# 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*

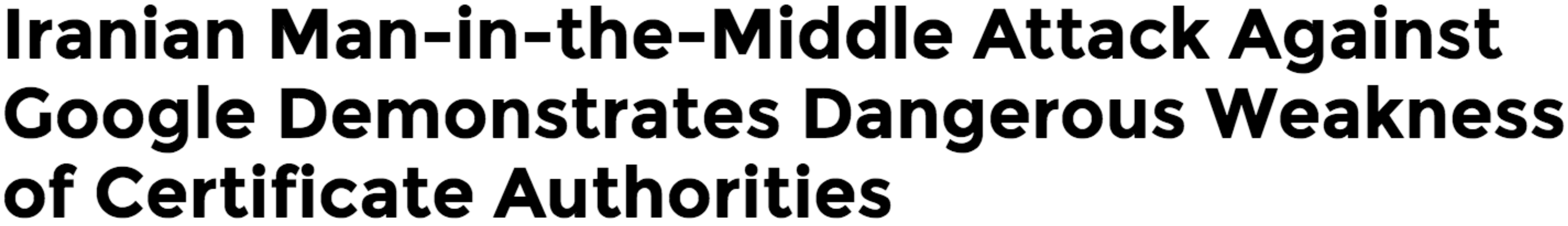
Joshua Mason
*University of Illinois*

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

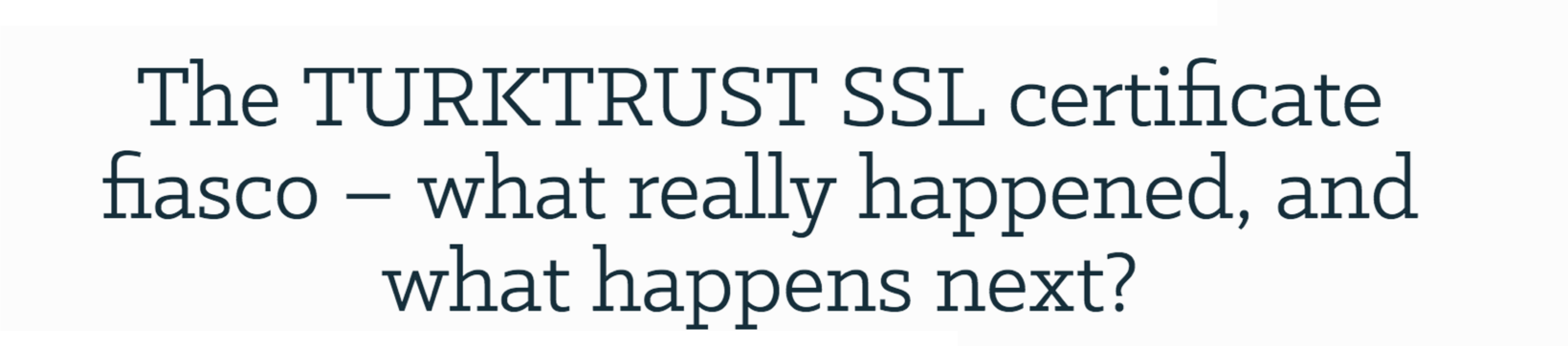
J. Alex Halderman
*University of Michigan*

Michael Bailey
*University of Illinois*

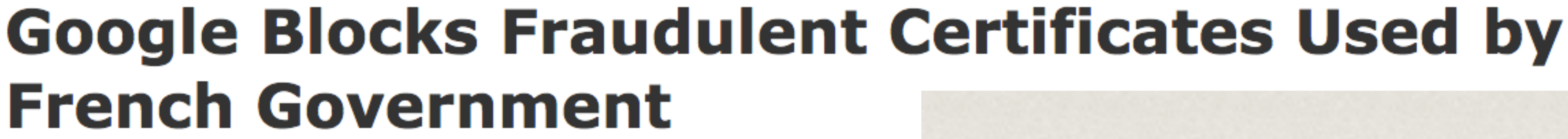
HTTPS relies on a supporting Public Key Infrastructure (PKI) composed of hundreds of Certificate Authorities (CAs)



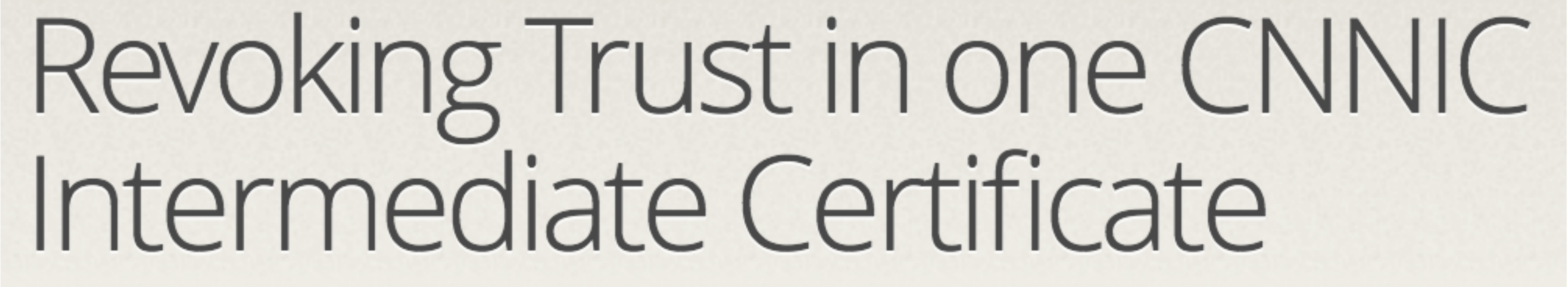
Iranian Man-in-the-Middle Attack Against Google Demonstrates Dangerous Weakness of Certificate Authorities



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



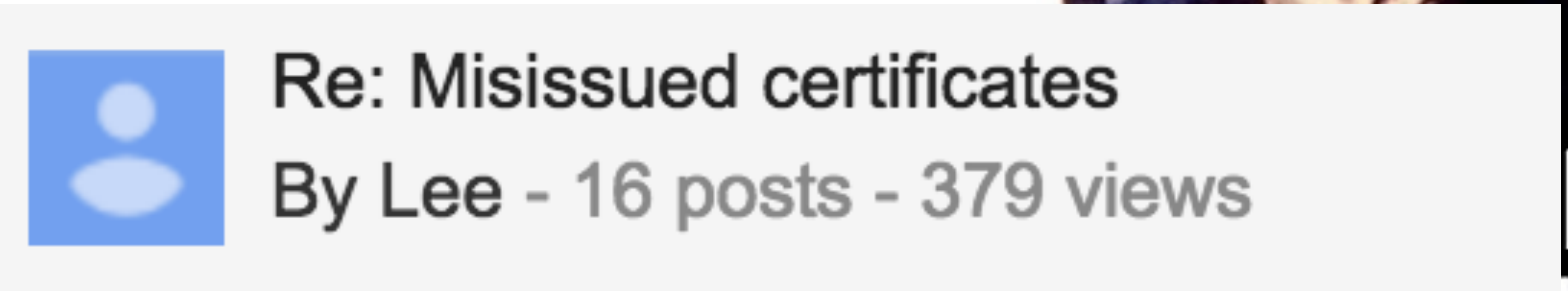
Google Blocks Fraudulent Certificates Used by French Government



