Challenge: Die Herausforderung

Lothar Ehnis/Helmut Springer

Die Geheim- oder die Zeichensprache, bei der ein nebenstehender Dritter die Unterhaltung der Kommunizierenden nicht verstehen kann, hat Menschen schon immer fasziniert. Jedoch haben derart Kommunizierende auch schon immer einen gewissen negativen Verdacht auf sich gelenkt. Besonders Regierungen, Behö rden und auch Vorgesetzten kann solches Tun ein Dorn im Auge sein.

Heute, im Zeitalter der Informations- und Kommunikationstechnik, hat sich an dieser Einstellung nichts geä ndert und verschiedene Institutionen wittern noch immer Verrat hinter verschlü sselten Informationen, obwohl kryptographische Verfahren vor allem im Banken- und Wirtschaftsbereich aus Vertraulichkeitsgrü nden ü blich sind.

So gibt es heute verschiedene Verfahrensweisen, wie mit Verschlüsselung umgegangen wird. In Frankreich ist die Verschlüsselung von Daten generell verboten, es sei denn, der Schlüssel ist bei einer staatlichen Institution hinterlegt. In der Bundesrepublik Deutschland gibt es bisher keine Einschränkungen. In den USA ist die Sachlage schwieriger: Dort selbst unterliegt die Verschlüsselung bisher keinerlei Einschränkung, allerdings ist der Export von Verschlüsselungssoftware, wie z.B. in Kerberos, PGP, Netscape, usw., so gut wie verboten. Ausnahmen, wie beispielsweise der Netscape WWW-Server mit Secure Socket Layer (SSL), sind nur mit der sehr mäßigen Schlüsselsicherheit von 40bit zugelassen. Der Grund dafür ist, den Geheimschlüssel mit angemessenem Rechenaufwand in einer endlichen Zeit auf Superrechnern doch errraten bzw. errechnen zu können. In dieser Art der Verschlüsselung wird der Benutzer keine Vertraulichkeit für seine Daten sehen und muß wissen, was für eine Art von Sicherheit bzw. Vertraulichkeit angeboten wird.

Verschiedene Fachleute haben sich über diese halbherzige Vorgehensweise schon mokiert, unter anderem auch die Firma RSA Data Security, die sich mit Algorithmen und Lizenzierung für Verschlüsselungsverfahren befaßt. Sie hat einen Wettbewerb, Challenge, ausgeschrieben, um die Nutzlosigkeit der exportierbaren Softwareschlüssel aufzuzeigen und damit Druck auf die Regierungen ausüben zu können, die Exportbestimmungen zu lockern, da Gefahr besteht, dadurch Anteile am Verschlüsselungsgeschäft zu verlieren.

Aufgrund der Ausschreibung haben sich Fachleute, unter anderem Germano Caronni an der ETH in Zürich, Gedanken gemacht, wie man hier zu Werke gehen kann; gilt es doch die leichte Knackbarkeit eines 40bit-Schlüssels nachzuweisen und die erforderliche Rechenleistung zum Knacken in einer angemessenen Zeit zu bekommen.

Caronni's Lösung: Durch Zerlegen des gesamten Schlüsselbereichs in viele Einzelbereiche braucht man nur diese entsprechend zu lösen, was am schnellsten durch parallele Verarbeitung mit vielen CPUs geschieht, man denke an massiv-parallele Rechner (MPP). Woher aber diese nehmen? Die Lösung ist ganz einfach: Man bitte alle CPU-Besitzer im Internet, die Idle Time ihrer CPU's zur Verfügung zu stellen! Also holen diese sich per Netz einen vorgegebenen Schlüsselbereich beim zentralen Server, bearbeiten diesen und sehen nach, ob der Schlüssel damit geknackt ist. So Rechenzeit vorhanden, kann man dann den nächsten Schlüsselbereich holen und lösen usw.

Mit einem ähnlichen Verfahren gelang es dann Ian Goldberg, University of Berkeley/Kalifornien mit etwa 250 Rechnern in etwas mehr als 3,5 Stunden einen 40-bit-Schlüssel zu knacken. Mit dem Züricher Ansatz und vereinten Kräften aus dem Internet ge-lang es nun, einen 48bit-Schlüssel in 13 Tagen zu knacken und einen vorgegebenen Kernsatz zu entziffern.

Dabei waren teilweise mehr als 4 500 CPU's mit einer Kapazität von 460 Mio. keys/s gleichzeitig im Einsatz. Zum Vergleich: Damit hätte man theoretisch den 40bit-Schlüssel in 25 Minuten geschafft. Der Lösungsschlüssel wurde übrigens an der Universität Münster errrechnet.
Weitere Informationen hierzu: http://www.klammeraffe.org/challenge/

An diesem Unternehmen Challenge waren viele Hochschulen in Europa mit Rechnern beteiligt, unter anderem auch aus Baden-Württemberg und dort von der Universität Stuttgart. Es ist anzumerken, daß die Stuttgarter Superrechner nicht im Einsatz waren; die 512 Alpha-Prozessoren der CRAY T3E wären CIA-like gewesen!

