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?
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

The owner of is indeed BoA

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What happens when a certificate is no longer valid?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What happens when a certificate is no longer valid?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What happens when a certificate is no longer valid?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

What happens when a certificate is no longer valid?

Browser

Attacker

Certificate Authority
Certificate revocation

What happens when a certificate is no longer valid?

- Browser
- Attacker
- Certificate Authority
- Please revoke

Certificate Revocation
Certificate revocation

What happens when a certificate is no longer valid?

Browser

Attacker

Certificate Authority

Please revoke
Certificate revocation

What happens when a certificate is no longer valid?

Periodically pull / query (CRL) (OCSP)

Certificate Authority

Browser

Attacker

Please revoke
Certificate revocation

What happens when a certificate is no longer valid?

Periodically pull / query (CRL) (OCSP)
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 do 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)

classify

38M certs

Non-CA

CA

1,946 certs
Dataset

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

  Classify

- 38M certs
  - Non-CA
    - 1,946 certs
  - CA

  Validate

- Leaf Set
  - 5M valid certs
Download revocation information daily
How frequently are certificates revoked?

![Graph showing the percentage of fresh certificates that are revoked over time.]

- X-axis: Date (01/14 to 03/15)
- Y-axis: Percentage of Fresh Certs that are Revoked (0.0 to 12.0)
- The graph shows an increase in the percentage of revoked certificates from January to July 2014, peaking in July 2014, and then gradually decreasing until March 2015.
How frequently are certificates revoked?

Significant fraction of certificates revoked
1% in steady state; more than 8% after Heartbleed
Are there revoked certificates being used?

Over 0.5% advertised certificates are revoked

Website admins failed to update their servers
Outline

Website admin behavior
  e.g., revocation is common ~8%

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

Client behavior
  e.g., do browsers check revocations?
CRLs, OCSP, and OCSP Stapling
CRLs, OCSP, and OCSP Stapling
CRLs, OCSP, and OCSP Stapling
CRLs, OCSP, and OCSP Stapling
Cost of obtaining CRLs
Cost of obtaining CRLs

CDF

76MB Apple CRL
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>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>
</tr>
<tr>
<td>RapidSSL</td>
<td>5</td>
<td>626,774</td>
<td>2,153</td>
</tr>
<tr>
<td>Comodo</td>
<td>30</td>
<td>447,506</td>
<td>7,169</td>
</tr>
<tr>
<td>PositiveSSL</td>
<td>3</td>
<td>415,075</td>
<td>8,177</td>
</tr>
<tr>
<td>Verisign</td>
<td>37</td>
<td>311,788</td>
<td>15,438</td>
</tr>
</tbody>
</table>

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

Diagram:

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

Connections:
- From **Browser** to **Website**
- From **Website** to **Certificate Authority**
- From **Certificate Authority** to **Browser**
CRLs, OCSP, and OCSP Stapling
CRLs, OCSP, and OCSP Stapling
OCSP prevalence

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

Browser

Website

Certificate Authority
CRLs, OCSP, and OCSP Stapling
CRLs, OCSP, and OCSP Stapling

Browser

Website

Certificate Authority

![Diagram showing the interaction between a browser, a website, and a certificate authority, demonstrating the concepts of CRLs, OCSP, and OCSP Stapling.]

- **CRLs (Certificate Revocation Lists)**: Used to check whether a certificate has been revoked.
- **OCSP (Online Certificate Status Protocol)**: An alternative to CRLs for checking certificate status.
- **OCSP Stapling**: A mechanism that allows a browser to request and receive certificate validation information (CRL or OCSP response) as part of a web transaction, reducing the overhead of making additional requests.
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
Outline

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?
Security vs speed in 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

