In: Alexander Rossnagel (Hg.): Handbuch des Datenschutzrechts, Beck Verlag, 2002.

2.1 Technische Grundlagen

Dr. Hannes Federrath, Prof. Dr. Andreas Pfitzmann

TU Dresden, Fakultät Informatik, 01062 Dresden

{federrath, pfitza}@inf.tu-dresden.de

Übersicht

Literatur

Chau_81 David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24/2 (1981) 84-88.

Chau_85 David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044.

Chau_88 David Chaum: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. Journal of Cryptology 1/1 (1988) 65-75.

CoBi_95 David A. Cooper, Kenneth P. Birman: Preserving Privacy in a Network of Mobile Computers. 1995 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamitos 1995, 26-38.

Denn_90 Peter J. Denning (ed.): Computers under attack: intruders, worms and viruses. ACM Press, New York 1990.

Fede_99 Hannes Federrath: Sicherheit mobiler Kommunikation. DuD Fachbeiträge, Vieweg, Wiesbaden 1999.

Ferb_92 David Ferbrache: A Pathology of Computer Viruses. Springer-Verlag, Berlin 1992.

GGHI_89 Winfried Gleißner, Rüdiger Grimm, Siegfried Herda, Hartmut Isselhorst: Manipulation in Rechnern und Netzen – Risiken, Bedrohungen, Gegenmaßnahmen. Addison-Wesley, Bonn 1989.

IHW_96 Proc. 1st Workshop on Information Hiding, LNCS 1174, Springer-Verlag, Berlin 1996.

IHW_98 Proc. 2nd Workshop on Information Hiding, LNCS 1525, Springer-Verlag, Berlin 1998.

KöKP_00 Kristian Köhntopp, Marit Köhntopp, Andreas Pfitzmann: Sicherheit durch Open Source? Chancen und Grenzen. Datenschutz und Datensicherung DuD 24/9 (2000), 508-513.

MüPf_97 Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-Longman 1997.

MüRa_99 Günter Müller, Kai Rannenberg (Ed.): Multilateral Security in Communications, Addison-Wesley-Longman 1999.

Pfit_90 Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz. IFB 234, Springer-Verlag, Berlin 1990.

Pfit_99 Andreas Pfitzmann: Datenschutz durch Technik – Vorschlag für eine Systematik; DuD, Datenschutz und Datensicherheit, Vieweg-Verlag 23/7 (1999) 405-408.

PfPf_90 Birgit Pfitzmann, Andreas Pfitzmann: How to Break the Direct RSA-Implementation of MIXes. Eurocrypt '89, LNCS 434, Springer-Verlag, Berlin 1990, 373-381.

PfPW_88 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Datenschutz garantierende offene Kommunikationsnetze. Informatik-Spektrum 11/3 (1988) 118-142.

PfPW_91 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: ISDN-MIXes – Untraceable Communication with Very Small Bandwidth Overhead. Proc. Kommunikation in verteilten Systemen, IFB 267, Springer-Verlag, Berlin 1991, 451-463.

PiSM_82 R.L. Pickholtz, D.L. Schilling, L.B. Milstein: Theory of Spread-Spectrum-Communications – A Tutorial. IEEE Transactions on Communications 30/5 (1982) 855-878.

PPSW_95 Andreas Pfitzmann, Birgit Pfitzmann, Matthias Schunter, Michael Waidner: Vertrauenswürdiger Entwurf portabler Benutzerendgeräte und Sicherheitsmodule. Hans H. Brüggemann, Waltraud Gerhardt-Häckl (ed.): 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.

PPWW_00 Andreas Pfitzmann, Alexander Schill, Andreas Westfeld, Gritta Wolf: Mehrseitige Sicherheit in offenen Netzen; Grundlagen, praktische Umsetzung und in Java implementierte Demonstrations-Software; DuD-Fachbeiträge, Vieweg-Verlag, Wiesbaden 2000.

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.

Schn_96 Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, (2nd ed.) New York 1996.

Torr_92 Don J. Torrieri: Principles of Secure Communication Systems. 2nd ed., Artech House Books, 1992.

WoPf_00 Gritta Wolf, Andreas Pfitzmann: Charakteristika von Schutzzielen und Konsequenzen für Benutzungsschnittstellen; Informatik-Spektrum 23/3 (2000) 173-191.

A. Einführung

Informationstechnische Systeme (IT-Systeme) verarbeiten, transportieren und speichern digitale Daten. Die Verarbeitung und der Transport werden immer schneller, das Speichern wird immer preiswerter. Es ist innerhalb der nächsten Jahrzehnte zu erwarten, daß immer kleinere und

leistungsfähigere Rechner überall zur Verfügung stehen werden. Während früher wenige Großrechner und Datenbanken durch wenige Betreiber, die vergleichsweise leicht kontrolliert werden konnten, bedient wurden, sind heute alle Betroffenen selbst Betreiber und Teilnehmer an der Datenverarbeitung. Diese neue Situation führt dazu, daß sich der Teilnehmer auch selbst um seine eigene und die Sicherheit anderer kümmern muß.

Die Großrechner vor 20 Jahren waren streng bewacht, d.h. für sie galten Zugangskontrollmaßnahmen (Pförtner, Stahltüren etc.), die nicht leicht zu überwinden waren. Die Vernetzung von Rechnern blieb Spezialanwendungen vorbehalten. Da personenbezogene Daten meist auf diesen zentralisierten Datenverarbeitungssystemen gespeichert wurden, waren die Daten, verglichen mit der Speicherung in den heutigen über das Internet verbundenen Systemen, gut gesichert: Mit dem Einzug des Internet und der Mobilkommunikation in alle Bereiche des Lebens fallen personenbezogene Daten in einer noch nie dagewesenen Menge an, deren Schutz selbst von den Betroffenen teilweise erstaunlich locker gesehen wird. Für die Aussicht auf ein kostenloses „Goodie“ werden Namen, Adressen und Telefonnummern im Internet preisgegeben; Kreditkartennummern werden über das unsichere Internet übertragen, um Waren und Dienstleistungen zu bezahlen. Globally Unique Identifier, Prozessor IDs und Ethernetadressen können einen Menschen, der einen Großteil seiner Aktivitäten „ins Netz“ verlagert, fast vollständig beobachtbar machen, da sie als Personenkennzeichen fungieren. Bereits vor 13 Jahren genügte die Speicherkapazität eines tragbaren Mediums (Magnetbandkassette), um die personenbezogenen Daten der Volkszählung von 1987 (knapp 2 Gigabyte) der Bürger der Bundesrepublik aufzunehmen. Auf vergleichbaren, heute verfügbaren Speichermedien fänden zusätzlich noch hochauflösende Fotos aller Bürger mitsamt den Fotos Ihrer Wohnhäuser Platz. Durch die Vernetzung ist es möglich, solche Datenmengen blitzschnell an das andere Ende der Welt zu transportieren. Die privaten Haushalte werden heute mit Übertragungskapazitäten zwischen 500 Kilobit/s und 1 Megabit/s angeschlossen. In ein paar Jahren wird sich die Übertragungskapazität von und zu privaten Haushalten verhundertfacht haben. Die verfügbaren Speichermedien, Netze und Übertragungsgeschwindigkeiten ermöglichen die kostengünstige und schnelle Vervielfältigung und Verbreitung auch von personenbezogenen Daten. Sie sind für den Betroffenen und seine Kommunikationspartner (und ggf. auch Unberechtigte) stets verfügbar, kaum endgültig löschbar, weil vielfach dupliziert, die Integritätssicherung erfordert viel Mühe bzw. ist nicht mehr möglich. Glücklicherweise existieren einerseits Datenschutzgesetze, andererseits Technik, die die Menschen schützen können. Technik kann dabei Daten und Menschen schützen: Während **Datensicherheit** die Daten schützen soll, schützt **Datenschutz** die Menschen.

- Datenschutz betrifft den Gebrauch von personenbezogenen Daten durch Berechtigte.
- Datensicherheit betrifft den Schutz von Daten vor Mißbrauch, (Ver)-Fälschung und Verlust bzw. Nicht-Verfügbarkeit
- Datenschutz ist primär aus der Sicht des Betroffenen interessant, während Datensicherheit primär die Sicht des Datenverarbeiters und –besitzers betrachtet.

Die Schutzziele in IT-Systemen lassen sich nach verschiedenen Kriterien gliedern, beispielsweise nach **Vertraulichkeit**, **Integrität** und **Verfügbarkeit**.

Datenschutz durch Technik bedeutet, daß sich die Gestaltung von Technik im Hinblick auf die Verarbeitung personenbezogener Daten am Ziel Datenschutz orientiert. Dabei kann Technik einerseits

die **Vertraulichkeit** von personenbezogenen Daten schützen, aber auch deren **Korrektheit** (inkl. ihrer Aktualität) [Pfit_99].

Wann immer möglich, sollten personenbezogene Daten vollständig vermieden werden (**Datenvermeidung**) oder wenigstens so wenig wie möglich personenbezogene Daten verarbeitet werden (**Datensparsamkeit**).

