Freie Universität Berlin

Vorlesung "Anwendungssysteme"

Privatsphäre

Prof. Dr. Lutz Prechelt
Freie Universität Berlin, Institut für Informatik
http://www.inf.fu-berlin.de/inst/ag-se/

- Definition,
- Begründung, Entwicklung
- Niederschlag in Grundrechte
- Beispiele
- Bedrohung durch Computerisierung
  - Fallbeispiele
  - Gegenmaßnahmen

Definition "Privatsphäre" (privacy)

Freie Universität Berlin

Definitionsversuch:

- Der Bereich, in dem eine Person selbst bestimmt (oder bestimmen können sollte), wem sie wann und warum welche Information über sich selbst zugänglich macht.

- Eine einheitliche Definition gibt es nicht
  - Die Meinungen gehen sogar recht weit auseinander

Philosophische Begründung

Freie Universität Berlin

- Die Forderung, Privatsphäre zu schaffen und zu schützen, ist ein Ausfluss der Goldenen Regel

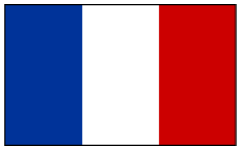
- Goldene Regel (Prinzip der Reziprozität):
  - Im Buddhismus (6. Jh. v. Chr.):
    "Verletze nicht andere auf Wegen, die Dir selbst als verletzend erschienen." (Udana-Varga 5, 18)
  - Als deutsches Sprichwort:
    "Was Du nicht willst, dass man Dir tu,
    das füg auch keinem Andern zu."
  - Als kategorischer Imperativ (Immanuel Kant):
    "Handle so, dass die Maxime deines Willens jederzeit zugleich als Prinzip einer allgemeinen Gesetzgebung gelten könne."
    (aus: Kritik der praktischen Vernunft, 1788)
  - u.s.w.

Historische Entwicklung

Freie Universität Berlin

- Seit Aufkommen der Rechtsstaatsidee wird auch die Idee von Persönlichkeitsrechten verfolgt
  - z.B. Recht auf Leben, Recht auf körperliche Unversehrtheit

- Mit dem allmählichen Ausbau solcher Rechte ordnen sich diese zunehmend der Idee der Selbstbestimmung unter
  - Meilensteine:
    Unabhängigkeitserklärung der USA 1776,
    französische Revolution 1789



- Mit zunehmender Computerisierung erweitert sich die Idee der Selbstbestimmung auf die Kontrolle über Information über sich selbst
  - Meilenstein: "Volkszählungsurteil" des deutschen Bundesverfassungsgerichts 1983
    ("Recht auf informationelle Selbstbestimmung")

Allgemeine Erklärung der Menschenrechte

Freie Universität Berlin

United Nations (UN), 1948:

- Artikel 12:
  - Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden.
  - Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.

- Siehe UN High Commissioner for Human Rights: http://www.unhchr.ch/udhr/lang/ger.htm

Grundrechte, die die Privatsphäre betreffen

Freie Universität Berlin

Grundgesetz der Bundesrepublik Deutschland:

- Artikel 2 (Entfaltung d. Persönlichkeit), Abs 1:
  - Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt u. nicht gegen die verfassungs-mäßige Ordnung oder d. Sittengesetz verstößt.
- Artikel 3 (Gleichberechtigung), Absatz 3:
  - Niemand darf wegen seines Geschlechtes, seiner Abstammung, seiner Rasse, seiner Sprache, seiner Heimat und Herkunft, seines Glaubens, seiner religiösen oder politischen Anschauungen benachteiligt oder bevorzugt werden. Niemand darf wegen seiner Behinderung benachteiligt werden.
- Artikel 4 (Glaubens-, Gewissens- und Religionsfreiheit)
- Artikel 8 und 9 (Versammlungs-/Vereinigungsfreiheit)

Grundrechte, die die Privatsphäre betreffen (2)

Freie Universität Berlin

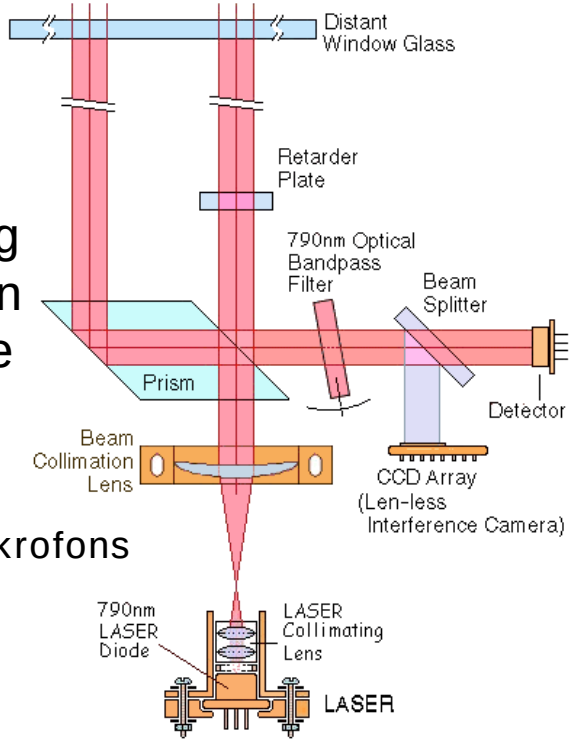
- Artikel 10 (Kommunikationsgeheimnis), Absatz 1 und 2:
  - (1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.
  - (2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung [...], so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird [...].

