Spätestens seit den Snowden-Enthüllungen ist klar, wie massenhaft der weltweite Internetverkehr angezapft und ausgewertet wird. Letzteres ist oftmals zu leicht – schließlich gibt es ein bewährtes Mittel gegen Mitleser: Verschlüsselung. Vor über 20 Jahren wurde mit der ersten Version des Netscape-Browsers die Erweiterung „Secure Socket Layer" (SSL) eingeführt, welche inzwischen als Transport Layer Security (TLS) bezeichnet wird. Mit TLS können Browser einen verschlüsselten Tunnel zum Server aufbauen, den ein Lauscher nur mit erheblichem Aufwand anzapfen kann.

Verschlüsselung ist nicht nur sinnvoll, wenn es um vertrauliche Informationen wie Zugangsdaten oder den digitalen Kontoauszug geht. Filtern Sie die Chronik Ihres Browsers einmal gezielt nach unverschlüsselt übertragenen http://-Aufrufen. Möchten Sie wirklich, dass Unbekannte bei minimalem Aufwand erfahren können, welche Artikel Sie auf Nachrichtenseiten lesen, für welche Produkte Sie sich beim Amazon-Shopping interessieren und welche Termine Sie bei Doodle planen? Zusammengenommen ergibt sich daraus ein umfangreiches Interessenprofil. Wird eine Website hingegen über HTTPS ausgeliefert, sieht ein Datenschnüffler zwar, dass Sie Datenpakete mit einer bestimmten Domain austauschen; URL und Inhalt der Datenpakete sind jedoch verschlüsselt.

Damit eine Webseite über HTTPS erreichbar ist, benötigt der Webmaster ein Zertifikat mit der Unterschrift eines Herausgebers, den die gängigen Browser als vertrauenswürdig einstufen. Zum einen gibt es allerhand kommerzielle Anbieter wie Symantec oder Thawte, die mindestens einen zweistelligen Eurobetrag pro Jahr und Zertifikat verlangen. Zum anderen gibt es kostenlose Zertifikate der Zertifizierungsstellen StartSSL aus Israel und WoSign aus China. Diese führen jedoch eher ein Schattendasein, da sie im Wesentlichen auf Mund-zu-Mund-Propaganda angewiesen sind.

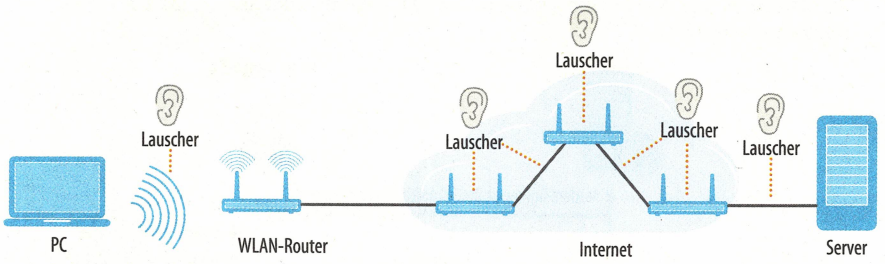
So wird ein großer Teil des Internetverkehrs zwanzig Jahre nach der Einführung von SSL/TLS immer noch im Klartext übertragen – laut der Statistikseite HTTP Archive rund drei Viertel. Einer der Gründe dafür ist, dass SSL den Ruf weg hat, teuer und kompliziert zu sein. Damit soll jetzt Schluss sein.

Zertifikate für alle!

