PRINCETON UNIVERSITY

CENTER FOR INFORMATION TECHNOLOGY POLICY
PRINCETON UNIVERSITY

December 21, 2023

Securing the Public Key Infrastructure Workshop Report

Executive Summary

The Public Key Infrastructure (PKI) on the internet enables the secure transmission of information across a range of industries such as commerce, banking, and healthcare. Stakeholders in this infrastructure include users, website operators, browsers, certification authorities, and content-delivery networks. But this system has weaknesses and interdependencies that can critically affect the resiliency and security of internet-based communications. In December 2022, CITP convened a small group of experts across the different stakeholder constituencies to discuss the challenges and opportunities for securing this critical infrastructure. We are already seeing results from our workshop; one technique we discussed, multi vantage domain validation, is becoming more widely implemented in the field. This report summarizes the key issues raised in the workshop and outlines directions for future research and collaboration.[1]

[1] Henry Birge-Lee, Grace Cimaszewski, Liang Wang, Klaudia Jaźwińska, Prateek Mittal, Mihir Kshirsagar, and Jen Rexford contributed to this report. This report is a product of CITP's Technology Policy Clinic, which provides nonpartisan research, analysis, and commentary to policy makers, industry participants, journalists, and the public. The workshop was sponsored by CITP and co-hosted with Let's Encrypt. We thank the participants listed in Appendix A for contributing their time and expertise.

A. Background on the Public Key Infrastructure

In the early days of the Internet, the main objective was to enable efficient communication among trusted parties. There were fewer well-established attacks on security and privacy, and a greater level of trust was placed in the networks that comprised the internet. As a result, less attention was given to ensuring that messages actually reached the intended recipients without being compromised along the way. But as the internet scaled up, this lack of attention introduced serious vulnerabilities for secure communications.

Bad actors, like foreign adversaries or cryptocurrency thieves, have a lot to gain by exploiting insecure communications. Such an actor might redirect internet traffic towards the wrong application server, causing unavailability; they might position themselves between the client and the application server to record unencrypted traffic; or they might impersonate legitimate servers. These attacks can have disastrous consequences when they could be leveraged to steal critical information like financial or medical data.

To prevent such attacks, engineers developed protocols that layer on top of the existing infrastructure to help mitigate the insecurity of the underlying system and build trust. One of these approaches is the use of cryptography to encrypt communications. **Public Key Infrastructure** (PKI)[2] is the umbrella term for the cryptographic algorithms, schemes, and protocols that work to secure end-to-end communications by verifying the integrity and authenticity of users and data. These protocols are used for encrypting the communication between client applications and servers, such as web browsers loading a website.

Public key certificates (or **digital certificates**) are a kind of license that proves the authenticity of an entity, such as a server. In the web PKI, digital certificates bind a domain name (e.g., www.example.com) to a public key (which can be used to encrypt data that only the corresponding private key holder/domain owner can decrypt). They are issued by Certificate Authorities (CAs) that are responsible for

[2] The Public Key Infrastructure (PKI) is a network security architecture that uses a combination of private and public key cryptography to enable security services such as data confidentiality, data integrity, and non-repudiation.

ensuring this binding is authentic. As a technical matter, the issuance of the certificate says nothing else about a site's content or who runs it. Specifically, the certificates do not include any information about a website's reputation or safety.

To obtain a digital certificate, a domain owner must first send a Certificate Signing Request to a CA. The CA then confirms that the entity submitting the request actually controls the domains covered by that request. This process, called domain control validation, ensures certificates are not incorrectly issued to adversaries that are posing as a domain they do not actually control.

B. Stakeholders

B.1. *Certification Authorities*

Certification Authorities (CAs) are organizations, companies or government agencies that issue certificates. In order to be included in the trust stores of browsers and operating systems, these organizations must undergo annual audits by third parties that ensure they are following rules regarding the proper vetting, issuance, and revocation of certificates.

B.2. *Browsers and Operating Systems*

Many browsers have associated "root programs" that maintain a definitive list of trusted CA certificates. This list, often referred to as a "**trust store**", is installed with every version of the browser. Usually a browser trust store is used for communication that originates from that browser. Some operating systems also have root programs, and an operating system trust store is used to validate the certificates of connections that originate outside of a browser (such as during an API call) or if the browser does not have a trust store. CAs can get added to a browser or operating system's trust store by applying to its root program and presenting third-party audits showing they follow the policies of that root program. This control over the list of acceptable CAs makes compliance with the regulations of major root programs essential to the operations of any publicly-trusted CA. While many root programs rely on the "Baseline Requirements" published by the CA/Browser Forum when determining whether to trust a CA, a root program

single-handedly has the authority to distrust a CA or select criteria required for inclusion in its trust store.

