Noten für SSL

von Dr. Stefan M. Ritter

Eine mit https geschützte Verbindung ist nicht zwangsläufig sicher, nur weil sie verschlüsselt ist. Es sind auch noch weitere Aspekte wichtig, zum Beispiel die Schlüssellänge und die Übereinstimmung des Domain-Namen im URL mit dem Common Name des Zertifikats. Das Firefox-Addon »SSL Validation« bewertet die Sicherheit von https-Verbindungen.

Das https-Protokoll ist der Standard für die verschlüsselte Übertragung von Daten über das Internet zwischen einem Webserver und einem Browser. Seine Grundlage sind Zertifikate, die auf dem X.509-Standard beruhen. Greift ein Browser per https auf eine geschützte Seite zu, überprüft er die Gegenstelle über ihr öffentliches SSL-Zertifikat. Zudem werden anhand der im Zertifikat hinterlegten Informationen und abhängig von den Fähigkeiten des Browsers geeignete Verschlüsselungsparameter gewählt, dazu gehören die Verschlüsselungsstärke und der Verschlüsselungsalgorithmus.

Heutige Browser zeigen eine verschlüsselte Verbindung auf ganz bestimmte Weise an. So enthält der Link der angezeigten URL in der Adreßzeile des Browsers immer das Kürzel *https://* und in der Statusleiste wird typischerweise ein kleines geschlossenes Schloß-Icon angezeigt. Da dies allein jedoch rein gar nichts über die Qualität der vorliegenden https-Verbindung aussagt, sucht man nach anderen Möglichkeiten, dem Nutzer die Stärke beziehungsweise Qualität der Verbindung deutlich zu machen.

Die einfachste Methode sind Farbcodes, die ohne weitere Details solche Hinweise geben. Sie basieren auf sogenannten EV-Zertifikaten (Extended Validation). Der Besitzer eines solchen Zertifikats hat eine aufwendige Identifizierungsprozedur durchlaufen, die Vergabepraxis ist relativ streng. Im Gegensatz dazu reicht bei den einfachen DV-Zertifikaten (Domain Validation) der Nachweis, daß der Käufer des Zertifikats der Besitzer der Domäne ist, für die er das Zertifikat erwirbt.

Liegt ein EV-Zertifikat vor, färbt sich im Firefox der Teil der Adreßleiste grün ein, in der der Herausgeber des Zertifikats ablesbar ist, beim SeaMonkey befindet sich der grüne Hinweisbereich in der Statuszeile. Dem Nutzer soll über die Farbe signalisiert werden, daß das SSL-Zertifikat und damit die besuchte Webseite besonders vertrauenswürdig ist. Man findet solche EV-Zertifikate häufig bei Online-Shops oder Bankseiten.

Calomel SSL Validation

Da jedoch im Prinzip jeder ein EV-Zertifikat erwerben kann, ist es aus Sicherheitssicht interessanter zu wissen, wie gut die aktuell ausgehandelte https-Verbindung tatsächlich ist. Dabei kommt es auf Parameter wie die Verschlüsselungsstärke, den Verschlüsselungsalgorithmus oder die Bitlänge der Signatur des Zertifikats an.

Von Calomel gibt es ein frei verfügbares Firefox Addon [1] namens *SSL Validation*, das genau solche Informationen liefert. SSL Validation liegt aktuell in der Version 0.43 vor und ist kompatibel mit Firefox 3.6 bis 4.0b6.

Die vom Add-on dargestellten Informationen zur https-Verbindung sind Gültigkeit und der Typ des Zertifikats (EV oder DV), der Common Name, der Verschlüsselungsalgorithmus und seine Bitlänge, der Signaturalgorithmus und seine Bitlänge sowie der Herausgeber/Inhaber des Zertifikats.

Das Addon beschränkt sich jedoch nicht darauf, passiv Informationen zu liefern, sondern bietet über entsprechende Konfigurationseinstellungen auch die Möglichkeit, das Verhalten des Browsers aktiv zu beeinflussen.

