# The ICSI SSL Notary

## Lessons and Insights from a Large-Scale Study of the SSL/TLS Ecosystem

Bernhard Amann[1], Matthias Vallentin[2], Robin Sommer[1,3]

International Computer Science Institute[1]
UC Berkeley[2]
Lawrence Berkeley National Laboratory[3]

# ICSI SSL Notary

Monitor certificates in real-time

Strong research interest in SSL

Problem: lack of data

- few measurements
- most of them active
- spanning a short time

Provide access to the community

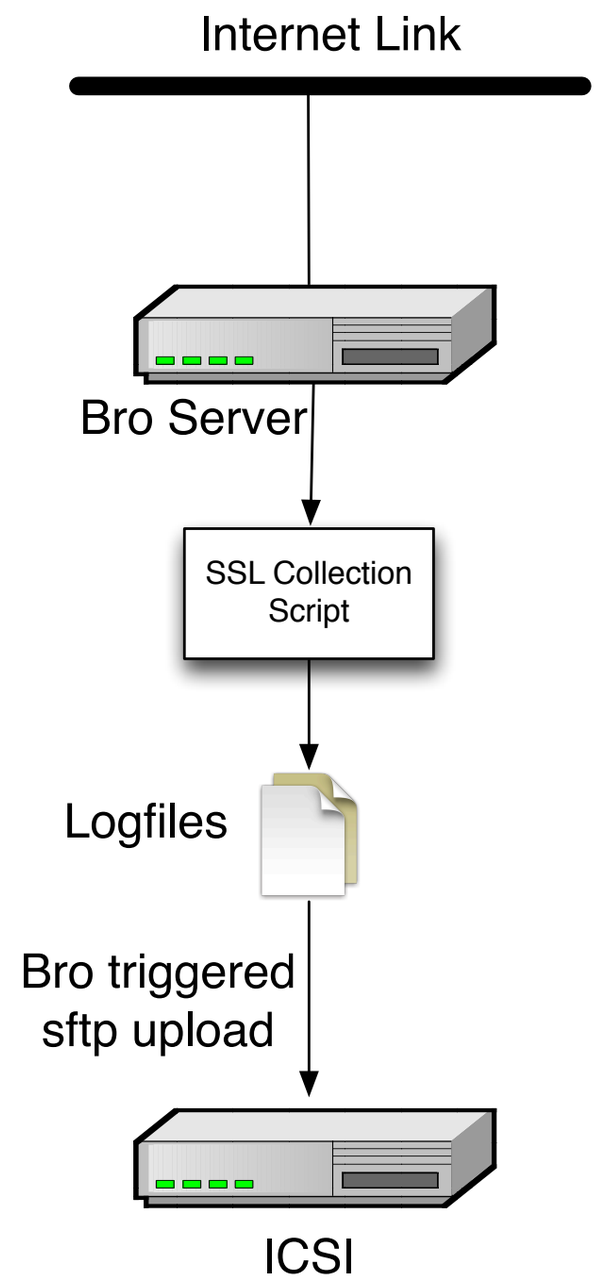
# Collection Setup

Sites running Bro network monitor
- add SSL data collection script
- SSL traffic identified using DPD

Result: 2 log files
- uploaded to ICSI on rotation
- not kept on local machine

collection script distributed via Git

ICSI has no access to raw data



# Collection Setup

## Collected Features:

| | |
|---|---|
| Available ciphers | Hash(server session ID) |
| Analyzer Error | Packet loss |
| Client TLS extensions | Selected cipher |
| Content length | Server certificates |
| Connection history | Server IP |
| Duration | Server Name Indication |
| Hash(client IP, server IP) | Ticket lifetime hint |
| Hash(client IP, SNI) | Timestamp |
| Hash(client session ID) | Version |

# Collection Setup

## Collected Features:

| | |
|---|---|
| Available ciphers | Hash(server session ID) |
| Analyzer Error | Packet loss |
| Client TLS extensions | Selected cipher |
| [illegible] | Server certificates |
| Connecti[illegible] | |
| Duration | Server Name Indication |
| Hash(client IP, server IP) | Ticket lifetime hint |
| Hash(client IP, SNI) | Timestamp |
| Hash(client session ID) | Version |

