Abhörsicher in die Zukunft

Das Internet bekommt mit dem TLS 1.3 einen neuen Standard für verschlüsselte Kommunikation. Forscher um Professor Marc Fischlin an der TU Darmstadt haben an der Analyse des Protokolls mitgewirkt und die kryptographischen Verfahren geprüft – sie sind effizienter und weniger fehleranfällig. Aber sind sie zukunftsfähig?

Von Boris Hänßler

Heartbleed, Triple Handshake, Crime – hinter diesen seltsamen Namen stecken Angriffe auf eines der Herzstücke des heutigen Internets: Das Transport Layer Security-Protokoll für verschlüsselte Kommunikation. Wir alle nutzen es: Wenn wir bei Google etwas suchen, in Online-Shops einkaufen oder E-Mails verschicken, werden unsere Daten damit geschützt. In der Regel können wir dem Protokoll vertrauen. Die folgenreichsten Hacker-Angriffe der letzten Jahre kamen stets zustande, weil das TLS nicht richtig implementiert wurde. Dennoch waren viele Experten mit dem Protokoll unzufrieden: Zum einen haben Forscher auch immer wieder kleinere Sicherheitslücken im Protokoll selbst entdeckt. Zum anderen war das bisherige Verfahren vielen Internet-Unternehmen zu umständlich – es war nicht schnell genug.

„Die Reduzierung der Roundtrips zählt zu den wichtigsten Neuerungen, birgt aber auch Risiken.“

Die internationale Organisation „Internet Engineering Task Force“ (IETF) hat deshalb mit dem TLS 1.3 ein neues Protokoll vorgestellt. Marc Fischlin, Professor der Informatik an der Technischen Universität Darmstadt, und sein Team waren mit ihrer Expertise für Kryptographie bei der Analyse des Standards involviert. Sie prüften während des mehrjährigen Entwicklungsprozesses, ob die vorgeschlagenen Verfahren mit ihren neuen Funktionalitäten tatsächlich sicher genug sind – und ob sie auch mit den kommenden technologischen Fortschritten noch mithalten werden.

Ein Sicherheitsrisiko, mit dem sich Fischlins Team beschäftigt, ergibt sich, weil in dem neuen Protokoll die sogenannten Roundtrips reduziert wurden. Bei einer TLS-Verbindung handeln Client – zum Beispiel der Rechner des Kunden eines Online-Shops – und der Server des Shops in mehreren Schritten eine Verschlüsselung aus. Zunächst meldet sich der Rechner des Kunden. Er sagt im übertragenen Sinne: „Hallo, ich möchte mit dir kommunizieren und folgende Verschlüsselungen biete ich an.“ Der Server sucht daraufhin einen Schlüssel aus und schickt zudem ein offizielles Zertifikat mit, das bestätigt, dass es sich tatsächlich um den Server des Shops handelt. Der Kunden-Rechner wiederum akzeptiert den Schlüssel; beide Seiten erklären nach einigen weiteren Schritten die Verhandlung für beendet und erst dann können die eigentlichen Daten ausgetauscht werden. Insgesamt besteht der technische Dialog aus sechs Einzelschritten. Ziel des neuen Protokolls war, diese Verhandlungen auf vier Schritte zu reduzieren. Das gelang den Entwicklern, indem sie jeweils zwei bisher getrennte Vorgänge zusammenlegten.

Kennen sich Client und Server bereits, weil zum Beispiel der Kunde zuvor im Online-Shop eingekauft hatte, kommunizieren beide Rechner in dem neuem TLS-Protokoll sogar sofort miteinander. Die Informatiker sprechen von einem Zero-Roundtrip, weil keine Extra-Runden bei der Verschlüsselungs-Verhandlung gedreht werden müssen. Der Rechner des Kunden identifiziert sich über ein sogenanntes „Session Ticket“, das er bei der letzten Kommunikation erhalten und gespeichert hatte – er kann mit diesem Ticket bereits seine Daten übertragen.

