Rechtliche Gestaltung der Informationstechnik; Fachtagung Darmstadt 1996; Alcatel SEL Stiftung, Stiftungsreihe 22, Seite 21-23

Mehrseitige Sicherheit in verteilten IT-Systemen

Andreas Pfitzmann
TU Dresden, Fakultät Informatik
D-01062 Dresden
Tel. 0351 / 463-8277, Fax -8255
e-mail: pfitza@inf.tu-dresden.de

Zusammenfassung

Nach einer Motivation der Notwendigkeit mehrseitiger Sicherheit wird skizziert, daß IT-Sicherheit eine wesentliche Voraussetzung ist und daß mehrseitige IT-Sicherheit nur durch verteilte IT-Systeme erreicht werden kann. Verteilte IT-Systeme bilden also nicht in erster Linie eine Gefährdung der Sicherheit, sondern bei geeigneter Gestaltung die einzige bekannte Möglichkeit, Sicherheit in demokratieverträglicher Weise – was bedeutet: mehrseitig – zu realisieren.

Einleitung

Gehen wir das Thema von hinten an:

Unter einem **verteilten IT-System** verstehe ich ein informationstechnisches (IT-) System, das räumlich verteilt ist und ohne eine zentrale, alles und jeden steuernde und kontrollierende Instanz auskommt. In aller Regel hat ein solches verteiltes IT-System nicht nur mehrere Benutzer, sondern auch mehrere Betreiber, Hersteller und Entwerfer seiner einzelnen Komponenten. Zwei Beispiele verteilter IT-Systeme mögen dies erläutern:

1. Zusammen mit anderen Komponenten bildet die Komponente „AntiBlockierSystem“ (ABS) das verteilte IT-System „Auto“. Viele Autos (und ggf. noch andere Komponenten wie Busse, Bahnen, Flugzeuge) bilden das verteilte IT-System „Verkehrssystem“.
2. Zusammen mit anderen Komponenten bildet die Komponente „Sicherheitsmodul“ das verteilte IT-System Personal Computer (PC). Viele PCs (und ggf. noch andere Komponenten wie Fernübertragungsleitungen, Funk- und Vermittlungssysteme, Großrechnern, Workstations etc.) bilden das Internet.

Sicherheit bedeutet, daß bestimmte wünschenswerte Eigenschaften, sogenannte Sicherheitseigenschaften, gegen potentielle Angreifer durchgesetzt werden. Es sind also zwei Fragen zu beantworten: Was ist zu sichern? Gegen wen ist es zu sichern?

Nun ist, was wünschenswert oder unangenehm ist, ebenso wie wer als potentieller Angreifer gilt, oft eine Frage der (eigenen) Interessen. Sicherheit kann also in aller Regel nicht global definiert werden. **Mehrseitige Sicherheit** [RaPM_96] bedeutet nun, daß jede(r) die aus seiner Sicht wünschenswerten Eigenschaften definieren kann – und, ggf. nach einem Aushandlungsprozeß mit den anderen Beteiligten und dabei bewußt eingegangenen Kompromissen mit deren Sicherheitsinteressen, auch durchsetzen oder zumindest ihre Einhaltung kontrollieren.

IT ermöglicht Selbstschutz auch in offenen Systemen

Einerseits ist es in vielen offenen verteilten IT-Systemen nicht mehr möglich, daß der Staat (oder eine andere Instanz) Teilnehmer wirksam schützt: Die verteilten IT-Systeme erstrecken sich über mehrere Rechtsräume, sind nicht global kontrollierbar oder auch nur beobachtbar. (Versuche, sie beobachtbar zu machen wie die Fernmeldeverkehr-Überwachungs-Verordnung (FÜV) oder die entsprechenden Paragraphen im Telekommunikationsgesetz (TKG), sind zum Scheitern verurteilt und den vorgeblichen Zwecken nicht dienlich [MöPS_94, HuPf_96].)

