Certificates-as-an-Insurance: Incentivizing Accountability in SSL/TLS

Stephanos Matsumoto
Carnegie Mellon University/ETH Zürich
smatsumoto@cmu.edu

Raphael M. Reischuk
ETH Zürich
reischuk@inf.ethz.ch

***Abstract*—We propose to leverage accountability mechanisms to deal with trust-related security incidents of certification authorities (CAs) in the SSL/TLS public-key infrastructure (PKI). We argue that, despite recent advances in securing certificate issuance and verification, the TLS PKI does not sufficiently incentivize careful identity verification by CAs during certificate issuance or provide CA accountability in the event of a certificate compromise. We propose a new paradigm, *Certificates-as-an-Insurance*, to hold CAs accountable for misbehavior by using insurance policies and benefits negotiated between the CA and the domain. In this positional paper, we only sketch an instantiation of our insurance model as an extension of the existing certification model and identify challenges for future research.**

I. Introduction

The authentication of web servers to clients is becoming an increasingly important problem in the current Internet. As the Internet becomes more integrated with everyday life in the developed world, questions of data privacy and user anonymity have become increasingly crucial. However, as the recent disclosures of global surveillance [1–7] have shown, attacking authentication is becoming the primary means to compromise users' privacy. Even the strongest authentication scheme cannot provide confidentiality if the user's communications are encrypted with the adversary's keys instead of the server's keys!

In part, these attacks against authentication have succeeded because today's authentication infrastructures are frighteningly fragile [8]. Compromises of certification authorities (CAs) have resulted in the issuance of unauthorized certificates for high-profile sites such as Google, Yahoo, and Skype (see Section II-B), enabling man-in-the-middle attacks to eavesdrop on or alter client-server communication.

Moreover, in such a fragile ecosystem where proper CA operation is critical to confidentiality, CAs lack incentives to take sufficient security measures [9]. While CAs should be in the business of verifying that a public key indeed belongs to a domain owner, some CAs fail to adequately verify this binding, resulting in the issuance of unauthorized public-key certificates.

In this paper, we ask "How can CAs be incentivized to more carefully ensure that a domain controls the key it claims to?" We observe that CAs are not held accountable to clients and domains in an enforceable way, and thus lack sufficient incentives to perform careful identity checks, in some cases even having a disincentive against thorough checks. We argue that the current authentication infrastructures have parties with greatly differing incentives and levels of power, further complicating the enforcement of accountability. To address these challenges, we then introduce Certificates-as-an-Insurance (CaaI), a new paradigm for increased, enforceable accountability.

II. Background

In this section, we provide a short background and overview of the current practices in the TLS PKI. We first briefly describe the history of SSL/TLS, contextualizing recent compromises and developments within a timeline. We then provide additional background on the CA attacks mentioned in Section I. We then discuss the practices of today's CAs, as well as recent proposals to improve the TLS PKI.

A. History of SSL/TLS

The Secure Sockets Layer protocol (SSL) is a cryptographic protocol developed by Netscape in 1994 (see Figure 1) to secure platform-independent communication between its browser (Netscape Communicator) and servers in the Internet. In 1999, SSL was standardized as Transport Layer Security (TLS) by the IETF [10]. Today, TLS is used to provide end-to-end encryption between users and sites such as those offering banking and other security-sensitive services.

In TLS, the client first performs an asymmetric key exchange with the server (using the server's public key) to set up a shared session key used to symmetrically encrypt client-server traffic. Using the public key of another party makes the client's encrypted session traffic vulnerable to MITM attacks. Furthermore, unless clients are also authenticated, the server has no means of detecting this kind of attack.

Certification Authorities (CAs) provide authenticity for TLS public keys by issuing digital certificates attesting that a given public key belongs to a particular domain name (Steps 1 and 2 in Figure 2a). Such certificates are digitally signed with the CA's private signing key and verified by browsers with the respective verification keys (Step 5 in Figure 2a), most of which are shipped with the browser or the underlying OS. The first and largest CA, Verisign, was founded shortly after SSL in April 1995 and has been operated by Symantec since 2010 with a market share of 35.5%[1].

