An End-to-End Measurement of Certificate Revocation in the Web’s PKI

Yabing Liu*, Will Tome*, Liang Zhang*, David Choffnes*, Dave Levin†, Bruce Maggs‡, Alan Mislove*, Aaron Schulman§, Christo Wilson*

*Northeastern University †University of Maryland
‡Duke University and Akamai Technologies §Stanford University
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?

Browser

Website

Certificate Authority
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?
Certificate revocation

What happens when a certificate is no longer valid?
Certificate revocation

What happens when a certificate is no longer valid?
Certificate revocation

What happens when a certificate is no longer valid?

Browser

Certificate Authority

Attacker
Certificate revocation

What happens when a certificate is no longer valid?
Certificate revocation

What happens when a certificate is no longer valid?
Certificate revocation

What happens when a certificate is no longer valid?
Certificate revocation

What happens when a certificate is no longer valid?

Periodically pull / query (CRL) (OCSP)

Certificate Authority

Please revoke
Certificate revocation

What happens when a certificate is no longer valid?

Periodically pull / query (CRL) (OCSP)

Please revoke

Certificate Authority

Browser

Attacker
Certificate revocation responsibilities

 Administrators must **revoke certificates** when keys are compromised

 Certificate authorities must **publish revocations** as quickly as possible

 Browsers must **check revocation status** on each connection

 **This talk:**
 Do these entities do what they need to do?
Outline

Website admin behavior
  e.g., what is the frequency of revocation?

Certificate authorities behavior
  e.g., how CAs serve revocations?

Client behavior
  e.g., do browsers check revocations?
Dataset

Rapid7 IPv4 scans

38M certs (~1/wk for 18mos)
Dataset

Rapid7 IPv4 scans

38M certs (~1/wk for 18mos)

38M certs

Non-CA

1,946 certs

CA

classify
Dataset

Rapid7 IPv4 scans
38M certs
(~1/wk for 18mos)

38M certs
Non-CA
1,946 certs

CA

validate

Leaf Set
5M valid certs

classify
Validate Leaf Set

5M valid certs

Download revocation information daily

38M certs (~1/wk for 18mos)

38M certs

Non-CA

CA

1,946 certs

Leaf Set

Rapid7 IPv4 scans
How frequently are certificates revoked?
How frequently are certificates revoked?

Significant fraction of certificates revoked
1% in steady state; more than 8% after Heartbleed
How frequently are certificates revoked?

Over 0.5% advertised certificates are revoked
Website admins failed to update their servers
CRLs, OCSP, and OCSP Stapling
CRLs, OCSP, and OCSP Stapling
CRLs, OCSP, and OCSP Stapling
CRLs, OCSP, and OCSP Stapling

Browser

Certificate Authority

Website

Certificate

Certificate

Certificate

Certificate

Certificate

Certificate

Certificate

Certificate

Certificate

Certificate

Certificate

Certificate

Certificate
Cost of obtaining CRLs
Cost of obtaining CRLs

CDF

76MB Apple CRL

CRL Size (KB)
Cost of obtaining CRLs

Most CRLs small, but large CRLs downloaded more often
Result: 50% of certs have CRLs larger than 45KB
## CRLs from different CAs

<table>
<thead>
<tr>
<th>CA</th>
<th>Unique CRLs</th>
<th>Total Certificates</th>
<th>Revoked Certificates</th>
<th>Avg. CRL size (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>GoDaddy</td>
<td>322</td>
<td>1,050,014</td>
<td>277,500</td>
<td>1,184.0</td>
</tr>
<tr>
<td>RapidSSL</td>
<td>5</td>
<td>626,774</td>
<td>2,153</td>
<td>34.5</td>
</tr>
<tr>
<td>Comodo</td>
<td>30</td>
<td>447,506</td>
<td>7,169</td>
<td>517.6</td>
</tr>
<tr>
<td>PositiveSSL</td>
<td>3</td>
<td>415,075</td>
<td>8,177</td>
<td>441.3</td>
</tr>
<tr>
<td>Verisign</td>
<td>37</td>
<td>311,788</td>
<td>15,438</td>
<td>205.2</td>
</tr>
</tbody>
</table>

