erschien in: Kubicek et al (Hrsg.): "Multimedia@Verwaltung", Jahrbuch Telekommunikation und Gesellschaft 1999, Hüthig, 124-132

Stand der Sicherheitstechnik

Hannes Federrath, Andreas Pfitzmann

TU Dresden, Fakultät Informatik, 01062 Dresden
E-Mail: {federrath, pfitza}@inf.tu-dresden.de

1 Was bedeutet Sicherheit

Die heutigen Computernetze sind meist große heterogene Gebilde mit sehr vielen Betreibern und Anwendern. Die neuen Kommunikationsmedien sind inzwischen zu einer bedeutenden Infrastruktur gewachsen. Interessengegensätze zwischen Betreibern und Anwendern, aber auch zwischen den Betreibern selbst und natürlich auch zwischen Anwendern werden künftig auch über diese neuen Infrastrukturen ausgetragen. Folglich bedarf es Sicherheitsmechanismen, die niemanden, weder Betreiber noch Anwender, von der Nutzung der neuen Möglichkeiten ausschließen, und auch möglichst keine neuen Risiken mit sich bringen.

Tabelle 1. Gliederung von Schutzzielen

	Inhalte Worüber?	Umfeld Wer, wann, wo, mit wem, wie lange?
Unerwünschtes verhindern	Vertraulichkeit von Nachrichteninhalten	gegenseitige Anonymität der Anwender; Unbeobachtbarkeit der Anwender durch die Betreiber
Erwünschtes leisten	Integrität von Nachrichteninhalten	Zurechenbarkeit von Nachrichten zu Absendern
	Verfügbarkeit von Daten und Diensten	Erreichbarkeit von Anwendern

Die neuen Kommunikationsmedien sollen zunächst natürlich erwünschte Funktionen leisten, allerdings ebenso unerwünschte Funktionen oder Verhaltensweisen verhindern (Tabelle 1). Hier zeigt sich bereits der **Gegensatz in den Interessen**. Beispielsweise möchte ein „Information Broker“ über eine Person möglichst schnell und effizient viele aktuelle und richtige Informationen sammeln, während die Person selber möglicherweise ein Interesse und ein Recht an der Privatheit und Vertraulichkeit gegenüber dem Information Broker besitzt.

Schutzinteressen können sich nicht nur auf die über die Netze ausgetauschten Nachrichteninhalte beziehen, sondern gelten ebenfalls für den Schutz von Kommunikationsumständen; z. B. ist zu schützen, wer wann mit wem kommuniziert hat

(Anonymität und Unbeobachtbarkeit), aber es ist auch sicherzustellen, daß eine Nachricht nachprüfbar und beweisbar von einem bestimmten Absender stammt (Zurechenbarkeit).

Mehrseitige Sicherheit (Tabelle 2) bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.

Tabelle 2. Mehrseitige Sicherheit

Sicherheit mit minimalen Annahmen über andere:
• Jeder Beteiligte hat Sicherheitsinteressen. • Jeder Beteiligte kann seine Interessen formulieren. • Konflikte werden erkannt und Lösungen ausgehandelt. • Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen durchsetzen.

Die Realisierung von mehrseitiger Sicherheit führt nicht zwangsläufig dazu, daß die Interessen aller Beteiligten erfüllt werden. Sie gewährleistet jedoch, daß die Partner einer mehrseitig sicheren Kommunikationsbeziehung in einem geklärten Kräfteverhältnis bzgl. Sicherheit miteinander interagieren.

2 Was bedeutet Stand der Sicherheitstechnik?

Natürlich existieren heute in der Forschung bereits Konzepte und Verfahren, die – wenn überhaupt jemals – erst in einigen Jahren als Produkte zu haben sind. Das Kontinuum des Entwicklungsstands reicht dabei über folgende Stufen:

- Stand der Forschung vs.
- Stand der Labormuster vs.
- Stand der verfügbaren Produkte vs.
- Stand der verkauften Produkte.

Mit der zunehmenden Sensibilisierung der Anwender und Betreiber und damit der verstärkten Nachfrage nach Sicherheit wird der Umsetzungsprozeß gerade auch im Sicherheitsbereich beschleunigt. Insbesondere im Bereich der Verschlüsselungstechnik wurde das in den letzten Jahren deutlich.

