access

THE WEAKEST LINK IN THE CHAIN: VULNERABILITIES IN THE SSL CERTIFICATE AUTHORITY SYSTEM AND WHAT SHOULD BE DONE ABOUT THEM

An Access Policy Brief Regarding the Consequences of the DigiNotar breach for Civil Society and Commercial Enterprise

Discussion Paper for Comment

November 2011

THE ISSUE

The SSL cryptosystem forms the basis for most web-based secure communications seen on the internet today. It is widely used to protect transactions for ecommerce and is used by civil society to secure webmail communications, interactions on social networking sites, and to protect what they view and publish online.

Since its introduction in the mid-'90s, SSL has proven to be a fairly robust system. However, issues including scalability and the increase in activities of the state-sponsored hackers of some regimes have significantly weakened the security of the system. So far, 2011 has been a terrible year for the technology, with multiple breaches of Certificate Authorities (the institutions that confer trust within the cryptosystem) as well as the authoring of a practical cracker tool, BEAST,[1] which attacks weaknesses within the cryptographic algorithms used in SSL that have been known theoretically for some time. This policy brief seeks to address the growing issues of scalability and trust within the cryptosystem.

SSL fulfills the need for a cryptosystem that can be used by parties unable to verify trust in each other when they need to conduct some form of confidential transaction, be that financial or otherwise private in nature. The system relies on the introduction of third parties, called Certificate Authorities, which specialize in managing this trustworthiness between the parties. Often, it is one party that requires this trust conference initially in order for the transaction to proceed. Take for example an online bank. A user needs to be confident they are interacting with the actual bank they want to interact with, and not someone posing as the bank, before they are willing to use their login credentials authenticating themselves to the bank. The SSL cryptosystem uses the CA to handle this initial verification, and it is the CA that confers trustworthiness in the bank to the user. For the bank's part, they too need to know the user is who they say they are. This is left up to the bank to verify once the secure encrypted connection is established with the user (usually this is achieved by the user providing a login ID and password to the bank). It is part of the CA's role to perform due diligence that the bank is actually the bank they claim to be and issue them with a certificate signed by the CA's root certificate, which in turn is explicitly trusted by the web browsers in common use.

Over time, and with the current proliferation of CAs, we have begun to see real weaknesses appear in the SSL cryptosystem. One symptom of the weakness inherent in SSL is the recent security breach at the DigiNotar CA, which resulted in valid SSL certificates being issued to parties not associated with the institutions and organizations listed on the certificates. There is currently no universal best-practice framework to guide the myriad governing bodies that oversee and set standards for the large number of Certificate Authorities. While such a framework would be difficult to enforce, the DigiNotar experience points to the fact that certificate security policies and procedures at every level need to be audited and improved. For example, a simple security audit of DigiNotar's practices (e.g., using Windows machines without any patching regime) would have quickly revealed vulnerabilities and gone a long way to preventing this hack from taking place.

THE CURRENT SECURITY CERTIFICATE SYSTEM

CAs are tasked with validating the identities of web servers that provide SSL. The basic model of SSL CA certification uses Public Key Infrastructure (PKI) to allow users (via their web browsers) to request a page from a site that uses SSL (HTTPS). The browser then receives the site's public key with its certificate information, and checks that information against its list of accepted CAs to see if the cert is from a trusted CA, and if it matches the name of the site it claims to represent. Browsers also check certificates against revocation lists to see if they are unrevoked and unexpired. If the certificate is deemed authentic, unrevoked, and current, the browser will send the site a symmetric key and receive, unencrypt, and display the requested page. The browser will also display a lock icon and (for certs that have received "Extended Validation") a colored browser bar for the user to signal the validity of the site's CA cert.

