What’s in a Name? Exploring CA Certificate Control

Zane Ma\textsuperscript{1}, Joshua Mason\textsuperscript{1}
Manos Antonakakis\textsuperscript{2}, Zakir Durumeric\textsuperscript{3}, Michael Bailey\textsuperscript{1}

\textsuperscript{1}University of Illinois at Urbana-Champaign
\textsuperscript{2}Georgia Institute of Technology
\textsuperscript{3}Stanford University
Delegated Authentication

Root Store
Inclusion/Removal

Certificate Authority

Identity Verification
Certificate Issuance

CA Certificate

Leaf Certificate

Relying Party

Web Browser
Email Client

Subscriber

Web Server
Email Server

TLS
Certificate exchange/validation
Symantec Distrust

- From 2009-2017 Symantec was responsible for over a dozen issues[1] that prompted removal from browser root stores

- Difficult to determine which root CA certificates Symantec operated!

---

**Comodo**

Root #1

<table>
<thead>
<tr>
<th>commonName</th>
<th>UTN-USERFirst-Client Authentication and Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>orgUnitName</td>
<td><a href="http://www.usertrust.com">http://www.usertrust.com</a></td>
</tr>
<tr>
<td>orgName</td>
<td>The USERTRUST Network</td>
</tr>
<tr>
<td>localityName</td>
<td>Salt Lake City</td>
</tr>
<tr>
<td>stateOrProvinceName</td>
<td>UT</td>
</tr>
<tr>
<td>countryName</td>
<td>US</td>
</tr>
</tbody>
</table>

**Symantec**

Root #2

<table>
<thead>
<tr>
<th>commonName</th>
<th>UTN-USERFirst-NetworkApplications</th>
</tr>
</thead>
<tbody>
<tr>
<td>orgUnitName</td>
<td><a href="http://www.usertrust.com">http://www.usertrust.com</a></td>
</tr>
<tr>
<td>orgName</td>
<td>The USERTRUST Network</td>
</tr>
<tr>
<td>localityName</td>
<td>Salt Lake City</td>
</tr>
<tr>
<td>stateOrProvinceName</td>
<td>UT</td>
</tr>
<tr>
<td>countryName</td>
<td>US</td>
</tr>
</tbody>
</table>

---

Symantec Distrust

• From 2009-2017 Symantec was responsible for over a dozen issues\(^1\) that prompted removal from browser root stores

• Difficult to determine which root CA certificates Symantec operated!

• Needed to whitelist independently-operated intermediate CAs

  • 6 Apple Intermediates
  • 1 Google Intermediate

Takeaways

1. TLS authentication trust occurs at the level of CAs (a.k.a. CA certificate operators), not CA certificates.

2. There are no guarantees that the identity in a CA certificate reflects the operator of the CA certificate.

3. Intermediate CA certificates may have separate operators that are independent of their root CA operator.
Previous Work

• No prior academic work on this problem

• Mozilla-organized Common CA Database (CCADB)
  
  • CCADB “owner” has intentional administrative focus - for CAs to upload policies and audits
  
  • E.g. Several Let’s Encrypt certificates (cross-signs) are “owned” by IdenTrust, despite being operated by Let’s Encrypt
  
  • Incomplete coverage: 20% of CA issuers trusted by Microsoft/Apple/Mozilla are not in CCADB
Approach

How can we determine the *operator* of a CA certificate / issuer?

1. Measure CA operational features to detect CA certificates with shared CA operators

<table>
<thead>
<tr>
<th>Certificates</th>
<th>Audits</th>
<th>Heuristic CA operator clusters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Fingerprints</td>
<td>foo.com</td>
<td>a2b3c4... Certificate SHA256/SHA1</td>
</tr>
</tbody>
</table>
Approach

How can we determine the operator of a CA certificate / issuer?

1. Measure CA operational features to detect CA certificates with shared CA operators

2. Carefully apply CCADB to label CA operator clusters
Certificate Fingerprints

Novel method to detect artifacts of issuance software/configuration

Goal: distinguish certificate entropy caused by issuance software from all other certificate entropy (e.g. serial number, public key value, subject name)

Insight: certificates are structured as an ordered tree (ASN.1 format), and issuance infrastructure controls the structure/order of tree
Certificate Fingerprints

Issuance software-independent entropy:
validity, subject names, signature

Issuance software-dependent entropy:
type and order of subject fields / extensions

Fingerprint = structure of certificate, ignoring all leaf node values beside enumerable OID
Certificate Fingerprints

CA issuers grouped by issuance profile, which is the set of issued FPs

Belgian Citizen CA

DigiCert
What's in a Name? Exploring CA Certificate Control

- **Certificate Fingerprints**
- **foo.com**
- **AIA/OCSP/CRL**
- **FQDNs + IPS**
- **Certificate SHA256/SHA1**

**Audits**

- **Min. 2-edge Combination**
- **Heuristic CA operator clusters**

**Certificates**

- **Labels**
- **Heuristic CA operator clusters**
- **CCADB Labels**
- **CA Operator Dataset**

Label correction and expansion
Cluster labeling

Heuristic CA operator clusters + CCADB Labels → Labeled clusters

Label correction

Label expansion
What's in a Name? Exploring CA Certificate Control

- **Certificates**
  - foo.com
  - Certificate Fingerprints
  - AIA/OCSP/CRL FQDNS + IPS

- **Audits**
  - a2b3c4...
  - Certificate SHA256/SHA1
  - Min. 2-edge Combination

- **Heuristic CA operator clusters**

- **CCADB Labels**

- **Label correction and expansion**

- **CA Operator Dataset**
Evaluation

No ground truth data!

Best approximation: manually resolved disclosure issues
Evaluation

Found all issues from May 2014 - July 2019

<table>
<thead>
<tr>
<th></th>
<th>Issuers</th>
<th>Issues Resolved By Dataset</th>
<th>Issues</th>
<th>Issues Resolved By Dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Issuers</td>
<td>103</td>
<td>48 (46.6%)</td>
<td>22</td>
<td>7 (31.8%)</td>
</tr>
</tbody>
</table>

100% specificity
46.6% recall
Discoveries

Improperly disclosed Camerfirma subordinate CA (MULTICERT)[1], yet another issue leading to Camerfirma removal from Mozilla

Refined CA operator label for 189 issuers (241 CA certificates)

Added new labels for 404 unlabeled issuers (651 CA certificates)

[1] https://bugzilla.mozilla.org/show_bug.cgi?id=1672029
Summary

CA certificate name != CA that operates the certificate key

Measurements of CA operations —> new CA operator dataset

CA operational transparency means:

1. More informed root store decision making
2. More accurate research / issue attribution
What’s in a Name?
Exploring CA Certificate Control

Zane Ma

University of Illinois Urbana-Champaign
zanema2@illinois.edu
https://zanema.com