In Tabelle 3 wird für die verschiedenen Bausteine der Sicherheitstechnik ein Überblick über den Entwicklungsstand gegeben. Die einzelnen Bausteine werden in Abschnitt 3 kurz erläutert.

Leider wurde die Entwicklung von Sicherheitsverfahren viele Jahre als **Geheimwissenschaft** angesehen. Diese Sicht hatte ihren Ursprung in der für militärische Zwecke und damit für eine geschlossene Benutzergruppe entwickelten Technik. Mit

dem Einsatz von Sicherheits- und Verschlüsselungstechniken im privaten, geschäftlichen und internationalen Bereich wächst jedoch die Offenheit der Kommunikation, das heißt, es kommunizieren auch Menschen miteinander, die nie vorher in irgendeiner Beziehung zueinander standen. Für viele Sicherheitsmechanismen müssen sich die kommunizierenden Partner aber auf eine gemeinsame technische Basis einigen, z. B. die Wahl des Verschlüsselungsverfahrens. Ein Verfahren, das der eine Kommunikationspartner für vertrauenswürdig und sicher hält, kann für den anderen jedoch als völlig unsicher, unbekannt oder möglicherweise verboten eingestuft sein. In offenen Netzen ist daher auch ein **offener Entwurf** der Sicherheitstechnik notwendig, damit die Stärke der Verfahren untersucht und bewertet wird und den guten Verfahren schließlich vertraut werden kann.

Tabelle 3. Stand der Sicherheitstechnik

Bausteine der Sicherheitstechnik	Physisch sichere Geräte	Betriebssysteme	Kryptographie	Steganographie	Datenvermeidungstechniken	Techniken zur Verteilung von Kontrolle
Stand der Forschung	kaum Veröffentlichungen	sehr gut	sehr gut	gut	sehr gut	sehr gut
Labormuster	schwer zu beurteilen, Me-Chip	gut, Hydra, Multics	gut	befriedigend	gut	gut
verfügbare Produkte	miserabel, Chipkarten	schlecht, Windows NT, Linux	gut, PGP	miserabel	befriedigend, Onion Routing	—
verkaufte Produkte	miserabel, Chipkarten	miserabel, Windows 98, Mac OS	gut, PGP	miserabel	schlecht, Proxies	—

3 Bausteine der Sicherheitstechnik

In den folgenden Abschnitten wird auf die folgenden Bausteine der Sicherheitstechnik (siehe auch Tabelle 3) jeweils kurz eingegangen:

- Physisch sichere Geräte,
- sichere Betriebssysteme,
- Kryptographie,
- Steganographie,

- Datenvermeidungstechniken, z. B. Anonymität, Pseudonymität und Unbeobachtbarkeit,
- Techniken zur Verteilung von Kontrolle.

Technik allein genügt jedoch nicht, um die Sicherheit der Betreiber und Anwender zu erreichen. Auch organisatorische Komponenten müssen realisiert werden, z. B.

- Zertifizierung von Komponenten,
- Zertifizierung von Schlüsseln (Public Key Infrastructure, PKI).

3.1 Physisch sichere Geräte und sichere Betriebssysteme

Um sichere Kommunikation zu erreichen, werden Geräte (Hardware) und Programme (Software) benötigt, die für denjenigen, der sie benutzt, sicher sind. Diese persönliche Rechenumgebung ist der **Vertrauensbereich** des Benutzers.

Dies betrifft zunächst den persönlichen Rechner zu Hause und am Arbeitsplatz. In den heute weit verbreiteten PC-Betriebssystemen (DOS, Windows 95/98, MacOS) fehlt leider die Zugriffskontrolle, so daß der Ausbreitung von Viren und trojanischen Pferden Tür und Tor geöffnet ist. Leider sind diese und weniger unsichere Betriebssystemvarianten wie Windows NT mit Zugriffskontrolle in ihren inneren Funktionen nicht bekannt genug und vom Hersteller offengelegt, um ihnen genügend vertrauen zu können. Die Existenz Trojanischer Pferde kann somit nicht völlig ausgeschlossen werden. Trojanische Pferde können nicht nur die Vertraulichkeit von privaten oder geschäftlichen Geheimnissen verletzen; sie sind in der Lage, alle Schutzziele, also auch Integrität und Verfügbarkeit zu verletzen. Im schlimmsten Fall kann ein Trojanisches Pferd seine Schadensfunktion modifizieren und sich so an seine aktuelle Umgebung anpassen und sogar sich selbst zerstören, nachdem es seine Aufgabe erfüllt hat, um die hinterlassenen Spuren zu vernichten.

