



Trust-Related Activities: Internet Certification Authorities

Revocation and SSL Replacements/Enhancements

Massimiliano Pala <pala@nyu.edu>
CRISSP – NYU Poly
OpenCA Labs

Scott Rea <Scott@DigCert.com>
DigiCert

Outline

▶ Proposal for “solving” TLS Trust Issues

- ◆ Background
- ◆ Summary of proposed solutions
- ◆ Current Activities

▶ Revocation Information Availability

- ◆ A Phased Approach
 - ◆ Lightweight OCSP, OCSP Stapling, CRL Sets
 - ◆ OCSP over DNS, Certificate Flag
 - ◆ LIRT and CA Whitelists

◆ IETF scheduled activities

Acknowledgments

▶ On-Going Work

- ◆ Dartmouth College
- ◆ NYU Poly
- ◆ DigiCert

▶ Collaborations w/ other partners from

- ◆ CAB Forum

▶ Future collaborations

- ◆ IETF (?)
- ◆ Other Edu (e.g., CMU, Stanford)

Background

- ▶ **Two Main Issues in Internet Certification Authorities and browser environments**
 - ◆ Solving the limitations of the flat trust model in Browsers
 - ◆ Availability of revocation information
 - ◆ **Soft- vs hard- failure systems**

Trust in Browsers

▶ **Number of compromises in 2011**

- ◆ Solutions in place for trust in browsers are inadequate
 - ◆ One “big” stick solution only
 - ◆ “Flat” trust model
 - ◆ How to verify that a domain owner asked for a particular cert when only using Domain Validated issuance processes
 - ◆ Besides EV & OV certs

▶ **Proposals for Internet CAs Trust Infrastructure**

- ◆ Enhancements (DANE, Certificate Pinning)
- ◆ Proposals for YATTP (Yet Another Trusted Third Party) (Perspectives, Convergence)
- ◆ Enhancements + TTP (Sovereign Keys, MECAI)

DANE

- ▶ **Certificate information in DNS**
- ▶ **Definition of a new DNS record (TLSA)**
 - ◆ Usage, Selector/Matching, Certificate Data
- ▶ **Usage**
 - ◆ CA Constraints (use a specific CA)
 - ◆ Service Certificate Constraints (accept only a specified cert)
 - ◆ Trust Anchor Assertion (use the domain-provided TA for validation)
- ▶ **Concerns**
 - ◆ Deployment of DNSSEC (and DNSSEC-enabled clients)
 - ◆ Migrating CAs operations to DNS operators is challenging
 - ◆ **DNSSEC might add delay for TLS** (caching would help)
 - ◆ Revocation Info could potentially be ignored (TLSA)

Certificate Pinning

- ▶ **Web hosts to express which certificates may be expected in the host's certificate chain**
 - ◆ HTTP Header with Subject Public Key Info (SPKI)
 - ◆ UA to store the Pinning information
 - ◆ Validation => set of presented certs intersects Pinning Metadata
- ▶ **Concerns**
 - ◆ Easy to lock-out domains
 - ◆ Management of PIN revocation information
 - ◆ Bootstrap problem
 - ◆ HSTS records via HTTP site can provide successful attack
 - ◆ Changes on Clients + Servers
 - ◆ Backup Certificate / CAs strongly suggested for recovery

Perspectives

▶ **Notary hosts to observe a server's public key**

- ◆ Notary Authority
 - ◆ **provides list of available notary servers and**
 - ◆ **their public keys to the notary clients**
- ◆ Notary Servers
 - ◆ **Keep records of server key data**
- ◆ Notary Shadow Servers
 - ◆ **Each notary server also acts as a “shadow server”**
- ◆ Notary Clients

▶ **Concerns**

- ◆ YATTP approach
- ◆ Multiple parties involved and high operational costs
- ◆ Oriented toward “power users” (proactive approach)

Convergence

▶ Sort of “Extended” Perspective

- ◆ Same entities as in Perspective
- ◆ Extended approach to allow for different backend
 - ◆ e.g. support for DNSSEC/DANE
- ◆ Currently it uses Perspective as backend
- ◆ Improves privacy (two notaries to collude to compromise history)
- ◆ Improved responsiveness via caching

▶ Concerns

- ◆ Too flexible – configurability seen as a weak point (use of defaults)
- ◆ Large companies would run the majority of servers (distribution)
- ◆ Multiple certificates for a domain (each connection) not supported