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

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

Re: Misissued certificates
By Lee - 16 posts - 379 views

PROCERT issuing certificates with non-random serial numbers
By Andrew Ayer - 3 posts - 145 views

Miss-issuance: URI in dNSName SAN
By Alex Gaynor - 17 posts - 720 views

Fwd: Misissued certificates - pathLenConstraint with CA:FALSE
By Alex Gaynor - 3 posts - 221 views

Certificate with invalid dnsName issued from Baltimore intermediate
By Jonathan Rudenberg - 41 posts - 1120 views

invalid dnsNames
erg - 1 post - 382 views

Bad characters in dNSNames
5 views

Re: Misissued certificates
By Lee - 16 posts - 379 views

Certificates with improperly normalized IDNs
By Jonathan Rudenberg - 8 posts - 275 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

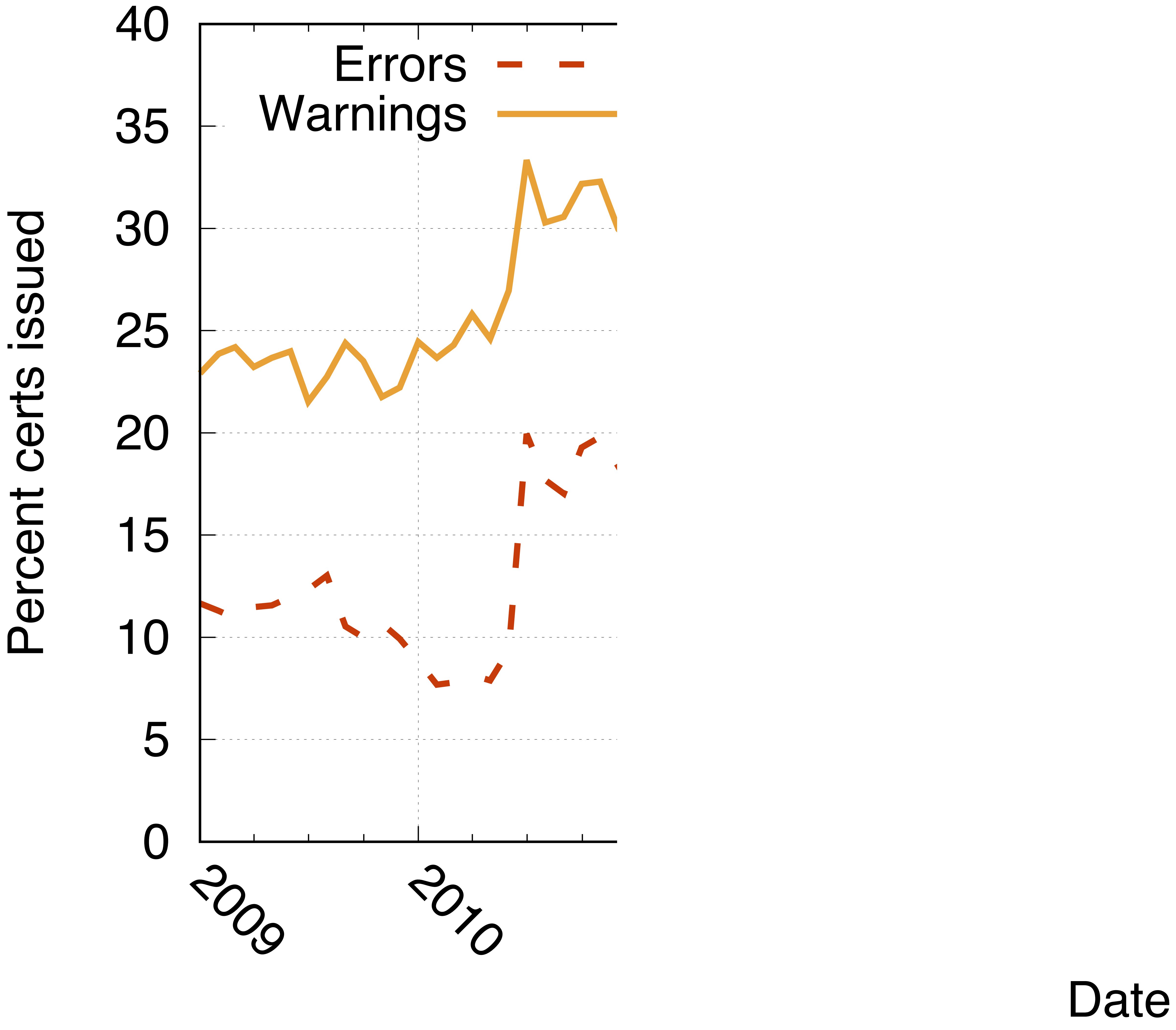