Die Sicherheit eines Betriebssystems ist essentiell für die sichere Benutzung von Anwendungen auf einem Rechner. Da alle Programmbefehle und Daten vom Betriebssystem interpretiert und verarbeitet werden, kann es keine Manipulationssicherheit oder Vertraulichkeit reiner Softwareanwendungen und ihrer Daten vor dem Betriebssystem geben (nach oben zeigender Pfeil in Abbildung 1).

Umgekehrt ist ein sicheres Betriebssystem jedoch in der Lage, sich vor Angriffen durch Anwendungen oder – prinzipieller formuliert – den höheren Schichten eines Systems zu schützen (durchgestrichener, nach unten zeigender Pfeil in Abbildung 1). Die Schichtenstruktur von Systemen macht auch klar, daß dies ebenso für die Beziehung zwischen Betriebssystem und Rechner gilt, auf dem das Betriebssystem läuft. Für den Fall, daß sichere Systemkomponenten lediglich kommunizieren, sind unkontrollierbare Angriffe nicht möglich, da hier nichts gegenseitig ausgeführt oder interpretiert wird. Um Angriffe des zwischen den Systemkomponenten liegenden

Mediums auszuschließen, kommen die klassischen kryptographischen Verfahren (siehe Abschnitt 3.2) zum Einsatz.

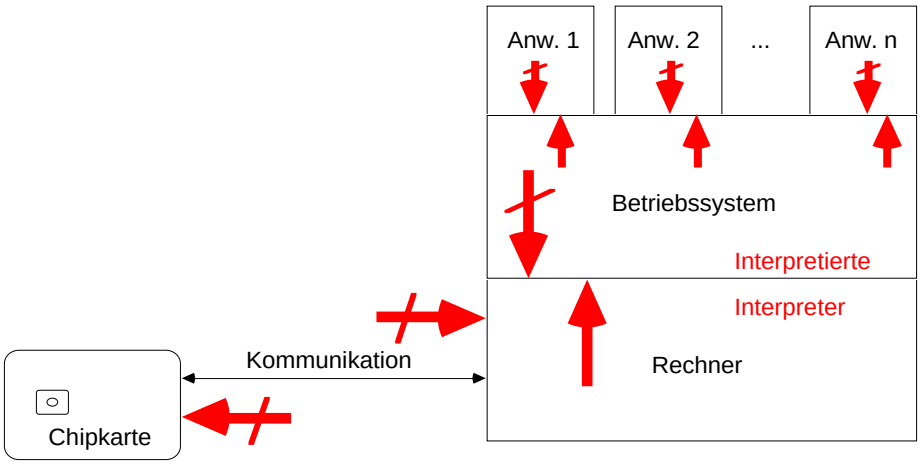

Abbildung 1. Verhältnis von Schichtenstruktur und Angriffserfolg

Die Notwendigkeit eines Vertrauensbereichs geht aber über den PC hinaus. Sie gilt je nach dem, wer sich schützen will (Betreiber, Anwender), in jeder Größenskalierung (siehe Abbildung 2).

