Tracking Certificate Misissuance in the Wild

Deepak Kumar  
*University of Illinois*

Zhengping Wang  
*University of Illinois*

Matthew Hyder  
*University of Illinois*

Joseph Dickinson  
*University of Illinois*

Gabrielle Beck  
*University of Michigan*

David Adrian  
*University of Michigan*

Joshua Mason  
*University of Illinois*

ZMap Durumeric  
*University of Illinois  
  University of Michigan  
  Stanford University*

J. Alex Halderman  
*University of Michigan*

Michael Bailey  
*University of Illinois*
HTTPS relies on a supporting Public Key Infrastructure (PKI) composed of hundreds of Certificate Authorities (CAs)
Iranian Man-in-the-Middle Attack Against Google Demonstrates Dangerous Weakness of Certificate Authorities

The TURKTRUST SSL certificate fiasco – what really happened, and what happens next?

Google Blocks Fraudulent Certificates Used by French Government

Revoking Trust in one CNNIC Intermediate Certificate
CA/Browser Forum Baseline Requirements:
CA must follow these to be browser trusted
I WANT YOU TO STOP MISISSUING CERTIFICATES
Re: Misissued certificates
By Lee - 16 posts - 379 views

I WANT YOU

MISISSUING
CERTIFICATES
I WANT YOU

More certificates with invalid dnsNames
By Jonathan Rudenberg - 1 post - 382 views

Re: Misissued certificates
By Lee - 16 posts - 379 views
“It's 2017 - it's both time to stop making excuses and time to recognize that the ability of CAs to adhere to the rules is core to their trustworthiness. Technical rules are but a proxy for procedure rules.” - Ryan Sleevi
ZLint: An X.509 Certificate Linter

• Codifies RFC 2119 rules in both RFC 5280 and the CA/Browser Forum Baseline Requirements
ZLint: An X.509 Certificate Linter

• Codifies RFC 2119 rules in both RFC 5280 and the CA/Browser Forum Baseline Requirements
  • “Certificates MUST be of type X.509 v3”
  • “…the subject key identifier extension SHOULD be included in all end entity certificates.”
ZLint: An X.509 Certificate Linter

• Written in Go
• Contains 220 lints
  • 95% coverage of Baseline Requirements
  • 90% coverage of RFC 5280
Lint Severity Levels

• ZLint encodes severity levels corresponding to different kinds of clauses
Lint Severity Levels

• ZLint encodes severity levels corresponding to different kinds of clauses

• **Error**: Violation of a *MUST* clause
  
  • “Certificates MUST be of type X.509 v3”
Lint Severity Levels

• ZLint encodes severity levels corresponding to different kinds of clauses

• **Error**: Violation of a *MUST* clause
  
  • “Certificates MUST be of type X.509 v3”

• **Warning**: Violation of a *SHOULD* clause
  
  • “…the subject key identifier extension SHOULD be included in all end entity certificates.”
How prevalent is certificate misissuance?
Collecting Certificates

• Ran ZLint over all certificates in Censys through July 2017
  • Analyzed those that chained to a root in NSS
Collecting Certificates

- Ran ZLint over all certificates in Censys through **July 2017**
  - Analyzed those that chained to a root in NSS
- **61M** non-expired certificates
Collecting Certificates

- Ran ZLint over all certificates in Censys through **July 2017**
  - Analyzed those that chained to a root in NSS
- **61M** non-expired certificates
- **171M** total certificates
Historical Misissuance

![Graph showing historical misissuance with dates from 2009 to 2017. The graph tracks the percent of certificates issued, with separate lines for errors and warnings. The data shows a notable increase in warnings around 2010.](image)
Historical Misissuance

![Graph showing historical misissuance with dates from 2009 to 2017 and percentages of errors and warnings over time.]

