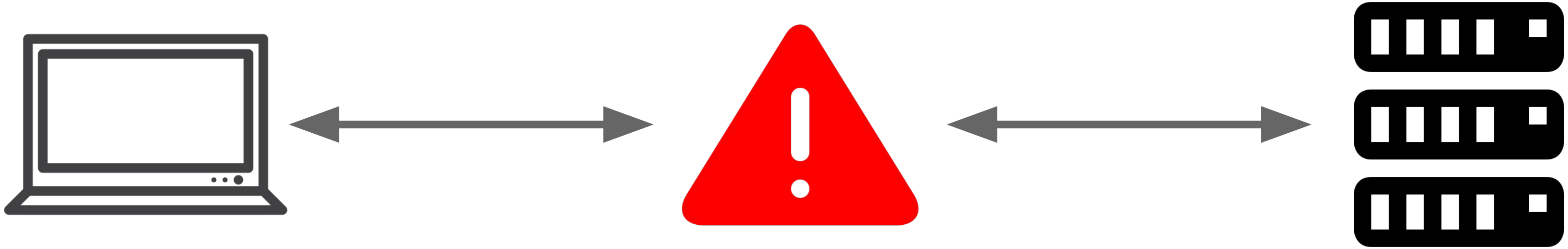
Let’s Revoke

Scalable Global Certificate Revocation

Trevor Smith - Luke Dickinson - Kent Seamons
Brigham Young University

Reason for Revocation

Public key infrastructure prevents Man-in-the-Middle attacks



Revocation protects clients from compromised certificates

Without revocation, these attacks would go undetected

Traditional Implementations

- Certificate Revocation Lists (CRLs)
  - Lists of Revoked Certificates
  - Include Revocation Dates and Reasons

- Online Certificate Status Protocol (OCSP)
  - On Demand Revocation Status Request to the CA

Efficient Revocation Checking

- CRLs and OCSP are Relatively Inefficient
- No Mobile Browsers Perform Revocation Checking

Heartbleed Vulnerability (2014)

- Compromised Many Certificates
- Increased Revocation Percentage to 11%
- Cost Cloudflare an Additional $400,000 per Month

Efficient Revocation Checking

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

- **Zakir Durumeric et al. (2014)**

Soft-Fail Revocation Checking

- Soft Failing
  - Accepting Certificates with Unknown Revocation Statuses
  - Primarily used by CRLs and OCSP to Avoid Availability Issues
- Active Attackers Can Trivially Block Revocation Requests
  - Man-in-the-Middle Attacks are Undetected

Soft-Fail Revocation Checking

“Soft-fail revocation checks are like a seat-belt that snaps when you crash. Even though it works 99% of the time, it's worthless because it only works when you don't need it.”

- **Adam Langley (2012)**

Modern Solutions

- CRLSets
  - More Efficient Version of CRLs
  - Removes Unnecessary Data
  - Selective Revocation Coverage (~ 40,000 Revocations)

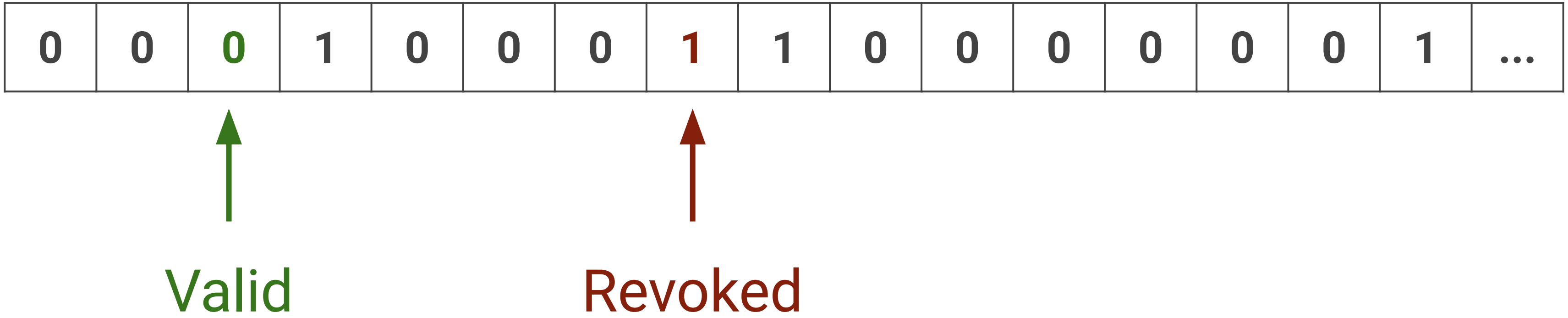
- CRLite
  - Cascading Bloom Filter
  - Revocation Status Aggregator
  - Efficient Global Revocation Coverage

