Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Informatikstrategieorgan Bund ISB
Informatiksicherheit SEC

Rolf Oppliger

28. Oktober 2011
(revidiert am 4. Mai 2012)

Technologiebetrachtung

Angriffe auf Zertifizierungsdiensteanbieter und Auswirkungen

1 Einleitung

In der jüngeren Vergangenheit sind verschiedene etablierte und von den Browser-Herstellern als vertrauenswürdig anerkannte Zertifizierungsdiensteanbieter (CSPs) angegriffen und in mindestens zwei Fällen (Comodo und DigiNotar) auch kompromittiert worden. Dabei ist es den Angreifern gelungen, falsche SSL/TLS-Server-Zertifikate auszustellen, mit denen z.B. in grossem Stil Man-in-the-Middle (MITM) Angriffe durchgeführt werden können. Im Rahmen dieser Technologiebetrachtung wird aufgezeigt, was passiert ist und welche Auswirkungen die Angriffe auf die Ausgestaltung von heutigen und zukünftigen Public Key Infrastrukturen (PKIs) möglicherweise haben werden.

2 Angriffe

Nachdem während Jahren die Sicherheit von CSPs und PKIs diskutiert worden ist und dabei primär sowohl die (kryptografische) Fälschungssicherheit von Zertifikaten als auch die Resistenz gegenüber falsch ausgegebenen Code-Signierzertifikaten im Mittelpunkt der Diskussion gestanden sind, hat Comodo[1] im März 2011 bekanntgegeben, dass es Angreifern gelungen ist, über mindestens 2 kompromittierte italienische Reseller (GlobalTrust.it und InstantSSL.it) 9 falsche SSL/TLS-Server-Zertifikate auszustellen. Diese Bekanntgabe hat international grosses Aufsehen erregt und die Sicherheitdiskussion neu angestossen. Die Bekanntgabe der niederländischen Firma DigiNotar[2], dass sie im Juli 2011 auch Opfer eines grossangelegten Angriffs geworden sei, hat die Diskussion weiter verschärft. Interessanterweise ist DigiNotar nicht nur von einer akkreditierten Stelle auditiert und zertifiziert worden, sondern sie hat mit PKIoverheid auch eine PKI für den niederländischen Staat betrieben (dieser Teil ist

[1] Comodo (http://www.comodo.com) ist ein weltweit führender CSP, der unter anderem auch verschiedene Klassen von SSL/TLS-Server-Zertifikaten ausgibt. Schätzungen zufolge liegt der Marktanteil von Comdo hier weltweit bei 20 - 25%.

[2] DigiNotar B.V. (http://www.diginotar.nl) ist eine Tochterfirma von VASCO Data Security International, Inc. (Vasco) gewesen.

vom Angriff allerdings nicht betroffen gewesen). Im Falle von DigiNotar sind 513 falsche SSL/TLS-Server-Zertifikate ausgestellt worden. Zum Teil handelt es sich dabei um Extended Validation (EV) Zertifikate, so dass hier durchaus von einem ernstzunehmenden Vorfall im PKI-Bereich gesprochen werden muss. Kurze Zeit nach Bekanntwerden des Vorfalls hat Vasco DigiNotar liquidiert.

In beiden Fällen haben die betroffenen Firmen zunächst argumentiert, dass sie Opfer einer Advanced Persistent Threat (APT) geworden seien, und dass möglicherweise sogar staatliche Stellen hinter den Angriffen stehen würden. Spätere Untersuchungen haben aber gezeigt, dass die Angriffe weit weniger spektakulär verlaufen sind als ursprünglich angenommen, und dass einmal mehr nicht gepatchte Server-Systeme und zu wenig gut kontrollierte Internet-Verbindungen die Angriffe ermöglicht haben [Fox11].

