Inhalt der Vorlesung:

D. Sosna:
Datenschutz und Datensicherheit

Diese Übersicht führt sichwortartig die wichtigsten Inhalte der Vorlesung auf und soll zur Wiederholung bzw. zur Prüfungsvorbereitung dienen.
Achtung: Ende Februar 07 erfolgt eine Ergänzung durch Fragen.

Literatur:

WEB: BSI,
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

Vorlesung:

Kapitel 1 : Einführung
Begriffe Datenschutz und Datensicherheit, Gültigkeitsbereich des Begriffes Datenschutz (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.

Neben Datensicherheit auch Strafrecht tangiert (§303a,b StGB,

$202a(1) StGB)

Kapitel 2: Angriffe
Was sind Angriffe auf Datenschutz und Datensicherheit?
Klassifikationsschemata für Angriffe
(nach Ursachen (Naturkatastropfen, Elementarereignisse, Unfall, Krieg, technisches Versagen einschl. technischer Mängel), nach Einwirkungsmedium (Feuer, Wasser, mechanisch), nach der Rolle des Menschen (Vorsatz, Fahrlässigkeit)
Grundsätzliche Bestandteile der Schutzmaßnahmen (konzeptionel, technisch-baulich, organisatorisch, (softwarebasiert).
Definitionen (3: theoretisch, praktisch - auf der Basis des Begriffes „Restrisiko“, induktiv)des Begriffes Sicherheit und bewertende Diskussion. (Transaktionskonzept = Beispiel ind. Sicherheit).
Prozess der Erarbeitung eines Sicherheitskonzeptes (auf der Basis der praktischen Definition des Sicherheitsbegriffen) - Bedeutung des externen Expertenwissens.
Die besondere Stellung des Menschen auf Grund seiner Fähigkeit zur Entscheidungsfindung , Einflußbereiche auf die Entscheidungsfindung eines Menschen, die besondere Stellung von Angriffen von innen, Maßnahmen zur Reduzierung der Angriffswahrscheinlichkeit durch Mitarbeiter.

2.1 Ausgewählte technische Angriffe:
Überspannung, Blitzeinwirkung.
Technischer Verschleiß (Badewannenkurve), Definition Ausfallrate, Einflußfaktoren auf technischen Verschleiß

2.2 Das Kanalmodell zur theoretischen Untermauerung des Sicherheitsbegriffes (am Beispiel der Verschlüsselung).
Funktionen /Eigenschaften der Rollen „Eva“, „Mallet“ , „Trent“.
Definition „Theoret. Sicherheit“ (mit Hilfe der Wahrscheinlichkeitstheorie)
One-Time-Pad = theoretisch sicher; Redundanz => nicht theoretisch sicher.
Praktische Sicherheit: s.o.

Angriffe auf Kommunikation: einfaches Abhören (Eva), Verändern, aktives Abhören (Mallet), Abstreiten der Sendung, Abstreiten des Empfangs,(Beweis der Sendung gegenüber Dritten, Beweis des Empfangs gegenüber dritten.)Informationsgehalt der Tatsache der Kommunikation

Kapitel 3: Kryptographisches Grundwissen

Zu diesem Kapitel Literatur: Bruce Schneier: ...

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

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

Verschlüsselung zur Signatur (Symmetr. / unsymmetr.).
Was beweist Signatur?
Bei symmetr. Verfahren kein Beweis gegenüber Dritten, bei unsymmetr. Verfahren Identifikation des Senders gegenüber Dritten.
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.)

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.

Kapitel 4: Grundfunktionen sicherer Systeme
Annahme: Rechner und Verbindung ist sicher, Nutzer vertraut Rechner, Rechner vertraut dem Nutzer nicht.

