acmqueue

Security Collapse in the HTTPS Market

Assessing legal and technical solutions to secure HTTPS

Axel Arnbak, University of Amsterdam
Hadi Asghari, Delft University of Technology
Michel van Eeten, Delft University of Technology
Nico van Eijk, University of Amsterdam

HTTPS (Hypertext Transfer Protocol Secure) has evolved into the de facto standard for secure Web browsing. Through the certificate-based authentication protocol, Web services and Internet users first authenticate one another ("shake hands") using a TLS/SSL certificate, encrypt Web communications end-to-end, and show a padlock in the browser to signal that a communication is secure. In recent years, HTTPS has become an essential technology to protect social, political, and economic activities online.

At the same time, widely reported security incidents—such as DigiNotar's breach, Apple's #gotofail, and OpenSSL's Heartbleed—have exposed systemic security vulnerabilities of HTTPS to a global audience. The Edward Snowden revelations—notably around operation BULLRUN, MUSCULAR, and the lesser-known FLYING PIG program to query certificate metadata on a dragnet scale—have driven the point home that HTTPS is both a major target of government hacking and eavesdropping, as well as an effective measure against dragnet content surveillance when Internet traffic traverses global networks. HTTPS, in short, is an absolutely critical but fundamentally flawed cybersecurity technology.

While the Heartbleed incident illuminated severe flaws in a widely used crypto-library of HTTPS (OpenSSL), the focus here is on the systemic security vulnerabilities in the HTTPS authentication model that precedes end-to-end encryption. Although some of these vulnerabilities have been known for years, the 2011 security breach at the small Dutch CA (certificate authority) known as DigiNotar was a watershed moment, demonstrating these theoretical man-in-the-middle vulnerabilities in the wild. Meanwhile, large CAs such as Comodo and Verisign have experienced breaches as well but didn't suffer similar consequences to DigiNotar. In fact, some large CAs actually *benefited* from the increased sense of HTTPS insecurity.

Policymakers and technologists are increasingly advocating various solutions to address the security collapse of HTTPS. The European Union is halfway through adopting the world's first comprehensive legislation on HTTPS. It will acquire immediate binding force in the legal systems of 28 European member states. As most large CAs operate (also) under E.U. jurisdiction, the legislation will impact HTTPS governance globally. In the U.S., on the other hand, attention has focused on technological solutions and industry self-regulation.

To evaluate both legal and technological solutions, an understanding of the economic incentives of the stakeholders in the HTTPS ecosystem, most notably the CAs, is essential.[2,3] This article outlines the systemic vulnerabilities of HTTPS, maps the thriving market for certificates, and analyzes the suggested regulatory and technological solutions on both sides of the Atlantic. The findings show existing yet surprising market patterns and perverse incentives: not unlike the financial sector, the HTTPS market is full of information asymmetries and negative externalities, as a handful of CAs dominate the market and have become "too big to fail." Unfortunately, the proposed E.U. legislation will reinforce systemic vulnerabilities, and the proposed technological solutions are far from being adopted at scale. The systemic vulnerabilities in this crucial technology are likely to persist for years to come.

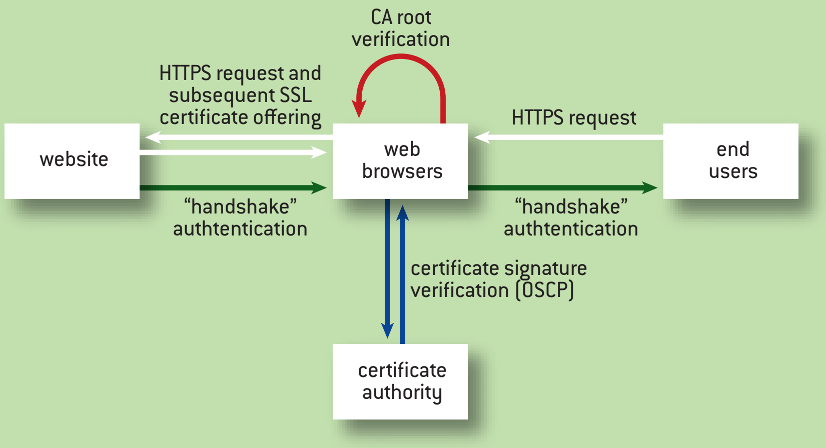
SYSTEMIC VULNERABILITIES IN THE HTTPS AUTHENTICATION MODEL

Essentially, HTTPS is a two-step process. First, a trust relationship (a handshake) is established between a Web site and an end user's browser. This is done with the help of a TLS/SSL (Transport Layer Security/Secure Sockets Layer) certificate containing basic information for authentication purposes. If the Web browser trusts the certificate and the issuing CA, then this authentication handshake succeeds. Second, successful authentication leads to a TLS/SSL-encrypted channel between the Web site and browser, called a *tunnel*.[1] Thus, the handshake authentication serves as the stepping stone for the confidentiality and integrity that HTTPS seeks to deliver. If the handshake succeeds, then the browser informs the user by, for example, depicting a padlock or a green address bar. If the TLS/SSL certificate or the issuing CA cannot be trusted, then the browser will show a security warning to the end user. The described data flows are shown in figure 1.

A Web site that wants to provide HTTPS communications to users needs to obtain a TLS/SSL certificate from a CA. Basically, these certificates are small computer files that contain information on hostname (Web site), certificate owner (Web-site owner), certificate issuer (CA), validity period, and public key.[1] The method for verification of the identity of a Web-site owner, among others, drives the costs of a certificate and is the key difference between DV (domain validated), OV (organization validated), and EV (extended validation) certificates.[2]

FIGURE 1

HTTPS Authentication Data Flows


CA root verification
HTTPS request and subsequent SSL certificate offering
HTTPS request
website
web browsers
end users
"handshake" authtentication
"handshake" authtentication
certificate signature verification (OSCP)
certificate authority

THE STAKEHOLDERS

The HTTPS market involves four central stakeholders, as depicted in figure 1: Web-site owners, certificate authorities, Web browsers, and end users.

