What’s in a Name? Exploring CA Certificate Control

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

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

CA/Browser Forum, October 13th
Authentication
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
Delegated Authentication

What's in a Name? Exploring CA Certificate Control • Zane Ma
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!

<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>

<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>

Comodo Root #1

Symantec Root #2

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 work on this general problem

• Mozilla-organized Common CA Database (CCADDB)
  • CCADDB “owner” has intentional administrative focus - for CAs to upload policies and audits
  • E.g. Several Let’s Encrypt certificates (cross-signs) were “owned” by IdenTrust, despite being operated by Let’s Encrypt
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
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

- Top DigiCert FPs
- Belgian Citizen CA
- DigiCert
What's in a Name? Exploring CA Certificate Control • Zane Ma
Cluster labeling

Heuristic CA operator clusters + CCADB Labels → Labeled clusters

Label correction

Label expansion
Evaluation

No ground truth data!

Best approximation: manually resolved disclosure issues
Evaluation

Found all issues from May 2014 - July 2019

<table>
<thead>
<tr>
<th>Operational Issuers</th>
<th>Issuers</th>
<th>Issues Resolved By Dataset</th>
<th>Issues</th>
<th>Issues Resolved By Dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td></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
# Results

<table>
<thead>
<tr>
<th>Cluster</th>
<th>CA1: # issuers (certs)</th>
<th>CA2: # issuers (certs)</th>
<th>Shared Features</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>CRL</td>
<td>OCSP</td>
</tr>
<tr>
<td>6</td>
<td>GlobalSign: 75 (118)</td>
<td>Google: 23 (33)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>21</td>
<td>GoDaddy: 9 (19)</td>
<td>Amazon: 2 (7)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>60</td>
<td>Digidentity B.V.: 3 (4)</td>
<td>PKIoverheid: 2 (2)</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>64</td>
<td>DigiCert: 2 (4)</td>
<td>Sectigo: 1 (1)</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>67</td>
<td>TC TrustCenter: 2 (3)</td>
<td>DSV GmbH: 1 (1)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>94</td>
<td>Deutsche Telekom: 2 (2)</td>
<td>DigiCert: 1 (1)</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>183</td>
<td>StartCom: 1 (1)</td>
<td>Certinomis: 1 (1)</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>212</td>
<td>E-Tugra: 1 (1)</td>
<td>e-tugra: 1 (1)</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>252</td>
<td>E-Tugra: 1 (1)</td>
<td>e-tugra: 1 (1)</td>
<td>-</td>
<td>✓</td>
</tr>
</tbody>
</table>
Results

<table>
<thead>
<tr>
<th>Discovery</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improperly disclosed Camerfirma subordinate CA (MULTICERT)[1]</td>
<td>Camerfirma removed from Mozilla root store, distrusted by Google products</td>
</tr>
<tr>
<td>Refined CA operator labels for 241 CA certs</td>
<td>CCADB exploring automated sub-CA consistency checking [2] and ownership annotation [3]</td>
</tr>
<tr>
<td>Added new labels for 651 unlabeled CA certs</td>
<td></td>
</tr>
</tbody>
</table>

CA operational transparency means:
1) More informed root store decision making
2) More accurate research / issue attribution

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

Direct disclosure of the legal entity that operates CA certificates

• Mozilla/Microsoft require ownership change disclosure

• CCADB considering addition of new field
Looking Forward

Direct disclosure of the legal entity that operates CA certificates

• Mozilla/Microsoft require ownership change disclosure

• CCADB considering addition of new field

Trust, but verify: additional observation of CA behavior

• Certificate issuance infrastructure, improved fingerprints

Expand to more nuanced view of CA certificate operations
What’s in a Name?
Exploring CA Certificate Control

https://github.com/zzma/ca-transparency

Zane Ma

Georgia Institute of Technology
zanema@gatech.edu
https://zanema.com