# Collecting Certificates

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

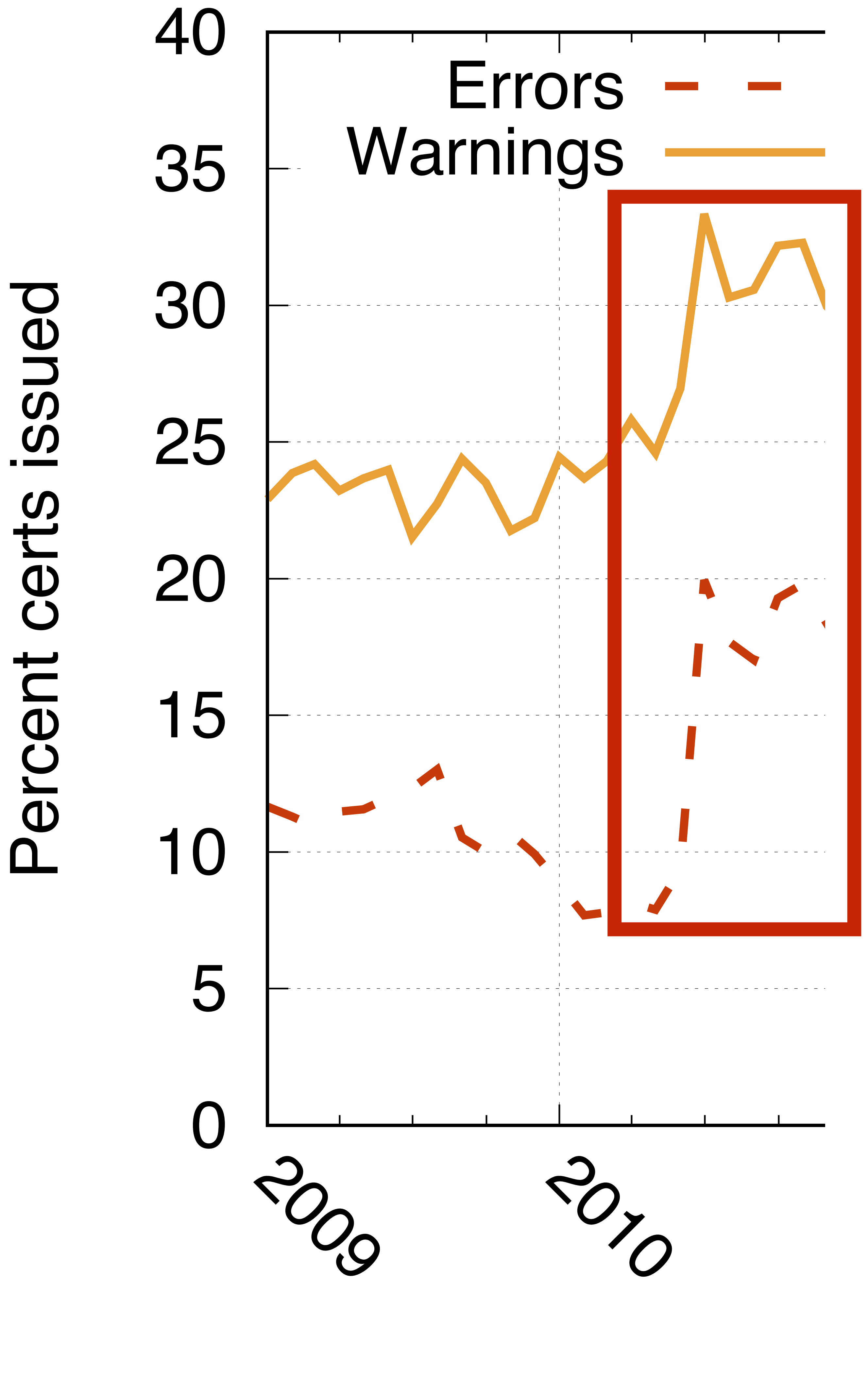
# Collecting Certificates

- 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

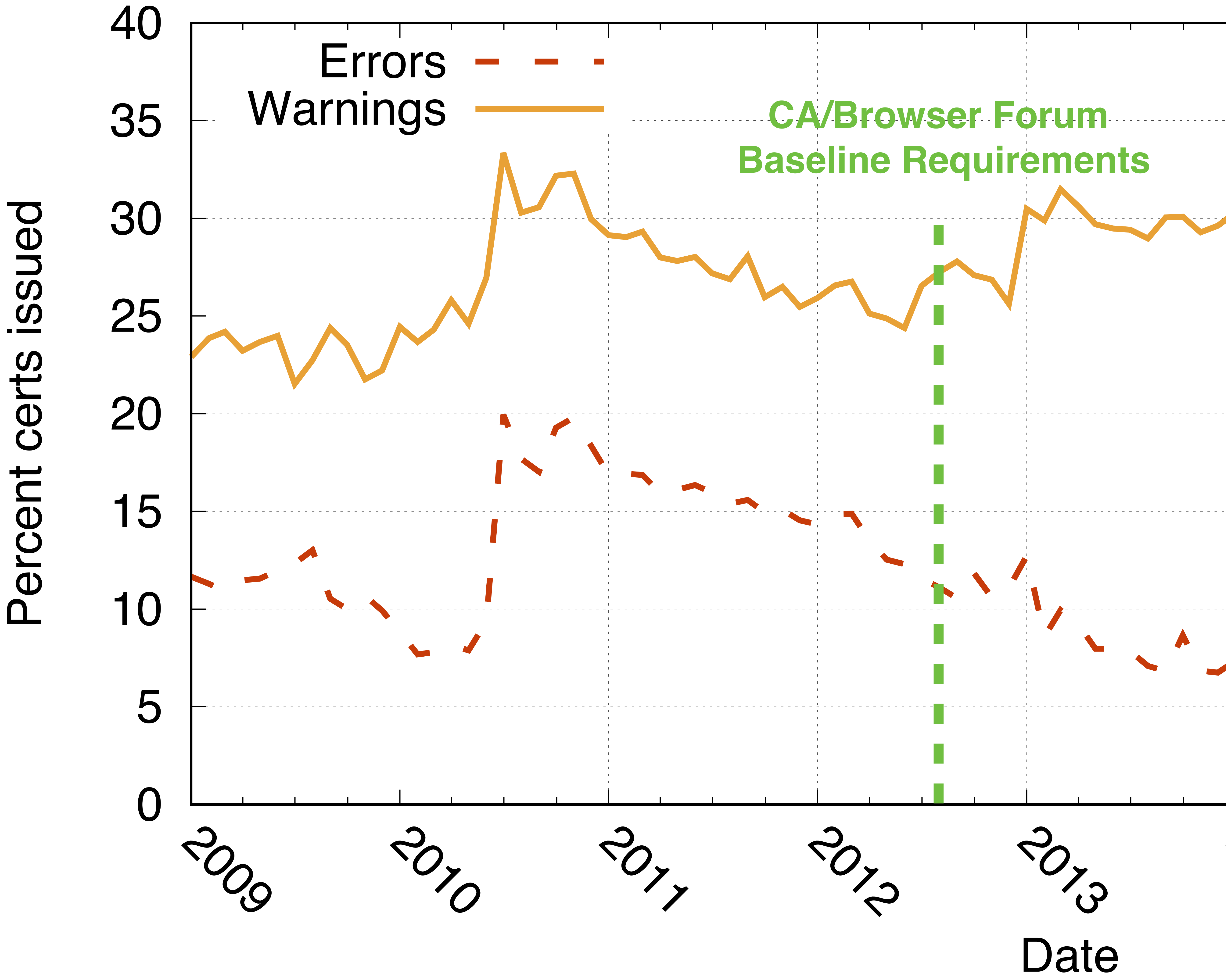
# Historical Misissuance



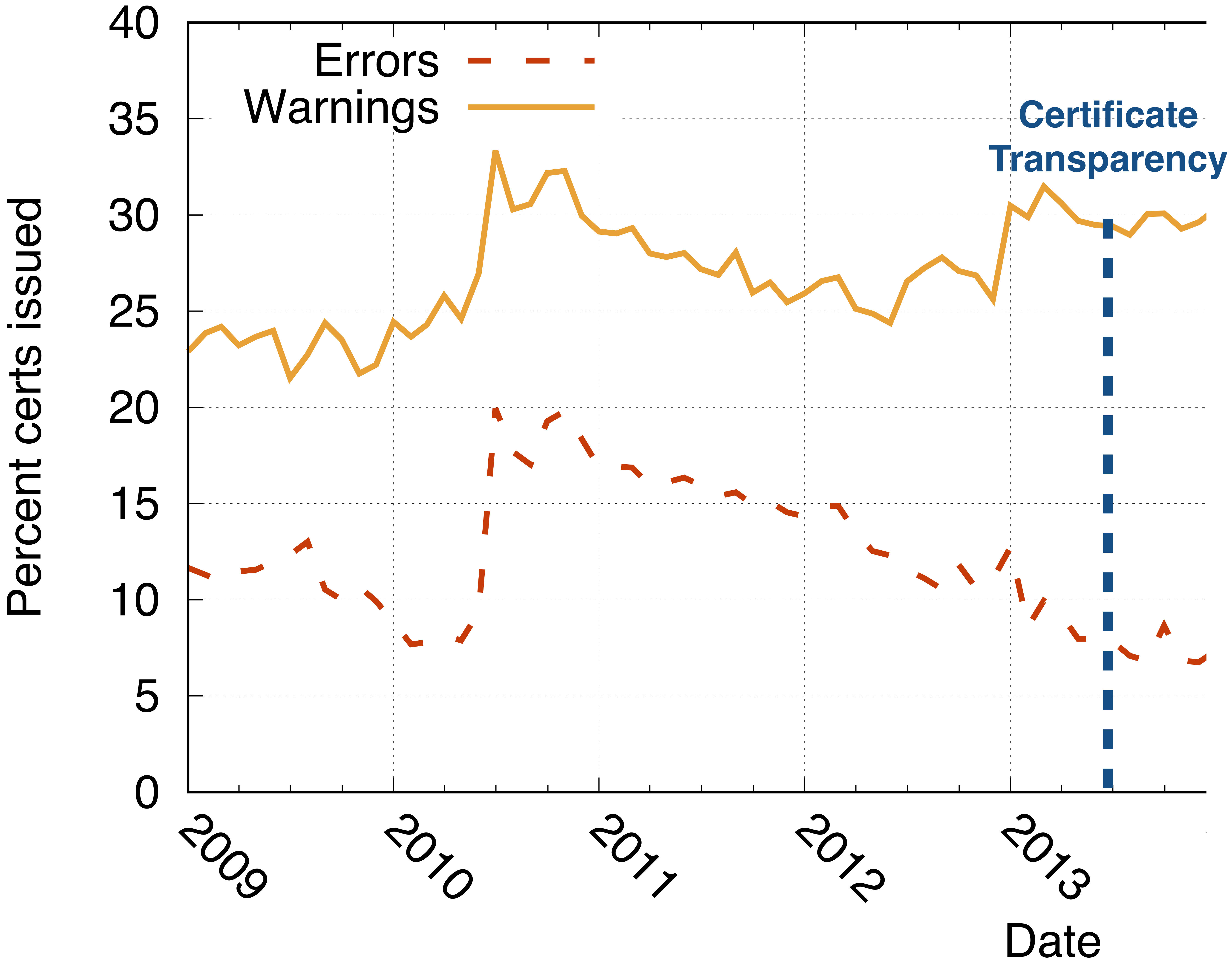
# Historical Misissuance



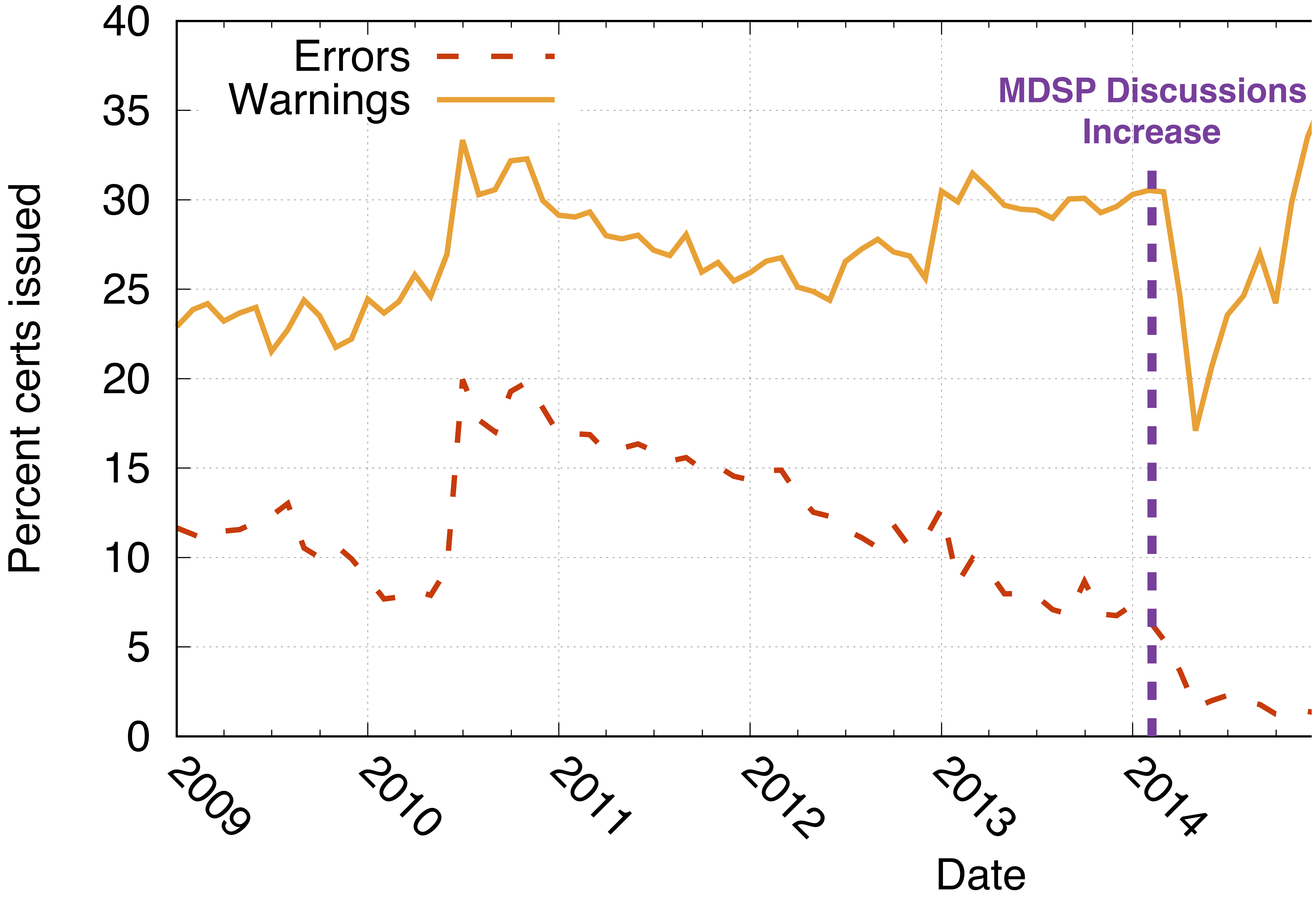