3 Auswirkungen

Der sichere Einsatz von Kryptosystemen mit öffentlichen Schlüsseln (sog. „Public Key“-Kryptografie) steht und fällt mit der Sicherheit der entsprechenden CSPs und PKIs[3]. Entsprechend ist die Sicherheit von CSPs und PKIs immer schon ein Thema gewesen, mit dem sich Sicherheitstechniker befasst haben. Im Mittelpunkt des Interesses sind dabei Szenarien gestanden, bei denen entweder Zertifikate (über Schwachstellen in der Kollisionsresistenz der eingesetzten kryptografischen Hashfunktionen[4]) gefälscht oder Code-Signierzertifikate missbraucht werden. Im zweiten Fall erlaubt – wie der Stuxnet-Wurm gezeigt hat [Lan11] – ein solches Zertifikat z.B. das Einbringen von Malware in Form digital signierter Treibersoftware in ein Betriebssystem. Die jüngsten Angriffe auf CSPs haben nun aber gezeigt, dass auch die Kompromittierung eines CSP zwecks Ausgabe falscher Zertifikate eine reale Bedrohung darstellt. Wie einleitend erwähnt, lassen sich mit Hilfe von falschen SSL/TLS-Server-Zertifikaten grossflächige MITM-Angriffe durchführen. Wenn sich ein Internet-Banking-Kunde mit Hilfe des Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) Protokolls auf einen Bankenserver verbinden will und es einem Angreifer gelingt, den Kunden auf einen von ihm kontrollierten Server umzuleiten und dem Browser im Rahmen des SSL/TLS-Verbindungsaufbaus ein gültiges Zertifikat zuzustellen, dann wird der Browser dieses Zertifikat ohne Rückfrage akzeptieren und der Angreifer kann sich als MITM in die Kommunikationsbeziehung zwischen Browser und Server einbringen. Er hat dann die volle Kontrolle über die übertragenen Daten und kann diese auch entschlüsseln und im Klartext aufzeichnen. Damit können solche Angriffe genutzt werden, um staatliche Überwachungen im Internet durchzusetzen [SS10]. So sind wahrscheinlich auch die falschen DigiNotar-Zertifikate im Iran zur Überwachung der Kommunikation von Oppositionellen in sozialen Netzwerken (insbesondere Facebook und Twitter) genutzt worden.

Wenn – wie in den vorliegenden Fällen – falsche Zertifikate ausgegeben werden, dann gilt es zunächst einmal zwei Punkte zu beachten:

- Auf der einen Seite versagen für solche Zertifikate alle im Einsatz stehenden Zertifikatsrevoziermechanismen auf der Basis von Sperrlisten (CRLs und/oder OCSP-Abfragen). Ein falsches (d.h. fälschlicherweise ausgegebenes) Zertifikat

[3] In diesem Sinne stellen die CSPs bzw. PKIs eine Achillesverse der „Public Key“-Kryptografie dar.

[4] Dieser Punkt wird z.B. in der „Technologiebetrachtung: Kollisionsresistenz und Brechung kryptografischer Hashfunktionen“ vom 4. August 2010 vertieft.

ist nicht zwingend gesperrt und entsprechend ist es auch nicht als solches erkennbar. Hier bräuchte es eine Unterscheidungsmöglichkeit für autorisierte (d.h. berechtigterweise ausgegebene) und nicht autorisierte Zertifikate. Allenfalls könnte hier ein „Whitelisting“ oder eine Art „Clearance“ korrekt abgewickelter Bestell- und Bezahlprozesse weiterhelfen. Allerdings wären solche Ansätze auch nicht resistent gegenüber Insider-Angriffen.

