Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

2th May 2019
Paderborn University

Enhanced Performance for the encrypted Web through TLS Resumption across Hostnames

Erik Sy

Introduction to TLS resumption

- TLS resumptions allow the communicating peers to mutually validate their identities based on the cryptographic state of a previous TLS session
- Saves expensive cryptographic operations compared to a full handshake where certificates are used to validate identities
- Enables zero round-trip time (0-RTT) connection establishments
- Privacy risk of web tracking[1]
- Resumption tickets are intended for single-use to prevent network attackers to identify connections established by the same client

[1]: Sy et al: Tracking Users across the Web via TLS Session Resumption, ACSAC'18, San Juan, USA

TLS 1.3 recommendation against resumptions across hostnames

- TLS 1.3 allows resumptions across hostnames, if the corresponding hostnames can be validated via the same server certificate

- Blind usage of resumption across hostnames wastes single-use tickets
  - Feature requires signaling to reduce failure rate of resumptions

Proposed TLS 1.3 extension

- Server signals that a group of hostnames mutually support TLS resumptions
  - Presented server certificate needs to be valid for theses hostnames
- SAN-list of certificate can be used to defined this group
  - Adds complexity to the generation of server certificates
  - Helps to avoid resumptions to hostnames for which the cert is not valid
- Extension for the NewSessionTicket frame

Performance evaluation 1/3: TLS 1.3 connection establishments

- Elapsed time

Network latency	Initial	1-RTT resumed	0-RTT resumed
0.3 ms	29.2 ms	6.3 ms	6.6 ms
50 ms	190.1 ms	160.1 ms	109.6 ms
100 ms	340.8 ms	310.3 ms	209.7 ms

- CPU time

Peer	Initial	1-RTT resumed	0-RTT resumed
Server	7.8 ms	2.3 ms	2.6 ms
Client	9.2 ms	2.4 ms	2.5 ms

Performance evaluation 2/3: Loading behavior of the Alexa Top Sites

- Facts on the average website
  - Requires 20.2 TLS connections to different hostnames
  - These hostnames form 9.5 TLS trust groups
    - Results based upon x 509 certificate and feasible TLS resumptions
  - Requires 4.0 sequential full TLS handshakes
    - Page loading time is affected several times by the delay overhead of the TLS connection establishment

Performance evaluation 3/3: Results for an average website

- Converts about 58.7% of the required full TLS handshakes to resumed connection establishments
- Reduces the required CPU time for the TLS connection establishments by about 44%
- Reduces the elapsed time to establish all required TLS connections by up to 30.6%

Privacy considerations

- The proposal enables tracking across hostnames that share the same private key of their server certificate
  - similar linking of user visits is feasible via redirects, hyperlinks, and connection reuse of HTTP/2

- Defense should focus on avoiding long-term tracking via session resumption

Security considerations

- TLS 1.3 allows resumptions across hostnames
  - Requires hostnames to be valid for the presented server certificate
- Security features are similar to HTTP/2 connection reuse
  - Client loads content from different virtual hosts on the same server over the same TLS connection
- Features derived from the TLS initial handshake now apply to a group of hostnames instead of a single hostname
  - Does this practice break the security assumptions of other TLS extensions?

Attack scenario: Self-signed certificates

- Client connects to Eve's server captiveportal.com and receives malicious certificate valid also for example.com
  - server signals session resumptions are feasible for example.com
- a) Client resumes with 0-RTT handshake to example.com, which allows Eve to read early data as a passive network observer
- b) Eve actively responds as example.com and establishes a resumed connection
- Countermeasure: Feature should be deactivated for self-signed certificates

Attack scenario: Pinned server certificates

- Example.com is always served via a pinned certificate. However, www.example.com is misconfigured and signals that issued tickets allow a resumption handshake with example.com

- Client is aware of the pinned certificate for example.com but does not check this requirement before attempting a 0-RTT handshake with the ticked issued by www.example.com
  - Allows www.example.com to read early data intended for example.com which circumvents the pinning

- Countermeasure: Resumptions to hostnames with pinned certificate should use only tickets that are issued within connections using these pinned certificates

Status quo

- IETF actively works on the adoption of this TLS extension
  - Receives support of major browser vendors and online services
- Academic article is still work in progress

Conclusion

- TLS resumption across hostnames provides huge performance benefits for the web
- The impact on the users' privacy is small in a web browsing scenario
- Security considerations make countermeasures necessary with regard to self-signed certificates and resumption handshakes to hostnames with pinned certificates

Thank you

Questions and Answers

E-mail: tls@erik-sy.de

Preprint: https://erik-sy.de/Paper104.pdf