# Historical Misissuance



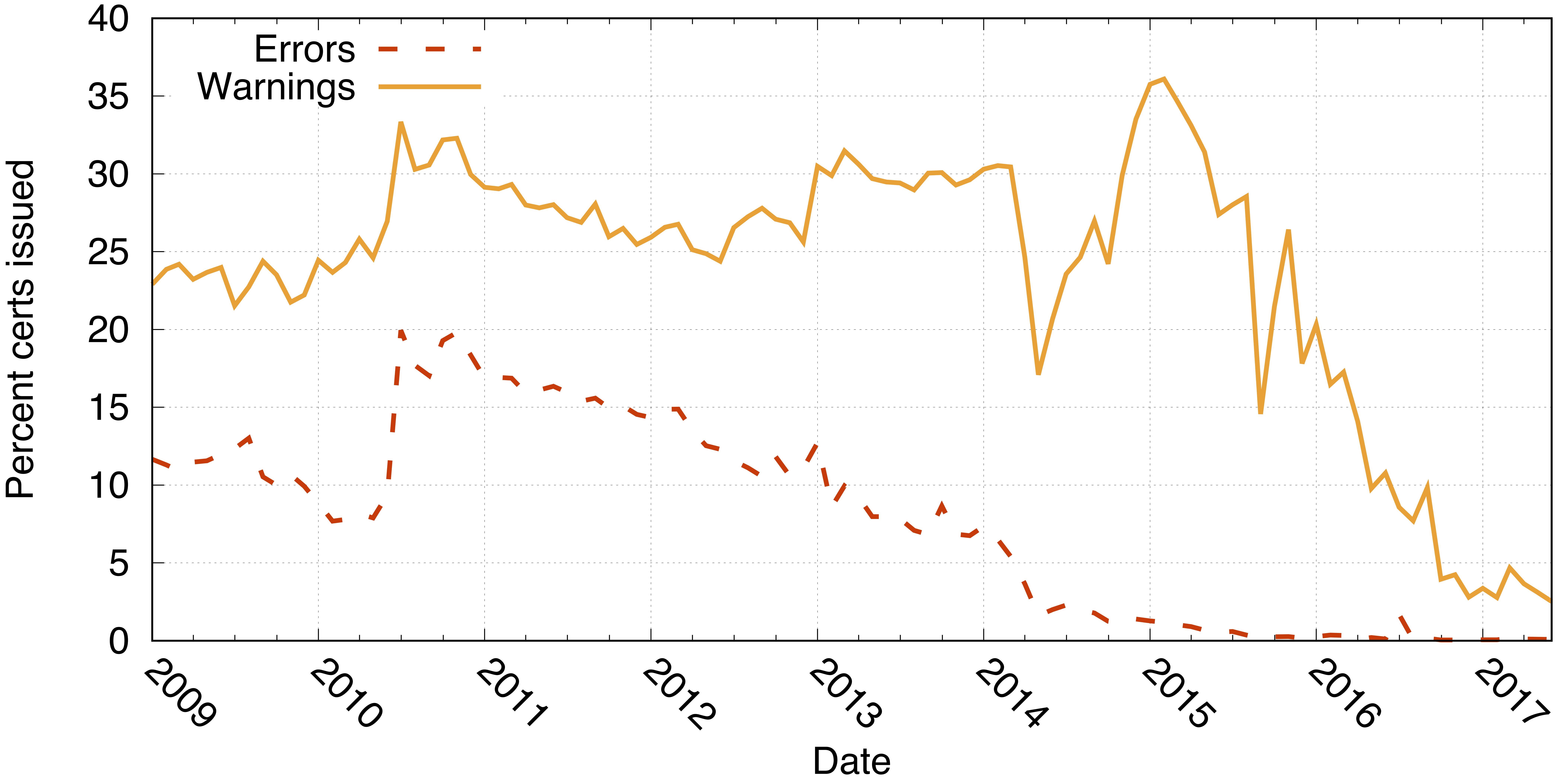
# Historical Misissuance



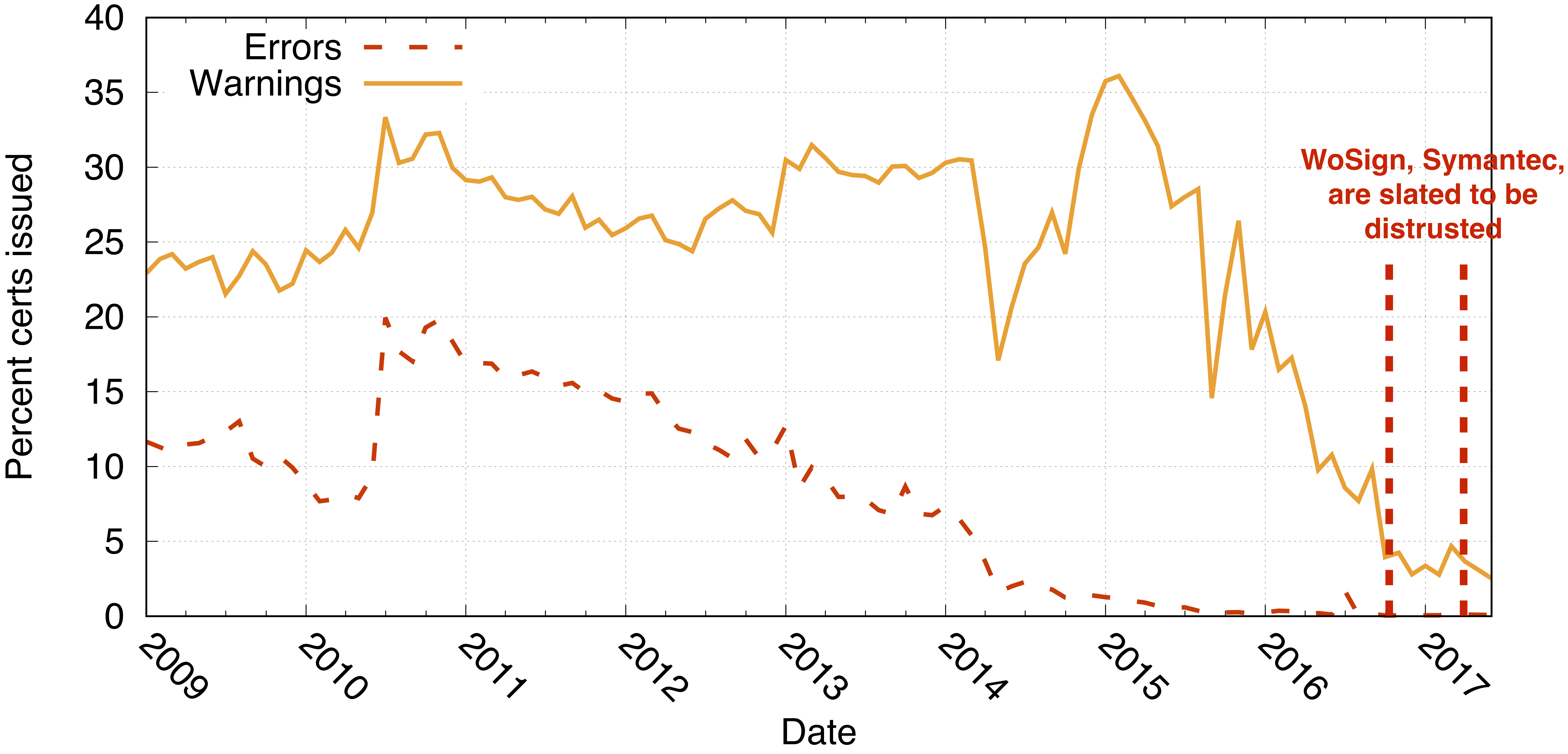
# Historical Misissuance



# Historical Misissuance

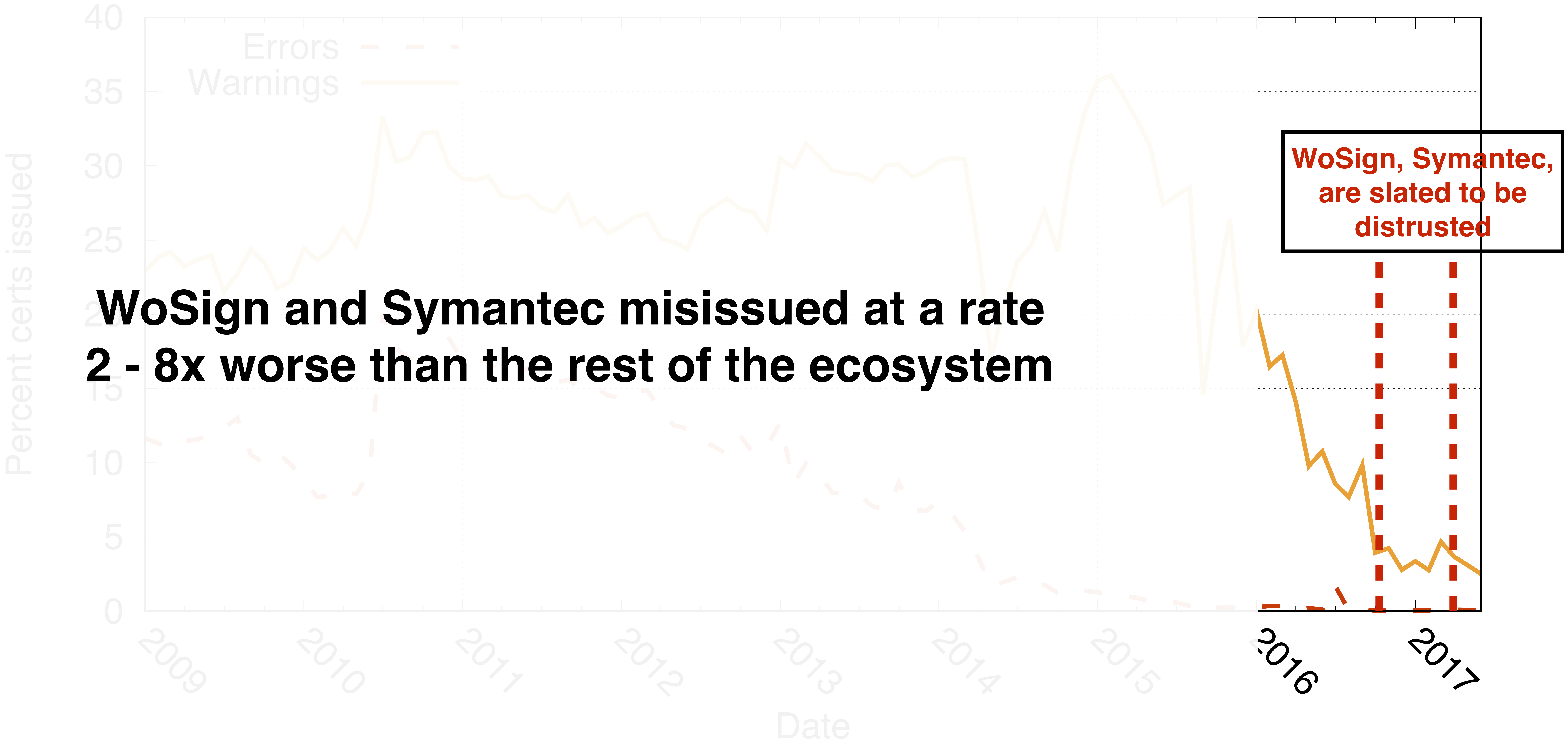


# Historical Misissuance



WoSign, Symantec, are slated to be distrusted

# Historical Misissuance



WoSign, Symantec, are slated to be distrusted

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