Let’s Revoke

- Inspired by CRLite
- Uses Bit Vectors to Improve Efficiency
- Eliminates Need for an Aggregator
- Maintains Global Revocation Coverage

Certificate Revocation Vectors (CRVs)

- Dynamically-Sized Bit Vectors
- Each Bit Represents a Revocation Status
- “1” Indicates the Certificate is Revoked



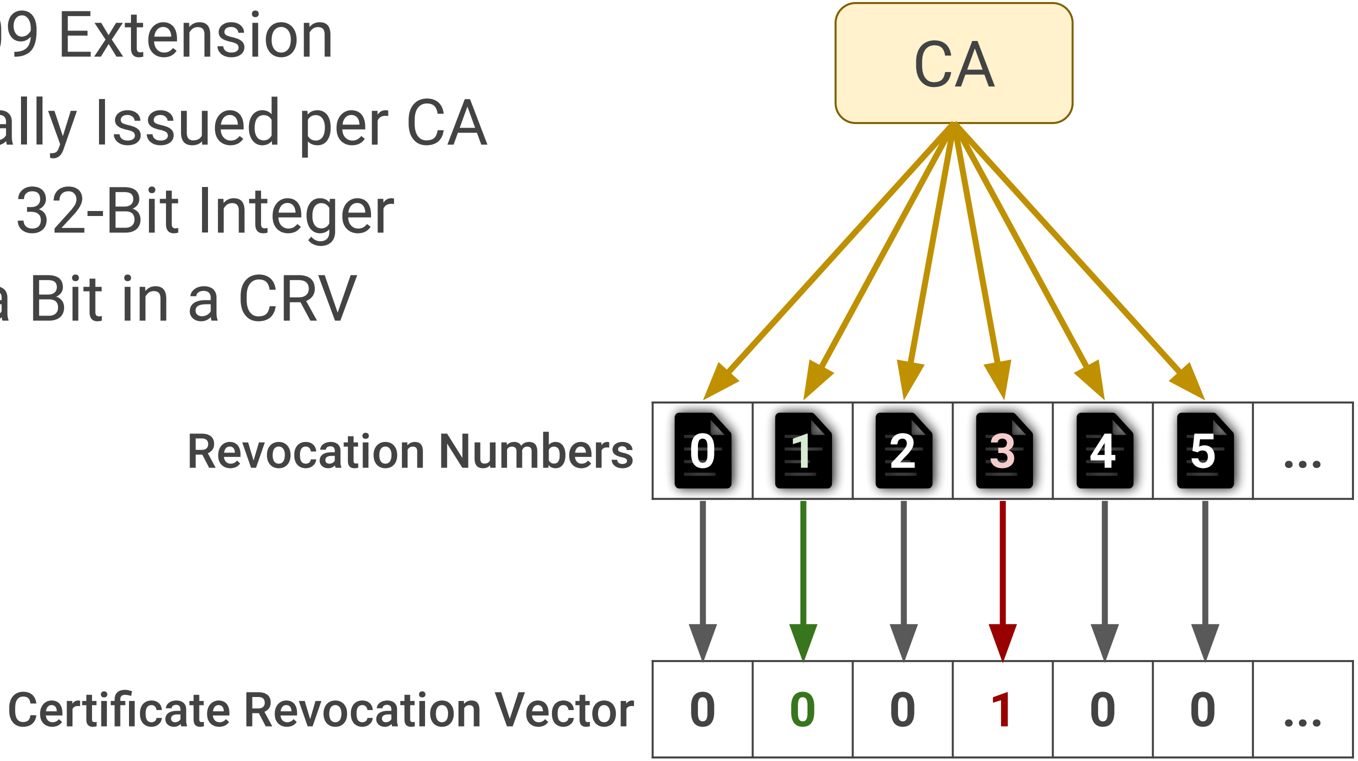
0	0	0	1	0	0	0	1	1	0	0	0	0	0	0	1	...

Valid

Revoked

Revocation Numbers

- New X.509 Extension
- Sequentially Issued per CA
- Unsigned 32-Bit Integer
- Index of a Bit in a CRV



CA

Revocation Numbers	0	1	2	3	4	5	...
Certificate Revocation Vector	0	0	0	1	0	0	...

