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

Band: 78 (2000)

Heft: 9

Artikel: Doppelt verschlüsselt, um sicher zu sein

Autor: Venner, Kurt

DOI: https://doi.org/10.5169/seals-876479

Sicherheit im Internet

Doppelt verschlüsselt, um sicher zu sein

Viele Menschen haben Angst, ihre Kreditkartennummer für Belastungen des Kontos dem Web zu überlassen. Die Banken haben deshalb Sicherheitsschlüssel geschaffen, um die Kundschaft für das virtuelle Banking, besonders für das Handybanking, bei Laune zu halten. Algorithmen und Kryptographie spielen im Bereich Sicherheitsschlüssel eine wichtige Rolle.

TopSec 701: Die einfach ins Laptop gestecke PC-Karte erlaubt mit Hilfe starker Verschlüsselung eine sichere Anbindung an Firmennetze über Mobilfunk. Foto: Siemens

Für die Schweizer Banken ist die Verschlüsselungstechnologie mit Blick auf die Weiterentwicklung des elektronischen Banking sehr wichtig. Jede Meldung über Hackererfolge verängstigt die Kundschaft und bedroht den Umsatz in diesem zukunftsträchtigen Markt.

KURT VENNER, BERN

Swisskey-Zertifikat

Die Banken sind daher äusserst innovativ, um für dieses Problem Lösungen zu finden. Am Beispiel UBS soll im Folgenden aufgezeigt werden, wie eine Bank das Problem angegangen ist. Sie bietet heute ihren Kundinnen und Kunden für das Telebanking die Public-Key-Verschlüsselung (verschiedene korrelierte Teilschlüssel) mit Einsatz von digitalen Zertifikaten und die Chipkarte mit Krypto-Coprozessor. Die Bank preist ihre Internet Card als «Multiapplikationskarte der neusten Generation». Es handelt sich um eine Java Card, die mit den Spezifikationen des Open Card Framework konform ist. Auf der Card ist das persönliche Swisskey-Zertifikat des Nutzers gespeichert. Das Zertifikat ist eine elektronische Form der Identitätskarte, die auf dem Internet übermittelt werden kann. Dadurch lässt sich ein Kommunikationspartner identifizieren. Swisskey ist eine unabhängige Zertifizierstelle, die für eine hohe Qualität ihrer Zertifikate bürgt. UBS untersützt diese Stelle bei der sorgfältigen Identifizierung von Personen, die ein Swisskey-Zertifikat beantragen. Wer ein solches Zertifikat besitzt, kann seine E-Mails, die Programmcodes oder einen Webserver digital signieren. Die Signatur bestätigt dem Empfänger, dass am E-Mail- oder Programmcode unterwegs nichts verändert wurde. Gleichzeitig wird auch die Identität des Benutzers gewährleistet. Ausser dem User kann niemand etwas mit dessen digitalen Signatur unterschreiben. Denn mit jeder digitalen Unterschrift versendet der Benutzer mit dem Zertifikat nur den so genannten Public Key. Zum Signieren wird aber auch der Private Key des Zertifikates benötigt, der sich nur auf dem eigenen PC befindet.

Verschlüsselungs-Toolkits

Die Banken setzen grosse Hoffnungen auf die Verschlüsselungstechnologie, die weltweit ein gewichtiges Diskussionsthema, aber auch ein Business geworden ist. Die amerikanische Firma, die RSA Security Inc., ist eines von vielen Unternehmen, die heute ihr Geschäft mit der Sicherheit im Internet machen. Das Unternehmen präsentierte an der CeBIT 2000 eine interessante Produktelinie. Sie konzentriert sich auf drei Kernbereiche: Authentisierung, Verschlüsselung und Public Key Infrastructure (PKI).

Bei der Authentisierung wird gewährleistet, dass nur autorisierte Anwender Zugang zu Netzwerkdaten, Applikationen und Kommunikationseinrichtungen haben. Die von der Firma angebotenen Verschlüsselungs-Toolkits bieten Softwareentwicklern die Möglichkeit, Verschlüsselungskomponenten sowie Tools unabhängig von der Plattform in die unterschiedlichsten Applikationen zu implementieren.