Link

Site

a

S

Vie

u

r

col

ICS

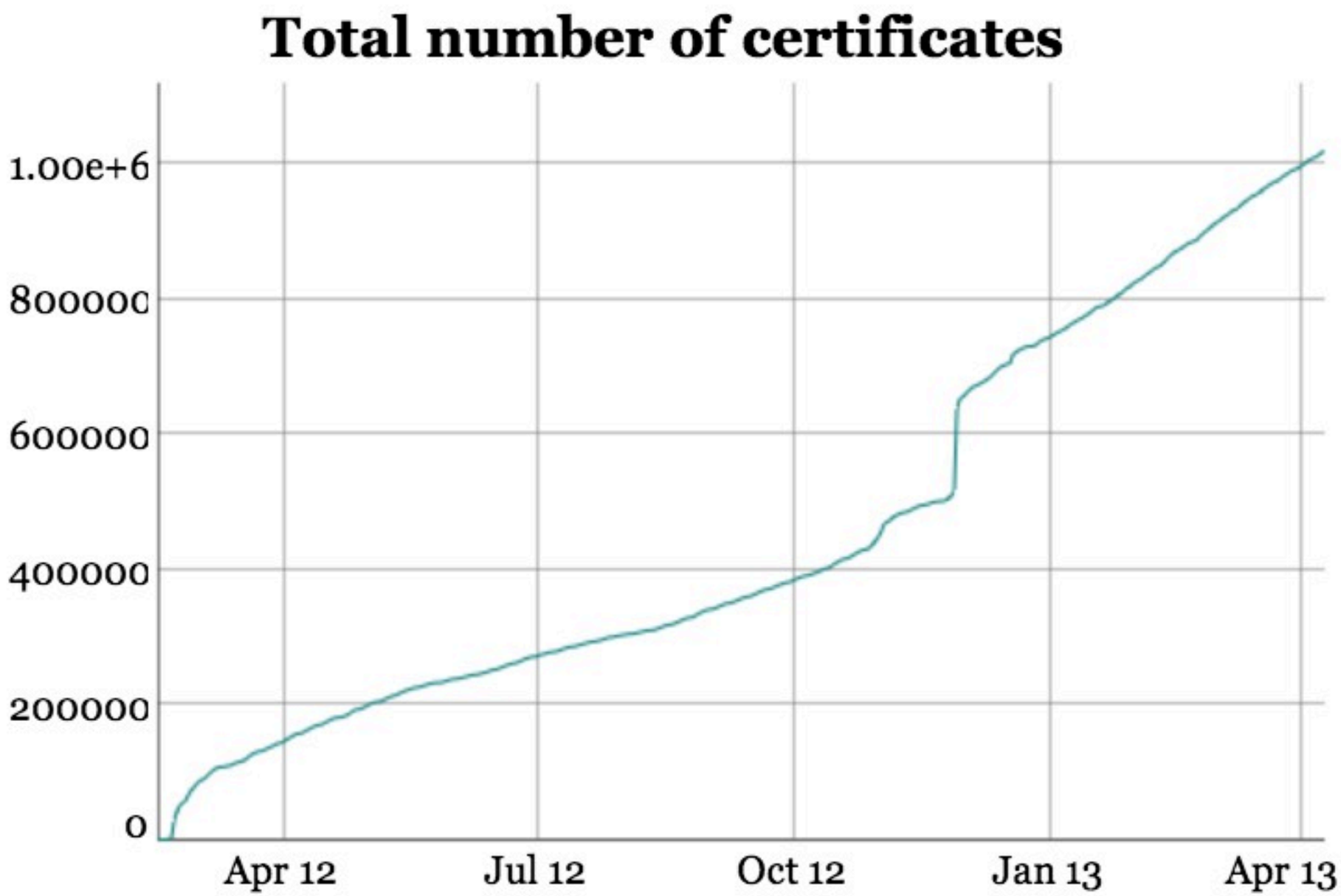
tion

ency

# Notary Data Providers

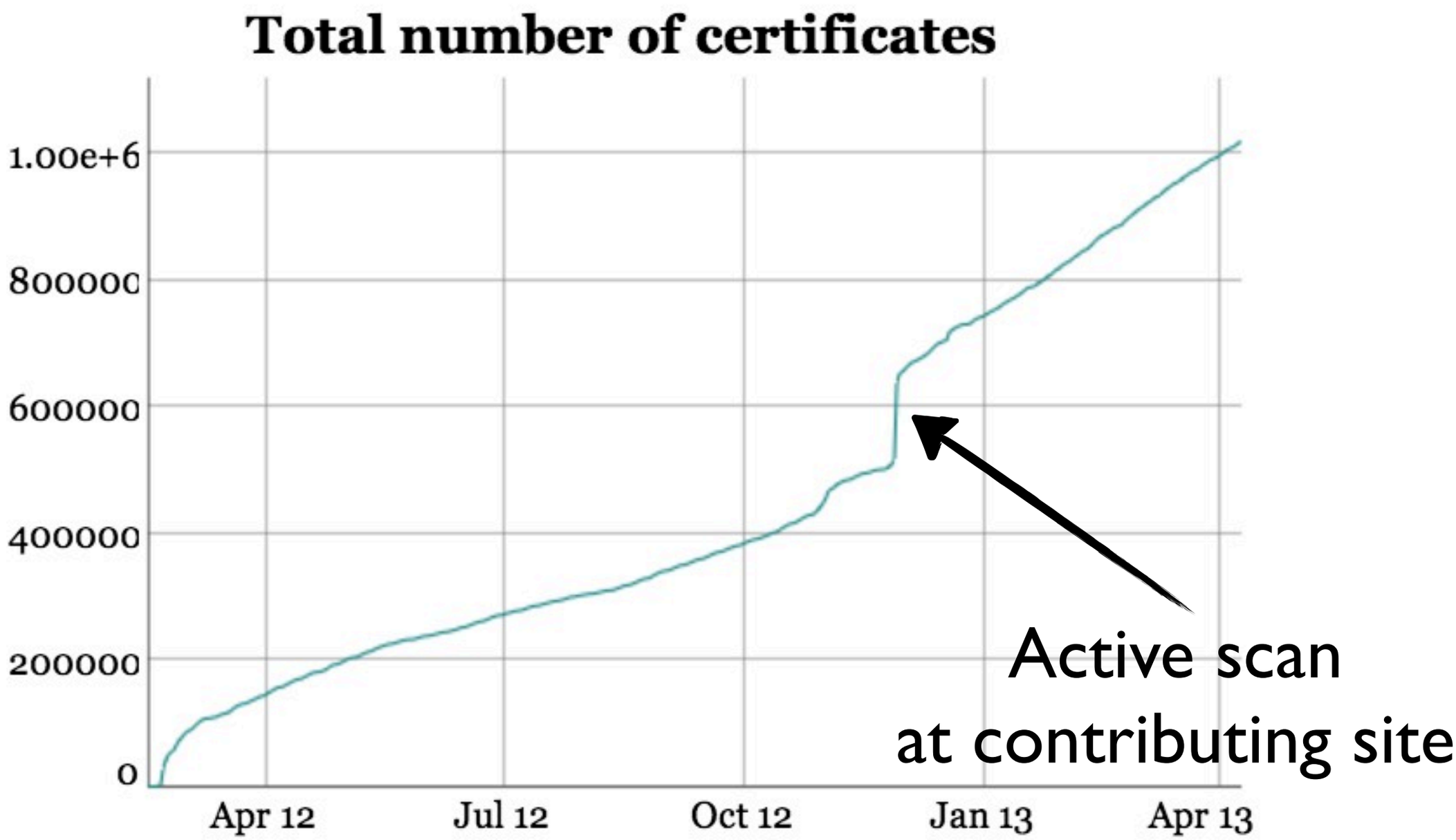
| Site | Users | Certs Total | Certs Filtered | Sessions | Duration (days) |
|---|---|---|---|---|---|
| University 1 | 90,000 | 36M | 631K | 6.2G | 339 |
| University 2 | 50,000 | 569K | 292K | 4.7G | 280 |
| University 3 | 3,000 | 14K | 8.8K | 10M | 142 |
| University 4 | 30,000 | 193K | 121K | 517M | 126 |
| University 5 | 100,000 | 355K | 195K | 3.3G | 118 |
| University 6 | 10,000 | 55K | 40K | 468M | 99 |
| Research Lab 1 | 250 | 443K | 35K | 72M | 350 |
| Research Lab 2 | 4,000 | 171K | 98K | 747M | 304 |
| Gov. Network | 50,000 | 137K | 127K | 228M | 317 |
| Backbone Net. | 30,000 | 18K | 18K | 65M | 107 |
| **Total** (Unique) | **314,250** | 37.5M | **842K** | **16.3G** | - |

