Device Bound Session Credentials

TPAC 2024 Breakout Session

https://github.com/WICG/dbsc/blob/main/README.md

Benjamin Ackerman (ackermanb@chromium.org)
Kristian Monsen (kristianm@google.com)
Arnar Birgisson (arnarb@chromium.org)
Sameera Gajjarapu (sameera.gajjarapu@microsoft.com)
Aleksandr Tokarev (alextok@microsoft.com)

For Announcements

Join dbsc-announce@chromium.org

Two ways:

- dbsc-announce+subscribe@chromium.org
- https://groups.google.com/a/chromium.org/g/dbsc-announce/

Why DBSC?

- Cookie theft is an ongoing issue and will be around as long as cookies are used for authentication

- This problem affects all web services that requires authentication
    - (and there's a reason for attackers to want access → 💰)

- We're looking at a more holistic solution to prevent these types of attacks from continuing to be profitable everywhere
    - Making this protocol as a browser standard should make adoption across the web easy for everyone

The attack cycle

1. User machine is infected by malware

2. Malware collects user cookies and sends them to an attacker controlled server

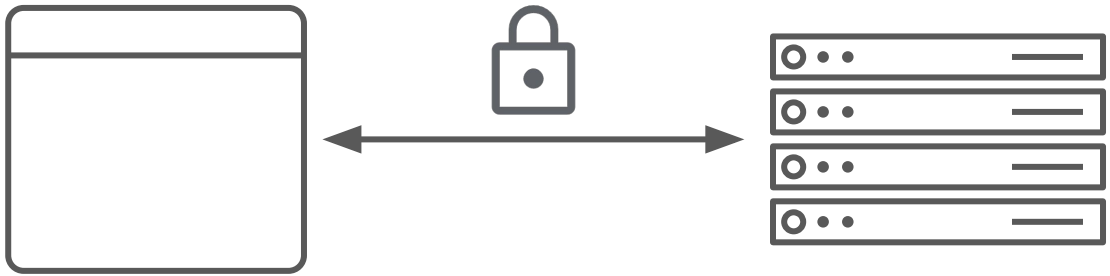
3. Cookies are auctioned off to different attackers who specialize in abuse on the desired platforms

4. Profit

What is DBSC?

At a high level it's a secure session that is created between the browser *on a specific device* and a web server

The goal is to make the business of exfiltrating cookies to 3rd party devices useless



How does this make cookies unappetizing?

- Change forever lived cookies to expire relatively quickly

- When the cookie expires have the server challenge the browser to validate for the DBSC session
    - if Yes → reissue cookie to device
    - if No → force user to reauthenticate

Can’t the attacker just fake a session?

Hopefully not 😆

The DBSC session is secured using a public/private key pair using *unexportable keys* on the device

Device Specific Key Generation Proposals

Windows:

- Trusted Platform Modules (TPMs)
- Virtualization-based security (VBS)

Mac: Secure Enclave

Linux: Trusted Platform Modules (TPMs)

Android: Trusted Platform Modules (TPMs - Keystore)

iOS: ¯_(ツ)_/¯

Will malware just stop after this?

One can dream!!!

But most likely not 😓

We think that malware will pivot to persistent on device attacks

- These attacks should be easier to detect and mitigate
- The goal of DBSC isn't to completely stop malware, but just make the cookie exfiltration a useless endeavour