Inhaltsübersicht zur Vorlesung von

Dieter Sosna
Datenschutz und Datensicherheit

gehalten im WS 07/08

Diese Übersicht führt sichwortartig die wichtigsten Inhalte der Vorlesung auf und soll zur Wiederholung bzw. zur Prüfungsvorbereitung dienen. Sie ersetzt keinesfalls den Vorlesungsbesuch bzw. das Selbststudium.

Literatur:
WEB: BSI (Bundesamt für Sicherheit in der Informationstechnik)
Grundschutzhandbuch (PDF: Achtung ca. 3000 Seiten)

Die folgenden Bücher befinden sich im Semesterapparat bis April, sind also in der ZW Informatik der UB stets verfügbar.

Empfohlene Literatur:

H.Kersten:
Einführung in die Computersicherheit.
Oldenburgverlag 1991, ISBN 3-486-21873-5 **(unbedingt lesen)**

Castano u.a.:
Database Security.
Add.-Wesley 1994 ISBN 0-201-59375-0

Bruce Schneier:
Angewandte Kryptographie
Add.-Wesley (mehrere Ausgaben, auch engl.)
- speziell zu Kap. 3

Ergänzende Literatur:
W. Gerhardt:
Zugriffskontrolle bei Datenbanken
Oldenburgverlag

---

1. Einführung

Begriffe *Informationen vs. Daten* (materialisiert, Speicherung durch Felder)

Was bestimmt den Wert der Daten ?
Wann sind Daten schutzwürdig ?

Begriffe Datenschutz, Datensicherheit

Gültigkeitsbereich des Begriffes Datenschutz mit Blick auf das Bundesdatenschutzgesetz (in Deutschland , im internationalen Vergleich).
Wachsende Bedeutung von Datenschutz und Datensicherheit auf Grund der immer umfassenden Nutzung elektronischer Medien. Auswirkungen der allgemein verfügbaren Vernetzung. - Profilerstellung.
Doppelrolle des Bundesdatenschutzgesetzes zum Schutz der Bürger und als Normativ vor einem vermeintlichem Schutzbedürfniss.

Datensicherheit: Schutz vor Verlust.

- drei Unterbegriffe von Datenverlust

Gesetzliche Regelungen (Bundesdatenschutzgesetz, Landesdatenschutzgesetze)
Personenbezogene Daten – in DL natürliche Personen, keine jur. Personen.
Unauthorisierter Datenzugriff und/oder Datenmanipulation – Straftatbestand (StGB §) – damit auch jurist. Mittel zum Schutz anderer Daten. s.u.

Begrif*f Angriff:*

Jedes Ereignis, das Verlust der Daten oder der Vertraulichkeit der Information nach sich zieht oder nach sich ziehen kann.

Klassifikation der Angriffe nach Ursache:

- Naturkatastrophen (Wasser, Erdbeben, Surm, Regen , Blitzschlag)
- Krieg
- Feuer , Brandstiftung
- technische Ausfälle, Fehlfunktion, Fehlfunktion der Versorgungssysteme
- Durch Menschen direkt verursacht:
  ohne Vorsatz (fahrlässig): versehentliche Fehlbedienung, versehentliche mech. Einwirkung.
  mit Vorsatz: vorsätzliches Herbeiführen von Datenverlusten oder Verlust der Vertraulichkeit
  durch Bedienfehler, Feuer, mech. Einwirkung….
  Terrorismus
  Unterteilung: **Angriffe von innen , von außen**

Abwehrmaßnahmen: Grundsätzliche Klassifikation

- Technische Maßnahmen (darunter als wichtiger Teilaspekt : bauliche Maßnahmen),
- Organisatorische Maßnahmen

- Personelle Maßnahmen

i.A. Kombination,
die Wirkung von Angriffen ist häufig sowohl bei Datenschutz als auch bei Datensicherheit zu spüren – Abwehrmaßnahmen wirken gegen beide

Definitionen „Sicherheit

- Absolute Sicherheit - Realisierbarkeit
- Induktiv definierte Sicherheit - Beispiel
- Sicherheit mit Restrisiko

  Ablaufschema zur Erstellung eines Sicherheitskonzepts im Modell „Sicherheit mit Restrisiko“
  Bedeutung der Einbeziehung externen Fachwissens in die Erstellung des Konzepts.

2. Angriffsszenarien

Die Stellung des Menschen

Was zeichnet den Menschen gegenüber anderen Komponenten eines Sicherheitssystems aus?
Wodurch wird das Verhalten von Menschen beeinflußt?

