Sicherheit, insbesondere mehrseitige IT-Sicherheit

Security, with particular reference to multilateral IT-Security

Kai Rannenberg, Andreas Pfitzmann, Günter Müller
Universität Freiburg, TU Dresden, Universität Freiburg

Zusammenfassung

Sicherheit besteht bei informationstechnischen (IT-) Systemen darin, daß *Schutzziele* trotz intelligenter *Angreifer* durchgesetzt werden. In diesem Text wird zunächst der Begriff *Sicherheit* im Kontext von IT-Systemen kurz diskutiert, insbesondere die Erweiterung, die er im Zuge der Entwicklung der IT und der Verbreitung ihrer Anwendung, speziell bei IT-gestützten Kommunikationssystemen erfahren hat. Danach werden potentielle Angreifer betrachtet. Eine Erläuterung und ein Beispiel für Sicherheitsanforderungen aus mehreren Sichten (*mehrseitige Sicherheit*) folgen. Eine kurze Betrachtung der Möglichkeiten, mehrseitige Sicherheit in verteilten Systemen zu realisieren, schließt den Text ab.

Abstract

Security, in respect of information technology (IT) systems, refers to the fact that *protection goals* are achieved in spite of intelligent attacks. This paper commences with a brief discussion of the term *security* in the context of IT systems. Of particular importance is the broadening of the term's meaning which has resulted from the development and more widespread deployment of IT, in particular IT supported communication systems. This is followed by a description of potential attackers and, subsequently, an explanation and example of security requirements arising from several perspectives (*multilateral security*). The paper concludes with a brief discussion of the opportunities for implementing multilateral security in distributed systems.

Gliederung

Lebensläufe

Kai Rannenberg, Dipl.-Inform. TU Berlin 1989. 1989-1993 Fachgebiet Informatik u. Gesellschaft/Datenschutz TU Berlin. 1990 Praktikum b. Berliner Datenschutzbeauftragten. 1993 IIG Uni Freiburg; Koordinator d. Kollegs „Sicherheit in der Kommunikationstechnik“ d. Gottlieb Daimler- u. Karl Benz-Stiftung. Forschungsschwerpunkt: Datenschutz u. IT-Sicherheit f. offene u. öffentliche Kommunikationssysteme.

Andreas Pfitzmann, Dipl.-Inform. Uni Karlsruhe 1982, Promotion 1989, Prof. an der TU Dresden seit 1993. Forscht seit 1983 über technischen Datenschutz. Seit 1991 Sprecher der GI-Fachgruppe 2.5.3 „Verläßliche Informationssysteme“, seit 1989 Mitglied des GI-Präsidiumsarbeitskreises "Datenschutz und IT-Sicherheit" sowie seit 1990 im Herausgeberrat von „DuD, Datenschutz und Datensicherung...“.

Prof. Dr. Günter Müller, Dipl.-Kfm. Uni Mannheim 1972; Prom. Duisburg 1976; venia legendi in Informatik Wien 1983. 1978 IBM Deutschland, 1985 Gründer u. Leiter Europäisches Zentrum f. Netzwerkforschung d. IBM. 1990 Ruf als Gründungsdirektor d. Institutes f. Informatik und Gesellschaft (IIG) u. Ordinarius für Telematik an d. Uni Freiburg. Leiter d. Kollegs „Sicherheit in der Kommunikationstechnik“.

Ansprechpartner

Kai Rannenberg

Abteilung Telematik, Institut für Informatik und Gesellschaft, Universität Freiburg
Friedrichstraße 50, D-79098 Freiburg
Telefon +49-761-203-4926, Fax +49-761-203-4929
E-Mail kara@iig.uni-freiburg.de