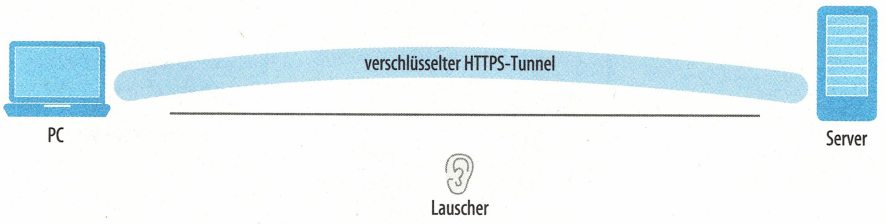
Vertreter von Netz-Größen wie Mozilla, Akamai, Cisco haben sich zur Internet Security Research Group (ISRG) zusammengefunden, um kostenlosen SSL-Zertifikaten zum Durchbruch zu verhelfen. Ein Vertreter der Electronic Frontier Foundation (EFF) nimmt eine Wächterfunktion ein. Im Zentrum der Initiative „Let's Encrypt" (siehe c't-Link) steht eine Zertifizierungsstelle (Certificate Authority, CA), die Domain-Inhabern kostenlos SSL-Zertifikate ausstellt. Es handelt sich dabei um sogenannte Domain-Validated-Zertifikate (DV), die für die meisten Zwecke ausreichen (siehe Kasten „Kleines Zertifikats-Einmaleins" auf Seite 138). Um ein solches zu erhalten, muss man gegenüber der CA lediglich beweisen, dass man die Domain unter Kontrolle hat, auf die das Zertifikat ausgestellt werden soll.

Datenübertragung mit HTTPS

Bei der unverschlüsselten HTTP-Übertragung kann ein Lauscher an vielen Stationen mithören.

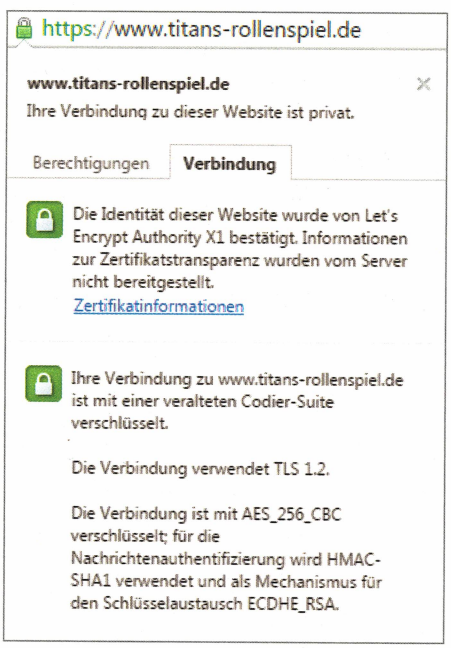


Surft man über HTTPS, baut der Browser einen verschlüsselten Tunnel zum Zielserver auf.



Konfigurationsroboter

Der vielleicht wichtigste Impuls der Initiative ist ein neu entwickeltes, offenes Protokoll, welches das Ausstellen von Zertifikaten automatisierbar macht. Es trägt den etwas sperrigen Namen Automated Certificate Management Environment, kurz ACME. Beantragt man als Webseiten-Betreiber ein Let's-Encrypt-Zertifikat, läuft das seitens der CA ohne menschliches Eingreifen ab – und somit ohne Personalkosten. Man installiert auf dem Server den Let's-Encrypt-Client, der über das ACME-Protokoll mit dem Tool Boulder spricht, welches auf der CA-Infrastruktur läuft. Der Client fordert ein Zertifikat für eine bestimmte Domain an, woraufhin ihm die CA eine Aufgabe stellt, die er lösen muss, um seine Hoheit über die Domain zu beweisen. Das kann zum Beispiel eine Datei sein, die über einem von der CA vorgegebenen Pfad unter der Domain erreichbar sein muss. Diese Aufgabe löst der Client automatisch. Anschließend holt er sich das Zertifikat ab und konfiguriert auf Wunsch selbstständig den Server. So einfach war HTTPS noch nie.



Let's Encrypt stellt kostenlos SSL-Zertifikate aus, welche die Browser als vertrauenswürdig einstufen.

