

Wie sicher ist eigentlich...

Secure Socket Layer (SSL)?



Zur Absicherung von geheimen oder vertraulichen Daten im Internet – beispielsweise Informationen beim Online-Banking oder -Shopping – wird häufig mit dem SSL-Protokoll (Secure Socket Layer) gearbeitet. Sie erkennen das daran, dass eine Webadresse mit **https://** statt mit **http://** beginnt und dass in der Taskleiste (Fusszeile) des Webbrowsers ein kleines geschlossenes Schloss-Symbol zu sehen ist.

In den meisten Fällen wird dann zum Übertragen der Daten eine 128-Bit-Verschlüsselung verwendet, die nach bisherigen Erkenntnissen als praktisch nicht zu knacken galt.

Doch Wissenschaftler der Ecole polytechnique fédérale de Lausanne (EPFL) konnten jetzt nachweisen, dass sich ein seit längerem bekannter theoretischer Schwachpunkt tatsächlich für so genannte Timing-Angriffe nutzen lässt. (Wir berichteten: <http://www.pctip.ch/webnews/wn/23347.asp>). Die Lausanner Forscher schafften es, mit einem selbst entwickelten Programm in weniger als einer Stunde ein SSL-geschütztes Passwort zu knacken, so die Pressemitteilung der EPFL, siehe http://lasecwww.epfl.ch/memo_ssl.shtml.

Beim Online-Banking ist die Sicherheit dadurch aber nicht wirklich gefährdet. Das Ermitteln der verschiedenen Zugangspasswörter würde einige Stunden dauern – länger als jede Online-Banking-Sitzung – und es müssten dazu schon spezielle Voraussetzungen erfüllt werden, wie auf der Website weiter ausgeführt wird.

So muss der Angreifer etwa *alle* Datenpakete einer SSL-Sitzung mitschneiden und der SSL-Server darf nur mit *einem einzigen* Benutzer beschäftigt sein, was höchstens spät in der Nacht der Fall sein dürfte. Ähn-

lich äusserten sich auch unabhängige Sicherheitsexperten wie etwa der Amerikaner Avi Rubin. Er erklärte, die Methode der Schweizer Forscher funktioniere nur bei E-Mail-Transaktionen und sei auch dort nur eingeschränkt anwendbar.

Auch die Schweizer Banken und Shopping-Anbieter geben sich gelassen. So schreibt z. B. die Post nach wie vor auf ihrer Website, eine korrekte SSL-Verbindung sei «in jedem Fall sicher, da die Daten bei der Übermittlung automatisch mit 128 Bit verschlüsselt werden und somit nicht abgefangen werden können». Und Postfinance-Mediensprecher Alex Josty betont: «Das Forschungsprojekt der EPFL wurde unter Laborbedingungen durchgeführt, die in der Praxis nicht üblich sind.»

Die Lücke wurde unter Open SSL nachgewiesen, einer Open-Source-Implementierung von SSL. Die Entwickler von Open SSL haben reagiert und die neuen Versionen 0.9.7a und 0.9.6i der Verschlüsselungsbibliothek für Linux und Unix bereitgestellt, die gegen diese Attacken immun sind (<http://www.openssl.org/source/>). Andere Hersteller von SSL-Software, etwa Microsoft, untersuchen ihre Produkte wie die Webserver-Lösung IIS (Internet Information Server) momentan auf ähnliche Schwachstellen. ([sz/idg](http://www.sz/idg))



http://www.bsi-fuer-buerger.de/02/02_05.htm: Hier informiert die deutsche Regierung über die Sicherheit von SSL.

Impressum

PCtip

IDG COMMUNICATIONS

Die Schweizer PC-Zeitschrift

Verlag IDG Communications AG

Witikonstr. 15, PF 253, 8030 Zürich, Tel. 01 387 44 44

Gesamtleitung IDG Gebhard Osterwalder

Redaktion Tel. 01 387 44 44, Fax 01 387 45 84, Postadresse wie Verlag

E-Mail redaktion@pctip.ch, Internet <http://www.pctip.ch/>

E-Mail für Pressemitteilungen: pr@pctip.ch

E-Mail für Free-/Shareware-Vorschläge: downloads@pctip.ch

PCtip-Kummerkasten: <http://www.pctip.ch/helpdesk/kummerkasten/anfrage.asp> (Telefonische Anfragen können nicht bearbeitet werden.)