This system is designed to work as seamlessly as possible for the user, and hinges on cooperation between web browsers and the CAs. Indeed a number of the flaws in the current system stem from its design in the early 1990s, when need for

1 http://www.readwriteweb.com/archives/breaking_the_internet_researchers_successfully_hac.php

SSL was extremely low and attacks almost entirely theoretical. Because of this, the flaws in the system have only become magnified as the demand for encryption of sites has skyrocketed, and the number of certificate authorities has expanded. There is no oversight or management mechanism for the more than 650 CAs worldwide, some of which are nation-states.[2] At its root, the most tenacious hurdle to improvement is the rapid growth of a system based on poor design decisions made before today's challenges could be foreseen. This has resulted in a system where:

- All certificate authorities are equally trusted in the SSL Public Key Infrastructure, and can provide certificates for any website. So users aren't just putting the security of their communications in the hand of one CA exclusively managing the certificate for a given site, but all of them.
- Certificates can be tied back to the CAs who created them, and the positive or negative reputation of a CA can affect their business. Supposedly, this provides sufficient incentive for CAs to self-police their systems in their own self-interest, with the theory being that if CAs mismanage their authority and systems (by, say, not effectively securing them from hackers), they can lose business and market share. While DigiNotar has filed for bankruptcy, this has not always been the experience of compromised CAs. As seen most publicly in the case of Comodo, there can be no negative consequences at all for a breach, and there is no over-arching standards-setting organization that monitors the CAs sufficiently.
- End users are at the mercy of how well managed the non-standardized system is between web sites' servers, web browsers, and CAs. It's fair to say that the vast majority don't even understand the overall CA system, let alone the possible vulnerabilities and risks that can affect an increasing amount of highly sensitive and personal data. Most users struggle to correctly interpret and make informed decisions when faced with certificate warnings in their browsers, causing them to accept them by default.
- Due to the considerable dependence on SSL and the CAs, web browsers default to giving CAs the benefit of the doubt when they cannot communicate authenticating queries to revocation lists and the CAs themselves. Instead of making sites inaccessible when this occurs, all of the major browsers tend to attribute a lack of an OSCP response to a temporary communication issue, and assume that the certificates should be considered trusted. This is a tendency exploited by MitM attacks.

SOME KEY STATISTICS

According to a talk given by Peter Eckersley and Jesse Burns at last year's DEFCON[3], as of mid-2010 there were:

- 651 CA organizations
- 1,167 distinct issuer strings
- 1,482 CA root certificates trustable by Windows or Firefox
- 1,377,067 SSL certificates issued by CAs in use on the Internet
- The CAs trusted by the four major browsers are located in 54 countries, resulting in at least as many governing bodies with jurisdiction over a part of the SSL CA system

2 https://www.eff.org/files/DefconSSLiverse.pdf

3 https://www.eff.org/files/DefconSSLiverse.pdf

There are significant issues with the current SSL CA system; unlike many other areas of digital security and Internet governance, where if say a large majority of the companies complied with the policy and regulations, then the system would still hold up. In many other systems, the more distributed the mechanism the more robust the security of entire system, because if one node is compromised you have plenty of others to correctly perform the role. However, for SSL, the opposite is true. With the SSL CA system, if a single one of the 650 CAs is compromised the entire system is compromised, so keeping 100% of the CAs at 100% compliance and 100% impervious from zero-day attacks is a very hard problem indeed. More CAs with DOD-style security practices would present a far more secure SSL environment for Internet users.

Interestingly, and alarmingly, the primary targets of the DigiNotar compromise and previous breaches of the CA system have been members of civil society and human rights organizations. More specifically, of the over 500 fraudulent certificates issued in the DigiNotar compromise, the only bad certificates we've seen used in the wild were for *.google.com and *.torproject.org, sites and services that activists rely on heavily. Of the 300,000 unique IP addresses requesting the bad certificate for google.com, 99.9% originated from Iran, and the remainder were almost entirely from TOR exit nodes, proxies, and other VPN services. This is peculiar, given the incredible reliance on the SSL CA system by private enterprise, healthcare providers, and financial institutions, and highlights the danger that civil society is under.

HISTORY

A brief overview of the compromises of the SSL CA seen to date:

2001 VeriSign (47.5% market share)

- Issued two certificates to someone falsely claiming to be from Microsoft.