Revocation IDs

- Separate CRVs based on Expiration Date

		Revocation Numbers								
		0	1	2	3	4	5	6	7	...
CRV IDs	CA 1: January 1, 2021	0	0	1	0	0	0	0	0	...
	CA 1: February 1, 2021	0	0	0	0	1	0	0	0	...
	CA 2: January 1, 2021	0	0	0	0	0	0	1	0	...
	CA 2: February 1, 2021	0	0	0	1	0	0	0	0	...

CRV Update Process

- ○ Expand CRV as Necessary
- ○ Set the Corresponding Bit

🟩 New Unrevoked Bits

🟨 New Revoked Bits

🟥 Old Revoked Bits

Revocation Numbers

	0	1	2	3	4	5	6	7	...
Initially Empty CRV									
1. Revoke 3	🟩 0	🟩 0	🟩 0	🟨 1					
2. Revoke 7	0	0	0	🟥 1	🟩 0	🟩 0	🟩 0	🟨 1	
3. Revoke 2	0	0	🟨 1	🟥 1	0	0	0	🟥 1	
3. Revoke 0	🟨 1	0	🟥 1	🟥 1	0	0	0	🟥 1	

Client Updates

- Updated CRVs Must be Sent to Clients

0	0	0	0	1	0	0	1	...	Original CRV
0	1	1	0	1	0	0	1	...	Updated CRV

- 3 Methods for Sending Updates

{1, 2} **ADD** - Send List of New RNs

0	1	1	0	0	0	0	0	...	**OR** - Send CRV with Only New RNs
0	1	1	0	1	0	0	1	...	**NEW** - Send Current CRV

Advantages

- Revocation Number Enable Efficiency
  - Smaller Identifier - 32 bits vs 128-256 bits
- CRVs are Computationally Efficient
  - Querying Revocation Statuses
  - Updating Stored Statuses
- CRVs are Highly Compressible
  - Saves Network Bandwidth
  - Saves Client Storage

Limitations

- Not Backwards Compatible
  - New Certificate Field
- Only Provides Revocation Statuses
  - No Revocation Date
  - No Revocation Reason

However, CRVs can be used in tandem with other revocation systems that address these limitations

Comparing Revocation Systems

○ Compared Let’s Revoke to Other Revocation Systems

○ Used 6 Criteria Outlined in CRLite Proposal

1. Efficiency
2. Timeliness
3. Failure Model
4. Privacy
5. Deployability
6. Auditability

Efficiency Comparison

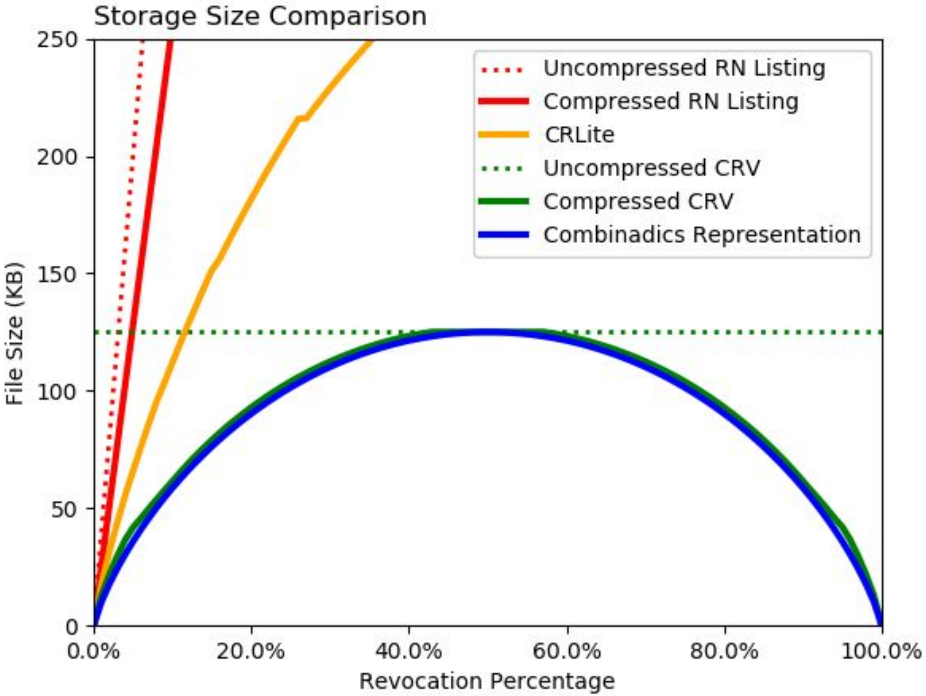
- Let’s Revoke Designed for Efficiency
  - Minimize Client Storage
  - Minimize Network Bandwidth
- Compared Storage Requirements
- Compared Bandwidth Requirements
- Difficult to Directly Compare Some Strategies
  - Compared an Approximated Model of these Strategies