Datenvermeidung: Die Vertraulichkeit von Daten ist dann am größten, wenn sie vollständig vermieden werden können – was natürlich nur bei für eine bestimmte Zweckerfüllung nicht benötigten Daten möglich ist. Dabei ist erstaunlich, wie viele einen Personenbezug herstellende Daten sich als unnötig herausstellen, wenn nur früh und gründlich genug nachgedacht und das System entsprechend gestaltet wird. Beispielsweise ist es keineswegs erforderlich, daß der einen Telekommunikationsdienst Erbringende erfährt, welche Kommunikationspartner er miteinander verbindet. Um die Korrektheit von Daten, die es nicht gibt, braucht man sich keine Sorgen zu machen: Diese Maßnahmengruppe ist und bleibt leer.

Datensparsamkeit: Kann man personenbezogene Daten nicht vermeiden, so ist das Nächstbeste, die Verwendungsmöglichkeit notwendiger Daten einzuschränken bzw. Betroffenen die Möglichkeit zu geben, die Daten insbesondere bei jeder Verwendung auf Richtigkeit und Aktualität zu überprüfen. Das Ziel der Datensparsamkeit umfaßt, die Verwendungsmöglichkeit notwendiger Daten einzuschränken.

B. Schutzziele

I. Gliederung der Schutzziele

Die neuen Kommunikationsmedien sollen zunächst natürlich erwünschte Funktionen leisten, allerdings ebenso unerwünschte Funktionen oder Verhaltensweisen verhindern. Entsprechend lassen sich die großen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit verfeinern.

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 und/oder Empfängern
	Verfügbarkeit von Daten und Diensten	Erreichbarkeit von Anwendern

Schutzinteressen können sich nicht nur auf die über die Netze ausgetauschten Nachrichteninhalte (Vertraulichkeit, Integrität) beziehen, sondern gelten ebenfalls für den Schutz von Kommunikationsumständen: In manchen Anwendungen ist zu schützen, wer wann mit wem

kommuniziert hat (Anonymität und Unbeobachtbarkeit), in anderen Anwendungen ist vor allem sicherzustellen, daß eine Nachricht nachprüfbar und beweisbar von einem bestimmten Absender stammt und/oder einen Empfänger nachweisbar erreicht (Zurechenbarkeit).

II. Angreifermodell

Die Schutzmechanismen, die die Schutzziele implementieren, schützen vor einem Gegner ganz bestimmter Stärke, die im Angreifermodell definiert wird. Ein **Angreifermodell** definiert die Stärke eines Angreifers, gegen den ein bestimmter Schutzmechanismus (z.B. ein ganz bestimmtes Verschlüsselungsverfahren) gerade noch sicher ist.

Dabei berücksichtigt es folgende Aspekte:

1. Aktive oder passive Rolle des Angreifers:
   - Was kann der Angreifer maximal passiv beobachten?
   - Was kann der Angreifer maximal aktiv kontrollieren (steuern, verhindern) bzw. verändern?
2. Mächtigkeit des Angreifers:
   - Wieviel Rechenkapazität besitzt der Angreifer?
   - Wieviel finanzielle Mittel besitzt der Angreifer?
   - Wieviel Zeit besitzt der Angreifer?
   - Welche Verbreitung hat der Angreifer? Oder spezieller: Welche Leitungen, Kanäle, Rechner kann der Angreifer beherrschen?

Als potentielle Angreifer können Außenstehende, Teilnehmer, Betreiber, Hersteller, Entwickler und Wartungstechniker betrachtet werden, die natürlich auch kombiniert auftreten können. Außerdem kann man nach Angreifern innerhalb des betrachteten IT-Systems (Insider) und außerhalb (Outsider) unterscheiden. Die Feststellung, daß eine Instanz angreifen kann, ist nicht gleichzusetzen damit, daß sie wirklich angreift.

Die Vertrauensverhältnisse zwischen den verschiedenen beteiligten Instanzen innerhalb eines IT-Systems entscheiden stark darüber, welches Schutzniveau für den einzelnen Beteiligten tatsächlich erreicht werden kann. Nicht selten gilt dabei, wie im „wirklichen Leben“, daß die Mächtigen ihre Interessen gegen die schwächeren Partner durchsetzen, zumindest solange sie dies auf legaler Basis tun können. Man könnte diesen Prozeß mit dem evolutionären Grundgedanken, daß der (genetisch) Stärkere den Überlebenskampf gewinnt, erklären und billigen. Glücklicherweise hat sich in den letzten Jahren eine Gegenströmung im Bereich der IT-Sicherheit etabliert, die dieser einseitigen Betrachtung von Sicherheit und Schutz das Konzept der mehrseitigen Sicherheit entgegenstellt.

III. Mehrseitige Sicherheit

Die Vertrauensverhältnisse zwischen den verschiedenen beteiligten Instanzen innerhalb eines IT-Systems entscheiden stark darüber, welches Schutzniveau für den einzelnen Beteiligten tatsächlich erreicht werden kann. Nicht selten gilt dabei, wie im **wirklichen Leben**, daß die Mächtigen ihre Interessen gegen die schwächeren Partner durchsetzen, zumindest solange sie dies auf legaler Basis tun können. Man könnte diesen Prozeß mit dem evolutionären Grundgedanken, daß der (genetisch) Stärkere den Überlebenskampf gewinnt, erklären und billigen. Glücklicherweise hat sich in den letzten Jahren eine Gegenströmung im Bereich der IT-Sicherheit etabliert, die dieser einseitigen Betrachtung von Sicherheit und Schutz das Konzept der mehrseitigen Sicherheit entgegenstellt.

Mehrseitige Sicherheit [MüPf_97, MüRa_99] bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung. Dabei gilt:

- 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 Kommunikation in einem geklärten Kräfteverhältnis bzgl. Sicherheit miteinander interagieren.

Die mehrseitige Sicherheit verbindet die Sichtweisen von Datenschutz und Datensicherheit zu einem gemeinsamen Konzept. Während sich Datenschutz hauptsächlich um die Interessen der Betroffenen kümmert, und Datensicherheit vor allem die Interessen der Datenbesitzer und –verarbeiter beachtet, wird bei mehrseitiger Sicherheit in einem Aushandlungsprozeß versucht, möglichst Beides, Datenschutz und Datensicherheit zu gewährleisten. Dies trägt der Entwicklung Rechnung, dass aus den bisher lediglich Betroffenen zunehmend informationstechnisch Beteiligte werden können und oftmals werden sollten.

C. Rechnersicherheit

Um sichere Kommunikation zu erreichen, werden Geräte (Hardware) und Programme (Software) benötigt, die für denjenigen, der sie benutzt, sicher sind. Diese persönliche Rechenumgebung (typischerweise der PC) ist der **Vertrauensbereich** des Benutzers: Es wird angenommen, daß Angriffe auf die Interessen des Benutzers innerhalb dieses Bereiches nicht stattfinden. In diesem Vertrauensbereich kann der Nutzer Berechnungen integer und ggf. vertraulich durchführen. Darüber hinaus muß das Gerät auch über ein vertrauenswürdiges Benutzerinterface verfügen. Ist ein Benutzerendgerät für den Teilnehmer nicht (mehr) vertrauenswürdig, so können noch so gute kryptographische Systeme ihm keinerlei Sicherheit bieten.

Der Vertrauensbereich ist vor Zugang und Zugriff durch Unberechtigte zu schützen. Dies muß zunächst durch physische Schutzmaßnahmen (Zugangskontrolle) erfolgen, bevor weitere Maßnahmen wie Zugriffskontrolle sinnvoll sind.

Dies betrifft zunächst den persönlichen Rechner zu Hause und am Arbeitsplatz. In den heute weit verbreiteten PC-Betriebssystemen (DOS, Windows 95/98/ME, MacOS) fehlt leider die Zugriffskontrolle, so daß der Ausbreitung von Viren und trojanischen Pferden Tür und Tor geöffnet ist. Leider sind aber auch weniger unsichere Betriebssysteme wie Windows NT und Windows 2000 mit Zugriffskontrolle in ihren inneren Funktionen vom Hersteller nicht genug offengelegt, um sie wirklich prüfen und ihnen danach ggf. 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 keine Spuren zu hinterlassen.

I. Physische Sicherheit

Alle technischen Schutzmaßnahmen benötigen eine physische „Verankerung“ in Form eines Systemteils, auf den der Angreifer keinen physischen Zugriff hat.

Beispielsweise ist es unmöglich, den Inhalt einer zu verschlüsselnden Nachricht vor dem Verschlüsselungsbaustein zu verbergen. Dies gilt analog für die eingesetzten kryptographischen Schlüssel.

Die Größe physisch sicherer Geräte muß skalierbar sein, d.h. ein Vertrauensbereich ist nicht notwendigerweise deckungsgleich mit dem PC (Bild 1).

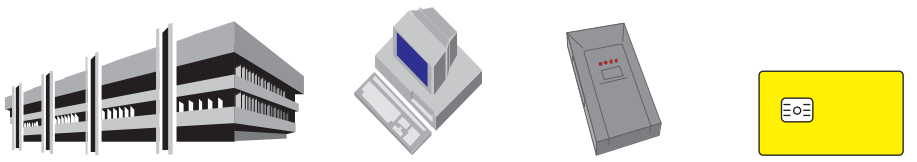

Bild 1: Die Größe physisch sicherer Geräte muß skalierbar sein

Beispiel: Es soll der Inhalt einer Festplatte vor unbefugtem Zugriff geschützt werden. Um zu verhindern, daß die Festplatte aus dem Rechner ausgebaut wird, muß der Rechner physisch sicher sein. Alternativ kann die Festplatte verschlüsselt werden. Die Ver- und Entschlüsselung der Festplatte erfolgt über ein Sicherheitsmodul, das während des Betriebs im Rechner steckt. Nun genügt es, daß das Sicherheitsmodul physisch geschützt wird. Wird der Rechner bzw. die Festplatte gestohlen, bleiben die gespeicherten Inhalte trotzdem vertraulich.