Boom für Kryptographieprogramme?
Mitte Januar hat das «US Bureau of Export Administration» beschlossen, die Exportregelungen für Verschlüsselungsprodukte zu lockern. Sie können nun in alle Länder exportiert werden. RSA erhofft sich von der Aufhebung des Exportstopps einen Boom für Kryptographieprogramme. Die Forschungsabteilung der Firma arbeitet zurzeit an biometrischen Technologien, drahtlosen Technologien und Entwicklungstools, um PKI-Infrastrukturen anzupassen. Sie entwickelt kryptographische Algorithmen und arbeitet an der Komprimierung von Public-Key-Algorithmen, sodass sie im drahtlosen Raum schneller arbeiten.

Von Algorithmen und Kryptographie
Algorithmen verwandeln Daten so, dass sie nur noch mit dem entsprechenden Schlüssel zurückverwandelt werden können. Der Schlüssel ist eine mehr oder weniger lange Kette von Ziffern, die in der Formel eingesetzt wird. Je länger der verwendete Schlüssel ist, umso aufwändiger ist es, ihn zu knacken. Der Schutz sensibler elektronischer Daten vor einem unzulässigen Zugriff kann durch die Kryptographie sichergestellt werden. Sie wird primär für die vertrauenswürdige Abwicklung von Geschäftsprozessen benötigt. Die Reduzierung von Risiken, die Schäden verursachen können, spielt eine wichtige Rolle. Es gilt, den Fortbestand und das Wachstum, aber auch das Ansehen eines Unternehmens nicht zu gefährden. Kryptographie ist die Wissenschaft des Verschlüsselns, Verbergens und Verheimlichens. Die dazu verwendeten mathematischen Methoden werden aber nicht nur zur Verheimlichung von Informationen verwendet. Sie werden auch zur Gewährleistung der Datenunversehrtheit, zur Bestätigung der Identität der Teilnehmer (Authentisierung) und des Ursprungs der Informationen benützt.

Die Schlüssel der Schlüssel – Horror für Hacker
Die Welt der Verschlüsselungen dürfte den Hackern das Leben schwer machen, denn die Systeme werden immer komplexer. So gibt es in der Kryptographie so genannte symmetrische und asymmetrische Verfahren. Symmetrische oder Private-Key-Verfahren sind Verfahren, bei denen für die Verschlüsselung von Daten der gleiche Schlüssel verwendet wird wie zur Entschlüsselung. Asymmetrische oder Public-Key-Verfahren arbeiten mit zwei verschiedenen, aber korrelierten Teilschlüsseln. Wird eine Verschlüsselung mit einem der beiden Teilschlüssel durchgeführt, kann nur mit dem dazu passenden Teilschlüssel die korrekte Entschlüsselung erfolgen. Aus der Kenntnis des einen Teilschlüssels kann der andere nicht berechnet werden. Deshalb wird einer der beiden Schlüssel ohne Risiko als «öffentlicher Schlüssel» publiziert. Der andere Schlüssel muss geheim gehalten werden und wird entsprechend als «geheimer Schlüssel» bezeichnet. Eine der wichtigsten Anwendungen von Public-Key-Verfahren ist die digitale Signatur als Ersatz für Signaturen im üblichen Sinne. Das bekannteste Public-Key-Verfahren ist das RSA-Verfahren, mit dem sowohl signiert als auch verschlüsselt werden kann.

Je schneller der PC, umso länger der Schlüssel
Für die Verschlüsselung sind vier Faktoren ausschlaggebend: der verwendete Algorithmus, die Schlüsselgenerierung, die Schlüssellänge sowie die Aufbewahrung des Schlüssels. Bei symmetrischen Verschlüsselungsverfahren geht man heute davon aus, dass die Praxissicherheit gegeben ist, wenn man eine Schlüssellänge von 128 bit verwendet, wie dies zum Beispiel bei Windows 2000 der Fall ist. Da aber die Geschwindigkeit von Computern immer weiter steigt, müssen in der Folge auch die Schlüssellängen vergrössert werden. Galt vor zehn Jahren noch eine praktische Sicherheit bei einer Schlüssellänge von 64 bit, so ist diese heute auf 128 bit gestiegen und wird möglicherweise in zehn Jahren 256 bit erfordern. Das Gleiche gilt auch für die Public-Key-Verfahren. In der Vergangenheit bezeichnete man eine Schlüssellänge von 512 bit als sicher und heute sind es 1024 bit. Um langfristig Sicherheit zu gewährleisten, werden die Benutzer zur Verwendung von 2048-bit-Schlüsseln übergehen müssen.