# Number of certificates



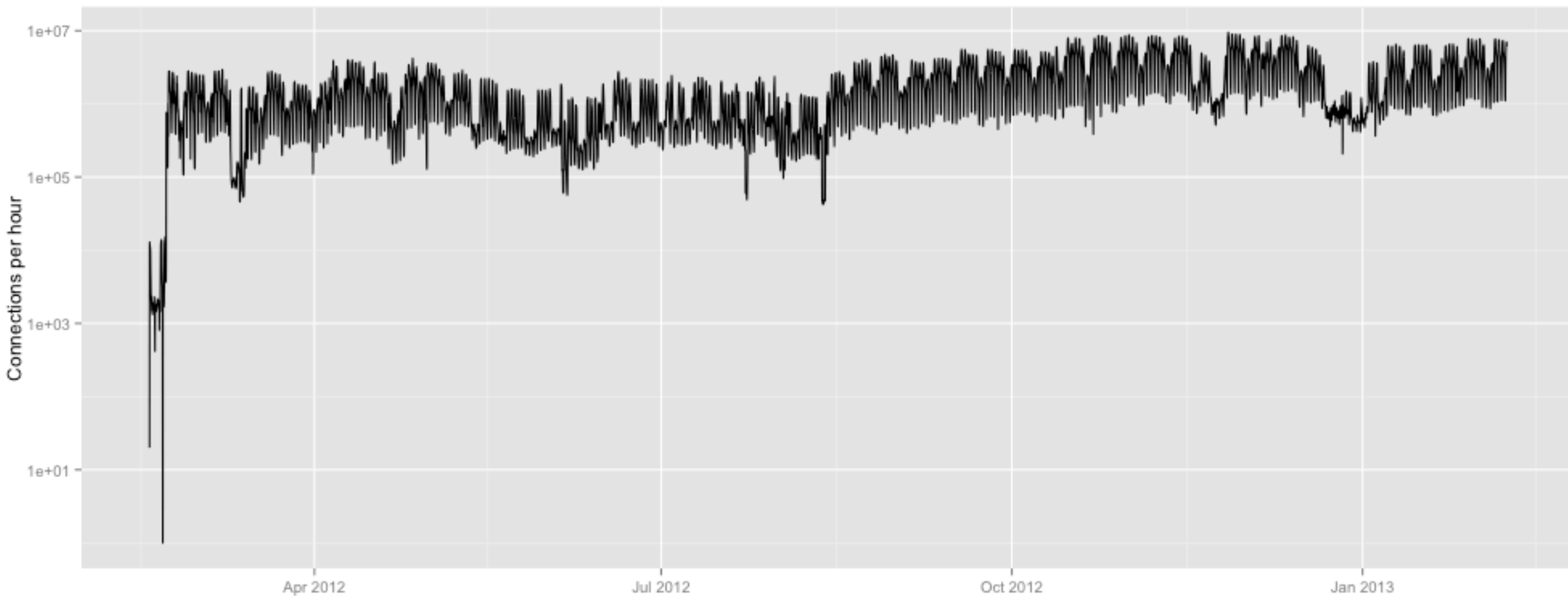

http://notary.icsi.berkely.edu

# Number of certificates

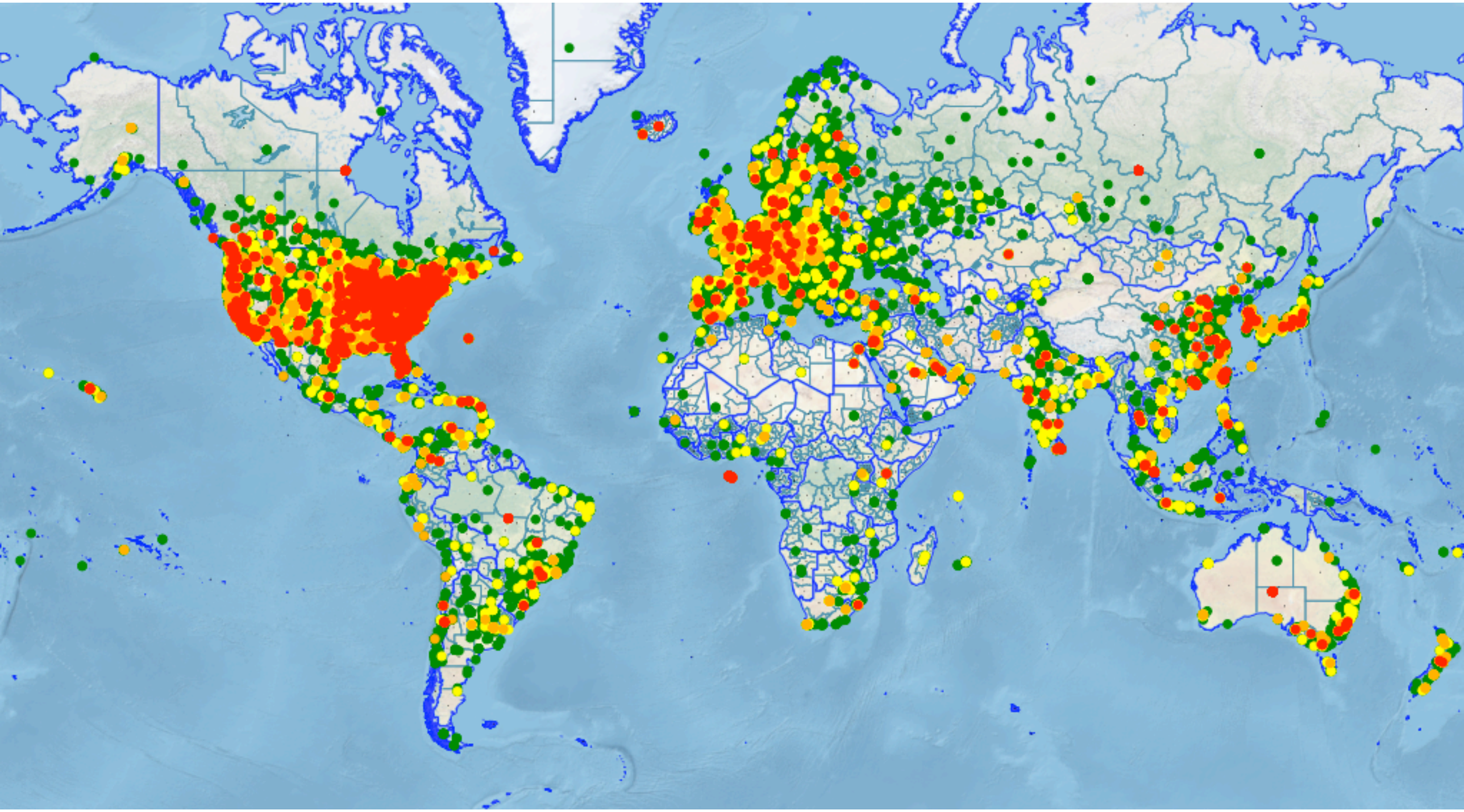



http://notary.icsi.berkely.edu

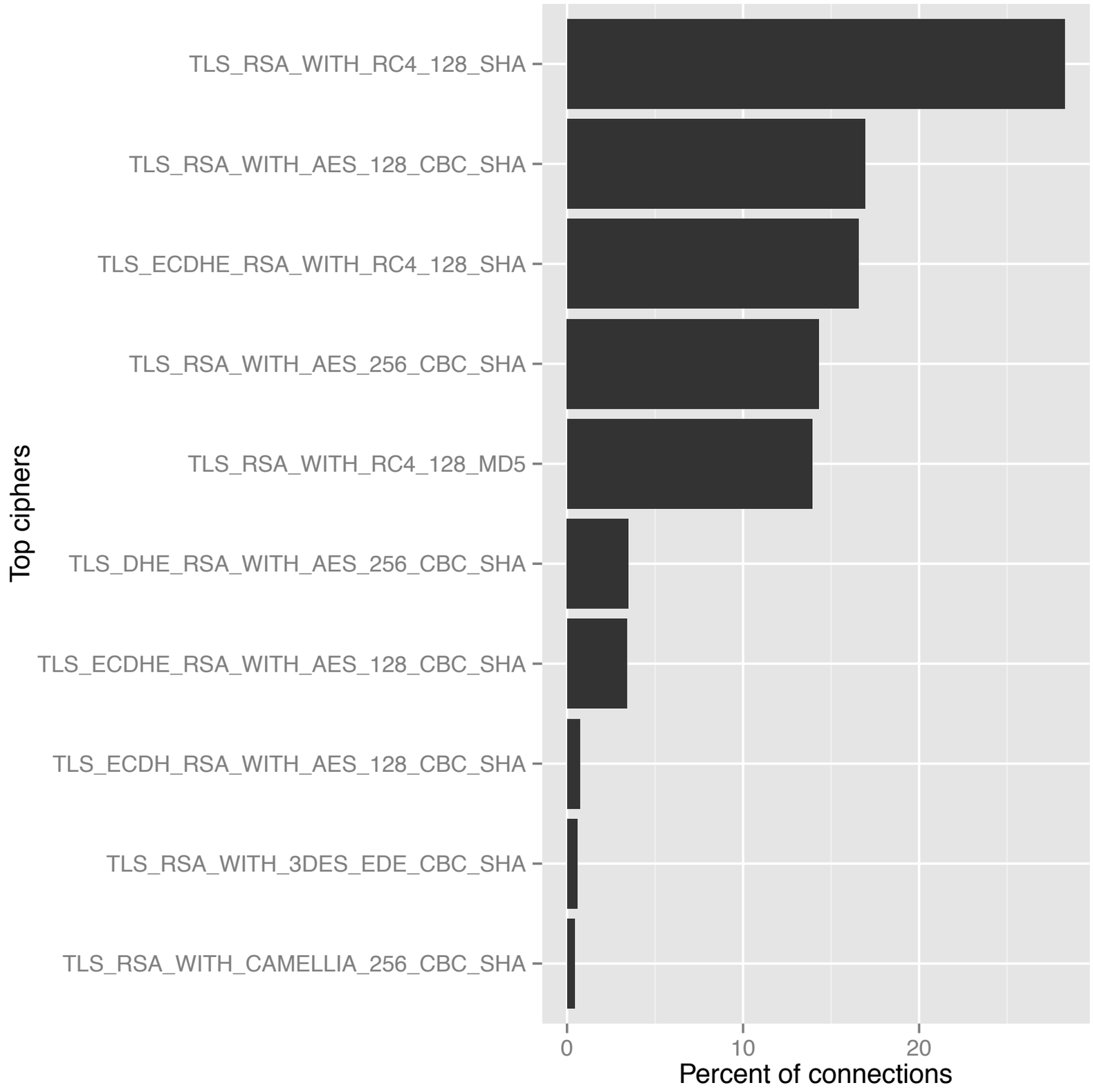
# Connections per Hour



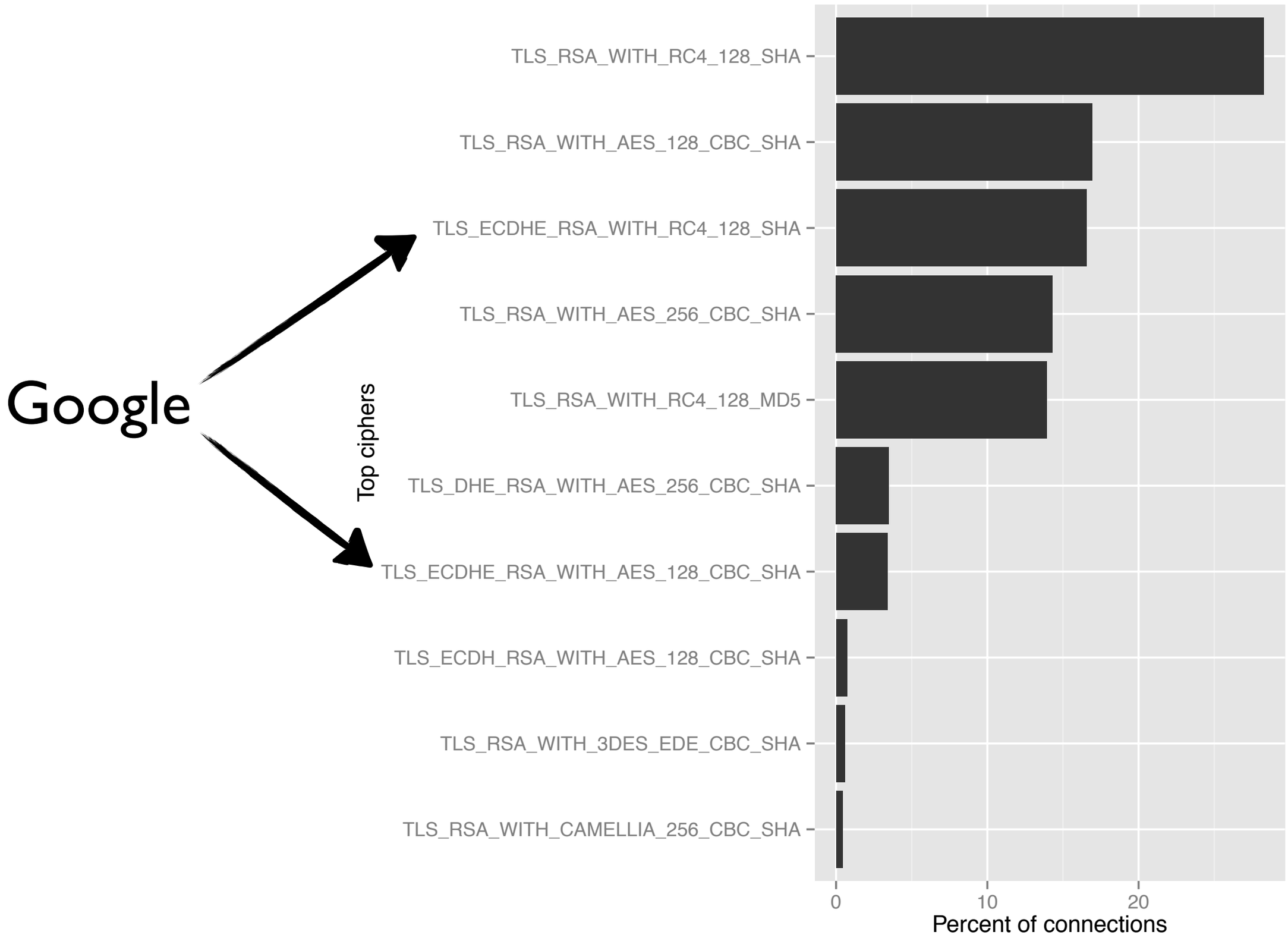
