Let’s Revoke
Scalable Global Certificate Revocation

Trevor Smith - Luke Dickinson - Kent Seamons
Brigham Young University
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
“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 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 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
## Revocation IDs

- Separate CRVs based on Expiration Date

<table>
<thead>
<tr>
<th>CRV IDs</th>
<th>Revocation Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA 1: January 1, 2021</td>
<td>0 0 1 0 0 0 0 0 ...</td>
</tr>
<tr>
<td>CA 1: February 1, 2021</td>
<td>0 0 0 0 1 0 0 0 ...</td>
</tr>
<tr>
<td>CA 2: January 1, 2021</td>
<td>0 0 0 0 0 0 1 0 ...</td>
</tr>
<tr>
<td>CA 2: February 1, 2021</td>
<td>0 0 0 1 0 0 0 0 ...</td>
</tr>
</tbody>
</table>
CRV Update Process

- Expand CRV as Necessary
- Set the Corresponding Bit

Initially Empty CRV

New Unrevoked Bits

New Revoked Bits

Old Revoked Bits

Revocation Numbers

1. Revoke 3

2. Revoke 7

3. Revoke 2

3. Revoke 0
Client Updates

- Updated CRVs Must be Sent to Clients

Original CRV

```
0 0 0 0 1 0 0 1 ...
```

Updated CRV

```
0 1 1 1 0 1 0 0 1 ...
```

- 3 Methods for Sending Updates

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

```
0 1 1 1 0 0 0 0 0 ...
```

OR - Send CRV with Only New RNs

```
0 1 1 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

<table>
<thead>
<tr>
<th></th>
<th>RN Listing</th>
<th>CRLite</th>
<th>CRVs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>114 KB per Day</td>
<td>408 KB per Day</td>
<td>114 KB per Day</td>
</tr>
</tbody>
</table>

**Note:** CRLSets, which only cover around 40,000 revocations, require 250KB for daily updates.
# Six Criteria Summary

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

* 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.

<table>
<thead>
<tr>
<th></th>
<th>Trusted Certificates</th>
<th>Valid Status</th>
<th>Revoked Status</th>
<th>Unknown Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>From CRL</td>
<td>26,772,989</td>
<td>25,983,705</td>
<td>789,284 (2.90%)</td>
<td>0</td>
</tr>
<tr>
<td>OCSP Let’s Encrypt</td>
<td>53,196,388</td>
<td>52,946,338</td>
<td>250,050 (0.47%)</td>
<td>0</td>
</tr>
<tr>
<td>OCSP Symantec</td>
<td>2,483,288</td>
<td>2,446,508</td>
<td>36,780 (1.48%)</td>
<td>0</td>
</tr>
<tr>
<td>OCSP DigiCert</td>
<td>1,157,956</td>
<td>1,149,840</td>
<td>8,116 (0.70%)</td>
<td>0</td>
</tr>
<tr>
<td>OCSP Other</td>
<td>542,641</td>
<td>541,807</td>
<td>807 (0.15%)</td>
<td>27</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>84,153,262</strong></td>
<td><strong>83,068,198</strong></td>
<td><strong>1,085,037 (1.29%)</strong></td>
<td><strong>27</strong></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Certificates</th>
<th>Revocation Percentage</th>
<th>Compressed Storage</th>
<th>Uncompressed Storage</th>
<th>Daily Update Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 Million</td>
<td>1%</td>
<td>1.3 MB</td>
<td>12.5 MB</td>
<td>62.6 KB</td>
</tr>
<tr>
<td>100 Million</td>
<td>10%</td>
<td>6.2 MB</td>
<td>12.5 MB</td>
<td>429.2 KB</td>
</tr>
<tr>
<td>1 Billion</td>
<td>1%</td>
<td>12.2 MB</td>
<td>125 MB</td>
<td>611.5 KB</td>
</tr>
<tr>
<td>1 Billion</td>
<td>10%</td>
<td>60.1 MB</td>
<td>125 MB</td>
<td>4.1 MB</td>
</tr>
<tr>
<td>10 Billion</td>
<td>1%</td>
<td>121.3 MB</td>
<td>1.25 GB</td>
<td>7.4 MB</td>
</tr>
<tr>
<td>10 Billion</td>
<td>10%</td>
<td>605 MB</td>
<td>1.25 GB</td>
<td>41.5 MB</td>
</tr>
</tbody>
</table>

1 Large CA with 100 CRVs
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