Die maximal erreichbare persönliche Sicherheit eines Benutzers eines IT-Systems kann – bezogen auf das IT-System – nie größer werden als die Sicherheit des Gerätes, mit dem er physisch direkt interagiert.

Angriffe auf die physische Sicherheit werden, unabhängig von der jeweiligen Größe des physischen Gerätes, durch Schirmung (z.B. gegen elektromagnetische Abstrahlung), Erkennen und Bewerten (z.B. durch entsprechende Sensoren) sowie Verzögern des Angriffs (z.B. durch hartes Material) realisiert. Bei Angriffen können als letzte Maßnahme die gespeicherten Geheimnisse gelöscht werden.

Die Realisierung eines physisch sicheren und für den Benutzer vertrauenswürdigen Endgerätes ist kein triviales Problem und gelingt bestenfalls auf Zeit, da immer wieder einmal neue Angriffe auf vermeintlich sicher geglaubte physisch sichere Geräte (z.B. Chipkarten) bekannt werden.

II. Sicherheit des Betriebssystems

Die Sicherheit des 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 Bild 2).

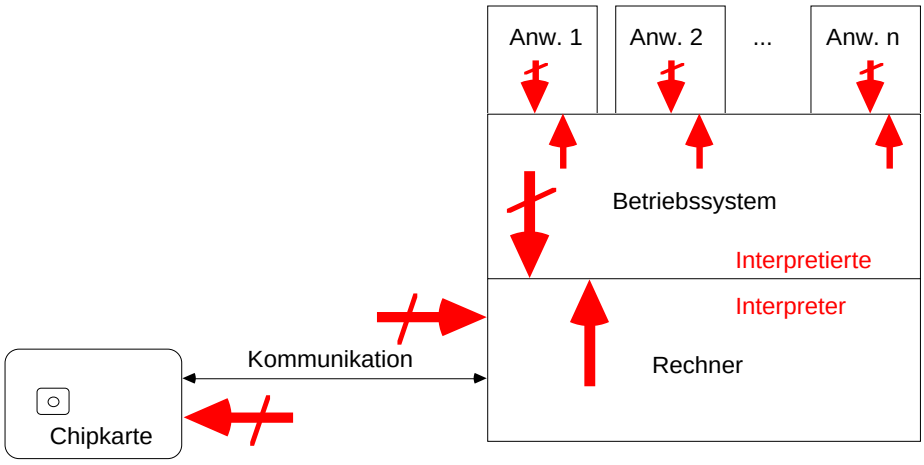

Bild 2. Verhältnis von Schichtenstruktur und Angriffserfolg

Umgekehrt ist ein sicheres Betriebssystem jedoch in der Lage, sich vor Angriffen durch Anwendungen oder – prinzipieller formuliert – durch höhere Schichten eines Systems zu schützen (durchgestrichene, nach unten zeigende Pfeile in Bild 2). 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 (Abschnitt D) zum Einsatz.

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.

III. Zugangskontrolle

Unter **Zugangskontrolle** versteht man, daß ein IT-System die Identitäten seiner Kommunikationspartner erfragt, prüft und nur mit berechtigten Partnern weiter kommuniziert.

Die Zugangskontrolle verhindert so mindestens die unbefugte Inanspruchnahme seiner Betriebsmittel. Ein IT-System kann einen Menschen daran erkennen (**Identifikation**), was er ist, hat oder weiß (Tabelle 2).

Tabelle 2: Identifikation von Menschen durch IT-Systeme

Was man	**ist:**	Handgeometrie Fingerabdruck Aussehen Eigenhändige Unterschrift Retina-Muster Stimme Tipp-Charakteristik (Tastenanschlag) DNA-Muster
	hat:	Papierdokument Metallschlüssel Magnetstreifenkarte Chipkarte Taschenrechner
	Weiß:	Passwort Antworten auf Fragen

Beispiele: 1. Ein (maschinenlesbarer) Personalausweis ist eine Kombination aus Foto („Aussehen“), eigenhändiger Unterschrift und Papierdokument. 2. Die in IT-Systemen derzeit noch am häufigsten vorkommende Form der Identifizierung ist das Passwort.

Biometrische Verfahren zur Identifikation von Menschen durch IT-Systeme gewinnen an Bedeutung. Da die biometrischen Merkmale eines Menschen nicht einfach weitergegeben oder kopiert werden können, hofft man in der Praxis eine sehr hohe Sicherheit zu erreichen. Allerdings stehen einer

Massenanwendung häufig psychologische Hindernisse und/oder drastische sicherheitstechnische Unsicherheiten im Weg. So hinterläßt beispielsweise die Abgabe eines Fingerabdrucks für den Kunden möglicherweise den Eindruck, als Krimineller oder Analphabet behandelt zu werden, was für die Akzeptanz sicher nicht förderlich ist. Andererseits kann ein Fingerabdruck in weichem Wachs, ausgegossen mit flüssigem Heftpflaster, und danach als Fingersubstitut verwendet, die angeblich hochsichere biometrische Fingerabdruckerkennung eines großen Sicherheitstechnik anbietenden Konzerns überlisten [Wau Holland in einem persönlichen Gespräch anläßlich des Datenschutztages 1999 in Kiel].

Es bietet sich also in der Praxis an, eine Kombinationen von Identifikatoren zu verwenden. Z.B. könnte bei der PIN-Eingabe an einem Geldautomaten gleichzeitig ein Fingerabdruck genommen werden.

IV. Zugriffskontrolle und Rechtevergabe

Unter **Zugriffskontrolle** versteht man, daß ein IT-System auch berechtigten Partnern nicht alles erlaubt: Jedes *Subjekt* (Mensch, IT-System, Prozeß) hat nur bestimmte *Rechte*, Operationen auf *Objekten* (Prozesse, Daten, Peripherie-Geräte, etc.) auszuführen.

Ein möglichst kleiner und gut abgegrenzter Teil des IT-Systems kontrolliert vor Ausführung aller Operationen, ob ihr Urheber die dafür nötigen Rechte hat. Dieser Teil des IT-Systems wird **Zugriffsmonitor** genannt (Bild 3). Der Zugriffsmonitor merkt sich ihm vorgelegte oder implizit entstehende Rechte und muß auch deren Ungültigwerden erkennen.

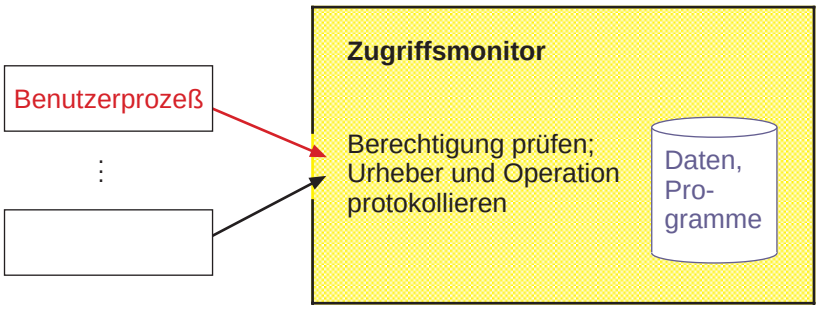

Bild 3: Gewährung von Rechten über einen Zugriffsmonitor

Beispiel: Rechte werden z.B. in einer Zugriffskontrollmatrix gespeichert. Typische Rechte sind Schreiben, Lesen, Verändern, Löschen, Ausführen.

Die Rechtevergabe selbst wird **Autorisierung** (*authorization*) genannt.

V. Schutz vor Computerviren

In vielen heute verbreiteten PC-Betriebssystemen (DOS, Windows 95/98/ME, MacOS) fehlt die Zugriffskontrolle. Dies begünstigt die Ausbreitung von Computerviren und Trojanischen Pferden erheblich.

Ein **Computervirus** ist ausführbarer Code, der sich in fremde Programme einpflanzt, dort ausgeführt wird und ggf. eine sog. **Schadensfunktion** ausführt. Ein **Wurm** ist ein ausführbares Programm, das sich über Computernetze verbreitet und ggf. eine Schadensfunktion ausführt. Ein **Trojanisches Pferd** ist ein Computerprogramm, das neben einer bekannten (vom Anwender gewünschten) Funktion eine (nicht gewünschte) Schadensfunktion ausführt.

Viren, Würmer und Trojanische Pferde können nicht nur die Integrität und Verfügbarkeit von Daten und Programmen verletzen, sondern alle Schutzziele, also auch die Vertraulichkeit von Daten. Im schlimmsten Fall können sie ihre Schadensfunktion modifizieren und sogar sich selbst zerstören, nachdem sie ihre „Aufgabe“ erfüllt haben, um die hinterlassenen Spuren zu vernichten.

In IT-Systemen mit Zugriffskontrolle kann die Ausbreitung von Viren durch das **Prinzip der geringstmöglichen Privilegierung** (*principle of least privilege*) verhindert werden. Das bedeutet, jedes Programm bekommt nur die minimal notwendigen (Schreib-)Rechte.

