Manche Webseiten sind sicherer als andere

Mit Sicherheit im Browser

Sicher surfen, sicher online zur Bank gehen, das haben die Leute schon zu Beginn jeglicher Online-Dienste wollen. So stammt das heute gebräuchliche Secure-Socket-Layer-Protokoll (SSL) noch von Netscape aus den Jahren vor 1995. Etwas angereichert, wird es seit 1999 als Transport Layer Security (TLS) von führenden Banken und Kreditkartenorganisationen eingesetzt. Jedesmal, wenn wir eine Website ansteuern, bei der es auf Sicherheit und Vertrauen ankommt, steht ein zusätzliches kleines „s“ in der Adresse, https statt bloß http.

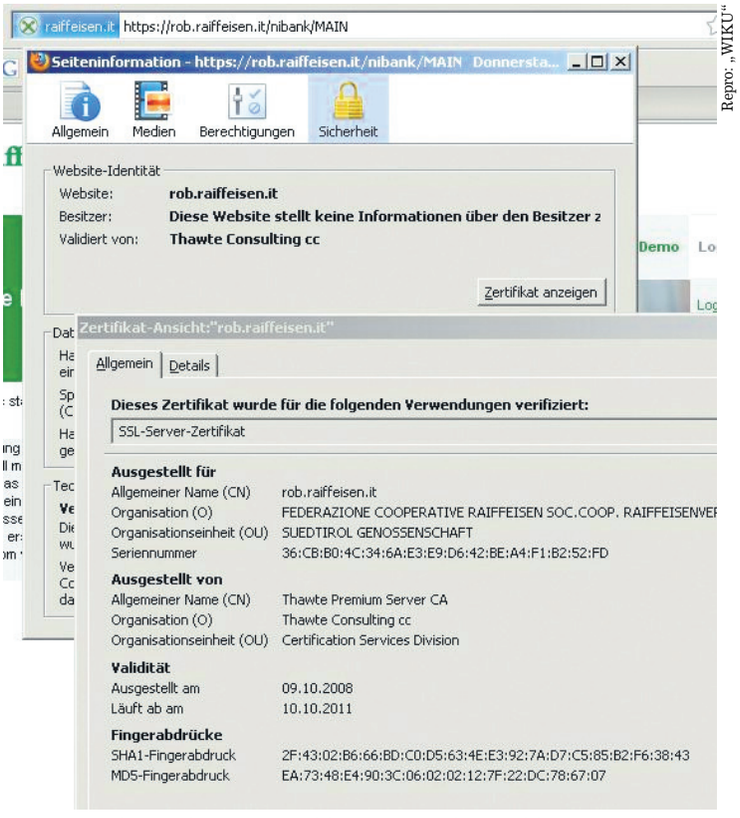
VON FRITZ JÖRN *

Eine sichere Verbindung erkennt man an einem kleinen, zugeschlossenen Vorhangschloss, im Explorer gleich hinter der Adresse, im Firefox ganz unten rechts im Browser, und an der Bezeichnung „https“ in der Seitenadresse vor dem Doppelpunkt. Entscheidend ist das „s“ (https: Hypertext Transfer Protocol Secure). Neuerdings werden blaue oder grüne Kästen vor dem „http gezeigt. Man arbeitet auf sicheren Seiten ansonsten genauso wie auf normalen. Zusperren braucht man das Schloss nicht, es geht alles von selber.

Beim Ansteuern einer Bank schickt der eigene Browser zuerst eine selbstgewählte Sitzungsnummer und eine Zufallszahl hinauf zum Server der https-Seite. Der Server antwortet mit seinem Sicherheitszertifikat, stellt sich sozusagen vor. Der Browser prüft das Zertifikat des Servers. Ist etwas faul, so wäre jetzt schon Schluss. Weil das Server-Zertifikat dessen öffentlichen Schlüssel enthält, kann nun unser Browser einen temporären Schlüssel verschlüsselt zum Server senden. Ab jetzt ist alles geheim. Aus diesem vorläufigen Schlüssel, den nun die beiden – und nur sie – kennen, bilden sie sich einen Sitzungsschlüsel für diese eine Verbindung (Session). Mit diesem nun symmetrischen Schlüssel wird jeglicher weiterer Verkehr geheim gehalten. Das alles ist im Netz etwa bei *http://bit.ly/ED3bW* genau beschrieben. Wer ein gutes Schloss hat, kann es auch zeigen.

