SelfLinux-0.10.0

Vorwort

Autor: Mike Ashley ()
Formatierung: Matthias Hagedorn (*matthias.hagedorn@selflinux.org*)

Inhaltsverzeichnis

1Vorwort

> **Grundgesetz Artikel 10, Absatz 1:** Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.
>
> **Eckpunkte der deutschen Kryptopolitik**, verabschiedet vom deutschen Bundeskabinett am 2. Juni 1999: **Der Einsatz kryptographischer Verfahren ist von außerordentlicher Bedeutung für eine effiziente technische Kriminalprävention. Dies gilt sowohl für die Gewährleistung der Authentizität und Integrität des Datenverkehrs wie auch für den Schutz der Vertraulichkeit.**

Elektronische Daten spielen im Zeitalter des Computers und der weltweiten Vernetzung eine herausragende Rolle. Privatleute, Firmen, Politiker, Organisationen und Behörden machen zunehmend Gebrauch von der bequemen, schnellen und preisgünstigen Möglichkeit, per E-Mail zu kommunizieren, und nutzen elektronische Speichermedien (Festplatten, Disketten, CDROMs), um darauf ihre persönlichen Daten, Forschungsergebnisse, Firmengeheimnisse, Kunden- oder Patienteninformationen, Statisken, Notizen, Entwürfe, Umsatzzahlen usw. zu speichern. Bei der Abwicklung von Geschäftsvorgängen (Bestellung, Bezahlung, Verträge) spielt das Internet eine immer wichtigere Rolle. Den Weg, den Ihre Daten über das Internet zu einer Zieladresse gehen, können Sie weder vorhersagen noch vorherbestimmen. Alle Daten, die unverschlüsselt (oder mit einer unsicheren Methode verschlüsselt) über's Netz gehen, sind quasi öffentlich. Man muß davon ausgehen, das diese Daten - von wem auch immer - mitgelesen oder manipuliert und - zu welchem Zweck auch immer - mißbraucht werden können. Daten, die Sie auf Ihrem Computer abgespeichert haben, sind meist nicht sicher vor unbefugten Zugriffen. Viele Rechner sind nicht einmal mit einem Paßwortschutz versehen, und selbst bei vorhandenem Paßwortschutz gibt es vielfältige Möglichkeiten, an diese Daten zu gelangen. Noch nie war es so einfach und effektiv möglich, in Ihre Privatsphäre einzudringen oder Zugang zu Ihren vertraulichen Informationen zu erlangen.

2 Warum Kryptographie?

Kryptographie (die Wissenschaft von der Verschlüsselung) gewährleistet

* **Vertraulichkeit**
* **Integrität** und
* **Authentizität**

Ihrer Daten und Ihrer Kommunikation.

Wenn Sie E-Mails unverschlüsselt verschicken, müssen Sie sich darüber im klaren sein, dass deren Inhalt weniger vertraulich ist als bei einer Postkarte. Die Administratoren sowohl Ihres Mailservers als auch des Empfängers könnten ohne weiteres ihre E-Mails lesen, abfangen oder verändern. Auf ihrem Weg zum Empfänger durchlaufen E-Mails unter Umständen etliche Rechner. Jeder, der Zugang zu einem dieser Rechner hat, auch jeder Cracker, der durch irgendwelche Sicherheitslöcher in diese Rechner eindringt, kann mühelos auf Ihre E-Mails zugreifen. Unter Umständen werden Ihre E-Mails sogar auf der Festplatte eines dieser Zwischenrechner gespeichert. Auch könnte der Carrier, also der, der die Datenleitungen zu Verfügung stellt (in Deutschland meist die Deutsche Telekom oder Colt-Telekom) die Datenpakete, die über seine Leitungen gehen, gezielt filtern. Es ist auch nicht auszuschließen, daß jemand diese Leitungen von außen anzapft.