[1] http://w3techs.com/technologies/overview/ssl_certificate/all

SENT '15, 8 February 2015, San Diego, CA, USA
Copyright 2015 Internet Society, ISBN 1-891562-39-8
http://dx.doi.org/10.14722/sent.2015.23009

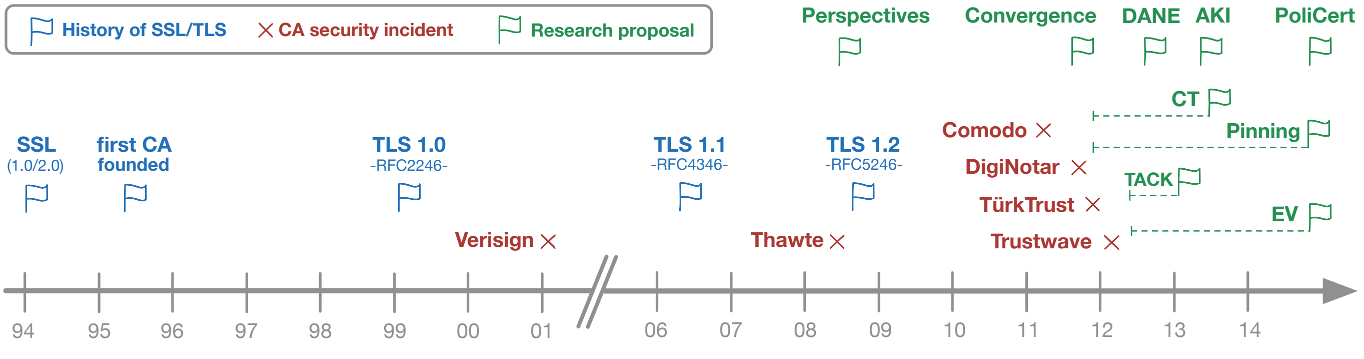

Fig. 1: Most significant events in the history of SSL/TLS.

B. CA Security Incidents

Security incidents at CAs have taken place almost since the beginning of TLS. In January 2001, Verisign mistakenly issued two certificates on behalf of Microsoft to an individual who claimed to be a Microsoft employee [11]. In 2008, a security researcher was able to obtain a rogue certificate for Microsoft's Live.com only by controlling `sslcertificates@live.com`, an address open to public registration [12].

CA mistakes and compromises consist of more than social engineering attacks, however. Others have used MD5 hash collisions to obtain a CA signing certificate authorizing the holder to issue certificates for any site in the Internet [13]. Hackers thought to originate from Iran gained access to a user account of a Comodo reseller, resulting in 9 fraudulent certificates being issued for high-profile sites such as Google, Yahoo, and Skype [14, 15]. An attack on the DigiNotar led to more than 200 rogue certificates being issued [16], and eventually ended in the CA declaring bankruptcy [17].

Some security incidents have shown that CA systems do not need to be breached at all. For example, in early 2012, Trustwave admitted to issuing a CA signing certificate to one of its corporate customers, allowing the customer to eavesdrop on all communications (even HTTPS) from its internal network [18]. In 2012, TürkTrust mistakenly issued two CA signing certificates instead of end-entity certificates (which cannot issue further certificates), allowing the holders to issue rogue certificates for Google [19].

C. Recent Proposals

We review a number of proposals to increase the reliability of the SSL/TLS PKI, most of which were published after the Comodo incident (see Figure 1). Most of these proposals focus on detecting CA misbehavior and making it more difficult for a misbehaving CA to forge a valid certificate.

Perspectives [20], **Convergence** [21], and **TACK** [22] are proposals dating between 2008 and 2013 based on *network perspective*, which allow users to validate a domain's public key based on other entities' view of the domain's key. In these proposals, CAs are not necessary at all if we assume that a majority of the entities tracking a domain's public key do not observe a compromised key. Users can select which entities' perspectives in the network they trust to authenticate a domain's public key and can change this decision at any time, a property called *trust agility* [23].

DANE [24], proposed in August 2012, leverages the DNS infrastructure to safeguard certificates against malicious replacement. More precisely, instead of letting a CA sign a certificate for a domain, the DNS's security extensions (DNSSEC) binds the domain's public keys directly to the corresponding DNS names. A domain hence shifts the trust from the *various* CAs to the DNS system by creating a *single* DNSSEC entry for that domain. DANE additionally allows for the direct specification of domain policies, i.e., a domain specifies permissible CAs that are allowed to issue certificates for that domain.
While DANE's primary goal is to address the SSL/TLS PKI's oligarchy problem, DANE still suffers from the dependency of DNSSEC: a compromised DNSSEC key could be used to specify arbitrary policies and could thus bind any public key to any domain. In such a case, DANE does not provide any means for holding sloppy CAs accountable, nor does DANE incentivize CAs to perform careful certification.

