Gesellschaftliche Spannungsfelder der Informatik (187.237)

Mitschrift GSI2 2007-05-22

Vortragender: Peter Purgathofer

Zur Ergänzung s. Folien unter http://twoday.tuwien.ac.at/gsi2

eigene Kommentare sind kursiv geschrieben und schließen mit (Henry)
nach eigenem Ermessen hab ich wichtiges **fett marktiert**

by Henry78, mailto:henry78@gmx.at

Inhalt

Organisatorisch

Ablauf & Bewertung:

- Fehlersuche
  Fehler der letzten Fehlersuche: “Gorillas” statt “Menschen” im Text!

- Fragenwiki:
  Es wird fleißig dran gearbeitet.

- Übungsbeispiel:

Fotos zu “Digital Divide” (letzte Übung) werden vorgestellt. Näheres zur aktuellen Vorlesung im Laufe der Lesung

- Verteilte Aufbereitung von Inhalten:
  Ein Beispiel für eine Ausarbeitung wird als Orientierungshilfe online gestellt. Gewichtung? Wenn wirklich viel Arbeit „reingestellt“ wird: kein Abschlusstest nötig.

Kapitel 3 Privacy (Fortsetzung)

staatliche Angriffe (Fortsetzung)

Warum gibt es eine **Privatsphäre** gegenüber dem Staat? **Wie viel soll der Staat über uns wissen**? „Nur soviel wie der Staat zu wissen braucht.“ Diese Argumentation erfolgt aus einer sehr wissenden Position. Dazu muss man wissen, dass es zwischen dem was der Staat wissen muss, und dem was es zu wissen gibt eine Lücke klafft.

Biometrie

Für die Biometrie werden alle möglichen Merkmale zur Identifizierung herangezogen: Iris, Retina, Ohrmuschelform, Tippmuster, ...

> Dazu gibt es die unterschiedlichsten Probleme: Was passiert bei einer Ohrmuschelerkennung, wenn ich mein Handy herborge?

Die Frage die sich stellt: **Braucht man eine absolute Identifikation**, und ist eine bestimmte Identifikation überhaupt absolut?

Genetischer Fingerabdruck

Die Identifikation über genetischem Fingerabdruck basiert auf der Tatsache, dass **das Genom des Menschen einmalig** ist. *(Hinweis: in Deutschland schätzen Experten die Falsch-Positiv-Ergebnisse durch unsachgemäße Handhabung, falsche Beschriftung, etc. auf 1:100, Quelle: Wikipedia, Henry)*.

Es gab jedoch einen Fall, bei dem der genetische Fingerabdruck auf einen Gefängnisinsassen passte. Dieser saß während der Tat hinter Gittern. Konnte es also nicht gewesen sein. Ursache für dieses Paradoxon: Der Inhaftierte war Empfänger einer Knochenmarksspende, die seinen **genetischen Fingerabdruck veränderte**.

„Je sicherer eine Identifikation ist, desto sicherer müssen die Daten in zentralen Datenbanken geschützt sein.“

In Amerika müssen sich Sexualverbrecher „outen“ und stehen in öffentlichen Verzeichnissen. Als Sexualverbrecher verurteilt wird man in US aber auch, wenn man z.B. an Demonstrationen ohne Kleidung teilnimmt, oder „in die Ecke pinkelt“

elektronischer Reisepass

Angeblich fälschungssicher. Probleme: **Kommunikation** zwischen Pass und Lesegerät **kann** aus bis zu 6 Metern **mitgehört werden**. Es gelten die gleichen Probleme wie für alle Biometrie: z.B. haben 10% der

Menschen keine brauchbaren biometrischen Merkmale.

In Amerika gab es zur Sklavenzeit handgeschriebenen Ausweise für Sklaven, in welchem vermerkt war, wem sie gehörten oder ob sie etwa frei waren. Diejenigen Sklaven, die des Schreibens mächtig waren, konnten sich daher selbst „Freibriefe“ ausstellen.

2. Weltkrieg in Norwegen: Alle Juden wurden innerhalb von 3 Wochen zusammen getrieben, da Norwegen ein ausgeprägtes Passwesen hatte, und auch die Religionszugehörigkeit vermerkt war.

Also: **Wieviel soll der Staat über uns wissen?**

Private Angriffe auf die Privatsphäre

Profiling

Von Profiling spricht man, wenn es gelingt, D**aten über einen Menschen zusammen zu führen** (wobei die meisten Informationen bei den Banken liegen): Was isst er, wie ist der Gesunheitszustand, wohin geht der Urlaub ... -> **gläserner Mensch**. Der gläserne Mensch ist eine recht neue Erscheinung. Früher, so wie jetzt noch in ländlichen Gebieten und Dörfern, wusste jeder „alles“ über jeden anderen. Allerdings in sehr begrenztem Rahmen.

Google betreibt diese Datensuche intensiv.

Des gibt Stimmen die reklamieren: „Aber ich habe doch nichts zu verbergen“. Dies ist eine schwierige Geschichte, und führt über den Rahmen der Vorlesung hinaus.