Web-site owners. Web-site owners decide whether to deploy HTTPS or not, and how securely to implement it on their servers. Deployment is a binary affair from the point of view of the end user. An outdated implementation, as long as the browser accepts it, appears similar to the state-of-the-art implementation. If embedded content from third-party Web sites (e.g., behavioral tracking across Web sites for advertising) is a part of the revenue model of a Web-site owner, then that operator has a strong incentive not to deploy HTTPS at all. Both deployment and secure implementation vary widely.[34]

Certificate Authorities. CAs sell TLS/SSL certificates, which come in three categories: root, intermediate/subordinate, and untrusted. *Root CAs* are trusted by default by browsers, after they have solicited for such a status with the browsers and complied with the varying browser CA trust policies. *Intermediate/subordinate CAs* are either directly verified by one root CA or they are part of a chain of trust of several intermediate CAs that ultimately ends with one root CA. Certificates of *untrusted CAs* are not issued by a CA linked to a root CA but are mostly self-signed by the owner of a Web site. Self-signed certificates evoke the “untrusted connection” security warning when served by a Web site to browsers. CAs are owned by such varying entities as multinational corporations, nation-states, universities, and hacker communities—anyone can start a CA operation relatively easily.

Web-browser vendors. These vendors play a key role in the HTTPS ecosystem. For example, they decide whether to trust a CA inherently, how to respond to a (suspected) CA compromise, and how to implement related trust revocation protocols such as the OCSP (Online Certificate Status Protocol). Over the years, various browser have developed different certificate policies, leading to varying numbers of root and intermediate CAs inherently trusted per browser.[3,9]

End users. Because their communications and valuable information are on the line, end users have an interest in seeking HTTPS communications with Web sites, but they depend to a large degree on security decisions made by the other stakeholders and can exert very little control over HTTPS.[4,12]

KNOWN CA BREACHES

DigiNotar. On Friday, September 2, 2011, a nocturnal press conference of the Dutch Minister of Internal Affairs marked the beginning of the DigiNotar affair. It was triggered by unauthorized access in mid-July 2011, reportedly by a hacker sympathizing with the government of Iran, to the root CA capacity of DigiNotar. When the breach became public three months later, it emerged that in this long period of obscurity 531 false certificates had been created for widely used and highly sensitive domain names such as *.google.com, *.facebook.com, update.windows.com, and *.cia.gov.[16] A small player in the global market with a strong presence in the niche for Dutch e-government services, DigiNotar had root status with all major browser vendors, leading those browsers to trust, by default, corrupt certificates for months.

According to the forensic report, 30 critical updates had not been performed, logging was insufficient, and no antivirus protection was in place at the time of the intrusion.[17] The damage was probably enormous but cannot be determined with certainty because of the unreliability of the log files. ENISA (European Network and Information Security Agency) speaks of breached communications of "millions of citizens," particularly connected to the *.google.com certificate, and notes that some experts believe that the lives of Iranian activists have been put at risk.[12] Upon publication of the breach, the trust in the entire range of DigiNotar activities was revoked by all the major browsers.

Comodo. The range of breaches at market-leading CA Comodo also received considerable media attention.[19] The best-documented breach was the compromise of Comodo's UTN-USERFirst-Hardware certificate. According to the EFF (Electronic Frontier Foundation) SSL Observatory, 85,440 public HTTPS certificates were signed directly by UTN-USERFirst-Hardware, and indirectly, the certificate had delegated authority to 50 more intermediate CAs.[10]

Verisign. Another dominant CA, Verisign, was hacked in 2010. The breach was not discovered until February 2012, after new SEC (Security and Exchange Commission) regulations mandated that companies notify investors of intrusions. In reporting its discovery, news agency Reuters quoted a former CTO who said Verisign "probably can't draw an accurate assessment" of the damage, given the time elapsed since the attack and the vague language in the SEC filing.[12]

Trustwave. Trustwave used its root CA status to enable third parties to issue SSL server certificates for the purpose of monitoring employees. While providing man-in-the-middle capabilities to private entities via sub-CAs does not technically breach the HTTPS trust model, it undermines it. This is especially true when end users are not informed of the monitoring. Trustwave claims that this is common practice among root CAs.[7] This illustrates the "compelled-CA attack" in real life: CAs are in a unique position to enable surveillance of end users.[32]

Steven B. Roosa and Stephen Schultze[29] report on several other breaches, including GlobalSign, KPN/Getronics, StartSSL, and TurkTRUST. From the known CA breaches, several patterns emerge.

SYSTEMIC VULNERABILITIES OF THE HTTPS AUTHENTICATION MODEL

The term *systemic vulnerabilities* refers to those vulnerabilities inherent in the HTTPS ecosystem, as opposed to incidental vulnerabilities that have occurred at a particular stakeholder during an isolated incident. Many security experts agree that the security of the HTTPS authentication model and thus the HTTPS ecosystem is systemically flawed as a result of these vulnerabilities.[1]

Weakest link. A crucial technical property of the HTTPS authentication model is that any CA can sign certificates for any domain name. In other words, literally *anyone* can request a certificate for a Google domain at any CA anywhere in the world, even when Google itself has contracted one particular CA to sign its certificate. CAs have certain institutional limits to issuing certificates (e.g., validation procedures) but no technical ones. If this second google.com certificate is obtained from one of the hundreds of intermediate CAs that link to root CAs trusted by browsers, users will get the familiar HTTPS notification (signaling all is OK).