- Artikel 11 (Freizügigkeit)
- Artikel 14 (Eigentum)
- Artikel 15 (Asylrecht)

Grundrechte, die die Privatsphäre betreffen (3)

Freie Universität Berlin

- Artikel 13 (Unverletzlichkeit der Wohnung), Absatz 3:
  - Begründen bestimmte Tatsachen den Verdacht, daß jemand eine durch Gesetz einzeln bestimmte besonders schwere Straftat begangen hat,
    so dürfen zur Verfolgung der Tat auf Grund richterlicher Anordnung technische Mittel zur akustischen Überwachung von Wohnungen, in denen der Beschuldigte sich vermutlich aufhält, eingesetzt werden,
    wenn die Erforschung des Sachverhalts auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre.
  - Die Maßnahme ist zu befristen. Die Anordnung erfolgt durch einen mit drei Richtern besetzten Spruchkörper. Bei Gefahr im Verzuge kann sie auch durch einen einzelnen Richter getroffen werden.



Funktionsprinzip eines Doppelstrahl-Lasermikrofons
www.williamson-labs.com/laser-mic.htm

Maßnahmen zum Schutz der Privatsphäre

Freie Universität Berlin

Sehr verschiedene Arten und Bereiche (Beispiele):

- Physische Blockaden: z.B.
  - Türen, Schlösser, Jalousien
  - Kleidung
- Höflichkeitsregeln: z.B.
  - Anklopfen
  - "So was fragt man nicht"
- Anonymität:
  - Geheime Abstimmungen
  - Vermummung bei Demonstrationen
  - Bezahlen mit Bargeld

Maßnahmen zum Schutz der Privatsphäre (2)

Freie Universität Berlin

- Geheimhaltungsgebote:
  - Bankgeheimnis
    - A, CH: Recht und Pflicht der Bank gemäß Bankgesetz
    - D: gesetzl. Recht der Bank gegen Staat, Vertragspflicht gegen Kunde
  - Schweigepflicht
    - §203 StGB: Ärzte, Rechtsanwälte, Sozialarbeiter u.a.

- Informationelle Selbstbestimmung (Beispiele):
  - Datenschutzrecht (z.B. bei Datenweitergabe)
  - Verschlüsselung von Daten(verkehr)
  - Anonymer Datenverkehr
  - Weglassen von vier Ziffern der gewählten Nummern auf Telefonrechnungen

- etc.

Privatsphäre und Computerisierung

- Im Vor-Computer-Zeitalter kannte man seine Privatsphäre recht gut
- und konnte Sie auch überwiegend genügend schützen
  - Einschränkungen betrafen hauptsächlich Kenntnisse von Personen in der nahen Umgebung
    - die nämlich schwierig zu beschränken sind
- Computerisierung bringt zahllose neue Bedrohungen der Privatsphäre hervor
  - Hauptsächlich im Umgang mit Informationen
  - Aber fast alle Aspekte der Privatsphäre schlagen sich in Informationen nieder…

Fallbeispiele

Für Zusammenhang zw. Privatsphäre und Computerisierung

- Telefonieren
- Bilder von Personen in der Öffentlichkeit
- Abruf von Webseiten
  - Inhaltsdaten
  - Verkehrsdaten
- Elektronisches Bezahlen
- Sozialversicherungsnummer

Fallbeispiel: Telefonieren

Freie Universität Berlin

- Angenommen, Sie führen ein Telefonat, von dem niemand außer dem Angerufenen etwas erfahren soll
  - (Beispiele sind auch ohne die Annahme krimineller Aktivitäten leicht zu finden)

- Wer kann davon erfahren?
  - Wer sich (unbemerkt?) im gleichen Raum(?) aufhält
  - Wer während dessen (unbemerkt?) dazu kommt
  - Wer den Raum(?) abhört (C)
  - Wer das Telefon abhört (C)
  - (all dies nochmals auf der Gegenseite)
  - Wer Zugang zu Aufzeichnungen über Telefongespräche hat
    - Mitschnitte C
    - Verbindungslisten C

C = Erst durch Computer möglich oder realistisch geworden, bzw. stark erleichtert

Fallbeispiel: Bilder

- Angenommen, Sie sind morgen in Stuttgart, ohne dass jemand davon etwas erfahren soll
  - (Beispiele sind auch ohne Annahme krimineller Aktivitäten leicht zu finden)
- Wer kann davon erfahren?
  - Jemand, der sie zufällig direkt in Stuttgart sieht
  - Jemand, der ein Foto davon im Web sieht, auf dem Sie zu erkennen sind
    - z.B. von einer Webcam aufgenommen C
    - z.B. von einer Privatperson zu anderem Zweck aufgenommen und mit 12 Megapixel Auflösung ins Netz gestellt C
  - etc.
- Das Veröffentlichen solcher Bilder ist theoretisch nicht ohne Weiteres erlaubt. Praktisch jedoch…

Fallbeispiele

Für Zusammenhang zw. Privatsphäre und Computerisierung

- Telefonieren
- Bilder von Personen in der Öffentlichkeit
- **Abruf von Webseiten**
  - **Inhaltsdaten**
  - **Verkehrsdaten**
- Elektronisches Bezahlen
- Sozialversicherungsnummer

Fallbeispiel: Abruf von Webseiten

Freie Universität Berlin

- Angenommen, Sie rufen Webseiten zu einem Thema ab, von dem niemand erfahren soll, dass es Sie interessiert
  - (Beispiele sind auch ohne die Annahme krimineller Aktivitäten leicht zu finden)

- Wer kann davon erfahren?
  - Wer Ihnen dabei zusieht
  - Wer Zugang zu den Abruflisten auf Ihrem Computer hat
    - z.B. ein Administrator/superuser
    - z.B. eine Spyware
  - Wer die Verbindung zwischen Ihrem Rechner und dem Server beobachten kann
    - und zugleich weiß, welche IP-Nummer Sie haben