# Largest Misissuers

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

# Largest Misissuers

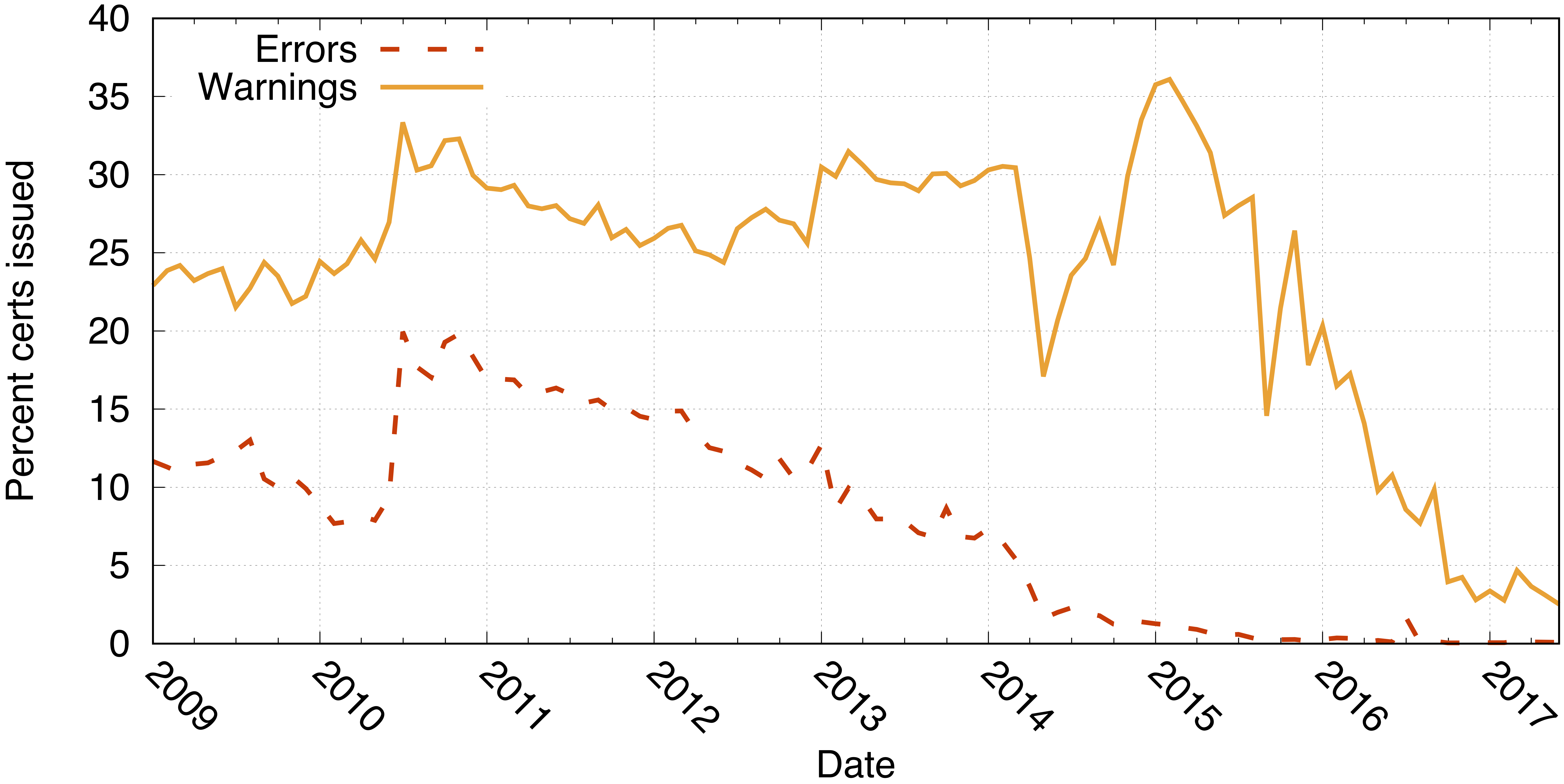
| Issuer | Certificates | w/ Errors |
|---|---|---|
| GoDaddy | 1.6M (2.7%) | 38,215 (2.4%) |
| **Symantec** | 2.7M (4.6%) | 23,053 (0.8%) |
| **StartCom, Ltd.** | 536K (0.9%) | 11,617 (2.1%) |
| **WoSign CA Lmtd.** | 196K (0.3%) | 9,849 (5%) |
| **VeriSign** | 43K (0.07%) | 9,835 (23.1%) |