While this ability to sign for any domain name has spurred a flourishing global market for certificates, it has profound implications for the security of the HTTPS ecosystem, commonly referred to as the *weakest-link* problem: if one CA suffers a breach, the entire ecosystem is under attack.[12,29] The scenarios for failure are manifold, from CA compromise, misconfiguration, and malpractice to state compulsion.[32]

Information asymmetry and ineffective auditing schemes. The recurring information asymmetries are a striking systemic vulnerability, making it very hard for other stakeholders to know about the security of CAs. The current regulatory regime in the E.U. and auditing obligations worldwide have proven ineffective. The qualified certificate practices of DigiNotar were regulated and passed the periodic audits based upon internationally recognized industry standards. The regulatory and auditing schemes deliver perceived security and enable liability dumping.[29]

Liability dumping. Web sites, browsers, and CAs push damages from security breaches downstream toward end users. CAs, for example, disclaim all liability for losses suffered via inappropriately issued certificates.[29,35] Because of the negative externalities at play, liability dumping is a common practice, and it is widely criticized for providing wrong incentives or actual security provision.[1,31] End users bear the burden of these security vulnerabilities and breaches, even though most users are probably unaware of this and cannot reasonably be held responsible for evaluating security practices in the HTTPS authentication model.

MAPPING THE HTTPS MARKET

To understand these systemic flaws better, a thorough understanding of the market dynamics of HTTPS is essential.[1] It is only in light of such data-driven findings that one can start to reflect on the need for legal and technical interventions in the current HTTPS ecosystem.

Several studies have surveyed the SSL certificate market. Two of the largest have been the EFF SSL Observatory in 2010 and the University of Michigan's HTTPS ecosystem scans in 2012-2014. Both projects systematically scanned the entire IPv4 address space, looking for publicly facing HTTPS servers. They retrieved the SSL certificates presented by these servers and later parsed and validated them to determine whether different browsers and operating systems would trust that certificate.

In an earlier study[3] we used the EFF data set, which contains approximately 1.5 million trusted certificates, in empirically establishing the number of CAs, the firms that own them, their market shares, and the pricing strategies. We compared our findings against the HTTPS ecosystem scan data set, which has approximately 3 million trusted certificates. Zakir Durumeric et al.[9] use this data set to analyze the HTTPS ecosystem. While the latter scan has collected more certificates than the EFF data set, this difference mostly reflects a linear growth pattern over time in the number of certificates in use on the Web, and to a limited extent improved scanning methodology. There is a difference of 400,000 certificates if the growth trend in the ecosystem scan data is extrapolated back in time to the EFF data-collection period. Despite these differences, the following patterns are consistent across both data sets.

Many CAs. Foremost, the number of organizations that can issue browser-trusted certificates is high. There are between 1,000 and 2,000 trusted CAs, including root and intermediate CAs. Multiple CAs might be owned by the same organization for a variety of operational and business needs, so the number of issuing organizations is lower. Mapping CAs to organizations leads to an estimated 250 to 700 trusted certificate-issuing organizations, located in 57 countries worldwide. Heterogeneity is often good for an ecosystem, especially in terms of resilience. Because of the weakest-link nature of the HTTPS system, however, this also means many more single points of failure in case of CA compromise or misconfiguration. What's particularly troubling is that a number of the trusted CAs are run by authoritarian governments, among other less trustworthy institutions. Their CAs can issue a certificate for *any* Web site in the world, which will be accepted as trustworthy by browsers of all Internet users.

HTTPS market concentration. Second, the market for SSL certificates is highly concentrated, despite the large number of issuers. In fact, both data sets find that around 75 percent of SSL certificates in use on the public Web have been issued by just three companies: Symantec, GoDaddy, and Comodo. Symantec, the largest commercial CA, owns multiple brands, including Verisign, GeoTrust, Thawte, RapidSSL, and TC TrustCenter. The distribution is heavily skewed, with smaller CAs having little or no presence on the public Internet. Power-law distributions, although not surprising in Internet service markets, pose a major risk for the HTTPS ecosystem: if one of the large CAs is compromised, its root status cannot be revoked by browser vendors without massive collateral damage. One particular CA of GoDaddy had signed 26 percent of all valid HTTPS certificates in March 2013. That means if it were compromised, 26 percent of all Web sites that rely on HTTPS would need to be immediately issued new certificates.[9] Otherwise, browsers ought to present certificate warnings or block access to those sites, posing an impossible tradeoff for the user between access and security. In other words, such large CAs are truly “too big to fail.”

Weak price competition. Mapping the prices for different certificate brands provides a sense of the degree to which the market is dominated by price competition. Figure 2 shows the price and market share for DV certificate offerings. Symantec/GeoTrust certificates (e.g., QuickSSL Premium) sell for $149 but have a much larger market share than Gandi SSL certificates selling at $16. OV and EV markets show similar dynamics, as presented in table 1.