Efficiency: Simulation

1. RN Listing Strategy
   - A highly efficient version of CRLs
2. CRLite
   - State of the art for efficiency
3. CRVs
4. Combinadics Representation
   - Lower bound for representing a combination of values
   - Not used because computationally expensive

Efficiency: Storage Results

- CRLite is more efficient than RN Listing
- CRVs are more efficient than CRLite
- CRVs approach the lower bound
- **CRVs are near optimal for storing revocation statuses**



1 Million Certificates

Efficiency: Bandwidth Results

- Measured Bandwidth for:
  - 100 Million Certificates
  - 2% Revocation Rate
  - 2 Million Revocations

RN Listing	114 KB per Day
CRLite	408 KB per Day
CRVs	114 KB per Day

Note: CRLSets, which only cover around 40,000 revocations, require 250KB for daily updates.

Six Criteria Summary

	Efficiency	Timeliness	Failure Model	Privacy Preserving	Deployability	Auditability
CRLs	173 KB per CRL	7 Days	Soft	Yes	Deployed	Yes
OCSP	1.3 KB per request	4 Days	Soft	No	Deployed	Yes
CRLSets	250 KB per day	1 Day	Soft	Yes	Deployed	No
RN Listing	* 5.1 MB + 114 KB per day	1 Day	Hard	Yes	Incremental	Yes
CRLite	* 3.1 MB + 408 KB per day	1 Day	Hard	Yes	Incremental	Yes
Let’s Revoke	* 2.2 MB + 114 KB per day	1 Day	Hard	Yes	Incremental	Yes

* Efficiency measured using 100 Million Certificates and 2% Revocation Rate

Internet-Wide Scan

- Used List of all Trusted Certificates from Censys.io (March 21, 2018)
- Acquired all Revocation Statuses using CRLs and OCSP.

	Trusted Certificates	Valid Status	Revoked Status	Unknown Status
From CRL	26,772,989	25,983,705	789,284 **(2.90%)**	0
OCSP Let's Encrypt	53,196,388	52,946,338	250,050 **(0.47%)**	0
OCSP Symantec	2,483,288	2,446,508	36,780 **(1.48%)**	0
OCSP DigiCert	1,157,956	1,149,840	8,116 **(0.70%)**	0
OCSP Other	542,641	541,807	807 **(0.15%)**	27
Total	84,153,262	83.068,198	1,085,037 **(1.29%)**	27

Results-Based Simulation

- 42 CA Entities
- 84.1 Million Certificates
- 1.29% Revocation Percentage
- 0.007% New Revocations per Day

5.0 MB Storage

25 KB Bandwidth per Day

The Google home page requires 400 KB of bandwidth

Results-Based Mass Revocation Simulation

- 42 CA Entities
- 84.1 Million Certificates
- 10.0% Revocation Percentage
- 0.06% New Revocations per Day

10.8 MB Storage

150 KB Bandwidth per Day

Viability Simulations

Certificates	Revocation Percentage	Compressed Storage	Uncompressed Storage	Daily Update Bandwidth
100 Million	1%	1.3 MB	12.5 MB	62.6 KB
100 Million	10%	6.2 MB	12.5 MB	429.2 KB
1 Billion	1%	12.2 MB	125 MB	611.5 KB
1 Billion	10%	60.1 MB	125 MB	4.1 MB
10 Billion	1%	121.3 MB	1.25 GB	7.4 MB
10 Billion	10%	605 MB	1.25 GB	41.5 MB

1 Large CA with 100 CRVs

Takeaways

Efficient Revocation Checking is Important!

- Rapidly Increasing Certificate Space
  - January 2017: 30 Million Certificates
  - January 2020: 434 Million Certificates
- Enable Revocation Checking in Constrained Environments
  - Mobile Devices
  - IoT Devices

Contact Info: tsmith@isrl.byu.edu