Schwachstellen der SSL/TLS Verschlüsselung im Internet

10.07.2013, 16:10 | IT, New Media & Software

Pressemitteilung von: *ISDSG – Institut für Sicherheit und Datenschutz im Gesundheitswesen*

Bild: Jäschke

Das TLS-Protokoll (besser unter seinem alten Namen SSL bekannt) bildet einen, wenn nicht sogar den entscheidenden, Pfeiler vieler Sicherheitsarchitekturen, die über das Internet kommunizieren. Seien es Webseiten, E-Mail-Programme oder VPN. Doch in letzter Zeit kommen immer wieder Zweifel daran auf, wie sicher das Protokoll wirklich ist.

TLS (Transport Layer Security), zu diesem Zeitpunkt noch SSL (Secure Sockets Layer), wurde 1994 neun Monate nach Mosaic, dem ersten verbreiteten Webbrowser, von Netscape veröffentlicht. Im Januar 1999 wurde SSL mit der Standardisierung durch die IETF (Internet Engineering Task Force) in TLS umbenannt. Die aktuelle Version 1.2 von TLS wurde im August 2008 verabschiedet.

Bei TLS handelt es sich um ein hybrides Verschlüsselungsprotokoll. Dies bedeutet, dass die beiden Kommunikationspartner zum Austausch eines symmetrischen Schlüssels eine asymmetrische Verschlüsselung nutzen. Die eigentliche Kommunikation findet dann mit der wesentlich schneller zu berechnenden symmetrischen Verschlüsselung statt. Bei der asymmetrischen Verschlüsselung gibt es einen öffentlichen und einen privaten Schlüssel. Wenn eine Nachricht mit dem öffentlichen Schlüssel verschlüsselt wird, lässt diese sich nur mit dem privaten Schlüssel wieder entschlüsseln. Um sicherzustellen, dass ein öffentlicher Schlüssel auch wirklich zu einer bestimmten anderen Stelle gehört, wurden CA (Certification Authority) eingeführt, die dies bestätigen können.

Wo sind nun die Schwachstellen an diesem Protokoll zu suchen? Die hybride Verschlüsselung ist technisch gesehen sicher, sofern zwei Annahmen getroffen werden:

• Es gibt nicht genügend Rechenleistung, um die Verschlüsselung mittels Brute-Force anzugreifen.
• Die Annahme der Theoretischen Informatik „P ist ungleich NP“ wird nicht als falsch bewiesen.

Demnach bleiben nur organisatorische Mängel im Zusammenhang mit den CA. Die beiden Wissenschaftler Steven Roosa (Holland & Knight LLP) und Stephen Schultze (Princeton University) zeigen in ihrem Arbeitspapier „Trust Darknet: Control and Compromise in the Internet's Certificate Authority Model“ (http://ssrn.com/abstract=2249042) verschiedene Schwachstellen des Modells auf:

• Die CA gliedern Teile ihrer Arbeit an SubCA aus. SubCA haben die Aufgabe selbst Zertifikate zu erstellen und nutzen dabei die Vertrauenswürdigkeit des CA. RA (Registration Authority) übernehmen die kritische Aufgabe der Verifizierung und prüfen, ob die Domainadresse dem Antragssteller gehört. Diese Unteranbieter stellen andere Sicherheitsanforderungen. So wurde bekannt, dass 2011 ein malaysischer SubCA kürzere Schlüssel als sein übergeordneter CA nutzte, wodurch Angreifer bekannte Schwachstellen der kurzen Schlüssel nutzen konnten und ihre Schadsoftware damit signieren konnten.

• Ein weiteres Problem ist, dass fast alle Nutzer durch die Voreinstellung ihrer Software denselben CA vertrauen müssen. Zusätzlich müssen diese CA sich ebenfalls untereinander vertrauen und auch jede Art von Webseiten authentifizieren. Zwar gibt es die Möglichkeit der Einschränkung von CA auf bestimmte Arten von Domains (z.B. nur .de). Diese wird jedoch nicht genutzt.
• In der Regel werden die Listen, die die vertrauenswürdigen CA enthalten als read-only Datenstrukturen in der Software

hinterlegt. Verliert nun ein CA seinen Status als vertrauenswürdig, weil er zum Beispiel, wie DigiNotar 2011, gehackt wurde, hat dies zur Folge, dass im Grunde jedes Softwareprodukt mit Updates versorgt oder sogar komplett neu installiert werden muss. Dies bedeutet eine enorme Inflexibilität.
• Problematisch ist auch die Unwissenheit vieler Endbenutzer über die Funktionsweise der vertrauenswürdigen CA. So zeigen Studien, dass viele Nutzer nach Einblendung des Warnhinweises Authentifizierung fehlgeschlagen die Warnhinweise ignorieren. Von einigen Forschern wird deswegen vorgeschlagen, den Nutzern die Möglichkeit, Warnmeldungen „weg zu klicken“, nicht mehr anzubieten.

Selbst eine perfekte Implementierung des spezifizierten Modells würde die bestehenden Probleme nicht lösen, sondern noch verstärken. Die gezeigten Schwachstellen können durch Veränderungen allerdings gemildert werden. Um Verbesserungen zu erreichen ist eine Veränderungen in drei Bereichen empfehlenswert. So soll die Arbeit der CA, RA und SubCA, sowie deren Verhältnisse untereinander transparenter werden. Für die Auditierung von RA und SubCA sollen dieselben Kriterien gelten, wie für CA, und mehr inhaltliche Ergebnisse der Audits öffentlich gemacht werden. Für die Selbstregulierung fordert das ISDSG, dass mit den Sicherheitsaspekten offener umgegangen und mehr Interessenvertreter mit einbezogen werden.

Viele Probleme beziehen sich auf die grundlegende Struktur des Systems. Jedoch besteht auch für Betreiber von Internetseiten, aber auch für ganz normale Nutzer, eine Chance die Sicherheit im Internet zu erhöhen. Als Webseitenbetreiber sollte auf die Vergabeweise der CA geachtet und anhand dessen entschieden werden, von wem Zertifikate bezogen werden. Als Endbenutzer ist unbedingt auf auftretende Meldungen im Browser zu achten, die auf ein erhöhtes Sicherheitsrisiko hinweisen. Jedem Internetnutzer sollte bewusst sein, dass keine Sicherheitsgarantie in der virtuellen Welt existiert und das blinde Vertrauen, genau wie auch in der physischen Welt, deplatziert ist.

Portrait

Das ISDSG – Institut für Sicherheit und Datenschutz im Gesundheitswesen in Dortmund beschäftigt sich mit allen Fragen zum Thema Informationssicherheit und Datenschutz mit Schwerpunkt auf die Akteure des Gesundheitswesens. Das Institut wurde vom Medizin-Wirtschaftsinformatiker Prof. Dr. rer. medic. Thomas Jäschke gegründet. Das Portfolio des ISDSG umfasst neben den frei zugänglichen Informationen und Dienstleistungen auch besonders ausgerichtete Angebote für Praxen und Unternehmen. Angetrieben wird das spezialisierte Team durch die fortschreitende Durchdringung der Digitalisierung in der Medizin, aufgrund der Potenziale neuer Informationstechnologien.

News-ID: 732757 • Views: 800 (Stand: 02.06.2026)

Link zur Pressemitteilung:

https://www.openpr.de/news/732757/Schwachstellen-der-SSL-TLS-Verschluesselung-im-Internet.html