Die besondere Gefährtung durch Angriffe von innen
Angriffe von innen vs von außen.
Warum sind Angriffe von innen besonders gefährlich ?

Wodurch wird das Verhalten von Menschen beeinflußt?
(Familie (beständig vs. stark wechselnd, Freundeskreis, Religion, Lebensstil – Verhältnis zu den Mitteln, bisheriges Leben (Erleben) , Erkrankungen – auch Spielsucht, Alkoholismus -> Geldprobleme, Bildung – Ausbildung, Anerkennung der bisherigen Lebensleistung)

Ansätze, die Wahrscheinlichkeit von Angriffen von inner zu reduzieren
(Menschenführung)

- Überprüfung der Mitarbeiter bei Einstellung und auch später (Lebenslauf analysieren, pol. Führungszeugnis, ...)
- Klare Strukturierung der Firma, klare Festlegung von Verantwortlichkeiten und Aufgaben, der Unterstellungsverhältnisse.
- Ausreichende Qualifizierung der Mitarbeiter, Möglichkeit der Weiterqualifizierung (wenn sich die Technik, die Aufgaben ändern), Vermeidung von Überqualifizierung.
- Anerkennung für geleistete Arbeit (finanziell (gutes Gehalt zahlen, Gewährung von Sonderleistungen, Privilegien(gegenüber anderen Betrieben) : ideelle, moralische Anerkennung), Erzeugen einer moralischen Bindung an die Firma, Identifikation mit der Firma (Siemensianer)
- Überprüfung der Tätigkeit,

- Protokollierung der Tätigkeit (Mitarbeiter soll informiert sein, dass alles protokolliert wird. Auswertung der Protokolle, Ziehen von Konsequenzen (für die Firma, für den Mitarbeiter) bis zur Entfernung von Mitarbeitern, die gegen die gesetzten und bekannten Regeln verstoßen – auf allen Ebenen (auch leitende Mitarbeiter).

Prinzip: Moralische Werte und Abschreckung durch die Konsequenzen.
Allen Beteiligten müssen die Konsequenzen von Fehlverhalten klar sein und auch praktisch erlebbar sein.
Das Wissen um die (fast) sichere Entdeckung eines Angriffes schreckt Angreifer von innen ab.
(Gegenbeispiel: Vorgesetzter unternimmt nichts gegen Datenmanipulation geschützter durch einen seiner Mitarbeiter, obwohl die Manipulation leicht beweisbar wäre,
Mögliche Konsequenzen: für Mitarbeiter nach § 303a StGB bis 3 Jahre Haft.
Für den Leiter: Strafvereitelung nach § 258 (1) StGB (in diesem Fall auch bis 3 Jahre Haft),
Sollte für den Leiter § 258a zutreffen (Strafvereitelung im Amt) bis 5 Jahre Haft.

Aus dem Beispiel wird klar: Auch Angriffe gegen den Datenschutz / die Datensicherheit können mit rechtlichen Konsequenzen abgewehrt werden – auch dort wo Bundesdatenschutzgesetz nicht zutrifft -
Dunkelziffer wird sehr hoch eingeschätzt. Tatsächliche Strafen fallen häufig viel geringer aus, haben weniger erzieherische Wirkung.

Technisch bedingte Angriffe (Ausfälle)

Allgemeines
Lebenszyklus von Geräten
(Ausfallrate /-wahrscheinlichkeit, „Badewannenkurve“: Frühausfälle, Normalbetrieb, Verschleiß)
Künstliche Alterung

Faktoren, die die Ausfallwahrscheinlichkeiten beeinflussen:
- Betriebsbedingungen grenzwertig (zu hoch, zu niedrig) : elektrische Spannungen, Temperaturen,
- sonstige Umweltbedingungen (schmutz, Staub, chemische Einflüsse (Flüssigkeiten, Dämpfe, Gase),
- elektrische, magnetische Felder
- bei Halbleitern insbesondere ionisierende Strahlung.

Sicherung gegen technische Ausfälle
Vorsorge durch Prüfung und Auswechseln
Redundante Auslegung (Rechenzentrum mit zwei unabhängigen Anschlussen an elektr. Netz, Kombination von USV (kurzzeitige sofortige Energielieferung) und Notstromaggregaten (die nach Anlaufzeit Energie liefern), Rechnerverbünde, RAID-arrays bei Platten.
Administrative Maßnahmen Maßnahmen zur Sicherung gegen technische Ausfälle (Pläne zur Organisation von Wartung usw., Verbote von Gefährtungen (Autoelektronik (Airbag, Abgasregelung) gestört durch starke HF-Felder, Hesteller verbietet Betrieb von

Funkgeräten im Auto bzw. schreibt Platz für Montage der Antennen sowie abgestrahlte Maximalleistung vor).

