SSL-Sicherheit in Gefahr

Der Einbruch bei DigiNotar, das BEAST und die Folgen

Sowohl der Einbruch bei der Zertifizierungsstelle DigiNotar als auch die Angriffe gegen SSL-Verbindungen mit dem BEAST-Tool haben eine heftige Diskussion über die Zukunft und die Sicherheit von SSL ausgelöst. Tragen die grundlegenden Konzepte noch, oder ist es Zeit für neue, völlig andere Konzepte?

Zertifizierungstellen haben eine wichtige Funktion: Sie verknüpfen einen Schlüssel mit der Identität des Schlüsselinhabers in einem sogenannten X.509-Zertifikat. So garantieren sie die Identität des Schlüsselbesitzers.

Gefälschte Zertifikate können große Schäden verursachen

Um die Identität eines Schlüsselinhabers sicherstellen zu können, wird diese eingehend geprüft. Mit der Qualität dieser Überprüfung steht und fällt das Zertifizierungssystem. Gelingt es einem Angreifer, ein Zertifikat mit einer falschen Identität zu erlangen, kann er im Internet unter dieser falschen Identität auftreten.

Da auch die Echtheitsprüfung bei Webseiten, z.B. beim Internetbanking, auf Zertifikaten beruht, lässt sich mit falschen Zertifikaten ein erheblicher Schaden anrichten.

Vertrauenswürdige Zertifizierungsstellen sind meist voreingestellt

Welche Zertifizierungsstellen soll man nun trauen? Diese Frage stellt man sich normalerweise nicht, da ein Betriebssystem typischerweise bereits viele „Vertrauenswürdige Stammzertifizierungsstellen“ mitliefert (siehe Abbildung 1).

Darüber hinaus bringen Browser wie Mozilla Firefox und Google Chrome eigene Listen für „Vertrauenswürdige Stammzertifizierungsstellen“ mit. Hier basiert das Vertrauen ausschließlich auf der Mitlieferung im Betriebssystem oder Browser. Kaum ein Nutzer hinterfragt, warum diese Zertifizierungsstellen vertrauenswürdig sind.

Der Angriff auf Comodo

Im März 2011 ist bei Wiederverkäufern der Zertifizierungsstelle Comodo ein Hacker eingebrochen und hat unberechtigt Zertifikate (z.B. für *google.com*, *mozilla.org*, *yahoo.com*, *skype.com*, *live.com*) ausgestellt, die daraufhin umgehend für ungültig erklärt wurden. Eine Art Bekennerschreiben sowie IP-Adressen aus Log-Dateien legten den Verdacht nahe, dass der Angriff aus dem Iran erfolgte.

Der Einbruch bei DigiNotar

Im Juni 2011 wiederum brach wahrscheinlich derselbe Hacker in die Zertifizierungsstelle DigiNotar ein.

Dabei wurden weit über 500 unberechtigte Zertifikate ausgestellt, unter anderem für Thawte Root CA, Equifax Root CA und VeriSign Root CA sowie für *www.sis.gov.uk* (MI6), *www.cia.gov*, *www.mossad.gov.il*, *microsoft.com*, *windowsupdate.com*, *login.live.com*, *skype.com*, *facebook.com*, *twitter.com*, *aol.com*, *android.com*, *secure.logmein.com*, *google.com*, *wordpress.com*, *addons.mozilla.org*, *login.yahoo.com* und *torproject.org*.

Die Zertifizierungsstelle DigiNotar ist mittlerweile insolvent und existiert nicht mehr. Alle Zertifikate sind inzwischen für ungültig erklärt.

Die forensische Analyse des Einbruchs bei DigiNotar

Die Firma Fox-IT hat den Einbruch forensisch untersucht (ausführliche Ergebnisse finden sich unter *www.rijksoverheid.nl/ministeries/bzk/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html*).