MECAI

▶ **Multiple Endorsing Certificate Authority Infrastructure**

- ◆ Simpler Perspectives-like approach run by friendly CAs
- ◆ Vouching Servers, Vouching Authorities
- ◆ Vouching Data
 - ◆ **hostname, server certificates**
 - ◆ **vouching statement from CA regarding revocation and timestamp**
- ◆ Client request VD from two different Cas

▶ **Concerns**

- ◆ Additional Servers required
- ◆ Economic incentives for a CA to provide services for competitors
- ◆ Availability of VD
- ◆ Very Early Stage – no formal protocol specs

Sovereign Keys

- ▶ **Persistent, secure association between Internet domain names and public-keys**
 - ◆ Operational public-keys cross-signed with sovereign keys
 - ◆ Timeline Servers
 - ◆ **Append-only data structures for mapping domains/keys**
 - ◆ **Require control over DNS and Timeline Servers**
 - ◆ OCSP response is required before adding keys/certs to TS
 - ◆ Support for different protocols (e.g., TLS for smtps)
- ▶ **Concerns**
 - ◆ YATTP
 - ◆ Public keys of the timeline servers are shipped with clients
 - ◆ No complete specifications

Metrics and Comparisons

▶ Developing a Solution-Comparison Metrics

- ◆ Generating a cost-based metrics
- ◆ Allow for comparison of different solutions
 - ◆ **Same solution can impact differently on deployed infrastructures**

▶ Status

- ◆ Work still in progress → data will be available shortly...

Activities on Revocation in ICA

► Different Problems from different Perspectives

- ◆ Revocation Data Availability Problem
- ◆ Access time to OCSP services
- ◆ High maintenance costs for high-volume environments

► Proposals

- ◆ Short term → Lightweight OCSP Profile [RFC5019] + CDN friendly
- ◆ Mid term → push for OCSP over DNS
- ◆ Long term → CA whitelists

Short-Term Approaches

▶ ICAs Best Practices

- ◆ pre-computed responses
- ◆ Publication every few hours / once a day
- ◆ High costs for deploying OCSP servers

▶ OCSP as small CRLs

- ◆ No need for OCSP requests
- ◆ Need to provide OCSP responses as efficiently as possible
- ◆ Use different distribution mechanisms → CDNs, Stapling

▶ Issues

- ◆ Only GET (POST can not be cached) → clients still use POST!
- ◆ Different encoding of the request → CDNs cache miss!

▶ Update for RFC5019 [?]

Mid-Term Approaches

▶ DNS can be used to distribute OCSP responses

- ◆ No need for request/response protocol
- ◆ Allows to lower the costs of distributing revInfo to clients
- ◆ **Use of the DNS caching system**
- ◆ Possible for SSL/TLS certificates for larger sites

▶ Current Challenges

- ◆ OCSP responses waste bits on the wire if cert is valid
- ◆ DNS allows for single UDP packet (if resp < 512bytes)
- ◆ Use of EC keys might be advisable
- ◆ Definition of DNS-based URLs for OCSP distribution
- ◆ Allow for fallback URLs for backward compatibility
- ◆ **Some clients only query the first URL in AIAs**

Long-Term Approaches

- ▶ **Lightweight Internet Revocation Tokens**
 - ◆ Similar to Request-less OCSP
 - ◆ Client-known data is not included in the response
 - ◆ Small size (< 200~300 bytes with EC signatures)
 - ◆ Compatible with different transport protocols
 - ◆ **HTTP (CDNs), DNS, Peer-to-peer**

- ▶ **Proposal for a new I-D for LIRT**

Long-Term Approaches (cont.)

▶ CA whitelisting

- ◆ Need for a mechanism to select different level of trust for CAs
- ◆ Possibly build a CA Body for CAs governance (CAB Forum WIP)

▶ Solutions are being discussed in CAB Forum

- ◆ No common vision, yet
- ◆ Costs and operational barriers
- ◆ ... summarizing, stay tuned to this space..!

Questions ?

► Contacts

- ◆ Massimiliano Pala <pala@nyu.edu> || <director@openca.org>
Research Professor at CRISSP – NYU Poly
Director at OpenCA Labs
- ◆ Scott Rea <Scott@DigiCert.com>
VP GOV/EDU Relations
Sr. PKI Architect