Tracking Users across the Web via TLS Session Resumption

Erik Sy, Christian Burkert, Hannes Federrath, Mathias Fischer
Introduction to TLS Session Resumption

- Allows a client-server pair to establish a new TLS connection with a previously exchanged symmetric key
  - Provides temporal and computational performance gains
  - The client is identified by the server (tracker) through knowledge of this secret key

- Deployment on the Internet
  - 96% of TLS-enabled Alexa Top Million Sites support session resumption
  - Google/Cloudflare report a share of approx. 50% of their connections to be established through TLS session resumption (SR)

- Privacy leakage by TLS version 1.2 and below allow a network-based attacker to track users via this mechanism
Opportunities and Limitations of Tracking via TLS SR

- **Opportunities compared to HTTP cookies/ browser fingerprinting**
  - Faster unique identification of a user
  - Tracking via TLS SR cannot be directly detected
  - Lower consumption of bandwidth and computational resources compared to browser fingerprinting

- **Limitations**
  - Browser restarts terminate a tracking period
  - TLS configuration of a browser
    - Session resumption lifetime
    - Feasibility of third-party tracking
Experiments to test Browsers’ default TLS Configuration

- **Measurement of the session resumption lifetime of 48 browsers**
  - Maximum delay between two website visits for which the browser still attempts to establish the new connection through TLS SR

- **Investigating the feasibility of third-party tracking via TLS SR**
Summary on the Browser’s default TLS Configuration

<table>
<thead>
<tr>
<th>Browser</th>
<th>Session Resumption Lifetime</th>
<th>Third-party Tracking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome</td>
<td>1 hour</td>
<td>viable</td>
</tr>
<tr>
<td>Firefox</td>
<td>24 hours</td>
<td>viable</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>10 hours</td>
<td>viable</td>
</tr>
<tr>
<td>Safari</td>
<td>24 hours</td>
<td>viable</td>
</tr>
</tbody>
</table>

Can a tracker extend these tracking periods?
Extending Tracking Periods beyond the TLS SR Lifetime

- Prolongation attack allows a Server to track the user across a chain of PSK’s

Successful TLS 1.3 resumption handshake with issuance of a new pre-shared key (PSK)
Evaluation of the Prolongation Attack

- Simulating users’ browsing behaviour based on a DNS data set
  - Pseudonymized DNS traffic logs of 3862 users over a 60-day period\(^1\)

- Approximating feasible tracking periods from a server perspective
  - Tracking period is extendible if the duration between to website visits is smaller than a given session resumption lifetime

- Estimating the share of permanently trackable user
  - The ratio of users in our data set that can be identified by the server beyond the boundaries of the DNS data set

\[1\]: D. Herrmann et al., Behavior-based tracking: Exploiting characteristic patterns in DNS traffic. (2013)
Feasible Tracking Periods based on the Prolongation Attack

Detailed Values
[ 1 h, 9 h]
[24 h, 8 days]
[48 h, 12 days]
The Share of Permanently Trackable Users

CDF permanently trackable user

Detailed Values
[1 day, 0.01]
[4 days, 0.20]
[7 days, 0.65]

Session resumption lifetime [days]
Countermeasures

- Disable TLS SR if a host must not track a user
  - Potentially impacts temporal and computational performance

- Restrict TLS SR to balance privacy and performance needs of the user
  - Limit lifetime of TLS SR and prevent the prolongation of this lifetime
  - Define the context of a connection (e.g. via browser tabs & visited website) and allow TLS SR only within the same context
  - Use a full handshake instead of the 1-RTT TLS 1.3 SR mode because the number of required round trips is identical
Evaluation of a limited TLS SR lifetime

CDF revisits of websites

Time between two consecutive visits [hours]

Detailed CDF-Values
- [5 min, 0.177]
- [10 min, 0.277]
- [30 min, 0.405]
- [60 min, 0.483]
- [24 h, 0.816]
- [48 h, 0.873]
Conclusion

- Do not depend on user behaviour (e.g. Browser restart) to prevent tracking via TLS SR

- TLS SR should be aligned with legitimate browser-based tracking mechanisms to achieve a better performance versus privacy tradeoff
  - For hosts that legitimately track a user, a longer TLS SR lifetime can be applied to realise more performance gains

- The recommended upper lifetime of TLS 1.3 SR of seven days enables in combination with the prolongation attack to permanently track 65% of users
Thank you

Questions and Answers

Slides available:  www.erik-sy.de/acsac
E-mail: acsac@erik-sy.de

I acknowledge support from the Federal Ministry of Education and Research within the AppPETs project.