Bei Würmern und Trojanischen Pferden kann der Schaden zumindest auf die autorisierten Ressourcen begrenzt werden. Die Beschränkung von Ausführungsrechten verhindert die Verbreitung von Würmern. So ist beispielsweise die Weiterverbreitung von E-Mail-Würmern durch die automatisierte Ausführung von in E-Mails eingebetteten ausführbaren Dateien sehr leicht möglich und führte zu großen Schäden (vgl. Loveletter, http://www.sarc.com/avcenter/venc/data/vbs.loveletter.fw.a.html).

Weitere Informationen zu Computerviren und trojanischen Pferden finden sich in [Denn_90, Ferb_92, GGHI_89]

VI. Verteilung von Kontrolle

Um Vertrauenswürdigkeit zu erreichen, muß es möglich sein, Systeme zu validieren. Das bedeutet, unabhängige, (frei) wählbare Experten vergewissern sich von der korrekten Implementierung und Arbeitsweise eines Systems gemäß einer allgemein akzeptierten Spezifikation. Da dem normalen Anwender meist weder die Mittel noch das Wissen zur Verfügung stehen, um Systemkomponenten oder gar ganze Systeme zu validieren (geschweige denn zu verifizieren), 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.

Ein interessantes Konzept zur Verteilung von Kontrolle ist die Politik der Offenheit, insbesondere bei der Erstellung und Validierung von Software. **Open Source** kann helfen, „Fehler“ in Software

schneller zu finden und die Qualität der Software durch Verfügbarkeit von allgemein nutzbaren Modulen zu verbessern. Im Sicherheitsbereich ist Offenheit ohnehin ein gutes Mittel zur Erhöhung der Vertrauenswürdigkeit. Kein Kundiger würde der Sicherheit eines Verschlüsselungsalgorithmus ernsthaft vertrauen, wenn dieser nicht öffentlich bekannt und durch Experten auf Sicherheitslücken geprüft worden ist. Weitere Informationen zu Open Source finden sich z.B. in [KöKP_00].

VII. Unterstützung rechtlicher Vorgaben

Aus Datenschutzsicht ist es wünschenswert, wenn auch rechtliche Ziele durch Technik unterstützt werden.

Durch Datenvermeidungs- und Datensparsamkeitstechniken wird die **unberechtigte Kenntnisnahme und Veränderung personenbezogener Daten** verhindert: Die Vertraulichkeit und Integrität von Daten kann durch kryptographische Mechanismen geschützt werden. Die Anonymität und Unbeobachtbarkeit von Menschen kann durch datenschutzfreundliche Kommunikationsnetze (z.B. Proxies, Mixe) erreicht werden. Durch

Die **technische Sicherung der Zweckbindung** gestaltet sich schwieriger. Leider gibt es kaum technische Hilfen, die Zweckbindung sicherstellen, etwa das Verhindern der unberechtigten Übermittlung von Daten, die man berechtigterweise zur Kenntnis bekommen hat.

Daten können z.B. Kennzeichen (*tags*) des Zwecks ihrer Erhebung mitgegeben werden, d.h. personenbezogene Daten werden mit ihrem Zweck gespeichert, auf die nur von ausgewählten Teilen der Anwendungssoftware unter strikter Kontrolle des Betriebssystems zugegriffen werden kann (sog. *tagged architecture*). Dies muß so erfolgen, daß die Kennzeichen nicht wiederum mißbraucht werden können, etwa zur Profilbildung.

Eine *tagged architecture* auf der Basis eines unsicheren Betriebssystems hilft natürlich nicht gegen einen Angreifer, der ernsthaft versucht, gegen die Zweckbindung zu verstoßen.

Grundsätzlich gilt, je weniger personenbezogen die zu verarbeitenden Daten sind, umso unproblematischer ist die Zweckbindung. Feingranulare Pseudonymität kann hier helfen: Pseudonyme (Abschnitt D.IV) werden Personen nicht über mehrere Zwecke oder gar mehrere Lebensbereiche zugeordnet, sondern für jeden Zweck wird ein anderes Pseudonym verwendet.

D. Netzsicherheit

I. Kryptographie

Kryptographische Systeme lassen sich sowohl zum Schutz der Vertraulichkeit (Konzelations- oder Verschlüsselungssysteme) als auch zum Schutz der Integrität (Authentikationssysteme) einsetzen.

Weiterführende Literatur zur Kryptographie: [Schn_96].

Wenn Sender und Empfänger über den gleichen kryptographischen Schlüssel verfügen, spricht man von symmetrischen Systemen, andernfalls von asymmetrischen (Tabelle 3).

Tabelle 3: Klassifizierung von Kryptosystemen mit Beispielen

	Konzelationssysteme	**Authentikationssysteme**
Symmetrische	DES, Triple DES, IDEA, AES, (Pseudo)-One-time-pad	Symm. Authentikationscodes
Asymmetrische	RSA, ElGamal, McEliece	RSA, GMR, DSS, ElGamal

Die folgenden Beispiele zeigen, welche kryptographischen Klassen in welchen Einsatzfeldern sinnvoll sind:

- Elektronisches Grundbuch: Digitale Signaturen. Es muß zurechenbar sein, wer welche Eintragungen im elektronischen Grundbuch vorgenommen hat.

- Archivierung von Datenbeständen: Symmetrische Konzelationssysteme und symmetrische Authentikationscodes mit sehr großer Schlüssellänge. Um die Vertraulichkeit der Datenbestände über einen längeren Zeitraum sicherzustellen, muß der Schlüsselraum ausreichend groß gewählt werden.

- Elektronische Post (E-Mail): Hybride Verschlüsselung, Digitale Signaturen. Mit einem asymmetrischen Konzelationssystem wird ein Sitzungsschlüssel verschlüsselt, unter dem dann die eigentliche Nachricht verschlüsselt wird. Falls über E-Mail rechtlich bindende Kommunikation abgewickelt wird, sind digitale Signaturen erforderlich.

- Meldedaten in Ortsämtern: Symmetrische Verschlüsselung, Digitale Signaturen. Um die unberechtigte Kenntnisnahme von zentral gespeicherten Meldedaten mittels Abhören auf Leitungen (Ethernet-Verkabelung, Telekom-Standleitungen etc.) zu verhindern, müssen alle Daten zwischen Zentrale und Terminalrechnern verschlüsselt übertragen werden. Weiterhin muß zurechenbar sein, wer welche Eintragungen im Melderegister vorgenommen hat.

1. Symmetrisches kryptographisches Konzelationssystem

Die bekanntesten und ältesten kryptographischen Systeme sind symmetrische Konzelationssysteme (Bild 4). Ihre bekanntesten modernen Vertreter sind DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm) und AES (Advanced Encryption Standard).

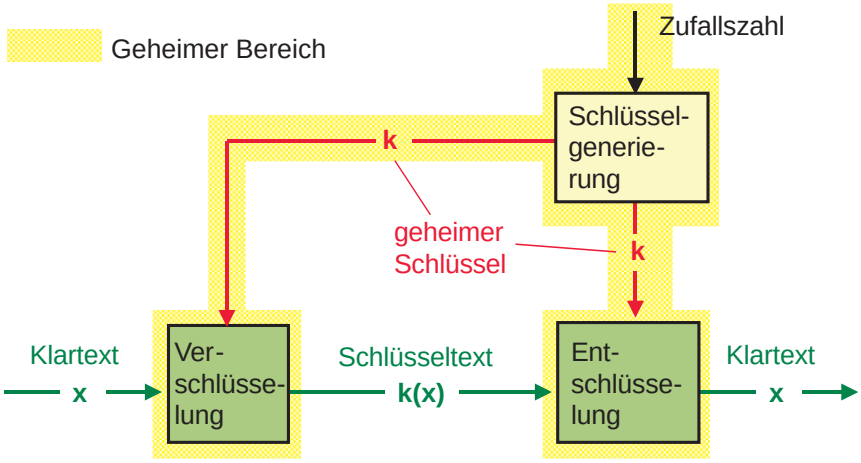

Bild 4: Symmetrisches kryptographisches Konzelationssystem

Wenn eine Nachricht x verschlüsselt über einen unsicheren Kanal gesendet werden soll, muß zuvor der Schlüssel k bei Sender und Empfänger vorliegen. Wenn sich Sender und Empfänger vorher getroffen haben, können sie k bei der Gelegenheit austauschen. Andernfalls muß k über eine vertrauenswürdige „Schlüsselverteilzentrale“ Z ausgetauscht werden (Bild 5): Hierzu melden sich die Teilnehmer A und B bei Z an und tauschen jeweils Schlüssel mit Z aus. A und Z tauschen k_{AZ} aus und B und Z tauschen k_{BZ} aus. Wenn A mit B kommunizieren will und noch keinen Schlüssel mit B gemeinsam hat, so fragt er bei Z an. Z generiert einen Schlüssel k und schickt ihn sowohl an A als auch an B, und zwar mit k_{AZ} bzw. k_{BZ} verschlüsselt (Abbildung 4).

