Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Band: 75 (1997)

Heft: 12

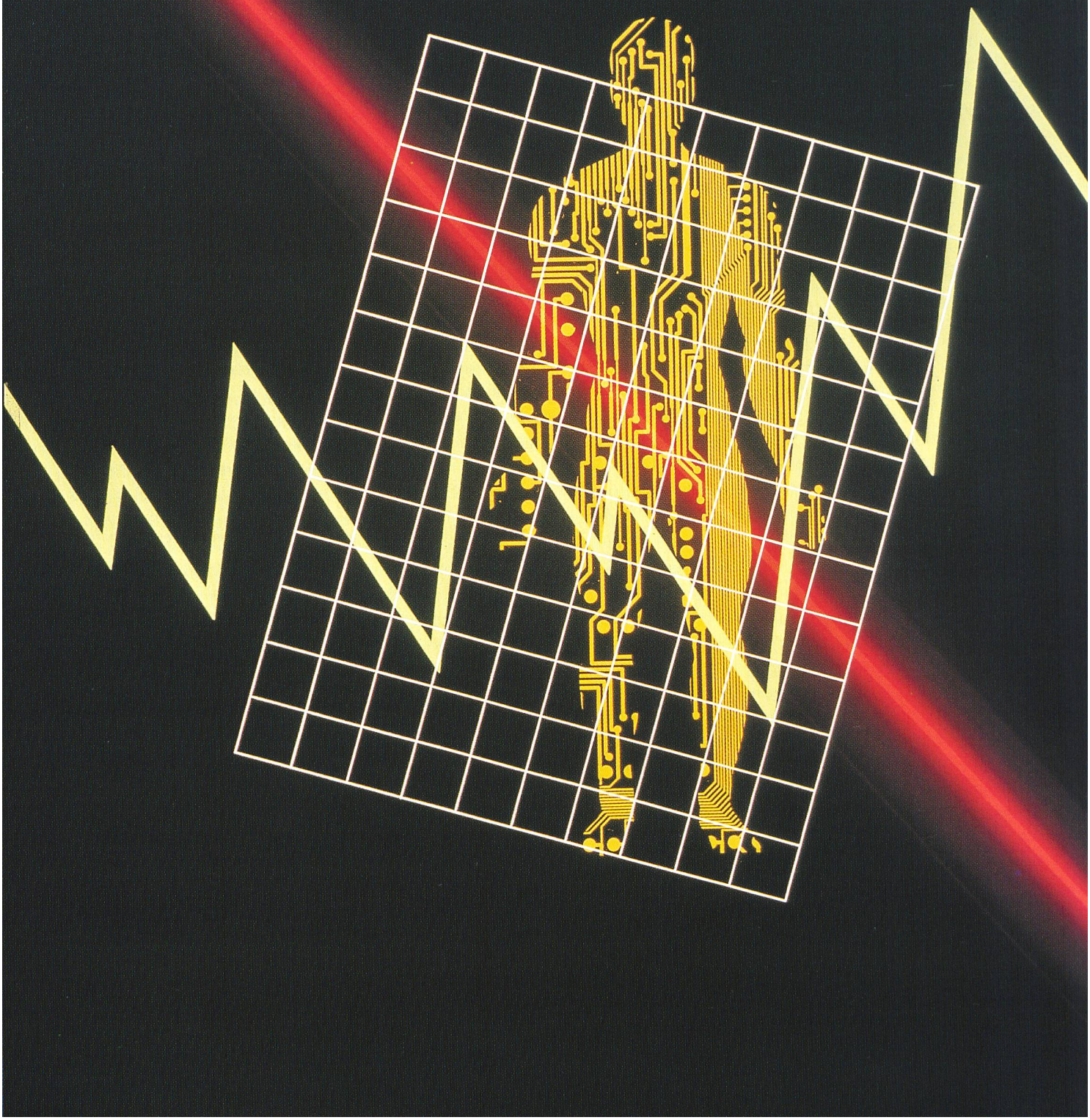
Artikel: Der Schlüssel zur Sicherheit

Autor: Schodl, Herbert

DOI: https://doi.org/10.5169/seals-876985

Sicherheit bei der Datenübertragung

Der Schlüssel zur Sicherheit



Die Vorteile privater und geschäftlicher Transaktionen über das Internet sind offensichtlich. Die Vernetzung hat aber durchaus ihre Schattenseiten. Während des Transports sind die Daten vor neugierigen Blicken wenig geschützt. In falsche Hände geratene Bankgeschäfte, Forschungsunterlagen oder Verwaltungsakten können katastrophale Folgen haben. Wie lassen sich die Daten jedoch bei der Übertragung schützen?

HERBERT SCHODL, VOLKETSWIL

Die einfachste Lösung ist die Chiffrierung der Daten mit einem Kryptosystem, bei dem Sender und Empfänger denselben Schlüssel und dasselbe Verschlüsselungsverfahren verwenden. Auf diese Weise arbeiten symmetrische Kryptosysteme, wie der Blockchiffrieralgorithmus *Data Encryption Standard* (DES), der von IBM entwickelt und 1977 vom National Bureau of Standards normiert wurde.
Bei der Blockchiffrierung wird der Klartext in eine Folge von Klartextblöcken fester Länge zerlegt und jeder davon mit Hilfe eines Schlüssels chiffriert. In der als *Electronic Code Book* (ECB) bezeichneten Grundbetriebsart des DES führt die Chiffrierung der Klartextblöcke mit ein und demselben Schlüssel zu Chiffretextblöcken, die unabhängig voneinander entschlüsselt werden können. Ein Übertragungsfehler hat in dieser Betriebsart daher auf die Dechiffrierbarkeit der anderen Blöcke keinen Einfluss. Da jedoch schon ein einziges Bit im Chiffretextblock zu erheblichen Verfälschungen im Klartextblock führen kann, wird schon bei einer relativ geringen Fehlerrate jede Kommunikation unmöglich.