Es geht aber nicht allein darum, sich gegen Cracker oder korrupte Sytemadministratoren zu schützen, sondern auch gegen das planmäßige Eindringen staatlicher Organisationen (des eigenen oder eines anderen Landes) in Ihre Privatsphäre. Die Geheimdienste vieler Länder filtern heutzutage nicht nur Telefongespräche, sondern zunehmend auch die Daten, die über das Internet transportiert werden, um daraus wirtschaftlich, politisch oder für die Strafverfolgung nutzbare Daten zu gewinnen. Eine Studie der **Kommission zur Technikfolgeabschätzung des Europaparlamentes** (STOA - Scientific and Technological Options Assessment) über die **Entwicklung von Überwachungstechnologie und dem Risiko des Mißbrauchs wirtschaftlicher Informationen** zeigt beispielsweise, daß das Belauschen elekronischer Kommunikation bereits systematisch und in großem Stil betrieben wird. Eines der prominentesten Beispiele ist das ECHELON-System, das von den USA, Kanada, Großbritannien, Australien und Neuseeland gemeinsam unterhalten wird. Ursprünglich zum Belauschen des Ostblocks konzipiert, sammeln heute über 120 Stationen mit großem Aufwand Informationen unter anderem durch Abhören von Satellitenverbindungen und Transatlantikkabeln, um Daten über Einzelpersonen, Organisationen, Regierungen, Wirtschaftsunternehmen, Forschungsprojekte und internationale Institutionen zu gewinnen. Auf europäischer Ebene plant die Arbeitsgruppe **Polizeiliche Zusammenarbeit** des Europa-Rats konkrete Maßnahmen für die Überwachung des Telekommunikations-Verkehrs. Das **ENFOPOL 98** genannte Dokument schließt ausdrücklich das Internet und zukünftige Technologien mit ein.

Auch Daten, die unverschlüsselt auf der Festplatte Ihres Rechners oder einem anderen Speichermedium liegen, sind vor unbefugten Zugriffen nicht sicher. Jemand könnte sich über eine Netzwerkverbindung Zugang verschaffen bzw. sich durch Diebstahl oder Einbruch in Besitz Ihrer Daten bringen. Wenn Sie Ihre Daten verschlüsselt haben, kann ein Angreifer - selbst wenn er physisch im Besitz der Daten ist - nicht auf diese zugreifen.

Ein weiteres Problem ist das Authentifizieren von elektronischen Daten. Wie bereits oben erwähnt, ist es möglich, die Absenderadresse und den Inhalt eines E-Mails zu fälschen. Gerade bei offizieller oder geschäftlicher Korrespondenz, dem Austausch von Dokumenten und dem Abwickeln von Geschäftsvorgängen über das Internet ist es wichtig, den Absender eindeutig zu identifizieren und die Integrität der Daten überprüfen zu können.

Die einzige Möglichkeit, um Vertraulichkeit, Integrität und Authentizität von elektronischen Dokumenten zu gewährleisten, ist die Benutzung wirkungsvoller kryptographischer Verfahren, wie sie etwa bei GnuPG

Anwendung finden. Durch Verschlüsselung erreichen Sie, dass Ihre Daten nur von den Personen gelesen werden können, für die sie auch bestimmt sind. E-Mails werden quasi in einen Briefumschlag gesteckt, der nur vom Empfänger geöffnet werden kann. Darüberhinaus wird durch digitale Unterschriften eine eindeutige Zuordnung zum Urheber der Signatur möglich, und Manipulationen des Dokumentes oder Vortäuschen eines falschen Urhebers (Absenders) lassen sich feststellen.