Certificate Transparency (CT) [25], **AKI** [26], and **PoliCert** [27] are examples of *log-based proposals*, which publicly log certificates or CA operations in an append-only database maintained by *log servers*. Log-based proposals additionally require proof that a certificate has been logged for it to be considered valid, and domains may also be able to specify policies governing key loss/compromise or certificate usage. Thus a CA forging a domain's certificate can easily be exposed by the log proof of the forged certificate. While these proposals provide increased security and enable detection of misbehaving CAs, they do not address the specifics of enforcing CA accountability, nor do they offer incentives for CAs to perform more careful checks. These proposals also may not specify how log servers themselves are held accountable to clients and domains.

Public-Key Pinning [28], first proposed in November 2011, recently revised in October 2014, and implemented in Firefox 32[2], is similar to PoliCert in that it allows domains to specify constraints on the CAs and on the certificates. Accountability, however, is not a goal.

Extended Validation (EV) Certificates [29] indicate that a CA performed a stricter set of checks to ensure that the recipient of an issued certificate is indeed the domain it claims to be. EV certificates require strict identity verification procedures, including a face-to-face meeting. However, the guidelines for issuing EV certificates are not a technical part

[2] https://wiki.mozilla.org/SecurityEngineering/Public_Key_Pinning

of the PKI system and thus cannot be enforced from within the PKI itself. Furthermore, it is impossible to verify whether a CA issuing EV certificates is actually following these guidelines. Therefore, a compromised CA can still issue an EV certificate for whatever entity it chooses regardless of whether or not it carries out the required checks.

III. Shortcomings in Accountability

In this section, we argue that CA accountability is highly lacking in the current PKI. In particular, based on the current practices discussed in Section II, we argue that CAs today are not held sufficiently accountable, that the business model of CAs even provides economic *disincentives* against accountability and proper behavior, and that the differing interests and incentives of each party in the TLS infrastructure have created a PKI in which accountability cannot be properly enforced.

A. Lack of Enforceable Accountability

One common shortcoming of the previously proposed schemes to improve the TLS PKI is a lack of focus on enforcing CA accountability. The schemes of Section II focus on ensuring that no entity can obtain a valid certificate for a domain it does not control (step 2 in Figure 2a), and that users can successfully verify a legitimately-obtained certificate and detect the use of all unauthorized certificates (step 5 in Figure 2a). However, once misbehavior is detected by a client (or any other party that can fetch and verify a domain's certificate), it is difficult to enforce accountability on CAs.

Browser vendors (hereafter simply referred to as "browsers"), for example, cannot effectively enforce accountability for CAs. The top three CAs (Symantec Group, Comodo, and GlobalSign) capture over 75%[1] of the TLS certificate market share, leading to CAs that are "too big to fail" — browsers cannot remove their root certificates without cutting off access to a large fraction of HTTPS sites [30]. Thus, since browsers control in part the set of root CAs used, they are forced to trade off between enabling access to HTTPS sites (completeness) and ensuring that connections to HTTPS sites remain secure (soundness). This tradeoff results in conflicting incentives for browsers, who are primarily in the business of enabling Web access to their users and must choose between maintaining broad access to HTTPS sites (possibly compromised ones) and ensuring the authenticity of connections to those sites.

In addition to browsers, *users* and *domains* also have a difficult time enforcing CA accountability because some CAs explicitly disclaim liability for damages to the domain resulting from compromises in their license agreements [31]. Such a disclaimer also makes it difficult for out-of-band parties such as judicial courts to enforce accountability in the case of CA misbehavior. The use of these disclaimers reveals that CAs are aware of, and trying to avoid, the liability they face in the wake of operational mistakes and compromises. While this behavior is standard in the legal realm (and intended in part to protect CAs against frivolous lawsuits), requiring such clauses for parties that rely heavily on CA services (such as online shops, banks, and social networks) contributes towards a lack of enforceable accountability in the TLS PKI.