Ausgewählte technische Ereignisse
Blitzschlag / Überspannung
Literatur: Führende Hersteller von Geräten, Material zum Blitzschutz, zur Überspannungsableitung beschreiben die Wirkung des Blitzes in Broschüren oder auf ihren WEB-Seiten. ES ist nicht möglich, dass hier Namen genannt werden.
(Google, Suchwort „blitzschutz“)

Wirkung des Blitzes relevant für IT-Anlagen, Schutz ist möglich, Kenntnisse werden von Informatiker erwartet, da einfache Maßnahmen / Kenntnisse in tägliche Arbeit einfließen. Blitzwirkung erzeugt Überspannungen, die zur Zerstörung der Halbleiter führen.

Blitzparameter:
I=100 … 200kA,
U= mehrere MV, Durchschlag Luft mehrere hundert Meter.
dI/dt ~100kA/µsec (Stromanstiegsgeschwindigkeit)
Blitzdichte in DL: ca. 4 Blitze / km².Jahr, abhängig von Landschaft.

Schäden (nach Versicherungsmeldungen): mehrere 100T Fälle/Jahr mit je ca. 1000 Euro Schaden.

Einschläge:
Direkteinschlag:
Ohne äußeren Blitzschutz: schwere Gebäudeschäden – Brände
Mit äußeren Blitzschutz und Potentialausgleich:
Übergangswiderstand Erder (Fundamenterder) – Erde : 1 Ohm (0,25 Ohm) -
Gebäude auf 100 – 200kV „angehoben“.
Versorgungsleitungen bleiben auf Niveau des fernen Versorgers (ca. 0 Volt)
-> Durchschläge (auch durch Mauern) , ca 100kV zwischen Adern des Stromnetzes (gn-ge wird angehoben, sw und ws bleiben auf 0 Volt. Kabeldurchschlag,
100kV am Netzteil des Computers. 100 kV zwischen Gehäuse und Stromnetz – Totalausfall.

Stufenweise Abbau der Überspannung durch Grobschutz, Mittelschutz (1,5kV) und Feinschutz (0,6kV/5kA). (0,4kV ist normale Spitzenspannung.) , eine richtig dimensionierte Schutzmaßnahme führt die Ströme im kA-Bereich kurzzeitg (msec) ab.
Wichtig: Stufenkonzept – Feinschutz ohne Grobschuz ohne Mittelschutz ist ku schwach - d.h. Steckdoseneinsätze zu schwach, ausreichende Leitungslänge zwischen Grob-Mittel-Feinschutz wirkt als Tiefpass und ist für Funktion wichtig.

Analoge Konzepte für jede Ader jeder Leitung (Telefon, Fernsehen, …)
-> aller Leitungen im Haus sind etwa auf dem Niveau der PAS, unabhängig von der Potentialhöhe.
Am Gerät verbleiben nur so geringe Spannungsdifferenzen, dass sie unschädlich sind.

Dazu noch Wirkung des Blitzstroms wie unten beschrieben.

Einschlag in der Umgebung:
Potentialtrichter -> auch Anhebung des Potential wie bei Direkteinschlag, aber in geringerem Maße.

Wirkung des Blitzstroms

dI/dt ~100kA/µsec (Stromanstiegsgeschwindigkeit)
in einer Schleife wird eine Spannung induziert u = k dI/dt, k~ 5000V/(kA/µsec)
Annahme, das der Blitz in einen Mast (Baum) einschlägt, der 1m vom Haus entfernt ist. Im Haus wird über die PAS folgender Leitungsverbund gebildet, der geometrisch ein Rechteck mit 10m Seitenlänge ist: Computer (Netzteil, Gehäuse) – Netzleitung – PAS – Telephonleitung – Modem (kleine unterbrechung (max. 10mm) – Datennetzkabel – Rechner (Netzkarte).
Am Rechner entstehen zwischen Netzkarte und Gehäuse (bzw. zwischen Dateneingang und Masse) ca. 500kV (bei dieser Spannung haben Grob, Mittel und Feinschutz angesprochen, der Spannungsabfall über ihnen ist gleich der Brennspannung, Schalter u.ä. werden durch Lichtbogen überbrückt -> Fast 500kV Zerstören mindestens die Netzkarte.
Schutz: keine großflächigen Schleifen, Überspannungsableiter kurz vor Kabeleinführung in Computer.
Omas Schutzschaltung: Bei Gewitter trenne man alle nicht unbedingt benötigten Geräte vom Netz (Stecker ziehen) und lege die Stecker mind. 1/2m von der Steckdose ab. Leider nicht 100% sicher, aber die ingenieurtechn. Lösung auch nicht.
In einem Kabel von 10m Länge werden unter ähnl. Bed. ca. 1kV induziert.

