Poster: Leveraging Locality of Reference for Certificate Revocation

Published Paper

Title: Leveraging Locality of Reference for Certificate Revocation

Authors: Luke Dickinson, Trevor Smith, and Kent Seamons
Email: ldickin@sandia.gov, tsmith@isrl.byu.edu, seamons@cs.byu.edu

Date: December 9 - 13, 2019
Venue: Proceedings of the 35th Annual Computer Security Applications Conference (ACSAC '19)
DOI: https://dl.acm.org/doi/10.1145/3359789.3359819

Abstract

X.509 certificate revocation defends against man-in-the-middle attacks involving a compromised certificate. Certificate revocation strategies face scalability, effectiveness, and deployment challenges as HTTPS adoption rates have soared. We propose Certificate Revocation Table (CRT), a new revocation strategy that is competitive with or exceeds alternative state-of-the-art solutions in effectiveness, efficiency, certificate growth scalability, mass revocation event scalability, revocation timeliness, privacy, and deployment requirements. The CRT design assumes that locality of reference applies to the certificates accessed by an organization. The CRT periodically checks the revocation status of X.509 certificates recently used by the organization. Pre-checking the revocation status of certificates the clients are likely to use avoids the security problems of on-demand certificate revocation checking.

To validate both the effectiveness and efficiency of our approach, we simulated a CRT using 60 days of TLS traffic logs from Brigham Young University to measure the effects of actively refreshing revocation status information for various certificate working set window lengths. A working set window size of 45 days resulted in an average of 99.86% of the TLS handshakes having revocation information cached in advance. The CRT storage requirements are small. The initial revocation status information requires downloading a 6.7 MB file, and subsequent updates require only 205.1 KB of bandwidth daily. Updates that include only revoked certificates require just 215 bytes of bandwidth per day.

Acknowledgment

We thank the Brigham Young University Office of Information Technology for their help in gaining access to outbound TLS traffic for the university campus network. We thank Daniel Zappala, Casey Deccio, and the anonymous reviewers for their helpful comments and feedback. This research is supported in part by the National Science Foundation under Grants No. CNS-1528022 and CNS-1816929.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government. SAND No. 2020-0533 C.

Leveraging Locality of Reference for Certificate Revocation

Luke Dickinson*, Trevor Smith‡, Kent Seamons‡
Sandia National Laboratories*, Brigham Young University‡

Seven Challenges Facing Certificate Revocation

1. Effectiveness during an Active Attack
2. Client Bandwidth Costs
3. Future Bandwidth Costs due to Certificate Growth
4. Mass Revocation Event Scalability
5. Revocation Timeliness
6. Exposure of Client Traffic Patterns
7. Deployment Requirements and Incentives

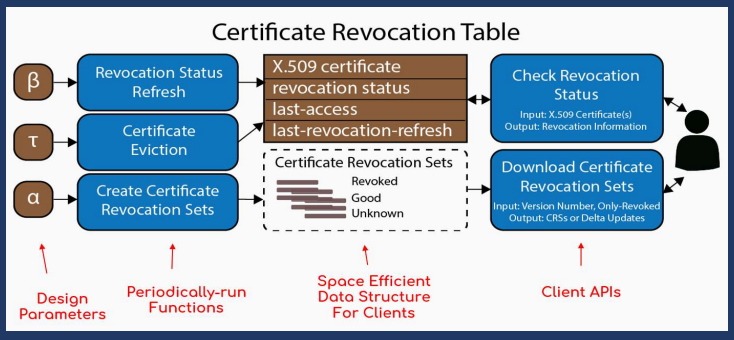
Solution: a new revocation strategy designed to cache revocation information at the organization level to be re-used by all clients in the organization

Certificate Revocation Table (CRT)

Certificate Working Set – Recent certificates used by an organization

Hypothesis: majority of certificates accessed in near future **W(t + α, α)** will reuse certificates seen in the recent past **W(t, τ)**, if α is small.

