Gesellschaftliche Spannungsfelder der Informatik (187.237)

Mitschrift GSI2 2007-05-15

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 markiert**

by Henry78, mailto:henry78@gmx.at

Inhalt

Organisatorisch

Ablauf & Bewertung:

- Fehlersuche
  2 Punkte für den gefundenen Fehler aus der Folien zur dritten Vorlesung.
  Statistik:
  - 105 Fehler gemeldet
  - 34 richitg
  - 27 andere (1 Punkt)
  - 44 Nicht-Fehler (nochmals posten, wenn man der Meinung ist es handelt sich doch um einen Fehler, durch das posten wird der gemeldete Fehler nochmals evaluiert)

  ! Zur richtigen Aufgabe posten !

- Fragenwiki:
  Bis jetzt sind über 4 Fragen eingepflegt - Wow!

- Übungsbeispiel:
  Auch heute wieder. Abwicklung wie gewohnt über die Arbeitsmappe. Beispiele für die 1. Übungsaufgabe werden von

Peter kurz gezeigt.

- Verteilte Aufbereitung von Inhalten: Mehr dazu während der VO
- koll. Mitschrift: auch heute wieder mit dem Texteditor „gobby“. Wieso wurde die letzte Mitschrift im Wiki nicht bearbeitet?

Kapitel 2 Verletzlichkeit der Informationsgesellschaft (Fortsetzung)

Gefährdungen und Schäden

Ursachen: systemische Bedingungen

14.10.1978: **Internationaler Börsencrash**. Warum? Kleine Händler orientieren sich an institutionellen Anlegern (große Kapitalgesellschaften in den USA). Letztere verwendeten vielfach **Software um auf Aktienkurse zu reagieren**. Kommen diese Softwaresyteme zu einem Trugschluss, auf grund der hohen Komplexität und falschen Marktmodellen (bzw. vorprogrammierten Kurskriterien) reagieren sie falsch. Nun lagen aber den meisten Systemen **die gleichen Modelle** zu Grunde und alle handelten gleich (falsch). Da die kleinen Händler diesem Muster folgten kam es zu dem Crash (dieser Ablauf wurde im Nachhinein rekonstruiert).
Eine Folge dessen: **heute schließt die Börse**, wen gewisse Kennziffern zu sehr absinken -> Handel wird eingestellt.

Der **IPv6 Protokoll bietet** (fast) **beliebig viele IP Adressen** (mehrere IP-Adressen pro m^2). Dies ermöglicht einen Anschluss von beliebig vielen Geräten. So plant z.B. Sony in Zukunft alle Produte mit einer IP-Adress auszustatten. Auch „Visionen“ wie das vollständig vernetzte Hause („intelligent house“) weisen in diese Richtung.
Damit steigt aber auch **die Gefahr für Angriffe**. Kann man z.B. seine Badewanne aus der U-Bahn einlaufen lassen, besteht auch die Möglichkeit, dass jemand eine Sicherheitslücke ausnützt, und das ebenfalls kann.
Wir wissen mittlerweile, dass Computer anfällig sind. **Dass Kühlschränke etc. auch betroffen sein können**, ist bei den Benutzern allerdings **nicht im Denken verankert**. Handys konnten früher nicht abstürzen, heute schon!

E-voting
Bei den letzten Wahlen in den USA gab es viele t**echnische Probleme**. Viele **politische und wirtschaftliche Verstrickungen** (Vorsitzender von Diebold ist ein erklärter Unterstützer der Republikaner, und auch im Vorstand des zweiten großen Wahlmaschinenherstellers) **führte zu vielen Verschwörungstheorien**, da die Ergebnisse der Wahl nicht nachvollziehbar sind.
Diebold Wahlmachinen konnten **mit einem Hotel-Mini-Bar-Schlüssel geöffnet** werden. Es entkam auch SourceCode ins Internet, und wurde von Avi Rubin von der John Hopkins analysiert. Diese Sicherheitsanalyse ergab schwere Sicherheitsmängel, wie einen **fest gecodeten DSA-Key** (DSA gilt seit 1997 als unsicher). Mit diesem Key war es möglich, alle Dieboldmachinen (da alle die gleiche Software verwendeten) zu beeinflussen. Da auch das **Auditlog nur ungenügend geschützt** war, konnte Software, die Wahlen manipuliert eingesetzt werden, ohne daß Spuren hinterlassen werden.

