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

Table of Contents

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:
  - NYU: Prof. Massimiliano Pala pala@nyu.edu
  - NYU: Mallik Arjun mallik.v.arjun@gmail.com
  - Dartmouth: Alexandra Grant Alexandra.C.Grant.12@Dartmouth.edu
  - Dartmouth: Prof. Sean Smith sws@cs.dartmouth.edu

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

CAs as a Source of Trust

- For an application to “trust” a credential, it must be issued by an authority (TA, or sub-CA that chains back to a TA) that is trusted for the intended purpose by the OS or application being used
  - Warnings are given to the user when this is not the case
- Not only are there root TAs that are a source of trust, but any subordinate CA to a root TA can also be targeted to subvert trust
  - There are various methods (platform specific) for how these sub-CAs are managed
- Some communities such as IGTF provide transitive trust services or trust recommendations by accrediting additional TAs that can be used to enhance or restrict the set of default CAs recognized by a grid compliant application

CAs: High-Value Targets

- Attackers are seeking to get control of credentials issued by trusted CAs so that unsuspecting users can be fooled into relying on transactions originating from a malicious source, without being aware via a process known as a Man-in-the-Middle (MitM) attack
- Instead of attacking a single web site directly to try to gain access to its private key, and thus impersonate that site, an attack is more efficient if it can target the issuing CA directly
  - This allows the attacker to generate as many keys as it wants and submit to a trusted CA : as long as they can convince the CA that they are really the authorized requestor in each case
  - Instead of just one domain compromise resulting from a MitM attack, they can potentially get many for the effort associated with just one compromise

Why Target CAs?

- Not all CAs are created equal
  - Out of the many CAs trusted as TAs for an application, some perform better than others in protecting their customers with better processes and more secure systems
  - Attackers of SSL/TLS systems are targeting lots of different CAs looking for any weaknesses they can exploit
  - One issue identified with the current Internet CA (ICA) system, is that all CAs are typically treated as equally trusted by an application/OS, when in fact they should/are not

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** (Dutch CA related to DigiNotar) – Nov 2011
  - **Breach of Server** : no certificates mis-issued
  - DoS of services to KPN customers result

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

Proposed Solutions to Mitigate Attacks

- There have been a number of proposals generated on ways to improve or replace the existing SSL/TLS system
- Until there is homogeneity of security and controls in all ICAs, the weakest link problem will continue to exist
  - unless relying parties have an easy way of identifying and constraining the range of ICAs appropriately
  - and applications/web clients/Operating Systems provide mechanisms for different levels of trust to be set and utilized in local trust policies
- This research looks at a set of proposed systems and/or protocols and seeks to gauge their potential effectiveness as an alternative and/or enhancements to the existing SSL/TLS system

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

Perspectives

- **Perspectives** see - http://perspectives-project.org/
- Overview:
  - This is a project that began around 2008 at Carnegie-Mellon. The objective was to improve the security of "trust on first use" (TOFU) services e.g. typical SSH connections or (relevant to SSL industry), browser based SSL connections using self-signed certificates.
  - The idea is to reduce Man-In-The-Middle (MITM) attacks in these scenarios by not letting an attacker inject an untrusted key at that critical first use point.
  - Using a set of distributed notary servers, one is able to get a "perspective" of what key was expected from the target service from a number of different locations, and over time. This reduces the vulnerability of localized attacks (the typical attack vector of most MITM) by exposing them with the broad "perspective" required for consensus by multiple notaries.

Perspectives

- Analysis:
  - Strength:
    - Ability to make trust decisions without having to rely solely on ICAs
    - Alternative for services looking to potentially avoid the costs of traditional PKI (this service could leverage self-signed certs)
    - More secure protocol for accepting previously unseen keys in comparison to the TOFU leap-of-faith
    - More flexible trust options for power users
  - Weakness:
    - Concern over “completeness”: verification is only done for initial HTTPS requests and not for subsequent elements such as scripts or images
    - Privacy not addressed as user browser activity revealed to notaries
    - Responsiveness concerns due to notary lag – time taken for notaries to update new info
    - Unclear how out-of-band notary authority public key information distribution will be handled (including adding new or revoking existing notaries that become untrustworthy)
    - Described by the authors as “not bullet-proof, only suitable for non-critical websites (NOT recommended for sites that require strong security and high uptimes)
    - Unclear who would serve as notary authorities or how they would be distributed
    - No business case for setup and operation of notaries
    - No specifications defined for notary authority security policies
    - No real gain in trust flexibility for the masses