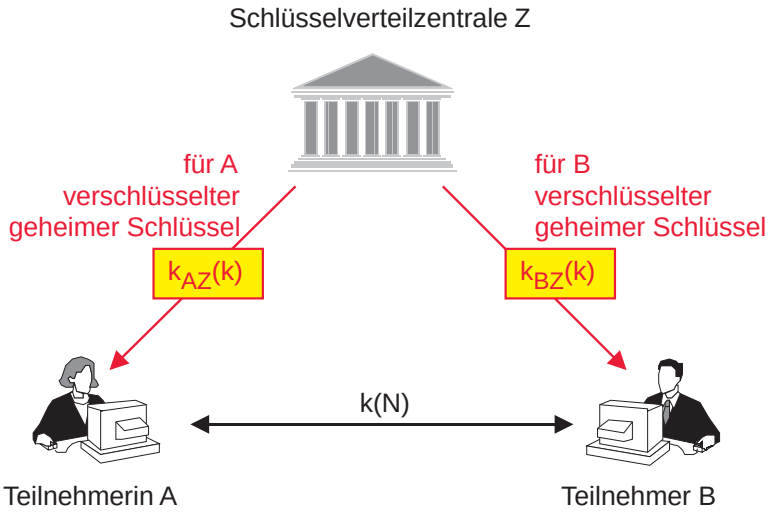

Bild 5: Schlüsselverteilung bei symmetrischen Konzelationssystemen

Ab jetzt können A und B den Schlüssel k benutzen, um in beide Richtungen verschlüsselte Nachrichten N zu schicken. Die Vertraulichkeit ist allerdings nicht sehr groß: Außer A und B kann auch Z alle Nachrichten entschlüsseln.

2. Asymmetrisches kryptographisches Konzelationssystem

Die bekanntesten Vertreter asymmetrischer kryptographischer Konzelationssysteme sind RSA und ElGamal (jeweils benannt nach ihren Erfindern Rivest, Shamir, Adleman bzw. ElGamal). Im Vergleich zu symmetrischen Konzelationssystemen sind sie deutlich rechenaufwendiger (etwa Faktor 100 bis 1000).

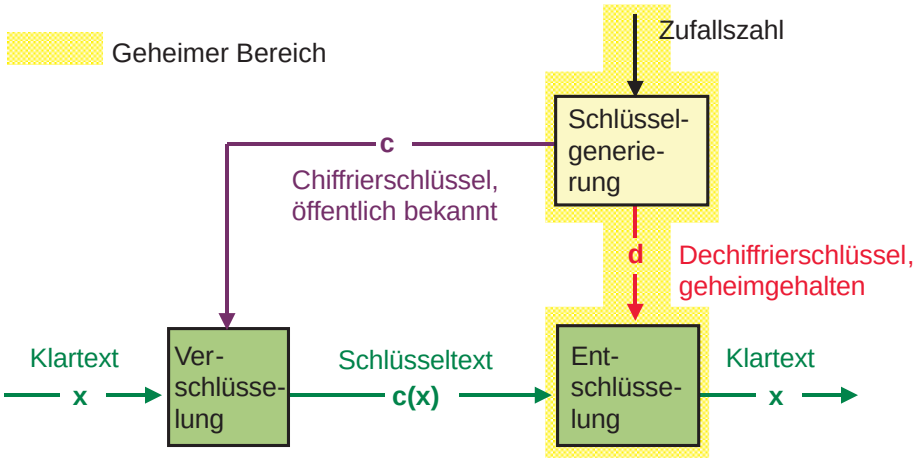

Bild 6: Asymmetrisches kryptographisches Konzelationssystem

Asymmetrische Konzelationssysteme (Bild 6) wurden erfunden, um die Schlüsselverteilung zu vereinfachen. Hier sind zum Ver- und Entschlüsseln verschiedene Schlüssel c und d erforderlich, und nur d muß geheimgehalten werden. Damit man c tatsächlich nicht geheimhalten muß, darf d nicht mit vernünftigem Aufwand aus c zu bestimmen sein.

Nun kann jeder Benutzer A sich selbst ein Schlüsselpaar (c_A, d_A) generieren und muß d_A nie jemand anderem mitteilen. Der öffentliche Schlüssel c_A muß so verteilt werden, daß jeder andere Teilnehmer B, der A eine vertrauliche Mitteilung schicken will, an c_A gelangt. B kann c_A offen in sein Adreßbuch schreiben. Auch können Bekannte sich c_A weitererzählen. Für Kontakte mit Unbekannten könnte c_A gleich mit in dem Verzeichnis stehen, wo B die Netzadresse von A nachschaut. Gibt es kein solches Verzeichnis außerhalb des Netzes, so kann ein im Netz agierendes Schlüsselregister R an seine Stelle treten. Man beachte, daß R die Nachrichten nicht entschlüsseln kann.

3. Symmetrisches kryptographisches Authentikationssystem

Bei symmetrischen kryptographischen Authentikationssystemen wird die Nachricht durch den kryptographischen Algorithmus links (Bild 7) nicht verschlüsselt, sondern es wird ein Prüfteil **MAC** (**Message Authentication Code**) an x angehängt. Der Empfänger kann anhand von x auch den richtigen MAC bilden und prüfen, ob der mit der Nachricht mitgekommene damit übereinstimmt.

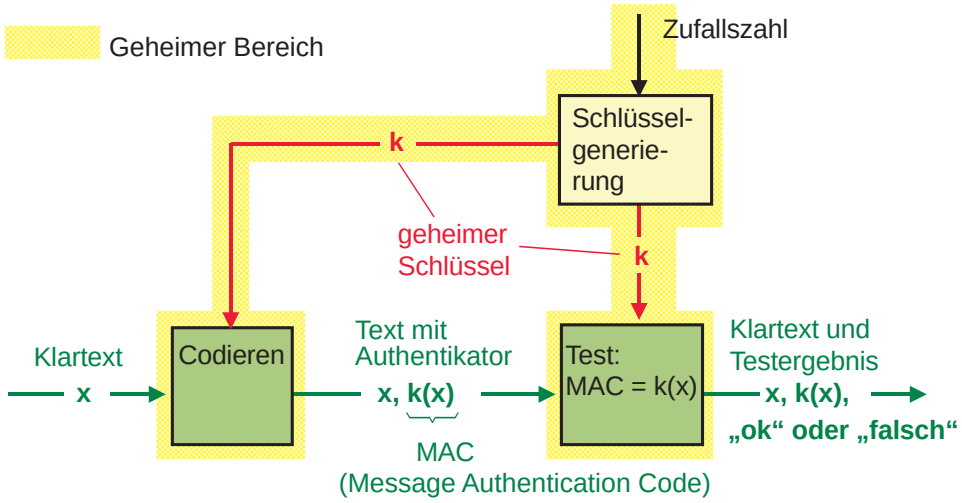

Bild 7: Symmetrisches kryptographisches Authentikationssystem

Die Schlüsselverteilung kann wie bei symmetrischen Konzelationssystemen erfolgen. Entsprechend könnte die Schlüsselverteilzentrale diesmal gefälschte Nachrichten unterschieben.

4. Asymmetrisches kryptographisches Authentikationssystem

Asymmetrische kryptographische Authentikationssysteme (Bild 8) werden **digitale Signatursysteme** genannt und vereinfachen zunächst die Schlüsselverteilung analog zu asymmetrischen Konzelationssystemen.

Ihr Hauptvorteil ist aber ein anderer: Der Empfänger *B* einer signierten Nachricht von *A* kann jedem, der *A*s öffentlichen Schlüssel t_A kennt, beweisen, daß diese Nachricht von *A* stammt.

Dies geht bei einem symmetrischen Authentikationssystem nicht: Selbst wenn z.B. vor Gericht die Schlüsselverteilzentrale bestätigen würde, welchen Schlüssel *A* und *B* hatten, kann *B* den *MAC* genausogut selbst erzeugt haben.

Bei digitalen Signatursystemen ist jedoch *A* der einzige, der die Signatur erzeugen kann. Im Streitfall können *A* und *B* eine Dritte Instanz einschalten, welche die Signatur nach objektiven Gesichtspunkten als korrekt anerkennt oder ablehnt, ohne daß die Schutzinteressen einer Partei (Sender, Empfänger, Dritter) verletzt werden. Bei der digitalen Signatur heißt dies konkret, daß der Signierer seinen geheimen Schlüssel niemals offenlegen muß. Allgemeiner formuliert bedeutet dies, daß nur der Signierer Signaturen leisten kann, während jeder andere die Korrektheit der Signatur überprüfen kann.

Deswegen sind digitale Signatursysteme unumgänglich, wenn man rechtlich relevante Dinge digital in *zurechenbarer* Weise abwickeln will, z.B. bei Electronic-Commerce und digitalen Zahlungssystemen. Digitale Signaturen haben dort die Funktion der eigenhändigen Unterschrift in heutigen Rechtsgeschäften.

Bekannte Signaturverfahren sind RSA (ebenfalls für asymmetrische Konzelation einsetzbar) und DSS (Digital Signature Standard).

Im Gegensatz zur symmetrischen Authentikation wird bei der digitalen Signatur ein eigener Testalgorithmus benötigt, der mit dem öffentlichen Schlüssel *t* arbeitet.

