SEARCH for Trust

SSL/TLS Enhancement or Alternatives for Realizing CA Homogeneity (SEARCH) for Trust

Research by Dartmouth College
and New York University
Reported by: Scott Rea
Sr. PKI Architect, DigiCert Inc.

Research Advisory

Research

- This is a report on research and development activities being undertaken by Dartmouth College and New York University in collaboration with industry and other partners.
- Collaborators:

  - Dartmouth: Alexandra Grant Alexandra.C.Grant.12@Dartmouth.edu
  - Dartmouth: Prof. Sean Smith sws@cs.dartmouth.edu

  - NYU: Prof. Massimiliano Pala pala@nyu.edu
  - NYU: Mallik Arjun mallik.v.arjun@gmail.com

CAs as a Source of Trust

- There are a number CA “Trust Anchor” (TA) certificates that come pre-installed in various Applications that are “trusted” to perform various security tasks
  - Verify identity of web sites, establish secure connections, encrypt data to/from
  - Verify identity of software makers, applications or plug-ins given kernel level privileges i.e. trusted extension of the Operating System
  - Verify identity of individuals, or source/destination of communications/data
- Many applications trust the set of pre-installed TAs in the underlying Operating System
- Depending which application on which operating system you are using, there may be a different set of TAs to contend with

NYU Dartmouth

ICAs in the News…

- **Comodo** – Mar 2011
  - **Multiple RA breaches** : mis-issuance of at least 9 certificates
  - Italian & Brazilian RAs were targeted
- **StartCom** – Jun 2011
  - **Breach of Server** : no certificates mis-issued
  - DoS of services to StartCom customers result
- **DigiNotar** – Jul 2011 (didn't disclose until Aug 2011)
  - **Major Breach** : 500+ certs issued caused by poor security
  - CA now out of business
- **Globalsign** – Sept 2011
  - **Breach of Server** : but no certificates were mis-issued
- **DigiCert Malaysia** (no relationship to US company) – Oct 2011
  - Issues certificates with weak keys, lacking extensions to revoke them
  - Bad certs were re-purposed to sign **malware**
  - CA certificate was revoked
- **KPN** (another Dutch CA) – Nov 2011
  - **Breach of Server** : no certificates mis-issued
  - DoS of services to KPN customers result

NYU Dartmouth

Overhaul the whole ICA system?

- Some folks are calling for an overhaul of the entire CA system
  - To better protect against MitM attacks
  - To eliminate the ICA weakest link issue
  - To standardize the processes used in identity verification and issuance
  - To provide capability of easily revoking less trustworthy entities and have that be honored by the system
  - To be able to represent TAs as having differing levels of trust for different purposes (rather than a one size fits all)
  - To allow users/communities be better able to manage the TAs and their issued certificates

NYU Dartmouth

Proposed Solutions to Mitigate Attacks

- The set of proposals being evaluated include:
  - Perspectives
  - Convergence
  - MECAI (Mutually Endorsing CA Infrastructure)
  - DANE
  - Public Key Pinning
  - Sovereign Keys
  - CAA Record in DNSSEC
  - Certificate Transparency

NYU Dartmouth

Analysis: Metric Overview

- A goal of the research is to construct a metric that will allow us to make a fair comparison between these proposed systems
- The methodology to achieve this entailed:
  - Defining categories for comparison
  - Defining scale of metric to be used
  - Applying the metric to the individual proposals
  - Ranking the proposals based on the metrics distilled
  - Drawing conclusions about the systems based on their ranking
- The Ranking System entails applying a score to each category on a scale 1 to 10 (10 = system successfully meets all the stated requirements, 1 = system either did not address the use case or failed to meet any of the goals)
- Once scores are assigned for each proposal under each category, the proposals can be ranked for overall effectiveness and likelihood of being successful

NYU Dartmouth

Analysis: Categories

#	Category
1	There must be resources available with a defined business case to form and operate the trust services
2	The proposed system should minimize changes to the experience of actors within the existing system (ICA practices changes are more favorable than web host changes, which are more favorable than web client changes)
3	Parties responsible for trust services must be trustworthy and employ good security practices
4	The system must scale
5	The security mechanisms of the system must not cause significant latency
6	Clients must be able to identify compromise and act accordingly
7	Clients must be able to revoke trust and users should have more control over their trust anchors
8	Default implementations should improve the flexibility/capability/protection of the majority of web users
9	The system must guard against DoS attacks in the event that a Trust Service is compromised or unresponsive to client requests. It should also not create a single point of failure.
10	The system should address the MitM problem of the current system by reducing the probability of this event or increasing a user's likelihood of identifying when they are under attack
11	User privacy must be protected

- This Table represents the categories used for analysis

NYU Dartmouth

Analysis: Categories

	Convergence	Perspectives	MECAI	DANE	CAA	Pinning	Sovereign Keys	CT
1. Resource Availability and Defined Business Case	4	4	9	3	7	6	2	5
2. Minimal Changes	3	4	3	2	6	3	3	4
3. Trustworthy & Secure Trust Services Source	2	2	5	3	3	5	3	4
4. Scalability	4	4	9	2	5	3	6	3
5. Latency	7	6	2	6	9	6	4	5
6. Compromise Detection	5	5	6	5	2	8	4	6
7. Trust Revocation	8	4	4	2	3	6	5	2
8. Improved protection/ flexibility/capability of web users	7	7	7	5	3	5	5	5
9. DoS/Failure Prevention	3	3	3	2	5	3	3	4
10. MitM Attack Prevention & Response	4	5	5	7	5	7	7	7
11. User Privacy	7	2	1	9	10	8	4	6
Totals	**54**	**46**	**54**	**46**	**58**	**60**	**46**	**51**

