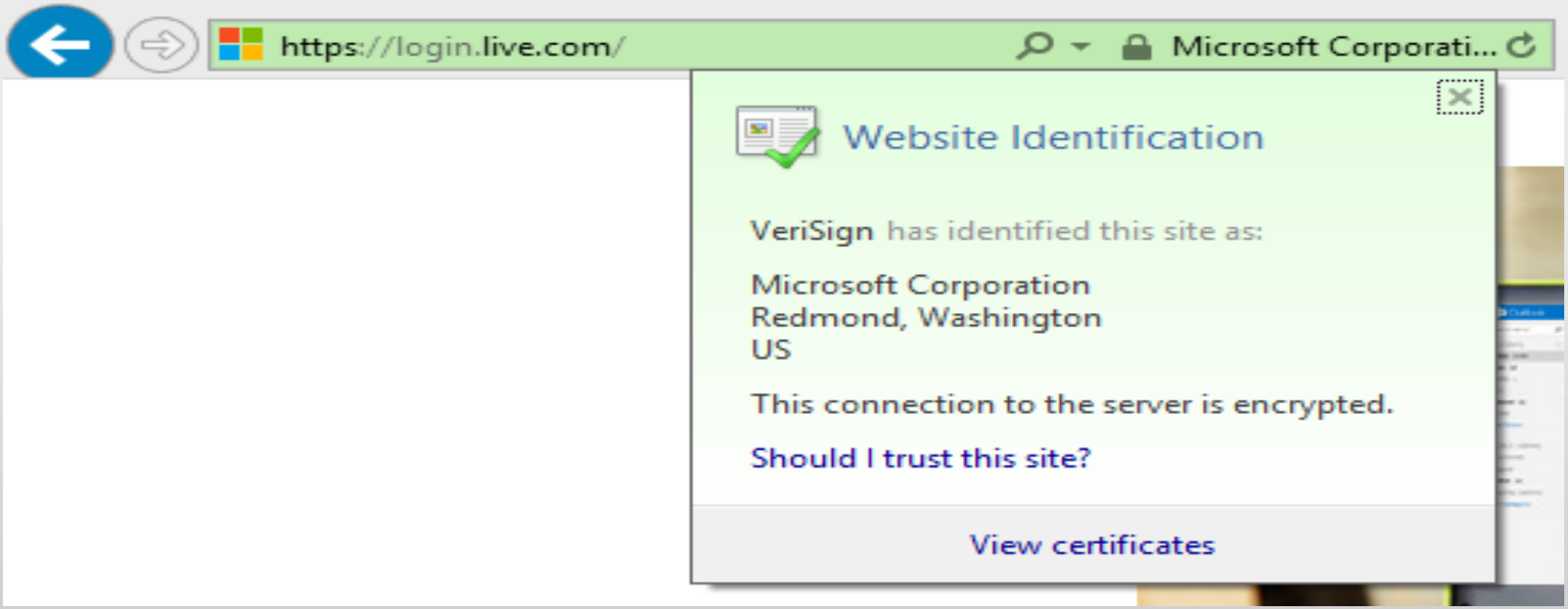
Microsoft® Research

Web PKI: Closing the Gap between Guidelines and Practices

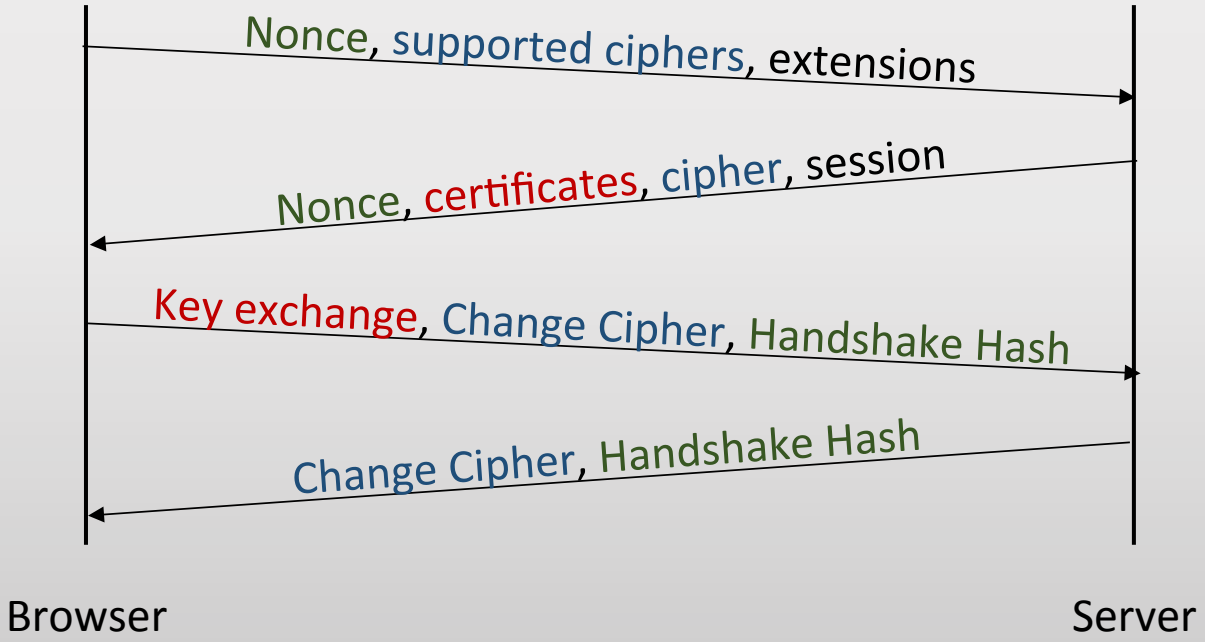
Antoine Delignat-Lavaud, Inria Paris

Joint work with Martín Abadi, Andrew Birrell, Ilya Mironov, Ted Wobber and Yinglian Xie, Microsoft Research