Aber zu welchen (Fehl)schlüssen die Verknüpfung von Daten gelangen kann, musste Jeff Boz, der Chef von Amazon erleben. Als er das Profiling seiner Firma *(wer kennt nicht die Vorschläge von Amazon, was man sich denn noch alles kaufen sollte, Henry)* vorführen wollte, war der oberste Eintrag ein Film fragwürdigen Hintergrunds. Ursache war, dass er unlängst *(den fantastischen, Henry)* SF-Klassiker „Barbarella“ gekauft hatte.

Tivo *(PVR Sysytem für TV-Set-Top-Boxen, in USA sehr verbreitet, Henry)* erstellt Benutzerprofile und empfiehlt darauf basierend Sendungen. Dabei kommt es immer wieder zu Fehlentscheidungen: Schwule schwangere Männer oder jüdische Nazis. Eine Gegenstrategie ist, tivo sinnlos zu programmieren, damit kein konsistentes Benutzerprofil erstellt werden kann.

Cookies

...sind **Informationen, die eine Internetseite auf dem Rechner des Benutzers ablegt**. Im Prinzip harmlos, solange keine Sicherheitslücke das Abrufen der Cookies von fremden Sites oder gar Hackern ermöglicht. Google (weltweit der Größte), doubleclick *(im April 2007 von google gekauft, Henry)* **sammeln (auch) über cookies personenbezogene**

Informationen, um benutzerspezifische Werbung ein zu blenden.

Webbugs

Funktionsweise: **Ein 1 Pixel großes Bild** (in der selben Farbe wie der Hintergrund) wird (z.B.) in einem WordDokument gespeichert. Diese Bilder müssen beim Lesen **von einem Server nachgeladen** werden. Damit kann überprüft werden wie oft ein Dokument geöffnet wurde, bzw. wer ein bestimmtes Dokument öffnet. **HTML in e-mails vermeiden**! Automatisches **Laden von Bildern deaktivieren**!

Internet Mining

Die Amazon Wishlist ein ein nettes Service. Wird diese Liste allerdings mit einer Liste von „gefährlichen“ Büchern schneidet, bekommt man eine Liste von „subversiven“ Leuten. Eine solche Liste in goolge-maps dargestellt findet man (s. Folie 5:54)

Jemand hat es unlängst so formuliert: **Wenn ich die CIA oder NSA wäre, hätte ich google gegründet**. Das **Geschäftsmodell** von goolge ist es, **so viele Informationen wie möglich** über alle Individuen **zu sammeln**.

Ein Mordfall in den USA konnte aufgeklärt werden, da die Täterin in den Tagen davor nach Informationen zu Morden (u.ä., Waffen, Methoden, ...) im Internet gesucht hatte. (Diese Informationen wurde allerdings auf dem Computer der Userin entdeckt, und nicht von google preisgegeben!)

Es gibt Auswege: Aber wieso müssen wir die verwenden, ist es nicht egal, was wir privat Machen? **Wollen wir ein einem pseudomymisierten öffentlichen Raum leben?**

Spyware

- Windows Media Player schickt MS seit vielen Versionen Informationen über die gehörten Medien.
- Es existierte DRM Software, die bei jeder Verwendung den Rechteinhaber informierte.
- Große Diskussion in Deutschland über die „virtuelle Hausdurchsuchung“ *(Auch 'unser' Innenminister hat gestern mit der Idee eines östrreischischen 'Bundestrojaners' aufhorchen lassen, Henry)*

Spam

Herkunft: Sketch von Monty Pythons.

Warum bekommen wir soviel Spam? -> Es ist ein **Businessmodell!** 11% der Benutzer kaufen Produkte basierend auf Spam. 9% haben dabei schon Geld verloren. Ein wichtiger Punkt: **Mail kostet kein Geld!** Jeder Gewinn ist 'Rein'gewinn.

Wo bekommen die Spammer die e-mail Adressen?

- „**Ernte**“ von Adresse in Newsgroups, Foren, etc.
- „**Dictionary Attack**“: zu einer TLD werden übliche Namen durchprobiert (z.B. anton@xyz.com, berta@xyz.com, ...)

Schutzmaßnahmen:

- Adresse möglichst n**icht herumreichen**
- e-mail Adress im Internet nur '**verschlüsselt**': anton AT xyz DOT com reich oft schon aus. (s.a. Folie 5:64)
- mailinator (s. Folie)
- **komplizierte Adressen** bekommen weniger Spam

Van-Eck-Phreaking

Elektromagnetische Abstrahlung kann „**mitgehört**“ werden. z.B. Bildschirminhalt von Röhrenschirmen sogar durch Wände hindurch!

Das sind alles „Angriffsvektoren“ (Richtungen aus denen Angriffe kommen), **die größte Gefahr geht aber immer noch von Social Engineering aus.**

Spear Fishing

Gezielte Attacken, die sich social engineering, basieren auf Daten aus dem Internet, bedient.