Convergence

- **Convergence** see- http://convergence.io/
- Overview :
  - This is a project started by security researcher Moxie Marlinspike, and announced at 2011's Black Hat conference, and is based on previous work from the Perspectives Project as detailed previously. This project however, is aimed squarely at replacing the existing SSL CA system - that is its stated goal.
  - Similar to the Perspectives strategy, Convergence authenticates connections by contacting external notaries, but unlike the Carnegie based notaries, Convergence notaries can also use a number of different strategies beyond network perspective in order to reach a verdict - it calls this extensible trust agility.
  - Technologies touted as additional mechanisms within the system that might allow a trust decision to "Converge" are DNSSEC, BGP data, "SSL observatory" results, or even the existing CA validation system it seeks to subvert.
  - Another difference from Perspectives is that ANYONE can run a Convergence notary, there is no notary authority, and it is a much more flexible mechanism (in terms of operations and configurability) of managing trust.

Convergence

- Analysis:
  - Strength:
    - Ability to make trust decisions without having to rely solely on ICAs (Trust Agility aspect improvement over Perspectives)
      - More than just ICA trust architecture supported e.g. DNSSEC, BGP, SSL Observatory etc are also potential options
    - Alternative for services looking to potentially avoid the costs of traditional PKI (this service could leverage self-signed certs and/or DNSSEC for trust basis)
    - More secure protocol for accepting previously unseen keys in comparison to the TOFU leap-of-faith
    - More flexible trust options for power users
    - User's active participation -
      - Ability to choose which notaries to query for key information
      - Ability to pick which notaries to add to the client's list of Trusted notaries, and to remove notaries which they feel are no longer trustworthy
    - Addresses the Perspectives "completeness" issue by checking all HTTPS requests through the notary mechanism rather than just initial connect
    - Uses Notary "bouncing" to address the Perspectives privacy deficiencies (two notaries would have to collude to compromise user privacy)
    - Uses caching to address the Perspectives notary lag issue

Convergence

- Analysis:
  - Weakness:
    - Most users would not change their default settings, so the default set of notaries included in the browser would remain unchanged, making those notaries subject to extremely high traffic loads, and potentially negating some of the responsive improvements
    - Advantages gained by placing the trust decision in the hands of users will likely be lost entirely for the majority
    - The system has the potential to continue to train most users to simply ignore security warnings and proceed to the site anyways as they do with the current SSL/TLS system
    - Unclear who would serve as notary authorities or how the master lists would be distributed/updated
    - No business case for setup and operation of notaries
    - No specifications defined for notary authority security policies
    - Does not support captive portals
    - Does not support sites with frequent updates to security and trust parameters very well e.g. “Citibank” use of one-time certs, or SLCS
    - Narrow community support (exists as a FF plugin only at this point)

Mutually Endorsing CA Infrastructure

- **MECAI** see- https://kuix.de/mecai/
- Overview :
  - The MECAI system makes use of Vouching Servers (VS), in which a CA that did NOT issue the certificate in question acts as a Vouching Authority (VA) for others
  - Similar to the Perspectives and Convergence strategy, MECAI authenticates connections by contacting external notaries (the VS), but unlike the previous notary proposed systems, MECAI notaries MUST be actually other CAs.
  - When a client connects to a server, the client may pick a vouching CA (or list of candidate vouching CAs) that it trusts.
  - A VS is required to keep a list of the currently accepted root CA certificates (trust anchors) as accepted by each of the Trust Lists the VA supports.
  - A VS is required to be in active human contact with the people that maintain the various Trust Lists