1 Einleitung

Sicherheit besteht bei informationstechnischen (IT-) Systemen darin, daß *Schutzziele* wie *Vertraulichkeit*, *Integrität*, *Verfügbarkeit* und *Verbindlichkeit* trotz intelligenter *Angreifer* durchgesetzt werden. Im Zuge der Entwicklung der Informationstechnik und der Verbreitung ihrer Anwendung hat der Begriff der Sicherheit eine erhebliche Erweiterung seiner Bedeutung erfahren, die zunächst kurz anhand einiger Beispiele diskutiert wird (Kapitel 2). Insbesondere bei offenen Kommunikationssystemen kann nicht davon ausgegangen werden, daß sich alle Beteiligten vollständig vertrauen. Im Gegenteil sind bei einer Analyse von deren Sicherheit prinzipiell alle Beteiligten auch als potentielle Angreifer zu betrachten (Kapitel 3). Gerade die Verbreitung IT-gestützter Kommunikationssysteme (etwa ISDN oder Electronic Mail) hat dazu beigetragen, daß nicht nur Systembetreiber und -hersteller, sondern auch Nutzer Sicherheit fordern (*mehrseitige Sicherheit*): Weil menschliche Kommunikation immer öfter technisch vermittelt wird, erwarten Nutzer, daß auch ihre bezüglich der Kommunikation grundlegenden Sicherheitsbedürfnisse bei der jeweiligen technischen Realisierung berücksichtigt werden (Kapitel 4). Möglich ist dies, wenn die Verteiltheit von Kommunikationssystemen richtig genutzt wird und insbesondere Informationen so dezentral verteilt werden, daß ein eventueller Mißbrauch unattraktiv wird (Kapitel 5).

2 Bedrohungen, Schutzziele und Schutzgüter

Da eine abschließende und kanonische Einteilung von **Bedrohungen** und damit korrespondierenden **Schutzzielen** für IT-Systeme nicht existiert, werden im folgenden zwei Einteilungen und ihre Grenzen anhand von Beispielen für **Schutzgüter** aus dem Bereich Gesundheitswesen vorgestellt und diskutiert.

Seit den frühen 80er Jahren findet sich eine Dreiteilung der *Bedrohungen* und korrespondierenden *Schutzziele* [9; 10]:

(1) *Unbefugter Informationsgewinn*, d.h. Verlust der **Vertraulichkeit** (Confidentiality): Patientendaten (etwa Untersuchungen, Diagnosen oder Therapieversuche) sollen Unbefugten nicht *zur Kenntnis gelangen*, seien dies nun andere Patienten oder auch die Mitarbeiter des Netzbetreibers, über dessen Netz sie von einem Krankenhaus zum anderen übertragen werden.

(2) *Unbefugte Modifikation von Informationen*, d.h. Verlust der **Integrität** (Integrity): Werden unbefugt und *unbemerkt* Daten *geändert*, z.B. die Dosierungsanweisung für ein zu verabreichendes Medikament, kann dies lebensbedrohliche Folgen haben.

(3) *Unbefugte Beeinträchtigung der Funktionalität*, d.h. Verlust der **Verfügbarkeit** (Availability): Ist die Krankengeschichte nur über ein Netz zugreifbar, dieses aber gerade *bemerkbar ausgefallen*, wenn eine Abfrage für eine Therapiemaßnahme erfolgen muß, kann auch Verlust der Verfügbarkeit lebensbedrohlich sein.

Leider ist keine Klassifikation der Bedrohungen bekannt. Insbesondere ist die obige Dreiteilung *keine Klassifikation*: Wird ein gerade nicht ausgeführtes Programm im Speicher unbefugt modifiziert, handelt es sich um unbefugte Modifikation von Information. Wird das in gleicher Weise unbefugt modifizierte Programm ausgeführt, handelt es sich um eine unbefugte

Beeinträchtigung der Funktionalität. Zugespitzt sorgen Maßnahmen zur Sicherung der Integrität dafür, daß das Richtige geschieht, und Maßnahmen zur Sicherung der Verfügbarkeit, daß es rechtzeitig geschieht. Diese Unterscheidung hat eine Entsprechung im *Korrektheitsbegriff*, wenn man sich auf die Attribute *unbemerkt* (bei Integrität) bzw. *bemerkbar* (bei Verfügbarkeit) bezieht:

Integrität (= keine unbefugte und unbemerkte Änderung von Information) entspricht dann der **partiellen Korrektheit** eines Algorithmus: Liefert er ein Ergebnis, ist es richtig.

Integrität und Verfügbarkeit zusammen erfüllen dann die Anforderungen der **totalen Korrektheit**: Es wird ein richtiges Ergebnis geliefert.