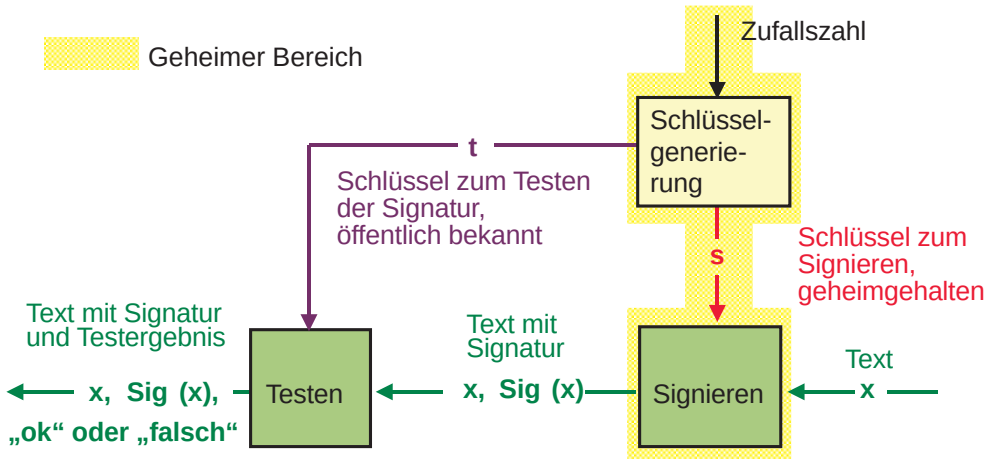

Bild 8: Digitales Signatursystem

Will man sicher sein, daß eine Signatur später ggf. vor Gericht anerkannt wird, muß man sich versichern, daß man den richtigen bzw. authentischen Testschlüssel hat. Die Authentizität eines öffentlichen Schlüssels kann durch die Prüfung eines Schlüssel-Zertifikats festgestellt werden.

Die **Zertifizierung** (Beglaubigung) **des öffentlichen Testschlüssels** bezieht sich nicht auf den Schlüssel allein, sondern auf den *Zusammenhang* zwischen Schlüssel und Teilnehmer. Bei der Zertifizierung überprüft die Zertifizierungsstelle (auch vertrauenswürdiger Dritter oder Trust Center genannt) die Identität des Teilnehmers (beispielsweise anhand seines Personalausweises) und erstellt ein **Schlüssel-Zertifikat**, d.h. eine digitale Signatur über der Identität und dem öffentlichen Schlüssel des Teilnehmers.

Zertifizierungsstellen sind die wesentlichen Komponenten einer Public Key Infrastructure (PKI), da sie die Gewähr dafür übernehmen, daß ein Testschlüssel auch wirklich zu einer Person gehört. Dies können rein technische Mittel nicht leisten. Nötig sind auch organisatorische Mittel, z. B. Überprüfung von Ausweisdokumenten und Regelungen für den Streitfall.

II. Steganographie

Bei Verwendung von Kryptographie ist im Kommunikationsnetz erkennbar, ob gerade vertraulich oder authentisiert kommuniziert wird, sofern keine weiteren Schutzmaßnahmen ergriffen werden. Bei Steganographie ist das nicht der Fall.

Steganographische Konzelationssysteme (Bild 9) betten geheimzuhaltende Nachrichten in harmlos wirkende Hüllnachrichten (z.B. digitalisierte Fotos oder Sound-Dateien) ein, so daß für Außenstehende, die nur den Stegotext beobachten, nicht einmal die Existenz der geheimen Nachricht erkennbar ist und damit auch nicht ihr Inhalt.

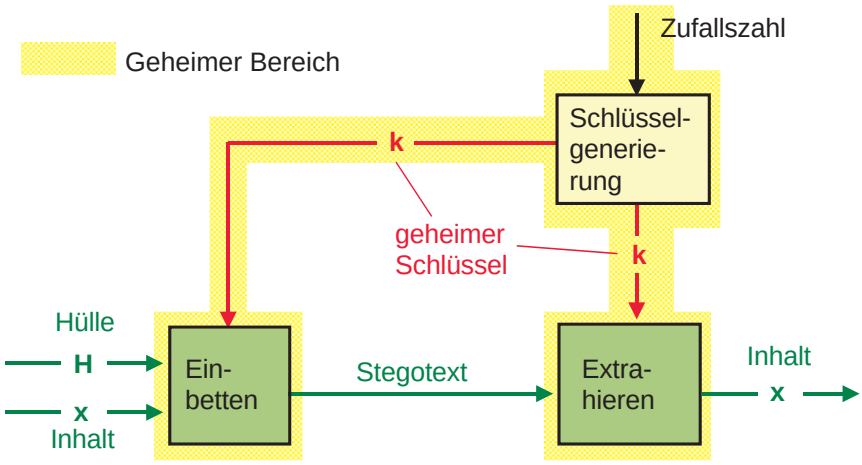

Bild 9. Symmetrisches steganographisches Konzelationssystem

Politische Diskussionen um ein Kryptoverbot führten zu einer verstärkten Beachtung der Steganographie, da mit Steganographie Verschlüsselungsverbote unterlaufen werden können.

Ein Nachteil der steganographischen Konzelation ist, daß zum Übertragen einer bestimmten Datenmenge ein Vielfaches an Stegotext benötigt wird. Der Grund liegt darin, daß *x* meist nur in manchen niederwertigsten Bits der Hüllinformation *H* untergebracht werden kann, da nur diese Bits je nach Hüllinformation derart indeterministisch sind, daß ihre Veränderung für den Außenstehenden zu keiner beobachtbaren Beeinträchtigung der Hüllinformation führt.

Bisher sind nur *symmetrische* steganographische Konzelationssysteme bekannt. Die selbstverständlich mögliche Hintereinanderschaltung eines asymmetrischen Konzelationssystems und symmetrischen Stegosystems führt nicht zu einem asymmetrischen Stegosystem.

Steganographische Authentikationssysteme werden **Watermarking-Systeme** genannt. Durch die zunehmende Bedeutung von Multimedia und dem damit verbundenen Wunsch, die Urheberrechte bei der Verbreitung digitaler Objekte (Daten, Programme, Computerkunst etc.) über CD-ROM und Internet zu sichern, gewinnen Watermarking-Verfahren an Bedeutung. Die Hülle (siehe steganographisches Konzelationssystem) stellt dabei die urheberrechtlich zu schützende Information dar. Die Urheberinformation sei *x*. Nun kommt es nicht darauf an, eine möglichst große Menge an Informationen *x* in die Hülle einzubetten. Vielmehr soll die Urheberinformation möglichst *robust* eingebettet werden. Am Beispiel digitaler Bilder wird dies deutlicher: Trotz einer Veränderung von Bildparametern (Größe, Farbe, Helligkeit etc.) oder Ausschneiden von Bildteilen zum Zwecke der eigenen Nutzung soll die Urheberinformation erhalten bleiben.

Das Einbetten von Daten über den Käufer eines digitalen Objektes nennt man **Fingerprinting**.

Weitergehende Informationen zu Steganographie und Watermarking finden sich in [IHW_96, IHW_98]

III. Anonymität und Unbeobachtbarkeit

Für einen Benutzer des Internet sollte es — wie im „wirklichen Leben“ — die Möglichkeit geben, wann immer er es wünscht, seine Identität vor Anderen zu verbergen, d.h. seine Anonymität zu wahren. Wer einen Laden betritt, um sich nur zu informieren, stellt sich dem Verkaufspersonal auch nicht mit vollem Namen und Adresse vor, sondern bleibt zunächst anonym. Ein Besuch eines Internet-Shops beginnt meist mit dem Übermitteln eines Cookies. Auf jeden Fall aber hinterlässt der Besucher bereits mit dem ersten Klick seine Internet-Adresse.

Bei *anonymer* Kommunikation verbirgt ein Kommunikationspartner seine Identität vor den anderen Kommunikationspartnern. Bei *unbeobachtbarer* Kommunikation kennen sich möglicherweise die Kommunikationspartner, allerdings kann niemand, nicht einmal die Betreiber des Kommunikationsnetzes, feststellen, dass die Kommunikationspartner tatsächlich miteinander kommunizieren.

Auch für Unbeobachtbarkeit findet man Anwendungen im wirklichen Leben: Firmen möchten möglichst unbeobachtbar Patentrecherchen betreiben, um eigene Forschungen und Entwicklungen vor der Konkurrenz geheimzuhalten. Beratungsstellen sollten kontaktiert werden können, ohne dabei Datenspuren beim Netzbetreiber zu hinterlassen.

Bei Anonymität ist geschützt, wessen Handlungen innerhalb einer sog. Anonymitätsgruppe nicht mit seiner Identität verkettbar sind. Genaue Definitionen findet man in [Pfit_90, S.15]. Da typischerweise eine Handlung nur dann anonym ist, wenn sie durch einen Angreifer nicht ihrem Urheber zugeordnet werden kann, müssen mehrere unterschiedliche und nicht angreifende Parteien innerhalb einer Anonymitätsgruppe agieren. Deshalb ist Anonymität nur multilateral, d.h. unter Mithilfe Vieler erreichbar. Die Handlung einer isoliert agierenden einzelnen Person kann nie anonym und unbeobachtbar erfolgen.

Steganographische Konzelationssysteme erlauben in gewissen Grenzen den unbeobachtbaren Austausch von Nachrichteninhalten, indem in einer unauffälligen Hüllnachricht verborgene Daten ausgetauscht werden können. Trotzdem bleibt der Zugriff auf die Hüllinformationen beobachtbar.

Auch Spread Spectrum Systems erlauben in gewissen Grenzen den unbeobachtbaren Austausch von Nachrichteninhalten, da der Träger des Funksignals für den, der nicht den Spreizcode kennt, im Rauschen verborgen bleibt.