Was gilt es zu schützen? 2 Bereiche:

- **Inhaltsdaten**: Welche Nachrichten werden übermittelt?
  - Inhalt von Emails, Dokumenten, Telefongesprächen etc.
  - Gewünscht: Offen zwischen Sender und Empfänger(n), verborgen gegenüber Dritten
- **Verkehrsdaten**: Wer kommun. wann wie viel mit wem?
  - Absender, Empfänger, Größe/Dauer/Art von Nachrichten
  - Gewünscht (Fall 1): Offen zw. Sender und Empfänger(n), verborgen gegenüber Dritten
  - Gewünscht (Fall 2): Zusätzlich ist auch der Sender gegenüber dem Empfänger verborgen
    - z.B. anonyme Beratung
    - z.B. Beiträge in Diskussionsforen

Technische Schutzverfahren

Freie Universität Berlin

- Inhaltsdaten: Verschlüsselung
  - Sender und Empfänger vereinbaren einen geheimen Code und verwenden diesen zur Darstellung der Daten
  - Ausgereifte Verfahren sind breit als SW verfügbar
    - Inkl. Verfahren, um die sichere Vereinbarung des Codes ohne einen Extrakanal zu ermöglichen (asymmetrische Verschlüsselung)
- Verkehrsdaten: Verbergung und Anonymisierung
  - Verkehrsdaten werden so über viele Beteiligte zersplittert, dass ein erfolgreiches Wiederzusammensetzen schwierig (also unwahrscheinlich) wird
  - Siehe nachfolgendes Beispiel

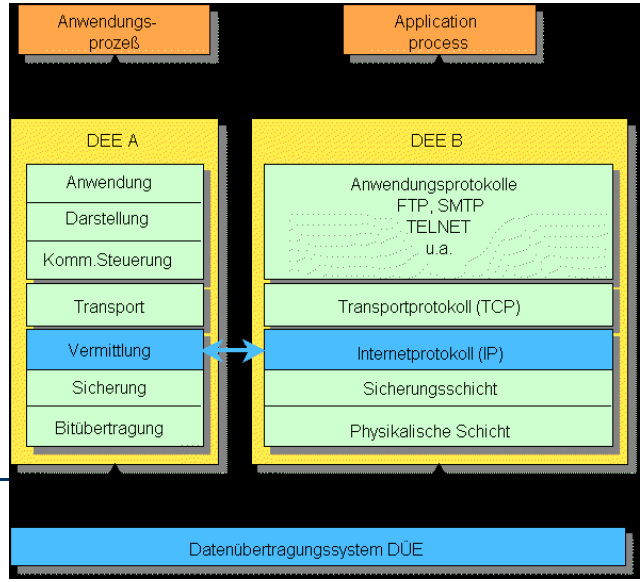
Technik: Abruf von Webseiten

Freie Universität Berlin

Vorgang:

- Browser schickt eine HTTP-Anfrage an den Server ab:
  - Von: 160.45.111.67
  - An: 201.143.22.109
  - Anfrage: GET //www.getnet.com/trace?160.45.111.67
- Diese Anfrage wandert über zahlreiche Zwischenstationen zum Server
- Der Server sendet die passende Seite über zahlreiche (evtl. andere) Zwischenstationen zurück zum Absender

- Diese Nummern (160.45.111.67) sind sogenannte IP-Nummern (internet protocol) und sind eindeutig einem Rechner zugeordnet (evtl. nur vorübergehend)



Zwischenstationen der Nachricht: traceroute

Freie Universität Berlin

- Nachricht von getnet.net (Arizona) nach inf.fu-berlin.de
  - 1 216.19.223.1 (216.19.223.1)
  - 2 phnx-core2-7513.getnet.net (216.19.201.248)
  - 3 s1-0.ca01.phx01.atlas.cogentco.com (38.112.7.25)
  - 4 s15-1.core01.san01.atlas.cogentco.com (154.54.2.5)
  - 5 p4-0.core01.lax01.atlas.cogentco.com (66.28.4.77)
  - 6 p1-0.core01.lax05.atlas.cogentco.com (154.54.2.210)
  - 7 208.50.13.197 (208.50.13.197)
  - 8 so5-0-0-2488M.ar2.FRA2.gblx.net (67.17.65.54)
  - 9 Dante-Frankfurt-1.so-6-0-0.ar2.FRA2.gblx.net (208.48.23.142)
  - 10 cr-berlin1-po2-2.g-win.dfn.de (188.1.18.186)
  - 11 ar-fuberlin1-po0-0.g-win.dfn.de (188.1.20.6)
  - 12 FUB.G-WiN.BRAIN.NET (160.45.0.1)
  - 13 zedat.spine.fu-berlin.de (130.133.98.11)
  - 14 taku9.router.fu-berlin.de (160.45.252.182)
  - 15 dhaka.mi.fu-berlin.de (160.45.111.67)

Zwischenstationen

- Im Beispiel waren also 7 Organisationen beteiligt, die die Nachricht "gesehen" haben:
  - getnet.net
  - cogentco.com
  - <unbekannt>
  - gblx.net
  - dfn.de
  - brain.net
  - fu-berlin.de

- Selbst wenn Sie Verschlüsselung verwenden (https), sehen alle diese immer noch, von welchem Server Sie Daten abgerufen haben
  - nur nicht mehr, welche

Zwischenstationen (2)

Freie Universität Berlin

Anmerkung:

- Die Zahl der Zwischenstationen kann auch bei Abrufen im gleichen Land noch erheblich sein