March 15, 2011 Comodo (15.44% market share)

- Certificates were falsely issued for seven domains, including Google, Yahoo, Skype, and Microsoft.
- Evidence of login.yahoo.com being used.
- Comodo was barely affected by this considerable breach of security. There were no negative consequences besides press coverage of the incident. Comodo's business, profits, and market share were not affected. Shockingly, the RSA went on to award Comodo CEO Melih Abdulhayoglu with 2011 Entrepreneuer of the Year for his work on Internet Security.[4]

July 10, 2011 DigiNotar (0.016% market share)

- Several hundred certificates issued, including Google, Microsoft, Skype, Tor, Wordpress, Yahoo, Twitter, Facebook, CIA, Mossad, MI6, and the top level domains *.com and *.org.
- Evidence of some being used in transparent man-in-the-middle (MitM) attacks

4 https://www.comodo.com/resources/it-manager/newsletters/apr-11/inside-scoop.php

September 5, 2011 StartCom (0.1% market share)

- "Comodohacker" claims to have breached the security of their network but failed to issue fake certs due to robust processes being in place that prevented this.

September 5, 2011 GlobalSign (1.75% market share)

- Suspended the issuing of certificates after "comodohacker" claimed to have compromised their security.
- Have since resumed issuing certificates after having an external security company investigate if their security had been breached.

TIMELINE OF DIGINOTAR COMPROMISE FROM FOX-IT'S REPORT (P.13)[5] :

06-Jun-2011	Possibly first exploration by the attacker(s)
17-Jun-2011	Servers in the DMZ in control of the attacker(s)
19-Jun-2011	Incident detected by DigiNotar by daily audit procedure
02-Jul-2011	First attempt creating a rogue certificate
10-Jul-2011	The first succeeded rogue certificate (*.Google.com)
20-Jul-2011	Last known succeeded rogue certificate was created
22-Jul-2011	Last outbound traffic to attacker(s) IP (not confirmed)
22-Jul-2011	Start investigation by IT-security firm (not confirmed)
27-Jul-2011	Delivery of security report of IT-security firm
27-Jul-2011	First rogue *.google.com OSCP request
28-Jul-2011	First seen that rogue certificates were verified from Iran
04-Aug-2011	Start massive activity of *.google.com on OCSP responder
27-Aug-2011	First mention of *.google.com certificate in blog
29-Aug-2011	GOVCERT.NL is notified by CERT-BUND
29-Aug-2011	The *.google.com certificate is revoked
30-Aug-2011	Start investigation by Fox-IT
30-Aug-2011	Incident response sensor active
01-Sep-2011	OSCP based on white list

According to the Fox-IT report commissioned by the Dutch Government to investigate the DigiNotar compromise, at least 531 fake certificates were generated by "comodohacker," but the authors state that there is a possibility that there may be more (p. 7). The full list of known fake certificates is available on page 10 of the Fox-IT report.

Finally, it should be noted that to the best of our knowledge, there doesn't seem to be any comprehensive assessment of how many total root certificates exist globally.

5 http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf

SOME CURRENT POLICIES

Current policies in the U.S. (where at least 80% of the CA market share is based) are governed by two major policies:

- The X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)[6] specifies the requirements to becoming a trusted CA.
- The Personal Identity Verification Interoperable (PIV-I) Certification Process Federal PKI Policy Authority[7] describes best practice guidelines that U.S. CAs should follow.

The efficacy of these policies are widely questioned and criticized. For example, the FBCA specifies that CAs should undergo an external security audit annually, but the policy gives no explanation of what this audit should specifically entail. For the vast majority of sites, only the successful receipt of a code from a CA needs to be received at the email attached to their site's WHOIS email account of record. For sites that want to proffer users the newer "green bar" in their browsers that denote "Extended Verification," a more in-depth verification of identity is established, including checking an organization's physical location. Proposed guidelines are in development by the CA/Browser Forum and they have released version 1.0, Interim Public Comment Draft 35 of their Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates[8]

CONCERNS

Great weaknesses in the SSL CA system include:

OVER-COMMERCIALIZATION OF THE CA RESPONSIBILITY

- A commercial playing field. This means the level of entry is based primarily on an entity having enough money to "buy" into the system. If too many organizations can afford this, then we end up with an unmanageable amount of CAs. There is currently no mechanism to limit the amount of CAs we end up with as part of the system, nor does there seem to be robust and universal standards for screening organizations or nation-states who want to become CAs.
- The commercialization leads to competition based on price and therefore the profit margins for certificate issuance goes down, putting unrealistic pressure on each CA's ability to fund good security.
- When there is a compromise, legitimate certificate holders for certificates issued by the compromised CA are adversely affected in the collateral damage.
- CAs operate in 54 jurisdictions, and there is at least one governing body for each of those jurisdictions. This creates inconsistency and quality control becomes a significant issue.
- Not enough checking built into the protocols involved. Therefore too much is left up to the local governing body to guide and police the CAs within their jurisdiction.