B.3. *CA/Browser Forum*

The CA/Browser (CAB) Forum is a voluntary group of CAs and certificate consumers that was organized in 2005 to serve as a hub to coordinate policies between certificate consumers (e.g., browser and OS vendors which contain trust stores) and certification authorities. It has become the de facto governance structure for accountability in the PKI system.

B.4. *Users*

The objective of the PKI is to protect users' communication via end-to-end (i.e., client to server) transport encryption. Even though users are the primary beneficiaries, they have little direct representation in the PKI ecosystem and their interests are often represented by browsers.

B.5. *Domain Owners*

Domain owners obtain certificates from CAs in order to secure their services with end-to-end encryption. Domain owners have a choice in which CA they use to obtain their certificates and can use this to exert an impact on the CA ecosystem.

B.6. *DNS Operators*

DNS Registrars and providers do not usually interact directly with PKI governance (i.e., the CAB Forum) but ultimately are indispensable to the function of the PKI. Not only do both browsers (when establishing a TLS connection) and CAs (when performing domain control validation) perform DNS lookups to find out information related to a domain, but DNS registrars maintain a business relationship with the authentic domain owners and can potentially serve as a source of ground truth. There are also several alternative ways DNS operators serve PKI-related information. Although largely unadopted in the web ecosystem [1], DNS-based Authentication of Named Entities (or DANE) provides information about TLS certificates to clients and Certificate Authority Authorization (or CAA)

records provide instructions for CAs when issuing certificates like specifying which CAs can issue a certificate for a given domain.

B.7. *CDN Providers*

Content Delivery Networks (CDNs) are also significant players in the PKI ecosystem. Many domain owners delegate the responsibility of delivering website content through CDN platforms (like Cloudflare) to optimize performance. Domain owners' requests for digital certificates from CAs are thus increasingly mediated through CDNs that serve corresponding content. Furthermore, some CDNs perform the process of requesting, validating, and deploying a certificate on a domain owner's behalf causing CDNs to develop business relations and interact directly with CAs.

C. Examples of PKI Vulnerabilities

There are many potential vulnerabilities that can compromise the PKI and thus the security of web traffic. There are two primary techniques for attacking the PKI: (a) compromising a CA's infrastructure and using it to sign malicious certificates, or (b) tricking a CA into issuing certificates to an adversary for a domain the adversary does not operate. Both of these techniques have been seen in the wild.

One potential way to trick a CA is by exploiting vulnerabilities in the Border Gateway Protocol (BGP). BGP is at the core of internet routing infrastructure.[3] At a high level, BGP acts like a postal service system for the internet. It is designed to find the routing path to travel from a sender (client) to recipient (application server). The design prioritizes efficiency.

Researchers have identified ways [2] in which network-level adversaries can manipulate BGP to intercept web traffic away from clients or certificate authorities in order to obtain bogus certificates from CAs, thereby allowing them to bypass cryptographic protection. An analysis of 1.8 million certificates found that the vast majority of domains – 72% – were vulnerable to attacks that would allow

[3] The purpose of the Border Gateway Protocol (BGP) is to exchange routing and reachability information among a series of smaller networks called autonomous systems (ASes). Each autonomous system is composed of a large pool of routers run by a single organization, such as AT&T or Verizon.

adversaries to obtain fraudulent certificates [3, 4] . These attacks pose serious security risks, and show the urgent need for practical defenses.

In 2022 two such attacks targeting cryptocurrencies were observed in the wild. The first was an attack on the Korean-based crypto exchange KLAYSwap where attackers used a BGP attack to target a javascript file loaded onto the KLAYSwap platform. The javascript file was loaded via HTTPS, and after the adversary launched its BGP attack, it approached the trusted certificate authority ZeroSSL and used its BGP attack to fraudulently pass domain control validation and obtain a trusted certificate for the domain serving the javascript file [5]. The second attack targeted the cryptocurrency service Celer Bridge and similarly used a BGP attack to obtain a malicious TLS certificate which was used to compromise the cryptocurrency app and route funds to the adversary [6].