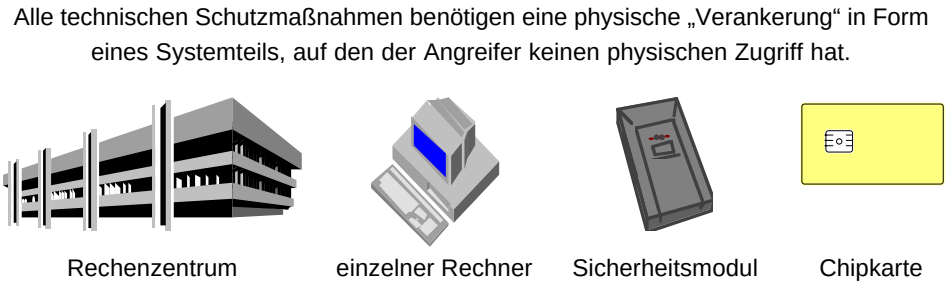

Abbildung 2. Die Größe physisch sicherer Geräte muß skalierbar sein

Besonders kritisch wird die Situation, wenn die für seinen Benutzer vertrauenswürdigen Systemteile (Geräte) zum Erbringen ihrer Funktion in Systemteile (Geräte) anderer integriert (z. B. hineingesteckt) werden müssen. Ein besonders kritisches Gerät ist in dieser Beziehung die Chipkarte. Im Normalfall muß die Chipkarte, die durch eine Persönliche Identifikationsnummer (PIN) vor unberechtigter Verwendung geschützt ist, bei der Benutzung in ein Lesegerät eingeführt werden. Die Tastatur am Lesegerät ermöglicht die Eingabe der PIN und damit die Aktivierung der Chipkarte. Der Besitzer der Chipkarte darf in einem solchen Fall nicht nur seiner Chipkarte vertrauen, sondern muß seinen Vertrauensbereich auch auf das Lesegerät

erweitern, da das Lesegerät in Kenntnis des Aktivierungscodes gelangt und somit in der Lage ist, nicht autorisierte Aktionen (z. B. Zahlungen, digitale Signaturen) auszulösen, zumindest solange die Chipkarte im Leser verbleibt oder wenn sie zu einem späteren Zeitpunkt erneut eingeführt wird.
Eine technische Darstellung zur Gestaltung physisch sicherer Geräte ist z. B. in [PPSW_95, PPSW_97] zu finden.

3.2 Kryptographie und Steganographie

Kryptographie ist die wichtigste Grundtechnik zur Sicherung der Vertraulichkeit und Integrität von übermittelten Nachrichten gegenüber Abhören (Konzelationssysteme) und Manipulation (Authentikationssysteme) durch Außenstehende. Bei **symmetrischen** Kryptosystemen besitzen sowohl der Sender als auch der Empfänger den gleichen Schlüssel. Bei **asymmetrischen** Kryptosystemen sind die Schlüssel unterschiedlich. In der Regel ist bei asymmetrischen Konzelationssystemen der Verschlüsselungsschlüssel öffentlich bekannt, während der Empfänger seinen Entschlüsselungsschlüssel geheim hält. Bei asymmetrischen Authentikationssystemen, die unter dem geläufigeren Namen „digitale Signatursysteme“ bekannt sind, wird der Signaturschlüssel geheim gehalten, während der Testschlüssel veröffentlicht werden kann. Mit dem Testschlüssel kann so jeder eine Signatur auf Echtheit überprüfen.
Symmetrische Kryptosysteme lassen sich meist effizienter realisieren als asymmetrische Kryptosysteme. Mit asymmetrischen Kryptosystemen lassen sich jedoch Anwendungen realisieren, die mit symmetrischen Kryptosystemen allein nicht realisierbar wären. Ein Beispiel hierfür ist die digitale Signatur. Da der Signaturschlüssel nur dem Unterzeichner einer Nachricht bekannt ist und niemandem sonst, ist auch nur er und sonst niemand in der Lage, eine Signatur zu leisten. Da der Testschlüssel zum Prüfen einer Signatur öffentlich ist, kann jeder, also nicht nur der Empfänger einer Nachricht, sondern auch Dritte (z. B. eine Schiedsstelle bei einem Streitfall) prüfen. Ein symmetrisches Authentikationssystem, das deutlich weniger rechenaufwendig ist als ein digitales Signatursystem, leistet dies jedoch nicht. Da hier sowohl der Unterzeichner einer Nachricht als auch der Empfänger den gleichen Schlüssel besitzen, ist auch der Empfänger einer Nachricht in der Lage, eine Nachricht zu unterzeichnen. Kommt es zwischen Empfänger und Sender zum Streit, wer die Nachricht unterzeichnet hat (z. B. könnte der Empfänger eine Warenbestellung des Senders manipulieren) ist für einen Dritten nicht entscheidbar, wer von beiden manipuliert hat.
Seit einigen Jahren entwickelt sich verstärkt ein neues Forschungsgebiet, das sich insbesondere mit dem Verbergen von Nachrichten beschäftigt. Mit **Steganographie**

