ABSTRACT

The security of the X.509 “oligarchy” Public Key Infrastructure for browsers and SSL web servers is under scrutiny in response to Certification Authority (CA) compromises which resulted in the circulation of fraudulent certificates. These rogue certificates can and have been used to execute Man-in-the-Middle attacks and gain access to users’ sensitive information. In wake of these events, there has been a call for change to the extent of either securing the current system or altogether replacing it with an alternative design. This panel will review the results of the research paper to be published that will explore the following proposals which have been put forth to replace or improve the CA system with the goal of aiding in the prevention and detection of MITM attacks and improving the trust infrastructure: Convergence, Perspectives, Mutually Endorsed Certification Authority Infrastructure (MECAI), DNS-Based Authentication of Named Entities (DANE), DNS Certification Authority Authorization (CAA) Resource Records, Public Key Pinning, Sovereign Keys, and Certificate Transparency. In the paper, a new metric is described that ranks each proposal according to a set of well-identified criteria and gives readers an idea of the costs and benefits of implementing the proposed system and the potential strengths and weaknesses of the design. The results of the research and the corresponding impacts for eResearchers and Government collaborators will be discussed by the panel.

INTRODUCTION

Recent attacks on Certification Authorities (CAs) [1, 2] trusted by default in popular web browsers and operating systems have led many to question the state of the Internet trust infrastructure. These security breaches of Internet Certification Authorities (ICAs), i.e. those utilized for trust in web based SSL, or their agents have allowed fraudulent certificates to be issued for popular domains, leading to compromised security and privacy for users of those domains in limited circumstances. While these breaches were quickly addressed once knowledge of them became public, they have turned a lot of heads and there is now a renewed effort to examine the trustworthiness of Public Key Infrastructures (PKIs) and the ICA system as a whole and how to efficiently address its current weaknesses.

The PKI system relies on the trustworthiness of ICAs to ensure that certificates are only issued after verification that the identity represented in the certificate is the one in control of the corresponding private key. This process, known as identity binding, should be as open and unambiguous as possible to allow the acceptance of the certificate by the broadest set of relying parties.

There are a variety of reasons why attackers would focus their efforts on ICAs (or their agents) as opposed to targeting an individual site or server and its corresponding certificate and associated private key. Compromising an ICA allows attackers to generate certificates on behalf of any person or entity that will be broadly trusted by the Internet community, providing many opportunities for further exploits. Unfortunately, in the eyes of the current web trust infrastructure, all ICAs are treated equally which, from a security perspective, is to say that they, and their certificates and records, are all trusted equally in generic applications like browsers or e-mail programs. Attackers always try to minimize the required efforts to achieve their goals. By attacking the least trustworthy ICAs, attackers can gain access to secure communications also to website protected by more trustworthy ICAs thanks to the flat trust model adopted in today’s applications.

With the number of recent attacks on ICAs, some have advocated that it is time to reevaluate PKI and to propose an alternative or enhancement to the ICAs behind the SSL/TLS system. The proposals which have attracted the most attention are Perspectives [5], Convergence [4], DANE [3], Public Key Pinning [6] or HSTS pinning [10], CAA Records in DNSSEC [7], Sovereign Keys [8], MECAI [9], and Certificate Transparency [11]. However, changes come with a price and it is paramount to understand the extent of costs and benefits (security, efficiency, and practicality) for each proposal to be able to compare these solutions. The approach described in the research paper allows to effectively determine the best routes to take in ensuring a secure, scalable, and efficient process for establishing trust relationships on the internet when considering an appropriate replacement or enhancement to the existing ICA trust system used by SSL/TLS.

Researchers and collaborators make extensive use of SSL/TLS connections when accessing, storing or manipulating data. What are the impacts to eResearchers of the vulnerabilities discovered, and if an alternative trust infrastructure were to be implemented? What are the implications to closed trust communities such as those utilized by high performance computing and grids? A panel will explore these questions and expound upon reactions to the release of the findings of the research paper.

EVALUATED PROPOSALS

Perspectives

The Perspectives [5] proposed design uses a network of entities called notary hosts to observe a server’s public key via multiple network vantage points. Perspectives allows to observe the public keys presented to different clients for the same query: any disagreement among the observed key values would indicate a potential problem.