Die Reduzierung der Roundtrips bemerken wir als Internet-Nutzer im Alltag nicht. Schon das alte Protokoll war so schnell, dass es sich auf die Geschwindigkeit unserer Kommunikation kaum auswirkte. Anders jedoch sieht es zum Beispiel für Google aus. Die Suchmaschine verzeichnete zuletzt rund zwei Billionen Suchanfragen pro Jahr – und jedes Mal, wenn jemand die Suchmaschine in seinem Browser neu aufruft, muss sie eine Verschlüsselung mit ihm aushandeln. Die Reduzierung der Roundtrips ist für Unternehmen wie Google daher eine enorme Entlastung. „Sie gehört zweifellos zu den wichtigsten Neuerungen bei TLS 1.3“, sagt Fischlin. „Aber sie bringt auch Risiken mit sich.“

Eines dieser Risiken ist Thema einer aktuellen Studie, die Fischlin und sein Team in diesen Wochen als Konferenzbeitrag zur 2nd IEEE European Symposium

Informationen
Fachbereich Informatik
Kryptoplexität
Prof. Dr. Marc Fischlin
marc.fischlin@cryptoplexity.de
http://bit.ly/2mlTbs9

on Security and Privacy in Paris vorstellen. Darin geht es um so genannte Replay-Angriffe bei Zero-Roundtrips. Im Falle eines solchen Angriffs würde ein Hacker versuchen, das Session Ticket abzufangen. Zwar könnte er damit nicht den Inhalt der übertragenen Daten auslesen oder ändern, aber er könnte das Session Ticket nutzen, um eine Anfrage mehrmals an einen Server zu schicken. Würde ein Kunde in einem Online-Shop ein Buch bestellen, könnte der Hacker die Bestellung tausendmal wiederholen.

In dem Protokoll TLS 1.3 sollten deshalb Online-Shops oder andere Dienstleister prüfen, ob eine Anfrage des Clients zum gleichen Ergebnis führt wie die Anfragen zuvor – ob zum Beispiel das gleiche Produkt bestellt wird. Falls ja, wird das Session Ticket für ungültig erklärt. Server und Client müssen einen neuen Schlüssel aushandeln, und damit ist der Hacker machtlos. Fischlin und sein Team konnten nachweisen, dass das Protokoll selbst bei allen möglichen Sonderfällen die relevanten Sicherheitsanforderungen erfüllt. „Risiken gibt es zwar nach wir vor, aber wir schätzen sie für so gering ein, dass wir den neuen Standard für robust halten“, sagt Fischlin.

Die Darmstädter Forscher blicken auch auf zukünftige Funktionen für TLS 1.3. Virenschutz-Hersteller wünschen sich zum Beispiel, dass ihre Software verschlüsselte Informationen durchsuchen dürfen – nicht erst die entschlüsselten Dateien. „Wir arbeiten an Verfahren, die das ermöglichen“, sagt Fischlin. „Eine Option wäre zum Beispiel, direkt auf der Verschlüsselung zu rechnen. Der Virenscanner würde anhand der Verschlüsselungsmuster erkennen, ob es sich um schadhaften Code handelt. Allerdings müssen wir verhindern, dass mit dieser Methode auch standardisierte Informationen in den Dateien wie etwa Bankdaten ausgelesen werden können.“

In ferner Zukunft wird ein weiteres Problem auf die Kryptographie-Experten zukommen: Eines Tages wird es womöglich Quanten-Rechner geben. Dann wäre das gegenwärtige Verschlüsselungsverfahren, das auf dem sogenannten Diffie-Hellman-Schlüsselaustausch basiert, hinfällig. Das Verfahren gilt als zuverlässig, weil ihm ein mathematisches Problem zu Grunde liegt, dessen Lösung für heutige Rechner zu aufwändig ist. Quantenrechner könnten es jedoch knacken. „Niemand weiß, wann es solche Rechner geben wird“, sagt Fischlin. „Aber sobald sie zur Verfügung stehen, wären die Verfahren auf einen Schlag unsicher. Darauf müssen wir vorbereitet sein“.

Ein möglicher Ersatz wäre das sogenannte Learning with errors (LWE)-Problem. Es ist vermutlich von Quantenrechnern nicht lösbar. Warum setzt man es also nicht jetzt schon ein? „Das würde die Protokolle wieder verlangsamen“, sagt Fischlin und lächelt. „Daran sieht man: So schnell gehen uns die Forschungsthemen in der Kryptographie nicht aus.“

Der Autor ist Wissenschaftsjournalist.

Abbildung: Katrin Binner

Forscht zu Kryptographie, Sicherheit und Komplexitätstheorie: Professor Marc Fischlin (re.)