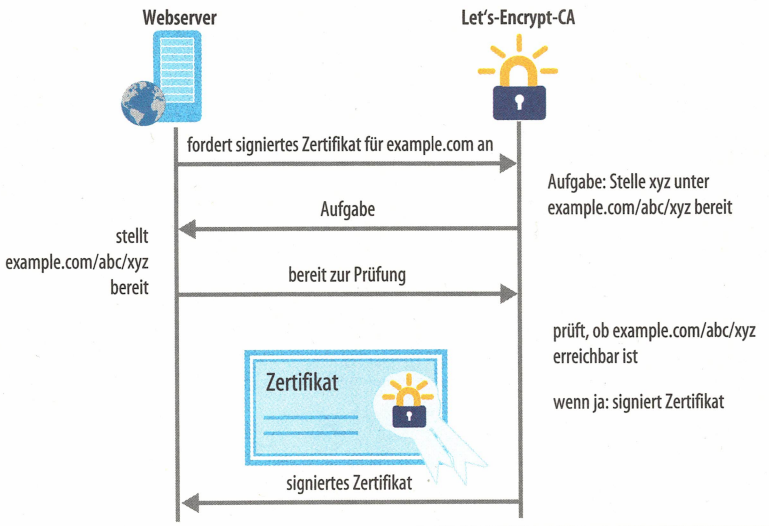
Die automatische Konfiguration funktioniert aktuell unter Ubuntu-Linux in Kombination mit Apache oder nginx. Windows-Server unterstützt der offizielle Client nicht. Gegenüber c't erklärte Josh Aas, Executive Director der ISRG, dass man zwar selbst keinen Windows-Client entwickle, einen solchen aber begrüßen würde. Da das Protokoll offen ist, kann sich jeder daran versuchen, einen ACME-Client zum Beispiel für Microsoft-Server zu bauen. Erste Versuche, etwa mit PowerShell-Skripten, findet man bereits bei Github (siehe c't-Link). Schon jetzt besteht die Möglichkeit, ein mit dem Linux-Client generiertes Zertifikat auf einen Windows-Server zu übertragen. Wie man Servern mit Let's Encrypt das Verschlüsseln beibringt, erfahren Sie en détail auf Seite 146.

Pro und Contra HTTPS

Wer seine Website über HTTPS ausliefert, tut nicht nur seinen Nutzern einen echten Gefallen, er wird auch noch belohnt: Über HTTPS erreichbare Sites werden von Google besser bewertet und tauchen weiter oben in den

Gratis-Zertifikate von Let's Encrypt

Der Let's-Encrypt-Client auf dem Webserver lässt ein zur Domain passendes Zertifikat von der CA signieren. Dafür muss er der CA beweisen, dass er für die Domain zuständig ist.



Suchergebnissen auf. Bereits auf seiner Entwicklerkonferenz Google I/O im Jahr 2014 forderte das Unternehmen sogar, dass sämtlicher Web-Traffic TLS-verschlüsselt übertragen werden soll – ein Ziel, das durch Let's Encrypt weiter in greifbare Nähe rückt. Die Medaille hat allerdings auch eine Kehrseite: HTTPS bedeutet ganz oder gar nicht. Wird eine Website verschlüsselt ausgeliefert, darf sie ausschließlich HTTPS-Ressourcen nachladen. Andernfalls zeigt der Browser eine Warnung an, dass die Seite sichere und ungesicherte Inhalte zu mischen versucht (Mixed Content).

Wer externe Elemente wie Werbung oder Anbindungen an soziale Netzwerke einbindet, muss sicherstellen, dass sie über HTTPS abgerufen werden – oder auf diese Elemente verzichten. Das wirkt sich insbesondere auf Online-Werbung aus, da noch nicht alle Anzeigenkunden in der Lage sind, ihre Marketing-Inhalte verschlüsselt auszuliefern [1]. Die Anzahl der Kunden, die bei Anzeigenetzwerken wie DoubleClick oder AdSense einen HTTPS-Werbeplatz buchen können, ist also kleiner als bei unverschlüsselten Sites. Wer Werbung auf seiner Site anzeigt, muss daher momentan noch damit rechnen, dass die Werbeeinnahmen zurückgehen. Die Chancen stehen aber gut, dass sich dies mit zunehmender Verbreitung von HTTPS ändert.

Auch wer Apps entwickelt, sollte über den Einsatz verschlüsselter Verbindungen nachdenken, um die Daten seiner Anwender zum Beispiel in öffentlichen Netzen wie dem Hotspot im Bahnhofscafé zu schützen. Apple erklärt in der Entwicklerdokumentation zu iOS 9, dass neue Apps exklusiv HTTPS zur Kontaktaufnahme einsetzen sollen. Bestehende Apps sollten „so viel wie möglich" Datenverkehr verschlüsseln.