Background: HTTPS

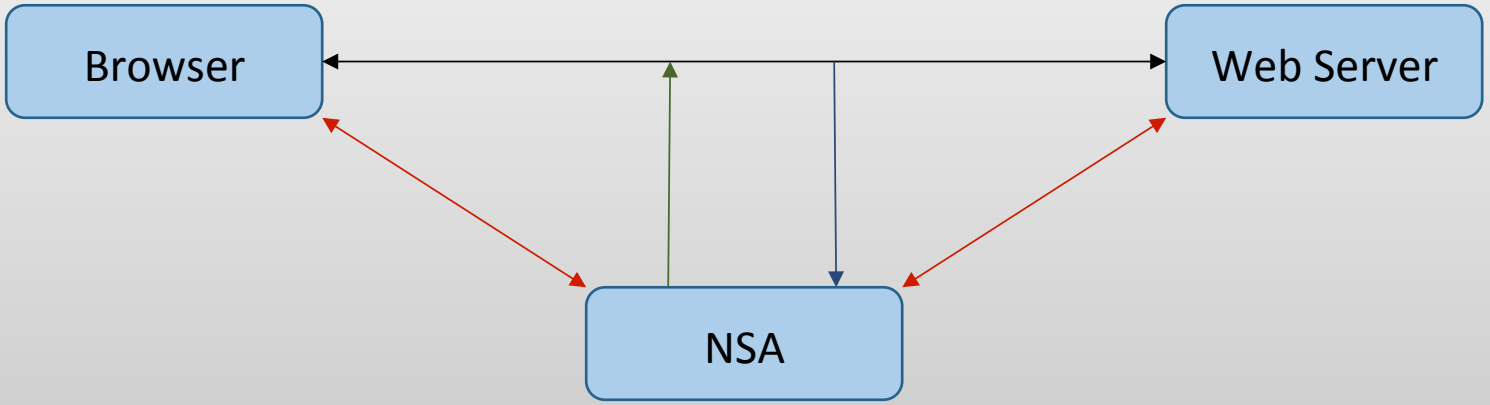


Background: TLS protocol

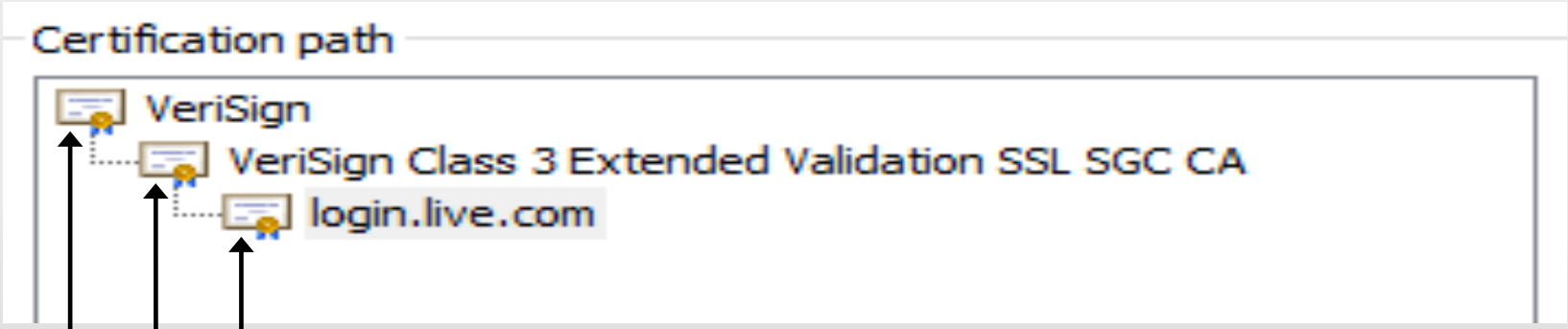


Background: TLS protocol

Authentication > Integrity > Confidentiality



Background: PKI

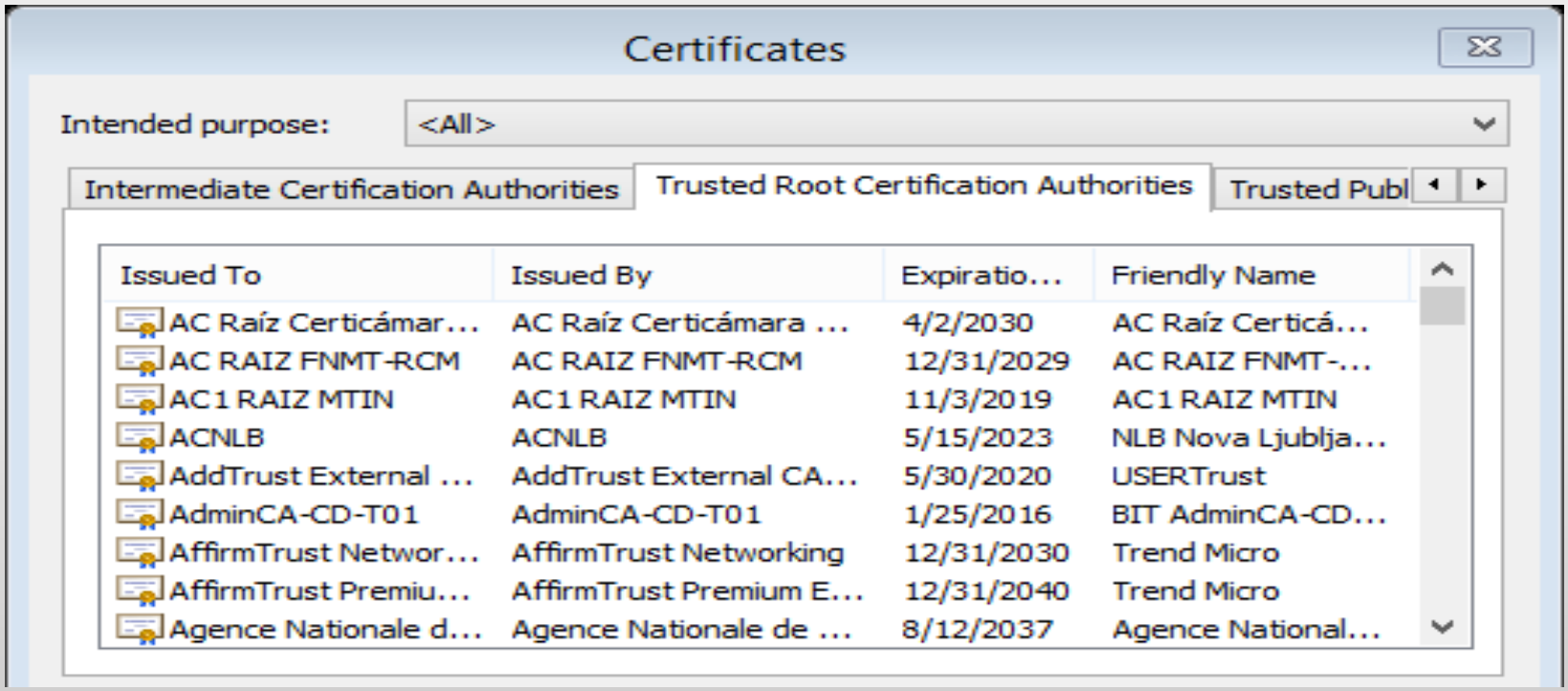


Endpoint certificate

Intermediate Certificate Authority certificate

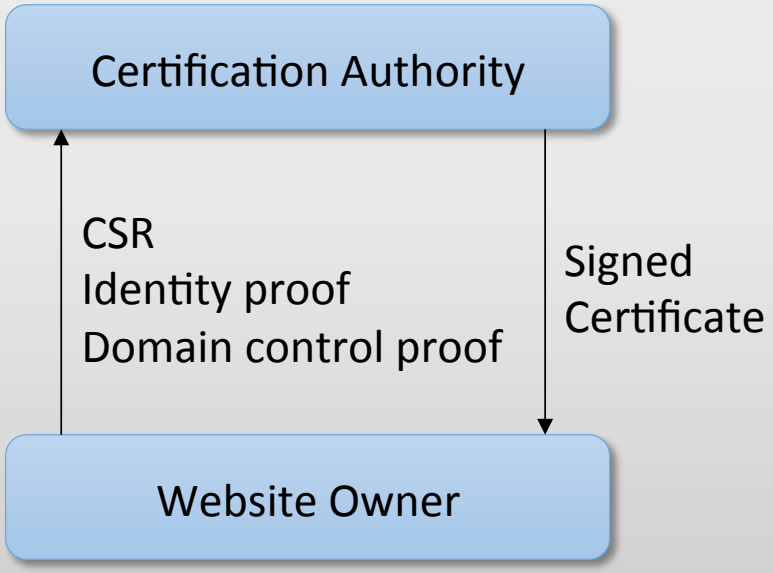
Root Certification Authority certificate

Background: PKI



Background: PKI

1. W generates (pK, sK)
2. W creates a CSR: {subject identity, applicable domains/IP addresses, pK} signed with sK
3. W sends CSR to CA with proof of identity and control over the listed domains
4. CA checks proofs and signs a certificate C with the private key of its CA certificate based on CSR data



Issues: Unreliable CAs

- Issuance errors
  - Jan. 2013: 2 CA-enabled certificates on Türktrust root
  - 2010-2011: 1580 CA-enabled certificates issued to Korean institutions. Several had a 512-bit key
- Deliberate attacks
  - Jul. 2011: hacker gains access to DigiNotar's HSM and creates multiple certificates used in MITM attacks

Issues: Unreliable CAs

- Reckless practices
  - Dec. 2013: MITM CA issued on ANSSI root (controlled by the French government)
  - Jan. 2012: MITM CA issued on Trustwave root
  - Mar. 2011: 9 rogue certificates issued on Comodo root because of dangerous delegation practices

Issues: Cryptographic Attacks

- Weak keys
  - 512 bit RSA
  - 512 bit DH primes
  - Weak RNG (OpenSSL entropy bug on Debian)
- Weak hashing algorithms
  - May. 2012: FLAME malware
  - Dec. 2008: rogue CA certificate created with MD5 collision

Proposed Solutions

1. Ditch certification authorities (e.g. DANE)
   - Interesting design question, new protocol design
   - Not practical yet
2. Detect malicious certificates in the browser
   - Some success already (MITM attacks detected by certificate pinning, minimum crypto requirements)
   - Many proposals, no standard
   - Not effective against all types of compromise