Mittels spezieller Schutzmechanismen kann jedoch die Unbeobachtbarkeit des Nachrichtenaustauschs allgemein und des Sendens und Empfangens von Nachrichten erreicht werden. Die hierzu verwendeten Mechanismen nutzen meist die oben (Abschnitt D.) beschriebenen kryptographischen Basismechanismen in speziellen Kommunikationsprotokollen und/oder speziellen Nachrichtenformaten aus.

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 die Mißbrauchsmöglichkeiten.

Bekannte Schutzmechanismen für **Anonymität** und **Unbeobachtbarkeit** sind

- Schutz des Empfängers durch Verteilung (Broadcast) und implizite Adressierung,
- Schutz des Senders durch Dummy Traffic, DC-Netze (überlagerndes Senden, [Chau_88]) und Ring-Netze [Pfit_90, S.101ff],
- Schutz der Kommunikationsbeziehung zwischen Sender und Empfänger durch Proxies und Mixe [Chau_81],
- Schutz von Datenbankzugriffen durch „Blindes Lesen“ (Blinded Message Service, [CoBi_95]),
- Schutz des Senders gegen Peilbarkeit (in Funknetzen) durch Bandspreiztechniken (Spread Spectrum Systems, siehe z.B. [Torr_92, PiSM_82]) und
- Schutz von Aufenthaltsorten (in Funknetzen und mobilen Festnetzen) durch spezielle Pseudonyme sowie anonyme und unbeobachtbare Verfahren zum Location Management (siehe z.B. [Fede_99]).

Im folgenden werden Proxies und Mixe exemplarisch vorgestellt.

1. Proxies

Proxies (Stellvertreter) verbergen den Ursprung einer Verbindung im Internet. Hierzu bauen die Programme eines Benutzers zunächst eine Verbindung zu einem Proxy-Server auf, der seinerseits (stellvertretend) die vom Benutzer gewünschte Verbindung zum Zielrechner (z.B. einem WWW-Server) aufbaut (Bild 10). Proxy-Server werden häufig zusammen mit Cache-Servern und **Firewalls** an der Übergangsstelle vom (firmeninternen) Intranet zum Internet betrieben. Beobachtern im Internet bleiben damit die (firmeninternen) Netzstrukturen und Adressen verborgen. Dies erschwert Hackern das Eindringen in das Intranet. Darüber hinaus verhindern sie die Beobachtung einzelner Nutzer, da die Ursprungsadresse einer Verbindung vor dem Internet verborgen wird.

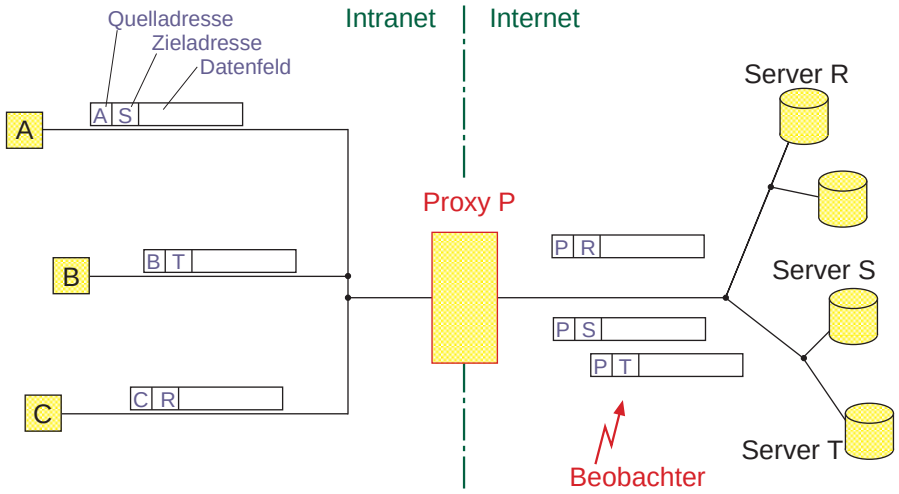

Bild 10: Proxies als Schutz vor Beobachtern im Internet

Proxies schützen nicht vor einem Beobachter, der im Intranet verbreitet ist. Ebenso schützen sie nicht, wenn der Proxy selber der Beobachter ist. Ein Verfahren, das selbst gegen Beobachtung durch den Betreiber des Proxys sicher ist, ist das Mix-Netz.

2. Das Mix-Netz

Das **Mix-Netz** [Chau_81, PfPW_88, Pfit_90, PfPf_90, PfPW_91] verbirgt die Kommunikationsbeziehung zwischen Sender und Empfänger einer Nachricht. Dabei darf ein Angreifer alle Leitungen des Kommunikationsnetzes beobachten, und trotzdem bleibt die Kommunikationsbeziehung unbeobachtbar. Hierzu wird die Nachricht über sog. Mixe geschickt. Ein Mix verbirgt dabei die Verkettung zwischen eingehenden und ausgehenden Nachrichten.

Von seiner Grundfunktion ist der Mix einem Proxy ähnlich. Allerdings schützt das Mix-Netz auch vor Beobachtung durch die Mixe selber. Hierzu wird eine Nachricht über mehrere Mixe zum Empfänger transportiert. Das Ziel des Mix-Netzes ist, daß alle Mixe, die von einer Nachricht durchlaufen wurden, zusammenarbeiten müssen, um die Kommunikationsbeziehung zwischen Sender und Empfänger aufzudecken. Die durchlaufenen Mixe sollten bzgl. ihres Entwurfs, ihrer Herstellung und insbesondere bzgl. ihres Betreibers möglichst unabhängig sein. Andernfalls könnten Mixe (oder gar ganze Mix-Ketten) überbrückt und so die Kommunikationsbeziehung aufgedeckt werden.

Ein Mix muß eingehende Nachrichten speichern, bis genügend viele Nachrichten von genügend vielen Absendern vorhanden sind, ihr Aussehen verändern, d.h. sie umkodieren, und die Reihenfolge der ausgehenden Nachrichten verändern, d.h. sie umsortiert ausgeben.

Die Kernfunktion eines Mixes ist das Umkodieren der Nachrichten. Das Umkodieren erfolgt mit einem asymmetrischen Konzelationssystem.

IV. Pseudonymität

Manche Anwendung erfordert trotz anonymer und unbeobachtbarer Kommunikation auch die Zurechenbarkeit von Aktionen (z.B. Bestellungen) zu ihrem Akteur. **Pseudonymität** gestattet die Verknüpfung von Anonymität und Zurechenbarkeit. Das bedeutet, Transaktionen werden nicht unter der Identität des Akteurs durchgeführt, sondern unter einem Kennzeichen (Pseudonym) – in aller Regel einem Schlüssel zum Testen digitaler Signaturen, vgl. D I 4. Um im Streitfall Schaden regulieren zu können, gibt es zwei Konzepte [PWP_90]:

- Für Pseudonyme wird vor der eigentlichen Transaktion haftendes Kapital hinterlegt, aus dem Ansprüche der Geschäftspartner befriedigt werden können. Ist genügend Kapital hinterlegt und mittels eines aktiven **Werte-Treuhänders** für die Transaktion reserviert, ist auch im Streitfall nie eine Aufdeckung der Identität nötig, so dass die Zuordnung Pseudonym <–> Identität niemand bekannt zu sein braucht. Ist sie allenfalls dem Inhaber des Pseudonyms bekannt, ist die Vertrauenswürdigkeit seiner Anonymität maximal.

- Um im Streitfall eine Aufdeckung der Identität (und damit Schadensregulierung außerhalb des IT-Systems) zu ermöglichen, kann ein **Identitäts-Treuhänder** verwendet werden. Er bestätigt durch seine digitale Signatur unter ein Pseudonym, dass er den Inhaber dieses Pseudonyms rechtsverbindlich identifizieren kann. Im Streifall werden die Identitäten der Beteiligten von den Identitäts-Treuhändern aufgedeckt, so dass eine Schadensregulierung ganz konventionell erfolgen kann – wenn genug haftende Werte vorhanden sind und ggf. sichergestellt werden können. Um das Risiko unbefugter oder gar verdeckter Aufdeckung der Identität eines Pseudonyminhabers zu verkleinern, kann statt einer einstufigen Implementierung des Identitäts-Treuhänders eine mehrstufige gewählt werden: Die einstufige Zuordnung Pseudonym zu Identität wird über mehrere Stufen „Pseudonym zu Zwischen-Pseudonym 1 zu Zwischen-Pseudonym 2 zu ... zu Zwischen-Pseudonym *n* zu Identität“ von insgesamt *n* unabhägigen Identitäts-Treuhändern vorgenommen, wobei jeder nur jeweils den Zusammenhang an den Enden eines der Pfeile kennt. So kann jeder Identitäts-Treuhänder allein die Nichtaufdeckung sicherstellen, alle *n* zusammen aber die Aufdeckung.

Primitive Pseudonymitätskonzepte wie die des deutschen Signaturgesetzes arbeiten ausschließlich mit Identitäts-Treuhändern und dies auch nur einstufig.

Fortgeschrittene Pseudonymitätskonzepte erlauben, Autorisierungen von einem Pseudonym auf andere Pseudonyme derselben Person zu übertragen [Chau_85].

