Tracking Users across the Web via TLS Session Resumption

Erik Sy, M.Sc.
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)
Opportunities and Limitations of Tracking via TLS SR

- **Opportunities compared to HTTP cookies/ browser fingerprinting**
  - Faster unique identification of a user
  - Lower consumption of bandwidth and computational resources

- **Limitations**
  - Browser restarts terminate a tracking period
  - TLS configuration of a browser
    - Session resumption lifetime
    - Feasibility of third-party tracking
Browser Restarts as a Limitation

- Analysis of reported browser uptime within crash reports (normalized over total browser uptime)
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>Microsoft Edge</td>
<td>10 hours</td>
<td>blocked</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 two 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

- **Browser vendors**
  - Disable third-party tracking via session resumption through sandboxing
  - Reduce TLS SR lifetime to a single page visit or at most six hours
  - Prevent a reset of the resumption lifetime

- **TLS Working Group**
  - Reduce the recommended upper lifetime limit in the draft of TLS 1.3
  - Recommend measures to prevent a reset of the TLS SR lifetime

- **Research Community**
  - Investigate handshake designs based on semi-static Diffie-Hellman key establishment such as OPTLS 1.3 and draft-rescorla-tls13-semistatic-dh
    - Public key is shared within an anonymity group
Conclusion

- TLS SR is a widely-supported mechanism, which allows unique user identification with a low bandwidth, computational and temporal overhead.

- Browser vendors and the TLS working group need to further restrict this privacy problem.

- Countermeasures heal the privacy problem but lead to a performance reduction.
Thank you

Questions and Answers

Slides available: www.erik-sy.de/hotpets
E-mail: hotpets@erik-sy.de
Preprint: Please request pre-print article per email.

I acknowledge support from the Federal Ministry of Education and Research within the AppPETs project.
Backup: When do Users revisit a Website?

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]