Sonja Wunsch (sw), Chefredaktion

Hansjörg Honegger (hh), Produktion/Stellvertretung Chefredaktion

Christian Bütikofer (chb), Beat Rüdt (rue), Gaby Salvisberg (sal),

Sascha Zäch (sz), Redaktion • Anne Kittel (ki), Assistenz/Abschluss,

Balbina Hossman (bh), Assistenz

Ständige freie Mitarbeit Bruno Habegger (bha), Markus Zitt (z),

Nelly Bach (Abschluss), Nadia Steinmann (Abschluss)

Beiträge aus IDG-Schwesterpublikationen sind mit (idg) gezeichnet.

PCtip-Kummerkasten Bruno Amsler (ba), Marci Castro (mc),

Ruth Gogoll (ggl), Monica Hubacher (mo), Martin Huber (mhu),

Antje Küchler (ak), Simon Wepfer (swe)

Layout/Gestaltung Daniel Brühlmann (Leitung), Hans-Jakob Rickli

Druck St. Galler Tagblatt AG, 9001 St. Gallen

Auf chlorfrei gebleichtem Papier gedruckt.

Leserschaft 271 000 Leser (MACH Basic 2002)

Verkaufte Auflage 60 060 (Jahr 2002 gemäss WEMF 2003)

Vertrieb & Marketing Jacqueline Ort, E-Mail jacqueline.ort@idg.ch

Bestellung Abo/bis zu 2 Jahre alte Ausgaben, Adressänderung

PCtip-Aboservice, PF 9001 St. Gallen, Tel. 071 272 71 90, Fax 071 272 73 84

E-Mail abo@pctip.ch, Internet <http://www.pctip.ch/abo/>

Bezugspreise PCtip erscheint monatlich (plus ein Sonderheft zur

Orbit/Comdex), die nächste Ausgabe am 24. 6. 2003.

Einzelausgabe Kiosk Fr. 3.80, Jahresabo Fr. 38.–

Anzeigen Schweiz Tel. 01 387 44 44, Fax 01 387 45 83

E-Mail anzeigen@pctip.ch und onlinewerbung@pctip.ch

Kurt Strebel, Gesamtleitung Anzeigen IDG • Rolf Fischer, Lokaler Verkauf

Urs Flückiger, Internationaler Verkauf/Online • Esther Majolet, Marktplatz

Natalie Rickli, Beatrice Meyer, Disposition • Nina Osterwalder, Assistenz

Anzeigen Deutschland Tina Ölschläger, IMS München

Tel. 0049 89 360 86 116, Fax 0049 89 360 86 263

Es gilt der Anzeigentarif 2003.

© 2003 IDG Communications AG, Zürich. ISSN 1422-4704

Alle Rechte vorbehalten. Die Urheberrechte für angemessene und veröffentlichte Manuskripte und Abbildungen liegen bei der IDG Communications AG. Nachdruck, Verbreitung und elektronische Weitergabe, auch auszugsweise, nur mit schriftlicher Genehmigung des Verlages. Dies gilt auch für in elektronischer Form verteilte Beiträge sowie für Beiträge auf <http://www.pctip.ch/>. Die ganze oder teilweise Verwertung von Inseraten (inkl. Einpreisung in Online-Dienste) durch unautorisierte Dritte ist untersagt. Alle Beiträge werden mit grösster Sorgfalt erstellt. Trotzdem können wir keine Haftung für deren Richtigkeit übernehmen. Insbesondere übernehmen wir keine Haftung für Kaufempfehlungen oder für Schäden, die beim Ausprobieren der Bauleitungen oder Tipps u. a. passieren. Ebenfalls keine Haftung wird übernommen für unverlangt eingesandte Manuskripte, Soft-/Hardware, CD-ROMs, Floppys, Fotos, Dias etc. Eine Rücksendegarantie geben wir nicht. Wir behalten uns das Recht vor, eingesandte Beiträge auf anderen Medien etwa auf CD-ROMs, in Sonderheften oder im Online-Verfahren herauszugeben.

Dirty Tricks: Tipps, die in keinem Handbuch stehen
Online-Fotolabors: Qualität und Preise im Test
Open-Office: So steigen Sie um aufs Gratis-Office
Notebooks: Kaufberatung mit Produktübersicht
Sicher und schnell: Zahlungssysteme im Internet

Nachzulesen im nächsten PCtip vom Juli 2003. Themen können aus aktuellem Anlass ändern.



Der nächste PCtip 7/2003 erscheint am Dienstag, 24. Juni 2003.