können geheime Nachrichten über offene, unsichere Datennetze übermittelt werden, ohne daß deren Existenz für Außenstehende überhaupt bemerkbar ist. Mit Steganographie wird eine geheimzuhaltende Nachricht in eine Hülle derart eingebettet, daß im Ergebnis die minimalen Veränderungen der Hülle kaum bzw. nicht erkennbar sind und die Veränderungen selbst mit Meßmethoden nicht nachweisbar sind.

Als Hülle kann jedes Medium dienen, das einen indeterministischen Prozeß, z. B. eine Quantisierung, durchlaufen hat. Digitalisierte Sprache oder Musik, digitalisierte Bilder, Videos etc. sind hervorragend als Medien geeignet. Im Computer künstlich erzeugte Grafiken sind weniger gut geeignet. Steganographie ist technisch gesehen keine Verschlüsselung von Daten. Abbildung 3 soll dies deutlich machen.

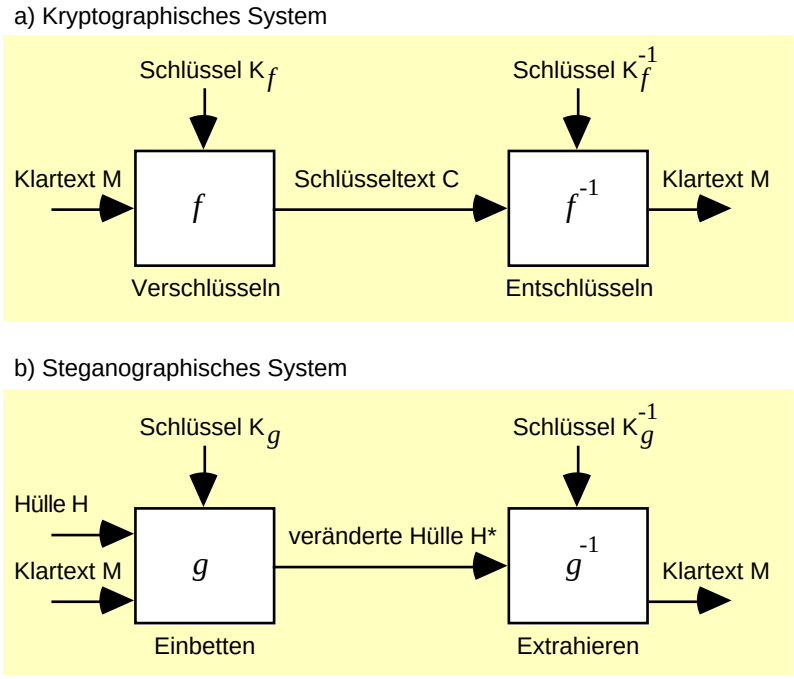

Abbildung 3. Grundaufbau von kryptographischem und steganographischem System

Während bei Kryptographie der Klartext M mittels einer kryptographischen Funktion f in einen für jeden Außenstehenden, d. h. jeden, der nicht den Schlüssel K_f^{-1} besitzt, unleserlichen Schlüsseltext C überführt wird, entsteht bei Steganographie als Ergebnis der Einbettungsfunktion g eine veränderte Hülle H^*, die für jeden Außenstehenden, d. h. jeden, der nicht den Schlüssel K_g^{-1} besitzt, ebenso eine unveränderte Hülle H hätte sein können.