6 http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf

7 http://www.idmanagement.gov/pages.cfm/page/IDManagement-PIVI-cross-certification

8 http://cabforum.org/Baseline_Requirements_Draft_35.pdf

ORGANIZATIONS, MERCHANTS, AND END USERS ARE LOSING CONFIDENCE IN THE SSL/TLS/HTTPS SYSTEM

- The myriad uses and management of SSL are diverse and complex. Various platforms, applications, and browsers store certificates from different root CAs in different places within the operating system or applications. This is causing confusion and a lack of certainty for end users trying to understand, troubleshoot, and update various platforms, particularly in the wake of DigiNotar-level security breaches before security updates are released.
- User and commercial confidence in the SSL system needs to be restored.
- The system struggles with transparency while providing a service that hinges on trust. This is also exacerbated by the commercialization of CAs' responsibilities, as private enterprises tend to have the flawed yet systemic belief that for commercial reasons of competitiveness, most details of their internal processes and security practices do not have to be revealed.
- Right now the only consequences for CAs that mismanage their services and systems is the possible threat of losing business. Although DigiNotar has had to file for bankruptcy in the wake of these events, other CAs who have suffered similar security breaches – most notably Comodo – have not lost business.
- Individuals living in countries with repressive regimes -- in particular those in Iran, which has been a frequent target of MitM attacks – are finding it increasingly difficult to ascertain whether their web activity is secure. Obviously, users face significant offline consequences when their web activity becomes compromised. Furthermore, once a large-scale compromise of the SSL CA cryptosystem is announced, it is extremely challenging for users to get back to a position of confidence in the security of their system, often leading to the added detrimental effect of self-censorship.

RECOMMENDATIONS

The DigiNotar case only highlights the challenging cluster of problems in the current system that require a multifaceted response and collaboration between all actors in the sector to fundamentally improve. What follows are points for discussion, recommendations from a policy perspective, areas for increased transparency, suggested improvements to system design, questions about actual SSL/TLS implementation, and areas where more education is required for users. Some organizations and individuals have stepped forward to propose technical re-implementations of SSL, or completely new cryptosystems to replace SSL. While ultimately such solutions may be necessary, it has to be understood that such technical solutions usually take a very long time to become adopted, even when security issues are known to exist in the current system. We see evidence of this already with other known vulnerabilities in TLS 1.0 being addressed in versions 1.1 and 1.2, however not even the major browsers have implemented those newer versions despite TLS 1.1 having been released in April 2006 and TLS 1.2 being released in August 2008. Ipv6 and DNSSEC are other examples of desperately required standards that have been out since December 1998 and August 2004 respectively that have not yet been widely adopted by the technology and internet communities. Therefore the following list of recommendations concentrates predominantly on policy fixes as this approach has a much greater prospect for success in the short term. This list is not exhaustive and is open for discussion, comment, and additions.

POLICY

- Form a substantial global governing body for all CA governing bodies. Currently there are only lightweight

central governing bodies such as the CA/Browser Forum[9] which is a membership of approximately 45 CAs and Browser Vendors. A more substantially resourced central governing body is required to get tighter control over the regional governing bodies and CAs worldwide.