- Beispiele (von FUB aus, Juli 2004):
  - www.spiegel.de: 12 Stationen, 5 Organisationen
  - www.web.de: 14 Stationen, 5 Organisationen
  - www.gmx.de: 11 Stationen, 5 Organisationen
  - www.google.de: >17 Stationen, 6 Organisationen
  - www.ebay.de: >9 Stationen, 5 Organisationen

Einblick in die Kommunikation

Freie Universität Berlin

Unvermeidlich sind folgende Einblicke:

- Serverseite: Der Besitzer des Servers weiß immer, was für Inhalte abgerufen wurden
  - Auch bei Verschlüsselung, denn die wird ja dort erst hergestellt
- Empfängerseite: Der Internet-Versorger (provider) weiß immer, wer den Abruf gemacht hat
  - Er kennt den Berechtigten für die Benutzung der IP-Adresse als konkrete Person oder Organisation
    - aus Gesetzes- und Haftungsgründen
    - für Abrechnungszwecke
  - Halbe Ausnahme: Internet-by-call
    - Abrechnung erfolgt per Telefonnummer über die Telefonrechnung
    - die Person dazu kennt nur die Telefongesellschaft
  - Ausnahme: offene W-LANs (rechtlich heikel)

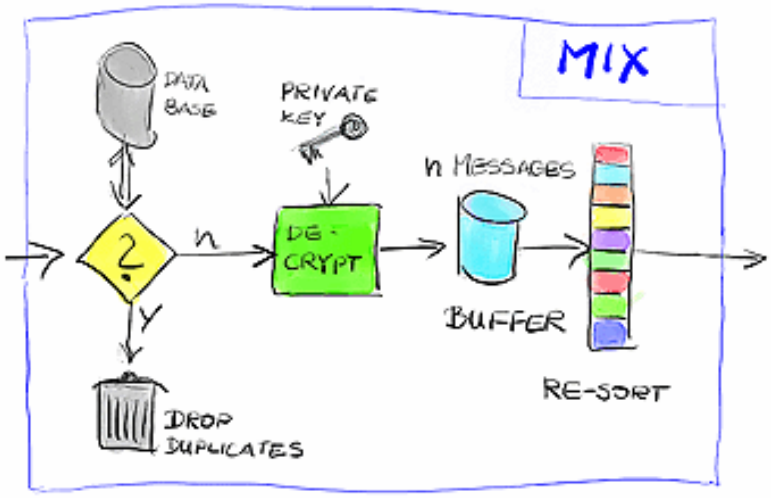
Grad der Anonymität und Privatsphäre

Freie Universität Berlin

- Wenn also Serverinhaber und Internet-Versorger kooperieren, ist selbst mit Verschlüsselung keine Anonymität gegeben
  - nicht selten sind beide identisch oder über Mutterfirmen miteinander verbunden
- ohne Verschlüsselung kann sogar jede (Zwischen)Station alle Verkehrs- und Inhaltsdaten sehen
- Das ist von Belang, weil der Gesetzgeber die Versorger zu immer mehr Aufzeichnungen und Auskunftgabe an Behörden verpflichtet
  - siehe z.B. http://www.datenschutzzentrum.de/ldsh/recht.htm

Schutz von Internet-Verkehrsdaten: JAP

- Ein Ansatz, um die Privatsphäre für Verkehrsdaten bei Internet-Benutzung zu schützen, funktioniert wie folgt:
  - Man schaltet absichtlich zusätzliche Zwischenstationen ein
    - genannt "Mixe"; viele Benutzer verwenden jeden Mix
  - Diese leiten die Daten nicht nur weiter, sondern geben sich dabei selbst als Absender aus
  - Um den wahren Absender aufzudecken, müssen nun neben Empfänger und Internet-Versorger auch noch alle diese Mixe mitarbeiten
    - evtl. Mixe in mehreren Ländern
    - und ein Mix-Betreiber will ja die Privatsphäre schützen!

