a strong indicator of one’s identity.

Organizations need this higher-level identity assurance because in today’s connected world it’s much harder to be sure that the person you are doing digital business with is who they say they are. Here are some of the most common ways that device fingerprinting is being used today.

83.6% of the visiting browsers had a unique fingerprint... among Flash or Java-enabled browsers, 94.2 percent had unique fingerprints...

When used in conjunction with risk based authentication device fingerprinting can increase security substantially without compromising on user convenience. It does this by associating the device's identity to the user's account and leverages this information verify user identity that is both strong and seamless to the user experience. Since both device fingerprinting and risk based authentication typically run in the background, it's invisible to the user. Security has been increased for the organization while keeping the user's experience as convenient as possible.

Using advanced authentication methods are part of a risk based infrastructure enables you to increase security while optimizing convenience. For example, when users log onto corporate services from their own fingerprinted devices (laptops, tablet, phone etc.), they can simply be given access for low risk assets without fetter on only perform a stepped-up authentication when access to higher risk information is sought. As an advanced authentication method, device fingerprinting can be used to lower business risk while delivering the best user experience.

Fraud Detection

A key business driver for device fingerprinting is protection against account hijacking. This is done by determining whether the computer that the organization is interacting with should be trusted or not.
Today, the prevalence of identity theft and hackers means that it is much harder to verify the digital identity that you're doing business with and the risks are higher.

- **Banking and financial institutions**—fraudsters use stolen credentials to gain access to banking sites and perform do some financial transaction on the banking sites.

- **Federal, state and local government Web sites**—as the threat from state sponsored cyberattacks continue to grow, the stakes have never been higher. Even state and local government websites are common targets for criminals that use stolen credentials to gather private information.

- **Social networks**—fraudsters hacking into legitimate user's account to malign his social image or gain his private information. They also leverage shared credentials to spread malware.

- **E-commerce sites**—criminals use stolen credentials for unauthorized online purchases. In spite of these risks, password fatigue continues to grow.

- **Company’s private website or web applications for its customers and employees**—fraudsters can use stolen accounts to gain company’s private information or initiate any process or transactions that leads to massive financial loss.

### Analytics

As organizations analyze their network and data services infrastructure, information fetched by device fingerprinting can give deep insight into company’s employee’s behavior and asset (devices) details.

As organizations measure current usage and predict future needs, usage information like geographic location, device hardware/software configurations, login time etc., infrastructure investment can be planned and corporate guidelines put in place on device usage (corporate issued and BYOD) for official business.

### Marketing/Advertising/e-commerce

Associating devices to accounts provides another degree of insight into customers beyond just fraud protection. Businesses can use this added piece of information for greater understanding of their customer.

For example, devices associated with 'good' customers or paying members can also be whitelisted in order to: show ads relevant to them, give personalized offers, facilitate streamlined purchases, same day deliveries, or other perks that improve the user experience and build loyalty. This can be done through the use of fingerprint scripts hidden in their innocuous advertising banners and web widgets, which silently collect the user’s/device’s information.
Device Fingerprinting Methodologies

Cookies have been used to identify devices for years; however, they are under the control of the user who commonly used tools to delete them anytime, reducing their value for device identification. Device fingerprinting allows a much stronger technique of device identification and that is not easily circumvented by users.

Here are some of the more common approaches to device fingerprinting.

Browser Fingerprinting

In browser fingerprinting, technologies like HTML, JavaScript, and Flash etc. are used to obtain characteristics of a client's machine. Fingerprint JavaScript is run in the background in a webpage to collect device information of the client's device in a seamless manner. Some example parameters collected are: html5 features support related details, browser details, browser plugins, mime support, OS and hardware details, user preferences set on the user's device, location details like locale, language settings and time zone on user's device, HTTP request headers information, Canvas fingerprint, WebGL fingerprint, TCP/IP fingerprint parameters (e.g., Operating system, etc.).