- Global moratorium on new CAs for one year. The proliferation of CAs has contributed to the weakness of the SSL system. A pause is required to review the system and to allow time for the system to be technologically enhanced before any new CAs are added and contribute to the weakening of the overall system.
- Government grants or subsidies for non-profit CAs so that they can provide DOD-level security. Non-profit CAs could offer certificates to activist sites and other at risk populations at cost or for free, which would dramatically increase the security of individuals accessing these sites. However, government funding is critical here to ensure that these CAs can provide the same or better level of security expected from commercial CAs.
- Improve the auditing of CA security. Questions now hang over the current practice of auditing CA security by third parties such as WebTrust.[10] Being a CA capable of issuing EV certificates, it is assumed DigiNotar underwent yearly security audits by a third-party security auditing company. Clearly this did not result in good security practices at the company as the post-mortem Fox-IT report[11] showed DigiNotar's security at the time it was breached was appalling. A more robust methodology to ensure a consistently high level of security needs to be implemented for CAs.
- Stricter data breach notification laws are required for CAs. The Fox-IT report showed that DigiNotar became aware it had been breached months before the story broke in the media. DigiNotar kept silent about the breach and it was not until an end user in Iran raised the alarm after a transparent Man-in-the-Middle attack was perpetrated and was picked up by Google Chrome's new pinning feature[12] that the story broke and DigiNotar was forced to acknowledge they were compromised. Given the significant impact on all users of HTTPS resulting from the breach of any CA, all CAs should be compelled by law to notify the public immediately of any real or suspected security breach of their systems.
- Implement penalties for CAs that experience data breaches, including one or more of the following:
    - Revocation of licenses;
    - Significant fines;
    - Compensation for a compromised CAs other customers who are adversely affected by the revocation of a CA's root certificate. Such customers become collateral damage after a CA breach, as occurred in the DigiNotar case, as browsers were reconfigured to reject all certificates issued by DigiNotar in the months following its compromise.
- Under the current system, any CA can sign a certificate for any domain. In the future, the most high-risk and high-profile targets should be allowed to designate a subset of CAs with the exclusive authority to issue certificates for their domain(s). By limiting the number of CAs for these sites, the vulnerability of the entire SSL CA cryptosystem will be significantly reduced. Given the size or significance of the organizations whose domains present the most desirable target domains for compromise, it is assumed those organizations would therefore nominate the CA with the best security practices to have exclusive authority to issue certificates for their domain(s). This would have the added effect of creating a market that rewards excellent security practices rather than rewarding the CAs who spend the least on security,

9 http://www.cabforum.org

10 http://www.webtrust.org/

11 http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf

12 http://www.imperialviolet.org/2011/05/04/pinning.html

which is the situation as it stands now.

- Promote the policy documents of IDManagement.gov and The National Institute of Standards and Technology (NIST)[13] and get them adopted more broadly around the world.

TRANSPARENCY

- To help manage the overall SSL system it would help to have a comprehensive database of SSL CAs, the regional governing bodies that oversee them, and the policy and legislation under which they operate within their jurisdiction. The Tractis[14] database currently attempts to compile such data by country. The database is very incomplete at this time, however, so encouraging wider adoption of the Tractis or a similar database is crucial. Such a database:
    - Would provide system transparency for users, which could help to restore confidence in the system.
    - Would need to be translated into multiple languages (currently Tractis is in Spanish).
    - Should have data provided by CAs, and governing bodies should compel them to do so.
- Task the global governing body with eliminating the black market business of generating certificates for parties other than those legally owning a domain. Utilizing this market of "certificates for hire," unauthorized parties and US law enforcement[15] for use in monitoring the online activities of citizens. The existence of this "dark trade" does not bode well for systems where trust is placed in CAs if those CAs cannot be trusted.
    - What role does (or could) the broken CA system play in the increasing use of infowar?

SYSTEM DESIGN

- Support the research and creation of new, effective mechanisms for users of the system to verify the validity of certificates and components within the system.
    - The Electronic Frontier Foundation (EFF) continues to shine a spotlight on these issues with its SSL Observatory[16] and is investigating possible solutions.[17]
    - Further exploration of how DNSSEC could be used. This would bundle the certificate system with DNS, allowing users to retrieve certificate information along with DNS look-up results, which could then be cross-checked with CA information for a given site.
    - Explore the strengths of Moxie Marlinspike's Convergence[18] proposal and evaluate it as a possible solution for users. Convergence uses a browser plugin to query multiple third parties (notaries) and gets them to evaluate the SSL certificate and then compares the results, thus casting a wider net for the trust evaluation of the certificate.
    - Google's certificate "pinning" system for Chrome. Could this be expanded or adopted by other web browsers? Chrome has also recently rolled out DNSSEC authenticated HTTPS for users as an