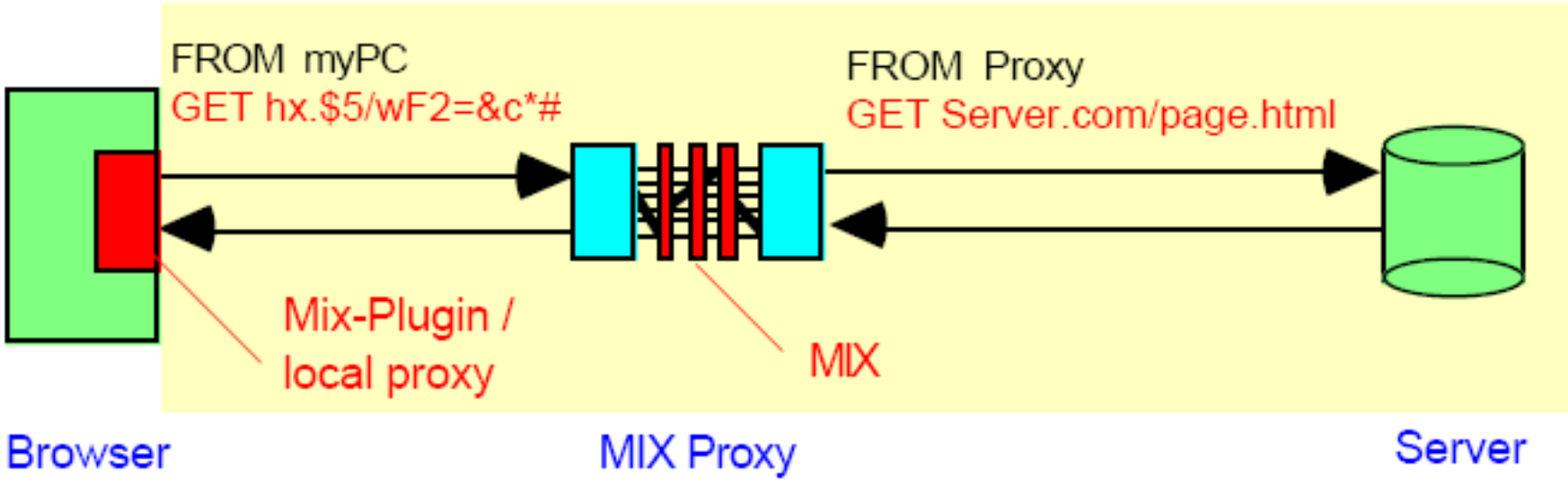


- Realisiert z.B. im Projekt JAP (TU Dresden)
  - http://anon.inf.tu-dresden.de

JAP: Funktionsprinzip

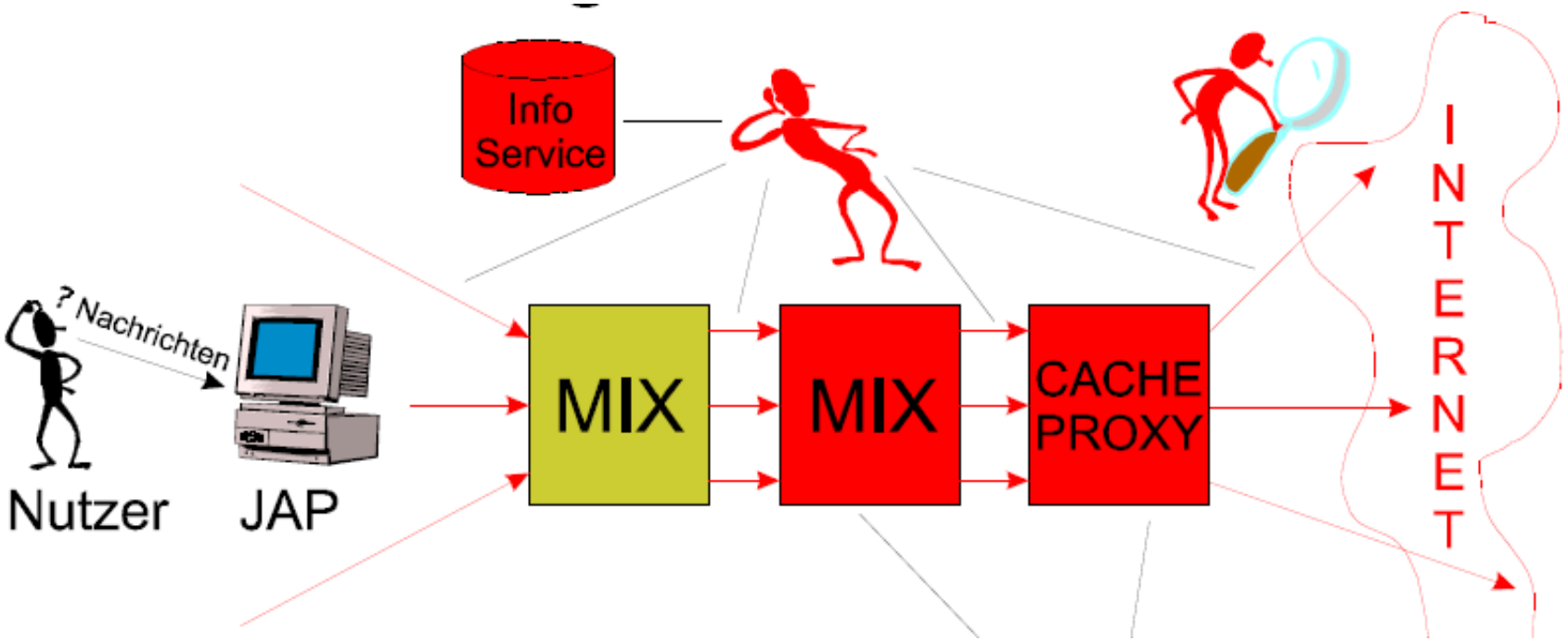
Freie Universität Berlin

- Nur der letzte Mix in der Kette macht eine normale, un-private Webabfrage
- Jeder Mix davor verbirgt eine Herkunft
- Auch für eigentlich unverschlüsselte Abfragen wird die Zieladresse verschlüsselt



Sicherheit von JAP:

- Anonymität ist immer gewährleistet, außer in 2 Fällen:
  - Alle Mixe werden zugleich kompromittiert
    - das ist wenig wahrscheinlich
  - Der Weg vom Benutzer zum ersten Mix wird kompromittiert
    - typischerweise direkt auf dem Rechner des Benutzers



Verkehrsdatenvolumen

Freie Universität Berlin

- Verkehrsdaten können auch interessant sein, wenn grundsätzlich schon bekannt ist, dass 2 Parteien gelegentlich miteinander Nachrichten austauschen
  - z.B. (Folklore-Theorem:)
    Pizzalieferanten im Raum Washington sehen Krisen ein bis drei Tage vor der Öffentlichkeit,
    weil Pizzabestellungen aus den Bürohäusern der Regierung sprunghaft ansteigen.
  - http://tafkac.org/politics/pentagon_pizza.html

Fallbeispiele

Für Zusammenhang zw. Privatsphäre und Computerisierung

- Telefonieren
- Bilder von Personen in der Öffentlichkeit
- Abruf von Webseiten
  - Inhaltsdaten
  - Verkehrsdaten
- **Elektronisches Bezahlen**
- Sozialversicherungsnummer