Auf den Punkt gebracht bedeutet dies, daß die Verwendung von Verschlüsselung für den Außenstehenden zumindest erkennbar ist. Obwohl er nicht in Kenntnis des Nachrichteninhalts kommt, entsteht zumindest der Verdacht, daß die Kommunikationspartner etwas zu verbergen haben. Die Steganographie geht hier einen anderen Weg und kann damit die Existenz einer geheimen Botschaft verbergen. In einer offenen, unverfänglichen und unverschlüsselten Kommunikation wird unbemerkt eine geheime Botschaft transportiert. Das Grundprinzip der Steganographie setzt keine vorherige Verschlüsselung der geheimen Botschaft voraus, obgleich sie der Geheimhaltung nicht schadet und zumindest bei Steganographie von zweifelhafter Stärke sehr zu empfehlen ist.
Auch die Diskussionen um ein Kryptoverbot führten zu einer verstärkten Beachtung der Steganographie. Neueste Erkenntnisse zeigen jedoch, daß einige der öffentlich bekannten und im Internet zugänglichen Verfahren Schwächen aufweisen und daß deren Beseitigung möglich ist (siehe z. B. [West_97]). So paradox es klingen mag: Die Kryptodebatte trägt dazu bei, daß steganographische Verfahren schrittweise verbessert und damit sicherer werden. Hinzu kam und kommt die zunehmende Bedeutung von Multimedia und der damit verbundene Wunsch, auch die Urheberrechte bei der Verbreitung digitaler Objekte (Daten, Programme, Computerkunst etc.) über CD-ROM und Internet zu sichern. Die hierzu verwendeten technischen Mechanismen des Watermarking und Fingerprinting sind der Steganographie sehr ähnlich. Anstelle einer geheimen Botschaft wird in das digitale Objekt Information über den Urheber bzw. Käufer eingebettet.

3.3 Datenvermeidungstechniken

Es ist nicht das primäre Interesse eines Betreibers, beispielsweise Daten über seine Nutzer zu sammeln, um diese anschließend mißbräuchlich zu verwenden. Im Gegenteil: Je weniger Daten ein Betreiber zur Diensterbringung benötigt, umso weniger Kosten fallen für deren Verarbeitung und Schutz an. Außerdem reduzieren sich natürlich die Mißbrauchsmöglichkeiten. Dieses Ziel verfolgen Datenvermeidungstechniken.
Mit Hilfe von Datenvermeidungstechniken kann anonyme und unbeobachtbare Kommunikation realisiert werden. Eine Darstellung der Verfahren zur unbeobachtbaren Kommunikation findet man z. B. in [FePf_97]. Manche Anwendung erfordert aber auch die Zurechenbarkeit von Aktionen (z. B. Bestellungen) zu ihrem Akteur (Tabelle 4). **Pseudonymität** gestattet die Verknüpfung von Anonymität und Zurechenbarkeit. Das bedeutet, Transaktionen werden nicht unter der Identität des Akteurs durchgeführt, sondern unter einem Kennzeichen (Pseudonym), das ggf. (z. B. im Streitfall) aufgedeckt werden kann, d. h. mit der Identität verknüpft wird. In

Anwendungen mit bekannter Schadenshöhe im Betrugsfall können Pseudonyme so gebildet werden, daß die Aufdeckung unmöglich ist, allerdings muß dann vom Akteur eine Geldhinterlegung bei einem aktiven Treuhänder erfolgen, damit im Betrugsfall ein Ausgleich des Schadens möglich ist. Eine Darstellung der Verfahren zur Pseudonymität findet man z. B. in [PWP_90].

Tabelle 4. Datenvermeidungstechniken

	Unbeobachtbare Kommunikation	Verfahren für pseudonyme Transaktionen
Wer ist zu schützen?	• Schutz des Senders • Schutz des Empfängers • Schutz der Kommunikationsbeziehung	• Schutz des Kunden • Schutz des Händlers • Schutz der Bank
Grundkonzepte	• Broadcast mit impliziter Adressierung • Dummy Traffic • Proxys • Mix-Netze • DC-Netze • Steganographie	• Pseudonymität, d. h. digitale Signaturen relativ zu Pseudonym (= öffentlicher Testschlüssel) - Identifizierung im Betrugsfall (Zertifizierungsinstanz, die Identität kennt): unkontrollierbar - Geldhinterlegung für Haftung (aktiver Treuhänder): kontrollierbar • Werteaustauschprotokolle • digitale Zahlungssysteme • Umrechenbare Beglaubigungen (Credentials)

3.4 Verteilung von Kontrolle und organisatorische Aspekte

Um Vertrauenswürdigkeit zu erreichen, muß es möglich sein, Systeme zu verifizieren. Das bedeutet, unabhängige, (frei) wählbare Experten vergewissern sich von der korrekten Implementierung und Arbeitsweise eines Systems gemäß einer vorherigen Spezifikation. Da dem normalen Anwender meist weder die Mittel noch das Wissen zur Verfügung stehen, um Systemkomponenten oder gar ganze Systeme zu verifizieren oder zumindest zu validieren, kann diese Aufgabe durch unabhängige Stellen durchgeführt und das System so zertifiziert werden.