- The CRT contains an organization's certificate working set (both revoked and non-revoked)
- Periodically the CRT will refresh status information, evict unused certificates, and create a data structure for clients
- Clients can download a local copy of the CRT to check revocation status



Design Strengths:

- Design parameters (τ, β, α) give flexibility to support different types of organizations and clients
- Incentive Alignment: network administrators assume control, responsibility, and cost burdens while local users receive the benefits

Measurement Study

Analyze TLS logs at BYU for April-June 2018

- 33,000+ students
- 4,144,404,123 TLS handshakes
- 112 revoked certificates in 228,427 handshakes (0.005%)

Simulated impact of CRT

- 99%+ of handshakes had cached revocation information
- Decreasing bandwidth as window size increases
- Small fraction of overall certificate space

τ: working set window length	TLS handshakes with known status		Certificates with known status		CRT total certificates	CRT idle certificates	Daily network bandwidth		Total storage	
	Any Certificate	Revoked Certificates	Any Certificate	Revoked Certificates			CRT	End client	CRT	End client
1 day	99.52%	96.55%	60.63%	77.42%	56,957.83	40.73%	72.31 MB	747.31 KB	220.27 MB	1.71 MB
5 days	99.71%	98.82%	80.01%	92.45%	127,702.09	42.87%	162.12 MB	401.45 KB	493.85 MB	3.83 MB
10 days	99.73%	99.59%	85.28%	94.84%	180,355.30	45.82%	228.97 MB	302.39 KB	697.47 MB	5.41 MB
15 days	99.73%	99.59%	87.34%	95.22%	223,133.91	48.95%	283.28 MB	265.04 KB	862.90 MB	6.70 MB
20 days	99.73%	99.55%	88.38%	95.20%	261,310.38	51.72%	331.74 MB	245.00 KB	1,010.54 MB	7.86 MB
25 days	99.76%	99.49%	89.34%	94.86%	297,767.51	54.15%	378.03 MB	229.07 KB	1,151.52 MB	8.96 MB
30 days	99.83%	99.65%	90.05%	95.90%	332,136.97	N/A	421.66 MB	216.17 KB	1,284.44 MB	10.00 MB
35 days	99.84%	99.67%	90.48%	96.16%	363,148.84	N/A	461.03 MB	209.08 KB	1,404.36 MB	10.94 MB
40 days	99.82%	99.67%	90.35%	95.96%	392,611.35	N/A	498.43 MB	208.71 KB	1,518.30 MB	11.83 MB
45 days	99.86%	99.61%	90.91%	95.28%	423,032.13	N/A	537.05 MB	205.09 KB	1,635.94 MB	12.75 MB

Comparison to Other Strategies

Certificate Revocation Table is competitive with or exceeds alternative strategies for each of the seven challenges facing certificate revocation.

Lowest deployment requirements with:

- Over 99% of TLS handshakes had revocation information cached on clients
- Revocation timeliness of 1-2 days
- Low client bandwidth - the only-revoked option requires just 200 bytes per day, which is three orders of magnitude smaller than other strategies

	TLS Handshakes Protected	Client Bandwidth Consumption	Global Certificate Growth Scalability	Mass Revocation Event Scalability	Revocation Timeliness	Privacy Preserving	Deployment Requirements
OCSP Must-Staple	100%†	1.3 KB per TLS handshake [24]	Minimal BG	No Changes	4 Days	Yes	Very High
CRLSets	Unknown‡	250 KB per day	Reduced Protection	Minimal Protection	1–2 Days	Yes	Deployed
CRLite (Jan. 2017)*	100%	Initially 10 MB; 580 KB per day	Significant BG	Significant BG	1–2 Days	Yes	High
CRLite (Mar. 2018)*	100%	Initially 18 MB; Unknown per day	Significant BG	Significant BG	1–2 Days	Yes	High
CRT	99.86%	Initially 6.71 MB; 205 KB per day	Minimal BG	Minimal BG	1–2 Days	Yes	Medium
CRT (only revoked)	99.86%	Initially 1.92 KB; 0.21 KB per day	Minimal BG	Significant BG	1–2 Days	Yes	Medium

(BG = Bandwidth Growth)

Full paper presented at Annual Computer Security Applications Conference (ACSAC 2019)

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2020-0533 C

This material is based on work supported by the National Science Foundation under Grants No. CNS-1528022 and CNS-1816929.