In particular, foreign adversaries and "espionage actors" have the capabilities to disrupt the flow of information between clients and servers. By attacking the PKI, they can use compromised certificates to intercept HTTPS traffic [7]. Furthermore, bad actors might try to directly compromise CAs. For example, a recent *Washington Post* article detailed how a root authority called TrustCore had ties to a company that produced spyware for the US government [8]. Subsequently, major web browsers announced that they would stop trusting certificates from TrustCore [9].

Other examples of certificate authority failures

Certificate Authority	*Year*	*Description of failure*
Comodo	2011	Because Comodo trusted resellers to perform domain validation control instead of doing it themselves, an attacker who obtained the username and password of a Comodo Trusted Partner was able to issue fraudulent certificates for Mozilla, Google, Yahoo and other domains [10]
DigiNotar	2011	Anonymous attacker obtained access to all of DigiNotar's CA systems and

		created fake certificates for hundreds of websites to eavesdrop on email and web browsing in Iran; this ultimately resulted in DigiNotar's bankruptcy [11]
Symantec	2015	Symantec distrusted by all major platforms after willfully issuing test certificates without proper authorization of domain owners for several years [12]
GoDaddy	2018	Self-audit exposed a vulnerability in its code that would allow its validation controls to be bypassed [13]
MonPass	2021	Attackers "backdoored" a Mongolian certificate authority, allowing them to spread malware to users [14]
KLAYSwap	2022	Attackers launched a BGP attack to hijack internet traffic and spoof domain control validation which led to a misissued certificate that served malicious javascript and stole cryptocurrency [5]
Celer Bridge	2022	Attackers launched a BGP attack to hijack internet traffic and spoof domain control validation to obtain a misissued certificate which was used to served a malicious smart contract that transferred users' funds to the adversary [6]

D. Operational and Security Challenges in the PKI

Routing attacks against domain control validation:

Misissued fraudulent certificates could enable many attacks such as man-in-the-middle and phishing. To prevent fraudulent certificate issuance, CAs perform domain control validation to validate the ownership of domains during certificate issuance. Current domain control validation methods involve domain owners demonstrating control of network services running on a domain as a means of proving control of that domain. However, given that a domain owner may be requesting a certificate for the first time, domain control validation sometimes has to occur over unauthenticated channels (e.g., plaintext HTTP) which require trustworthy network forwarding. Current validation methods, like HTTP and DNS validation, are examples of domain control validation methods that are not protected cryptographically and can be forged. One security challenge for CAs, that has gained considerable attention in recent times, is that the adversary could leverage network attacks, particularly routing attacks, to fool domain control validation to obtain fraudulent certificates, as in the KLAYSwap attacks in 2022 [5].

While the proper function of the PKI is highly dependent on secure internet routing, there is relatively little conscious interaction between entities participating in the PKI ecosystem, e.g., root programs and CAs, and routing security. Root programs often deploy certificate stores in end-user software, which does not interact directly with internet routing. CAs typically purchase internet connectivity from datacenters or ISPs and are not directly responsible for (or capable of) maintaining routing security; only a handful of CAs actually operate their own BGP-speaking routers.

Nevertheless, improvements to routing security can translate to significant security benefits for CAs. One such improvement, the Resource Public Key Infrastructure (RPKI), creates a digitally-signed database of Route Origin Authorizations (or ROAs) that list which Autonomous Systems (or ASes) are authorized to announce which IP prefixes. This database can then be checked when a router is processing route updates in a process known as Route Origin Validation or ROV. Based on the result of ROV, routers can drop potentially malicious updates that violate the information contained in cryptographically-authenticated ROA records. RPKI has seen substantial deployment with roughly 40% of the routing table being covered by ROAs [15] and many major networks performing ROV [16]. The deployment of RPKI has a

substantial impact on the security of the PKI particularly against routing attacks on domain control validation [4].

Timely revocation of certificates:

Delays in revocation of compromised or expired certificates could give the adversary more time to exploit these invalid certificates. In addition, CAs must ensure that the status of certificates, whether through Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP), is regularly updated and distributed promptly; otherwise, invalid certificates can be used continually.

Mass revocation:

Mass revocation refers to the scenario where the CA must revoke ALL invalid certificates in a timely manner. This occurs in cases where the CA suffers a security compromise, realizes it has issued certificates with improper domain control validation, or discovers it has violated the CAB Forum Baseline Requirements[4]. This has a significant impact on the operations of a CA as in the unlikely event of such a compromise, a CA must have a mechanism for removing a potentially sufficient number of certificates and rapidly renewing them to prevent disruptions to secure websites that depend on TLS certificates.

