SAND2019-14356C

Leveraging Locality of Reference for Certificate Revocation

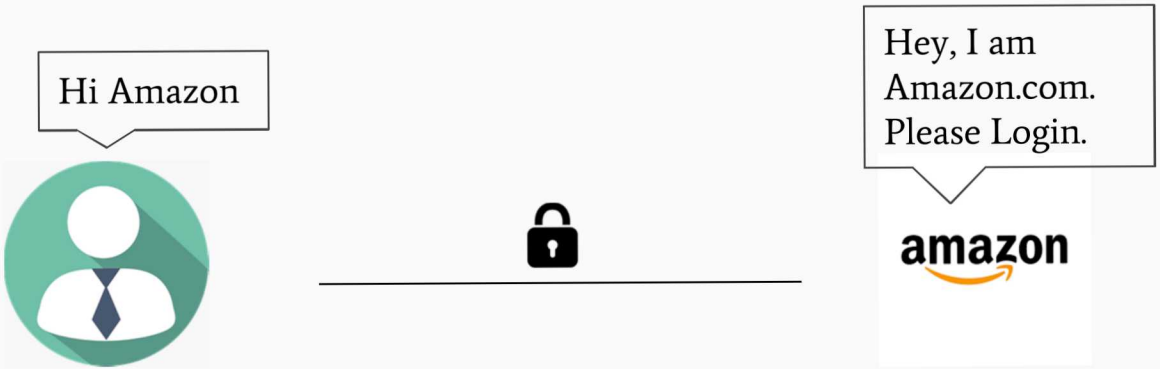
Luke Dickinson, Sandia National Laboratories
Trevor Smith, Brigham Young University
Kent Seamons, Brigham Young University

35th Annual Computer Security Applications Conference (ACSAC)
Condado Plaza Hilton, San Juan, Puerto Rico
December 9th – 13th, 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.

X.509 Certificates

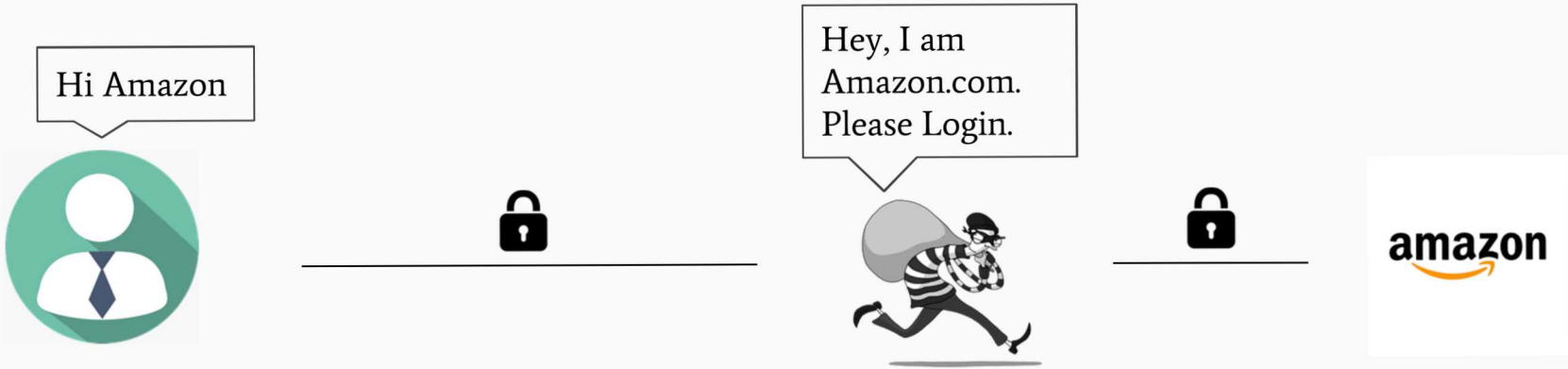
Certificates are used to authenticate TLS communication between clients and servers.



Certificate Revocation

A malicious actor with access to the private key of a certificate can impersonate another party undetected.

Compromised certificates can be revoked to help clients avoid these connections.



Seven Challenges of Certificate Revocation

We identify seven challenges facing certificate revocation strategies today.

These challenges have limited clients' ability to detect a revoked certificate.