Zertifizierte Sicherheit

In offenen Systemen ist diese Form der Chiffrierung allerdings nicht besonders hilfreich, da der gemeinsame Schlüssel normalerweise erst auf sicherem Weg zum Empfänger übertragen werden muss. Als Alternative bieten sich hier die sogenannten asymmetrischen Kryptosysteme an. Sie beruhen darauf, dass jeder Teilnehmer im Netz einen öffentlichen Schlüssel bereitstellt, mit dem an ihn gerichtete Sendungen von jedermann chiffriert werden können, die aber nur er mit seinem geheimen Schlüssel dechiffrieren kann.
Mit demselben Kryptosystem kann auch die Authentizität einer Nachricht sichergestellt werden. Dazu verschlüsselt der Sender ein Komprimat der Nachricht mit seinem geheimen Schlüssel und erzeugt damit eine Signatur, die jeder im Netz mit dem öffentlichen Schlüssel des Senders nachprüfen kann. Schliesslich ist es möglich, beide Möglichkeiten zu kombinieren, indem der Sender die Nachricht erst mit dem eigenen geheimen Schlüssel signiert und anschliessend mit dem öffentlichen Schlüssel des Empfängers verschlüsselt, während der Empfänger umgekehrt verfährt.
Damit die Urheberschaft einer Sendung zweifelsfrei ist, muss allerdings eine dritte Instanz für die Übereinstimmung zwischen öffentlichem Schlüssel und Sender bürgen. Das geschieht über eine Zertifizierungsinstanz, die öffentliche Schlüssel mit ihrem geheimen Schlüssel signiert. Die Richtigkeit des Zertifikats kann dann mit dem öffentlichen Schlüssel der Zertifizierungsinstanz nachgeprüft werden.