Mutually Endorsing CA Infrastructure

- Analysis:
  - Strength:
    - More secure protocol for accepting previously unseen keys in comparison to the TOFU leap-of-faith
    - Business case for setup and operation of notaries established
    - Notary authority security policies established (leverage existing ICA security policies)
    - More flexible trust options for ALL users
  - Weakness:
    - Immaturity: No current implementation or formal spec
    - Little incentive for ICAs to adopt business case for setup and operation of notaries (unless common agreement is established – potential for trust cartels)
    - Advocates the creation of a TLS/SSL handshake extension in order to expedite the server certificate verification process
      - Takes a lot longer for adoption in community when protocol is being amended
      - Could introduce significant latency due to the increased size of the handshake
      - Requires that web servers upgrade to support the MECAI design (from an implementation perspective this might be considered unreasonable unless there is sufficient incentive for sites to support it)

DANE

- **DANE** see - https://datatracker.ietf.org/wg/dane/charter/
- Overview:
  - DANE stands for DNS-based Authentication of Named Entities and is actually an IETF working group item.
  - The basis of the DANE approach is to leverage signed DNS entries (DNSSEC) to make some inferences about the legitimate certificates or potentially just keys that are protecting web sites.
  - If a certificate (or public key) is seen by a client (e.g. browser) that isn't consistent with the DANE record, it can be treated with suspicion - this will help eliminate Man-In-The-Middle (MITM) attacks, and can also facilitate elimination of false issuance problems from the set of authorized CAs
  - DANE relies upon DNSSEC for trusts establishment in replacement of the existing CA hierarchy, despite DNSSEC only providing integrity checks on source data and not authentication of that data.
  - DANE potentially moves the responsibility of web site security into the span of control of DNS

DANE

- Analysis:
  - Strength:
    - Domain operators have the power to advertise new trust anchors or revoke ICAs as they see fit which adds trust flexibility not available within the current PKI system
    - No requirement to rely upon the ICA system at all if desired, at least for secure domain associations
    - DANE can only certify trust for the domain – this limits the scope of trust just to the domain in question, so if a compromise occurs, only the subject domain is effected by it
  - Weakness:
    - Requires DNSSEC to be implemented – ubiquitous implementation will provide greatest benefit and realistic platform for DANE
    - Domain operators may become the focus of existing attacks, and inheriting the responsibility of web site security into the span of control of DNS operators who typically have not needed to deal with security elements may be a barrier
    - Whilst internal domain operations may know organizational trust preferences, any outsourced domain management will have to establish controls around this new trusted role
    - Trust is embodied into a single DNSSEC root – potentially creating a single point of failure for the entire system
    - There may be added latency to the TLS connect process due to DANE trust processing
      - Large text records over DNS have not proven efficient
    - DANE can only certify trust for the domain – ICAs services being replaced can provide more than domain validation e.g. EV and OV validated credentials

Public Key Pinning

- **HSTS Pinning** see - http://www.imperialviolet.org/2011/05/04/pinning.html
- Overview :
  - Web sites may want to restrict the CAs who can issue certificates for their domain to one or a few that they trust.
  - This can be accomplished via a list of certificate fingerprints/ names/keys that are exclusively allowed to act as trust anchors for a given domain
  - This list can be included in specific site HTML or HSTS headers or in a DNS record served up over DNSSEC

Public Key Pinning

- Analysis:
  - Strength:
    - Puts control for managing weakest link issue into the hands of web site admins providing trust flexibility
    - Automatic lockout when under active attack (does not need user interaction)
    - Web hosts are the only resource that need configuration (although clients also need to be updated initially in order to support pinning)
  - Weakness:
    - As with all TOFU systems, there is a bootstrap issue where the initial visit to a new site is open to attack which if successful, impacts the system for the rest of its lifetime
      - Preloading PINs avoids this, but produces a scaling issue
    - Client can't pin to a cross-certifying root without potentially erroneously rejecting or validating pins
    - Potential for users to become "locked out" in the event of inadvertent pin failure or failed validation
    - When DNSSEC option is used:
      - Requires DNSSEC to be implemented – ubiquitous implementation will provide greatest benefit and realistic platform
      - It potentially moves the responsibility of web site security into the span of control of DNS operators who typically have not needed to deal with security elements
      - A potential issue for relying on DNSSEC is that it only provides integrity checks on source data and not authentication of that data