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

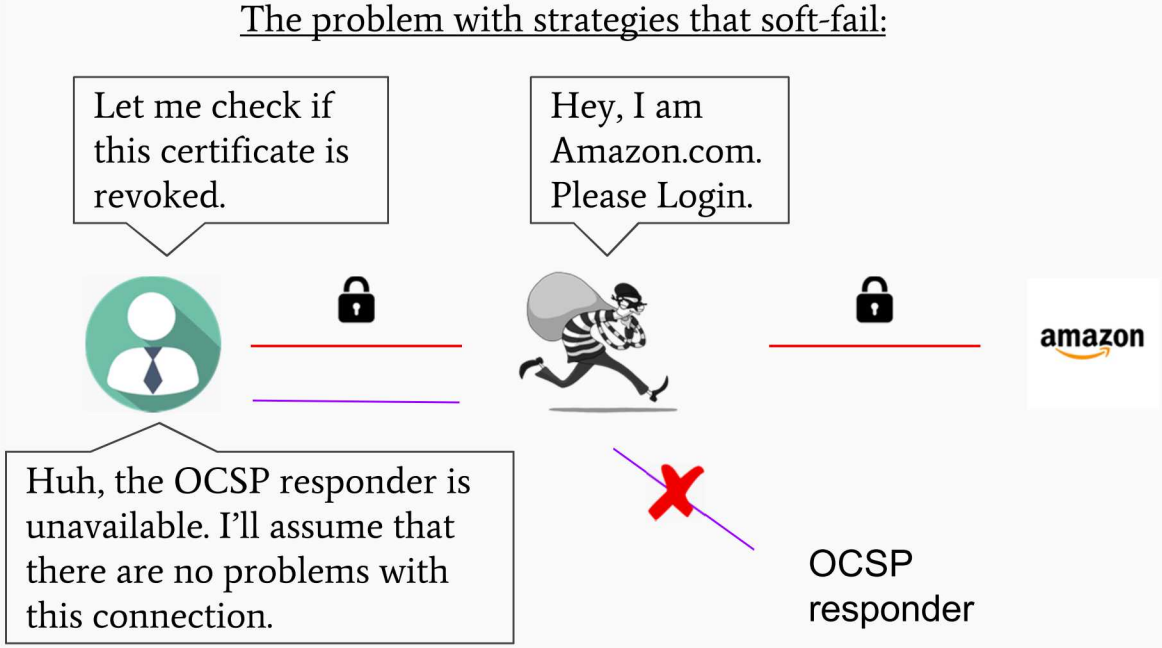
Seven Challenges of Certificate Revocation

We identify seven challenges facing certificate revocation strategies today.

These challenges have limited clients' ability to detect a revoked certificate.

1. Effectiveness during an Active Attack

"Soft-fail revocation checks are like a seat-belt that snaps when you crash." (Langley 2012)



Seven Challenges of Certificate Revocation

We identify seven challenges facing certificate revocation strategies today.

These challenges have limited clients' ability to detect a revoked certificate.

2. Client Bandwidth Costs

Many clients are dissuaded to participate. (Liu et al. 2015)

Seven Challenges of Certificate Revocation

We identify seven challenges facing certificate revocation strategies today.

These challenges have limited clients' ability to detect a revoked certificate.

3. Future Bandwidth Costs due to Certificate Growth

There has been a order of magnitude increase in live, trusted certificates from Jan 2017 to Nov 2019.

30 Million -> 407 Million

Live, trusted certificates globally

Seven Challenges of Certificate Revocation

We identify seven challenges facing certificate revocation strategies today.

These challenges have limited clients' ability to detect a revoked certificate.

4. Mass Revocation Event Scalability

"The community needs to develop methods for scalable revocation that can gracefully accommodate mass revocation events, as seen in the aftermath of Heartbleed."

(Durumeric et al. 2014)

