Datenschutz und Datensicherheit Rechtliche und technische Aspekte Vortrag, Sommersemester 2008

Johannes Waldmann, HTWK Leipzig

14. Mai 2008

— Typeset by FoilTeX —

Überblick

Begriffe

- Datenschutz:

  Schutz der informationellen Selbstbestimmung von (natürlichen) Personen.

  gesetzliche Vorschriften zur Verarbeitung personenbezogener Daten.

- Datensicherheit:

  technische Realisierung von Zugriffsbeschränkungen be Übertragung und Speicherung von Daten

Typeset by FoilTeX

Datensicherheit als technische Frage

Themen

- Sicherheit von Daten in einem Computer (Rechte von Dateien und Prozessen)
- Authentifizierung (Paßwörter)
- Sicherheit der Datenübertragung (unsichere Kanäle, symmetrische und asymmetrische Verschlüsselung)

Typeset by FoilTeX

Sicherheit von Dateien

(unter UNIX, andere Systeme ähnlich)
für jede Datei wird gespeichert

- Eigentümer
- Gruppe

und 3 mal 3 Rechte:

- lesen (r), schreiben (w), ausführen (x)
- für Eigentümer (u - user), Gruppe (g), Welt (o - others)

Anzeigen `ls -l`, Rechte ändern `chmod go-r *`,
Besitzer ändern `chown heinz log.txt`
Diese Rechte stehen nicht in der Datei, sondern im Verzeichnis, das ist selbst eine Datei (mit Rechten).

Typeset by FoilTeX

Sicherheit von Prozessen

- Benutzer startet Prozesse, diese greifen auf Hardware zu (Hauptspeicher, Festplatte, Tastatur, Grafikkarte . . .)
- jedes Gerät hat Rechte (wie Datei)
- jeder Prozess hat Eigentümer/Gruppe
- Prozess darf nur das, was nach voriger Folie möglich ist.
- System vernünftig organisieren: Rechte fein abstufen, für jeden Prozeß nur soviel Rechte, wie nötig.

Aufgabe: welche Geräte sind datenschutzkritisch?
Aufgabe: welche Rechte-Konzepte bei E-Learning/Dok-Mngmt-Systemen (z. B. OPAL)?

Typeset by FoilTeX

Authentifizierung

Feststellen der Identität einer Person (eines Systembenutzers).
benutzt Merkmale, die sich nicht übertragen lassen (sollen

- biometrische Daten (Fingerabdruck, Stimme,. . .)
- Sachen (Schlüssel, Speicherkarte)
- Wissen (Paßwort)

nach Authentifizierung können Rechte zugeordnet werden
Aufgabe: diskutiere anonyme Rechtezuordnung (E-Learning)

Typeset by FoilTeX

UNIX-Passwörter

- ist Zeichenfolge, aber wird *nicht* als solche abgespeichert
- (der Administrator kann `/etc/passwd` lesen, erfährt daraus aber nicht die Paßwörter)
- benutzt Einbahnfunktion $f : w \mapsto f(w)$, speichert $f(w)$
- gleiche Paßwörter $\rightarrow$ gleicher Eintrag
- deswegen zusätzliches Argument (salt) s würfeln (beim Einrichten des Accounts) und das Paar $(s, f(s, w))$ speichern.

Authentifizierung bei Webdiensten

für jeden Dienst ein Account/Paßwort: unübersichtlich. Verringert Akzeptanz.
Aufgabe: wieviele Accounts/Paßwörter haben Sie?
zentraler Dienst (OPAL) delegiert Authentifizierung: Shibboleth.

- Benutzer an OPAL: ich bin XYZ und will es gegenüber HTWK beweisen.
- OPAL an HTWK-RZ: ist XYZ bekannt?
- Benutzer an HTWK-RZ: Paßwort-Login
- HTWK-RZ an OPAL: Ja.

wichtig: Paßwort wird nur gegenüber HTWK-RZ benutzt

Sicherheit der Datenübertragung

- Internet ist offenes System: jeder Rechner sieht alle Datenpakete (seines Subnetzes)
- d. h. Email = Postkarte, usw.
- kann man überhaupt über unsichere Kanäle sicher kommunizieren?
- Übertragung verschlüsseln, aber wie überträgt man die Schlüssel?
- Beispiel Kiste mit Schlössern

Diffie-Hellman (symmetrische Schlüssel)

Grundlage: Rechnen im Restklassenkörper (modulo einer Primzahl).
Beispiel: $9 \cdot 5 \bmod 11, 3^5 \bmod 11$
Diffie-Hellman-Verfahren zur Generierung eines Schlüssel k