# Server distribution



# Top connection Ciphers



# Top connection Ciphers



# Certificate Issuers

| | Root |
|---|---|
| 19% | GeoTrust |
| 18% | Go Daddy |
| 12% | AddTrust |
| 10% | VeriSign (1) |
| 6.1% | GlobalSign |
| 5.0% | USERTRUST |
| 4.6% | DigiCert |
| 4.0% | Thawte (1) |
| 3.8% | Thawte (2) |
| 3.4% | VeriSign (2) |

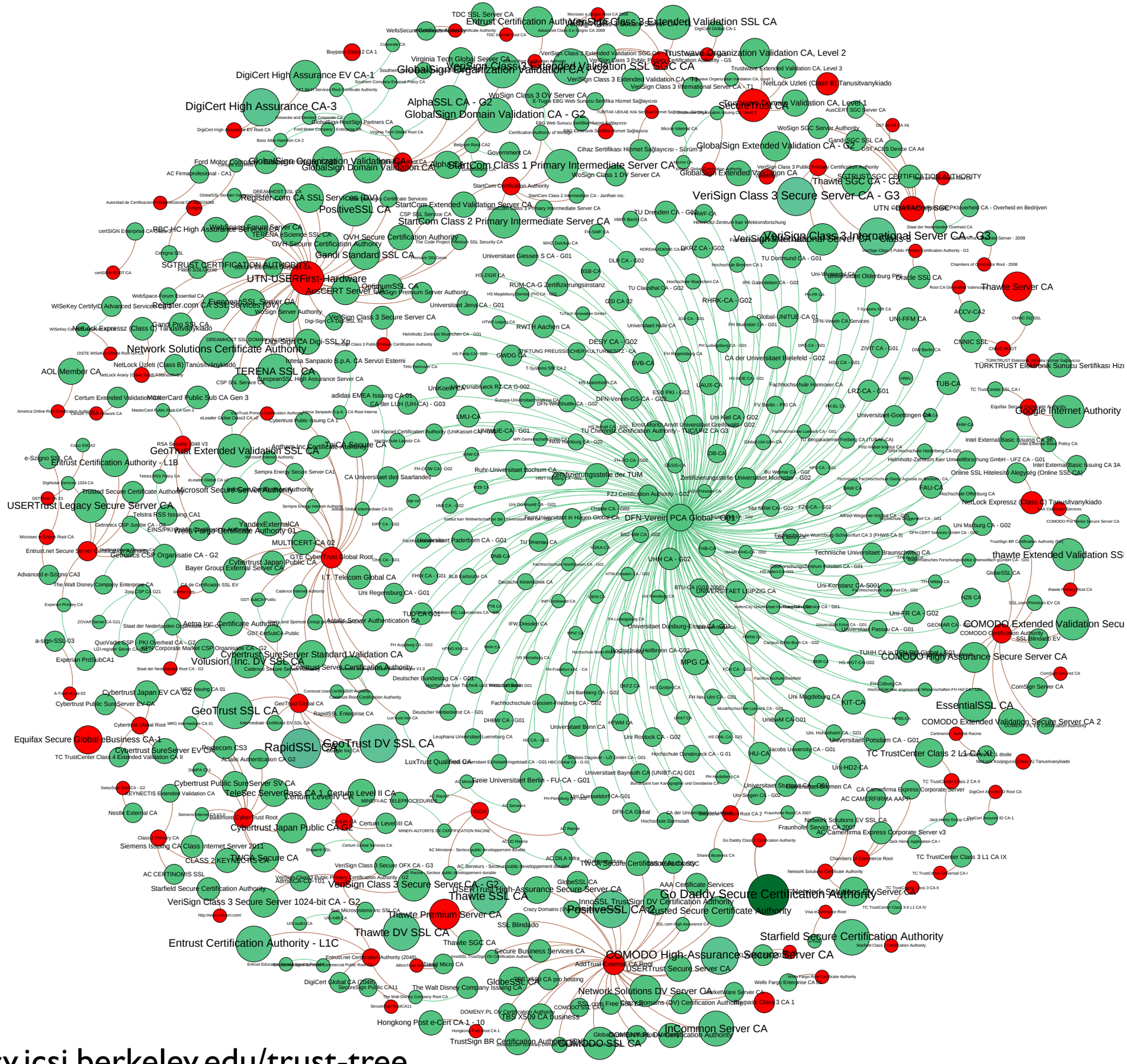
# Certificate Issuers

| | Root | Owner |
|---|---|---|
| 19% | GeoTrust | Symantec |
| 18% | Go Daddy | GoDaddy |
| 12% | AddTrust | Comodo |
| 10% | VeriSign (1) | Symantec |
| 6.1% | GlobalSign | GlobalSign |
| 5.0% | USERTRUST | Comodo |
| 4.6% | DigiCert | DigiCert |
| 4.0% | Thawte (1) | Symantec |
| 3.8% | Thawte (2) | Symantec |
| 3.4% | VeriSign (2) | Symantec |