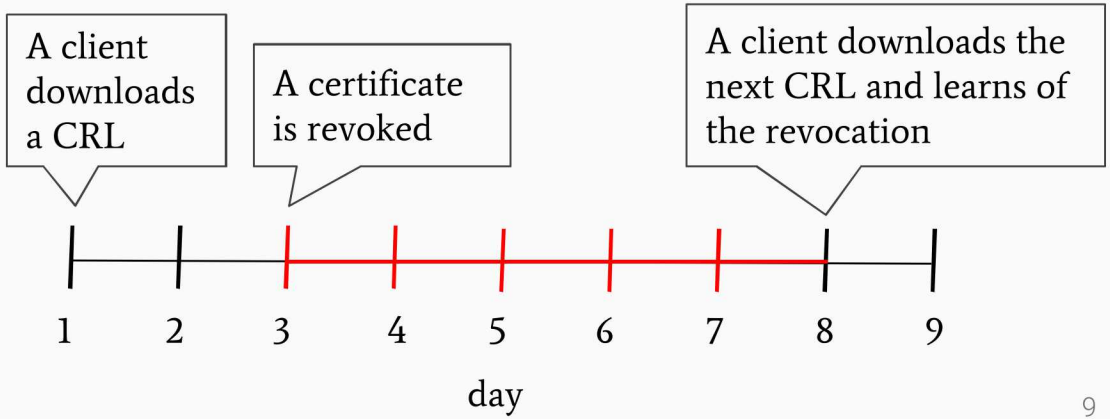
Seven Challenges of Certificate Revocation

We identify seven challenges facing certificate revocation strategies today.

These challenges have limited clients' ability to detect a revoked certificate.

5. Revocation Timeliness

Clients may not be able to detect a certificate has been revoked until days after the revocation has occurred.



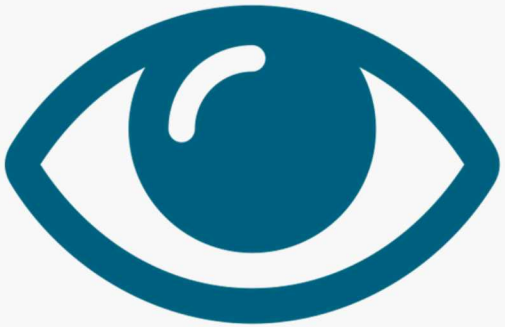
Seven Challenges of Certificate Revocation

We identify seven challenges facing certificate revocation strategies today.

These challenges have limited clients' ability to detect a revoked certificate.

6. Exposure of Client Traffic Patterns

Some revocation strategies share detailed client traffic patterns to third-parties.



Seven Challenges of Certificate Revocation

We identify seven challenges facing certificate revocation strategies today.

These challenges have limited clients' ability to detect a revoked certificate.

7. Deployment Requirements and Incentives

Other strategies require significant infrastructure changes, require participation and additional costs by CAs and/or third parties, or exposing new attack surfaces.

Roles, Responsibilities, and Costs of:

- Certificate Authorities
- Website Administrators
- End-clients
- Other Third-parties

Introduction and Maintenance of Hardware for:

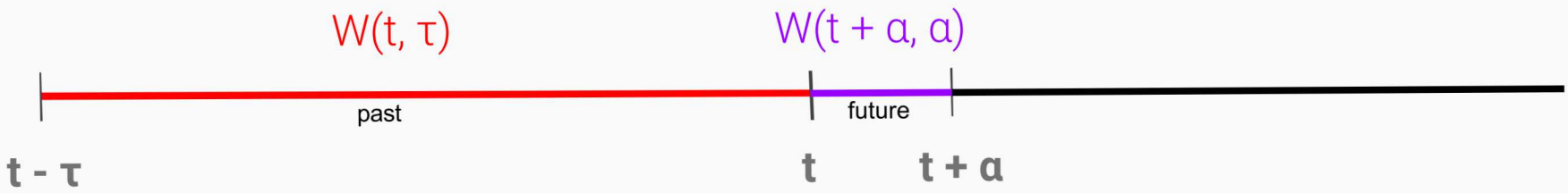
- End-clients
- Internet Infrastructure

Our Solution

We Take Advantage of Certificate Working Sets

A certificate working set $W(t, \tau)$ of an organization is the collection of all certificates used by the organization over the period of time $t - \tau$ to t.

We hypothesize that a majority of certificates in a $W(t + \alpha, \alpha)$ will reuse certificates seen in a $W(t, \tau)$, if α is small.