- Percent certs issued
- Errors
- Warnings

Date

2009 - 2010
Historical Misissuance

![Graph showing historical misissuance with dates from 2009 to 2016 on the x-axis and percent certificates issued on the y-axis. The graph includes lines for errors and warnings, marked with the CA/Browser Forum Baseline Requirements.]
Historical Misissuance

Errors

Warnings

Certificate Transparency

Percent certs issued

Date


Errors

Warnings

Certificate Transparency
Historical Misissuance

- Errors
- Warnings

---

Errors: 
Warnings: 

MDSP Discussions: Increase

---


Percent certs issued

---

Tracking Certificate Misissuance in the Wild • Deepak Kumar
Historical Misissuance

- **Errors**
- **Warnings**

<table>
<thead>
<tr>
<th>Date</th>
<th>Errors</th>
<th>Warnings</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Historical Misissuance

Errors

Warnings

WoSign, Symantec, are slated to be distrusted
Historical Misissuance

WoSign and Symantec misissued at a rate 2 - 8x worse than the rest of the ecosystem
### Largest Misissuers

<table>
<thead>
<tr>
<th>Issuer</th>
<th>Certificates</th>
<th>w/ Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>GoDaddy</td>
<td>1.6M (2.7%)</td>
<td>38,215 (2.4%)</td>
</tr>
<tr>
<td>Symantec</td>
<td>2.7M (4.6%)</td>
<td>23,053 (0.8%)</td>
</tr>
<tr>
<td>StartCom, Ltd.</td>
<td>536K (0.9%)</td>
<td>11,617 (2.1%)</td>
</tr>
<tr>
<td>WoSign CA Lmtd.</td>
<td>196K (0.3%)</td>
<td>9,849 (5%)</td>
</tr>
<tr>
<td>VeriSign</td>
<td>43K (0.07%)</td>
<td>9,835 (23.1%)</td>
</tr>
</tbody>
</table>
# Largest Misissuers

<table>
<thead>
<tr>
<th>Issuer</th>
<th>Certificates</th>
<th>w/ Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>GoDaddy</td>
<td>1.6M (2.7%)</td>
<td>38,215 (2.4%)</td>
</tr>
<tr>
<td><strong>Symantec</strong></td>
<td>2.7M (4.6%)</td>
<td>23,053 (0.8%)</td>
</tr>
<tr>
<td><strong>StartCom, Ltd.</strong></td>
<td>536K (0.9%)</td>
<td>11,617 (2.1%)</td>
</tr>
<tr>
<td><strong>WoSign CA Ltd.</strong></td>
<td>196K (0.3%)</td>
<td>9,849 (5%)</td>
</tr>
<tr>
<td><strong>VeriSign</strong></td>
<td>43K (0.07%)</td>
<td>9,835 (23.1%)</td>
</tr>
</tbody>
</table>
## Largest Misissuers

<table>
<thead>
<tr>
<th>Issuer</th>
<th>Certificates</th>
<th>w/ Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>GoDaddy</td>
<td>1.6M (2.7%)</td>
<td>38,215 (2.4%)</td>
</tr>
<tr>
<td>Symantec</td>
<td>2.7M (4.6%)</td>
<td>23,053 (0.8%)</td>
</tr>
<tr>
<td>StartCom, Ltd.</td>
<td>536K (0.9%)</td>
<td>11,617 (2.1%)</td>
</tr>
<tr>
<td>WoSign CA Lmtd.</td>
<td>196K (0.3%)</td>
<td>9,849 (5%)</td>
</tr>
<tr>
<td>VeriSign</td>
<td>43K (0.07%)</td>
<td>9,835 (23.1%)</td>
</tr>
</tbody>
</table>

Browsers are taking down the largest offenders
Historical Misissuance

Errors

Warnings

Date

Percent certs issued


Tracking Certificate Misissuance in the Wild • Deepak Kumar
<table>
<thead>
<tr>
<th>Issuer</th>
<th>Certificates</th>
<th>w/ Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Let’s Encrypt</td>
<td>37M (61%)</td>
<td>13 (0.0%)</td>
</tr>
<tr>
<td>Comodo</td>
<td>6.7M (11%)</td>
<td>3,219 (0.0%)</td>
</tr>
<tr>
<td>cPanel</td>
<td>4.7M (7.8%)</td>
<td>131 (0.0%)</td>
</tr>
<tr>
<td>Symantec</td>
<td>2.8M (4.6%)</td>
<td>23,053 (0.8%)</td>
</tr>
<tr>
<td>GeoTrust, Inc.</td>
<td>1.9M (3.2%)</td>
<td>5,694 (0.3%)</td>
</tr>
<tr>
<td>GoDaddy</td>
<td>1.6M (2.7%)</td>
<td>38,215 (2.0%)</td>
</tr>
<tr>
<td>GlobalSign</td>
<td>1.2M (1.9%)</td>
<td>837 (0.0%)</td>
</tr>
</tbody>
</table>
### Misissuance by Largest Issuers