Umgekehrt reicht jedoch im allgemeinen der Nachweis der totalen Korrektheit allein als Nachweis für Verfügbarkeit nicht aus. Zusätzlich muß mindestens noch die Verfügbarkeit der benötigten Betriebsmittel analysiert und nachgewiesen werden. Charakteristisch für fast alle Anwendungen mit Verfügbarkeitsanforderungen ist ja, daß richtige Ergebnisse nicht irgendwann in der Zukunft, sondern zu bestimmten Zeitpunkten (etwa bei der nächsten nötigen Therapiemaßnahme) benötigt werden.

In [7] wird moniert, daß in [10] die Bedrohung *Verlust der Verbindlichkeit* nicht aufgeführt ist. Ein entsprechendes Schutzziel wird in den Kanadischen IT-Sicherheitsevaluationskriterien [2; 3] als zusätzliches viertes eingeführt:

(4) *Unzulässige Unverbindlichkeit*, d.h. Verlust der **Zurechenbarkeit** (Accountability): Wenn für Vorgänge in IT-Systemen, etwa für den Versand von Diagnosen oder Abrechnungen, nicht die jeweils Verantwortlichen auszumachen sind, kann dies zu verantwortungslosem Handeln führen. Außerdem können die Folgen eines Fehlers für die Geschädigten noch verschlimmert werden, weil möglicherweise unklar bleibt, an wen sie sich mit ihren Schadensersatzansprüchen zu halten haben.

Man kann mit Hilfe der Vierteilung manche Schutzziele prägnanter beschreiben, vgl. 4. Umgekehrt kann man versuchen, solche Bedrohungen bzw. Schutzziele auch unter Integrität zu fassen, um mit möglichst wenigen Bedrohungstypen auszukommen.

3 Potentielle Angreifer

Einerseits wirken auf jedes und in jedem technischen System die Naturgesetze und, wenn man es nicht davor schützt, auch die Naturgewalten. Als Folge der Naturgesetze altern Bauteile und funktionieren schließlich nicht mehr wie vorgesehen. Naturgewalten führen zu Gefahren wie Überspannung, Spannungsausfall, Überschwemmung oder Temperaturänderungen. Vorkehrungen in Bezug auf Naturgesetze und Naturgewalten sind die Domäne des Fachgebietes Fehlertoleranz.

Andererseits können Menschen, sei es aus Unfähigkeit oder Nachlässigkeit, sei es bewußt unbefugt handelnd, unerwünscht auf das System einwirken. Gemäß ihrer Rolle in Bezug auf das IT-System ist es sinnvoll, verschiedene Gruppen zu unterscheiden, etwa (vgl. Bild 1):

- Außenstehende,
- Benutzer des Systems,
- Betreiber des Systems,
- Wartungsdienste,

- Produzenten des Systems,
- Entwerfer des Systems,
- Produzenten der für Entwurf und Produktion des Systems verwendeten Hilfsmittel,
- Entwerfer der für Entwurf und Produktion des Systems verwendeten Hilfsmittel,
- Produzenten der für Entwurf und Produktion der Hilfsmittel verwendeten Hilfsmittel,
- Entwerfer der für Entwurf und Produktion der Hilfsmittel verwendeten Hilfsmittel,
- Produzenten …,
- …

Natürlich existieren auch zu allen oben aufgeführten Hilfsmitteln wiederum Benutzer, Betreiber und Wartungsdienste.

Die hohe Komplexität heutiger IT-Systeme verhindert in der Regel eine genügend rigorose Kontrolle dieser Systeme. Deshalb müssen auch die Produzenten und Entwerfer, seien es Menschen oder wiederum (irgendwann auch von Menschen geschaffene) IT-Systeme, als mögliche **Angreifer**, d.h. unbefugt Handelnde, betrachtet werden. Beispielsweise können sie in den von ihnen entworfenen oder produzierten Systemteilen **Trojanische Pferde** [5] verstecken. Insbesondere **universelle** trojanische Pferde, deren Schadensfunktion der Angreifer noch nach der Unterbringung steuern kann, sind gefährlich, des weiteren **transitive** Trojanische Pferde, die ihrerseits trojanische Pferde erzeugen [8; 5]. Ein populäres Beispiel für transitive trojanische Pferde sind Computerviren, die sich von Programm zu Programm und Speichermedium zu Speichermedium weiter fortpflanzen. Durch die Transitivität Trojanischer Pferde wird der Kreis derer, die als potentielle Angreifer betrachtet werden müssen, weiter vergrößert. Entsprechend läßt sich die Liste potentieller Angreifer prinzipiell fortsetzen, bis man zu Systemen kommt, für deren Entwurf und Produktion keine oder triviale Hilfsmittel verwandt wurden.