Staatlicher Widerstand

Wichtig ist natürlich, dass der geheime Schlüssel wirklich geheim und an den Eigentümer gebunden bleibt. Dies lässt sich dadurch erreichen, dass alle an den Eigentümer gebundenen sicherheitsrelevanten Daten entweder mit einem PIN-Code verschlüsselt werden, der nur dem Eigentümer allein bekannt ist, oder dass eine PIN-geschützte SmartCard verwendet wird, auf der die kryptographischen Berechnungen durchgeführt werden.
Das bekannteste asymmetrische Kryptosystem ist das von R. Rivest, A. Shamir und L. Adleman 1978 am *Massachusetts Institute of Technology* (MIT) entwickelte RSA-System. Es nutzt die Tatsache, dass das Produkt zweier Primzahlen für die Verschlüsselung ausreicht, für die Entschlüsselung jedoch beide Primzahlen bekannt sein müssen. Zwar lassen sich die Primzahlen theoretisch durch Auspro-

Glossar

Kryptographie:
Die Kryptographie ist eine Disziplin innerhalb der Informatik, die sich mit der Entwicklung und Bewertung von Verschlüsselungsverfahren beschäftigt.

Kryptosystem:
Ein Kryptosystem ist ein Verfahren, das einen Klartext mit Hilfe eines Schlüssels umkehrbar in einen Kryptotext transformiert.

Symmetrisches Kryptosystem:
Bei einem symmetrischen Kryptosystem wird für die Ver- wie für die Entschlüsselung der gleiche Schlüssel benutzt. Ohne die Kenntnis des geheimen Schlüssels ist es praktisch unmöglich, die Ver- und Entschlüsselung durchzuführen.

Asymmetrisches Kryptosystem:
Bei einem asymmetrischen Kryptosystem werden für die Ver- und Entschlüsselung zwei unterschiedliche Schlüssel benutzt. Sie stehen zwar in Beziehung zueinander, lassen sich aber praktisch nicht voneinander ableiten.

◄
Die Vorteile privater und geschäftlicher Transaktionen über das Internet sind offensichtlich. Die Vernetzung hat aber durchaus ihre Schattenseiten. Während des Transports sind die Daten vor neugierigen Blicken wenig geschützt (Foto: H. R. Bramaz).

bieren oder Faktorisierungsverfahren ermitteln, praktisch ist es jedoch mit den bisherigen Rechnern zu zeitaufwendig, das Produkt zweier grosser Primzahlen wieder in seine Primzahlen zu zerlegen. Als sicher gelten daher zurzeit Primzahlen mit etwa 300 Dezimalstellen, das entspricht einer Länge des Schlüssels von 1024 bit.
Noch ist offen, ob und wie die Kryptosysteme zukünftig eingesetzt werden. Natürlich werden auch Kriminelle und Verfassungsfeinde davon Gebrauch machen. Welche Regierung will das schon? Manche Länder versuchen daher die Länge des Schlüssels zu beschränken, um ihren Sicherheitskräften die Gelegenheit zu geben, den Schlüssel notfalls zu knacken. Was heute aber nur Sicherheitskräften möglich ist, kann mit einer neuen Rechnergeneration morgen jeder Hacker, und interessierte Kreise verfügen schon heute über eine gleichwertige Ausstattung wie die Sicherheitskräfte. Damit wären neue Möglichkeiten für Betrug und sonstigen Missbrauch gewissermassen vorprogrammiert. Andere Länder verbieten die Verschlüsselung gleich ganz oder verlangen einen Zugang zu den Schlüsseln, um Nachrichten gegebenenfalls lesen zu können. Ob das Erfolg haben wird, darf bezweifelt werden, denn die Verschlüsselung lässt sich zwar verbieten, verhindern wird man sie jedoch nicht können. [7]

Herbert Schodl
NCP engineering SA, Volketswil

Summary

The key to security

The advantages of routing private and business transactions via the Internet are obvious. But networking also has its drawbacks. During the transport the data are little protected against eavesdropping. The consequences can be catastrophic, if banking transactions, research documents or administrative documents fall into the wrong hands. But how can the data be protected during transmission?
The most simple solution is data encryption with a system in which the sender and the recipient use the same key and the same encryption method. This is the principle adopted by symmetrical encryption systems such as the block ciphering algorithm Data Encryption Standard (DES), which was developed by IBM and standardized by the National Bureau of Standards in 1977.