In der Elektronischen Datenverarbeitung sollte für Sie die gleiche Sicherheit selbstverständlich sein wie in anderen Bereichen. Wahrscheinlich würden Sie weder ein intimes Liebesgeständnis, noch eine Mitteilung an Ihren Rechtsanwalt, noch Ihre wissenschaftliche oder geschäftliche Korrespondenz per Postkarte schicken. Auch lassen Sie wahrscheinlich keine vertraulichen Dokumente offen in Ihrer Wohnung oder an Ihrem Arbeitsplatz liegen. Ebensowenig würden Sie einen Kaufvertrag ohne rechtsgültige Unterschrift akzeptieren. Verschlüsselung und digitale Signaturen sollten also ein alltäglicher Vorgang für Sie sein. Ob Sie nun berufliches oder privates Interesse am Schutz Ihrer Daten haben: mangelndes Problembewußtsein ist das größte Risiko.

3 Warum GnuPG?

GnuPG (der GNU Privacy Guard) ist ein Programm zum Verschlüsseln und Signieren von digitalen Daten und arbeitet unabhängig von den jeweiligen Datenformaten (E-Mail, Textdateien, Bilddaten, Sourcecode, Datenbanken, komplette Festplatten usw.). Es entspricht der im RFC2440 festgelegten OpenPGP-Spezifikation und ist kompatibel zu PGP 5.x der Firma NAI. GnuPG verwendet dazu hauptsächlich ein hybrides Verfahren mit öffentlichem Schlüssel. Zum Verschlüsseln kann GnuPG aber ebenso ausschließlich symmetrische Verfahren einsetzen.

GnuPG ist derzeit eine der sichersten Anwendungen zum Verschlüsseln und Signieren von Daten. Bei sorgfältiger Anwendung ist eine Verschlüsselung mit GnuPG auch in absehbarer Zukunft nicht zu knacken. Im Gegensatz zu anderen Verschlüsselungsprogrammen wie beispielsweise PGP von der Firma NAI ist GnuPG freie Software. Das bedeutet unter anderem, dass der Programm-Quellcode frei verfügbar, frei von Patenten und frei von einschränkenden Lizenzbedingungen ist [2]. Jeder Anwender kann so das Programm auf seine Integrität hin prüfen. Das heißt beispielsweise, dass sich Hintertüren (Key Recovery) oder 'Generalschlüssel' (Key Escrow) nicht versteckt einbauen lassen und jeder Anwender die Möglichkeit hat, Fehler zu beseitigen, das Programm zu verbessern oder nach seinen Vorstellungen zu verändern. Darüberhinaus ist GnuPG nicht - wie beispielsweise amerikanische Verschlüsselungsprogramme - durch Ausfuhrbestimmungen künstlich in seiner Funktionalität und Sicherheit beschränkt.

4 Aufbau des Buches

Die grundlegenden Konzepte und Hintergründe der Verschlüsselung und digitaler Signaturen werden in Kapitel 1 Konzepte behandelt. Kapitel 2 Grundlagen führt in die Arbeit mit GnuPG ein; die wichtigsten Funktionen, Arbeitsschritte und Optionen werden dort am Beispiel erklärt. In Kapitel 3 Schlüsselverwaltung wird ausführlich auf das Editieren, Authentifizieren und Verwalten von Schlüsseln eingegangen. Auf die wichtigsten Aspekte des praktischen Einsatzes und das **Web of Trust** wird in Kapitel 4 GnuPG im Alltagsgebrauch eingegangen. Kapitel 5 gibt einen kurzen Überblick über die Kryptographie-Gesetzgebung. Im Anhang des Buches finden Sie ein ausführliches Glossar, das die verwendeten Fachausdrücke erklärt, ein Literaturverzeichnis, eine Sammlung von Internet-Ressourcen sowie eine Anleitung zur Installation von GnuPG.

5 Fußnoten

Cracker
Eine Person, die vorsätzlich, unbefugterweise und oft mit bösartiger Absicht in fremde Rechnersysteme

eindringt, im deutlichen Gegensatz zu **Hacker**, womit ein gutmeinender Computer-Freak gemeint ist (RFC 1983)

Lizenzbedingungen
GnuPG steht unter der sogenannten GNU General Public License (GPL) der Free Software Foundation.