- This Table represents the Scores assigned to proposals

NYU Dartmouth

Analysis: Categories

Rank	Proposal	Total Score
1.	Pinning	60
2.	CAA	58
3.	MECAI	54
4.	Convergence	54
5.	CT	51
6.	DANE	46
7.	Perspectives	46
8.	Sovereign Keys	46

- This Table represents the Ranking of proposals based on scores

NYU Dartmouth

Initial Conclusions

- Based on this analysis, be believe the systems listed below have little chance currently of being viable solutions to address the following issues:
  - Present an alternative Trust Source mechanisms to existing ICAs
  - Reliably detect compromise and MitM attacks and protect user accordingly
  - Provide users with greater flexibility and configuration of trust services while protecting privacy

- ✖ **Sovereign Keys**
- ✖ **DANE**
- ✖ **Certificate Transparency**
- ✖ **Perspectives**
- ✖ **Convergence**
- ✖ **MECAI**

NYU Dartmouth

Initial Conclusions

- Based on this analysis, we believe the following systems may represent viable solutions/enhancements

HSTS CA Pinning

CAA Records in DNS

  - (However this system provides very little real incremental protections unless it is deployed in conjunction with other solutions and also supported by majority of ICAs)

NYU Dartmouth

Industry Response

- In light of recent attacks, the ICA industry has also mobilized to address the deficiencies.
- CAB Forum is focusing on the following areas to bolster ICA consistency, security, and reduce the potential for breakdowns due to the weakest link principle:
  - Published a minimum set of security standards for operations and identity vetting to which EVERY ICA must attest
  - Support implementation of available Revocation mechanisms and define more timely, available, and efficient protocols to be implemented in the future
  - Implement controls that enhance the system's ability to discover and repel MitM Attacks
  - Working with industry audit professionals to define stronger audit controls that can be applied to demonstrate compliance with standards and best practices

NYU Dartmouth

Analysis: Existing System

	Existing SSL/TLS System	SSL/TLS with CAB Forum Projects Implemented	Pinning
1. Resource Availability and Defined Business Case	**9**	**8**	**8**
2. Minimal Changes	**10**	8	3
3. Trustworthy & Secure Trust Services Source	**5**	7	5
4. Scalability	**8**	8	3
5. Latency	**7**	9	6
6. Compromise Detection	**5**	7	8
7. Trust Revocation	**6**	9	6
8. Improved protection/ flexibility/capability of web users	**5**	8	5
9. DoS/Failure Prevention	**6**	8	3
10. MitM Attack Prevention & Response	**4**	7	7
11. User Privacy	**7**	7	8
Totals	**72**	**86**	**62**

- This Table represents the Scores assigned to leaving the system in status quo vs implementing the CAB Forums set of initiatives vs best of proposals

NYU Dartmouth

Analysis: Existing System

	Existing SSL/TLS System	SSL/TLS with CAB Forum Projects Implemented	Pinning
1. Resource Availability and Defined Business Case	9	8	8
2. Minimal Changes	x	x	x
3. Trustworthy & Secure Trust Services Source	5	7	5
4. Scalability	8	8	3
5. Latency	7	9	6
6. Compromise Detection	5	7	8
7. Trust Revocation	6	9	6
8. Improved protection/ flexibility/capability of web users	5	8	5
9. DoS/Failure Prevention	6	8	3
10. MitM Attack Prevention & Response	4	7	7
11. User Privacy	7	7	8
Totals	62	78	59

- This Table represents the Scores assigned to leaving the system in status quo vs implementing the CAB Forums set of initiatives vs best of proposals

NYU Dartmouth

Conclusions

- Based on this analysis, it would appear that taking steps to mitigate MitM attacks and improving revocation efficiency by using any of the proposed systems actually degrade the existing infrastructure overall when considering the criteria selected for this research
  - The top two scoring proposals (Pinning and CAA Records), rely upon the existing system remaining in place
  - While addressing the MitM threat, the top two proposals actually create additional burdens on the system in terms of latency, scalability, and DoS threats
  - The existing system scores better than the top proposals based on our criteria
  - Implementing the CAB Forum initiatives will improve the system overall and scores far superior to ratings to any of the eight original proposals

Implementation of the CABF initiatives:

- 1) Common minimum security practices, 2) Improved revocation processing, 3) Mitigation of MitM attacks and 4) Better audit.

NYU Dartmouth

Summary

- As a result of successful and high profile attacks on ICAs, trust in the general CA system of SSL/TLS PKI has been degraded.
- A number of alternative and/or enhancements to the existing system have been proposed
  - Many of these are in development / research stage still
- This research has considered 8 different systems as alternatives and evaluated them each against a common set of criteria developed for this purpose
- CAB Forum is implementing a number of initiatives to improve the existing ICA system
- More research & evaluation is needed – this is a WIP

NYU Dartmouth

Summary

- Many proposals are immature and under-deployed
- Further correlation is needed
- Re-evaluation of the systems may be possible at later dates
- There are no proposals in their current state of definition/ implementation that are ready today to take over from the existing SSL/TLS ICA system
- The current system with some proposed enhancements ranks best and is leading solution for improving security
- CAB Forum initiatives to improve the existing system addresses deficiencies in the current system

NYU Dartmouth

DigiCert Contacts

Website: http://www.DigiCert.com/

Email: support@DigiCert.com

Scott Rea: (801) 701-9636, Scott@DigiCert.com
http://www.digicert.com/news/bios-scott-rea.htm

NYU Dartmouth