- Auf der anderen Seite hat sich gezeigt, dass das (zentralistische und hierarchische) Vertrauensmodell von ITU-T X.509 grundsätzlich problematisch ist. Wird in diesem Modell ein CSP bzw. eine als vertrauenswürdig anerkannte Root CA kompromittiert, dann sind davon alle Entitäten betroffen, die sich auf diese CA berufen (im Extremfall können das alle Internet-Benutzer sein). Sicherheitstechnisch sitzen alle im gleichen Boot und die Wahrscheinlichkeit, dass eine Root CA kompromittiert wird, steigt mit der Länge der Liste. Werden z.B. n Root CAs $CA_1,\ldots,CA_n$ als vertrauenswürdig anerkannt und wird jede dieser Root CAs mit einer Wahrscheinlichkeit p_i (für Root CA_i) kompromittiert, dann entspricht die Wahrscheinlichkeit P, dass keine Root CA kompromittiert wird, dem Produkt aller $(1 - p_i)$ für $i = 1,\ldots,n$, d.h. $P = \prod_{i=1,\ldots,n}(1 - p_i)$. Wenn für alle Root CAs die Wahrscheinlichkeit p_i gleich ist, dann lässt sich P auch als $(1-p_i)^n$ berechnen. Umgekehrt beträgt die Wahrscheinlichkeit1-P, dass Probleme (im Sinne von mindestens einer kompromittierten Root CA) auftreten. Damit ist ein Simulationsmodell gegeben, mit dem man unter anderem zeigen kann, dass sich für realistische Werte für p_i bzw. p die Wahrscheinlichkeit, dass Probleme auftreten, mit steigendem n relativ schnell 1 annähert. Für $p = 0.01$ und $n = 100$ ($n = 200$) beträgt die Wahrscheinlichkeit z.B. bereits 0.64 (0.87).

Nach diesen Vorbemerkungen stellt sich die Frage, welche Vorkehrungen man treffen kann, um unter den gegebenen Umständen MITM-Angriffe bestmöglichst zu verhindern. Weil es nur wenig Lösungsansätze zur Verhinderung von MITM-Angriffen (z.B. [OHB08]) gibt, wird man versuchen müssen, MITM-Angriffe für den Angreifer möglichst schwer und aufwändig zu machen. Dabei gilt es zu unterscheiden, ob man am Vertrauensmodell Änderungen vornehmen kann oder nicht.

- Kann man am Vertrauensmodell keine Änderungen vornehmen, dann empfiehlt es sich, mit vorwiegend leeren Listen vertrauenswürdiger Root CAs bzw. mit einer selektiven Aufnahme von nur bestimmten Root CAs zu arbeiten. Google nutzt diese Möglichkeit bereits seit Chrome Version 13 unter dem Begriff „Public Key Pinning“. Will man den Ansatz auf beliebige Domänen verallgemeinern, dann bietet sich eine Verbindung zum Domain Name System (DNS) an. So ist z.B. im Rahmen der IETF-Arbeitsgruppe DNS-based Authentifcation of Named Entities (DANE) eine Möglichkeit entwickelt und für die Einreichung in die Internet-Standardisierung vorbereitet worden[5], mit der man im DNS für Domänen bestimmte Zertifikate und/oder öffentliche Schlüssel festlegen und damit autorisieren kann. Kompromittierte CSPs können dann nicht mehr Server-Zertifikate für beliebige Domänen ausstellen, so dass sich die Auswirkungen von erfolgreichen Angriffen in Grenzen halten lassen. Die Abfragen entsprechender TLSA Resource Records sind dann ihrerseits idealerweise mit DNS Security (DNSSEC) abzusichern.
- Kann man am Vertrauensmodell Änderungen vornehmen, dann kommen grundsätzlich neue Lösungsansätze in Frage. Hier böte sich ein Vertrauensmodell an,