Primitive	*Security Properties Offered*							*Evaluation of Impact on HTTPS*									
	A				B		C	*Security & Privacy*				*Deployability*				*Usability*		
	Detects MITM	Detects Local MITM	Protects Client Credential	Updatable Pins	Detects TLS Stripping	Affirms POST-to-HTTPS	Responsive Revocation	Intermediate CAs Visible	No New Trusted Entity	No New Traceability	Reduces Traceability	No New Auth'n Tokens	No Server-Side Changes	Deployable without DNSSEC	No Extra Communications	Internet Scalable	No False-Rejects	Status Signalled Completely	No New User Decisions
Key Pinning (Client History)	○	○	○					●	●		●	●	●	●	●				
Key Pinning (Server)	○	○	○					●	●				●	●	●	●		●
Key Pinning (Preloaded)	●	●	●	●				○	●		●	○	●	●		●	○	●
Key Pinning (DNS)	●	●	●	●				○	●	●		○		●	●	●	○	●
Multipath Probing		●		●							●	●	●		●		●	
Channel-bound Credentials			○					●	●		●		●	●	●	●	○	●
Credential-bound Channels			○					●	●		●		●	●	●	●	○	●
Key Agility/Manifest				●				●	●				●	●	●	●	●	●
HTTPS-only Pinning (Server)					○	○		●	●				●	●	●	●		●
HTTPS-only Pinning (Preloaded)				●	●	●		○	●		●	○	●	●		●	○	●
HTTPS-only Pinning (DNS)				●	●	●		○	●			○		●	●	●	○	●
Visual Cues for Secure POST						●		●	●		●	●	●		●		●	
Browser-stored CRL							●	○	●		●	●	●	●	●	●	●	●
Certificate Status Stapling							●	●	●	●			●	●	●	●	○	●
Short-lived Certificates							●	●	●	●	●		●	●	●	●	●	●
List of Active Certificates							●	●		●	●	●	●		●	●	●	●

J. Clark et al. - SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements

Proposed Solutions

3. Force CAs to adopt best practices
   - New regulations in response to attacks
   - More involvement of root program managers
4. Monitor the PKI for weaknesses
   - Several past *ad hoc* measurements: Durumeric *et al*. (IMC13), Levillain *et al*. (ACSAC12), Holz *et al*. (IMC11) EFF Observatory (2010) …
   - This paper: PKI monitoring framework

CA/B Forum Baseline Requirements

- Uniform set of requirements for all CAs
- Only went into effect in July 2012
- Covers different aspects of operations:
  - Security of CA network and private keys
  - Identity verification process
  - …
  - **Certificate content requirements**

CA/B Certificate Requirements Goals

- Proper identification of subject, issuer and issuance policy of the certificate
- Clear definition of the scope of the certificate (which entities it applies to, for which purposes)
- Efficient revocation status checking
- Chain reconstruction support

Contents of a Certificate

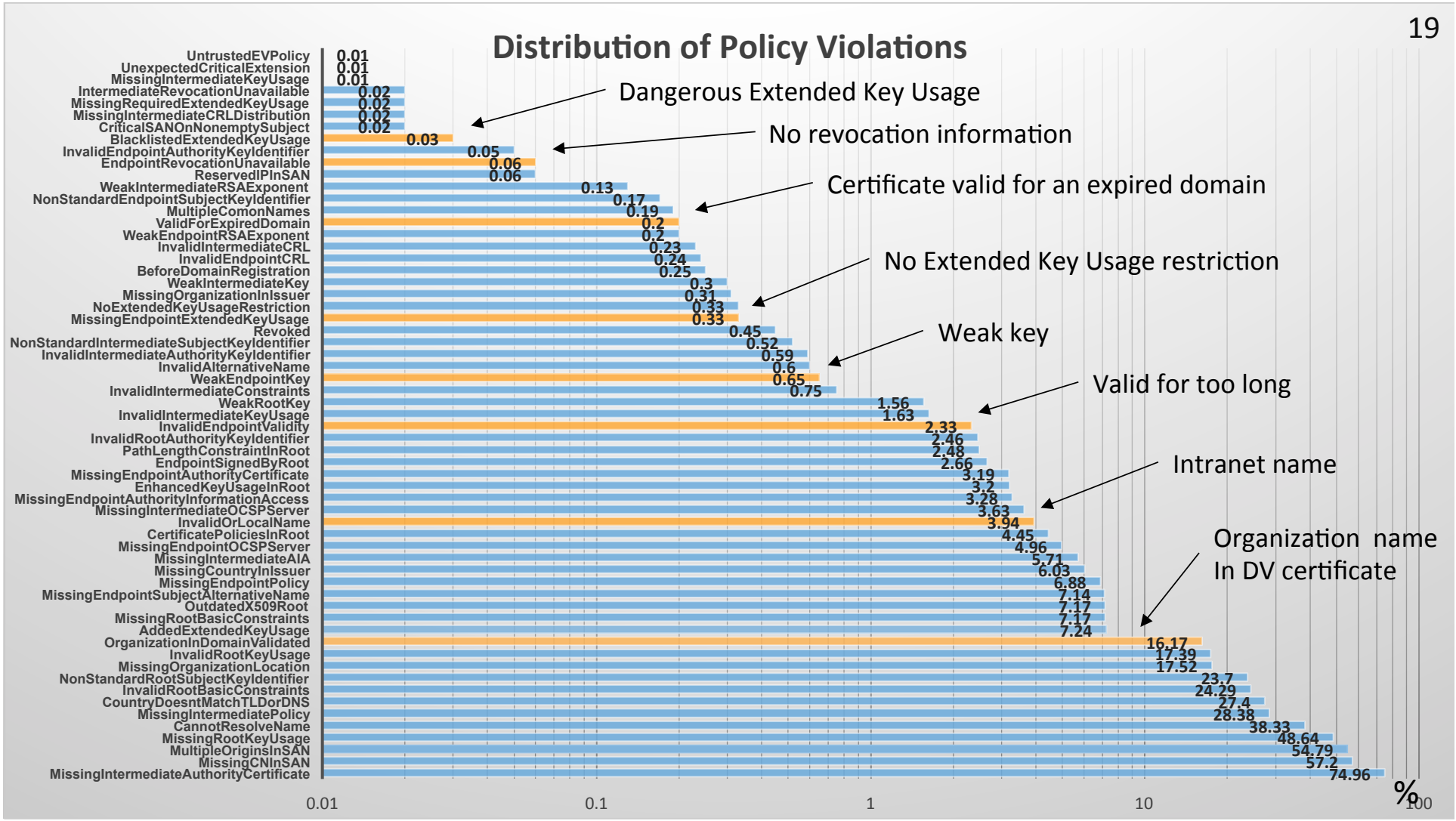
Certificate Fields
Serial Number, Signature Algorithm
Issuer, Subject
Validity Period
Public Key
Extensions
Usage Restrictions
Revocation Information
List of applicable names
Issuance policy
Additional issuer information
Signature

Levels of Assurance

Domain Validated	Organization Validated	Extended Validation
Free or <$60 /year	$100-$300 /year	$350+ /year
Email sent to WHOIS email address, DNS record, hosted file	Manual verification by CA	Proof of incorporation
Asserts control over listed domains	Asserts subject identity	Stricter key and validity period restrictions
Online issuance	Offline issuance	Offline issuance
Padlock	Padlock	Organization + green bar