1. Identifikation
2. Authentifizierung - Nachweis der Identität
3. Rechteverwaltung
4. Zugriffskontrolle
5. Protokollierung
   Protokollauswertung
6. Fehlererkennung, Fehlerüberbrückung

Funktionen im Netz:
Annahme: Netz unsicher, Rechner vertraut nur sich selbst.
wechselseitige Identifizierung, wechsels. Authentifizierung,

Grundfunktionen im Detail:

1. Identifikation
   Angabe der Identität - Prüfung, ob die angegeb. Id. im System bekannt ist. Meist nicht einzeln realisiert, sondern in Verbindung mit
2. Authentifizierung - Nachweis der Identität - Forderung der Untäuschbarkeit.
   A. durch Wissen, durch Besitz, durch biometr. Merkmale (als Sonderform von Besitz - Was sind die Unterschiede zum Besitz einer Sache?
   A. durch Wissen: Passwortverfahren, Angriffe gegen P. Schwache Passwörter und deren Vermeidung, Einmalpassworte, Zero-Knowledge-Protokolle.

A. durch Besitz (einer Sache) - Fälschungsproblem, Verlustproblem.
Biometr. Daten - Stand - Angriffsversuche

3. Zugriffskontrolle
   grundlegender Ablauf: Zugriffsanforderung -> Rechteprüfung -> Gewährung oder Ablehnen des Zugriffs - Protokoll.
   Offenes vs. geschlossenes System - need-to-know- Prinzip
   Bewertungen dazu

4. Rechteverwaltung / Rechtevergabe
   Welche Rechte? (r, w, x, grant, revoke), Detailfragen zu „write“
   Granulat der Rechtevergabe, Domain-Modelle
   Zentrale vs. dezentrale Rechtevergabe

   DAC , MAC, MAC-Elemente von Windows-XP

   Hierarchische Modelle:
   Ziele (Schutz vor Informationsabfluß vs. Qualitätssicherung der Daten, Kombination mit Domain-Modellen.

   Konkrete Modelle: Subjekt - Objekt - Festlegung,
   Matrixmodell ,
   Take-Grant-Modell (Ausscheiden aus der Vergabekette, Probleme bei Graphen mit Zyklen)
   Bell-LaPadulla,
   Clark-Wilson.

5. Protokollierung Protokollauswertung
   Zugriffskontrolle nur sinnvoll bei Kontrolle, Kontrolle erfordert Auswertung.
   Untäuschbarkeit: Sicherheit des Protokolls gegen Fälschung, gegen Vernichtung, gegen Lücken.
   Problem: Protokolldetails vs. Auswertbarkeit
   Rollen / Aufgabenverteilung als Schutz vor inneren Angriffen

6. Fehlererkennung, Fehlerüberbrückung
   Redundanz als Grundelement der Fehlerbehandlung
   Fehlererkennende Codierung, Fehlerkorrigierende K.,
   Redundante Hardware. (USV, RAID, ...)
   Fehlerbehandlung vs. Sicherung von Daten.

Kapitel 5: Zertifizierung

Orangebook USA 1989: Grundidee und Wertung
Funktionalitätsklassen (F1 - F10): Inhaltliche Einteilung (getrennt nach F1-F5 und F6-F10) und Zuordnung zu den Grundfunktionen.
Vergleich Orangebook - F-Klassen
Methodische Verbesserungen der F-Klassen gegenüber Orangebook.

Bewertung: Qualität = Stärke des Algorithmus + Korrektheit der

Implementierung
Stufen für Stärke des Algorithmus.

Beispiel für Stärken:
Garantie der Eindeutigkeit der Identität (w Wahrscheinlichkeit der nicht Korrekten Identifizierung)

w	Bewertung
10E-8 ...10E-6	sehr stark
10E-6 ...10E-4	stark
10E-4 ...10E-2	mittelstark
10E-2 ... 1	schwach

Stufen für Korrektheit der Implementierung
Sinnvolle Kombinationen, Ausschlußverfahren bei Q0.

Bespiele: ; Passwortverfahren mit Speicherung im urspr. UNIX als Beispiel, wie sich die Bewertung zeitlich ändert (Vergleich 1985 vs. heute)

Zertifizierung
3 Stufen
Vorbereitung ... -> Vertrag
Prüfung ... -> Interner Bericht (Was ist Inhalt ?)
Kontrolle durch unabh. Gruppe
-> Zertifikat, Externer Bericht (Was ist Inhalt?)

Gültigkeit des Zertifikats bei Versionswechsel ?

Ist zertifizierte Software sicher hinsichtlich Datenschutz und Datensicherheit ?