Besonders interessant ist die Analyse der Log-Datei des Online-Certificate-Status-Protocol-(OCSP-)Servers von DigiNotar. Da der Hacker alle Protokolleinträge über die von ihm ausgestellten Zertifikate gelöscht hatte, war am Anfang nämlich unklar, welche Zertifikate missbraucht wurden.

Was macht ein OCSP-Server?

Wann immer ein Browser bei https-Verbindungen eine Serveridentität überprüft, fragt er über OCSP bei der Zertifizierungsstelle nach, ob mit dem Zertifikat alles in Ordnung ist.

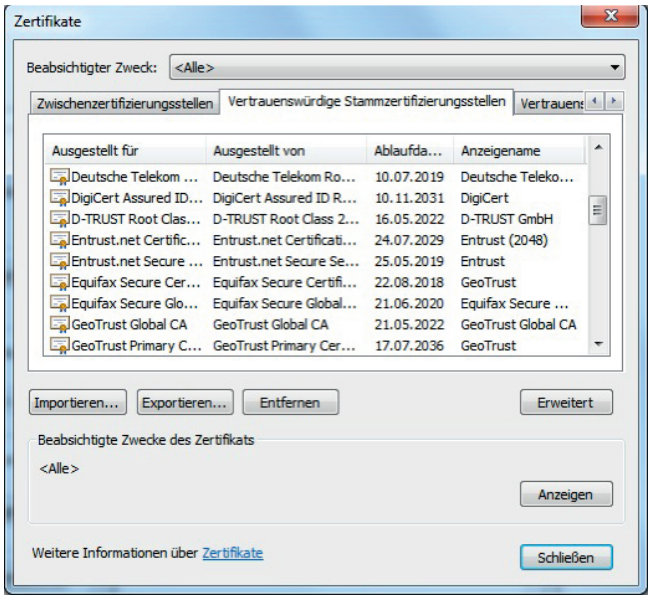

Abbildung 1: Vertrauenswürdige Stammzertifizierungsstellen in Microsoft Windows 7

Abbildung 2: Die roten Punkte markieren den regionalen Ursprung der OCSP-Abfragen während des Einbruchs bei DigiNotar. Quelle: Fox-IT, Interim Report DigiNotar Certificate Authority breach „Operation Black Tulip“ vom 5.9.2011 (www.fox-it.com/).

Wird nun ein Zertifikat mit einer Seriennummer nachgefragt, die es in der Datenbank der Zertifizierungsstelle nicht gibt, antwortet der OCSP-Server trotzdem standardkonform mit „alles ok“ (siehe Kasten RFC 2560).

Keine Unterlagen bei der Zertifizierungsstelle? Trotzdem alles ok!

In anderen Worten, wenn ein Zertifikat so aussieht, als sei es von einer Zertifizierungsstelle ausgestellt worden, sie jedoch über keinerlei Unterlagen über dieses Zertifikat verfügt, meldet sie dennoch, das alles in Ordnung sei. Und das ist auch noch standardkonform!

Die Auswertung der OCSP-Server-Logs durch Fox-IT ergab, dass über 99 % der Anfragen von IP-Adressen im Iran kamen (siehe Abbildung 2). Die IP-Adressen außerhalb des Irans gehören überwiegend zu TOR-Exit-Konten, Proxys oder VPN-Servern, also von Servern, die die eigene Herkunft verschleiern sollen.

OCSP-Server nicht erreichbar? Auch alles in Ordnung!

Es gibt mit dem OCSP aber noch ein weiteres Problem. Es kommt manchmal vor, dass ein OCSP-Server wegen Netzwerkproblemen nicht erreichbar ist. Alle Browser produzieren dann keine Fehlermeldung, sondern gehen standardmäßig von der Ordnungsmäßigkeit des Zertifikats aus.

Sicherheitsoption ist standardmäßig deaktiviert

Lediglich Firefox bietet eine Konfigurationsmöglichkeit wie in Abbildung 3 (siehe Seite 10). Das dringend erforderliche Häkchen vor der Option „Wenn eine OCSP-Server-Verbindung fehlschlägt, …“ ist aber standardmäßig nicht gesetzt.