Other challenges and PKI resiliency:

There are many other security challenges associated with CAs. The adversary may try to launch Distributed Denial of Service (DDoS) or network attacks to affect the availability and reachability of CAs; the private signing keys could be compromised via insider attacks or other software/hardware vulnerabilities; subordinate CAs could be less protected and easier to get compromised, which consequently could undermine the security of the entire chain of trust.

Today's PKI has a large degree of centralization with roughly six major CAs signing over 90% of all TLS certificates issued. Experiencing attacks or facing security breaches, these CAs could become a single point of failure and can potentially disable a substantial portion of the Internet. It is important to develop

[4] https://cabforum.org/baseline-requirements-documents/

technologies that help websites switch between CAs in case their current CA stops functioning.

Challenges facing Root Programs:

While CAs and root programs share some similar challenges (e.g., improving PKI resilience), root programs also have a distinct perspective on the PKI because they primarily care about the operations of the PKI as a whole as opposed to the operations of a single CA. One challenge facing root programs is the relatively slow rate of progress and technological improvements in the PKI industry. Even if some CAs are acting in a technologically progressive manner, there is a "long tail" of CAs that sign a small fraction of certificates but still present a weak link for an attacker to target. Adopting a new technology across the PKI industry requires not just support from the handful of major CAs, but support from the long tail that may have significantly fewer technological resources than the CAs which are operating at larger volumes. Thus the rate of new technology adoption in the industry can be slow as each new technology needs to be easily deployable even by smaller CAs before it can be adopted.

Another challenge root programs have is that they must decide whether or not to trust a CA based solely on 3rd-party evidence. CAs obtain an audit from an accredited auditor and present this audit along with other supporting information to root programs for inclusion. In this system, root programs do not directly inspect and verify the CAs that are ultimately included. This can cause concerns by root programs over insufficient audits and low transparency into CAs' operations.

E. Strategies to Mitigate Attacks on the PKI

We outline a number of proposed strategies (in various stages of implementation) that can help increase the security of the Web PKI.

E.1. *multiVA*

Recall that a BGP attack can redirect traffic away from the victim's webpage and cause plaintext traffic (which is required for domain control validation) to be

redirected to an adversary.[5] This adversary can then request a certificate containing the victim's domain and spoof the domain control validation challenge to trick the CA into signing the certificate even though the adversary does not have control over the victim's domain.

One potential countermeasure for these attacks is known as multiple vantage point domain control validation (or "multiVA"[6]). This measure validates the domain ownership from multiple vantage points spread across the Internet. MultiVA exploits the fact that many BGP attacks (particularly equally-specific BGP attacks) are localized to a portion of the Internet and do not affect the entire Internet. Thus, a CA's remote vantage points which are not affected by the adversary's attack can route to the victim's domain and realize the true victim domain has not completed the domain control validation challenge and block issuance.

This approach was proposed by Birge-Lee et al. in 2018 [2]. This strategy has been deployed by Let's Encrypt and Google Trust Services and has been shown to be effective at mitigating the effects of ethically-conducted real-world BGP attacks on domain control validation. In the workshop, several participants shared their firsthand experiences of implementing multiple vantage point domain control validation and how potential challenges were overcome.

There is potential for multiple vantage point domain control validation to be standardized by the CAB Forum. However, there are a number of concerns and questions for multiple vantage point domain control validation that must be addressed. Several are summarized in the following table.

Issue	*Concerns*	*Responses*
Audit requirements	If made mandatory, multiVA may add to the already arduous audit	multiVA may not be subject to audit

[5] At the workshop we witnessed a real-world demonstration of an ethically-launched BGP attack (i.e., attacking an IP prefix controlled by the party conducting the demo that was registered solely for the purpose of conducting this demonstration). The attack was capable of obtaining a certificate for a victim domain (created solely for the purpose of the demo which served no real network services) without actually having control of any of the victim's network infrastructure.
[6] Some other articles also refer to this technology as Multi-Perspective Domain Control Validation (MPDV) or Multi-Perspective Issuance Corroboration (MPIC).