Engl. Stichworte: EMP – electromagnetic pulse, lightning.

Beispiele, wo Resistenz gegen Blitzschlag notwendig ist: Flugsicherung, Flugzeugelektronik und -informationssysteme, moderne Kraftfahrzeuge, Steuerungen von Industrieanlagen mit gefährlichen Stoffen (chem. Reaktoren, kerntechnische Anlagen, ...)
Details zu ingenieurtechnischer Lösung: Materialien von Firmen, die Blitzschutz anbieten (.
Verschiedene Schutzklassen möglich. Kein absoluter Schutz.

Kriegseinwirkung NEMP (nuclear electromagnetic pulse): eine Atomwaffenexplosion in der Ionosphäre erzeugt dort unvorstellbar starke Ionenströme, deren magnet. Induktionswirkung auf der Erde großflächig (Europa) alle ungeschütze Elektronik zerstört.

Wirkung der Sonne
Sonne Strahlungsquelle für Strahlen aller Frequenzen. auch im UV-, Röntgen-, Gammabereich.
Zerstört Halbleiter (wichtig für Anwendungen im Weltraum)
Kommunikation (Internet) z.T. über Satelliten, Verfügbarkeit kann gestört werden.
Sonnenwind – Nordlichter – starke Ionenströme in Ionosphäre (mehrere 100 kA bis MA) – Magnetstürme.
Magnetstürme: beeinflussen Kurzwelle, Mittelwelle, Langwelle, Überreichweiten bei UKW

Stärke des Magnetfelds auf der Erde so, dass Transformatoren nicht mehr arbeiteten
Info: http://www.valdostamuseum.org/hamsmith/13Mar89.html#13Mar89.
6Mill. Menschen in Province Quebec ohne Strom.

Technische Probleme beim Datenschutz:
Jede Datenübertragung an elektromagnetische Wellen gebunden.
Mit Ausnahme der Lichtübertragung über Lichtwellenleiter gibt es stets eine Abstrahlung dieser Wellen – bei Funkübertragung gewollt, bei Kabelübertragung ungewollt. - Ansatzpunkt für Angriffe.
Funkübertragung: Empfänger i.A. nicht feststellbar, E. muß sich nur im Empfangsgebiet aufhalten _ Abwehr: kleine Sendeleistung,Richtantennen (Empfangsgebiet einschränken) – Verschlüsselung. (Problem verlagert zur Qualität der Kryptograph. Verfahren.
Kabelübertragung: Abschirmung (verringert das Gebiet, wo das Feld zum Abhören reicht), Verschlüsselung – s.o.
Schutz des Kabels durch bauliche Maßnahmen vor Anzapfen, Messung der technischen Parameter des Kabels.

Stand allgemein verfügbarer Technik:
Literatur: „SAT-Spionage für Insider. Geheime Satsignale sichtbar, lesbar machen“
PC + Empfänger für ca. 3000 Euro – alles übliche Handelsware.

Es ist nicht offengelegt: Was leistet Spezialhardware

Röhrenmonitor: liefert analoge Hochfraquenzsignale mit Bildinhalt – aus 10-20m sicher empfangbar, Schutz bauliche Maßnahmen, Abschirmung
LCD: keine Aussage.

Allg. Sicherheitsprobleme im DV-Anlagen
Passworte – schwache PW, Lexikonangriff , ...
Bewegliche Datenträger (Daten mit nach außen bringen, Daten einbringen, Viren einbringen
(Schutz: Org. Maßnahmen, Techn. Maßnahmen, Protokollierung
Kryptograph. Protokolle

Def.: Protokoll – Folge von Einzelaktionen, die i.A. verteilt zwischen mehren Partnern ablaufen, von einen Ausgangszustand des Systems zu einem Zielzustand zu gelangen.