Sovereign Keys

- **Sovereign Keys** see - https://git.eff.org/?p=sovereign-keys.git;a=blob_plain;f=sovereign-key-design.txt;hb=master
- Overview :
  - This system implements a persistent, secure association between Internet domain names and public-keys called Sovereign keys.
  - Sovereign public keys can be registered for a particular service under a particular domain, clients/user agents (UAs) using that service must verify the operational public-keys (such as those at the end of X.509 certificate chains) have been cross-signed by the Sovereign keys.
    - If verification fails i.e. if one cannot verify a signature from the Sovereign Key over the server's key, client/UA must terminate the connection after informing the user with appropriate message.
  - Sovereign Keys are registered and validated using *Timeline Servers* which are responsible for storing the mappings between domain names and sovereign keys with a reliable timestamp.
    - Timeline servers maintain public and private key pairs which are used to authenticate themselves and the public keys for these are shipped with client software
    - The timeline servers exist for the sole purpose of recording and preserving a correct history of claims to Sovereign Keys.
    - Clients believe the oldest claim to a key for any given name plus any self-signed updates it has subsequently published

Sovereign Keys

- Analysis:
  - Strength:
    - Reduces the number of attack points so that compromise can be more easily detected and quickly dealt with
    - Automatic lockout when under active attack (does not need user interaction)
    - Reduces the amount/scope of reliance on ICAs (but still requires them for validation operations)
  - Weakness:
    - Author indicated it would take a “significant” effort and a “major migration of internet resources” to implement
    - Embedded keys for timeline servers in clients may lead to update issues as timeline servers are added, changed or reneged
    - Does not appear to be definitions/standards around operation and management of timeline server yet – incomplete definition of system
    - Business case for setup and operation of timeline servers NOT established
    - There may be added latency to the TLS connect process due to SK trust processing
    - Sovereign Keys need to be backed up redundantly and revocation and re-issuance need to be managed well.
      - Anyone can do this, but specialized service providers will be the lowest-effort way to do it, potentially introducing another TTP

CAA Record in DNSSEC

- **CAA record in DNSSEC** see - http://tools.ietf.org/html/draft-hallambaker-donotissue-04
- Overview :
  - The goal of the (CAA) DNS Resource Record is to allow a domain owner to choose which ICAs should be authorized to issue certificates for that domain.
  - Under this system, ICAs must follow the policies defined in the Certificate Policy Statement in order to issue certificates. The CAA records will be the basis for an ICA's validation requirements.
  - The system mimics DANE's design in that a domain publishes a record in DNS restricting the ICAs which can issue certificates for it. However, rather than addressing this information to a client, the record is intended for use by the ICAs who will be responsible for checking the record and only issuing a certificate if their name is on the list.
  - This setup would require the ICAs to honor the CAA records and behave correctly. (This system still relies on web clients trusting ICAs).
  - Each CAA record contains a [tag, value] pair, The **CAA Issue Property** grants authorization to certificate issuers and also enables restriction processing for the domain
  - While DNSSEC is recommended for additional security it is not a required part of the CAA record implementation.

CAA Record in DNSSEC

- Analysis:
  - Strength:
    - Provides flexibility and capability for domain admins to advertise and optionally limit the ICAs which can issue certificates for their domain
    - Leverages but does not require DNSSEC
      - Implementable as DNSEC capabilities transition over time
    - Does not require any changes to processing of systems other than ICA procedures
      - Inexpensive implementation
  - Weakness:
    - Still relies on ICAs to behave well with no real deterrent mechanism other than sullied reputation
    - Client behavior does not change, there is no enforcement in the client
      - Unless poor reputation causes clients to de-list an ICA in future
    - Very weak impact on addressing MitM attacks with minimal reduction in risk from such attacks compared to status quo
    - Weakest link issue is not addressed
  -