The situation is extreme in the EV market, as shown in figure 3. The market leader, Verisign, sells certificates for approximately $1,000 and has a 63 percent market share. GoDaddy, offering certificates at a fraction of that price ($100), captures a mere 5 percent of the market. (These

FIGURE 2

Price and Market Share of DV Certificates

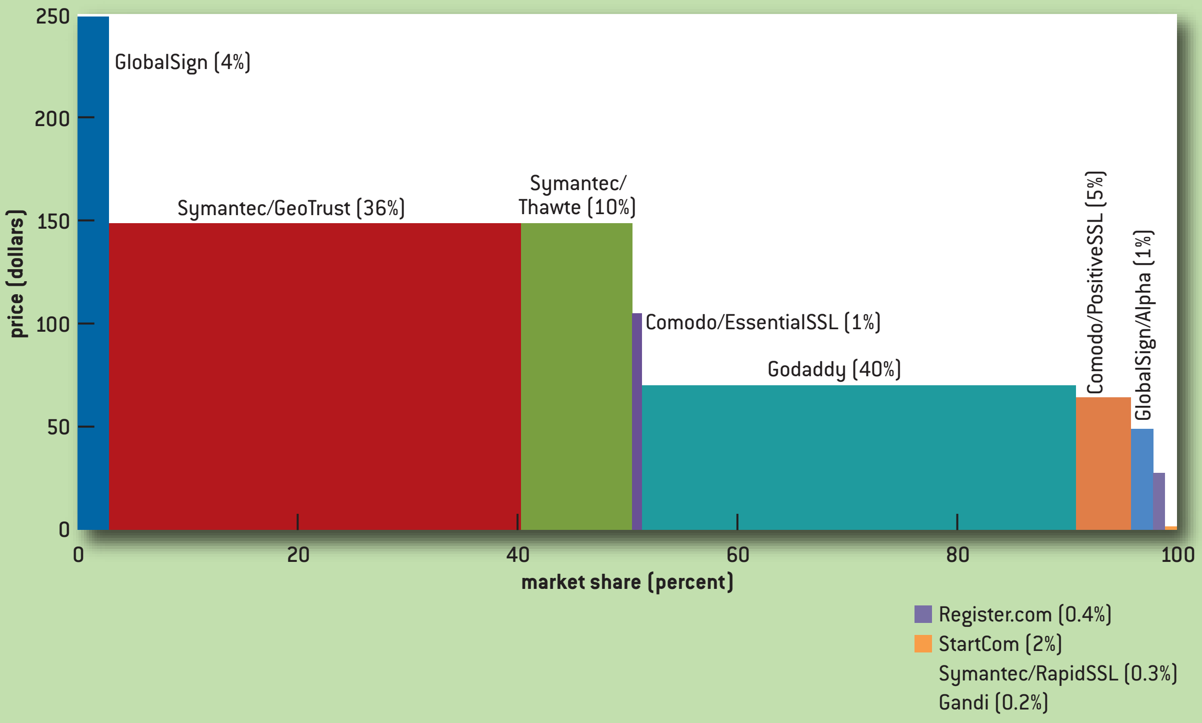


TABLE 1: **Price ranges of different certificates**

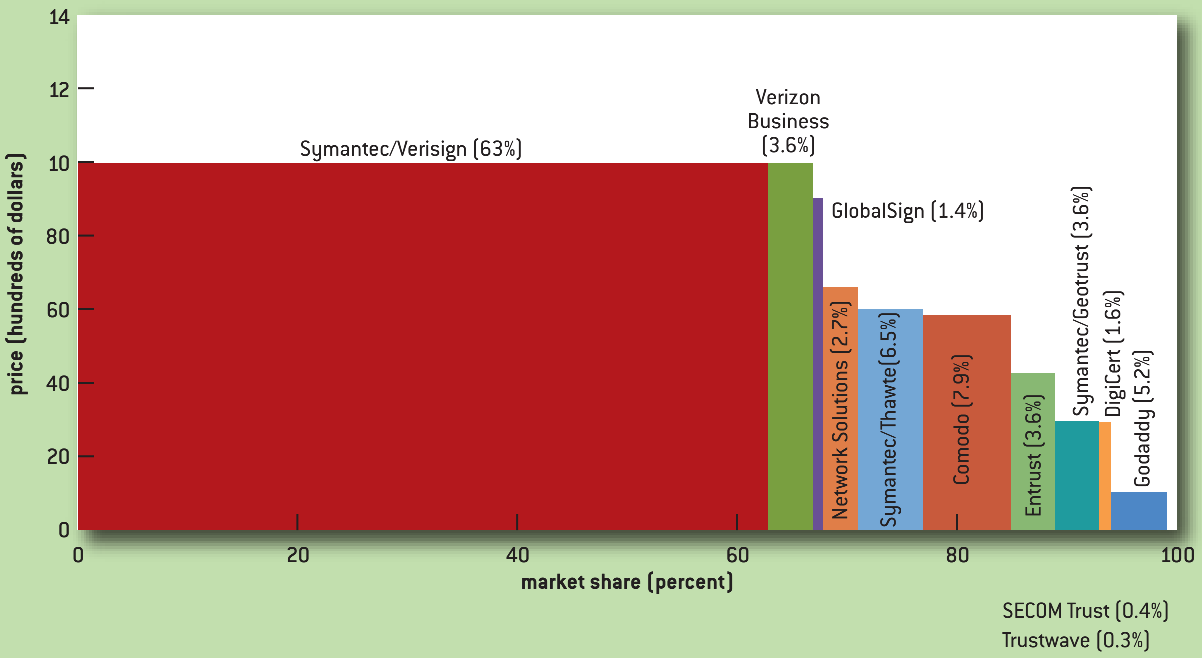
Certificate type	Min price	Max price	Average (std. dev.)
DV	$0	$249	$81 (74)
OV	$38	$1172	$258 (244)
EV	$100	$1520	$622 (395)

comparisons have certain limitations, most notably that prices are as advertised by vendors in March 2013, while market shares were from the EFF 2010 data set.[3] The more recent and longitudinal HTTPS ecosystem scan data shows that similar market shares hold over time, with a slight shift of a few percentage points away from Symantec to cheaper providers.) The differences are intriguing, as certificates themselves are perfect substitutes (within each validation category). The differences might be explained by features bundled with the certificates, discussed in the next section. In sum: the SSL market shows few signs of intense price competition.