Man unterscheidet Personen- und Rollenpseudonyme, die bezüglich ihrer Anonymität skalierbar sind. In [PWP_90] wurden die verschiedenen Arten von Pseudonymen grob eingeteilt nach

- Personenpseudonymen
  - Öffentliches Personenpseudonym,
  - Nichtöffentliches Personenpseudonym,
- Anonymes Personenpseudonym,

- Rollenpseudonymen;
- Geschäftsbeziehungspseudonym,
- Transaktionspseudonym.

Im Kapitel „Datenschutzfreundliche Technologien“ werden Pseudonyme genauer dargestellt.

V. Festlegung und Aushandlung der Schutzziele und Sicherheitsmechanismen durch die Nutzer

Die vollständigste Sammlung von Schutzzielen und die wirkungsvollsten Sicherheitsmechanismen nützen nichts, wenn die Nutzer ihre Schutzziele nicht ausdrücken und die Verwendung der Sicherheitsmechanismen nicht steuern (können).

Da der allgemeine Kenntnisstand über die in Netzen auftretenden Sicherheitsprobleme und die zur Verfügung stehenden Methoden des Schutzes nur langsam wächst, muß diese Benutzungsschnittstelle so einfach gestaltet sein, daß sie auch von Sicherheitslaien benutzt werden kann.

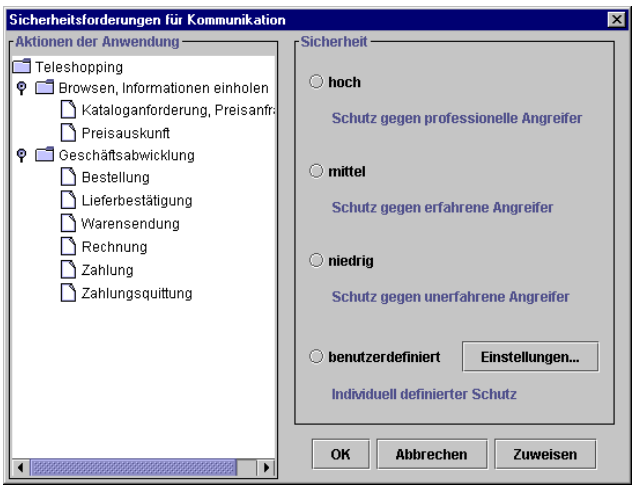

Bild 11: Einsteiger-Ebene der Sicherheitskonfigurierung: wähle hohe, mittlere, niedrige Sicherheit oder benutzerdefinierte Einstellungen für Experten

Deshalb wurden in den letzten Jahren vermehrt prototypische Benutzungsoberflächen erstellt, die auch bzgl. Datenschutz und IT-Sicherheit unerfahrenen Benutzern erlauben, ihre Sicherheitsinteressen auszudrücken und geeignete Sicherheitsmechanismen zu konfigurieren [WoPf_00, PPWW_00]. Die Bilder 11 bis 13 zeigen drei Screenshots des in [WoPf_00] genauer beschriebenen und bewerteten Prototypen.

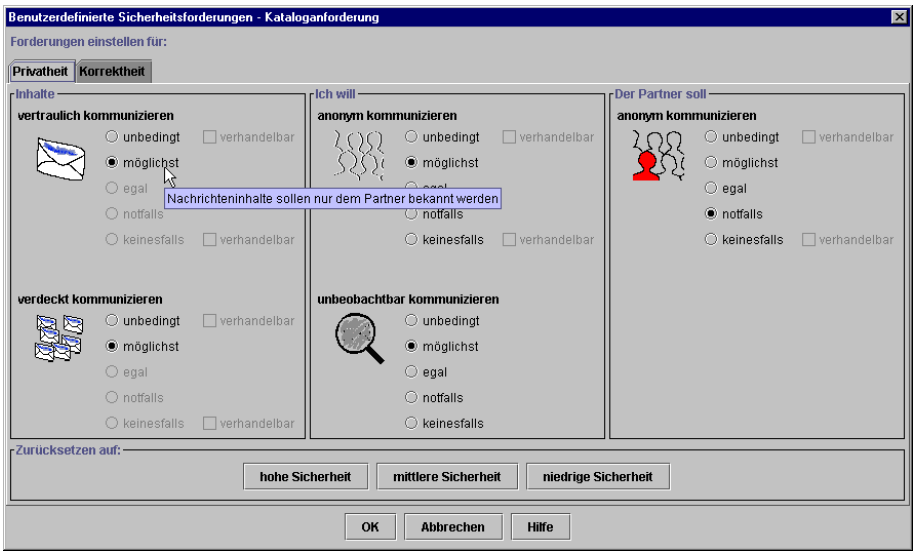

Bild 12: Dialogfenster für die benutzerdefinierten Einstellungen der Privatheit – Tooltip für das Schutzziel Vertraulichkeit

In Bild 11 wird die einfachste Ebene einer Sicherheitskonfiguration dargestellt. Gerade für Einsteiger bietet sich eine sehr stark kategorisierte Wahlmöglichkeit des gewünschten Sicherheitsniveaus an. Für Experten können die Einstellungen in komplexen Dialogen konfiguriert werden. Die Bilder 12 und 13 zeigen Beispiele solcher Dialoge für die Schutzziele Vertraulichkeit (Privatheit) und Integrität und Verfügbarkeit (Korrektheit).

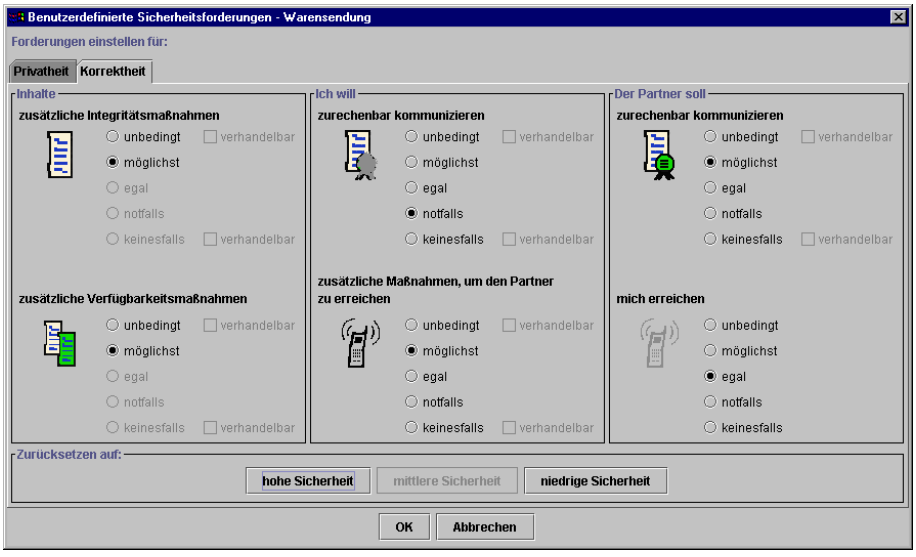

Bild 13: Dialogfenster für die benutzerdefinierten Einstellungen der Korrektheit

Zwar ist gerade bezüglich Nutzerverständlichkeit und -freundlichkeit noch eine menge Forschungs- und Entwicklungsarbeit zu leisten, die Ergebnisse der bisherigen Experimente und Befragungen potentieller Nutzer sind aber durchaus ermutigend.

E. Schlußbemerkungen

In komplexen IT-Systemen, wie es unsere heutigen und zukünftigen Kommunikationsnetze sind, handeln verschiedene Subjekte (Organisationen, Personen). Sie können dabei nicht nur kooperieren, sondern auch konkurrieren (z. B. um Betriebsmittel), sabotieren (z. B. Kommunikation behindern, stören, blockieren, lahmlegen), fingieren (z. B. Identitäten vortäuschen, Daten verändern) oder abhören (z. B. bespitzeln, lauschen). Um Funktion und Eigenschaften eines Systems beim Auftreten von nicht erwünschten Ereignissen aufrecht zu erhalten, sind daher Schutzmaßnahmen erforderlich. Diese Schutzmaßnahmen müssen insbesondere auch **intelligenten Angreifern** standhalten. Aus der Sicht der Datensicherheit sind die Verfügbarkeit und die Verbindlichkeit von Daten wichtig. Aus der Sich des Datenschutzes müssen Daten vor allem vor unberechtigter Kenntnisnahme und Veränderung gesichert werden.

Bei den heute verfügbaren und kostengünstig einsetzbaren Datenschutztechniken kann man zwischen „Pflicht und Kür“ unterscheiden:

Die Pflicht: Verschlüsselung, Integritätssicherung (durch Message Authentication Codes) und – wo vom Dienst gefordert – Verbindlichkeit (durch Digitale Signaturen) werden zukünftig den technischen Grundschutz aus Datenschutzsicht bilden. Diese Techniken sind heute weitgehend verfügbar und ausgereift. Sie bilden das Rückgrat des Datenschutzes in IT-Systemen.

Die Kür: Verfahren zur unbeobachtbaren und anonymen Kommunikation, Identitätsmanagement und Pseudonymität bilden zusammen mit dem technischen Grundschutz die Basis für eine mehrseitige Sicherheit, die die Interessen der Betroffenen und Verarbeiter von Daten berücksichtigt. Diese Techniken erleben derzeit ihren Übergang von der akademischen zur kommerziellen Bedeutung. Sie werden zukünftig ein entscheidendes Marketinginstrument sein.

* * *