Bild 1: Calomel SSL-Validation für die Calomel-Homepage

So kann die Verschlüsselungsstärke (in gewissem Rahmen) eingestellt, RAM-Caching aktiviert oder die Anzeige animierter GIFs unterbunden werden. Zum Schutz der Privatsphäre ist es darüber hinaus möglich, zum Beispiel Tab-Beschriftungen oder das nicht unumstrittene Safe Browsing zu unterbinden.

Die zunächst im Vordergrund stehende Information über eine aufgebaute https-Verbindung wird über einen Toolbar-Button bereitgestellt, der sich neben der Adreßleiste befindet und ähnlich wie bei einem EV-Zertifikat einen farblichen Hinweis auf die Qualität der https-Verbindung enthält. In aufsteigenden Stufen sind dies Grau (keine Verschlüsselung), Rot, Orange, Gelb, Blau bis Grün (höchste Bewertung).

Um die jeweilige Farbe festzulegen, bewertet das Plugin die zuvor erwähnten Parameter (wie zum Beispiel den Verschlüsselungsalgorithmus) und kommt so insgesamt zu einem Scoring von maximal hundert Punkten, das der Einfachheit halber als Farbe dargestellt wird. In Bild 1 ist bei der die Calomel-Homepage der Toolbar-Button links neben der Adreßleiste grün eingefärbt, weil er nach dem Scoring des Addons die höchste Bewertung erhalten hat.

Ein Klick auf den Button zeigt die ebenfalls in Bild 1 dargestellte Seite mit detaillierteren Informationen.

Bild 2: SSL Validation Preferences

SSL-Validation

In der ersten Zeile (Connection) wird der insgesamt erzielte Score ausgegeben, zusammen mit dem zugeordneten Farbwert. In diesem Beispiel gilt die Verbindung als SECURE. Dann folgen die einzelnen Bewertungen sowie weitere Informationen zum Zertifikat, die jedoch rein informativer Art sind.

Die erzielten Scores betreffen die Zertifikats-Validierung, die Übereinstimmung des Common Name mit dem angezeigten URL-Host, die Art und Stärke des symmetrischen Verschlüsselungsalgorithmus sowie die Art und Stärke der Signaturalgorithmen; letzteres gilt sowohl für den Aussteller (der das Zertifikat signiert) als auch für den Zertifikatinhaber.

Bei der Validierung prüft das Addon, ob das Zertifikat online mit dem Online Certificate Status Protocol (OCSP) verifiziert werden kann. Ist das nicht möglich oder meldet der Herausgeber ein Problem, wird dies mit -50 Punkten gewertet, ansonsten mit +30. Ein selbstsigniertes oder zurückgerufenes Zertifikat wird grundsätzlich als negativ gewertet. Der Grund ist, daß einem nicht verifizierbaren Zertifikat nicht vertraut werden sollte und durch dieses negative Scoring wird der Farbcode dementsprechend immer rot sein. Wird zum Beispiel dem Herausgeber nicht vertraut, weil dessen Root-Zertifikat nicht im Browser hinterlegt ist, erscheint die Warnung »WARNING! Issuer not trusted.«

Ein häufig auftretendes Problem liegt darin, daß der im Zertifikat hinterlegte Domain-Name (Common Name) nicht mit dem in der URL angezeigtem übereinstimmt (Domain Mismatch). Im Falle von zum Beispiel *https://www.example.com* muß das Zertifikat für die Domäne *www.example.com* gültig sein, nicht nur für *example.com*. Liegt eine Übereinstimmung vor, gibt dies 10 Punkte, ansonsten 0 Punkte. Hier ist allerdings kritisch zu erwähnen, daß in der Praxis ein Mismatch mit maximaler Punktzahl bewertet wird, sofern der Nutzer zuvor die Firefox-Warnung über einen solchen Mismatch akzeptiert hat. Hier sollte im Scoring zumindest darauf hingewiesen werden und keine maximale(!) Punktzahl vergeben werden; immerhin werden die beiden Namen untereinander aufgelistet, so daß man den Unterschied erkennen kann.