ANALYSIS OF HTTPS MARKET INCENTIVES

Various researchers and industry observers have claimed that a "race to the bottom" exists in the HTTPS market: a market dominated by fierce competition pushing prices toward marginal cost, with perverse incentives for security.[1,31] Some have pointed to this as an explanation for the poor security practices at DigiNotar and other compromised CAs.[20,26,29,35]

FIGURE 3 **Price and Market Share of EV Certificates**



One would indeed expect such a race. Certificates are perfect substitutes, suggesting a completely commoditized market. Also, buyers can't meaningfully distinguish secure from less secure offerings; and even if they could, buying from a more secure CA cannot protect the site owner against the threat of an attacker fraudulently signing the domain with a certificate from a compromised CA.

The empirical data, however, clearly suggests otherwise, showing market concentration and little price competition. In one sense, it is good news that the market is not driven by a race to the bottom, given the perverse security incentives associated with such a race. Rather than certificates themselves, however, the HTTPS market is driven by:[3]

- Bundled security services such as scans of the buyer's s site for malware.
- Enterprise certificate management services such as support for management and billing of large numbers of certificates.
- Brand reputation as a liability shield against shareholders, regulators, or others who may hold the buyer accountable in the face of security issues.
- Trust or security signals aimed at third parties and end users such as site seals, warranty amounts and the high price of a certificate itself.
- Higher continuity in case of security failures at the CA, because of the too-big-to-fail dynamic of market-leading CAs.

Knowledgeable buyers understand that security in this market is a weakest-link problem and thus determined by the weakest CA. They also understand that three of the four market leaders got hacked in recent years and that some of the "security" features of these services do not really provide actual security. Nonetheless, buying from the market leaders is still rational, given the liability shield and higher continuity. The price differences are not enough to overrule these advantages. They may be large in a relative sense, but they are modest in absolute terms, compared with other cost components in large firms.

Given that the market leaders successfully differentiate their products via, among other things, security-related features, buyers appear to be willing to pay for security. Two classic problems, however, as mentioned earlier, affect the proper alignment of incentives:

- **Information asymmetry prevents buyers from knowing what CAs are really doing.** Buyers are paying for the perception of security, a liability shield, and trust signals to third parties. None of these correlates verifiably with actual security. Given that CA security is largely unobservable, buyers' demands for security do not necessarily translate into strong security incentives for CAs.

- **Negative externalities of the weakest-link security of the system exacerbate these incentive problems.** The failure of a single CA impacts the whole ecosystem, not just that CA's customers. All other things being equal, these interdependencies undermine the incentives of CAs to invest, as the security of their customers depends on the efforts of all other CAs.

The most powerful incentive for security seems to be reputation effects, but this does not necessarily make them more sensitive to the reputation damage caused by breaches. While they have more to lose compared with smaller brands, large CAs are less threatened by the ultimate reputation effect: being removed from the root stores.

Ironically, the security problems that have plagued the HTTPS ecosystem over the past few years, including the breaches at market leaders, may in fact benefit these same market leaders. The breaches have increased the demand for security, and this demand seems to latch onto whatever security signals are available, regardless of their relationship to actual security. All of this may impact the attempts to fix the systemic vulnerabilities of the system. The dominant players might be reluctant—or less eager—to push for adoption of one of the proposed technological solutions. This is not to suggest that market leaders will act against them, but rather that the status quo works quite well for them.

IMPROVING HTTPS GOVERNANCE

In the aftermath of these CA breaches, policymakers and technologists have suggested regulatory and technical solutions to the systemic vulnerabilities of HTTPS. Let's evaluate these solutions in light of the market-incentive analysis.

REGULATORY SOLUTIONS

The HTTPS authentication model is by and large unregulated in both the U.S. and the E.U. This is bound to change in the near future. The two entities have opted for completely different approaches: the U.S. gives priority to technological solutions and lets industry self-regulate in the meantime. The European Commission (the executive branch of the E.U.), on the other hand, proposed the Electronic Identification and Trust Services Regulation in June 2012. Unlike the more common E.U. *directives* that require implementation in national law, *regulations* acquire direct binding force of law in all E.U. member states upon adoption in Brussels. In April 2014 the European Parliament adopted the commission proposal with substantial amendments, leaving the regulation only for the E.U. Council (national governments of the E.U.) to approve.

This section outlines the scope, underlying values, security requirements, security breach notification requirements, and liability regime of the E.U. proposal,13 as well as the recent proposals by Mozilla for "chain of trust transparency."*2,3*

Scope. The E.U. proposal regulates *trust service providers*, including CAs.[13] All major CAs appear to fall within both U.S. and E.U. jurisdiction.[3] While inherently local, regulation may therefore be an effective instrument to address the observed market failures and positively influence HTTPS security globally. Other critical stakeholders in the HTTPS ecosystem, however, such as browser vendors and Web-site operators, remain unregulated in the proposal. This limited scope impacts the proposed security measures considerably.

Underlying values. The E.U. proposal focuses on availability interests to boost trust in e-commerce, neglecting confidentiality and integrity concerns connected to the systemic HTTPS vulnerabilities already outlined. Apart from failing to observe privacy and communications secrecy obligations under the E.U. Charter of Fundamental Rights, the proposal completely ignores the Snowden revelations. The BULLRUN and MUSCULAR disclosures have made clear that HTTPS significantly raises the costs of mass dragnet surveillance and has been a primary target of intelligence agency subversion. Large Internet companies have now started or accelerated efforts to encrypt communication paths both with users and within their own networks using TLS. The April 2014 E.U. Parliament amendments not only ignore these developments, but also make explicit that the HTTPS provision is "entirely voluntary" for Web services (recital 67).