Some new elements in HTML5, viz. Canvas (2D image), Web-GL (3D images), require browser to work more closely with the operating system and system hardware (GPU) for rendering a 2D or 3D image on the screen. So, the browser's ability to render such images, varies depending on the behavior of these underlying resources and thus it gives a quite unique fingerprint of a client's device. Fonts that can be displayed on the browser also depends on the browser as well as the underlying Operating system. Information of supported or unsupported fonts on a device also adds good uniqueness to the overall fingerprint.

Defense Against Browser Fingerprinting?

With the advances in device fingerprinting technology, awareness of being tracked has also increased among some users. Browsers ask for user's consent when a site tries to draw a canvas image or tries to access HTML5 media. There are some browser plugins to block such activity (e.g., canvas Block plugins). Users can disable JavaScript in the browser for their defense. However, this is not a good and sustainable option for any user. There are some browsers like "Tor browser" which are known to be most resistant to Browser fingerprinting.

In browser fingerprinting, technologies like HTML, JavaScript, and Flash etc. are used to obtain characteristics of a client's machine. Fingerprint JavaScript is run in the background in a webpage to collect device information of the client's device in a seamless manner.
Is the Technology Effective?
Electronic Frontier Foundation, did a study to assess browser fingerprinting in 2010 (see [www.eff.org/deeplinks/2010/05/every-browser-unique-results-fom-panopticlick](http://www.eff.org/deeplinks/2010/05/every-browser-unique-results-fom-panopticlick)). Their study found that out of around 1 million visits to their study website, 83.6% of the browsers seen had a unique fingerprint; among those with Flash or Java enabled, 94.2%.

This study shows that browser fingerprinting is effective and this approach is a currently most widely used fingerprinting technique. Not only is this tracking hard to detect and prevent, setting Browsers to “private-mode” doesn’t make a much difference as JavaScript still would be able to fetch the device details. Use of browser plugins or settings that help in preventing browser fingerprint, also adds more uniqueness to the overall fingerprint.

Strong Browser Fingerprinting Techniques
Here are some key techniques for strong browser fingerprinting:

- Fingerprint technique should depend on multiple points of information from the browser.
- Also, same information if possible should be retrieved from multiple sources and cross checked. Spoofing browser parameters is possible, but spoofing all the parameters correctly to match a particular fingerprint is very difficult considering the number of parameters used for fingerprinting and unawareness of fingerprint configuration details for the hacker.

Passive Fingerprinting
Passive fingerprinting as the name suggests happens without directly querying the client system in a passive manner. There are some techniques that passively sniff the TCP/IP traffic from the client machine and gives accurate information about the client's Operating system, device uptime, distance, connection type and speed, etc. based on various TCP/IP headers (Window size, Initial TTL, do not fragment etc.). As spoofing TCP/IP packets are quite difficult, this method is considered to be reliable and strong for fingerprinting.

Active Fingerprinting
Active fingerprinting as the name suggests happens by directly querying the client system in an active manner. A common active fingerprinting technique sends queries to the target using different and analyzes the response. For instance, some tools can send special packets to a device and study the response packets and determine the operating system of that device. Some tools can query different ports on a device and if the device responds on those port, they can identify what type of server it is. An example would be if a host responds on port 25, it is likely to an email server from this addition queries can verify and gather more information if desired.
Other such fingerprinting technique may ask user to install some applet or executable code that obtains detailed information like MAC address from his machine, which otherwise wouldn’t be available.

These techniques are also strong; however, they wouldn’t be suitable for the Enterprises where one doesn’t have control over the end consumers (e.g., B2C scenarios) and where one wants fingerprint process to be seamless to the end user. They might not be feasible in many cases due to a network privacy settings.

**Characteristics of a Strong Device Fingerprinting Solution**

There are a number of factors to consider when implementing a device fingerprinting solution. Ideally your fingerprinting solution should have close to zero impact on the user’s experience. Device measurement technologies invoked also need to burden or complicate your IT infrastructure as little as possible. Here is a list of other factors for your consideration.