Weitersagen!

Wenn alles nach Plan läuft, hat Let's Encrypt bereits den regulären Betrieb aufgenommen, wenn Sie diesen Artikel in den Händen halten. Um die Krypto-Revolution voranzutreiben, können Sie selbst aktiv werden: Liefern Sie etwaige eigene Websites über HTTPS aus und machen Sie Admins in Ihrem Umfeld auf Let's Encrypt aufmerksam! Aber auch Anwender sollten HTTPS-Verschlüsselung schätzen lernen und wissen, worauf sie bei dessen Nutzung achten müssen. Genau darum bemühen wir uns in dem nächsten Artikel: Er erklärt leicht verständlich, woran man sichere Verbindungen erkennt und wie man möglichst oft auf den HTTPS-Versionen der Sites landet. Sie dürfen ihn gerne weitergeben, wir haben ihn unter die Creative-Commons-Lizenz gestellt. (rei@ct.de)

Literatur

[1] Herbert Braun, Werbung versus Sicherheit, Probleme bei der Umstellung von Websites auf HTTPS, c't 2/15, S. 132

c't Gratis-Zertifikate und Tools: ct.de/y6d6

Kleines Zertifikats-Einmaleins

Zertifikate sind ein elementarer Bestandteil von HTTPS: Durch sie kann man nachvollziehen, dass man tatsächlich mit dem Server spricht, den man angesteuert hat und die übertragenen Informationen nicht auf dem Transportweg manipuliert wurden. Gäbe es diesen Identitätsnachweis nicht, könnte sich ein Angreifer als Man-in-the-Middle in die verschlüsselte Verbindung einklinken.

Das Fundament des Zertifikatssystems bilden die Stammzertifikate der Zertifizierungsstellen (Certificate Authority, CA). Die Browser bringen eine lange Liste von Stammzertifikaten mit, die sie als vertrauenswürdig einstufen. Dieses Vertrauen überträgt sich auf alle Zertifikate, die von den CAs signiert wurden.

Zu jedem Stammzertifikat gehören ein öffentlicher Schlüssel und ein geheimer, den nur die CA kennt. Mit dem geheimen Schlüssel signiert die CA zum Beispiel das Zertifikat für example.com; mit dem öffentlichen kann der Browser überprüfen, dass die Signatur echt ist. Darüber hinaus gibt es sogenannte Intermediates, die das Vertrauen der CA genießen und in deren Namen Zertifikate signieren dürfen.

Möchte ein Webmaster ein als vertrauenswürdig eingestuftes Zertifikat für die Domain example.com, muss er der CA beweisen, dass er der legitime Besitzer der Adresse ist. Dafür gibt es verschiedene Abstufungen: Bei den sogenannten Domain-Validated-Zertifikaten (DV) überprüft die CA, ob der Antragsteller die Kontrolle über die Domain hat. Dazu muss er etwa eine bestimmte Datei über die Domain erreichbar machen, ihre DNS-Einträge verändern oder einen Bestätigungslink anklicken, den die CA an webmaster@example.com schickt.

Neben DV-Zertifikaten gibt es vor allem Extended-Validation-Zertifikate (EV), bei denen die CA größeren Aufwand unternimmt, um die Identität des Zertifikatsinhabers in spe zu überprüfen. Unter anderem stellt sie dabei sicher, dass ein Zertifikat für ein bestimmtes Unternehmen ausgestellt wurde und der Antragsteller Eigentümer der Domain oder zumindest nutzungsberechtigt ist. Daraus resultieren mehr Vertrauen und eine bessere Bewertung durch den Browser (siehe S. 140), was insbesondere Betreibern kommerzieller Dienste Pluspunkte bringt. Let's Encrypt stellt lediglich DV-Zertifikate aus. Diese sind für die meisten Anwendungsfälle ausreichend: Aus technischer Sicht sind sie genauso sicher wie die teuren EV-Zertifikate. Wie Sie die Sicherheit verschlüsselter SSL-Verbindungen weiter erhöhen können, erfahren Sie auf Seite 150.