Im weiteren Sinn bedeutet Verteilung von Kontrolle auch, daß Systeme nicht nur von einem Hersteller (Entwicker, Administrator) entwickelt, produziert, angeboten und betreut werden sollen, sondern von vielen. Solange beispielsweise kein perfektes Betriebssystem existiert, sollte der Anwender die Auswahl unter mehreren Betriebssystemen haben.

Die Zertifizierung von öffentlichen Testschlüsseln der digitalen Signatursysteme wird meist in einer Zertifizierungsstelle durchgeführt. Diese Einrichtung ist eine sehr wesentliche Komponente einer Public Key Infrastructure (PKI), da sie die Gewähr dafür übernimmt, daß ein Testschlüssel auch wirklich zu einer Person gehört. Dies kann nicht durch rein technische Mittel erbracht werden, sondern umfaßt auch organisatorische Mittel, z. B. Überprüfung von Ausweisdokumenten und Regelungen für den Streitfall.

4 Sicherheitsinfrastruktur

Für eine gute und tragfähige Sicherheitsinfrastruktur wird folgende **Basisstruktur** benötigt:

- für den Teilnehmer sichere (portable) Endgeräte,
- zertifizierte Testschlüssel für digitale Signatursysteme,
- ein verfügbares Kommunikationsnetz,
- verfügbare Verzeichnisdienste sowie
- ein entsprechender Rechtsrahmen.

Die derzeit schwächste und am wenigsten tragfähige Komponente sind die für den Teilnehmer sicheren Endgeräte mit ihrer darauf laufenden Software. Besonders in diesem Bereich müssen noch erhebliche Entwicklungsarbeiten geleistet werden. Außerdem zeigt sich, daß beispielsweise die Sicherheit von Chipkarten bestenfalls auf Zeit gelingt, da neue Angriffsmöglichkeiten entdeckt werden.

Literatur

FePf_97 Hannes Federrath, Andreas Pfitzmann: Bausteine zur Realisierung mehrseitiger Sicherheit. in: Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-Longman 1997, 83-104.

PPSW_95 Andreas Pfitzmann, Birgit Pfitzmann, Matthias Schunter, Michael Waidner: Vertrauenswürdiger Entwurf portabler Benutzerendgeräte und Sicherheitsmodule. in: Hans H. Brüggemann, Waltraud Gerhardt-Häckl (Hrsg.): Verläßliche IT-Systeme, Proceedings der GI-Fachtagung VIS '95, DuD Fachbeiträge, Vieweg, Wiesbaden 1995, 329-350.

PPSW_97 Andreas Pfitzmann, Birgit Pfitzmann, Matthias Schunter, Michael Waidner: Trusting Mobile User Devices and Security Modules. Computer 30/2 (1997) 61-68.

PWP_90 Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen. Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315.

West_97 Andreas Westfeld: Steganographie in komprimierten Videosignalen. Diplomarbeit, TU Dresden, Institut für Theoretische Informatik, Juli 1997.

STICHWORTE: Sicherheit, Mehrseitige Sicherheit, Datenschutz, Sicherheitsinfrastruktur, Chipkarten.

HANNES FEDERRATH ist Wissenschaftlicher Mitarbeiter an der Fakultät Informatik der Technischen Universität Dresden. Promotion über die Sicherheit in Mobilkommunikationsnetzen, Arbeitsgebiete: Sicherheit in verteilten Systemen, Technischer Datenschutz in Mobilkommunikationssystemen, Anonymität im Internet.

ANDREAS PFITZMANN ist Professor für Informations- und Kodierungstheorie an der Fakultät Informatik der Technischen Universität Dresden. Arbeitsgebiet: Technischer Datenschutz durch verteilte Systeme.