Endpoint Extension Requirements

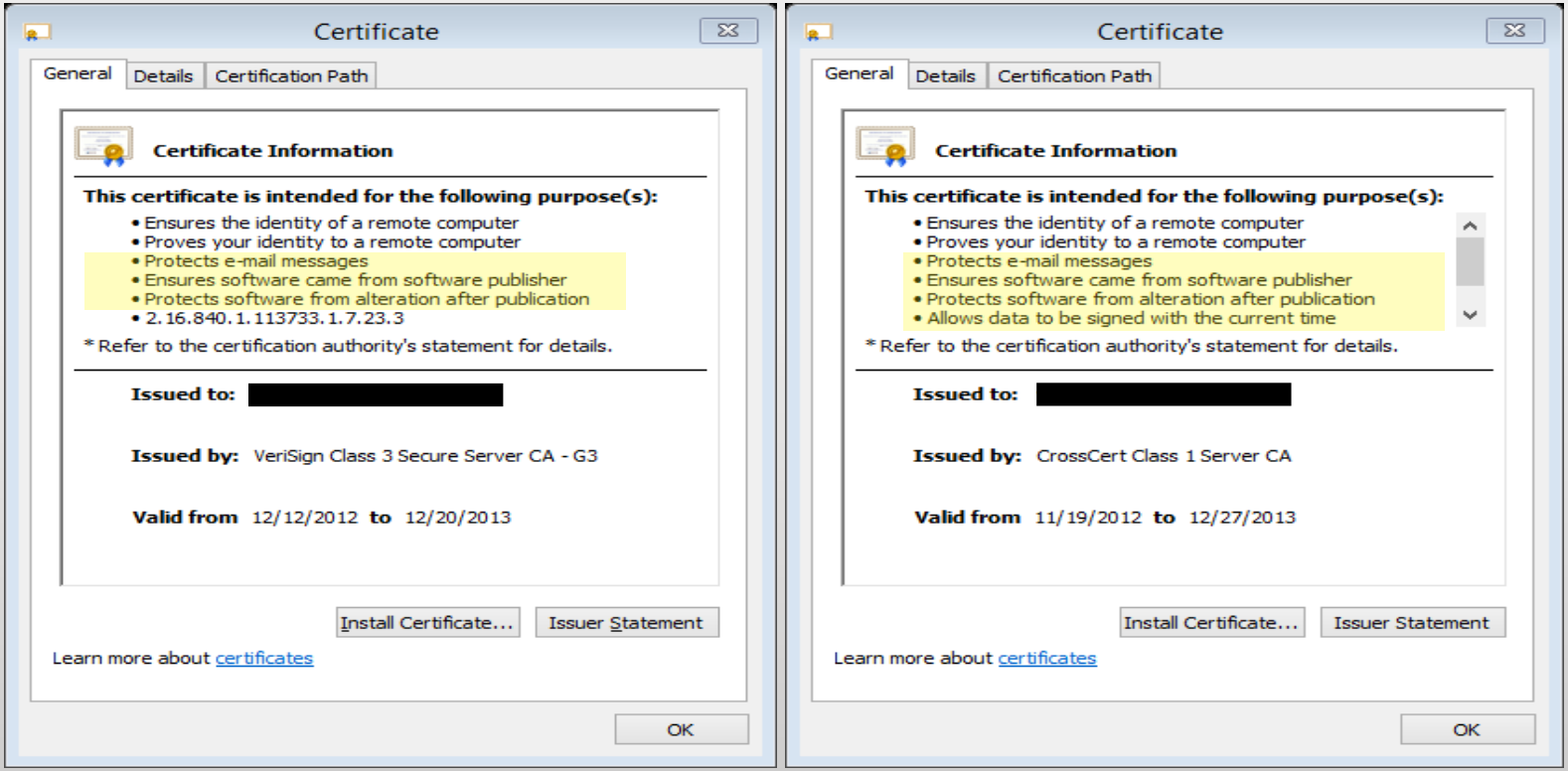
Extension Type	Requirements
Certificate Policies	Must reflect issuance policy and point to *CPS*
CRL Distribution Points	Must appear and include HTTP URL of *CRL file*
Authority Information Access	Must include HTTP URL of *OCSP responder* and *issuer certificate file*
Basic Constraints	*CA bit* must never be set
Key Usage	*Digital Signature* and *Key Encipherment*
Extended Key Usage	(*Client*)/*Server Authentication*, (*Email Protection*)
Subject Alternative Names	Must list all applicable domains and IP


Distribution of Policy Violations
UntrustedEVPolicy 0.01
UnexpectedCriticalExtension 0.01
MissingIntermediateKeyUsage 0.01
IntermediateRevocationUnavailable 0.02
MissingRequiredExtendedKeyUsage 0.02
MissingIntermediateCRLDistribution 0.02
CriticalSANOnNonemptySubject 0.02
BlacklistedExtendedKeyUsage 0.03
InvalidEndpointAuthorityKeyIdentifier 0.05
EndpointRevocationUnavailable 0.06
ReservedIPInSAN 0.06
WeakIntermediateRSAExponent 0.13
NonStandardEndpointSubjectKeyIdentifier 0.17
MultipleComonNames 0.19
ValidForExpiredDomain 0.2
WeakEndpointRSAExponent 0.2
InvalidIntermediateCRL 0.23
InvalidEndpointCRL 0.24
BeforeDomainRegistration 0.25
WeakIntermediateKey 0.3
MissingOrganizationInIssuer 0.31
NoExtendedKeyUsageRestriction 0.33
MissingEndpointExtendedKeyUsage 0.33
Revoked 0.45
NonStandardIntermediateSubjectKeyIdentifier 0.52
InvalidIntermediateAuthorityKeyIdentifier 0.59
InvalidAlternativeName 0.6
WeakEndpointKey 0.65
InvalidIntermediateConstraints 0.75
WeakRootKey 1.56
InvalidIntermediateKeyUsage 1.63
InvalidEndpointValidity 2.33
InvalidRootAuthorityKeyIdentifier 2.46
PathLengthConstraintInRoot 2.48
EndpointSignedByRoot 2.66
MissingEndpointAuthorityCertificate 3.19
EnhancedKeyUsageInRoot 3.2
MissingEndpointAuthorityInformationAccess 3.28
MissingIntermediateOCSPServer 3.63
InvalidOrLocalName 3.94
CertificatePoliciesInRoot 4.45
MissingEndpointOCSPServer 4.96
MissingIntermediateAIA 5.71
MissingCountryInIssuer 6.03
MissingEndpointPolicy 6.88
MissingEndpointSubjectAlternativeName 7.14
OutdatedX509Root 7.17
MissingRootBasicConstraints 7.17
AddedExtendedKeyUsage 7.17
OrganizationInDomainValidated 7.24
InvalidRootKeyUsage 16.17
MissingOrganizationLocation 17.39
NonStandardRootSubjectKeyIdentifier 17.52
InvalidRootBasicConstraints 23.7
CountryDoesntMatchTLDorDNS 24.29
MissingIntermediatePolicy 27.4
CannotResolveName 28.38
MissingRootKeyUsage 38.33
MultipleOriginsInSAN 48.64
MissingCNInSAN 54.79
MissingIntermediateAuthorityCertificate 57.2
74.96
Dangerous Extended Key Usage
No revocation information
Certificate valid for an expired domain
No Extended Key Usage restriction
Weak key
Valid for too long
Intranet name
Organization name
In DV certificate
0.01
0.1
1
10
100
%

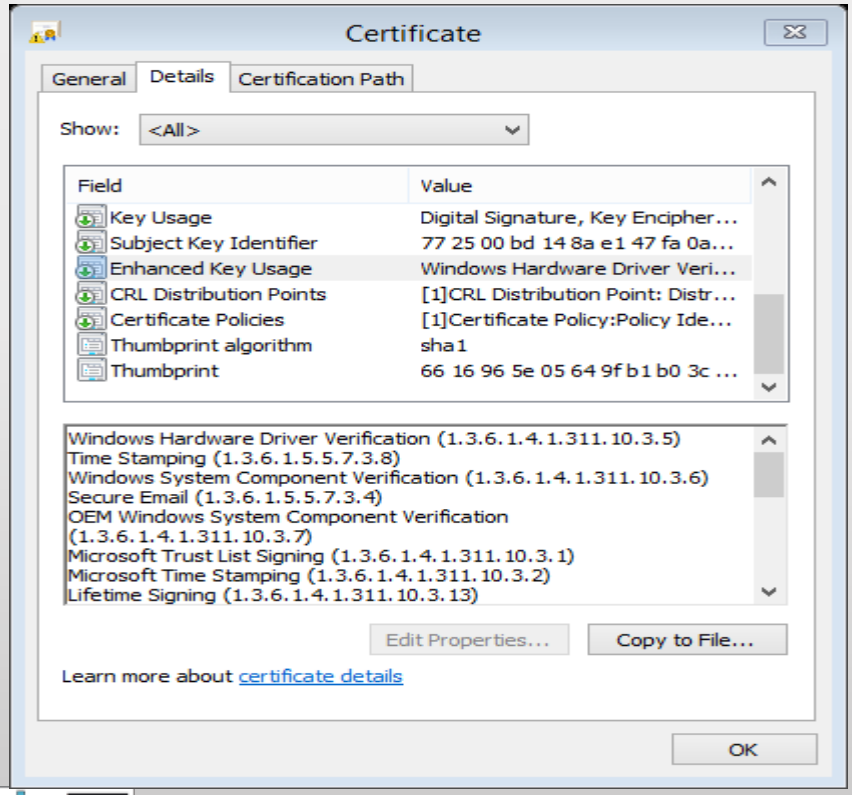
Main Observations

- Compared to certificates issued before BR adoption violation rates are down 2.6pp on average
- For instance, the lack of an OCSP service is down about 20pp between the two periods
- Serious and relatively common key usage issues
- Intranet names are still widely used in certificates
- Certificates valid for expired domains are a problem