# Largest Misissuers

| Issuer | Certificates | w/ Errors |
|---|---|---|
| GoDaddy | 1.6M (2.7%) | 38,215 (2.4%) |
| Symantec | 2.7M (4.6%) | 23,053 (0.8%) |
| StartCom Ltd. | 580K (0.9%) | 1,617 ([illegible]1%) |
| WoSign CA Lmtd. | 196K (0.3%) | **9,849 (5%)** |
| VeriSign | 43K (0.07%) | **9,835 (23.1%)** |

Browsers are taking down the largest offenders

# Historical Misissuance



# Misissuance by Largest Issuers

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

# Misissuance by Largest Issuers

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

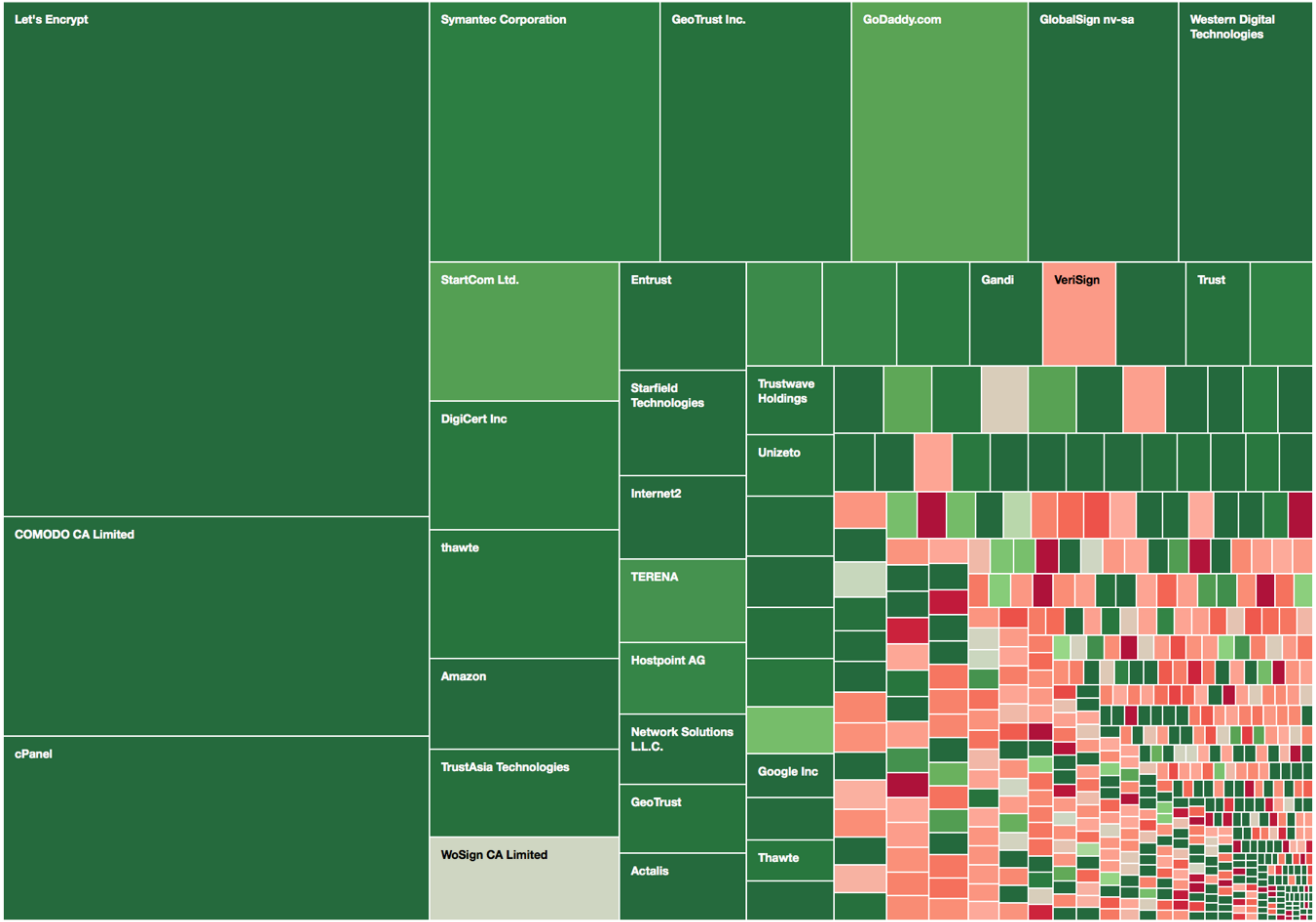
# Misissuance by Largest Issuers

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

# Misissuance by Largest Issuers

| Issuer | Certificates | w/ Errors |
|---|---|---|
| Let's Encrypt | 37M (61%) | **13 (0.0%)** |
| Comodo | 6.7M (11%) | **[illegible] (0.0%)** |
| cPanel | 4.7M (7.8%) | **131 (0.0%)** |
| Symantec | 2.8M (4.6%) | **23,053 (0.8%)** |
| GeoTrust, Inc. | 1.9M (3.2%) | **5,694 (0.3%)** |
| GoDaddy | 1.6M (2.7%) | **38,215 (2.0%)** |
| GlobalSign | 1.2M (1.9%) | **837 (0.0%)** |

Large CAs misissue a small fraction of their certificates


Let's Encrypt
Symantec Corporation
GeoTrust Inc.
GoDaddy.com
GlobalSign nv-sa
Western Digital Technologies
StartCom Ltd.
Entrust
Gandi
VeriSign
Trust
Starfield Technologies
Trustwave Holdings
DigiCert Inc
Unizeto
Internet2
COMODO CA Limited
thawte
TERENA
Amazon
Hostpoint AG
Network Solutions L.L.C.
cPanel
TrustAsia Technologies
Google Inc
GeoTrust
WoSign CA Limited
Thawte
Actalis