B. Imbalance of Control and Liability

Today's PKI suffers from an additional weakness: parties that wield the most control carry little of the liability for a compromise. CAs, on the one hand, wield the power to sign public-key certificates and are thus essential to the TLS PKI; browsers, on the other hand, select the root CAs that are trusted for TLS connection establishment, giving both of these parties a great deal of control over the TLS ecosystem. However, MITM attacks affect communication between the client and domain, who possess comparatively little control over TLS. Additionally, due to the liability disclaimer included in many CAs' license agreements, CAs transfer most of their liability to domains, causing clients and domains to hold most of the liability while the CAs and browsers hold much of the control.

This imbalance of control and liability can be illustrated with a simple real-life example. Suppose that a scammer obtains a forged medical license for a real doctor and begins practicing medicine in the doctor's name. If a patient dies due to the scammer's medical incompetence, it would be preposterous to prosecute the doctor whose credentials were forged. On the other hand, the organization that issued the license, as well as the governmental organization that approved the license as a requirement for practicing medicine, have much of the control in this system (since they can issue the license or determine who is authorized to issue such licenses) and very little of the liability — it is the patient (client) and the doctor (server) that suffer when a malicious party masquerades using a fake medical license (certificate).

C. Disincentives for Accountability

CAs also have a strong *disincentive* against more accountability. For example, when CA breaches come to light, they often result in the loss of reputation and business for the compromised CA [32], which in the case of DigiNotar even led to bankruptcy [17]. Therefore, CAs have an incentive *not* to disclose compromises, and indeed, DigiNotar failed to report the compromise until several months later [33, 34].

Asghari et al. have recently shown that certificates are often marketed not by price, but by bundled services, such as technical support and management [32]. Some CAs advertise speedy issuance of certificates, sometimes as fast as on the order of hours for EV certificates. Such advertisements indicate an economic disincentive for CAs to carefully check the identities of those requesting certificates. After all, the CA gets paid regardless of whether or not the certificate is correct. Some certificates are even sold with warranties, in which the CA pays out to users (but not domains) who fall victim to fraud from use of the certificate. Not only are such warranties difficult to enforce, most users are unaware of them. However, such services are used as a basis for competition, providing an economic incentive that adds to the murkiness of CA accountability.

IV. Research Questions

In this section, we identify several important areas of future research, based on the problems of Section III. Specifically, we discuss enforceable CA accountability, collocated control and liability, and incentives for trustworthy CA behavior. For each area, we identify the main challenges as well as related work that has attempted to address these challenges.

Attacker model. We assume an attacker model as depicted in Figure 2b: The 3-party scenario contains a single adversary whose goal is to impersonate another domain. The adversary is able to obtain an unauthorized public-key certificate for a

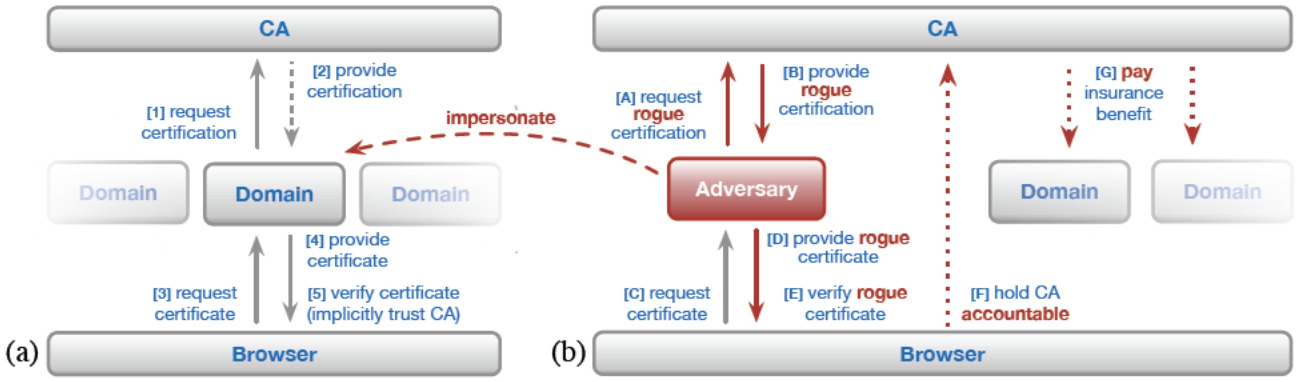
CA
[2] provide certification
[1] request certification
impersonate
Domain
Domain
Domain
[4] provide certificate
[3] request certificate
[5] verify certificate (implicitly trust CA)
(a)
Browser
CA
[A] request rogue certification
[B] provide rogue certification
[G] pay insurance benefit
Adversary
Domain
Domain
[D] provide rogue certificate
[C] request certificate
[E] verify rogue certificate
[F] hold CA accountable
(b)
Browser

Fig. 2: Standard 3-party certification model (a) in comparison to our extended insurance model (b).

domain from a CA, whether by exploiting a CA mistake or by colluding with a malicious CA.