Missing Extended Key Usage

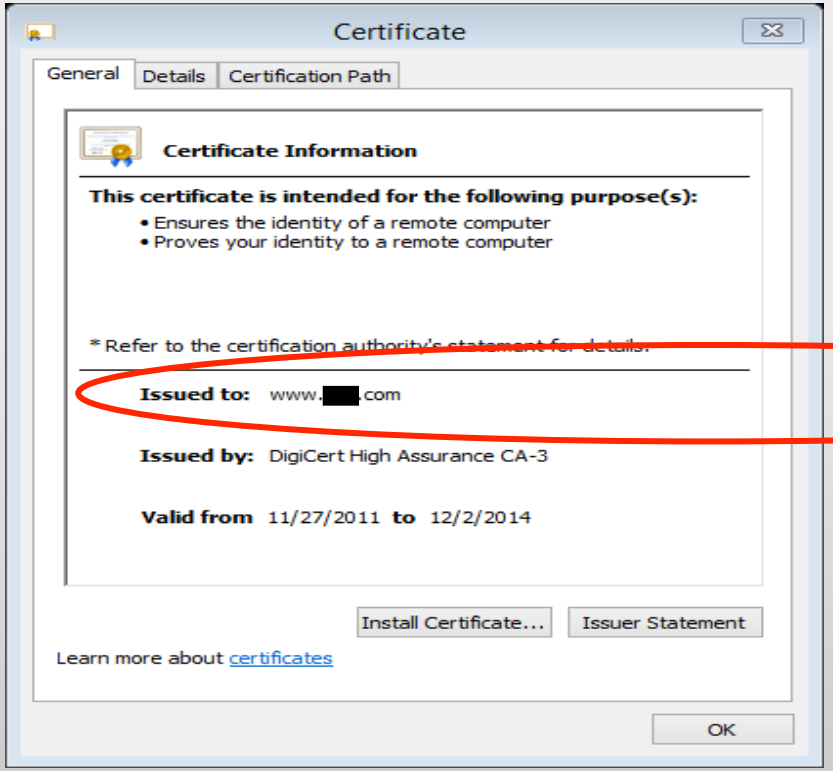


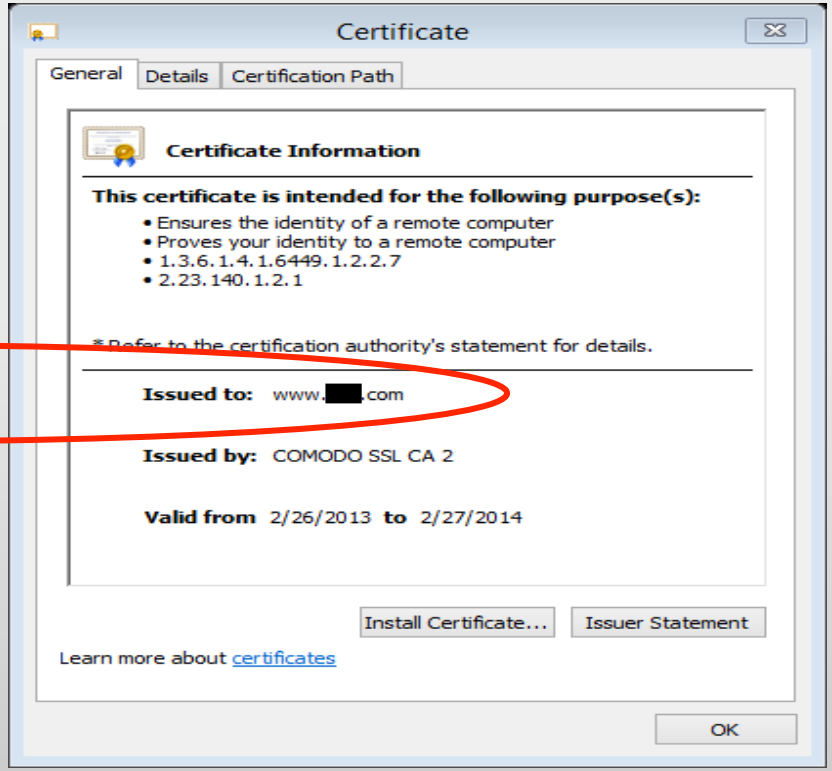
Abusive Extended Key Usage



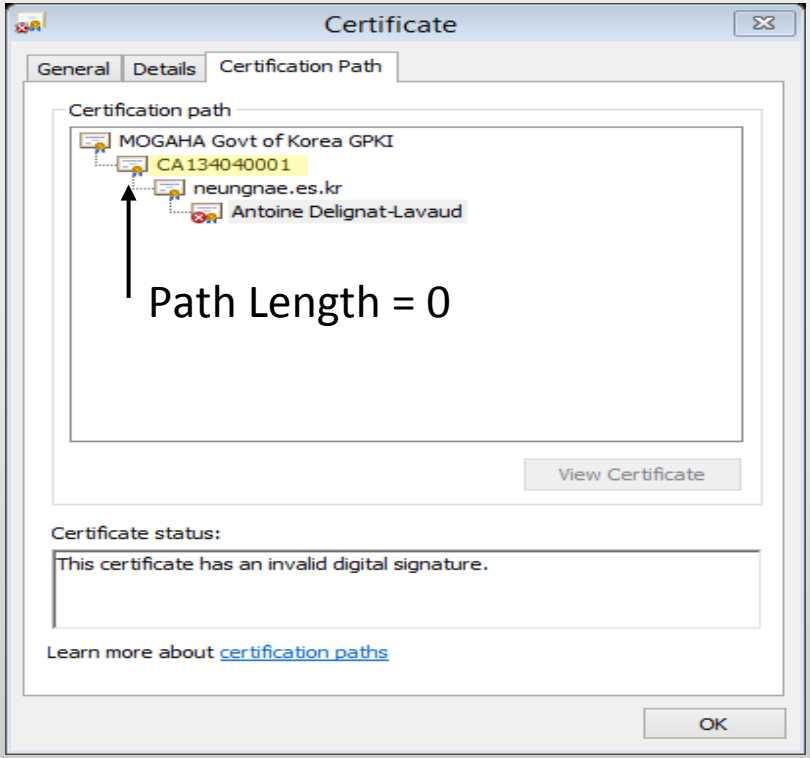

```
Windows Hardware Driver Verification
(1.3.6.1.4.1.311.10.3.5)
Time Stamping (1.3.6.1.5.5.7.3.8)
Windows System Component Verification
(1.3.6.1.4.1.311.10.3.6)
Secure Email (1.3.6.1.5.5.7.3.4)
OEM Windows System Component Verification
(1.3.6.1.4.1.311.10.3.7)
Microsoft Trust List Signing (1.3.6.1.4.1.311.10.3.1)
Microsoft Time Stamping (1.3.6.1.4.1.311.10.3.2)
Lifetime Signing (1.3.6.1.4.1.311.10.3.13)
License Server Verification (1.3.6.1.4.1.311.10.6.2)
Key Pack Licenses (1.3.6.1.4.1.311.10.6.1)
IP security user (1.3.6.1.5.5.7.3.7)
IP security tunnel termination (1.3.6.1.5.5.7.3.6)
IP security IKE intermediate (1.3.6.1.5.5.8.2.2)
IP security end system (1.3.6.1.5.5.7.3.5)
File Recovery (1.3.6.1.4.1.311.10.3.4.1)
Encrypting File System (1.3.6.1.4.1.311.10.3.4)
Embedded Windows System Component Verification
(1.3.6.1.4.1.311.10.3.8)
Document Signing (1.3.6.1.4.1.311.10.3.12)
Directory Service Email Replication
(1.3.6.1.4.1.311.21.19)
Code Signing (1.3.6.1.5.5.7.3.3)
Client Authentication (1.3.6.1.5.5.7.3.2)
Server Authentication (1.3.6.1.5.5.7.3.1)
```