	requirements that CAs face. This will also necessitate agreeing on a set of audit validation checks. Auditing the physical security of cloud infrastructure (an option for hosting vantage points) is also not feasible.	requirements because it strictly *makes issuance more restrictive*: remote validation points can only deny issuing a certificate. multiVA is front-facing and can be verified by a user -- simply request a certificate and record requests to your webserver.
Need for standardization	Need a clearer definition of what multiVA is: how many vantage points, and where? How is information from vantage points used to make an issuance decision (quorum policy)?	Public working groups (such as this workshop) can help kickstart dialogue to codify requirements for multiVA.
Security benefit	multiVA is a partial defense: it is not guaranteed to detect all BGP hijacks. The strength of multiVA is dependent on its implementation specifics. It is also hard to describe the extent of security gain that multiVA provides.	A formal definition of multiVA will provide a starting point from which security can be evaluated. The Princeton team is working on releasing software that will enable CAs to quantify the security for apples-to-apples comparison of multiVA deployments.
Implementation challenges and barrier to entry	Smaller CAs may lack the technical expertise and resources to build multiVA by themselves. multiVA is a weakest-link problem:	This underscores the importance of CAB forum acceptance of multiVA as a baseline requirement.

	if not all CAs use it, an attacker can choose a non-multiVA for his attack.	These smaller CAs can be considered when writing requirements; some public efforts to “open source” aspects of multiVA are underway and can lower the barrier to entry.

E.2. *Shortening Certificate Lifetimes*

This technique is beneficial for improving the security posture of the web PKI and the revocation process. If a certificate is valid for a short enough period (e.g., less than 10 days), there is a less pressing need for revocation procedures such as Online Certificate Status Protocol (OCSP) or Certificate Revocation Lists (CRLs), making automation processes easier. However, adopting certificate lifetime shortening requires new forms of thinking about disaster recovery, which may be challenging for CA operators. For example, if there is a total outage, there is a limited window of time to replace the certificate; if a certificate is only valid for ten days, then the renewal window is only about 3 days assuming that most people renew certs at the two-third point.

E.3. *ACME Client Fallback*

The Automatic Certificate Management Environment (ACME) protocol is a protocol for automatically managing certificate issuance and renewal, which has been widely adopted by CAs (e.g., Let’s Encrypt). With ACME client fallback, the client can switch to another ACME CA to get the cert if the original ACME CA goes down. This approach makes client configuration more complicated, e.g., how to select the set of CAs that the client is prepared to use as a backup and determine their priorities? This technique may also make CAA checking and billing more complicated.

E.4. *ACME CAA Extensions*

With the ACME CAA extensions [17] enabled, clients must establish CAA records, and CAs must verify these records during the domain ownership validation process. Despite its potential to greatly enhance security, this approach has yet to gain widespread adoption due to the additional efforts required from both parties.

E.5. *ACME Renewal Information*

ARI is a new extension to the ACME specification. This extension allows for the CA to specify the window of time during which a certificate should be renewed. ARI has several benefits. First, it provides peace of mind for site operators, as there is no loss of continuity of business during the renewal process. Second, it is ideal for short-lived certificates, as it shortens their lifetime by encouraging people to renew them faster. Third, it is advantageous for CA operators, as it encourages clients to renew their certificates faster, which can help in the event of a mass-revocation event. Finally, this new extension proactively smooths out the load over the next few months (e.g., 60 days) to avoid sudden renewal request spikes. One of the main challenges is getting ACME client authors to adopt it: the clients need to frequently check the CAs to get the most-recent, arranged renewal times, which requires software changes on a wide range of devices. Additionally, clients designed to be run routinely do not have control over when they wake up, which can further complicate the adoption process. Despite these challenges, the new extension to the ACME specification has the potential to greatly improve the certificate renewal process.

During the discussion, the participants outlined the key priorities for implementing the techniques. The foremost priority is to expand the deployment of ACME in order to encourage as many CAs and clients as possible to adopt it, and to facilitate further development of ACME clients. The second priority is to enable CAs to implement ARI. The third priority is to deploy ACME fallback, and a potential strategy to facilitate this is to create a community website that lists ACME-supporting CAs. Lastly, for shortened certificate lifetimes, a proposed approach to incentivize deployment is to incorporate it into the baseline requirements.