A. Enforceable CA Accountability

One important problem to solve in TLS is providing a mechanism to *efficiently and effectively enforce accountability* when a CA misbehaves. Accountability may be enforced by revoking the forged certificate or the CA's signing key, or by some out-of-band mechanism such as financial penalties or loss of business reputation. However, both of these mechanisms come with their own drawbacks.

– Revoking a compromised certificate is a well-explored challenge, and prior work has proposed maintaining a list or database of revoked certificates [35, 36] or of currently valid certificates [26, 27, 37], as well as checking revocation status via a third party [38]. If instead the CA's signing key is revoked, there is a high probability of "collateral damage" in which valid, unauthorized domain certificates signed by the revoked CA become invalid. Some CAs sign hundreds of thousands of certificates [39], and revoking the keys of these CAs can cause massive collateral damage.

– Out-of-band solutions cannot always be efficiently automated, and the difficulty or delay of enforcing accountability manually can provide disincentives against carrying out the enforcement. For example, suing a CA to claim damages resulting from the use of a compromised certificate would require a legal team and would likely take on the order of months until damages can be paid. This process is further complicated by the fact that CAs operate all over the world, covering more than 50 countries' jurisdictions according to the EFF's SSL Observatory project [40]. These difficulties notwithstanding, we note that out-of-band regulatory mechanisms can complement in-band solutions [7].

B. Collocated Control and Liability

Control and liability can be better balanced in the TLS PKI by either transferring more control from CAs and browsers to domains and clients, or by transferring the liability of domains and clients to CAs and browsers.

– Transferring control from CAs and browsers to domains and clients can be achieved by providing domains and clients with the ability to specify trusted CAs or to add external mechanisms for verifying identity, as in network perspective-based proposals. However, the trust agility provided by network perspective is client-focused and can unnecessarily restrict domains. Conflicts among various perspectives may be difficult to resolve if a domain uses multiple public keys concurrently, as only the domain knows which public keys are actually authentic, and the average user likely cannot select the correct key based on the perspectives alone.

– Transferring liability from domains and clients to CAs and browsers has proved a difficult challenge due to the economic model under which the TLS PKI operates. Enforcement of liability is problematic, particularly for clients, since quantifying the value of clients' financial losses is often difficult, and it is unrealistic to expect CAs to pay out to all clients of a compromised domain.

C. Incentives for Trustworthy Behavior

We observe that the current PKI needs to better incentivize trustworthy behavior and accountability in CAs. In particular, the TLS PKI should provide incentives for CAs to act in a more trustworthy manner, carefully verifying identity and voluntarily holding themselves accountable. We note that being able to enforce CA accountability and collocating control and liability would provide strong incentives to encourage security-conscious CA operation.

We envision that the most effective incentives will be economic. CAs should face disincentives against improperly checking a requester's identity and against failing to report breaches, rather than being incentivized to market certificates with other services and to conceal breaches. Additionally, CAs should be offered greater incentives to more carefully verify a domain's identity, such as when issuing an EV certificate. Such a tiered incentive system could cause the PKI to become better integrated with a system of trust levels such as those in PGP [41], rather than differentiating certificates primarily in the user interface as EV certificates are today.

V. Certificates-as-an-Insurance

In this section, we present our proposed model, called *Certificates-as-an-Insurance* (CaaI), that addresses the open problems of the previous section. We first provide a brief overview, and then describe remaining details of our model that pose further research challenges.

A. Overview

The main idea of Certificates-as-an-Insurance is to *build accountability enforcement directly into the PKI*. In particular, we want to *automate* the detection of CA misbehavior and the subsequent responses to the misbehavior. Achieving this goal requires us to solve several important challenges:

1) expressing insurance policies able to cover a variety of certificate compromises, including those that might lead to MITM attacks against client-domain communication,
2) designing enforceable insurance benefits that incentivize proper CA behavior, and
3) using non-repudiable, signed statements to prove CA misbehavior and trigger payout of the insurance benefits, ideally automatically.