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

<table>
<thead>
<tr>
<th></th>
<th>Chrome 44 OS X</th>
<th>Chrome 44 Win.</th>
<th>Chrome 44 Lin.</th>
<th>Firefox 40</th>
<th>Opera 12.17</th>
<th>Opera 31.0</th>
<th>Safari 6-8</th>
<th>IE 7-9</th>
<th>IE 10</th>
<th>IE 11</th>
<th>Mobile Browsers iOS 6-8</th>
<th>Mobile Browsers Andr. 4.1-5.1</th>
<th>Mobile Browsers Chrome 8.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CRL</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Int. 1</td>
<td>EV ✔ EV ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>X</td>
<td>X ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>X</td>
<td>X ✔</td>
<td>X ✔</td>
</tr>
<tr>
<td>Unavailable</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>X ✔</td>
<td>X ✔</td>
<td>X ✔</td>
</tr>
<tr>
<td><strong>OCSP</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Int. 1</td>
<td>EV ✔ EV ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>X</td>
<td>X ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>X</td>
<td>X ✔</td>
<td>X ✔</td>
</tr>
<tr>
<td>Unavailable</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ › ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>X ✔</td>
<td>X ✔</td>
<td>X ✔</td>
</tr>
<tr>
<td>Int. 2+</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>X</td>
<td>X ✔</td>
<td>X ✔</td>
</tr>
<tr>
<td>Unavailable</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>X ✔</td>
<td>X ✔</td>
<td>X ✔</td>
</tr>
<tr>
<td>Leaf</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>X ✔</td>
<td>X ✔</td>
<td>X ✔</td>
</tr>
<tr>
<td>Revoked</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>X ✔</td>
<td>X ✔</td>
<td>X ✔</td>
</tr>
<tr>
<td>Unavailable</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔</td>
<td>X ✔</td>
<td>X ✔</td>
<td>X ✔</td>
</tr>
</tbody>
</table>

- **Will cover few highlights...**
## Certificates with CRLs

### Browser Checks for CRLs

<table>
<thead>
<tr>
<th>CRL</th>
<th>Chrome 44 OS X</th>
<th>Chrome 44 Win.</th>
<th>Chrome 44 Lin.</th>
<th>Desktop Browsers</th>
<th>Safari 6-8</th>
<th>Opera 12.17</th>
<th>Opera 31.0</th>
<th>Firefox 40</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int. 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revoked</td>
<td>EV ✓</td>
<td>EV ✓</td>
<td></td>
<td>X</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>Unavailable</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Int. 2+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revoked</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>Unavailable</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Leaf</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Revoked</td>
<td>EV ✓</td>
<td>EV ✓</td>
<td></td>
<td>X</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>Unavailable</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

### Browser Behavior

- **Chrome:** Only checks CRLs for **EV certificates**
- **Firefox:** **Never** checks CRLs
- **Most browsers** accept certificate if **CRL server unavailable**
- **IE** performs the most checks (!)
## Certificates with OCSP

<table>
<thead>
<tr>
<th>OCSP</th>
<th>Chrome 44 OS X</th>
<th>Chrome 44 Win.</th>
<th>Chrome 44 Lin.</th>
<th>Firefox 40</th>
<th>Opera 12.17</th>
<th>Opera 31.0</th>
<th>Safari 6-8</th>
<th>IE 7-9</th>
<th>IE 10</th>
<th>IE 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int. 1</td>
<td>EV</td>
<td>EV</td>
<td>EV</td>
<td>EV</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Revoked</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Unavailable</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Int. 2+</td>
<td>EV</td>
<td>EV</td>
<td>EV</td>
<td>EV</td>
<td>X</td>
<td>X</td>
<td>L/W</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Revoked</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Unavailable</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Leaf</td>
<td>EV</td>
<td>EV</td>
<td>EV</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Revoked</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Unavailable</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Reject unknown status</td>
<td>X</td>
<td>X</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Try CRL on failure</td>
<td>EV</td>
<td>EV</td>
<td>–</td>
<td></td>
<td>X</td>
<td>X</td>
<td>L/W</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Chrome:** Only checks OCSP for EV certificates