Nach diesem gelungenen Unternehmen, das zeigte, daß "edblbase;Kleinvieh auch Mist machen bzw. Geheimschlüssel knacken kann", bleibt die Hoffnung, daß die entsprechenden Behörden und Regierungen durch dieses Exempel vielleicht doch Einsehen haben und die bisher verfolgte Politik in Sachen Verschlüsselung ändern und freien Zugriff auf Methoden, Algorithmen und Software gewähren bzw. beibehalten.

Dr. Lothar Ehnis, NA-5985
E-Mail: ehnis@rus.uni-stuttgart.de

Helmut Springer
E-Mail: springer@rus.uni-stuttgart.de

Netzsicherheitsexperten lehnen Einschränkung strikt ab

Die Verschlüsselungsfreiheit

Als Teilnehmer der vom DFN-CERT (Computer Emergency Response Team des Deutschen Forschungsnetzes) in Hamburg durchgeführten Tagung *Sicherheit in vernetzten Systemen*, als DV-Verantwortliche, als Nutzer der Datenautobahn, aber auch als Bürger lehnen wir ein von Politikern und Sicherheitsdiensten angestrebtes Verschlüsselungsverbot strikt ab. Wir fordern den Erhalt frei wählbarer und einsetzbarer Verschlüsselungsverfahren und die Geheimhaltung unserer frei gewählten kryptographischen Schlüssel.

Wir benötigen starke Verschlüsselung dringend, um Rechner im Netz sicher betreiben zu können. Die bisherigen Netzdienste übertragen alle Informationen unverschlüsselt, auch Benutzerkennungen und Passworte. Durch Abhorchen der Netze kommt somit jeder an alle Informationen, um fremde Rechner unerlaubt und unbemerkbar nutzen zu können. Nur durch die Verschlüsselung aller übertragenen Daten ist zu verhindern, daß Hacker über bestehende Verbindungen in fremde Rechner eindringen und sich dabei für später einen uneingeschränkten Zugang verschaffen.

Leistungsfähige Verschlüsselungsverfahren helfen uns Angriffe von Hackern auf vernetzte Rechner und deren Daten abzuwehren sowie die übertragenen Daten effektiv zu schützen. Nur so können wir den Absenderangaben und der Unverfälschtheit dieser Daten vertrauen. Die Verschlüsselung ist die Grundlage für die notwendige Vertraulichkeit, um die Netze wirtschaftlich nutzen (z.B. Bestellungen und Homebanking) oder um sensitive Daten übertragen zu können (z.B. Gesundheits- oder Abrechnungsdaten). Sie ist aber auch Arbeitsvoraussetzung ganzer Berufsgruppen (z.B. Ärzte, Rechtsanwälte, Notare, Steuerberater, Journalisten). Auch für unsere elektronische Post (E-Mail), die bisher so wenig vertraulich war wie Postkarten, ist endlich die Wahrung des Briefgeheimnisses möglich.

Nur die Verwendung digitaler Signaturen ermöglichen eine sichere Überprüfung der Absenderangabe sowie eine sichere Aufdeckung von Datenmanipulationen. Dadurch wird die Voraussetzung für die seit langem geforderte Rechtssicherheit in Datennetzen geschaffen. Eine wirtschaftliche Nutzung von Datennetzen verbunden mit einem Verschlüsselungsverbot ist daher unsinnig und wird eine solche verhindern. Denn nur wer als einziger auf seinen privaten Schlüssel zugreifen kann, kann auch sicher sein, daß seine Signaturen nicht gefälscht werden, und nur dann kann er seine Identität wahren und verläßlich Transaktionen im Netz durchführen. Eine glaubwürdige digitale Signatur ist nur mit einer starken Verschlüsselung zu haben. Es ist technisch nicht möglich, kryptographische Verfahren nur für digitale Signaturen und Benutzerzugangsprüfungen zu erlauben, ihren Einsatz für die Verschlüsselung aber zu verhindern. Zur Abwehr gefälschter Schlüssel benötigen wir eine Beglaubigung der Schlüssel. Diese Aufgabe können nur vertrauenswürdige Instanzen wahrnehmen, die auf der Grundlage genauer gesetzlicher Bestimmungen handeln. Dazu ist das im Entwurf befindliche Signaturgesetz zu überarbeiten und schnell zu verabschieden.

Trotz all dieser sinnvollen und notwendigen Einsatzmöglichkeiten soll nun die Verschlüsselung entweder ganz verboten oder nur einfache Verfahren, die leicht und schnell entschlüsselbar sind, zugelassen werden. Alternativ soll der Zugriff auf unsere geheimen Schlüssel erzwungen werden. Ein solche Einschränkung der Verschlüsselungsfreiheit verhindert den Einsatz sicherer Netzdienste. Der Gesetzgeber fordert zwar von uns den Schutz der uns anvertrauten Daten und Rechner, will uns aber die dazu notwendigen Mittel verbieten.