To address these challenges, we extend today's certification model (Figure 2a) to an insurance model (Figure 2b). In particular, we add two additional steps to the current certification model: holding a sloppy CA accountable [F] and paying the insurance benefits to its clients [G]. Our proposed model allows CAs and domains to negotiate an insurance policy that covers the issuance of unauthorized public-key certificates due to such causes as operational mistakes or CA compromises. The benefits paid to the domain may be financial, or may require the CA to publicly disclose the event.

We argue that this CaaI model addresses each of the previously discussed research problems. In particular, automatically triggering a payout of insurance benefits would achieve efficiently enforceable accountability. Well-negotiated policies would minimize collateral damage to both CAs and to domains. Making CAs become insurers would transfer some liability to CAs, who have a great deal of control in the TLS PKI. In addition to collocating control and liability, the insurance model would also create an extra business for CAs, thus incentivizing them to more carefully verify domains and quantify their risk of compromise.

Given that many recent proposals have focused on detecting and proving misbehavior, we propose to develop a mechanism that uses such proof of misbehavior to determine whether or not the compromise is covered by the insurance policy and trigger the insurance benefits if the incident is covered. Ideally, detection, coverage checking, and payout of benefits should be *automatic* and the enforcement should not depend on additional parties in the infrastructure.

The idea of using insurance for authentication has been proposed before [42, 43] as a way of helping users evaluate the trustworthiness of certificates; however, more recent work has moved towards analyzing insurance as an incentive for clients and domains rather than CAs to invest more resources in security [44, 45]. Some of these proposals also suggest that misbehaving CAs pay verifying end-users who are affected by an unauthorized certificate. However, there several major logistical problems arise: first, while users with an high-value account on the domain are clearly affected by a forged certificate, it can be difficult to determine users who are simply visiting a site. Second, users themselves are required to pay an insurance premium to be commercially viable, which is an unrealistic expectation given the huge numbers of diverse users for the most popular sites.

B. Remaining Challenges

Our model, as outlined above, can enhance the current TLS PKI with additional important properties and benefits. However, while the high-level idea of Certificates-as-an-Insurance is promising, the devil is in the details. We therefore identify several concrete questions regarding specific details of CaaI required to bring our proposal to fruition, particularly with respect to the challenges we identify above. We propose these questions to the community as motivation for further research.

The first challenge concerns the *negotiation and expression of insurance policies*. What kinds of compromises should be covered by CAs? Should higher-quality certificates (such as EV) correspond to higher benefits and/or higher premiums? What information should be visible to domains and CAs during the negotiation process, and what policy information should be visible to clients? How can these policies be expressed within the infrastructure so they can be efficiently verified?

Another challenge lies with *proving CA misbehavior*. In particular, we observe some challenges not addressed by previous work as described in Section II-C: does a certificate suffice as evidence of CA misbehavior, and should a proof of misbehavior be solely cryptographic or also rely on out-of-band information? What parties can verify a proof of misbehavior, and what criteria (e.g. majority agreement, specific verifiers) should be required to convincingly prove that a CA has misbehaved? How can false positives be minimized?

Enforcing insurance benefits poses a further challenge. What insurance benefits can be enforced, and by whom? Which benefits provide the most effective incentives for CAs to behave in a more trustworthy manner? Should enforcement occur in-band, out-of-band, or in combination? What additional parties are required to enforce benefits, if any? How would the compromise of the private key used to sign an insurance policy affect enforcement? How would economic issues (such as CA bankruptcy and long-term damages) be taken into account?

Finally, we also consider the challenges of *deploying CaaI*. What incentives can we offer browsers to adapt to this new model? How much deployment is necessary to begin reaping the benefits of CaaI? In what ways can we leverage the existing infrastructure, and what additional infrastructure, if any, is necessary for the deployment? Furthermore, legal and jurisdictional concerns also present challenges for deployment and enforcement, as described in the previous paragraph.

VI. Conclusions

In this positional paper, we have shown that accountability mechanisms for CAs are lacking, despite CAs' critical role in the TLS PKI. Worse yet, few incentives exist for CAs to behave in a security-conscious manner. We have therefore proposed a 3-party insurance model that provides a promising solution to deal with security incidents of certification authorities: after a CA has been compromised or has issued rogue certificates, the CA's customers receive some insurance benefits such as financial compensation or public disclosure of the CA's misbehavior. Though increased accountability achieved through our model would incentivize CAs to perform more careful checks when issuing certificates, many challenges still remain. We encourage the community to tackle these challenges in order to provide accountability in what is arguably the most important protocol for secure communication in the Internet.