Certificate Transparency

- **Certificate Transparency** see - http://www.certificate-transparency.org
- Overview :
  - Certificate Transparency is the system proposed by Google to prevent certificate abuse and it relies on the idea that every certificate should be published in an audit log which is publicly available.
  - There is a certain amount of cooperation between parties which is necessary with such a system since Certificate Authorities must have published accompanying audit proofs for each certificate they issue.
  - The incentive from them to publish this information stems from the fact that clients will not accept certificates if they do not collude with any of the ICA's audit logs.
  - The system strives to ensure that no certificate will be issued for a domain without the domain owner's knowledge. It also reduces the client's need to solely trust ICAs since a certificate may be recognized as fraudulent using information from the logs.
  - CT relies on audit logs, audit proofs, and Merkle trees to look up and crosscheck certificate information to ensure their validity. An audit proof created by an ICA is placed in the audit log to be verified by clients
    - The Merkle tree is a type of hash tree where nodes higher up on the tree are the hashes of their children.
    - In this case the, the leaves of the Merkle tree will be the hashes of the certificates which need to be signed and the root of the Merkle tree will be the hash over all the children.
    - For each certificate, the signature includes the root hash value along with the path from the particular signature up the tree to the root. An **audit proof** includes the Merkle signature on the top hash along with the list of hashes from the top of the Merkle tree down to the particular certificate.

Certificate Transparency

- Analysis:
  - Strength:
    - Domain owners have an opportunity to be aware of the certificates which have been issued for their domain
      - Helps protect users from accepting fraudulent certificates if domain owners proactively police issuance
      - Helps in the case of mis-issuance
  - Weakness:
    - Malicious issuers will not participate, does not deter issuance of malicious certificates for MitM attacks (but does help identify them)
    - Adds significant burden to ICA issuance process
      - Lowers ICA's incentive to participate
      - Increases issuance lag time for ICA customers
    - Audit log monitoring is more efficient to outsource to trusted third party
      - Issues associated with setting up and operating YATTP including who is qualified, business case for viability, standards for operations etc etc
    - A single public audit log would potentially become a single point of failure or introduce scalability issues to the system
    - Does not address revocation
    - Limited support (only Chrome browser to date)
    - Minimally effective unless widely supported
  -

Analysis: Metric Overview

- A goal of the research was 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

Analysis: Metric Ranking

- The Ranking System entails applying a score to each category
- The scale of the scoring utilized was 1 to 10 where a 10 represented the system successfully meets all the stated requirements of the category, and a 1 indicates the system either did not address the use case or failed to meet any of the goals of the category.
- Once scores are assigned for each proposal under each category, the proposals can be ranked for overall effectiveness and likelihood of being successful

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

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

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

Conclusions

- Based on this analysis, be believe the systems listed below have little chance 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**

Conclusions

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

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)

Conclusions

- 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

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

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.

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
  - Each system was ranked in accordance with greatest overall compatibility and ease of implementation
  - The existing system was also evaluated based on the criteria and scored better that any of the other individual systems evaluated
- CAB Forum is implementing a number of initiatives to improve the existing ICA system
  - If their initiatives reach stated objectives, it will improve the overall system
  - Combining these initiatives with one or more of the proposed systems has potential to address all the concerns raised by the attacks

Summary

- This is a WIP: More research is needed
  - Many proposed systems are still very immature in their definition and implementation or deployment making a consistent assessment difficult
  - Further correlation of existing rankings should be performed based on common threads of trust, this may lead to more consistent outcomes
  - The relative closeness of the evaluated rankings may indicate correlation has not been adequately addressed (we expected greater variance – this should be evaluated further)
  - As proposals mature and functionality is added they should be re-evaluated against the developed criteria
  - There are no proposals in their current state of definition/implementation that are ready to step up and take over from even the existing SSL/TLS ICA system with its identified shortcomings
  - Those proposals that ranked the best were enhancements to the existing trust infrastructure rather than replacements for it
  - CAB Forum has identified several initiatives that will improve the overall system, and combining these with some of the proposals evaluated may address ALL of the deficiencies in the existing system
    - This approach would be contingent on enhancing the existing system and not replacing it

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