Das BEAST-Tool: Ein weiterer Angriff auf die SSL-Sicherheit

Im September 2011 stellten die Forscher Juliano Rizzo und Thai Duong das Tool „Browser Exploit Against SSL/TLS“ (BEAST) vor. Damit lassen sich im lokalen Netz übertragene Browser-Cookies bei SSL/TLS-verschlüsselten Verbindungen wieder entschlüsseln.

Voraussetzung ist der Einsatz der eigentlich guten Verschlüsselungsalgorithmen AES oder 3DES im sogenannten CBC-Modus. Gerade AES-CBC ist ein weit verbreiteter Standard. Ein Downgrade auf den eigentlich schlechteren Algorithmus RC4 hilft als Workaround. Alle Versionen der SSL- bzw. TLS-Verschlüsselung bis TLS 1.0 (entspricht SSL 3.1) sind angreifbar. Erst mit TLS 1.1 ist der Fehler im Protokoll behoben.

Die nicht angreifbare Verschlüsselungsvariante TSL 1.1 wird bisher kaum unterstützt

Da sich Server und Browser beim Verbindungsaufbau immer auf die höchste von beiden unterstützte Verschlüs-

Auszug aus RFC 2560 „X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP“

„This specification defines the following definitive response indicators for use in the certificate status value:

- good
- revoked
- unknown

The „good“ state indicates a positive response to the status inquiry. At a minimum, this positive response indicates that the certificate is not revoked, but does not necessarily mean that the certificate was ever issued or that the time at which the response was produced is within the certificate's validity interval. (…)

The „revoked“ state indicates that the certificate has been revoked (either permanantly or temporarily (on hold)).

The „unknown“ state indicates that the responder doesn‘t know about the certificate being requested.“ (Quelle: *http://tools.ietf.org/html/rfc2560*)

selungsvariante einigen, ist es nicht ausreichend, wenn eine Seite TLS 1.1 oder TLS 1.2 unterstützt. Standardmäßig unterstützt kein aktueller Browser TLS 1.1 oder TLS 1.2. Lediglich im Internet Explorer und in Opera 8 lassen sich beide Varianten aktivieren.

Schaltet man im Internet Explorer beide Varianten ein und gleichzeitig alle alten Varianten von SSL und TLS ab, sieht man sehr schnell, welche Webserver die aktuellen TLS-Versionen unterstützen: praktisch keine.

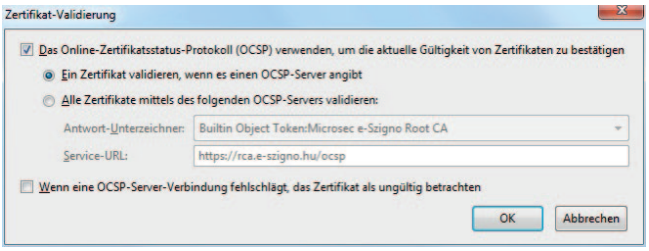

Abbildung 3: Ein Konfigurationsdialog für Einstellungen für OCSP-Abfragen. Der Dialog zeigt die Default-Einstellungen.

Technische Warnung des Bürger-CERT mit Empfehlungen vom 24.09.2011 – TW-T11/0066

„Kurzfristig ist mit Workaround-Patches der Browserfamilien zu rechnen, die die Wahrscheinlichkeit eines erfolgreichen Angriffs z.B. durch Padding mit zufälligen Zeichen verringern.

Bis dahin können Anwender mit einigen Maßnahmen die Wahrscheinlichkeit eines erfolgreichen Angriffs zwar nicht ausschließen, aber zumindest reduzieren.