Unsichere «geheime» Algorithmen
Trotz aller Bemühungen: Es gibt keine absolute Sicherheit, da die Sicherheit anwendbarer Algorithmen mathematisch nicht bewiesen werden kann. Ein Algorithmus gilt dann als sicher, wenn fünf Jahre nach dessen Veröffentlichung die Mathematiker der Welt nicht in der Lage sind, diesen mathematisch erfolgreich anzugreifen. Nicht publizierte «geheime» Algorithmen gelten – weil nicht durch Experten überprüfbar – als unsicher.

Manipulationssicherer mobiler Ausweis
Die Verschlüsselung spielt heute in der IT-Welt eine zentrale Rolle. So haben beispielsweise anfangs Februar Sonera SmartTrust – ein weiterer Anbieter von Sicherheitslösungen auf der Grundlage des PKI-Standards – und Finnlands zentrale Einwohnermeldebehörde eine Vereinbarung unterzeichnet. Sie wollen die elektronischen Identifizierungszertifikate in mobilen Netzen realisieren. Die Einwohnermeldebehörde und Sonera kooperieren in dem Projekt zur Integration der elektronischen Identifikation in die SIM-Karte von Mobiltelefonen. Als Ergebnis der Zusammenarbeit wird ein manipulationssicherer mobiler Ausweis entwickelt. Im Weiteren haben eQ Securities Ltd. und Sonera SmartTrust einen sicheren Brokerage-Service für Mobiltelefone entwickelt. eQ arbeitet auf der Grundlage der PKI-Infrastruktur, der digitalen Signatur sowie einer leistungsfähigen Datenverschlüsselung und ermöglicht damit den mobilen Aktienhandel in einem – wie Sonera unterstreicht – «sicheren Umfeld». Sie weist darauf hin, dass die Benutzerinnen und Benutzer von eQ Free sicher über ihr Mobiltelefon Aktien kaufen und verkaufen sowie Marktinformationen, Charts und Nachrichten über Aktienkurse empfangen können.

Sicherheit im Netz – ein Sorgenkind
Heute sind gegen dreissig Millionen Firmen im E-Kommerz tätig. Jährlich werden nur einige hunderttausend Pakete an Sicherheitssoftware verkauft. Doch nun soll der Weltmarkt bis 2004 auf annähernd 15 Mia. Franken wachsen. Bereits heute sind ganze Fachmessen dem Thema Sicherheit gewidmet. Das hat seinen Grund. Markus Trinkner, Sales Manager ECU Depth., Microsoft AG, Wallisellen, stellt fest, dass zum Angriff auf das Web heute viel Raum offen stehe. Die Quellen seien im Internet vor-

handen, sogar Anleitungen zum Hacken. Da werde etwa mit falschen IP-Adressen operiert. Sehr oft handle es sich um konzertierte Aktionen. Wie viele andere Softwarefirmen legt auch Microsoft grossen Wert auf den Sicherheitsaspekt bei der Produktentwicklung. Trinkner meint jedoch, es müssten noch sehr viele Erfahrungen gesammelt werden. Wenn die Sicherheit im Internet für alle Benutzer hergestellt werden solle, dann sei die Koordination, das heisst die koordinierte Aktion aller Hersteller nötig. Gemeinsame Lösungen seien gefragt. Die User ihrerseits müssten die Installation und die Konfiguration äusserst sorgfältig und genau abwickeln. Trinkner weist darauf hin, dass Microsoft verschiedenen Universitäten in den USA Forschungsaufträge erteilt habe: «Die Attacken werden unter die Lupe genommen. Es bestehen so genannte Penetration-Testteams, die Attacken durchführen.»