Digitale Unterschrift für elektronische Dokumente

Was auf herkömmlichen Geschäftsdokumenten die Unterschrift, ist im elektronischen Geschäftsverkehr auf dem Internet die digitale Signatur. Im Rahmen des Schwerpunktprogramms «Informations- und Kommunikationsstrukturen» des Schweizerischen Nationalfonds entwickeln die Schweizer Handelskammern zusammen mit spezialisierten Unternehmen ein einfach anzuwendendes digitales Signatursystem mit dem Namen Digisigna. Wenn sich damit schon bald Geschäfte im Internet technisch und rechtlich sicher abwickeln lassen, ist eine wichtige Voraussetzung für den grossen Aufschwung des elektronischen Marktes erfüllt. Denn Digisigna verhindert, dass elektronisch übermittelte Bestellungen, Zahlungsanweisungen und vertrauliche Informationen durch Unbefugte ausgelöst, abgefangen, eingesehen oder verfälscht werden. Geschäftspartner im Internet können damit ohne vorgängige gegenseitige Vereinbarung ihre Identität wechselseitig überprüfen und ihre Kommunikation verschlüsseln. Jeder Teilnehmer von Digisigna, sei es ein Firmenvertreter oder eine Privatperson, verfügt über zwei zusammengehörende Codes in Form von Zeichenreihen: Der öffentliche Schlüssel kann nach einem Beglaubigungsverfahren, welches in der Schweiz nach schweizerischem Recht abläuft, in einer Datenbank auf dem Internet abgerufen werden. Der nur dem Inhaber bekannte geheime Schlüssel ist über ein mathematisches Verfahren, das jeden Missbrauch ausschliesst, mit dem öffentlichen verknüpft. Wer digital signiert, verwendet seinen geheimen Schlüssel. Mit dem zugehörigen öffentlichen Schlüssel kann sein Geschäftspartner die Signatur überprüfen. Eine vertrauliche Botschaft verschlüsselt der Sender mit dem öffentlichen Code des Empfängers. Dieser entschlüsselt sie mit seinem privaten Code.

Die elektronischen Geschäftstransaktionen müssen technisch sicher und rechtlich sauber erfolgen können. So muss die Identität des Geschäftspartners einwandfrei feststehen. Wer ein elektronisches Dokument empfängt, muss Gewähr haben, dass dieses bei der Übermittlung nicht verändert wurde. Wie bei eingeschriebenen Postsendungen darf es dem Absender zudem nicht möglich sein, abzustreiten, ein Dokument geschickt zu haben. Schliesslich muss eine gute Verschlüsselung gewährleisten, dass vertrauliche Informationen nicht in falsche Hände gelangen.
Die Schweizer Handelskammern haben Digisigna als elektronischen Registrier- und Zertifizierungsdienst eingerichtet. Wollen Firmen oder Einzelpersonen miteinander ins elektronische Geschäft kommen, brauchen sie nicht mehr eine gegenseitige Vereinbarung zu treffen oder miteinander Chiffrierschlüssel auszutauschen. Digisigna sorgt für die Beglaubigung der digitalen Signaturen und betreibt eine Datenbank mit den öffentlichen Codes der Teilnehmenden.

Dr. Otto Müller
Zürcher Handelskammer
Bleicherweg 5
CH-8001 Zürich
Tel. 01 221 07 42
Fax 01 211 76 15
E-mail: omueller@zurichcci. ch
http://www.zurichcci.ch