<table>
<thead>
<tr>
<th>Issuer</th>
<th>Certificates</th>
<th>w/ Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Let’s Encrypt</td>
<td>37M (61%)</td>
<td>13 (0.0%)</td>
</tr>
<tr>
<td>Comodo</td>
<td>6.7M (11%)</td>
<td>3,219 (0.0%)</td>
</tr>
<tr>
<td>cPanel</td>
<td>4.7M (7.8%)</td>
<td>131 (0.0%)</td>
</tr>
<tr>
<td>Symantec</td>
<td>2.8M (4.6%)</td>
<td>23,053 (0.8%)</td>
</tr>
<tr>
<td>GeoTrust, Inc.</td>
<td>1.9M (3.2%)</td>
<td>5,694 (0.3%)</td>
</tr>
<tr>
<td>GoDaddy</td>
<td>1.6M (2.7%)</td>
<td>38,215 (2.0%)</td>
</tr>
<tr>
<td>GlobalSign</td>
<td>1.2M (1.9%)</td>
<td>837 (0.0%)</td>
</tr>
</tbody>
</table>
## Misissuance by Largest Issuers

<table>
<thead>
<tr>
<th>Issuer</th>
<th>Certificates</th>
<th>w/ Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Let's Encrypt</td>
<td>37M (61%)</td>
<td>13 (0.0%)</td>
</tr>
<tr>
<td>Comodo</td>
<td>6.7M (11%)</td>
<td>3,219 (0.0%)</td>
</tr>
<tr>
<td>cPanel</td>
<td>4.7M (7.8%)</td>
<td>131 (0.0%)</td>
</tr>
<tr>
<td>Symantec</td>
<td>2.8M (4.6%)</td>
<td>23,053 (0.8%)</td>
</tr>
<tr>
<td>GeoTrust, Inc.</td>
<td>1.9M (3.2%)</td>
<td>5,694 (0.3%)</td>
</tr>
<tr>
<td>GoDaddy</td>
<td>1.6M (2.7%)</td>
<td>38,215 (2.0%)</td>
</tr>
<tr>
<td>GlobalSign</td>
<td>1.2M (1.9%)</td>
<td>837 (0.0%)</td>
</tr>
</tbody>
</table>
### Misissuance by Largest Issuers

<table>
<thead>
<tr>
<th>Issuer</th>
<th>Certificates</th>
<th>w/ Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Let’s Encrypt</td>
<td>37M (61%)</td>
<td>13 (0.0%)</td>
</tr>
<tr>
<td>Comodo</td>
<td>6.7M (11%)</td>
<td>3,219 (0.0%)</td>
</tr>
<tr>
<td>cPanel</td>
<td>4.7M (7.8%)</td>
<td>131 (0.0%)</td>
</tr>
<tr>
<td>Symantec</td>
<td>2.8M (4.6%)</td>
<td>23,053 (0.8%)</td>
</tr>
<tr>
<td>GeoTrust, Inc.</td>
<td>1.9M (3.2%)</td>
<td>5,694 (0.3%)</td>
</tr>
<tr>
<td>GoDaddy</td>
<td>1.6M (2.7%)</td>
<td>38,215 (2.0%)</td>
</tr>
<tr>
<td>GlobalSign</td>
<td>1.2M (1.9%)</td>
<td>837 (0.0%)</td>
</tr>
</tbody>
</table>

**Large CAs misissue a small fraction of their certificates**
<table>
<thead>
<tr>
<th>Let's Encrypt</th>
<th>Symantec Corporation</th>
<th>GeoTrust Inc.</th>
<th>GoDaddy.com</th>
<th>GlobalSign nv-va</th>
<th>Western Digital Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>StartCom Ltd.</td>
<td>Entrust</td>
<td>Gandi</td>
<td>VeriSign</td>
<td>Trust</td>
<td></td>
</tr>
<tr>
<td>DigiCert Inc</td>
<td>Starfield Technologies</td>
<td>Trustwave Holdings</td>
<td>Unizeto</td>
<td>Internet2</td>
<td></td>
</tr>
<tr>
<td>COMODO CA Limited</td>
<td>Thawte</td>
<td>TERENA</td>
<td>Hostpoint AG</td>
<td>Network Solutions LLC</td>
<td>Google Inc</td>
</tr>
<tr>
<td>Amazon</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cPanel</td>
<td>TrustAsia Technologies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WuSign CA Limited</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Problem with Small CAs