Als nächstes werden der symmetrische Verschlüsselungsalgorithmus und seine Bit-Stärke analysiert. Maximale Punktzahlen (34 beziehungsweise 14) gibt es für AES oder Camellia mit mindestens 256 Bit Schlüssellänge. 3DES etwa wird als schwächer berücksichtigt.

Das X.509-Zertifikat ist vom Herausgeber digital signiert, sein Algorithmus sowie die Bitlänge werden als nächstes untersucht. Eine Schlüssellänge von weniger als 2048 Bit führt dabei bereits zu einer Kennzeichnung »weak«, was sich in einem verminderten Scoring (0 statt maximal 6 Punkte) niederschlägt. Genauso kann (sofern im X.590-Zertifikat ausgewiesen) der Zertifikatsschlüssel selber zum digitalen Signieren verwendet werden und wird analog bewertet.

Die Art des Zertifikats, ob also ein EV- oder ein DV-Zertifikat vorliegt, wird zwar aufgeführt, fließt jedoch nicht in das Scoring ein, da dies nach Ansicht des Entwicklers kein sinnvolles, weil letztlich schwaches Kriterium ist.

Auch die Gültigkeit des Zertifikats fließt nicht direkt ins Scoring ein; ist das Zertifikat aber abgelaufen, führt das immer zu einem ungültigen Zertifikat und damit zu einem roten Farbcode.

Eine Besonderheit gilt es zu beachten: Das Scoring bezieht sich auf die https-Elemente einer Webseite. Sind auf der Webseite http-Elemente vorhanden – die also im Klartext übertragen wurden –, wird trotz

eines möglicherweise hohen Scorings ein roter Farbcode angezeigt, da die Verbindung nicht vollständig verschlüsselt ist. Da das zum Beispiel bei eingebundenen Bildern häufig der Fall ist, wird man in der Praxis auf nicht wenige https-Seiten treffen, die rot markiert werden. In der Scoring-Liste erkennt man das an der abschreckenden Meldung »This connection is either partially encrypted or completely broken«.

Konfiguration

Konfigurationsmöglichkeiten des installierten Addons findet man im Firefox unter *Extras | Calomel SSL Validation*. Dort sind neben der Möglichkeit, Statistiken über die Cache-Nutzung des Browsers abzurufen auch Einstellmöglichkeiten vorhanden, die sicherheitsrelevant sind. Grundsätzlich sind nach der Installation des Addons alle zusätzlichen Einstellungen zunächst einmal deaktiviert.

Interessant ist die oberste Option *toggle high ciphers (temporarily)*. Sollen nur https-Verbindungen mit Verschlüsselungsalgorithmen hoher Stärke akzeptiert werden (AES beziehungsweise Camilla mit mindestens 256 Bit, siehe dazu auch [2]), kann man dies in den Konfigurationsoptionen aktivieren. Mit der Toggle-Möglichkeit läßt sich dies temporär deaktivieren oder aktivieren.

Wählt man *Preferences* aus, gelangt man zur eigentlichen Konfiguration, dargestellt in Bild 2. Im Rahmen von Sicherheitsbetrachtungen sind die Tabs *Security* sowie *Privacy* interessant. Auf ersterem können wie erwähnt starke Sicherheitseinstellungen erzwungen werden. Neben starken Algorithmen zählen dazu auch die zwingend notwendige Validierung eines Zertifikats über OCSP sowie das Deaktivieren von SSLv2 sowie SSLv3, also der Voraussetzung von TLS (dem Nachfolger von SSL).

Die Option *disable short URL keyword guessing* hindert Firefox daran, Vorschläge für URLs zu machen, wenn man sie einzutippen beginnt. Aus Sicherheitssicht ist eine solche Tipphilfe nicht unproblematisch, da man unter Umständen zu einer vollkommen anderen Seite kommt als ursprünglich geplant war.