Convergence

Convergence [4] builds on Perspectives’ design, extending the basic system to include more features as well as fixing some noted weaknesses in the Perspectives model. Convergence’s “trust agility” is based on two main principles. First, a trust decision can be easily revised at any time. Second, individual users can decide where to anchor their trust. The difference between Perspective’s basic distributed design and Convergence lies in the user’s active participation in choosing which notaries to query for key information.
**MECAI**

Mutually Endorsed Certificate Authority Infrastructure (MECAI) [9] proposes a system which, much like Perspectives and Convergence, relies on the implementation of web notaries responsible for making statements about facts that can be discovered on the web. However, instead of replacing the ICA system tout court, MECAI’s notaries will be run by the ICAs. In MECAI, ICAs are granted the power to issue shorter lived vouchers confirming facts seen on the web from the perspective of a notary.

**DANE (DNS-Based Authentication of Named Entities)**

DANE [3] works by embedding certificate information into DNS records so that a client can receive authentication data directly from domain operators. Client applications query the domain operator about which certificates they should accept as credentials for that domain. While there is currently no way to check which ICAs are supposed to be issuing certificates for a domain, DANE allows domain holders to put restrictions on which certificates should be accepted based on ICA and service type. This allows certificate misuse to be detected more easily because clients will be able to report certificates they are presented that do not belong to the set of trusted ICAs. To ensure that the DNS records carrying DANE’s authentication information, DANE relies on the deployment of DNSSEC that allows for DNS records to be digitally signed.

**Public Key Pinning**

Public Key Pinning [10] places web hosts in charge of informing clients on which certificates they should expect to see in the host's certificate chain. When a User Agent (UA) receives response from the host, it validates the pinning header and, upon successfully meeting the required criteria (described in the next section - Components), stores the pinning metadata which is composed of the pin data and the max-age. Pin validation works by computing the fingerprints of the Subject Public Key Info structures in each certificate in the host’s validated certificate chain, checking to ensure that the set of fingerprints intersects with the set of fingerprints in the host’s pinning metadata.

**Sovereign Keys**

The Sovereign Keys [8] 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 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, the client will terminate the connection after informing the user with an appropriate message. This approach is somewhat similar to DANE, but it mandates for the use of a new set of servers to be setup instead of relying on an existing infrastructure like the DNS.

**CAA Record in DNSSEC**

The Certificate Authority Authorization (CAA) DNS Resource Record allows 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 which ICAs can issue certificates for it.

**Certificate Transparency**

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 ICAs must have published accompanying audit proofs for each certificate they issue. The incentive for them to publish this information stems from the fact that clients will not accept certificates if they do not collate 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.

**REFERENCES**

ABOUT THE AUTHOR(S)

Scott Rea, CISSP

Scott Rea is the VP of Government/Education Relations & Sr. PKI Architect at DigiCert Inc., a global Certification Authority. Rea has an established career as an innovative thought leader and sought-after public speaker who participates in, and influences the development of, emerging PKI policies, practices and applications.

Prior to joining DigiCert in 2009, Rea served as the Sr. PKI Architect for Dartmouth College where he also operated the Higher Education Bridge Certification Authority (HEBCA). Previous to his time at Dartmouth, he provided professional services for PKI integration for Identities. Rea is a founding member and current Vice Chair of The Americas Grid Policy Management Authority (TAGPMA), a previous Chair of TAGPMA and also of the International Grid trust Federation (IGTF). Rea is a board member and director/administrator of the Research & Education Bridge Certification Authority (REBCA), and past director/administrator of the U.S. Higher Education Root (USHER) and the Higher Education Bridge Certificate Authority (HEBCA).

Rea, a native Australian and CISSP, holds an MS in Computer Science from Queensland University of Technology as well as BS degrees in Mathematics and Computer Science. He and his wife, Andrea, and nine children reside in Lake Shore, Utah, U.S.A.

TBA Gov

AU Gov representative – To Be Advised

TBA EDU

EDU.au representative – To Be Advised