Datenübertragung: Sender – Kanal – Empfänger (Kanal kann auch als ein Speicher oder eine andere techn. Einrichtung realisiert sein)
Im Modell gilt der Kanal als Unsicher
Was ist schützenswert:
a) Inhalt der Nachricht – Schutz: Schutz vor Mitlesen, Verschlüsselung
b) Senderidentität (Anonymisierungdienste)
c) Empfängeridentität (Rundsprüche, Anonymisierungsdienste)
d) Tatsache, dass eine Kommunikation stattfand (Anonymisierungsdienste, Rauschen)

Typische Angriffe:
a) Passives Mitlesen eines Datenstroms (eye dropper -Eva) , Schutz: Verhindern des

Zuganges, Krypt. Verschlüsselung.

b) Aktive Teilnahme mit Datenveränderung (malique - Mallet), Schutz : + div. Kryp.Protokolle
Hier Man-in-the-middle einordnen (Serverangriffe – Identität eines Dienstanbieters annehmen und fehlerhafte Dienste erbringen.
c) Empfänger leugnet Erhalt des Inhalts: Vergleich mit Einschreiben, Zustellung durch Gerichtsvollzieher, ohne Mitarbeit des Empfängers nur durch Einsatz eines glaubwürdigen Drittens (Zeuge, Notar), elektron. Lösung ist nicht besser.

d)Sender leugnet, gesendet zu haben: unsymm. Kryptographie. - hier wird mehr erreicht als im Leben.

3. Kryptographisches Grundwissen

Zu diesem Kapitel Literatur: Bruce Schneier: ...

Definition: Symmetrische Verschlüsselungsverfahren, unsymmetrische Verschlüsselungsverfahren. (Mathematische Grundlagen zum RSA-Algorithmus in der Literatur nachlesen!),
Theoretische Sicherheit von Verschlüsselungsverfahren.
Komplexität der Schlüsselverwaltung, Arbeitsgeschwindigkeit => hybride Verfahren.

Schlüsselaustauschproblem (bei symmetr. Verfahren, bei unsymmetr. Verfahren),
the-man-in-the-middle-Angriff
Verfahren zum Schlüsselaustausch mit /ohne Notar bei symmetr. Verfahren.
Schlüsselaustausch bei unsymm. Verfahren, Vertauenshierarchien (Schlüsselzentren)

Verschlüsselung zur Signatur (Symmetr. / unsymmetr.).
Was beweist Signatur? (Bei symmetr. Verfahren kein Beweis der Id. des Senders gegenüber Dritten, bei unsymmetr. Verfahren Identifikation des Senders gegenüber Dritten.)
Problem der Empfangsbestätigung (Notar vs. schrittweiser Austausch.

Hashfunktionen und Signatur.
Definition Hashfunktion, Kollisionsproblem, Erzeugung eines Dokuments gegebenem Inhalts und gegebenen Hashwerts.
Vorteile des Einsatzes von Hashfunktionen. (geringeres Volumen. Varianten der Bestätigung des Senders ohne den Inhalt zu offenbaren mit Notar.)

Was ist außer dem Inhalt noch schützenswert (Senderidentität, Empfängeridentität, Tatsacher der Kommunikation):
Senderidentität: Anonymisierdienste
Empfängeridentität: Broadcasting

Geheimhalten der Kommunikation an sich:
a) Rauschen auf dem Kanal .
b) Verdeckte Kanäle (Steganographie, Was ist ein verdeckter Kanal? Progammstart-Beispiel, Kanäle im Hashwert, in Signatur,..., Länge der Grashalme in einer Strichzeichnung ergibt Morsekode, Nutsi)
c) Anonymisierungsdienste als Netzwerk.

5. Grundfunktionen sicherer Systeme

1. Indentifikation
2. Authentifizierung
3. Rechteprüfung
4. Rechteverwaltung
5. Protokolle und Protokollauswertung
6. Fehlererkennung, Fehlerbehebung
7. Wiederaufbereitung
8. Probleme im Netz.

5.1 Identifikation: Jede Komponente im System hat eine Identität, insbesondere Nutzer. Es wird unterstellt, dass diese Identität fest ist, genauer, dass es schwierig ist, die Identität zu wechseln (ohne dass dies bemerkt wird). (Unterschied: Nutzer in Betriebssystem vs. Teilnehmer an P2P-Systemen, bei letzterem ist Wechseln leicht, Nichtwechseln wird aber „belohnt“.)