Andererseits ermöglichen verteilte IT-Systeme die Realisierung mehrseitiger Sicherheit und damit wirksamen Selbstschutz, wie die folgenden Beispiele zeigen:

Sichere portable Benutzerendgeräte [PPSW_95]:
Lokale sichere Rechenumgebung für jede(n) an jedem Ort

Digitale Signaturen [DiHe_79, PWP_90]:
Ende-zu-Ende-Integrität und Verbindlichkeit

Konzelationssysteme oder Stegosysteme [PfPW_88, FJPP_95, MöPS_94]:
Ende-zu-Ende-Vertraulichkeit

DC-Netz oder MIX-Netz [Chau_88, Chau_81, PfPW_89]:
Unbeobachtbarkeit der Kommunikationsbeziehungen

Funk-MIXe, HPC oder MF-MIXe [Pfit_93, FJKPS_96]:
Vertraulichkeit des Aufenthaltsortes von Mobilteilnehmern

Diversitäre Netze und Multi-Netz Endgeräte, z.B. kombinierte GSM und DECT-Handies:
Verfügbarkeit

Wünsche an das Recht

Aus den technischen Sachverhalten und elementaren Überlegungen zu den Zielen unserer Verfassung ergeben sich die folgenden Wünsche, was rechtlich getan und unterlassen werden sollte:

Tun:

+ Infrastruktur für mehrseitige Sicherheit fördern, d.h.
  - Vertrauenswürdige Benutzerendgeräte
    mit digitalen Signatursystemen
    mit Konzelationssystemen
  - Schlüsselzertifizierung und Verzeichnisdienst für digitale Signaturen
+ Sicherheitseigenschaften für manche Anwendungsbereiche vorschreiben

Unterlassen:

- symbolische Politik, die Entwicklung und Einsatz sicherer IT behindert, z.B. Krypto-regulierung, Exportverbote für sichere IT, überzogene Fernmeldeüberwachung (FÜV und die entsprechenden Paragraphen im TKG)
- den Bock zum Gärtner machen: Geheimdienste wollen unsichere IT

Mehrseitige Sicherheit durch verteilte IT-Systeme

Das könnte und sollte das Ziel für IT-Entwickler, -Anwender und juristische Gestalter sein.

Literatur

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

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

DiHe_79 Whitfield Diffie, Martin E. Hellman: Privacy and Authentication: An Introduction to Cryptography; Proceedings of the IEEE 67/3 (1979) 397-427.

FJKPS_96 Hannes Federrath, Anja Jerichow, Dogan Kesdogan, Andreas Pfitzmann, Otto Spaniol: Mobilkommunikation ohne Bewegungsprofile; it+ti 38/4 (1996) 24-29.

FJPP_95 Hannes Federrath, Anja Jerichow, Andreas Pfitzmann, Birgit Pfitzmann: Mehrseitig sichere Schlüsselerzeugung; Proc. Arbeitskonferenz Trust Center 95, DuD Fachbeiträge, Vieweg, Wiesbaden 1995, 117-131.

HuPf_96 Michaela Huhn, Andreas Pfitzmann: Technische Randbedingungen jeder Kryptoregulierung; DuD, Datenschutz und Datensicherheit, Vieweg-Verlag 20/1 (1996) 23-26.

MöPS_94 Steffen Möller, Andreas Pfitzmann, Ingo Stierand: Rechnergestützte Steganographie: Wie sie funktioniert und warum folglich jede Reglementierung von Verschlüsselung unsinnig ist; Datenschutz und Datensicherung DuD 18/6 (1994) 318-326.

Pfit_93 Andreas Pfitzmann: Technischer Datenschutz in öffentlichen Funknetzen; Datenschutz und Datensicherung DuD 17/8 (1993) 451-463.

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

PfPW_89 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Telefon-MIXe: Schutz der Vermittlungsdaten für zwei 64-kbit/s-Duplexkanäle über den (2•64 + 16)-kbit/s-Teilnehmeranschluß; Datenschutz und Datensicherung DuD 13/12 (1989) 605-622.

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.

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.

RaPM_96 Kai Rannenberg, Andreas Pfitzmann, Günter Müller: Sicherheit, insbesondere mehrseitige IT-Sicherheit; it+ti 38/4 (1996) 7-10.