**Firefox:** Only checks intermediates for EV certificates

Most browsers accept certificate if **OCSP server unavailable**

**IE** again performs the most checks
Web servers with OCSP Stapling

<table>
<thead>
<tr>
<th>OCSP Stapling</th>
<th>Chrome 44 OS X</th>
<th>Chrome 44 Win.</th>
<th>Chrome 44 Lin.</th>
<th>Firefox 40</th>
<th>Opera 12.17</th>
<th>Opera 31.0</th>
<th>Safari 6–8</th>
<th>Safari 7–9</th>
<th>Safari 10</th>
<th>Safari 11</th>
<th>IE 7</th>
<th>IE 8</th>
<th>IE 9</th>
<th>IE 10</th>
<th>IE 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request OCSP staple</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Respect revoked staple</td>
<td>X</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
<td>L/W</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

All browsers support OCSP Stapling… *except* Safari

Chrome bug: accept *any* Staple on OS X, including revoked
What about mobile browsers?

|                  | iOS 6-8 | Mobile Browsers | Mobile Browsers | Mobile Browsers | Mobile Browsers | Mobile Browsers | Mobile Browsers | Mobile Browsers | Mobile Browsers | Mobile Browsers |
|------------------|---------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|
|                  |         | Andr. 4.1-5.1  | Stock          | Chrome         | IE 8.0         |                 |                 |                 |                 |                 |                 |
| CRL              |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Int. 1           | x       | x              | x              | x              | x              | x              | x              | x              | x              | x              |
| Revoked          |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Unavailable      |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Int. 2+          |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Revoked          |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Unavailable      |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Leaf             |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Revoked          |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Unavailable      |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| OCSP             |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Int. 1           |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Revoked          |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Unavailable      |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Int. 2+          |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Revoked          |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Unavailable      |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Leaf             |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Revoked          |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Unavailable      |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Reject           |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| unknown status   |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Try CRL on failure |     |                |                |                |                |                 |                 |                 |                 |                 |                 |
| OCSP Stapling    |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Request OCSP staple |     |                |                |                |                |                 |                 |                 |                 |                 |                 |
| Respect          |         |                |                |                |                |                 |                 |                 |                 |                 |                 |
| revoked staple   |         |                |                |                |                |                 |                 |                 |                 |                 |                 |

Mobile browsers *never* check Android devices request Staples ...and promptly ignore them.
What about mobile browsers?

<table>
<thead>
<tr>
<th></th>
<th>iOS 6-8</th>
<th>Mobile Browsers</th>
<th>IE 8.0</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Andr. 4.1-5.1</td>
<td>Stock</td>
<td>Chrome</td>
</tr>
<tr>
<td>CRL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Int. 1</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Revoked Unavailable</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Int. 2+</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Revoked Unavailable</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Leaf</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Revoked Unavailable</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>OCSP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Int. 1</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Revoked Unavailable</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Int. 2+</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Revoked Unavailable</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Leaf</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Revoked Unavailable</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Reject unknown status</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Try CRL on failure</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>OCSP Stapling</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request OCSP staple</td>
<td>x</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Respect revoked staple</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
</tbody>
</table>

Mobile browsers never check

Android devices request Staples
...and promptly ignore them

No desktop or mobile browser correctly checks 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 curated list of revocations, called CRLSet

Limits: filtered with reason code, size limited to 250 KB, etc.
Chrome pushes out curated list of revocations, called CRLSet

Limits: filtered with reason code, size limited to 250 KB, etc.

Only 0.35% of all revocations appear in CRLSet

Only 10.5% CRLs have any revocations covered
Chrome pushes out curated list of revocations, called CRLSet

Limits: filtered with reason code, size limited to 250 KB, etc.

Only 0.35% of all revocations appear in CRLSet

Only 10.5% CRLs have *any* revocations covered

If we focus on revocations from popular sites (Alexa):

3.9% top 1M, 10.4% top 1K
More results in the paper

- Analysis of EV certificate revocation
- Revoked but alive certificates
- Speed of CRLSet updates
- 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
Backup Slides
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
CRLs

Fraction of Revoked Certs on CRLSet

CRLSet Reason Codes
All Revocations

0 0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 1

0 0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 1