3.2 Authentifizierung: Nachweis, dass eine Komponente die angegebene Identität wirklich besitzt.

Unvernetzte Rechner (oder Konsole): Unterstellung, dass der Rechner korrekt arbeitet, nur der Nutzer authentisiert sich. (im Netz: kein Vertrauen – wechselseitige Authentisierung -ssh).

Authentisierung durch Besitz (von Gegenständen , auch von biometr. Merkmalen) oder durch Wissen.

Besitz: Gefahr durch Verlust, Fälschung , Erpressung

Fälschung nicht verhinderbar, Sicherheit: Aufwand zur Fälschung muß höher sein als der erzielte Nutzen, schützt nicht vor idealistischem Fanatismus.

Wissen: Versch. Verfahren.

Mit Übertragung des Wissens (z.B. Passwortverfahren): Übertragung des Wissens ist verfahrensbedingte Schwachstelle (im unvernetzten Rechner und Stand der Rechnerverbreitung 1985 akzepierbar, 2005 unakzepabel, zusätzlicher Schutz nötig (z.B. ssh, ...)). Dazu noch Anwenderbedingte Schwachstellen: schwache Passwörter.

Verbesserungen:
Einmalpasswörter: (Bespiel TAN), Schutz vor Wiederverwendung; Algorithmus zur Verwendung von Einmalpasswörtern mit Hashfunktion.

Zero-Knowledge-Protokolle (Authentifizierung ohne Übertragung des Wissens):

Beispiel Cardani-sche Formel.

Nichteignug eines Public.key-Verfahrens (PGP, RSA) (es wird Wissen übertragen, Nutzer signiert Nachricht, deren Bedeutung er nicht kennt (evt. kommutativ !)).

Geeignete spezielle Public-Key-Verfahren:
Feige-Shamir (1 bit wird noch übertragen)
Fiat-Feige-Shamir

Details zu beiden Verfahren: Wikipedia.

5.3 /5.4 Rechteprüfung / Rechteverwaltung:

Subjekt-Objektmodell: Definitionen Subjekte, Objekte, Doppelrolle von Programmen

Rechte: Attribute der Beziehung zwischen Subjekten und Objekten.

Arten der Rechte: read, write, append, create, alter, ..., grant, revoke.

Grant – Revoke: Problem der Rechteweitergabe und von Entzugsketten, Rechtegraph.

Klassifikationen: Offen vs. abgeschlossen

Definition: Offenes System:
Abgeschlossenes System:

Diagramm zur Rechteprüfung im abgeschl. und im offenen System.

Folgerung zur Sicherheit.

Klassifikation: Zentrale Verwaltung vs. dezentrale Verwaltung

Vor- und Nachteile.

Klassifikation: MAC vs. DAC (Stand 15.1.08)
MAC (mandadory access control) Regelbasierte Zugriffskontrolle, vorgeschriebener Zugriffsschutz.
DAC (discretionary access control) Individuelle Zugriffskontrolle

MAC liefert tendenziell sicherere Systeme – bei höheren Anforderungen Pflicht (s. später F-Klassen),

Weitergabe von grant und revoke : siehe oben.

Häufig Mischformen Windoes, UNIX (individuelle Vergabe, aber Regeln zur Vererbung in Unterverzeichnisse, Regeln bei neu erstellte Dateien, ...)

in Betriebssystemen: Rechte auf Datei und Verzeichnisebene, Trend zur feineren Unterscheidung, z.B. in DBVS: Rechte auf Attributbasis, bisher wenig realisiert Rechte auf

Contentbasis (in DB: nur Zugriff auf aggregierte Daten, nicht auf Einzelwerte,) oder kontextabhängige Rechte (wertabhängig , zeitabhängig, history-abhängig).

Realisierungen: (Beispiele)

Matrix-Modell: Matrix der Subjektze-Objekte. Elemente: Vektor der Rechte, die ein konkretes Subjekt an einem konkreten Objekt hat.

Leicht zu implementieren, Hoher Aufwand, zur Verwaltung, insbesondere wenn Prinzipien durchzusetzen sind.

Verbesserungen: Gruppeneinteilungen – Rollen, Übergang zu regelbasierten Systemen oder Mischformen.. Rechtevergabe auf Gruppenbasis, Gruppenmitglieder „erben“ die Rechte der Gruppe.

Schutzklassenmodelle (multi level systems)

Bell – LaPadulla (1976)

System high

Clark-Wison(1987)

5. 5 Protokolle

5. 6 Fehlererkennung
5. 7 Wiederaufbereitung

6. Softwarezertifizierung