- **Uniqueness**—is how accurately the technique can identify a device and differentiate it from other similar devices. As you look for attributes to retrieve that is should be based on information that gives high level of uniqueness. It also needs to be collected from a reliable source on the devices. For example, some techniques can fetch the device’s GPU’s information which tend to contain unique information. Other good sources of unique information include canvas, font, WebGL, TCP/IP, OS fingerprinting.

- **Persistence**—is how long you expect to be able to depend on an attribute as a reliable component of the device’s fingerprint. Since ideally you want the fingerprint to last as long as possible, choose properties that either will last the lifetime of the device or are slow to change.

- **Flexible fingerprint matching logic**—is important as user’s device configuration change over time, which results in fingerprint drift. Fingerprinting needs to accommodate the inevitable little changes in user’s device to ensure that even legitimate changes in the device (e.g., companywide operating system patch upgrade or time zone changes due to travel), do not make the system to consider it as an unidentified device and increase the security threshold for that device.

- **Readily obtainable**—has to do with how fast fingerprint can be obtained from the client’s machine. For example, JavaScript used for browser fingerprinting should be quite fast in obtaining the fingerprint from the user’s machine, so that it is seamless to the user and it doesn’t affect the performance of your application much.
While not a panacea, device fingerprinting can be a powerful method of measuring risk and adapting the authentication experience accordingly.

- **Performance impact**—in critical applications, factors like fingerprinting approach’s efficiency, play an important role. Suppose if someone deploys fingerprinting solution in their infrastructure to secure the login process. If they have a peak login traffic time for their applications where many people login at the same time, e.g., morning hours in stock exchange applications, then this fingerprint solution should not slow down the server’s capability to handle logins/second drastically or it should not eat up the resources on the server extensively such that it slows down the application itself.

- **Suitable metrics**—is important because ideally device fingerprinting technology should get added in a transparent way to your enterprise applications. For example, employees working in an enterprise environment may very well be expected to install an executable or applet on his machine to enable device fingerprinting identity, but that same approach will likely not be palatable for most customers. For them zero impact methods that preserves the customer experience and does not require registration is often the only practical method.

- **Support of multiple devices per user**—is fundamental because most users have multiple devices (e.g., laptop, desktop, tablet, mobile etc.). The fingerprinting solution that you implement should be able to associate multiple number and types of devices to a particular user. If your solution that doesn't support multiple devices, your ability to leverage fingerprinting to verify the user’s identity will be limited. The result being that the user will be required to go through a stronger authentication procedure each time he changes his device.

- **Risk based / adaptive authentication framework**—should be used with fingerprinting to get the highest level of security and optimized user experience. Generally, device fingerprint shouldn’t be the only authentication method in your login framework. Fingerprinting is typically used in a probabilistic approach by first testing to see if the device can be identified correctly from which a risk associated with a login can be calculated. Depending on the sensitivity of the information being accessed, if the device fingerprint matches the user that it’s assigned to he can be allowed to access it in a seamless way without making him to undergo any formal login process. For highly protected information, users on matched devices can be challenged with simple login methods like name/password. If a fingerprint mismatch happens then the risk based authentication engine can increase the authentication level needed to verify the user’s identity using methods like challenge questions, one time password, or biometric.

- **Supportable**—whatever technique or technology that you chose should be such that administrators can configure, update and effectively debug their fingerprinting methods. And as part of the broader risk based authentication configuration, a supportable fingerprint will depend on how granular and customizable the configuration is, and how non-intrusive the mechanism is. Because different industries have different requirement you may have to do some research. For example, authentication involving regulated information may have specific requirements.
Conclusion

As digital transactions and interactions continue to grow in volume and importance, the inevitably of fraud will continue to grow with it. A new, more powerful way of verifying the identify for these remote dealing is required manage the risk to your organization as well as the people that interact with you. While not a panacea, device fingerprinting can be a powerful method of measuring risk and adapting the authentication experience accordingly.

About NetIQ

To learn how to get the most out of your access management investment: www.netiq.com/solutions/identity-access-management/