Schutzmaßnahmen (ganz kurz)

- **gesetzlicher Schutz**: TKG von '97, Updates: 99, 2005
- **Privacy Policy:** Automatisierung: Ich stelle lokal ein, welchen Dingen ich zustimme, Software stimmt dies automatisch mit PPs die von Services (etc.) angeboten werden, ab. Hat sich nie durchgesetzt!
- **Kryptographie**: Klassische kryptographisches Problem: Es sind viele Schlüssel nötig. Lösung: Public-Key-Verfahren. Problem: Beim (initialen, also noch unverschlüsseltem) Austausch der Public Keys kann der richtige Abgefangen werden und durch einen (anderen) PK getauscht werden. So mit hat der „Man in the Middle“ Alle Schlüssel, und kann jede Kommunikation über diesen (vermeintlich sicheren) Kanal mithören.
  - Private Kryptographie ware den „mächtigen“ immer ein Dorn im Auge, da dann Private unbemerkt Informationen austauschen können.
    - Exportbeschränkung für Kryptographie in den USA
    - Verfolgung von Phil Zimmerman (PGP)
    - Clipper-Chip
    - DSS
    - Frankreich: Bis in die 90er Verbot von starker Kryptographie

- **Steganographie**: Die Farbcodierung eine Bildpunktes ist gegenüber den niedrigsten Bits sehr fehlertolerant (kaum zu sehen). So kann Information übertragen werden, ohne dass man weiß, dass Information ausgetauscht wird.
    - Bestes Kennzeichen einer optimalen Verschlüsselung: Es bleibt nur noch Rauschen.
- **Pseudonyme**: Ermöglichen die **Rechtssicherheit von persönlichen Daten** und offenbaren gleichzeitig **keinen Personenbezug**.
    - Aber: Wollen wir in einem pseudomymisierten öffentlichen Raum leben?
- Anonymes e-mail und surfen (remailer und Proxies)

Zum Abschluss des Kapitels wieder **Praxistipps** und „**die drei Thesen**“ (s. Folien 5:90ff)

Copyright/Copyleft

- Der Film Munich konnte an einem europäischen Wettbewerb nicht teilnehmen, da für NTSC verschlüsselt wurde.
- In den USA gibt es ein Patent auf „das Schauklen“ (mit einer (Kinder)schaukel).
- In Australien gab es ein Patent auf das Rad. Es wurde aberkannt, da nachgewiesen werden konnte, das es das Rad schon vorher gab (Prior Art)

Intellectual Property

Geschichte

Im **Mittelalter waren Ideen Allgemeingut** (keinerlei Schutz). Die Idee: Ein **zeitlich begrenzter Schutz, damit der Erfinder** bzw. der Autor **eine Zeit lang** alleine **davon profitieren kann**.

Dabei muss zwischen

Verwertungsrecht	↔	**Urheberrecht**
(übertragbar)		(nicht übertragbar)
Anglomamerikanisch		europäisch

unterschieden werden.

Es gibt einen alten Streit über den Wert von Patente zwischen Ingenieuren und Volkswirten.

- Ingenieure: Wir geben Erfindungen nicht mehr Preis, wenn wir kein Geld (Verwertung) dafür bekommen.
- Volkswirte: Patentrecht ist volkswirtschaftlich nicht gut.

In Holland gab es lang keine Patente, trotzdem ist Holland kein „rückständiger“ Staat.

Jede gesetzliche Regelung in diesem Bereich **hat die Funktion einer Waage**. Es muss ein **Ausgleich zwischen** den **Interessen der Autoren/Erfinder und der Öffentlichkeit** gefunden werden. So gibt es in diesen Bestimmungen **Schranken** (z.B. zeitliche Beschränkung, Beschränkungen im Bildungskontex, Bibliotheken, Privatkopie). **Schrankenbestimmungen sollen Ausgleich schaffen.**

Neue Technologien ermöglichen neue Umgangsweisen. Früher war man z.B. in der Lage Platten auf Kassetten zu überspielen. Musik konnte gehört werden, ohne die Platten zu besitzen -> Leerkassettenabgabe. Aber der Konflikt ist schon älter...

Pianola

Ein Pianola ist ein Klavier, dass Musik auf eine Art Lochstreifen prägt, und davon (automatisch) wieder abspielen kann. Jetzt kam man auf **die Idee**, **Noten auf viele Lochstreifen zu übertragen.** Damit vielen die Rechteinhaber um die **Einnahmen aus den Notenverkäufen** um.

John Philip Sousa klagt, bekommt aber nicht recht. Die solomonische Lösung des Gerichts: **Jeder darf eine Kopie herstellen** (für 2 ¢).

Diese Art von Konflikt hat sich immer wieder Wiederholt. Sowie beim Auftauchen des ersten Sony-Videorekorders. Sony wird von der Filmindustire verklagt, weil Sony „Raubkopien“ unterstützt. Da Supreme Court weist die Klage aber zurück, weil es genügend legitime Anwendungen gibt. W**enn sich der Markt verändert, habe sich die Filmindustrie darauf einzustellen!**