E.6. *F-PKI or Trust Flexibility*

The PKI is often considered too rigid due to the equal trust placed into a fixed set of CAs. Different users may have different trust views, such as highly trusting one CA over another. In the original Web PKI, it was difficult to express this trust. To address the issue that attacks could be detected but not prevented, a more flexible trust system called F-PKI [18] was developed. F-PKI allows users to blocklist CAs and achieve the property that they cannot be attacked by a less trusted CA, while ensuring that domains issued by the less trusted CA remain available. This is achieved through proof of absence, where, for example, "CA1 does not issue a certificate for D2." F-PKI also allows for trust preferences to be defined, such as highly trusting CAs using multi-vantage point ACME or CAs located in the user's own country. Additionally, domain-dependent trust can be established, such as highly trusting Google CAs for domains in Google Cloud or US CAs for US .gov domains. Overall, F-PKI provides a more flexible trust system that better suits the needs of our heterogeneous global society, but requires further research in how to overcome the associated deployment challenges

E.7. *Integration with Onion Services*

The traditional onion address in the Tor network is a long, random-looking string, which makes it challenging for users to associate it with a specific domain and ensure its accuracy. This issue renders onion sites vulnerable to phishing attacks. To address this problem, the sauteed onion certificate combines traditional and onion address formats to create Self-Authenticating Traditional Addresses (SATAs) [19]. A sauteed onion certificate is a TLS certificate for a domain that includes its onion address as a subdomain in SAN. The onion address resolution is based on CT logs, ensuring transparency and consistency. This approach enables users to resolve onion addresses without accessing the original sites, ensuring all users receive the same onion association, and enabling site owners to detect attacks on their sites. Sauteed onion certificates are incrementally deployable while offering enhanced security without requiring changes to existing internet PKI infrastructure, and forward authority-independent authentication/revocation. Sites with existing onion addresses can obtain sauteed onion certificates, and services and clients require only minor modifications to serve SATAs.

F. Workshop Outcome/Impact and Next Steps

One of our main goals for the workshop was to bring together stakeholders in this critical, interdependent infrastructure and have them work across different silos to tackle problems that affect the public interest. That approach has already started to bear fruit. After this workshop, many of the participants and other members of the PKI community grouped together and began a work team to formalize the details on how multiVA could be included in the CA and Browser Forum Baseline Requirements as an industry-wide standard [20]. Other proposals discussed at the workshop are also seeing implementation. Recent initiatives at the CA and Browser Forum incentivise the reduction of certificate lifespans [21] and ACME Extensions have been deployed by Let's Encrypt [22]. In these ways, the momentum gained at this workshop is helping to provide a more secure and more flexible PKI.

Appendix

A. List of Participants

Josh Aas, *Let's Encrypt/ISRG*
Maria Apostolaki, *Princeton University*
Henry Birge-Lee, *Princeton University*
Grace Cimaszewski, *Princeton University*
Robert Danford, *Salesforce*
Ryan Dickson, *Google*
Roger Dingledine, *The Tor Project*
Nick France, *Sectigo*
Aaron Gable, *Let's Encrypt/ISRG*
Sharon Goldberg, *BastionZero Inc.; Boston University*
Jeffrey Haas, *Juniper Networks*
Hamed Haddadi, *Brave Software* & *Imperial College London*
J. Alex Halderman, *University of Michigan*
Ryan Hurst, *Google*
Klaudia Jaźwińska, *Princeton University*
Mallory Knodel, *Center for Democracy & Technology*
Cyrill Krähenbühl, *ETH Zürich*
Mihir Kshirsagar, *Princeton University*
Doug Madory, *Kentik*
Prateek Mittal, *Princeton University*
Doug Montgomery, *NIST*
James Renken, *Let's Encrypt/ISR*G
Jen Rexford, *Princeton University*
John Sarapata, *Google*
Anees Shaikh, *Google*
Karina Sirota Goodley, *Microsoft*
Yixin Sun, *University of Virginia*
Paul Syverson, *U.S. Naval Research Lab (NRL)*
Wayne Thayer, *Fastly*
Liang Wang, *Princeton University*
Bas Westerbaan, *Cloudflare*

B. References

[1] Huque, Shumon. “Whither DANE?” https://indico.dns-oarc.net/event/31/contributions/707/attachments/682/1125/whither-dane.pdf

[2] Henry Birge-Lee, Yixin Sun, Anne Edmundson, Jennifer Rexford, and Prateek Mittal. “Bamboozling Certificate Authorities with BGP.” In USENIX Security ‘18. https://www.usenix.org/conference/usenixsecurity18/presentation/birge-lee