- A und B vereinbaren (offen) Primzahl p und primitive Wurzel g von p
- A wählt (geheim) Zahl a, publiziert $g^a \bmod p$
- B wählt (geheim) Zahl b, publiziert $g^b \bmod p$
- A berechnet $k = (g^b)^a \bmod p$
- B berechnet $k = (g^a)^b \bmod p$

RSA (asymmetrische Schlüssel)

Vorbereitung: Person A erzeugt

- öffentlichen Schlüssel o
- geheimen Schlüssel g (Umkehrung von o)

so, daß $\forall n : g(o(n)) = n$
Nachricht n von B an A

- B berechnet $o(n)$
- A berechnet $g(o(n)) = n$.

o muß Einbahnfunktion sein.
Benutzt schwere zahlentheoretische Aufgaben, z. B. Faktorisierung von großen Zahlen (2000 Binärstellen)

Signaturen

- Bei RSA-Verfahren gilt $g(o(n) = n$ und $o(g(n)) = n$.
- Damit ist auch Authentifizierung möglich:
- B signiert Nachricht durch Verschlüsseln mit g, jeder kann mit o entschlüsseln (= Signatur prüfen).
- Verwaltung von öffentl. Schlüsseln auf Keyservern
- Zuordnung Schlüssel–Person? Signieren von Schlüsseln (zentral — CA, verteilt — web of trust)

Benutzung von RSA bei SSH, HTTPS
Aufgabe: untersuche einige HTTPS-Zertifikate

Datenschutz als Persönlichkeitsrecht

Themen

- Grundbegriffe
  - personenbezogene Daten
  - Datenverarbeitung
  - rechtliche Grundsätze
- Geschichte, Einordnung in Rechtssystem
- Quellen (EU-Richtlinien, Bundesdatenschutzbeauftragter, Sächsischer Datenschutzbeauftragter)
- Beispielfälle, besonders aus Bereich Studentendaten/E-Learning

Vorwort

`http://www.datenschutz.sachsen.de/`
Der Mensch ist zur Freiheit geboren. Die Freiheitsrechte des Einzelnen kennzeichnen den modernen Rechtsstaat. Deshalb muss jede Obrigkeit - egal in welchem Gewande sie daherkommt - sich aus der privaten Freiheitssphäre de Einzelnen heraushalten. Jeder soll möglichst frei tun und lassen dürfen, was er will. Und dazu gehört, dass er dabei nicht amtlich beobachtet und bewertet wird.
Datenschutz ist die Lehre von der Begrenzung der staatlichen Neugier. Damit wird die Gewährleistung der Freiheit abgesichert. Ein Kennzeichen des totalitären Staates ist es, alles über seine Bürger zu sammeln, wobei er diese kalkuliert im Unklaren lässt, was er über sie weiß.

Vorwort (II)

Nach der Sächsischen Verfassung und nach dem Grundgesetz in der Auslegung des Bundesverfassungsgerichts soll das anders sein: Wenn eine Behörde die für ihr legitimes Handeln geeignete, erforderliche und zumutbare Informationen über Menschen sammeln will, muss sie sich dazu auf eine gesetzliche, d. h. in einem öffentlichen Verfahren demokratisch legitimierte Grundlage stützen können. Sie muss ihr Handeln überschaubar machen (Transparenzgebot). Jeder muss sich in einem freien Land darauf verlassen können, dass er nicht unrechtmäßig beobachtet oder gar ausgeforscht wird.

Gesetze

- Bundesdatenschutzg.

  regelt Datenverarbeitung zw. Privatpersonen
- Sächsisches DSG

  regelt Datenverarbeitung öffentlicher Stellen

Geschichte: Volkszählungsurteil 1983, DSG Hessen, Bund
Grundrechte als Abwehrrechte

Grundbegriffe

- personenbezogene Daten

  Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person

- Verarbeitung

  umfaßt Erheben, Speichern, Verändern, Anonymisieren, Übermitteln, Nutzen, Sperren, Löschen

Grundsätze

Verarbeitung personenbezogener Daten nur erlaubt, wenn

- Gesetz oder Rechtsvorschrift dies erlaubt
- oder Betroffener einwilligt

Betroffener hat dann Recht auf

- Auskunft
- Berichtigung, Löschung, Sperrung
- Widerspruch, Schadenersatz, Anrufung DBS

Art der Verarbeitung

Erhebung

- nur, wenn zur Aufgabenerfüllung erforderlich
- nur beim Betroffenen mit dessen Kenntnis

Löschung

- sobald Daten zur Aufgabenerfüllung nicht mehr erforderlich