• Browsers are taking action against *big, obvious players*
The Problem with Small CAs

• Browsers are taking action against *big, obvious players*

• Smaller problematic CAs are “hiding in obscurity”
  
  • PROCERT is a notable counter-example
    
    • 39 issued certificates, 100% misissuance
The Problem with Small CAs

- Browsers are taking action against *big, obvious players*
- Smaller problematic CAs are “hiding in obscurity”
  - PROCERT is a notable counter-example
    - 39 issued certificates, 100% misissuance
  - If PROCERT gets the boot, at *least 17* others should go too!
“It’s 2017 - it’s both time to stop making excuses and time to recognize that the ability of CAs to adhere to the rules is core to their trustworthiness. *Technical rules are but a proxy for procedure rules.*”
Is certificate misissuance correlated with other mismanagement?
CA Management: Revocation

- OCSP Responders
- CRLs

Strict rules associated with revocation service response times
CA Revocation Measurement

- Made a valid OCSP, CRL request to all responders every hour from Sept 1 - 20, 2017
CA Revocation Measurement

- Made a valid OCSP, CRL request to all responders every hour from Sept 1 - 20, 2017
- Most responders follow 10s rule, but long tail
  - 53 OCSP responders worst case >10s
  - 2 CRL distribution points worst case >10s
## Correlating ZLint with Mismanagement

<table>
<thead>
<tr>
<th></th>
<th>Errors</th>
<th>Warnings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OCSP Responders</strong></td>
<td>0.10 (p-value: &lt; 0.01)</td>
<td>0.19 (p-value: &lt; 0.01)</td>
</tr>
<tr>
<td><strong>CRL Distribution Points</strong></td>
<td>0.07 (p-value: 0.01)</td>
<td>0.17 (p-value: &lt; 0.01)</td>
</tr>
</tbody>
</table>
## Correlating ZLint with Mismanagement

<table>
<thead>
<tr>
<th></th>
<th>Errors</th>
<th>Warnings</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCSP Responders</td>
<td>0.10 (p-value: &lt; 0.01)</td>
<td>0.19 (p-value: &lt; 0.01)</td>
</tr>
<tr>
<td>CRL Distribution Points</td>
<td>0.07 (p-value: 0.01)</td>
<td>0.17 (p-value: &lt; 0.01)</td>
</tr>
</tbody>
</table>
ZLint is Open Source

code: https://github.com/zmap/zlint

certificates: Available through Censys
ZLint is Deployed

code: https://github.com/zmap/zlint
certificates: Available through Censys
ZLint will be Deployed

code: https://github.com/zmap/zlint
certificates: Available through Censys
Moving Forward

- PKI community is using ZLint to focus removal investigations

- We need a systematic way to identify who to trust in the ecosystem

- ZLint enables monitoring of the certificate misissuance ecosystem

- We still need tools to measure other forms of mismanagement

- As new rules are ratified, we need to be watching
Moving Forward

• PKI community is using ZLint to focus removal investigations

• We should consider if small, regularly offending CAs are worth our trust
Moving Forward

• PKI community is using ZLint to focus removal investigations

• We should consider if small, regularly offending CAs are worth our trust

• ZLint enables *monitoring* of the certificate misissuance ecosystem

• We still need tools to measure other forms of mismanagement
Moving Forward

• PKI community is using ZLint to focus removal investigations

• We should consider if small, regularly offending CAs are worth our trust

• ZLint enables *monitoring* of the certificate misissuance ecosystem

• We still need tools to measure other forms of mismanagement

• As new rules are ratified, we need to be watching
Moving Forward

- PKI community is using ZLint to focus removal investigations
- We should consider if small, regularly offending CAs are worth our trust
- ZLint enables monitoring of the certificate misissuance ecosystem
- We still need tools to measure other forms of mismanagement
- As new rules are ratified, we need to be watching

Questions?

dkumar11@illinois.edu
@_kumarde