References

[1] B. Gellman and L. Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," http://www.washingtonpost.com/investigations/us-intelligence-mining-

data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html, Jun. 2013.

[2] G. Greenwald and S. Ackerman, "How the NSA is still harvesting your online data," http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection, Jun. 2013.

[3] J. Borger, "GCHQ and European spy agencies worked together on mass surveillance," http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden, Nov. 2013.

[4] G. Weston, G. Greenwald, and R. Gallagher, "Snowden document shows Canada set up spy posts for NSA," http://www.cbc.ca/news/politics/snowden-document-shows-canada-set-up-spy-posts-for-nsa-1.2456886, Dec. 2013.

[5] J. Cremer, "Denmark is one of the NSA's '9-eyes'," http://cphpost.dk/news/denmark-is-one-of-the-nsas-9-eyes.7611.html, Nov. 2013.

[6] J. Biggs, "Regin spying software has been attacking governments and corporations since 2008," http://techcrunch.com/2014/11/24/regin-spying/, Nov. 2014.

[7] A. Arnbak, H. Asghari, M. V. Eeten, and N. V. Eijk, "Security collapse in the HTTPS market," *Comm. of the ACM*, vol. 57, no. 10, Oct. 2014.

[8] J. Clark and P. C. van Oorschot, "SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements," in *Oakland '13: IEEE Symp. on Security and Privacy*, May 2013.

[9] N. Gruschka, L. L. Iacono, and C. Sorge, "Analysis of the current state in website certificate validation," *Security and Communication Networks*, vol. 7, no. 5, Jul. 2013.

[10] T. Dierks and C. Allen, "The TLS procotol, version 1.0," RFC 2246, Internet Engineering Task Force, Jan. 1999. [Online]. Available: http://www.ietf.org/rfc/rfc2246.txt

[11] Microsoft, "Erroneous verisign-issued digital certificates pose spoofing hazard," https://technet.microsoft.com/library/security/ms01-017, Mar. 2001.

[12] M. Zusman and A. Sotirov, "Sub-prime PKI: Attacking extended validation SSL," *Black Hat Security Briefings, Las Vegas, USA*, 2009.

[13] M. Stevens, A. Sotirov, J. Appelbaum, A. Lenstra, D. Molnar, D. A. Osvik, and B. De Weger, "Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate," in *CRYPTO '09*, 2009.

[14] E. Mills and D. McCullagh, "Google, Yahoo, Skype targeted in attack linked to Iran," http://www.cnet.com/news/google-yahoo-skype-targeted-in-attack-linked-to-iran/, Mar. 2011.

[15] "Comodo fraud incident 2011-03-23," https://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html, Mar. 2011.

[16] H. Hoogstraaten, R. Prins, D. Niggebrugge, D. Heppener, F. Groenewegen, J. Wettink, K. Strooy, P. Arends, P. Pols, R. Kouprie, S. Moorrees, X. van Pelt, and Y. Z. Hu, "Black Tulip: Report of the investigation into the DigiNotar certificate authority breach," www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf, Aug. 2012.

[17] "VASCO announces bankruptcy filing by DigiNotar B.V." https://www.vasco.com/company/about_vasco/press_room/news_archive/2011/news_vasco_announces_bankruptcy_filing_by_diginotar_bv.aspx, Sep. 2011.

[18] N. Percoco, "Clarifying the Trustwave CA policy update," http://blog.spiderlabs.com/2012/02/clarifying-the-trustwave-ca-policy-update.html, Feb. 2012.

[19] A. Langley, "Enhancing digital certificate security," http://googleonlinesecurity.blogspot.ch/2013/01/enhancing-digital-certificate-security.html, Jan. 2013.

[20] D. Wendlandt, D. G. Andersen, and A. Perrig, "Perspectives: Improving SSH-style host authentication with multi-path probing," in *USENIX Annual Technical Conference*, Jun. 2008.

[21] M. Marlinspike, "SSL and the future of authenticity," http://www.youtube.com/watch?v=Z7Wl2FW2TcA, BlackHat 2011., Aug. 2011.