Bild 3 zeigt die *Privacy*-Einstellungen des Addons. Hiermit kann man Firefox daran hindern, den Tabs eine Überschrift oder ein Icon zu geben (*do not show tabs titles or icons*). Die Option *disable safe browsing* unterbindet das in Firefox integrierte Google Safe Browsing. Safe Browsing schützt den Nutzer vor Phishing-Seiten, ist allerdings nicht unumstritten, da hier unter Umständen Daten über den Anwender zu Google geschickt werden, was seine Privatsphäre berührt. Die Option *disable geo location* verhindert, daß eigene Daten zum Google Location Service geschickt werden, um Lokalisierungsdaten zu erfassen.

Die letzte Option *disable dns prefetch* verhindert, daß zum Beispiel DNS-Anfragen von in einer Webseite enthaltenen Links während des Ladens der eigentlichen Seite ausgeführt werden. Um sie anschließend schneller bereitstellen zu können, sollte der Nutzer einen entsprechenden Link anklicken. Auch dieses Verhalten ist aus Sicherheitssicht nicht unproblematisch, selbst wenn es einen leichten Geschwindigkeitsgewinn bringen kann.

Die Tabs *Optimization* und *Annoyances* sind für verschiedene Performance- und User-Experience-Einstellungen vorgesehen, wie man sie von verschiedenen anderen Addons kennt. So ist es zum Beispiel möglich, animierte GIFs oder Werbung zu deaktivieren. Die Optionen sind dabei weitgehend selbsterklärend, eine tiefergehende Erläuterung erhält man auf der Homepage von Calomel [2].

Die Idee, dem Nutzer einer https-Verbindung tiefergehende Informationen zu liefern als das mit einem reinen Farbcode bei EV- oder DV-Zertifikaten möglich ist, ist naheliegend und definitiv sinnvoll, da man sich zwar mit Firefox-Bordmitteln auch Informationen zum Zertifikat selber ausgeben lassen kann, diese Angaben aber nicht vollständig sind. Ob es allerdings mit dem Addon von Calomel gelingt, ist durchaus diskutabel. Das Bereitstellen von Informationen in Form eines Scorings ist nützlich, allerdings erscheinen die fünf verschiedenen Farbcodes für eine https-Verbindung vielleicht etwas zu viel des Guten, auch wenn die dahinterstehende Idee einer nicht zu groben Einteilung einsichtig ist. Kritikwürdig ist auch das Scoring für Domain-Mismatches.

Fazit

Hat hier nämlich der Nutzer der Ausnahmeregelung des Browsers zugestimmt, sieht man zwar im Addon, daß der Common Name nicht der gleiche wie der Domänen-Name der angefragten URL ist, aber dennoch erscheint im Scoring eine volle Wertung – ein Verhalten, das eher verwirrt.

Zwar wird heute allgemein dazu geraten, bei Public-Key-Verfahren mit einer Schlüssellänge von mindestens 2048 Bit zu arbeiten, dennoch bedeutet dies nicht, daß 1024 Bit (Abzug im Scoring) per se als unsicher zu werten sind. Eine geringere Farbwertung als Grün signalisiert also möglicherweise Unsicherheiten, die nicht zwingend der Fall sein müssen.

Jemand, der die relevanten Parameter einer https-Verbindung technisch versteht, wird zweifellos Nutzen aus diesem Addon ziehen, da man auf einen Klick wichtige Informationen erhält, die einiges über die Gegenstelle verraten. Bei einem »normalen« Nutzer bleibt jedoch fraglich, ob das Mehr an Informationen unbedingt Klarheit schafft. ◆

Links

[1] Calomel SSL Validation-Addon für Firefox:
https://addons.mozilla.org/en-US/firefox/addon/207653/
[2] Calomel SSL Validation Addon-Homepage:
https://calomel.org/firefox_ssl_validation.html