digicert®

Your Success is built on Trust™

CAs and the New Paradigm

ICANN 47 ccNSO Tech Day

Dan Timpson

Looking Back (2011)

- **Problem:** Hacking/complete compromise of CA system over many months; cert issuance logs erased (no record); 531 or more fake certs issued
- **Harm:** Potentially great (many OCSP checks from Iran). Hacking claims by “Iranian hacker” never verified
- **Response:** Some certs revoked by CA (no complete list). DigiNotar roots became “untrusted” by browsers; CA went out of business

Discussion

- The state of SSL is stronger than ever and continues to incrementally improve.
- Ongoing Industry Improvements
  - CA/B Forum Enhanced BR's & Networking guidelines
  - Improved customer
  - CAs proactively responding to emerging threats
- Forward looking: Good IETF proposals are on the table
  - Certificate Transparency (CT)
  - Certificate Authority Authorization (CAA)
  - Public Key Pinning

Industry - Raising the Bar

- CA's, browsers and industry groups are constantly improving standards (Self Regulated)
  - Mozilla/Microsoft root program requirements
  - CA/Browser Forum (2005 to date) – raised the bar:
    - EV Guidelines revamped (2012),
    - Baseline Requirements updated (2013)
    - *New - Network and Security Controls (2013)
  - *New - CA Security Council www.casecurity.org
  - WebTrust, ETSI audit requirements (2000 - date)
  - Online Trust Alliance (OTA) encourages CA Best Practices
- CA's are continuously improving security, processes and responding quickly to issues as they surface (ex. gTLD's)

Putting it in Perspective

Relatively few CA security issues over 15 years…

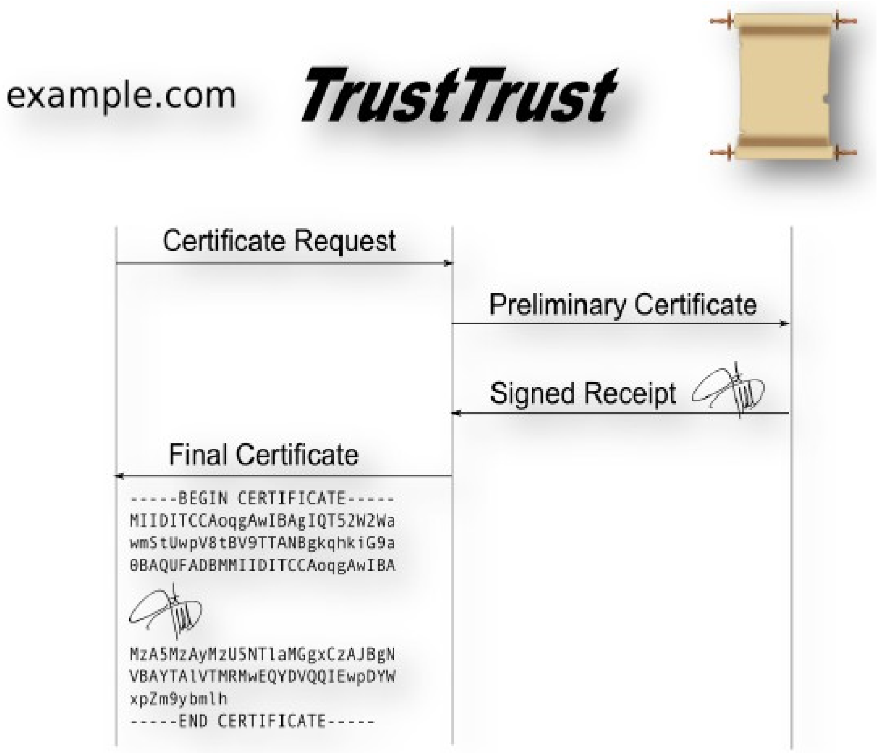
- Certs issued worldwide: 2,000,000 per year
- Bad certs issued: maybe 1,000 over 11 years (~91 bad certs per year) – mostly single incident (DigiNotar)
  - Most breaches resulted in no tangible harm and were remediated quickly
- Accuracy ratio for certs issued each year: 99.995% (Error rate 0.005%) - US Passport Office and state Departments of Motor Vehicles are **NOT** this accurate
- Significant harm from bad certs? Only likely in DigiNotar case (actual harm unknown)
- The state of SSL is stronger today as result of industry responses

Networking Requirements

- Effective 1/12013 (CA/B) – New networking Requirements
  - Protection of networks and supporting systems Zoning, air gapping critical systems etc.
  - Implementation of trusted roles and system accounts
  - Vulnerability and patch management
    - Includes penetration testing
  - Logging, Monitoring and Alerting

Certificate Transparency (CT)