CAs use only a small number of CRLs.
CRLs, OCSP, and OCSP Stapling
CRLs, OCSP, and OCSP Stapling
CRLs, **OCSP**, and OCSP Stapling

- **Browser**
- **Certificate Authority**
- **Website**

The diagram illustrates the interaction between a browser, a website, and a certificate authority, highlighting the use of CRLs, OCSP, and OCSP stapling in ensuring secure communication.
CRLs, OCSP, and OCSP Stapling

Browser

Certificate Authority

Certificate

Website

Certificate

Certificate

Certificate

Certificate
CRLs, OCSP, and OCSP Stapling
OCSP prevalence

Fraction of New Certificates with Revocation Information

Date Certificate Issued

CRL

OCSP
OCSP prevalence

RapidSSL begins supporting OCSP

OCSP now universally supported
CRLs, OCSP, and OCSP Stapling
CRLs, OCSP, and OCSP Stapling

Browser

Website

Certificate Authority

✗ Certificate

✔ Certificate
CRLs, OCSP, and OCSP Stapling
Limited OCSP Stapling Support

- IPv4 TLS Handshake scans by University of Michigan on 3/28/15
  - Every IPv4 server on port 443
  - Look for OCSP stapling support

- 2.2M valid certificates
  - 5.19% served by at least one server supports OCSP Stapling
  - 3.09% served by servers that all support OCSP Stapling

Website admins rarely enable OCSP Stapling
Website admin behavior
  e.g., revocation is common ~8%

Certificate authorities behavior
  e.g., high cost in distributing revocation info

Client behavior
  e.g., do browsers check revocations?
Website admin behavior
  e.g., revocation is common ~8%

Certificate authorities behavior
  e.g., high cost in distributing revocation info

Client behavior
  e.g., do browsers check revocations?
What’s the concern of browsers?

Browser → Website (Certificate) → Certificate Authority
What’s the concern of browsers?

On the web, latency is king

Browsers face tension between security and speed
Must contact CA to ensure cert not revoked
Test harness

Goal: Test browser behavior under different combinations of:
- Revocation protocols
- Availability of revocation information
- Chain lengths
- EV/non-EV certificates

Normal

Extended Validation

Implement 244 tests using fake root certificate + Javascript
- Unique DNS name, cert chain, CRL/OCSP responder, …
Do browsers check revocations?

**Supports CRLs**

- **Desktop:**
  - Google Chrome
  - Mozilla Firefox
  - Safari
  - Microsoft Edge
  - Opera

- **Mobile:**
  - Google Chrome
  - Mozilla Firefox
  - Safari
  - Microsoft Edge
  - Opera

**Supports OCSP**

- **Desktop:**
  - Google Chrome
  - Mozilla Firefox
  - Safari
  - Microsoft Edge
  - Opera

- **Mobile:**
  - Google Chrome
  - Mozilla Firefox
  - Safari
  - Microsoft Edge
  - Opera

**Supports OCSP Stapling**

- **Desktop:**
  - Google Chrome
  - Mozilla Firefox
  - Safari
  - Microsoft Edge
  - Opera

- **Mobile:**
  - Google Chrome
  - Mozilla Firefox
  - Safari
  - Microsoft Edge
  - Opera
Do browsers check revocations?

Supports CRLs

Desktop: 🌟 🌟 🌟 🌟
Mobile: ✗ ✗ ✗ ✗

Supports OCSP

Desktop: 🌟 🌟 🌟 🌟
Mobile: 🌟 🌟 🌟 🌟

Supports OCSP Stapling

Desktop: 🌟 🌟 🌟 🌟
Mobile: 🌟 🌟 🌟 🌟
Do browsers check revocations?