[22] M. Marlinspike and T. Perrin, "Trust assertions for certificate keys," https://tools.ietf.org/html/draft-perrin-tls-tack-02, (work in progress), Jan. 2013.

[23] M. Marlinspike, "SSL and the future of authenticity," http://www.thoughtcrime.org/blog/ssl-and-the-future-of-authenticity, Apr. 2011.

[24] P. Hoffman and J. Schlyter, "The DNS-based authentication of named entities (DANE) transport layer security (TLS) protocol: TLSA," RFC 6698, Internet Engineering Task Force, Aug. 2012. [Online]. Available: http://www.ietf.org/rfc/rfc6698.txt

[25] B. Laurie, A. Langley, and E. Kasper, "Certificate transparency," https://tools.ietf.org/html/rfc6962, Jun. 2013.

[26] T. H.-J. Kim, L.-S. Huang, A. Perrig, C. Jackson, and V. Gligor, "Accountable key infrastructure (AKI): A proposal for a public-key validation infrastructure," in *Proceedings of the 22nd international conference on World Wide Web*, May 2013.

[27] P. Szalachowski, S. Matsumoto, and A. Perrig, "PoliCert: Secure and flexible TLS certificate management," in *CCS '14: ACM Conference on Computer and Communications Security*, Nov. 2014.

[28] E. Evans, C. Palmer, and R. Sleevi, "Public key pinning extension for HTTP draft-ietf-websec-key-pinning-21," http://tools.ietf.org/html/draft-ietf-websec-key-pinning-21, Oct. 2014.

[29] C. Forum, "Guidelines for the issuance and management of extended validation certificates (v. 1.5.2)," https://cabforum.org/wp-content/uploads/EV-V1_5_2Libre.pdf, Oct. 2014.

[30] ENISA, "Operation black tulip: Certificate authorities lose authority," http://www.enisa.europa.eu/media/news-items/operation-black-tulip, Dec. 2011.

[31] N. Vratonjic, J. Freudiger, V. Bindschaedler, and J.-P. Hubaux, "The inconvenient truth about web certificates," in *Economics of Information Security and Privacy III*, 2013.

[32] H. Asghari, M. J. Van Eeten, A. M. Arnbak, and N. A. van Eijk, "Security economics in the HTTPS value chain," in *Proceedings of the Twelfth Workshop on the Economics of Information Security (WEIS 2013)*, Nov. 2013.

[33] J. Nightingale, "DigiNotar removal follow up," https://blog.mozilla.org/security/2011/09/02/diginotar-removal-follow-up/, Sep. 2011.

[34] "Operation Black Tulip: Certificate authorities lose authority," https://www.enisa.europa.eu/media/news-items/operation-black-tulip, 2011.

[35] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and T. Polk, "Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile," https://tools.ietf.org/html/rfc5280, 2008.

[36] A. Langley, "Revocation checking and Chrome's CRL," https://www.imperialviolet.org/2012/02/05/crlsets.html, Feb. 2012.

[37] M. D. Ryan, "Enhanced certificate transparency and end-to-end encrypted mail," in *NDSS '14*, Feb. 2014.

[38] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X.509 Internet public key infrastructure online certificate status protocol - OCSP," https://tools.ietf.org/html/rfc6960, Jun. 2013.

[39] P. Eckersley and J. Burns, "An observatory for the SSLiverse," https://www.eff.org/files/defconssliverse.pdf, Jul. 2010.

[40] ——, "Is the SSLiverse a safe place?" https://www.eff.org/files/ccc2010.pdf, Dec. 2010.

[41] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer, "OpenPGP message format," https://tools.ietf.org/html/rfc4880, 2007.

[42] C. Lai, G. Medvinsky, and B. C. Neuman, "Endorsements, licensing, and insurance for distributed system services," in *CCS '94*, Nov. 1994.

[43] M. K. Reiter and S. G. Stubblebine, "Authentication metric analysis and design," *ACM Transactions on Information and System Security*, vol. 2, no. 2, May 1999.

[44] M. Lelarge and J. Bolot, "Economic incentives to increase security in the Internet: The case for insurance," in *IEEE INFOCOM 2009*, 2009.

[45] N. Shetty, G. Schwartz, M. Felegyhazi, and J. Walrand, "Competitive cyber-insurance and Internet security," in *Economics of Information Security and Privacy*, 2010.