Während es üblich ist, Außenstehenden und Benutzern der betrachteten IT-Systeme zu mißtrauen und deshalb zu versuchen, sich gegen ihre unbewußten Fehler und bewußten Angriffe zu schützen, ist dies bezüglich der anderen Rollenträger (insbesondere auch bezüglich der Einwirkung weiterer IT-Systeme) oft nicht der Fall. Ob dies daran liegt, daß sich Mitglieder der gleichen Berufsgruppe meist vertrauen und bei Beschuldigungen von anderen oft gegenseitig decken, oder an der gedanklichen Schwierigkeit und dem technischen Aufwand, sich auch gegen Mitglieder der eigenen Profession zu sichern, sei dahingestellt.

Werden bei einer Risikoanalyse potentielle Angreifer nicht berücksichtigt, kann dies zu erheblichen Sicherheitsproblemen führen, denn nicht nur unbewußte Fehler, auch bewußte Angriffe können sich entlang der Entwurfs- und Produktionslinie fortpflanzen. In Bild 1 muß beispielsweise mitnichten der Mensch oben links an Fehlern des von ihm rechnerunterstützt entworfenen Rechners oben rechts schuld sein. Es könnte auch der Mensch links unten oder der Rechner unten rechts sein. Natürlich kämen auch die anderen „beteiligten“ Menschen und Rechner in Betracht.