Expired / Renewed Domains





Invalid Basic Constraints



- Factorable 512-bits keys ($240 on Amazon EC2)*
- No revocation
- Saved by Path Length Constraint
  - **Is it properly enforced?**

*Nadia Heninger, *Factoring as a Service* CRYPTO'13 rump session

Digression: Certificate Validations

- Certificate validation is a difficult challenge, often delegated to the application (Georgiev *et al.* and Fahl *et al.* at CCS12)
- We found several problems related to enforcement of key usage, path length and other constraints in GnuTLS, OpenSSL and Windows
- API problem: certificate accept callback

Ad: https://www.mitls.org

CA/B Requirements Adherence

- Individual certificate inspection
  - Key strong enough / not compromised?
  - Certificate valid for intranet names?
  - Validity period within limits?
  - May require network queries (DNS, WHOIS, GeoIP…)
- Many constraints apply to the CA's issuance **profile**

Field	Value
Version	V3 (2)
Serial Number	Unique number
Issuer Signature Algorithm	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Issuer Distinguished Name	Unique X.500 CA DN. CN = DigiCert Global CA OU = www.digicert.com O = DigiCert Inc C = US
Validity Period	1, 2 or 3 years expressed in UTC format
Subject Distinguished Name	cn = <Name of Website or Domain> ou = <Organizational Unit of Subscriber> o = <Full Legal Name of Subscriber> l = <Locality of Subscriber> s = <State of Subscriber> c = <country of Subscriber>
Subject Public Key Info	1024 or 2048-bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 1}
Issuer's Signature	sha-1WithRSAEncryption {1 2 840 113549 1 1 5}
Extension	**Value**
Authority Key Identifier	c=no; a7 c7 13 a0 7a 01 3c 9d ef 82 48 82 48 d5 73 51 b6 12 56 2a
Subject Key Identifier	c=no; Octet String – Same as calculated by CA from PKCS#10
Key Usage	c=yes; Digital Signature, Key Encipherment (a0)
Extended Key Usage	c=no; Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Certificate Policies	c=no; Certificate Policies; {2.16.840.1.114412.1.3.0.1} [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.digicert.com/ssl-cps-repository.htm [1,2] Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Any use of this Certificate constitutes acceptance of the DigiCert CP/CPS and the Relying Party Agreement which limit liability and are incorporated herein by reference.
Subject Alternative Name	c=no; Name of Device1 (e.g., domain.com) Name of Device2, etc.
Authority Information Access	c=no; Access Method= - Id-ad-ocsp (On-line Certificate Status Protocol - 1.3.6.1.5.5.7.48.1); URL =http://ocsp.digicert.com
CRL Distribution Points	c = no; CRL HTTP URL = http://crl3.digicert.com/DigiCertGlobalCA.crl CRL HTTP URL = http://crl4.digicert.com/DigiCertGlobalCA.crl - OR, if the certificate has a dedicated CRL file - CRL HTTP URL = http://crl3.digicert.com/[SERIAL].crl CRL HTTP URL = http://crl4.digicert.com/[SERIAL].crl

Profile Reconstruction

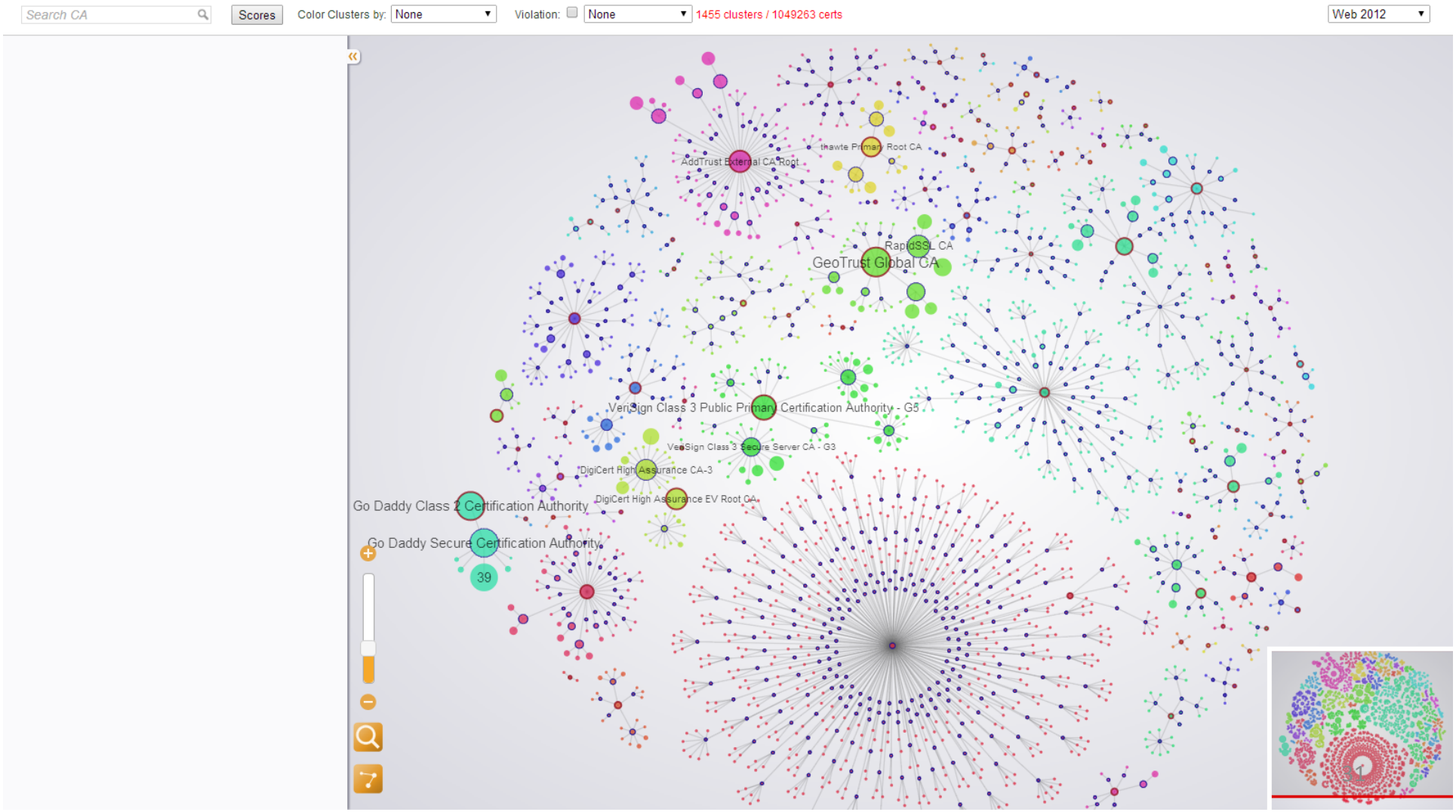
- Run clustering algorithm based on profile features
- Yields global picture of CA issuance practices
- Easy to find nearest cluster for manual inspection
- Easy investigation of outliers