Das Zertifikat

Meint nun einer, er könne sich in den Verkehr einschleichen, um mitzuhören oder vielleicht gar Banküberweisungen zu ändern, der müsste beiden Seiten die jeweils andere vorgaukeln. Davor schützt das Zertifikat der Bank, das er im entscheidenden Moment nicht vorweisen kann. Und wenn, so hätte er nicht deren privaten Schlüssel zum Entschlüsseln der nächsten Nachricht vom Kunden.



Repro: „WIKU“

Vom „https“ bis zum geschlossenen Vorhangschloss – so sieht eine sichere Website aus.

Dieses digitale Zertifikat kann unser Browser beim Zertifikatsgeber nachprüfen und dessen Zertifikat wieder mit einem der vielleicht 230 in Windows bereits seit Installation vorgegebenen Zertifikate. Hier zeigt sich das Grundprinzip jeder Verschlüsselung, dass nämlich der Schlüssel auf einem anderen Weg als die verschlüsselten Nachrichten zum Empfänger gelangen muss. Der Ur-Schlüssel kommt mit der Installations-CD, die Signatur der Bank über das Internet. Die Hierarchie der Schlüssel nennt sich public key infrastructure (PKI). Jedes digitale Zertifikat ist selbst durch eine digitale Signatur geschützt, deren Echtheit mit dem öffentlichen Schlüssel des Ausstellers des Zertifikates geprüft werden kann.

Was keiner leicht versteht, sind die zu Beginn verwendeten asymmetrischen Schlüssel. Da lässt sich ein Schloss mit einem Schlüssel zusperren und nur mit einem anderen wieder aufsperren. Die Idee für dergleichen Schlüssel kam vor 40 Jahren auf. 1977 entwickelten Ronald L. Rivest, Adi Shamir und Leonard M. Adleman ihr RSA-Verfahren, das heute noch gültig ist. Die beiden Schlüssel hängen zwar zusammen, wenn man sie erzeugt und gebraucht. Aus dem einen lässt sich hinterher aber der andere nicht mehr rekonstruieren (selbst der Verschlüssler kann sein eigenes Chiffrat nicht mehr entschlüsseln.)

Einer der beiden Schlüssel wird zum Entschlüsseln öffentlich bekanntgegeben, den anderen behält sich hier der Zertifikatsgeber Z, um damit zu verschlüsseln oder umgekehrt. Wer Zs Nachricht mit dessen öffentlichem Schlüssel entschlüsseln kann, der weiß, dass die Nachricht wirklich von Z ist. Asymmetrische Schlüssel werden bei unserem sicheren Browsen nur bis zum Aushandeln des Betriebsschlüssels benutzt, weil sie viel Rechenzeit kosten. Im eigentlichen Dialog wird dann herkömmlich symmetrisch verschlüsselt, also mit demselben Schlüssel ver- und entschlüsselt. Beim nächsten Aufruf der https-Seite gibt's dann wieder einen neuen Schlüssel.

Je länger desto sicherer

Spezielle Banking-Verfahren wie Pin-Tan, HBCI oder wie bei Raiffeisen-Online mit kleinen Einmal-Tan-Generatoren wären einen eigenen Artikel wert. Jedenfalls achten die Banken sehr auf Sicherheit. So garantiert beispielweise Raiffeisen Online ein SSL-Protokoll mit 128 Bit Schlüssellänge (je länger, desto sicherer, aber auch rechenintensiver) und HTML-Kode ohne Java-Applets. Ein Kurzzeit-Cookie Jsessionid sichert die ungebrochene Kontinuität einer Sitzung. Frames mit Werbeeinblendungen Dritter sind verpönt, weil sie fremden Kode unter der SSL-Flagge einfahren könnten. Kurz: SSL hat sich (als TLS) bewährt.

Angriffe durch Trojaner, die im PC des Bankkunden noch vor der Verschlüsselung agieren, gefälschte Browser und andere Horrorszenarien scheiden für die tägliche Praxis aus. Im Netz wird an „DNS Security Extensions“ bereits gearbeitet. W

** Fritz Jörn ist freier Journalist in Bonn*