Security requirements. The E.U. proposal introduces new obligations for CAs to adopt security requirements. Their details will be determined by the European Commission in a so-called implementing act. While such delegation to the executive branch provides some flexibility to adapt requirements to new technological developments, the E.U. proposal fails to specify regulatory priorities or underlying values. Moreover, the April 2014 parliament amendments literally state that "industry-led initiatives (e.g., CA/Browser Forum)" influence such requirements (recital 67). Naming a CA industry group as influential in a law that seeks to address failing security practices of CAs indicates control by dominant market players.

SBN (Security breach notification).

In theory, SBNs help minimize the damage after a breach has occurred and provide incentives for organizations to invest in information security upfront. The E.U. proposal introduces an SBN regime stating that notification needs to occur "within 24 hours" to relevant authorities if the breach "has a significant impact," a concept that is not defined in the law. The general public is informed when a breach harms the "public interest" (also undefined). Again, the European Commission will determine those details, but the parliament proposal states that CAs should be subject to "light-touch and reactive ex-post supervisory activities" and that there exists "no general obligation to supervise non-qualified service providers" (i.e., CAs offering certificates for HTTPS).

Aforementioned information asymmetries and CA breaches render defensible a strict regime for notifications—which types of breaches should be made public by default, for example. Experiences with SBN legislation in the U.S., moreover, suggest that SBNs need to be complemented with punitive (e.g., sanction and liability regimes) and proactive enforcement (e.g., as part of annual reporting) to create real incentive to notify—and avoid noncompliance by less well-intentioned companies.[1,31] In addition, reputation losses might not affect major CAs that do not risk being thrown out of root stores for nonreporting. Reporting not only breaches, but also the vulnerabilities that led to them, would be a major step forward, as would a scheme of responsible disclosure. Such lessons are not included in the E.U. proposals or considerations. Moreover, the parliament has further weakened the SBN regime by mandating light-touch and ex-post supervision. Again, these amendments indicate capture of the regulatory process by dominant CAs.

Liability. As already observed, liability for security breaches is disclaimed across the HTTPS ecosystem and transferred through terms and conditions to end users. The 2012 E.U. Commission proposal sought to address such liability dumping by imposing a strict liability regime on CAs for "any direct damage," with CAs bearing the burden of proving that they handled the situation non-negligently. The 2014 parliament amendments reverse this burden of proof; customers and users now have to prove malicious intent or negligence at CAs post-breach. Moreover, CAs are allowed to transfer liability in their terms and conditions to end users. Astonishingly, the parliament explicitly codifies liability dumping. Again, there are traces of regulatory capture at the E.U. parliament.

The weakest-link problem of HTTPS creates more fundamental problems with security through liability: small CAs will be unable to conduct business with large corporations processing vast amounts of sensitive data. Consider DigiNotar, with an annual budget of a few million U.S. dollars; it could never cover damages for the rogue certificates that were issued for Google, Facebook, Skype, cia.gov, etc. in the midst of its security breach. Smart CAs will thus circumvent liability by creating subsidiary special-purpose companies that bear full liability and can easily file for bankruptcy. Indeed, DigiNotar quickly went bankrupt post-breach, while its parent company Vasco has escaped unscathed.

Tackling fundamental issues with liability regimes requires carefully crafted policies or broad mandates for enforcement. Liability should be matched with security requirements and distributed among all stakeholders: domain owners should have incentives to protect their assets through HTTPS offering and implementation,[2] while browsers should strengthen their CA policies (as discussed later). The European Commission failed to consider such fundamental drawbacks, and the parliament amendments make matters worse by codifying liability dumping and reversing the burden of proof.

Chain of trust transparency. Unrelated to the E.U. proposals, Mozilla has proposed the so-called "chain of trust transparency." As discussed earlier, one cannot assure that HTTPS communications are subject to systematic but unnoticed surveillance without transparency,[32] but today it is only starting to emerge through various (research) projects such as the browser plug-in CertPatrol for Firefox.

In a recent amendment to its CA policy, Mozilla requires that subordinate CA certificates "either be technically constrained or be publicly disclosed and audited."[27] Subordinate CAs, in other words, must either be constrained to issue certificates for only a small set of domain names—on internal networks, for example—or their chain of trust must be publicly disclosed and audited. The aim is to hold subordinate CAs to similar standards as root CAs and make a root CA accountable for all the sub-certificates it signs. Existing subordinate CA certificates were given until May 15, 2014, to comply, so it's too early to observe how Mozilla enforces noncompliance. Nonetheless, chain of trust transparency warrants at least consideration and, from a theoretical perspective, encouragement throughout the HTTPS ecosystem.[30] So far, it has not been part of any regulatory proposal.

TECHNOLOGICAL SOLUTIONS

A host of technological solutions to the systemic vulnerabilities of the current system are being developed. Among the most prominent are Convergence,[8] Perspectives,[28] DANE,[18] Sovereign Keys,[11] Certificate Transparency,[6,23] Public Key Pinning,[14] and TACK.[24,33] From the perspective of governance, we can make several general observations:

- All proposals attempt to solve the weakest-link problem by introducing another authority to check whether the certificate that is validated through the normal HTTPS process is indeed the correct one.
- All proposals reduce the information asymmetry of buyers and users, versus the CAs, by systematically uncovering suspect certificates.
- All proposals can function on top of the current CA system, leaving it in place or depending on it; a subset can also replace it.
- All proposals can follow incremental adoption paths (albeit some are a lot more difficult than others), and all need support from browsers.

