Browser Cookies

Definition/Description

Browser identifiers are a subset of more general device identifiers that provide a means to identify and later recognize a user's device. One the first methods of doing this was browser cookies.

Browser cookies were one of the first tools enterprises used for authentication and fraud detection. Cookies allow a device to be tagged and used as the "something you have" component of the authentication process, replacing hardware tokens. If a device is unknown, the enterprise could use additional step-up authentication measures.

Applicability

Channel	Applicable?	Use Case	Applicable?	Stakeholder	Applicable?
In-app [merchant app]	NA	Customer onboarding	NA	Merchants	Yes: internal
Mobile browser	Yes	Authentication (onboarding)	NA	Issuers	NA
Desktop/laptop computer	Yes	Authentication (transaction)	Yes	Issuer processors	NA
Phone	NA	Authorization	Yes	Wallet/online payment providers	NA
		Post-authorization review	Yes	Acquirer processors	Yes: for clients[1]

Technical Features/How the Technique Works

Browser cookies allow a merchant to identify familiar devices, by associating bits of data to a specific device/user. Cookies are small amounts of data stored as text files on a browser.

For example, when a user visits a website, the site may deliver a cookie to the browser identifying the user as "User X." If the user leaves the site and returns to it again, that cookie will be used by the website to recognize that the user is the same User X that was at the site previously.

Cookies necessarily contain, at a minimum, two pieces of data: a unique user identifier and some information about that user.

Risks Associated with Technique

Cookies can be easily erased, making the device anonymous and usually requiring stepped-up authentication.

Modern device ID solutions have become significantly more sophisticated than the early cookie-based solutions, so browser cookies are often used as part of a multi-layered solution.

[1] Typically done by whoever provides website.

Customer Impact/Level of Friction

Cookies are invisible to the customer. However, customers will experience friction if a cookie is deleted and they are asked to authenticate their identity through a different method.

Implementation Considerations

The merchant website would be implemented to store cookies on users' browsers and use them to identify returning customers.

Maturity

Internet browser cookies were first patented in the late 1990s. They are widely used today.

Applicable Industry Standards

The Internet Engineering Task Force (IETF) 6265 standard defines cookies.

Publicly Available Statistics on Implementations and Use

Browser cookies are very widely used. Published statistics are not available.

Further Reading

https://securityintelligence.com/why-device-id-may-not-be-enough-to-stop-fraud/

https://www.whoishostingthis.com/resources/cookies-guide/

https://sift.com/sift-edu/prevent-fraud/device-ip-analysis

Cookie patent:
https://worldwide.espacenet.com/patent/search/family/024155035/publication/US5774670A?q=pn%3DUS5774670

Source Document: This technique is extracted from the *Card-Not-Present (CNP) Fraud Mitigation Techniques* white paper. That white paper was developed to provide a high-level document that directs readers to relevant fraud mitigation techniques while providing easy access to details about the solutions. The whitepaper is available at: https://www.uspaymentsforum.org/card-not-present-cnp-fraud-mitigation-techniques/

support, maintain or update the Information, regardless of any such change. Use of or reliance on the Information is at the user's sole risk, and users are strongly encouraged to consult with their respective payment networks, acquirers, processors, vendors and appropriately qualified technical and legal experts prior to all implementation decisions.