Fallbeispiel: Kaufverhalten

Freie Universität Berlin

- Angenommen, Sie möchten nicht, dass jemand einen vollen Überblick über Ihr Kaufverhalten bekommt
  - (Beispiele sind auch ohne die Annahme krimineller Aktivitäten gut zu finden, z.B. Sexspielzeug, Alkohol, Medikamente)

- Wer könnte einen solchen Überblick bekommen?
  - Jemand, der Ihnen ständig hinterher läuft
  - Jemand, der eine hübsche elektronische Zusammenfassung all Ihrer Käufe bekommt
    - weil das Bezahlen nicht anonym war
    - oder weil Sie eine Kundenrabattkarte benutzen

- Die Anonymität von Zahlungsmitteln ist also von Interesse

Anmerkung zur Anonymität von Geld

- Hartgeld (Münze) ist hochgradig anonym
- Papiergeld (Schein) hat eine Seriennummer
  - Wenn also jemand, der mich kennt und mir Geld gibt, mit dem späteren Empfänger kooperieren würde, könnte die Anonymität durchbrochen werden
- Buchgeld (Konto) ist in der Regel an natürliche oder juristische Personen gebunden
  - Seine Verwendung unterliegt allerdings dem Bankgeheimnis
  - Die Anonymität ist aber erheblich eingeschränkt
- Elektronisches Bezahlen hat häufig Buchgeldcharakter

Elektronisches Geld

Freie Universität Berlin

- Definition "Elektronisches Geld" (eGeld):
  - Datenpakete mit bestimmtem, weithin akzeptiertem Wert
    - praktisch gleichwertig zum gesetzlichen Zahlungsmittel
  - inhabergebunden, anonym, nichtverfolgbar
  - Rein technisch gibt es solche Systeme! (z.B. eCash)

- Definition "elektronisches Bezahlsystem" (eBS)
  - Ein definiertes Verfahren (Protokoll), mit dem die Übertragung von Geld zwischen Personen arrangiert werden kann

- Die meisten elektronischen Bezahlsysteme sind aber kein eGeld in diesem Sinne
  - Sie sind insbesondere meist nicht anonym

Eigenschaften von Zahlungssystemen

Freie Universität Berlin

- *Sicherheit:*
  Schwierigkeit/Kosten von Fälschung
- *Zahlungszeitpunkt*:
  vor/nach/beim Kauf
- *Transaktionskosten* (auch: Bequemlichkeit)
- *Anonymität*:
  Identifikation vermeidbar?
- *Direktübertragung*:
  Kann Geldübertragung ohne Mitwirkung Dritter erfolgen?
- *Verfolgbarkeit*:
  Kunden aufdeckbar? (ehrliche, betrügerische)

Eigenschaften von Zahlungssystemen (2)

Freie Universität Berlin

	Barg.	*Buchg.*	*eGeld*	*and.eBS*
• *Sicherheit*:	o	+	??	??
• *Zahlungszeitpunkt*:	bei	nach	bei	vor/bei/nach
• *Transaktionskosten*:	*+?*	+	+	*??*
• ***Anonymität***:	+	-	+	-?
• *Direktübertragung*:	+	-	??	-
• ***Verfolgbarkeit***:	-	o	-?	??

Ein populäres eBS: ClickandBuy

Freie Universität Berlin

- Konzipiert für das Bezahlen von Leistungen, die über WWW abgerufen werden

- Kunde und Händler müssen beide einen Account bei ClickandBuy besitzen
- Transaktionsablauf:
  1. Händler lenkt den Kunden beim Bezahlvorgang zu einer Seite von Firstgate
     - und gibt Beschreibung von Artikel und Preis mit
  2. Kunde meldet sich dort an und bestätigt Artikel, Betrag und Zahlung
  3. Firstgate meldet Zahlung an Händlerserver und lenkt Kunden auf die "Kauf ist erfolgt"-Seite des Händlers
     - bei elektronischen Leistungen erfolgt hier jetzt der Abruf

ClickandBuy (2)

Freie Universität Berlin

- Zahlungsabwicklung:
  - ClickandBuy kumuliert alle Zahlungen eines Kunden und stellt sie dem Kunden monatlich in Rechnung
  - Zahlungsmöglichkeiten des Kunden sind Lastschrift oder Kreditkarte oder Debit-Konto (Vorausbezahlung)
  - ClickandBuy überweist dem Händler den Betrag für alle Kunden eines Zeitraums
- ClickandBuy lebt von einer Provision des Händlers
  - normalerweise je monatl. Umsatz 9,5% bis 15% plus 50 Cents Grundgebühr! (Stand Sept. 2005)
- In Deutschland derzeit (Stand 2004) ca. 2,5 Mio. Nutzer und ca. 3000 Händler in 7 Ländern
  - unterstützt (Stand 2010-03) 50 nationale Bezahlmethoden

ClickandBuy: Vertraulichkeitsprobleme

Freie Universität Berlin

- Transaktionsdaten des Kunden:
  - Ist Kunde anonym gegenüber dem Händler?
    - Das ist bei ClickandBuy nicht klar dokumentiert
  - Jede Transaktion eines Kunden wird ClickandBuy offen gelegt
    - Händler, Kunde, Artikel, Betrag
    - ClickandBuy kann also ein ggf. umfangreiches Kaufprofil anlegen
- Betriebsgeheimnis des Händlers:
  - Zahlen darüber, welche Produkte im Detail wie viel Umsatz erzielen, sind normalerweise Firmengeheimnisse
    - ClickandBuy bekommt Teile dieser Daten
  - Ebenso Nachfrageprofile ("wer A kauft, kauft auch B")
    - ClickandBuy bekommt Teile dieser Daten
- Wurde 2010-03 plötzlich Tochter der Deutschen Telekom