None of these solutions is close to large-scale adoption. That said, they do seem promising in terms of addressing the current weaknesses, especially the weakest-link problem, for which regulatory solutions appear ineffective. Therefore, in the long run they are preferable, and it's relevant to assess how they relate to the incentives of the HTTPS stakeholders. Some scholars predict multiple proposals will eventually be adopted.[5]

As argued earlier, the insecure status quo can be beneficial for market leaders. In light of this, one might assume that CAs are not particularly keen on actively helping any of these proposals along, especially the ones that theoretically could make them obsolete. In practice, however, some CAs are involved in developing potential solutions—for example, DigiCert and Comodo are experimenting with Certificate Transparency.[21] Other proposals require nontrivial activities on the part of the domain owner, which may be done by their CA as a complementary service to current business models.

Furthermore, each proposal is intensely debated in relation to browser performance. Any form of large-scale adoption requires default support by browser vendors. Google and Mozilla have been particularly active in this area.

While none of these solutions is easy to scale, there are benefits for early adopters, a key requirement for any solution to take off. Whether the costs are worth it depends on the kinds of threats HTTPS stakeholders want to defend themselves against. An average cybercriminal might not be interested in breaching a CA and manipulating network traffic already encrypted through HTTPS, as financially attractive information can be acquired through more cost-effective attacks.[15,22] From previous breaches, it appears that state-sponsored attackers and large corporations, rather than profit-driven criminals, are more likely to engage in the complex man-in-the-middle attacks in the realm of HTTPS. For some user groups and domains, such adversaries make early adoption attractive.

CONCLUSION

Recent breaches at CAs have exposed several systemic vulnerabilities and market failures inherent in the current HTTPS authentication model: the security of the entire ecosystem suffers if any of the hundreds of CAs is compromised (weakest link); browsers are unable to revoke trust in major CAs ("too big to fail"); CAs manage to conceal security incidents (information asymmetry); and ultimately customers and end users bear the liability and damages of security incidents (negative externalities).

Understanding the market and value chain for HTTPS is essential to address these systemic vulnerabilities. The market is highly concentrated, with very large price differences among suppliers and limited price competition. Paradoxically, the current vulnerabilities benefit rather than hurt the dominant CAs, because among others, they are too big to fail.

In terms of solutions, the E.U. has opted for a regulatory response, while the preference in the U.S. is for industry self-regulation and technological solutions. In general, the technological solutions aim to solve the weakest-link security problem of the HTTPS ecosystem. Several proposals are promising, but none is near large-scale adoption. Industry self-regulation has only augmented market failures, rather than solving them.

The proposed E.U. regulation does not consider the role of all stakeholders in the HTTPS ecosystem, thus reinforcing systemic vulnerabilities by creating new long-term institutional dependencies on market-leading CAs. The April 2014 E.U. Parliament amendments make matters much worse. The E.U. Parliament seems to have been successfully captured by CA lobbying efforts.

Regardless of major cybersecurity incidents such as CA breaches, and even the Snowden revelations, a sense of urgency to secure HTTPS seems nonexistent. As it stands, major CAs continue business as usual. For the foreseeable future, a fundamentally flawed authentication model underlies an absolutely critical technology used every second of every day by every Internet user. On both sides of the Atlantic, one wonders what cybersecurity governance really is about.

ACKNOWLEDGMENTS

For inspiration and comments, the authors would like to thank: Bernhard Amann, Ian Brown, Peter Eckersley, Edward Felten, Sharon Goldberg, Joris van Hoboken, Ralph Holz, Chris Hoofnagle, Kees Keuzenkamp, Samad Khatibi, Arman Noroozian, Bruce Schneier, Stephen Schultze, Christopher Soghoian, Sid Stamm, Marcelo Thompson, and participants of TPRC 2012, WEIS 2013, two

workshops at the Berkman Center in Spring 2014, 29c3, a UC Berkeley TRUST Seminar January 2013, and an HKU Law & Tech Talk, February 2013. The authors are solely responsible for this article.