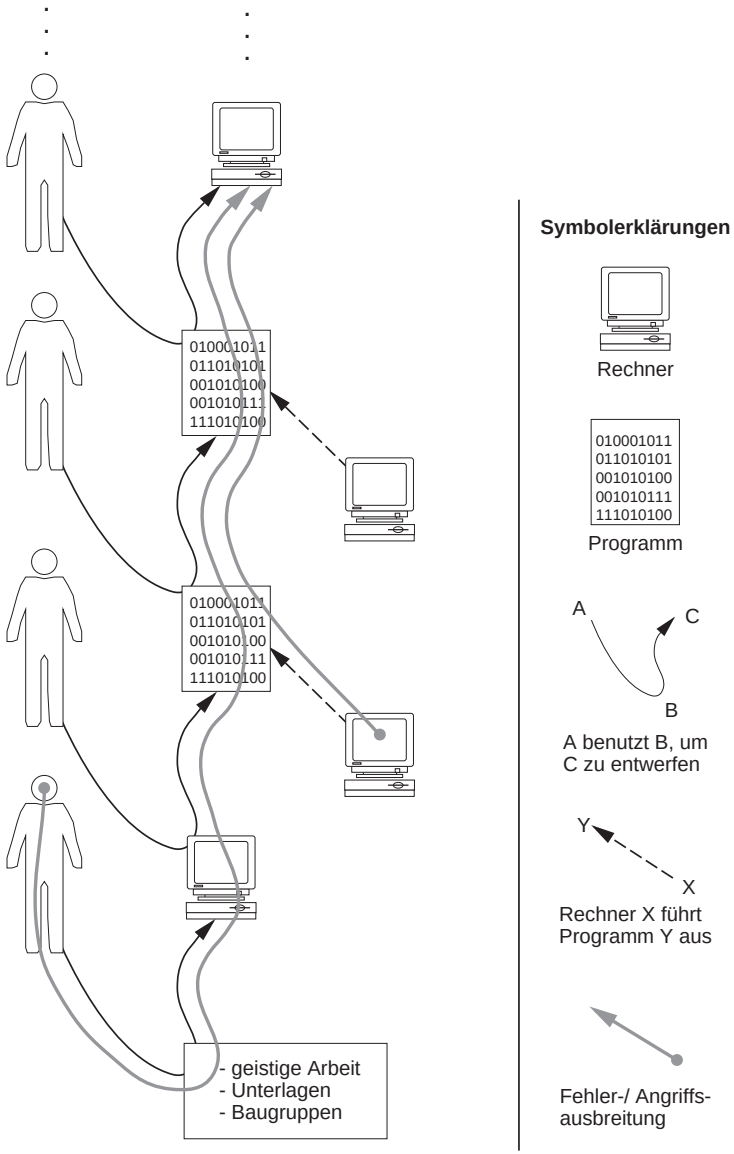

Bild 1: Transitive Ausbreitung von Fehlern und Angriffen

4 Mehrseitige Sicherheit

Mehrseitige Sicherheit bedeutet die Berücksichtigung der Sicherheitsanforderungen nicht nur einer der beteiligten Parteien. Da sich die Beteiligten, speziell bei offenen Kommunikationssystemen, nicht per se vertrauen, sind sie auch sämtlich als potentielle Angreifer zu sehen. Entsprechend sind die Anforderungen mehrseitiger Sicherheit bei für universelle Nutzung gedachten öffentlichen Kommunikationsnetzen besonders anspruchsvoll. Im folgenden sind sie in Anlehnung an [6], jedoch vierfach gegliedert, dargestellt (für eine dreifache Gliederung sind die unter Zurechenbarkeit gefaßten Anforderungen unter Integrität zu fassen).

Schutzziel Vertraulichkeit (Confidentiality)

c1 *Nachrichteninhalte* sollen vor allen Instanzen außer dem Kommunikationspartner vertraulich bleiben.

c2 *Sender* und/oder *Empfänger* von Nachrichten sollen voreinander *anonym* bleiben können, und *Unbeteiligte* (inkl. Netzbetreiber) sollen *nicht in der Lage* sein, sie *zu beobachten.*

c3 Weder potentielle Kommunikationspartner noch Unbeteiligte (inkl. Netzbetreiber) sollen ohne Einwilligung den *momentanen Ort* einer mobilen Teilnehmerstation bzw. des sie benutzenden Teilnehmers ermitteln können.

Schutzziel Integrität (Integrity)

i1 Fälschungen von *Nachrichteninhalten* (inkl. des *Absenders*) sollen erkannt werden.

Schutzziel Verfügbarkeit (Availability)

a1 Das Netz ermöglicht Kommunikation zwischen allen Partnern, die dies *wünschen* (und denen es nicht verboten ist).

Schutzziel Zurechenbarkeit (Accountability)

z1 Gegenüber einem Dritten soll der Empfänger *nachweisen* können, daß Instanz *x* die Nachricht *y gesendet hat*.

z2 Der Absender soll das *Absenden* einer Nachricht mit korrektem Inhalt *beweisen* können, möglichst sogar den Empfang der Nachricht.

z3 Niemand kann dem Netzbetreiber *Entgelte* für erbrachte Dienstleistungen vorenthalten – zumindest erhält der Netzbetreiber bei Dienstinanspruchnahme entsprechende Beweismittel. Umgekehrt kann der Netzbetreiber nur für korrekt erbrachte Dienstleistungen Entgelte fordern.

5 Realisierung mehrseitiger Sicherheit in verteilten Systemen

Die Anforderungen mehrseitiger Sicherheit sind nicht unbedingt konfliktfrei und deshalb beim Entwurf und Betrieb der Systeme in eine sinnvolle und für alle Beteiligten akzeptable Balance zu bringen.

Manchmal stehen sich die Inhaber gleicher Rollen konträr gegenüber, bei den Sicherheitsanforderungen in Kapitel 4 etwa Teilnehmer bezüglich der Schutzziele c2 (Möglichkeit der Anonymität der Teilnehmer voreinander, etwa beim Anruf bei einer Beratungsstelle) und z1 (Nachweisbarkeit des Versandes von Nachrichten, beispielsweise zum Schutz vor belästigenden oder störenden Anrufen). In solchen Fällen, bei denen die potentiellen Kontrahenten oft die prinzipiell gleichen Voraussetzungen haben, kann es helfen, wenn die Benutzer ihren Teil des Systems, etwa ihr Telekommunikationsendgerät, möglichst flexibel auf ihre eigene Bedürfnisse hin einrichten können. Ein Beispiel dafür ist der im Rahmen des Kollegs „Sicherheit in der Kommunikationstechnik“ als Demonstrator entstehende Erreichbarkeitsmanager [1]: Er erspart seinem Besitzer u.a. Störungen und Belästigungen, indem er einfache Verhandlungen mit dem potentiellen Kommunikationspartner (etwa über die Sicherheitsbedingungen der Kommunikation) übernimmt.