**Supports CRLs**

- **Desktop:**
  - EV only
  - Chrome
  - Safari
  - Edge
  - Opera

- **Mobile:**
  - Chrome
  - Safari
  - Edge
  - Opera

**Supports OCSP**

- **Desktop:**
  - EV only
  - Firefox
  - Chrome
  - Safari
  - Edge
  - Opera

- **Mobile:**
  - Firefox
  - Chrome
  - Safari
  - Edge
  - Opera

**Supports OCSP Stapling**

- **Desktop:**
  - Firefox
  - Chrome
  - Safari
  - Edge
  - Opera

- **Mobile:**
  - Chrome
  - Safari
  - Edge
  - Opera
Do browsers check revocations?

**Supports CRLs**

- **Desktop:**
  - **EV only**
- **Mobile:**
  - **EV only**

**Supports OCSP**

- **Desktop:**
  - **EV only**
- **Mobile:**
  - **EV only**

**Supports OCSP Stapling**

- **Desktop:**
  - **EV only**
- **Mobile:**
  - **EV only**
<table>
<thead>
<tr>
<th>Check intermediate</th>
<th>Revocation unavailable</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Desktop:</strong></td>
<td><strong>Mobile:</strong></td>
</tr>
<tr>
<td>![Browser Icons]</td>
<td>![Browser Icons]</td>
</tr>
<tr>
<td>![Browser Icons]</td>
<td>![Browser Icons]</td>
</tr>
</tbody>
</table>
Do browsers check intermediates?

Check intermediate

Desktop: EV EV OCSP Firefox Edge Chrome
Mobile: ☒ ☒ ☒ ☒

Revocation unavailable

Desktop: Google Chrome Firefox Firefox Edge Chrome
Mobile: Google Chrome Firefox Edge
Do browsers check intermediates?

Check intermediate

**Desktop:** EV EV OCSP  ✓  ✓  ✓

**Mobile:** ✓  ✓  ✓

Revocation unavailable

**Desktop:** EV CRL X CRL  ✓  ✓  ✓

**Mobile:** ✓  ✓  ✓
Do browsers check intermediates?

Check intermediate

Desktop: EV EV OCSP ✔ ✔ ✔
Mobile: ✔ ✔ ✔

Revocation unavailable

Desktop: EV ✔ CRL ✔ ✔ ✔
Mobile: ✔ ✔ ✔

No browser correctly checks all revocations
Takeaways

Revocations common

~1% in steady state; more than 8% after Heartbleed

Obtaining revocation information can be expensive

CRLs large, OCSP Stapling rarely supported

Many browsers don’t bother to check revocation

Mobile browsers completely lack of revocation checking
Chrome pushes out list of select revocations, called CRLSet

Chromium developers only state:

1. The full list [of covered CRLs] isn’t public
2. CRLs on the list are fetched infrequently
3. Entries in the CRL are filtered by reason code.
4. Size limited to 250 KB
CRLSet coverage

Only 0.35% of all revocations appear in CRLSet

Only 295 (10.5%) CRLs have any revocations covered
CRLSet coverage

Only 0.35% of all revocations appear in CRLSet

Only 295 (10.5%) CRLs have any revocations covered

CRLSet only has a low coverage
More results in the paper

- Analysis of EV certificate revocation
- Revoked but alive certificates
- Improve CRLSets with Bloom Filters
  and more …
Summary

• An end-to-end measurement of certificate revocation in the web
  • Covers all parties: website administrators, CAs and browsers

• Key findings
  • Extensive inaction with respect to certificate revocation
  • Browsers fails to check certificate revocation
  • Mobile browsers are lack of revocation checking

• We can improve
  • CAs can maintain more small CRLs
  • Website admins can deploy OCSP stapling
Summary

• An end-to-end measurement of certificate revocation in the web
  • Covers all parties: website administrators, CAs and browsers

• Key findings
  • Extensive inaction with respect to certificate revocation
  • Browsers fails to check certificate revocation
  • Mobile browsers are lack of revocation checking

• We can improve
  • CAs can maintain more small CRLs
  • Website admins can deploy OCSP stapling

Questions?
securepki.org