Von einem Verschlüsselungsverbot wären alle Bürger betroffen. Sollen z.B. unsere Kontoauszüge oder Patientendaten unverschlüsselt übertragen werden? Ein Verschlüsselungsverbot würde sogar die Grundrechte aller Bürger massiv einschränken, insbesondere das Briefgeheimnis, das auch für die Elektronische Post gilt.

Als wichtigstes Argument für ein Verschlüsselungsverbot wird die Bekämpfung des organisierten Verbrechens aufgeführt. Dieses Argument ist nicht stichhaltig, denn Geheimbotschaften können selbst in unverschlüsselten Texten stecken: Der Empfänger muß nur den vereinbarten Code kennen. Darüber hinaus kann jeder Nachrichten in umfangreichen Texten oder Bildern sogar so verstecken, daß dies nicht einmal mehr nachweisbar ist (Steganographie). Der Jurist folgert alleine daraus die Verfassungswidrigkeit eines Verschlüsselungsverbotes, weil die vorgeschriebene Verhältnismässigkeit nicht eingehalten wird.

Ein Verschlüsselungsverbot ist zur Verbrechensbekämpfung völlig ungeeignet. Es gestattet einzig und allein die genauere Überwachung gesetzestreuer Bürger und macht diese zu Gläsernen Bürgern. Gleichzeitig bedeutet es eine nicht zu verantwortende Gefahr für die am Netz angeschlossenen Rechner, deren Daten und aller übertragenen Informationen.

Wenn man statt eines generellen Verschlüsselungsverbotes aber nur schwache, von den Sicherheitsdiensten kontrollierbare Verschlüsselungsverfahren zuläßt oder alle verpflichtet, ihre geheimen Schlüssel bei einer Behörde zu hinterlegen, wird die Gefahr eines Missbrauches unnötig und erheblich vergrößert. Die notwendige Sicherheit fehlt, die Schlüssel sind unsicher und der bürokratische Aufwand sowie die staatliche Bevormundung nehmen zu.

Wir fordern deshalb alle auf, die Hamburger Erklärung für Verschlüsselungsfreiheit nach besten Kräften zu unterstützen!

Gesehen in einer Internet Mail des DFN-CERT

Für Verschlüsselungsfreiheit

Die Hamburger Erklärung

- Aus Verantwortung für die an den Netzen angeschlossenen Rechner mit all ihren Daten und Programmen,
- aus Verantwortung für die Benutzer der von uns betreuten Systeme,
- aus Verantwortung für die sichere Nutzung der Netzdienste,
- aus Verantwortung für die Vertraulichkeit der übertragenen Daten, die insbesondere
    - zum Schutz des geistigen Eigentums (Urheberrecht),
    - zum Schutz der personenbezogenen Daten (Datenschutz),
    - zum Schutz der Schweigepflicht und zum Informantenschutz ganzer Berufsgruppen sowie

    - für die wirtschaftliche Nutzung der Datennetze notwendig ist
- und aus Verantwortung für die Grundrechte aller

fordern wir

1. 1. die freie Wahl der Verschlüsselungsverfahren und
2. 2. die freie Wahl und Geheimhaltung der Schlüssel.

Dipl.-Ing. Götz Babin-Ebell
Dr. Johann Bizer (Universität Frankfurt)
Dipl.-Chem. Peter-Ch. Gentz (Network-Consultant)
Karl-Peter Gietz, M.A. (Universität Tübingen)
Dipl.-Inf. Stefan Kelm (Universität Hamburg)
Georg Koch
Dipl.-Inf. Klaus-Peter Kossakowski (Universität Hamburg)
Dipl.-Inf. Britta Lietke (Universität Hamburg)
Dipl.-Inf. Wolfgang Ley (Universität Hamburg)
Dr. Hans-Joachim Mück (Universität Hamburg)
Dr.-Ing. Rudolf Theisen (Forschungszentrum Jülich)

Die vollständige Erklärung

finden Sie z.B. unter
ftp://TROLL.HZ.KFA-Juelich.De/pub/KRYPTO/hh.htm bzw. hh.txt

Nur einen Unterschriftstext und eine Regieanweisung, wie man diesen Text mit PGP signiert enthält hh2.txt

Sie unterstützen diese Erklärung, indem Sie sich diese als Textfile kopieren, Ihre vollständige Anschrift hinzufügen und dann PGP-signiert per Mail umgehend (spätestens bis 30. Mai 997) an krypto@cert.dfn.de (Subject: Für Verschlüsselungsfreiheit) senden oder indem Sie damit weitere Unterschriften sammeln und diese per Post an DFN-CERT, Universität Hamburg, Vogt-Kölln-Str. 30, 22527 Hamburg oder per Fax (040-54942241) dorthin schicken.

Gesehen in einer Internet Mail des DFN-CERT