# Certificate Issuers

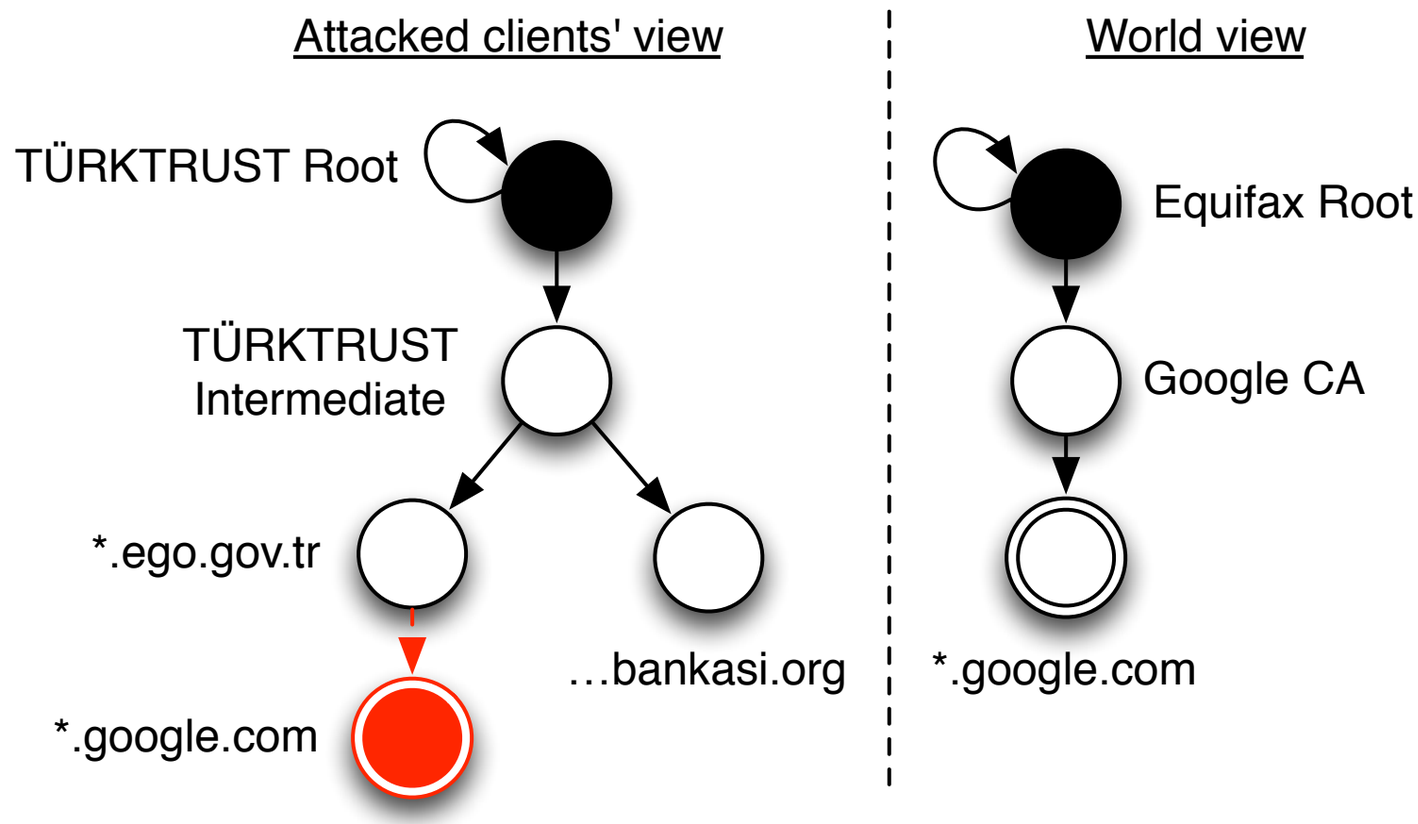
| | Root | Owner |
|---|---|---|
| 19% | GeoTrust | Symantec |
| 18% | Go Daddy | GoDaddy |
| 12% | AddTrust | Comodo |
| 10% | VeriSign (1) | Symantec |
| 6.1% | GlobalSign | GlobalSign |
| 5.0% | USERTRUST | Comodo |
| 4.6% | DigiCert | DigiCert |
| 4.0% | Thawte (1) | Symantec |
| 3.8% | Thawte (2) | Symantec |
| 3.4% | VeriSign (2) | Symantec |

| | Used Roots | Owner |
|---|---|---|
| 42% | 13 | Symantec |
| 20% | 3 | GoDaddy |
| 19% | 5 | Comodo |
| 6.3% | 2 | GlobalSign |
| 4.6% | 3 | DigiCert |
| 3.1% | 3 | Entrust |
| 1.5% | 1 | StartCom |
| 1.2% | 3 | Verizon |
| 0.87% | 2 | Trustwave |
| 0.47% | 1 | Telekom |




http://notary.icsi.berkeley.edu/trust-tree

# CA Incidents: Türktrust



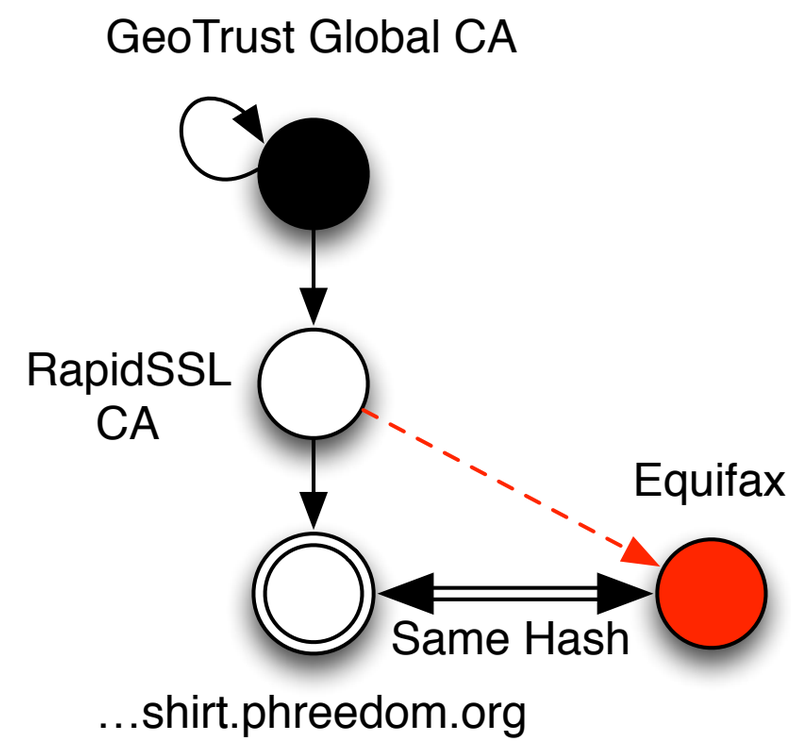

Türktrust issued two CA certificates to two of their customers
Reason: wrong profiles were copied between test and production

At some point one of the sites apparently noticed
...and began to MITM their local users

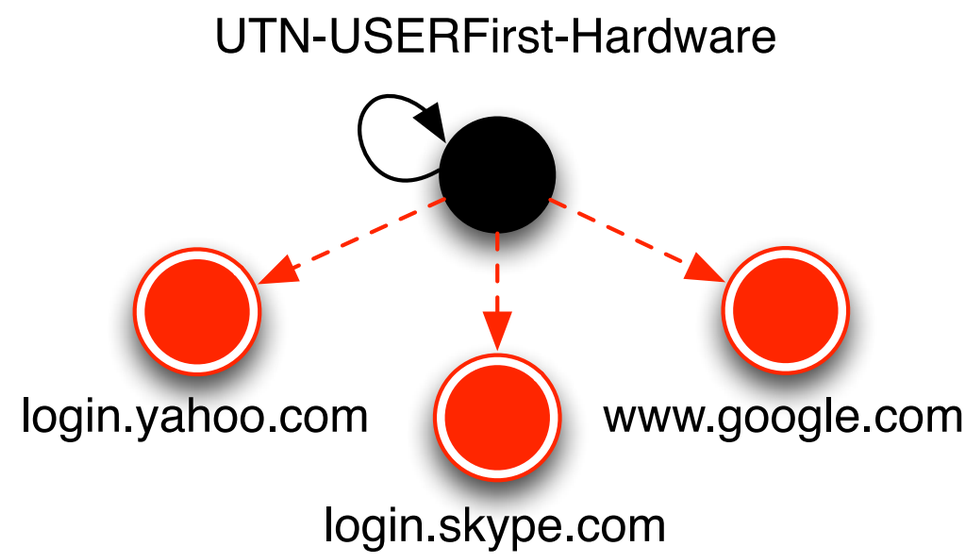
# CA Attacks: RapidSSL, Flame

RapidSSL: MD5 collision attack
- Demonstrated at CCC
- Not enough certificate entropy
- Predicatable serial & timestamp