Zusammenarbeit gross geschrieben

Gefährlich sind die Betriebs- und die Entwicklungsblindheit. Das Einzelkämpfertum muss unter allen Umständen vermieden werden, indem unabhängige firmenexterne Stellen Überprüfungen der Sicherheitssysteme vornehmen. Um der Bedeutung der Sicherheit bei der neuen Generation von Softwareprodukten Rechnung zu tragen, hat Microsoft eine umfassende Sicherheitsinitiative ins Leben gerufen. Die neue Strategie beinhaltet neben der intensiven Zusammenarbeit mit namhaften, auf Computer- und Netzwerksicherheit spezialisierten Unternehmen auch das Engagement in Sicherheitsorganisationen. Microsoft ist aktives Mitglied bei der InfoSurance, einer Stiftung für die Sicherheit der Informationsinfrastruktur der Schweiz. Windows 2000 ist das erste Betriebssystem, das mit der 128-bit-Verschlüsselung ausgeliefert wird.

Im Juni 2000 wird in den USA erstmals ein Sicherheitsgipfel veranstaltet, an dem Vertreter aus Politik und Wissenschaft sowie der IT-Industrie und verschiedenen Kundensegmenten die dringlichsten Sicherheits- und Datenschutzfragen diskutieren und Lösungen erarbeiten werden. Der Gipfel soll in Zukunft jährlich stattfinden. Für Privatanwender ist zudem die Lancierung einer Sicherheits- und Datenschutzwebsite geplant. [7]

Kurt Venner, *Swisscom AG, Bern*

Summary

Double encoding, to be on the safe side

Many people are anxious about giving their credit card number for debiting their account on the Web. Banks have therefore developed a security code in order to reassure customers when they undertake virtual banking transactions, in particular banking on their mobile phone. Algorithms and cryptography play an important role in security codes. The banks have high hopes for encoding technology. There are four key factors for encoding: the algorithm used, code generation, code length and safekeeping of the code.

Ericsson

« Auf Vorwärtsstrategie »

Ein Ericsson-Handy mit Hochgeschwindigkeits-Funktionalität, Amerika-Frequenz und Bluetooth kommt anfangs des nächsten Jahres auf den Markt.

Der Aufbau der UMTS-Netze in Europa wird ein Marktvolumen von 300 bis 400 Mia. Franken auslösen. Ericsson rühmt sich derzeit eines Marktanteils von 30% am weltweiten

KURT VENNER, BERN

Branchenumsatz und ist hervorragend positioniert für die Zukunft. Aber auch der GSM-Ausbau (GPRS) ist ein wichtiges Thema für Ericsson. Die Firma präsentierte an einer Pressekonferenz das Ericsson-R520m – das erste GPRS-Telefon (General Packet Radio Services) mit Bluetooth.

Das Triple-Bandgerät R520m bietet sämtliche Funktionen für die rasche Datenübertragung: GPRS, High Speed Circuit Switched Data (HSCSD), drahtlose Bluetooth™-Technologie und WAP.

Neben maximaler Geschwindigkeit bietet das R520m dank des eingebauten Bluetooth-Chips umfassende drahtlose Verbindungsmöglichkeiten. Das R520m kann beispielsweise:

- zusammen mit dem Bluetooth-Headset verwendet oder über die Ericsson-Bluetooth-PC-Card mit einem PC verbunden werden.
- Das Gerät enthält ferner einen Terminkalender. Die automatische Datenabgleichung mit einem PC per WAP / Internet, Bluetooth, Infrarottechnologie oder Kabel ist möglich.
- Das R520m bietet einen Lautsprecher mit Freisprechfunktionen.
- Funktionen sind beispielsweise ein Telefonverzeichnis mit bis zu 511 Kontakten und intuitive Texteingabe. Anstatt für jeden Buchstaben mehrmals dieselbe Taste drücken zu müssen, wählt die Software im R520m aus einem Lexikon Wörter und Wendungen aus und nimmt vorweg, welches Wort oder welche Wendung der Benützer gerade schreibt. – Das Aussprechen eines Wortes genügt. Bereits sorgt die Spracherkennung dafür, dass das R520m aus der Bereitschaftsbetriebsart aktiviert wird und für die Sprachbefehle empfänglich ist.