Als Verteidigung gegen das Einschleusen fremden Codes in eine Verbindung empfehlen sich die folgenden Maßnahmen:

- HTTPS-Verbindungen sollten mit einem frisch gestarteten Browser durchgeführt werden
- Das Öffnen von anderen Webseiten (z.B. durch Tabs oder parallele Fenster) sollte während schützenswerter Sitzungen vermieden werden.
- SSL-Verbindungen sollten möglichst kurz gehalten und aktiv durch Ausloggen aus der Webanwendung und anschließendes Schließen des Browsers beendet werden.
- Da nach bisherigem Kenntnisstand die aufwändigen Berechnungen des Angriffs Java benötigen (nicht zu verwechseln mit JavaScript), sollten Java-Plug-ins im Browser deaktiviert werden.

Die Schwachstelle ist zwar in den TLS-Versionen 1.1 und 1.2 nicht mehr vorhanden, diese werden aber bisher von so gut wie keinem Browser unterstützt. Darüber hinaus müssen auch die Webserver-Hersteller erst diese Version kompatibel zu den Browsern entwickeln und aktivieren.“ (Quelle: *www.buerger-cert.de/archive?type=widtechnicalwarning&nr=TW-T11-0066*)

Was tun? Empfehlungen für die Praxis.

Erfreulicherweise kann man über ein Microsoft-fix-it-Tool für den Internet Information Server TLS 1.1 und höher aktivieren (*http://support.microsoft.com/kb/2588513*). Im Bereich der Open-Source-Server wie z.B. Apache wird überwiegend die OpenSSL-Bibliothek verwendet. Hier helfen vorhandene Workarounds, die man aber ausdrücklich aktivieren muss.

Alle Änderungen müssen intensiv auf Nebenwirkungen getestet werden. So wirken sich z.B. Änderungen der Konfigurationseinstellungen im Internet Explorer auf die Verschlüsselungsbibliothek des Betriebssystems (schannel.dll) aus. Das hat zur Folge, dass z.B. der Cisco AnyConnect VPN Client nicht mehr funktioniert. Denn er bedient sich der Verschlüsselungsbibliothek des Betriebssystems. Somit gelten die Änderungen auch für ihn. Zudem verwenden die Cisco-VPN-Server SSL 3.0/TLS 1.0.

Fazit: Es sind dringend grundlegende Verbesserungen nötig!

Wenn etwas nicht funktioniert, wird es schon in Ordnung sein – das ist anscheinend die Philosophie des Designs grundlegender Sicherheitsmechanismen im Public-Key-Infrastruktur-Umfeld: Ist der OCSP-Server nicht zu erreichen, ist das Zertifikat bestimmt gültig. Kennt der OCSP-Server das Zertifikat nicht, darf er grundsätzlich ok melden.

Hier muss nachgebessert werden. Es geht dabei allerdings nicht einfach um Programmierfehler, sondern um fehlerhafte Konzepte.

Die Bequemlichkeit geht auf Kosten der Sicherheit

Wenn Software-Hersteller das Vertrauen in Zertifizierungsstellen mitliefern, ist das zwar bequem für den Nutzer, aber unter Umständen katastrophal für die Sicherheit.

Das Vertrauen in Zertifizierungsstellen selbst zu konfigurieren, setzt einen mündigen und sachkundigen Nutzer voraus. Nur: Wer vermittelt diese Fachkunde?

Die Unternehmen sind gefragt: https-Server müssen mindestens mit TLS 1.1 arbeiten

Alle Server, die SSL verwenden, müssen TLS 1.2 beherrschen oder andere Workarounds implementieren, damit das BEAST nicht angreifen kann.

Dieses Problem ist für den Nutzer allein nur schwer zu lösen, da er keinen Einfluss auf die Serverkonfiguration hat. Alle Unternehmen sollten ihre https-Server daher so schnell es geht mindestens TLS-1.1-tauglich machen oder entsprechende Workarounds aktivieren!

Prof. Dr. Rainer W. Gerling

Rainer W. Gerling ist Datenschutz- und IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft und Honorarprofessor für IT-Sicherheit an der Hochschule München.