13 http://csrc.nist.gov/

14 https://www.tractis.com/countries/

15 http://www.wired.com/threatlevel/2010/03/packet-forensics/

16 https://www.eff.org/observatory

17 https://www.eff.org/deeplinks/2011/08/iranian-man-middle-attack-against-google

18 http://convergence.io/

experimental feature.[19]

- Review the trust mechanisms inherent in the SSL CA system's "chain of trust model;" The PGP/GPG web-of-trust model may be an attractive model here.[20]
- Audit of the procedures web browsers are using to trigger alerts about SSL certificates.
- Include more information in the browser alerts that are triggered when a website has a SSL certificate error. This would allow users to make more informed decisions about whether to continue to the requested site, in the process educating users about the errors they're seeing, which will hopefully lead to greater and more accurate reporting of these errors as they occur.

SSL/TLS/HTTPS SYSTEM IMPLEMENTATION

- The revocation system is profoundly flawed and defaults to "fail open." This means that if the revocation list managed by the OCSP or the CAs are unreachable by browsers checking certificates on the behalf of users requesting a site, they default to secure (with some caveats depending on the browser warnings) instead of having a "hard fail," and defaulting the certificate as possibly untrusted. Hackers attempting MitM attacks against users can demonstrably exploit this — the various web browsers handle and denote this differently, but it is a shared issue. Browsers should change this policy to "fail closed" instead of the current practice of "failing open."
- Web browsers are frequently slow to push out updates in response to crises like DigiNotar, and initially ask users to manually update their trusted CAs, which is less likely to effectively assist individuals during the windows of heightened vulnerability, as most users will not manually alter their browser settings. This issue is compounded for mobile browsers, where the lag in updates from browser and app developers is even greater.
- Adding to the risk mobile users face from slower updates from browser and app developers following a compromise of a CA is the fact that most mobile platforms do not allow users to manually manage the SSL certificates that they trust. However, in response to DigiNotar, The Guardian Project recently released its CACertMan app for Android,[21] which allows users with rooted Android devices to do just this.

EDUCATION

- The current system is not only flawed, it is also complex. There is a need to educate users on the mechanisms used on different platforms, applications, and browsers, and show them how to ensure their systems are up to date. This could be accomplished by:
    - The production of a matrix of how common platforms, software, applications, browsers implement SSL, with recommendations for users, would be useful.
    - Teach users how to read certificates, particularly certificate alerts for revoked, expired, or unauthenticated certificates.
    - Remind web café customers that they should close out any previous users' web browsing sessions and review the accepted certificate preferences. Previous users may have accepted unwanted or unauthorized certificates either permanently or temporarily during their session.

19 http://www.imperialviolet.org/2011/09/19/dnsseclive.html

20 For more information about the PGP/GPG see: https://www.accessnow.org/page/-/docs/GPG_Guide_for_Secure_Communications.pdf

21 https://guardianproject.info/?s=cacertman

- Highlight the particular issues for mobile devices and browsers and create more tools for end users.
- As we've seen with the comodohacker's actions, there is a need for tailored education and outreach for users in Iran and other uniquely targeted civil society communities.

CONCLUSION

It was the "trusted third-parties," the CAs, that originally gave the SSL cryptosystem its strong design for use as a verifier to confer enough trust in users to have confidence in handing over their login credentials to a site to complete the two-way authentication cycle. Now, however, it is these same CAs that have become the SSL cryptosystem's greatest weakness. The CA "trusted third-party" design has introduced a weakest-link-in-the-chain problem where a breach of a single irresponsible CA, such as DigiNotar, compromises the whole cryptosystem and endanger all who use it. While technical re-implementations and patches of SSL as well as entire replacement cryptosystems are being proposed and developed, such solutions can only be realized in the long term due to the fact that new technology adoption is a slow process even when a system is critically under threat. However, there is still hope for the SSL CA cryptosystem. There are many policy and procedural changes outlined in this document that can be quickly mandated, adopted, implemented, and enforced to strengthen the weakest aspects of the SSL cryptosystem.