Repeated by flame
- with higher amount of entropy
- Attackers had to predict timestamp with millisecond resolution



# Other CA Incidents




Comodo: certificates for google, mozilla, live.com, skype, ...

DigiNotar: completely compromised CA
- *.google.com, *.skype.com, *.*.com
- intermediate CAs
- enabled for EV

Trustwave: issued intermediate CA for DLP system

# Changes in January 2013

741,424 total certificates

489,551 valid

80,477 new

54,321 validate correctly

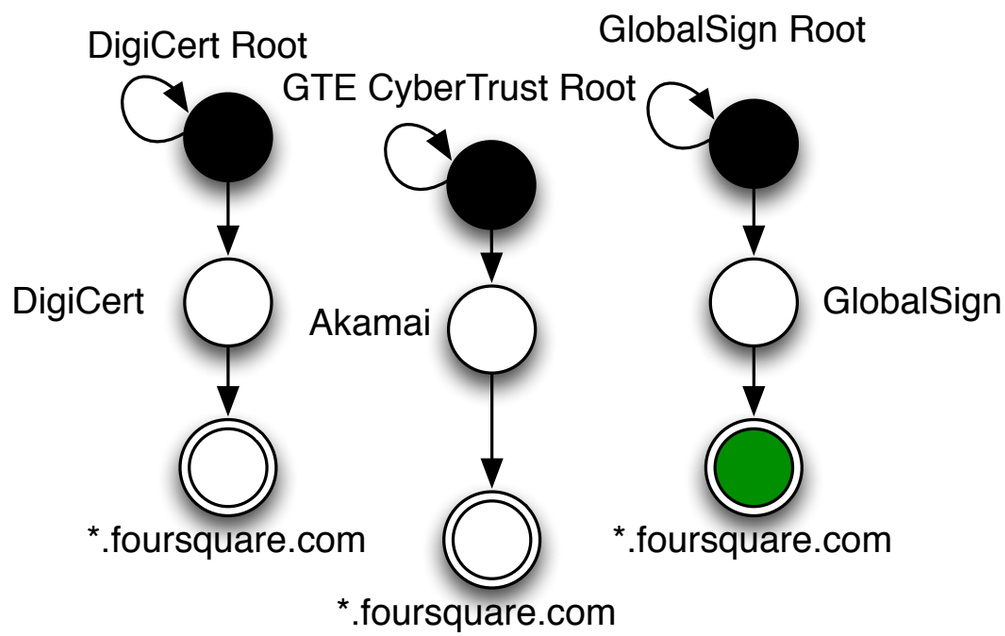
40,885 are for “new” domains

9,400 match exactly one other certificate

1,382 match more than 20

224 match more than 100

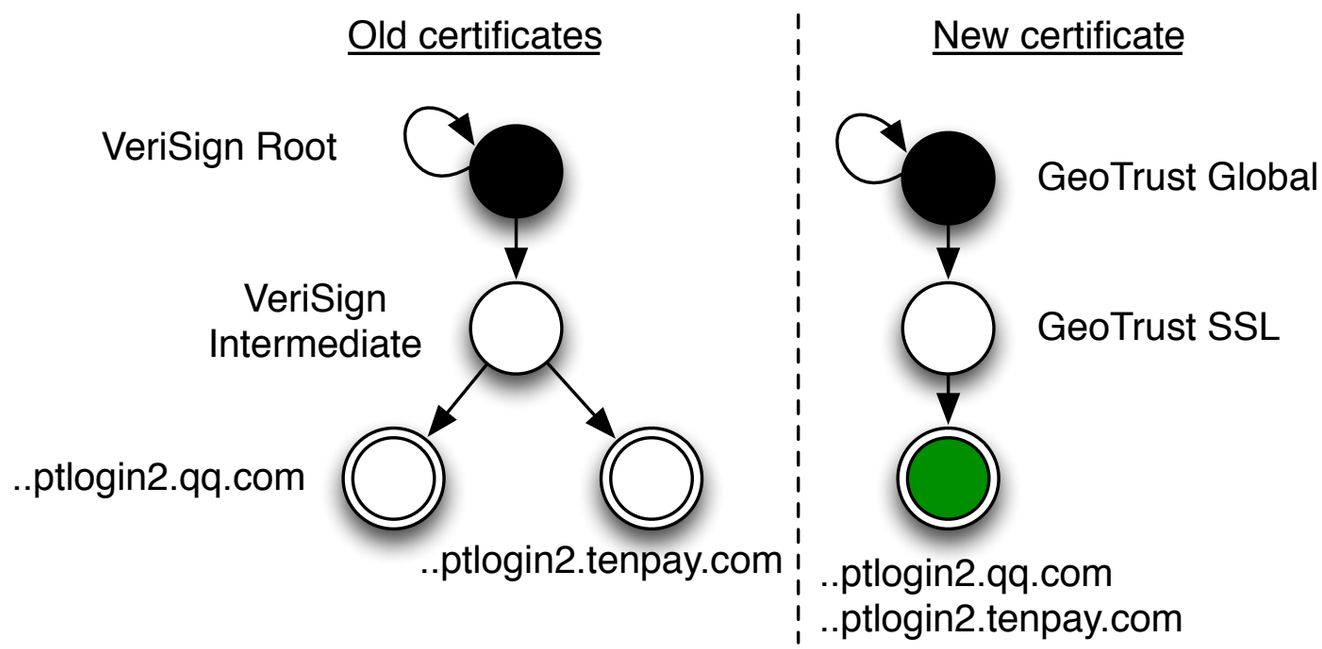
# Legitimate Changes: Foursquare




Several well-known certificates

Suddenly a new certificate for the same domain appears

# Legitimate Changes: qq.com




Chinese instant messenger service

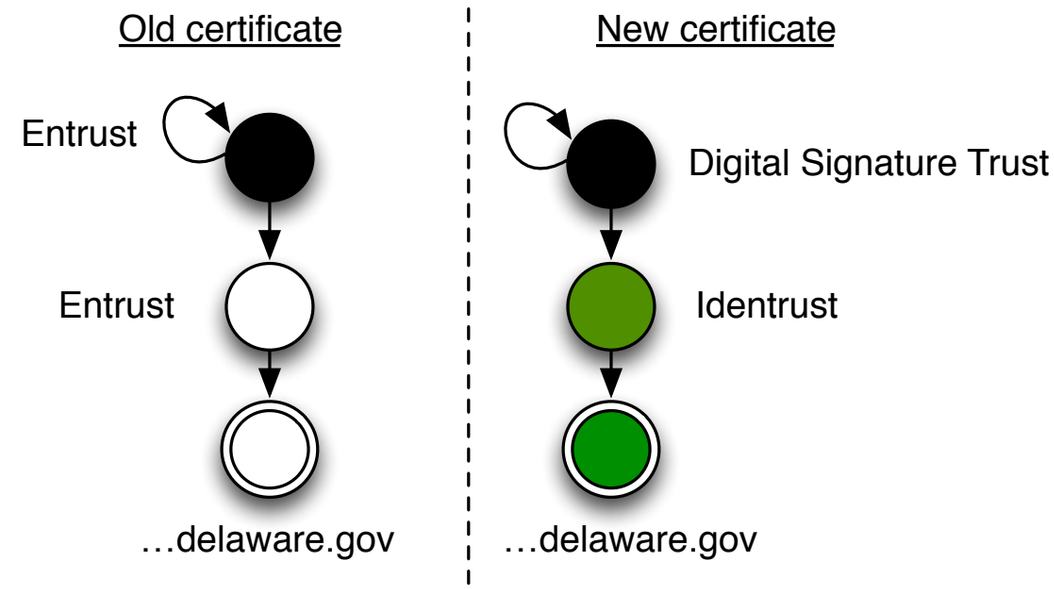
Alexa position: 8

# Other Changes we see

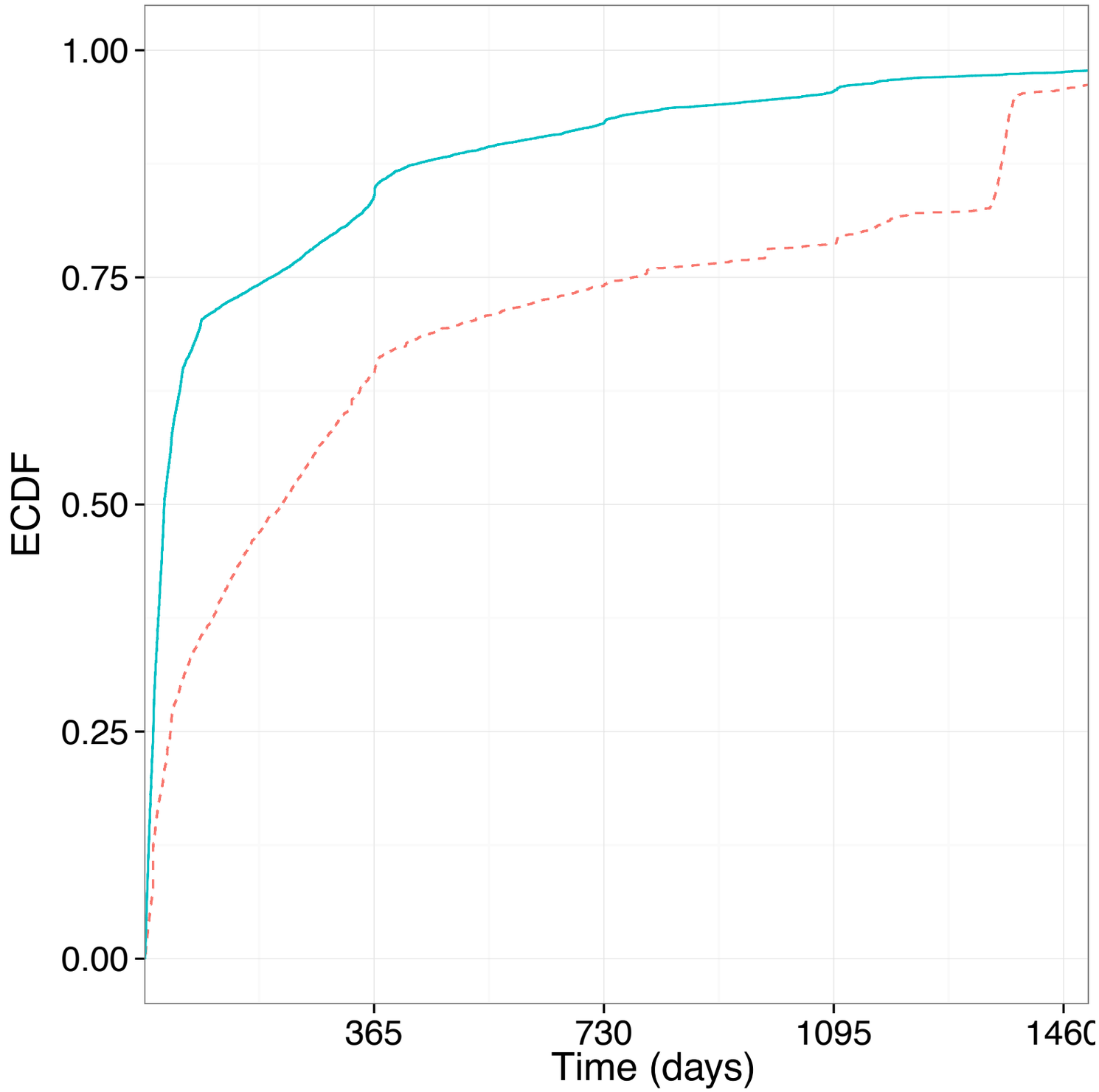
New intermediates for known domains

Suddenly appearing new certificates for banks, e.g. americanexpress.com

Switches of CA countries
- nova scotia department of education,
- privacybox.de to Israel
- zekur.nl from US to Bermudas



# Validity Overlap



# Proposed Remedies

User-side monitoring

Monitoring for CA country changes

Notary systems

Certificate Transparency

# Proposed Remedies

Not practical

User-[illegible]itoring

Monitoring for C[illegible]ntry changes

Notary systems

Certificate Transparency

# Proposed Remedies

User-[illegible]itoring

Not practical

Monitoring for C[illegible]ntry changes

Notary syste[illegible]

Privacy and other problems

Certificate Transparency

# Proposed Remedies

U

N

N

C

CT opens up possibilities...

parties can prove possession of old keys
to CA while requesting certificate
in new certificate extension
or pin new key to their domain

# Summary

Our notary is an on-going large-scale measurement effort

It seems impractical to spot malicious certificates using only structural properties

Resolving these problems involves multiple actors