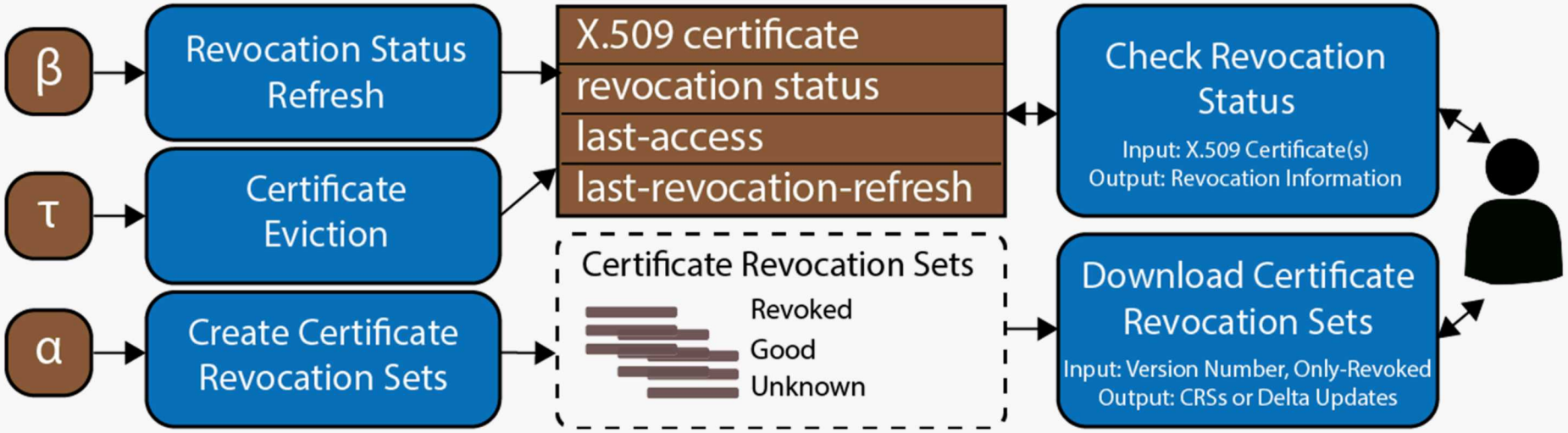


Certificate Revocation Table

We use a Certificate Revocation Table (CRT) to capture an organization's certificate working set.

The rest of the design is used to collect certificate usage information, manage the CRT, and deliver revocation information to client.

Certificate Revocation Table



Design Parameters

Periodically-run Functions

Space Efficient Data Structure For Clients

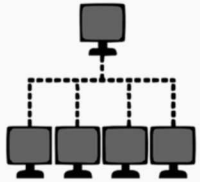
Client APIs

Strengths of CRT

Enables network administrators to protect their own clients without third-party support.

Revocation information is available for websites regularly visited in a population.

Design parameters (τ, β, α) give flexibility to support different types of organizations and clients.



Deployment Alternatives

- Middlebox / Network Gateway
- Cloud service
- Distributed Third Parties

Measurement Study

Methodology

Coordinating with the network administrators at Brigham Young University, we obtained TLS logs generated by the Bro Network Security Monitor from April to June 2018.

Because of the private nature of this data, these logs were only processed on the network administrator owned devices and all results exported were anonymized.

We used these logs to measure the effects of running BYU-shared CRT.

Results: BYU-shared CRT

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

Increasing toward 100%

400,000 certificates = 0.13% of global space

Decreasing because of delta updates

Comparison to Alternative State-of-the-art Solutions

OCSP Must-Staple, CRLSets, and CRLite

Comparison to Other Strategies

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)

Close to 100%, adjustable with parameter choices

Small bandwidth requirements (esp. only revoked)

Handles global certificate growth and revocation well

Low barrier-to-entry requirements

Comparison to Other Strategies

While 100% is protection possible, current adoption rates (0.03%) protect fewer TLS handshakes

The number of globally live X.509 certificates was 30 Million in January 2017 and 84 Million in March 2018

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)

We have no way of measuring CRLSets for TLS Handshakes Protected.
CRLSets contain a fixed number of revoked certificates (roughly 40,000).
As the certificate spaces grows, the percentage of unaccounted revocations grows.

Contributions

Analyzed related work to describe seven challenges facing current revocation strategies

Applied the concept of working sets to improve certificate revocation

Provided the design of Certificate Revocation Table

Performed a measurement study with real traffic data to analyze the strengths and weaknesses of Certificate Revocation Table

Future Work

Anticipating certificate renewal

Early removal of irrelevant certificates

Exploring design parameters α and β

Experiments using alternative deployment scenarios:

- Single client
- Home network
- General region
- Smart grid AMI network

Conclusion

Using an organization-shared CRT is competitive with or exceeds alternative state-of-the-art solutions for each of the seven challenges of certificate revocation.

Questions?