[5] Internet-Draft, Using Secure DNS to Associate Certificates with Domain Names for TLS, September 27, 2011, draft-ietf-dane-protocol-12

in dem Kompromittierungen auch nur lokale Auswirkungen haben. Ein solches Modell muss zwingend verteilt sein und dynamische Vertrauensbeziehungen unterstützen[6]. Forscher der Carnegie Mellon Universität haben z.B. gezeigt, dass Angriffe meist lokal stattfinden, und dass man falsche Zertifikate deshalb im Abgleich mit geografisch verteilten Notariatsdiensten feststellen kann. Auf dieser Idee basierend haben sie 2008 mit Perspectives[7] eine Prototypimplementierung als Firefox-Erweiterung entwickelt [WAP08]. Die Idee ist 2011 von Moxie Marlinspike aufgegriffen worden, der mit Convergence ebenfalls eine Firefox-Erweiterung entwickelt und an der Black Hat-Konferenz vorgestellt hat. Es wird sich zeigen, ob derart verteilte Ansätze eine brauchbare Alternative zu konventionellen ITU-T X.509-basierten PKIs darstellen.

4 Schlussfolgerungen und Ausblick

Wie jedes sozio-technische System verfügt auch ein CSP über Schwachstellen und Verwundbarkeiten, die im Rahmen von Angriffen adressiert und (mehr oder weniger gezielt) ausgenutzt werden können. Dabei beziehen sich die Schwachstellen und Verwundbarkeiten weniger auf die eingesetzten kryptografischen Verfahren und Mechanismen als auf die Schnittstellen zu den entsprechenden Zertifikatsausstell- und -ausgabeprozessen. Angriffe sind hier denkbar und – wie die jüngsten Angriffe dokumentieren – auch realisierbar. Als Analogie kann man einen Notengeldfälscher betrachten: Dieser kann entweder Notenscheine fälschen oder – was allerdings komplizierter und aufwändiger ist – in eine Notendruckzentrale einbrechen und die dort installierten Maschinen zur Ausgabe von regulären Notenscheinen missbrauchen. Es liegt auf der Hand, dass die zweite Möglichkeit zwar schwieriger zu realisieren dafür aber umso einträglicher ist. Ein analoger Angriff ist jetzt im PKI-Bereich gelungen und es ist möglich und wahrscheinlich, dass solche und ähnliche Angriffe in Zukunft wieder gelingen werden. Entsprechend lohnt es sich, solche Möglichkeiten in die Überlegungen zur Ausgestaltung zukünftiger PKIs mit einzubeziehen.

Abkürzungen

APT	Advanced Persistent Threat
CRL	Certificate Revocation List
CSP	Certification Service Provider
DANE	DNS-based Authentication of Named Entities
DNS	Domain Name System
DNSSEC	DNS Security
EV	Extended Validation
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
MITM	Man-in-the-Middle
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastruktur
RR	Resource Record
SSL	Secure Sockets Layer

[6] Moxie Marlinspike hat im Rahmen eines Vortrages an der diesjährigen Black Hat-Konferenz dafür den Begriff „trust agility“ also „Vertrauensagilität“ geprägt.

[7] http://perspectives-project.org

TLS Transport Layer Security

Referenzen

[Fox11] Fox-IT, DigiNotar Certificate Authority breach “Operation Black Tulip”, Interim Report, September 5, 2011

[OHB08] Rolf Oppliger, Ralf Hauser und David Basin, SSL/TLS Session-Aware User Authentication, *IEEE Computer*, Vol. 41, No. 3, 2008, pp. 59 – 65

[Lan11] Ralph Langner, Stuxnet: Dissecting a Cyberwarfare Weapon, *IEEE Security & Privacy*, Vol. 9, No. 3, 2011, pp. 49 – 51

[SS10] Christopher Soghoian und Sid Stamm, Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL, *Proceedings of the 10th Privacy Enhancing Technologies Symposium (PETS 2010)*, Berlin, Deutschland, 21. – 23. Juli 2010

[WAP08] Dan Wendtandt, David G. Andersen und Adrian Perrig, *Perspectives:* Improving SSH-style Host Authentication with Multi-Path Probing, *Proceedings of the USENIX 2008 Annual Technical Conference (ATC 2008),* USENIX Association, Berkeley, CA, 2008