Beispiel 2: Paypal

Freie Universität Berlin

- Konzipiert für das schnelle Bezahlen von Käufen bei ebay
  - auch über Länder- und Währungsgrenzen hinweg
- Käufer und Verkäufer müssen beide einen Account bei Paypal besitzen
  - damit haben Sie ein Paypal-Konto

PayPal® ein eBay Unternehmen

- Paypal ähnelt dem Überweisungssystem für Girokonten bei einer Bank
  - es ist jedoch zusätzlich eng mit ebay verknüpft
  - Überweisungen nach ebay-Transaktionen können halbautomatisch abgewickelt werden (ohne sep. Eingaben)

Paypal (2)

- 210 Mio. Mitglieder in 190 Ländern (Stand 2010)
- Vertragspartner für deutsche Benutzer ist *Paypal (Europe) Ltd.* in England
  - War anfangs als bank-ähnliche Institution registriert und der Finanzaufsicht unterworfen
  - Inzwischen (2007) eine echte Bank geworden
- Muttergesellschaft ist *Paypal Inc.* in Kalifornien

Paypal: Probleme

- Paypal ist weder für Verkäufer noch für Käufer anonym
  - weder gegenüber einander noch gegenüber Paypal
- Paypal erlangt ähnlich viel Informationen über Transaktionen wie eine Bank
  - (denen sind wir ja immerhin gewohnt zu vertrauen)
- allerdings potentiell angereichert mit Detailinformationen, die bei ebay hinterlegt sind
  - Artikelbeschreibungen (Gebote, Käufe, Verkäufe)
  - Gebote
  - Bewertungen
- Das anwendbare Datenschutzrecht ist eine Mischung aus dem deutschen, britischen, kalifornischen und US-amerikanischen
  - also nicht durchschaubar

Markttrend
bei elektronischen Bezahlsystemen

Freie Universität Berlin

Zur Zeit gibt es Tendenzen vor allem in zwei Richtungen:

- Zahlungen über Mittler, die den Abwicklungskomfort erhöhen und den Händlern abnehmen, eigene Systeme zu betreiben
  - z.B. PayPal
- Zahlung mit Hilfe des Mobiltelefons als Bediengerät
  - z.B. Paybox
  - Gleichermaßen für Web-Transaktionen und Transaktionen in der physischen Welt (Bargeldersatz) geeignet

- Anonymität ist in vielerlei Hinsicht nicht gegeben
- Echtes eGeld ist kaum gefragt:
  - Die Deutsche Bank hat ihr eCash-Angebot mangels Nachfrage wieder eingestellt
  - http://de.wikipedia.org/wiki/ECash

Fallbeispiele

Für Zusammenhang zw. Privatsphäre und Computerisierung

- Telefonieren
- Bilder von Personen in der Öffentlichkeit
- Abruf von Webseiten
  - Inhaltsdaten
  - Verkehrsdaten
- Elektronisches Bezahlen
- **Sozialversicherungsnummer**

Zusammenhang
Privatsphäre und Sicherheit

Freie Universität Berlin

- Selbst wenn man seine Privatsphäre nicht an sich wichtig fände, gäbe es Gründe, sie zu schützen

- Denn Wissen über eine Person kann benutzt werden, um dieser Schaden zuzufügen
  - Klarer Fall: Kenntnis von Zugangsgeheimnissen für Informationssysteme
    - z.B. Passwörter und PINs
  - Weniger klarer Fall: Kenntnis von eigentlich nichtgeheimen Informationen

Warnendes Beispiel: US-Sozialversicherungsnummer

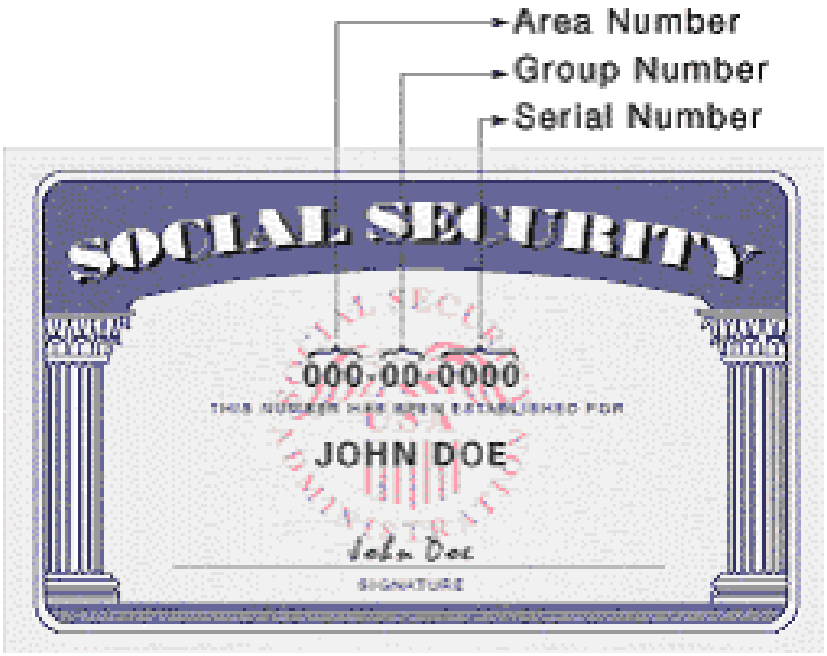
Freie Universität Berlin

- Die Sozialversicherungsnummer (Social Security Number, SSN) ist eine neunstellige Zahl, die einer Person zugeordnet wird
- Eingeführt 1935
  - zunächst ausschließlich zur Nutzung im Wohlfahrtsprogramm
- 1943: Roosevelt ordnet an, dass die SSN in allen neuen staatlichen Aktensystemen zu verwenden sei
- 1961: Die Finanzbehörden (IRS) verwenden die SSN als Identifikationsnummer für jede/n Steuerzahler/in
- 1976: Zahlreiche staatliche Stellen dürfen die SSN zur Identitätsprüfung verwenden
- seit den 1980er Jahren: Zahllose private Einrichtungen aller Art verlangen ebenfalls die SSN