Stehen sich Inhaber verschiedener Rollen gegenüber, ist oftmals die Infrastruktur der Systeme in die Betrachtung miteinzubeziehen, insbesondere wenn es um die Sicherheitsanforderungen von Teilnehmern im Verhältnis zu denen von Betreibern geht: Beispielsweise wollen Teilnehmer eines Mobilkommunikationsdienstes meist nicht, daß bekannt wird, mit wem sie wann wie lange und von wo aus kommuniziert haben (c2, c3). Darum ist es ihr Interesse, daß möglichst wenig Daten über sie anfallen. Umgekehrt haben die Betreiber das Interesse, die mobilen Teilnehmer möglichst effizient zu adressieren, um Aufwand zu vermeiden. Außerdem wollen sie oft für den Fall eines Streites um die einem Teilnehmer zuzurechnenden Kosten (z3) möglichst wirkungsvolles Beweismaterial über die in Anspruch genommenen Leistungen erfassen.

Die wirksamste Strategie zur Vermeidung von Vertraulichkeitsrisiken ist die Vermeidung möglichst vieler riskanter Daten (**Datensparsamkeit**). Sind Daten nicht vermeidbar, etwa weil sie zur ordnungsgemäßen Erbringung oder Abrechnung eines Dienstes unverzichtbar sind, ist ihre Verteilung auf mehrere Teile eines verteilten Systems (**Dezentralisierung**) die wesentliche konstruktive Maßnahme, um die Attraktivität und die Folgen eines Mißbrauchs zu begrenzen. Beispielsweise müssen Kunden, die ihren Dienstleistungserbringern nicht vertrauen wollen oder können, dann nicht befürchten, allwissenden oder allmächtigen Angreifern gegenüberzustehen. Vorschläge aus dem Kolleg in diese Richtung finden sich in [4].

6 Literatur

[1] Andreas Bertsch, Herbert Damker, Hannes Federrath: Persönliches Erreichbarkeitsmanagement; in diesem Heft (Informationstechnik und technische Informatik 38/4 (1996))

[2] Canadian System Security Centre: The Canadian Trusted Computer Product Evaluation Criteria, Version 2.0, Final Draft; December 1990, 76 pages; Communications Security Establishment, Government of Canada

[3] Canadian System Security Centre: The Canadian Trusted Computer Product Evaluation Criteria, Version 3.0e; January 1993, 233 pages; Communications Security Establishment, Government of Canada

[4] Hannes Federrath, Anja Jerichow, Dogan Kesdogan, Andreas Pfitzmann, Otto Spaniol: Mobilkommunikation ohne Bewegungsprofile; in diesem Heft (Informationstechnik und technische Informatik 38/4 (1996))

[5] Andreas Pfitzmann: Entwicklungslinien der Informationstechnik und Informatik und ihre Auswirkungen auf rechtliche Beherrschung; Datenschutz und Datensicherung DuD 14 (1990), Nr. 12, Dezember 1990, 620-627

[6] Andreas Pfitzmann: Technischer Datenschutz in öffentlichen Funknetzen; Datenschutz und Datensicherung DuD 17 (1993), Nr. 8, August 1993, 451-463

[7] Dirk Stelzer: Kritik des Sicherheitsbegriffs im IT-Sicherheitsrahmenkonzept; Datenschutz und Datensicherung DuD 14 (1990), Nr. 10, Oktober 1990, 501-506

[8] Ken Thompson: Reflections on Trusting Trust; Communications of the ACM 27 (1984), No. 8, August 1984, 761-763

[9] Viktor L. Voydock, Stephen T. Kent: Security Mechanisms in High-Level Network Protocols; ACM Computing Surveys 15 (1983), No. 2, June 1983, 135-170

[10] Zentralstelle für Sicherheit in der Informationstechnik (Hrsg.): IT-Sicherheitskriterien; Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT); 1. Fassung vom 11.1.1989; Köln, Bundesanzeiger 1989