REFERENCES

1. Anderson, R.J. 2008. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
2. Arnbak, A., van Eijk, N. 2012. Certificate Authority collapse: regulating systemic vulnerabilities in the HTTPS value chain. TPRC (Research Conference on Communication, Information and Internet Policy); http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2031409.
3. Asghari, H., van Eeten, M.J., Arnbak, A.M., van Eijk, N.A. 2013. Security economics in the HTTPS value chain; http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2277806.
4. Bakos, Y., Marotta-Wurgler, F., Trossen, D. 2009. Does anyone read the fine print? Testing a law and economics approach to standard form contracts. Fourth Annual Conference on Empirical Legal Studies.
5. Bonneau, J. 2013. Fixing HTTPS: new models for distributing transport security policy. Center for Information Technology Policy (CITP) Seminar; https://docs.google.com/presentation/d/1dxWwKUOVjO1MnOJQkyxCS03VfFp_kmPeAmneJ9KLd-M/edit?usp=sharing.
6. Certificate Transparency. 2012; http://www.certificate-transparency.org/.
7. Constantin, L. 2012. Trustwave admits issuing man-in-the-middle digital certificate; Mozilla debates punishment. *ComputerWorld* (February 8); http://www.computerworld.com/s/article/9224082/Trustwave_admits_issuing_man_in_the_middle_digital_certificate_Mozilla_debates_punishment.
8. Convergence. 2011; http://convergence.io/details.html.
9. Durumeric, Z., Kasten, J., Bailey, M., Halderman, J.A. 2013. Analysis of the HTTPS certificate ecosystem. Internet Measurement Conference.
10. Eckersley, P. 2011. Iranian hackers obtain fraudulent HTTPS certificates: How close to a Web security meltdown did we get? Electronic Frontier Foundation; https://www.eff.org/deeplinks/2011/03/iranian-hackers-obtain-fraudulent-https.
11. Electronic Frontier Foundation. 2011. The Sovereign Keys Project; https://www.eff.org/sovereign-keys.
12. ENISA. 2011. Operation Black Tulip: Certificate Authorities lose authority, version 2 (December); http://www.enisa.europa.eu/media/news-items/operation-black-tulip.
13. European Union. 2014. Electronic identification and trust services for electronic transactions in the internal market. Amended proposal, 2012/0146(COD), A7-0365/201; http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0282#title3.
14. Evans, C., Palmer, C, Sleevi, R. 2012. Public key pinning extension for HTTP. Internet Engineering Task Force; http://tools.ietf.org/html/draft-ietf-websec-key-pinning-04.
15. Florêncio, D., Herley, C. 2011. Where do all the attacks go? Workshop on Economics of Information Security (WEIS); http://research.microsoft.com/pubs/149885/WhereDoAllTheAttacksGo.pdf.
16. Fox-IT. 2011. DigiNotar Certificate Authority breach (September 5); http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html.
17. Fox-IT. 2012. Black Tulip – Report of the investigation into the DigiNotar Certificate Authority breach; http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update.html.

18. Hoffman, P. 2012. The DNS-Based Authentication of Named Entities (DANE), Transport Layer Security (TLS) Protocol: TLSA. IETF, RFC 6698; http://tools.ietf.org/html/rfc6698.
19. InfoSecurity. 2011. Comodo admits two more registration authorities hacked; http://www.infosecurity-magazine.com/view/16986/comodo-admits-two-more-registration-authorities-hacked.
20. Kelkman, O.M. 2013. DNSSEC Musings: DigiNotar, DANE and Deployment. NLnet Labs; http://conference.apnic.net/__data/assets/pdf_file/0005/58901/dnssec-diginotar-dane_1361864377.pdf.
21. Langley, A. 2012. Certificate transparency. ImperialViolet; http://www.imperialviolet.org/2012/11/06/certtrans.html.
22. Langley, A. 2013. Real World Crypto 2013. ImperialViolet; http://www.imperialviolet.org/2013/01/13/rwc03.html.
23. Laurie, B., Langley, M., Kasper, E. 2013. Certificate Transparency. Internet Engineering Task Force; http://tools.ietf.org/html/draft-laurie-pki-sunlight-12.
24. Marlinspike, M., Perrin, T., ed. 2013. Trust assertions for certificate keys. Internet Engineering Task Force; http://tools.ietf.org/html/draft-perrin-tls-tack-02.
25. Menn, J. 2012. Key Internet operator VeriSign hit by hackers. Reuters (February 2); http://www.reuters.com/article/2012/02/02/us-hacking-verisign-idUSTRE8110Z820120202.
26. Mills, E. 2011. Google users in Iran targeted in SSL spoof. CNET (August 30); http://news.cnet.com/8301-27080_3-20099421-245/google-users-in-iran-targeted-in-ssl-spoof/.
27. Mozilla. 2013. Mozilla CA certificate policy, version 2.2 (February 14); http://www.mozilla.org/projects/security/certs/policy/.
28. Perspectives Project. 2011. What is perspectives?; http://perspectives-project.org/.
29. Roosa, S.B., Schultze, S. 2010. The “Certificate Authority” trust model for SSL: a defective foundation for encrypted Web traffic and a legal quagmire. *Intellectual Property & Technology Law Journal* 22(11): 3-8.
30. Roosa, S.B., Schultze, S. 2013. Trust Darknet: control and compromise in the Internet’s Certificate Authority Model; http://ssrn.com/abstract=2249042.
31. Shapiro, C., Varian, H. 1998. *Information Rules*. Harvard Business School Press.
32. Soghoian, C. Stamm, S. 2012. Certified lies: detecting and defeating government interception attacks against SSL. In *Financial Cryptography and Data Security*. Springer: 250-259.
33. TACK. TACK, for pinning. 2012; http://tack.io/.
34. Trustworthy Internet Movement. 2014. SSL Pulse. Survey of the SSL implementation of the most popular Web sites; https://www.trustworthyinternet.org/ssl-pulse/.
35. Vratonjic, N., Freudiger, J., Bindschaedler, V., Hubaux, J.-P. 2011. The inconvenient truth about Web certificates. In Workshop on Economics of Information Security (WEIS) (Fairfax, VA).

LOVE IT, HATE IT? LET US KNOW

feedback@queue.acm.org

AXEL ARNBAK is a cybersecurity and information law researcher at the University of Amsterdam, and Research Fellow at the Berkman Center (Harvard University) and at CITP (Princeton University). Publications and full bio at: https://www.axelarnbak.nl/.

HADI ASGHARI is a researcher in the economics of cybersecurity at Delft University of Technology, Faculty of Technology, Policy and Management. Publications and full bio at: http://member.acm.org/~hasghari.

MICHEL VAN EETEN is a professor of governance of cybersecurity at Delft University of Technology, Faculty of Technology, Policy and Management. Publications and full bio at: www.tbm.tudelft.nl/econsec.

NICO VAN EIJK is professor of media and telecommunications law and director of the Institute for Information Law (IViR, Faculty of Law, University of Amsterdam). Publications and full bio at: http://www.ivir.nl/staff/vaneijk.html.