[3] Henry Birge-Lee, Liang Wang, Daniel McCarney, Roland Shoemaker, Jennifer Rexford, and Prateek Mittal. “Experiences Deploying Multi-Vantage-Point Domain Validation at Let's Encrypt.” In USENIX Security ‘21. https://www.usenix.org/conference/usenixsecurity21/presentation/birge-lee

[4] Grace Cimaszewski, Henry Birge-Lee, Liang Wang, Jennifer Rexford, and Prateek Mittal. “How Effective is Multiple-Vantage-Point Domain Control Validation?” In USENIX Security ‘23. https://www.usenix.org/conference/usenixsecurity23/presentation/cimaszewski

[5] Henry Birge-Lee, Liang Wang, Grace Cimaszewski, Jennifer Rexford, and Prateek Mittal. “Attackers exploit fundamental flaw in the web’s security to steal $2 million in cryptocurrency.” https://freedom-to-tinker.com/2022/03/09/attackers-exploit-fundamental-flaw-in-the-webs-security-to-steal-2-million-in-cryptocurrency/

[6] Peter Kacherginsky. “Celer Bridge incident analysis.” https://www.coinbase.com/blog/celer-bridge-incident-analysis

[7] Warren Mercer and Paul Rascagneres. “DNSpionage Campaign Targets Middle East.” https://blog.talosintelligence.com/dnspionage-campaign-targets-middle-east/

[8] “TrustCor Systems Verifies Web Addresses, but Its Address Is a UPS Store - The Washington Post.” https://www.washingtonpost.com/technology/2022/11/08/trustcor-internet-addresses-government-connections/.

[9] Menn, Joseph. “Web Browsers Drop Mysterious Company with Ties to U.S. Military Contractor.” *Washington Post*, December 1, 2022. https://www.washingtonpost.com/technology/2022/11/30/trustcor-internet-authority-mozilla/.

[10] Nightingale, Johnathan. “Comodo Certificate Issue – Follow Up.” Mozilla Security Blog. https://blog.mozilla.org/security/2011/03/25/comodo-certificate-issue-follow-up.
[11] Keizer, Gregg. “Hackers Spied on 300,000 Iranians Using Fake Google Certificate.” Computerworld, September 6, 2011. https://www.computerworld.com/article/2510951/hackers-spied-on-300-000-iranians-using-fake-google-certificate.html.
[12] Google Security Blog. “Sustaining Digital Certificate Security.” https://security.googleblog.com/2015/10/sustaining-digital-certificate-security.html
[13] “1484766 - GoDaddy: Random Value Vulnerability in Domain Validation.” https://bugzilla.mozilla.org/show_bug.cgi?id=1484766.
[14] The Record by Recorded Future. “Mongolian Certificate Authority Hacked Eight Times, Compromised with Malware,” July 1, 2021. https://therecord.media/mongolian-certificate-authority-hacked-eight-times-compromised-with-malware/.
[15] NIST. NIST RPKI Deployment Monitor. https://rpki-monitor.antd.nist.gov/
[16] Cloudflare. “Is BGP Safe Yet?” Monitor. https://isbgpsafeyet.com/
[17] H. Landau. “Internet Draft: CAA Record Extensions for Account URI and ACME Method Binding.” https://datatracker.ietf.org/doc/html/draft-ietf-acme-caa-06
[18] Laurent Chuat, Cyrill Krähenbühl, Prateek Mittal, and Adrian Perrig. “F-PKI: Enabling Innovation and Trust Flexibility in the HTTPS Public-Key Infrastructure.” NDSS Symposium 2022. https://www.ndss-symposium.org/wp-content/uploads/2022-241-paper.pdf
[19] Sauteed Onions. https://www.sauteed-onions.org/
[20] https://github.com/ryancdickson/staging/pull/6
[21] Let’s Encrypt Blog. “Shortening the Let's Encrypt Chain of Trust.” https://letsencrypt.org/2023/07/10/cross-sign-expiration.html
[21] The CA and Browser Forum. “Ballot SC-063 v4: Make OCSP Optional, Require CRLs, and Incentivize Automation.” https://cabforum.org/2023/07/14/ballot-sc-063-v4make-ocsp-optional-require-crls-and-incentivize-automation/
[22] Let’s Encrypt API Announcements. “Enabling ACME CAA Account and Method Binding.” https://community.letsencrypt.org/t/enabling-acme-caa-account-and-metho

d-binding/189588