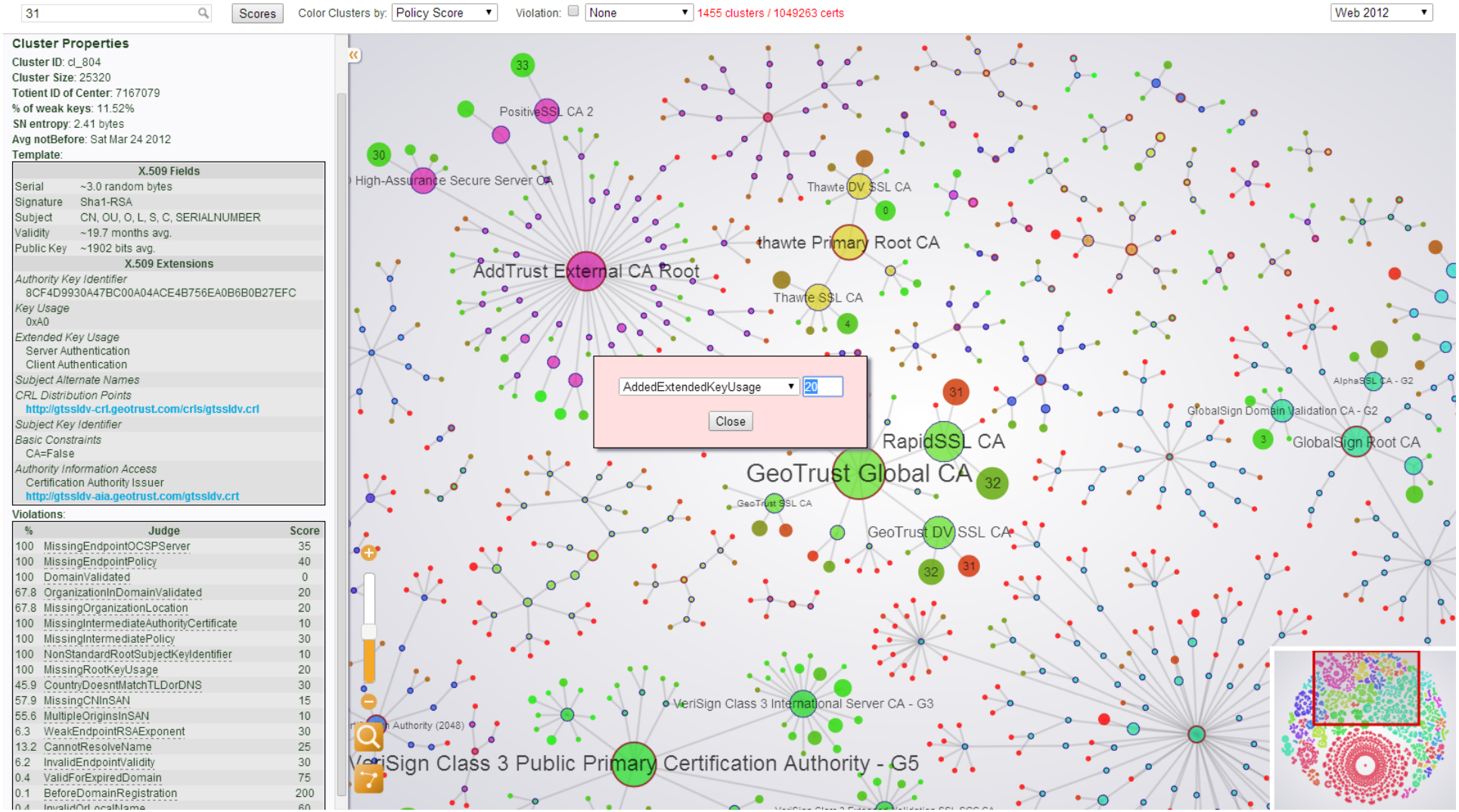
Template Clustering Features

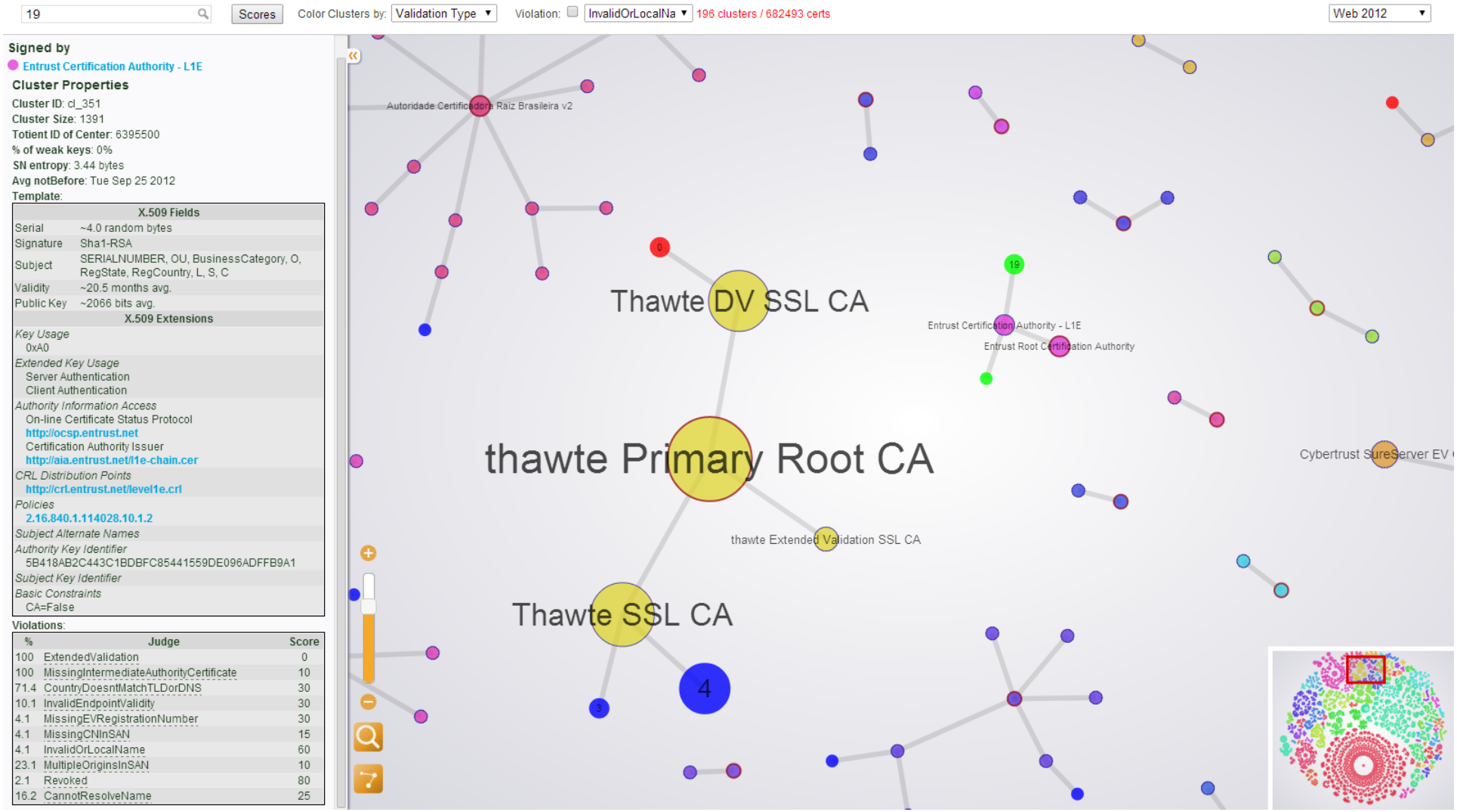
High Weight	Medium Weight	Low Weight
Issuer X509 extensions Policy identifiers (Extended) key usage Basic constraints Authority Info Access	Subject fields CRL distribution points Signature algorithm Public key algorithm	Key size Validity period Issuance date Serial number format