- Goal: Prevent misissued certificates by ensuring they are not issued without domain owner's knowledge.
- CT provides publicly published logs to audit issued certificates.
- Anyone can see what CAs are asserting about your organization.



```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIQT52W2Wa
wmStUwpV8tBV9TTANBgkqhkiG9a
0BAQUFADBMMIIDITCCAoqgAwIBA

MzA5MzAyMzU5NTlaMGgxCzAJBgN
VBAYTAlVTMRMwEQYDVQQIEwpDYW
xpZm9ybmlh
-----END CERTIFICATE-----
```

Certificate Transparency

- Is based on existing technologies that are easily supported with industry coordination
- Internal CAs are not impacted: internal certificates do not need to be logged
- Internal hostnames in public certificates don't need to be logged - clients can be configured with a list of internal domains or intermediate CAs can be name constrained

Certificate Transparency

Pros

- Enhances the current CA infrastructure rather than replacing it.
- Doesn't require any actions by sites in the vast majority of cases.

Cons

- Requires all CAs to be updated.
- Deployment will take many years.
- Public records require vigilance to be useful.

Certification Authority Authorization

- Certification Authority Authorization (CAA)
  - IETF RFC 6844 drafted by Comodo
  - Mechanism for preventing and detecting misissued certificates from CAs

- Mechanism
  - Based on DNS resource record that lists CAs authorized to issue certs for a domain
  - PRIOR to issuing a certificate, CA checks for a CAA record to ensure CA is allowed to issue cert for that domain

Certification Authority Authorization

- Context and Key Points
  - Benefit in that it’s a verification to see whether a CA should be associated with a cert for a specific domain
  - This is a “preventative” approach to issuing rogue certs without replacing current system
  - CAA record doesn’t say which key must be in the end-entity cert – entry is at the CA level
  - Supports wildcard certs
  - More than one CA may be specified for each DNS record
  - CABF is starting discussions on CAA for potential usage by CAs

Certification Authority Authorization

Pros

- Good complement to existing ecosystem to prevent and detect mis-issuance from CAs
- Low barrier for deployment for CAs – CAs need to check CAA record
- Does not require big-bang adoption – can be phased per CA and per certificate customer
- Raises the bar on CA security – bad actor must be able to attack DNS or suppress CA's CAA check

Certification Authority Authorization

Cons

- DNSSEC is recommended but not required, opening up potential for DNS record manipulation
- CA and customer opt-in nature makes CAA non-deterministic
- Potential perception of CAA being a mechanism for CAs to “lock in” customers

Public Key Pinning

- Client (browser) tracks what certs are used by a website
  - Can be preloaded into browser
  - Alternatively, Web server can make an assertion in the HTTP Header about what certificate(s) it must use
- Generate an alert or block the connection if a different cert is used
- Two current IETF drafts:
  - Trust Assertions for Certificate Keys
  - Public Key Pinning Extension for HTTP

Public Key Pinning

Pros

- Reduces attack surface for a given site from approx. 65 roots (and potentially hundreds of intermediates) down to 1-2
- Proven value in detecting compromise
  - Would've detected DigiNotar problems
- Enhances existing ecosystem
- Doesn't suffer from CAA's potential "lock in" perception

Public Key Pinning

Cons

- Trust on First Use – doesn’t protect initial connection
- Doesn’t protect against key compromise
- Creates operational challenges with key exchanges
- May be best as a reporting mechanism
  - Long deployment horizon
  - Impact of false positives in "hard fail" mode

Endgame

- Where do these proposals go from here?
  - Which proposals get adopted (CT, CAA, Pinning) – and in which form(s) – is yet to be decided and groups will continue good research
- Incremental improvements will progress
  - Continue to monitor emerging security threats
  - Improving WHOIS – CA's must be informed of ownership changes
  - Impact of gTLD MITM
- SSL will improve. Systems that retain the improvements made by CA's as the knowledgeable trust anchors will advance internet security most effectively.

Next Steps

- More research and multi-stakeholder collaboration is needed with ICANN community.

- CA's are interested in improving the landscape and DigiCert is taking a lead role, especially with CT.

- Many smart people are working on these issues, and the future looks good.

More Info

- Resources
  - CA/B - Baseline Requirements for the Issuance of Publicly Trusted Certs
  - CA/B - Network and Certificate System Requirements
  - CA/B - Letter to ICANN - Security Implications of New gTLD's
  - Mozilla - CA Certificate Policy v2.1
  - Microsoft - Root Certificate Program
  - Online Trust Alliance - CA Best Practices
  - CA Security Council
  - WebTrust - Audit Criteria for CAs
- Open Proposals
  - Certificate Transparency Overview (CT)
  - Certificate Transparency (CT) - rfc6962
  - Certificate Authority Authorization (CAA) - rfc6844
  - Public Key Pinning - IETF Draft