# 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?

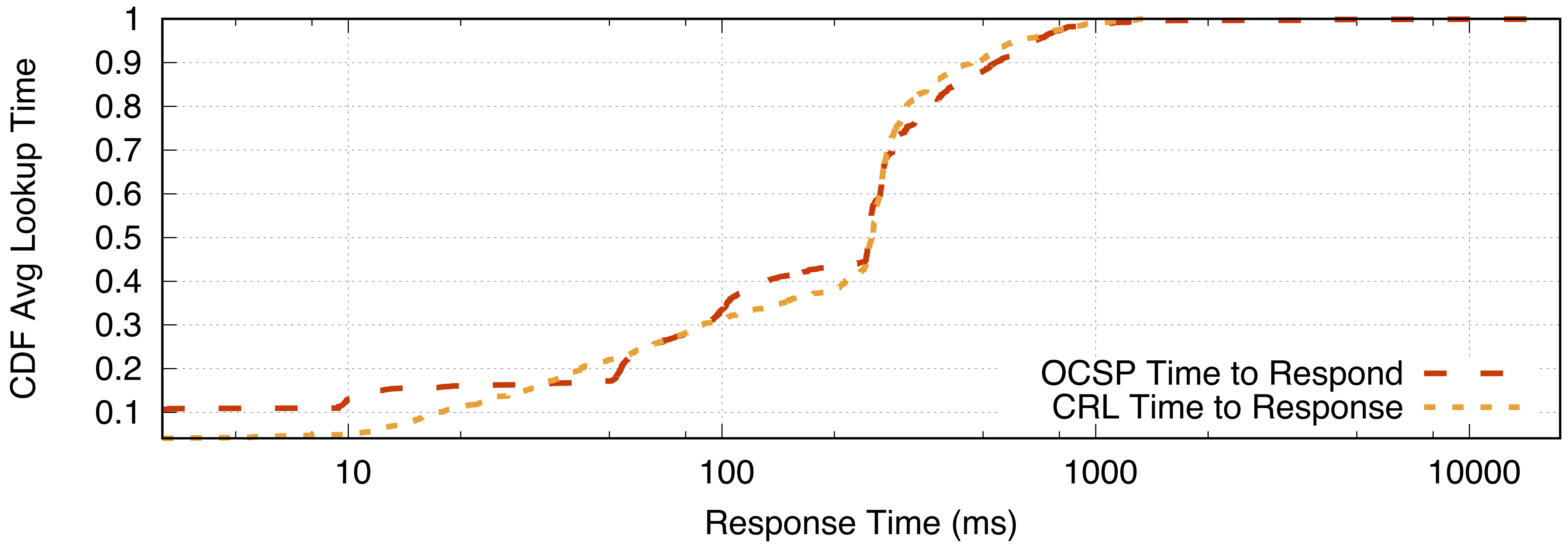
# CA Management: Revocation

- OCSP Responders
- CRLs

**Strict rules associated with revocation service response times**

# CA Revocation Measurement

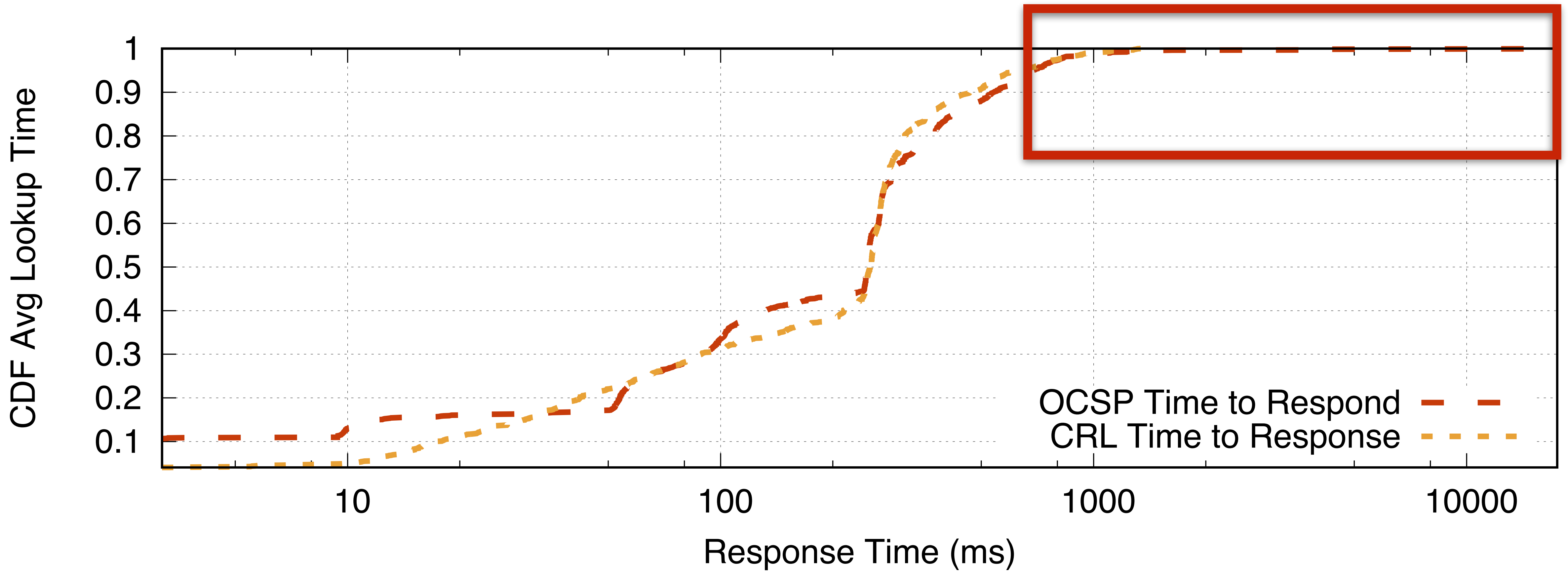
- Made a valid OCSP, CRL request to all responders every hour from Sept 1 - 20, 2017



# 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

| | Errors | Warnings |
|---|---|---|
| **OCSP Responders** | 0.10 (p-value: < 0.01) | 0.19 (p-value: < 0.01) |
| **CRL Distribution Points** | 0.07 (p-value: 0.01) | 0.17 (p-value: < 0.01) |

# Correlating ZLint with Mismanagement

| | **Errors** | **Warnings** |
|---|---|---|
| **OCSP Responders** | **0.10 (p-value: < 0.01)** | **0.19 (p-value: < 0.01)** |
| **CRL Distribution Points** | 0.07 (p-value: 0.01) | **0.17 (p-value: < 0.01)** |

# 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

crt.sh

censys
Security driven by data

# ZLint will be Deployed

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

**certificates**: Available through Censys

crt.sh

censys

Security driven by data

Google

# Moving Forward

- PKI community is using ZLint to focus removal investigations

# 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**