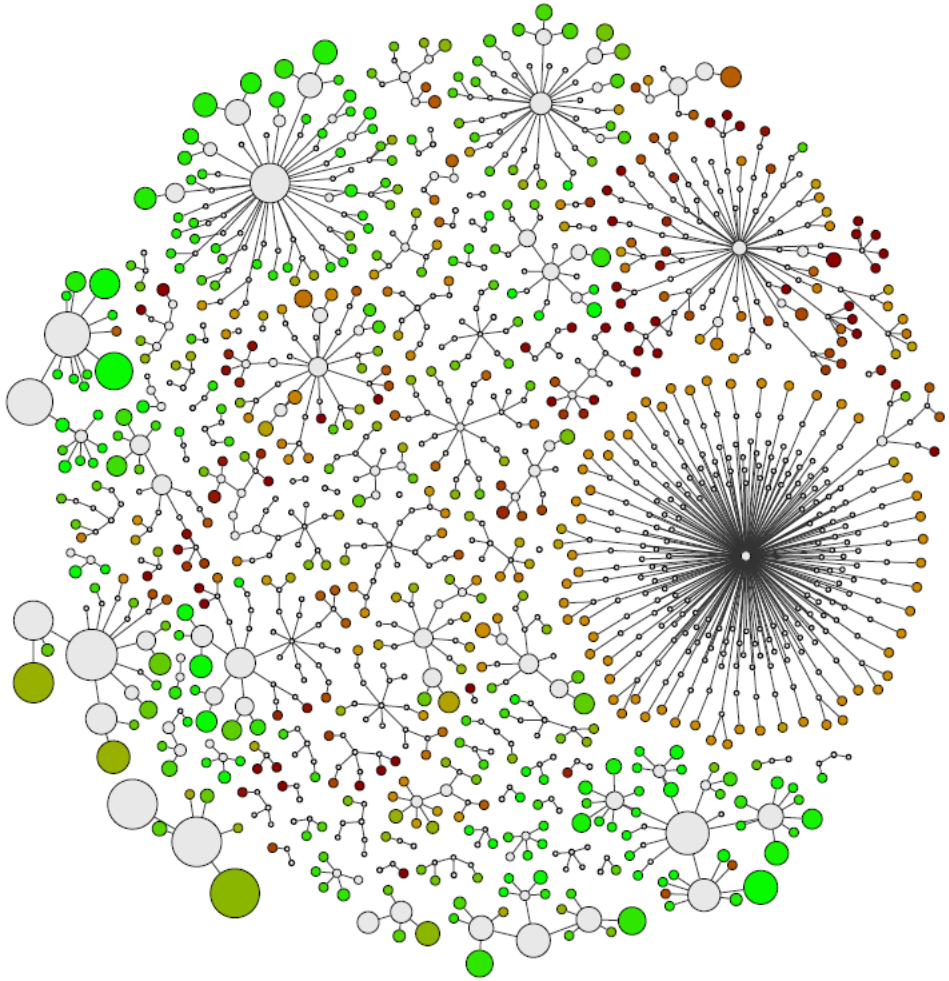
Clustering Results

- < 1500 clusters out of 1M certs issued since 2012 (only 30% contain more than 5 certificates)
- We run in-depth individual evaluation on random samples from each cluster
- Comparison of template and individual violations


Search CA
Scores
Color Clusters by: None
Violation: None
1455 clusters / 1049263 certs
Web 2012
thawte Primary Root CA
AddTrust External CA Root
RapidSSL CA
GeoTrust Global CA
VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign Class 3 Secure Server CA - G3
DigiCert High Assurance CA-3
DigiCert High Assurance EV Root CA
Go Daddy Class 2 Certification Authority
Go Daddy Secure Certification Authority
39


31
Scores
Color Clusters by: Policy Score
Violation: None
1455 clusters / 1049263 certs
Web 2012
Cluster Properties
Cluster ID: cl_804
Cluster Size: 25320
Totient ID of Center: 7167079
% of weak keys: 11.52%
SN entropy: 2.41 bytes
Avg notBefore: Sat Mar 24 2012
Template:
X.509 Fields
Serial ~3.0 random bytes
Signature Sha1-RSA
Subject CN, OU, O, L, S, C, SERIALNUMBER
Validity ~19.7 months avg.
Public Key ~1902 bits avg.
X.509 Extensions
Authority Key Identifier
8CF4D9930A47BC00A04ACE4B756EA0B6B0B27EFC
Key Usage
0xA0
Extended Key Usage
Server Authentication
Client Authentication
Subject Alternate Names
CRL Distribution Points
http://gtssldv-crl.geotrust.com/crls/gtssldv.crl
Subject Key Identifier
Basic Constraints
CA=False
Authority Information Access
Certification Authority Issuer
http://gtssldv-aia.geotrust.com/gtssldv.crt
Violations:
% Judge Score
100 MissingEndpointOCSPServer 35
100 MissingEndpointPolicy 40
100 DomainValidated 0
67.8 OrganizationInDomainValidated 20
67.8 MissingOrganizationLocation 20
100 MissingIntermediateAuthorityCertificate 10
100 MissingIntermediatePolicy 30
100 NonStandardRootSubjectKeyIdentifier 10
100 MissingRootKeyUsage 20
45.9 CountryDoesntMatchTLDorDNS 30
57.9 MissingCNInSAN 15
55.6 MultipleOriginsInSAN 10
6.3 WeakEndpointRSAExponent 30
13.2 CannotResolveName 25
6.2 InvalidEndpointValidity 30
0.4 ValidForExpiredDomain 75
0.1 BeforeDomainRegistration 200
33
PositiveSSL CA 2
30
High-Assurance Secure Server CA
Thawte DV SSL CA
0
thawte Primary Root CA
AddTrust External CA Root
Thawte SSL CA
4
AddedExtendedKeyUsage
20
Close
31
RapidSSL CA
GeoTrust Global CA
32
GeoTrust SSL CA
GeoTrust DV SSL CA
32
31
AlphaSSL CA - G2
GlobalSign Domain Validation CA - G2
3
GlobalSign Root CA
VeriSign Class 3 International Server CA - G3
VeriSign Class 3 Public Primary Certification Authority - G5


19
Scores
Color Clusters by: Validation Type
Violation:
InvalidOrLocalNa
196 clusters / 682493 certs
Web 2012
Signed by
Entrust Certification Authority - L1E
Cluster Properties
Cluster ID: cl_351
Cluster Size: 1391
Totient ID of Center: 6395500
% of weak keys: 0%
SN entropy: 3.44 bytes
Avg notBefore: Tue Sep 25 2012
Template:
X.509 Fields
Serial ~4.0 random bytes
Signature Sha1-RSA
Subject SERIALNUMBER, OU, BusinessCategory, O, RegState, RegCountry, L, S, C
Validity ~20.5 months avg.
Public Key ~2066 bits avg.
X.509 Extensions
Key Usage
0xA0
Extended Key Usage
Server Authentication
Client Authentication
Authority Information Access
On-line Certificate Status Protocol
http://ocsp.entrust.net
Certification Authority Issuer
http://aia.entrust.net/l1e-chain.cer
CRL Distribution Points
http://crl.entrust.net/level1e.crl
Policies
2.16.840.1.114028.10.1.2
Subject Alternate Names
Authority Key Identifier
5B418AB2C443C1BDBFC85441559DE096ADFFB9A1
Subject Key Identifier
Basic Constraints
CA=False
Violations:
% Judge Score
100 ExtendedValidation 0
100 MissingIntermediateAuthorityCertificate 10
71.4 CountryDoesntMatchTLDorDNS 30
10.1 InvalidEndpointValidity 30
4.1 MissingEVRegistrationNumber 30
4.1 MissingCNInSAN 15
4.1 InvalidOrLocalName 60
23.1 MultipleOriginsInSAN 10
2.1 Revoked 80
16.2 CannotResolveName 25
Autoridade Certificadora Raiz Brasileira v2
Thawte DV SSL CA
Entrust Certification Authority - L1E
Entrust Root Certification Authority
thawte Primary Root CA
Cybertrust SureServer EV
thawte Extended Validation SSL CA
Thawte SSL CA
4



Limitations of CA/B requirements

- Business-minded security advances
- Violations mostly have no consequence on CAs
- Don't cover all issues of identity and domain control validation (CDN, expiration…)
- Missing some simple and effective requirements (e.g. path length=0 in all issuing intermediates)

Feedback from CAs

- Contacted by 3 different CAs, including 2 of the most compliant ones
- Notified two CAs of serious template errors. Affected certificates have been revoked.
- One CA complained that we applied requirements on the full chain instead of the leaf only

Conclusions

- Most worrying compliance problems are now at the periphery of CA graph
- Difficult to influence CA behavior except through root program managers
- Important next step: enforce strong certificate policies in all browsers, including baseline requirements

Questions

http://research.microsoft.com/en-us/projects/totient/

End-User Policy Enforcement