Annahmen über die SSN

Die meisten Verwendungen vermuten die folgenden Eigenschaften für die SSN:

- Eindeutigkeit
  - "Es gibt keine zwei Personen mit derselben SSN"
- Universalität
  - "Jeder hat eine SSN"
- Identifikation
  - "Die SSN identifiziert eine Person eindeutig und zuverlässig"



SSN: Alles falsch!

Freie Universität Berlin

Keine dieser Eigenschaften ist für die SSN gegeben:

- Eindeutigkeit
  - Mehrfach wurden gleiche Nummern an verschiedene Personen ausgegeben – weil sie Name und Geburtsdatum gemein hatten!
- Universalität
  - Kleine Kinder und Organisationen haben keine SSN
- Identifikation
  - Angegebene SSN werden selten überprüft
  - Bis vor kurzem waren die SSN-Ausweise nicht fälschungssicher
  - Tippfehler führen meist zu gültigen SSN
    - keine Prüfziffer, wenig Lücken im Nummernbereich
  - SSN-Fehler können jahrelang unbemerkt bleiben

SSN: Es kommt noch schlimmer…

- Einige tausend Amerikaner haben jahrelang die selbe SSN 078-05-1120 benutzt
  - Diese war auf SSN-Ausweis-Dummies in Portemonaies abgedruckt, die in den 1940er und 1950er Jahren verkauft wurden
  - www.ssa.gov/history/ssn/misused.html

- Viele computerisierte Systeme verwenden die SSN als Passwort
  - z.B. die Kontoauskunftsterminals vieler Banken

SSN: Folgen

Freie Universität Berlin

- Aufgrund der weiten Verwendung der SSN kann man bei ihrer Kenntnis in USA sehr viele Information über einen Menschen bekommen:
  - Geburtsurkunde
  - Aktuelle Adresse
  - Telefonnummern (z.T. auch geheime)
  - Kreditwürdigkeit
  - Vorstrafen und Ordnungswidrigkeiten
  - Alimentzahlungen an Ex-Ehepartner und Kinder
  - etc.

- Mal ansehen (sehr beeindruckend):
  - http://www.net-vestigator.com/?hop=strange
  - *"Find out anything about anybody – without anyone knowing!"*

SSN: Folgen (2)

- Durch die Allgegenwart der SSN kommt es leicht zu Missbrauch:
  - absichtlich oder
  - versehentlich
- Zugleich kann dieser sehr schwerwiegende Folgen haben
  - z.B. Verlust der Kreditwürdigkeit
  - z.B. Verfälschung der Polizeiakten

Was ist das Problem?

Freie Universität Berlin

- Eine SSN ermöglicht einerseits den Zugang zu sehr vielen Informationen über eine Person
- Zugleich ist es schwierig, seine SSN geheim zu halten
- Das Problem kommt daher, dass die Aufgabe der SSN ohne Nachdenken über Privatheitsüberlegungen immer mehr erweitert wurde
  - Inzwischen haben aber Stellen,
    die unnötigerweise die SSN verlangen,
    erhebliche Akzeptanzprobleme bei *einigen* ihrer Kunden

...und in Deutschland?

- Das deutsche Gegenstück zur SSN ist die *Versicherungsnummer* (Rentenversicherungsnummer)
  - Sie kodiert das Geburtsdatum, das Geschlecht und den Anfangsbuchstaben des Geburtsnamens
  - z.B. 170493 P 528

- Die erlaubte Verwendung der Versicherungsnummer als Personenkennzeichen ist in Deutschland gesetzlich stark beschränkt
  - nicht einmal die Krankenversicherung darf sie benutzen
  - siehe http://de.wikipedia.org/wiki/Versicherungsnummer

Authentisierung zum Schutz der Privatsphäre

Freie Universität Berlin

- Oft kann die Identität einer Person nicht verborgen werden
- Dann muss Sie zum Schutz der Privatsphäre verlässlich und nachprüfbar offen gelegt werden

- Authentisierung:
  - Verfahren um festzustellen, dass jemand wirklich die Person ist, für die er/sie sich ausgibt.
    - z.B. Anmeldung mit Name und Passwort

- Warnendes Beispiel: Email-Spamming
  - Viele Spam-Emails haben als (vermeintlichen) Absender die Adressen von realen, aber völlig unbeteiligten Personen
  - Das ist für diese gefährlich, denn es kann ihren Ruf schädigen
    - z.B. sind manche der so beworbenen Aktiviäten in vielen Empfängerländern illegal

Zusammenfassung

Freie Universität Berlin

- Die Wahrung der Privatsphäre ist ein wichtiges Persönlichkeitsrecht
- Computerisierung verursacht eine große Zahl neuer Bedrohungen für die Privatsphäre
- Es gibt im Prinzip technische Wege, diesen Bedrohungen zu begegnen
  - Wenn auch teilweise recht aufwendig

Danke!