Eine (Demo)software („Vote stealing“) wurde geschrieben, die sich automatisch von einer auf andere auf Wahlmaschinen kopieren ließ, und **beliebig die Wahlen fälschen** könnte. Was für solche Angriffe noch fehlt ist **der physikalische Zugang** zu den Geräten. Der Umgang mit den Wahlmaschinen ist aber erwiesener Maßen **äußerst lasch**. So „stolperte“ Ed Felten (einer der Autoren der „Vote stealing“ Software) auf seinem Arbeitsweg über unbewachte Wahlmaschinen, die für die nächste Wahl angeliefert wurden. In Deutschland wurden laut CCC Wahlgeräte **oft nur vom Hausmeister „bewacht“**.
Das Wichtige ist aber nicht die Wahl-Software, sondern **die Wahl-Prozedur**, die immer **einfach, kontrollierbar** war und die Wahrung der staatsbürgerlichen Pflichten ermöglichte. Bei Wahlmaschinen ist k**eine Kontrolle mehr möglich**. Die Folge ist, dass **das Vertrauen in e-voting fehlt**.
Folgen:

- Italien stoppt den Einsatz von Wahlcomputern. Vorwurf an sforza Italia: 1 Million Leerstimmen wurden der sforza zugeschlagen.
- Californien verbietet den Einsatz von Diebold Geräten

Ursachen: mangelndes Sicherheitsbewusstsein

Kurzvortrag über Sicherheitsrisiken beim m-Payment von Constantin Hofstetter (hier nicht Niedergeschrieben – darf ich das? Wenn mit Peter geklärt, kann ich das gerne nachliefern, ist lokal vorhanden, Henry):

Firmen sparen an der Sicherheit und Sicherheit schränkt Komfort ein. Wenn der Komfort sinkt, sinkt aber auch die Anzahl der Kunden, die das Produkt verwenden. Dadurch wird das Produkt irgendwann uninteressant.

In Thailand waren 2001 hunderte Kopien von XP (vor dem Launch!) im Umlauf. Bruce Schneider: (...) Users prefer cool Features to security (...). Vor wenigen Wochen gab es einen 0-Day-Exploit für Mouse-Cursors auf Webseiten. MS wußte seit Dezeber davon, hat aber erst jetzt einen Patch (außerhalb des Patchday) veröffentlicht.

Sicherheit vs. Freiheit

Wollen wir **Offenheit oder Sicherheit**? Bombenbauanleitungen im Netz, Seiten zu billigen Lokalen zum Koma-Saufen im Netz, ...

In Deutschland verwenden Nachrichtendienste malware auf Rechnern von Verdächtigen, um ihn auszuspionieren. Das ist natürlich verfassungstechnisch sehr bedenklich. In Deutschland soll daher die Verfassung geändert werden. Ist das nötig?

Attacken auf Atomkraftwerke können immense Schäden anrichten.

Dadurch entsteht ein „Sicherheitszwang“.

Aber **ist eine gesicherte Gesellschaft eine sichere Gesellschaft**?

Fahrradhelme: Das Tragen von Fahrradhelmen führt dazu, dass Radfahrer riskanter fahren, und Autos knapper überholen. Studien in Kanada und Neuseeland (Helmzwang), zeigen, dass Fahradhelme die Anzahl der Kopfverletzungen nicht verringern.

Im Moment ist unklar, ob die Waage in Richtung Freiheit oder verstärkter Sicherheit im Internet ausschlägt.

Bruce Schneider initiiert 2006 den **Movie-Plot Threat Contest**. (*Als Movie-Plot Threats werden Ängste von spezifischen Attacken bezeichnet, die speziell und unwahrscheinlich sind. So wurden z.B. spitze Gegenstände in Flugzeugen verboten, da die 9/11 Attentäter diese benutzten, um die Flugzeuge zu entführen. Oder es wurden nach dem Bombenattentat von Richard Reid Schuhe kontrolliert. Diese Sicherheitsmaßnahmen sind aber nur für die spezifischen Attacken sinnvoll, und solange Schuhe kontrolliert, und spitze Gegenstände konfisziert werden, wird der nächste Angriff auf einem anderen Weg erfolgen. Also rief Schneider zu einem Wettbewerb auf, um möglichst unwahrscheinliche, aber mögliche Terorristenangriffe zu beschreiben. Eine Liste ist unter http://cockeyed.com/citizen/terror/plans/terrorwatch.html vefügbar, Henry).* **Ergebnis** des Contest waren hunderte von Movie-Plots, die insgesamt **195 Seiten Text** ergeben. Fazit: **Es gibt immer noch eine Sicherheits-Schwachstelle!**

Key-Bumping: Eine **äußerst einfach Möglichkeit**, **alle Sicherheitsschlösser** (bis auf ein österreichisches Produkt) **zu knacken**, und keine (oder kaum) Spuren zu hinterlassen! (Wie macht man so etwas seiner Versicherung klar?)

Roßnagel schlägt **10 Prinzipien** vor. Folgen wir diesen, verlassen wir uns nicht auf eine „monotithische“ Sicherheit, sondern versuchen Sicherheit systematisch zu erreichen:

1. Statt Verhinderung von Mißbrauch: **Folgen reduzieren, Schäden minimieren**
2. Statt Automatisierung und Übernahme von Aufgaben: **Technik als Unterstützung, menschliches Zusammenwirken als Grundlage**
3. Statt Monopolen: **Alternativen erhalten**, Vielfalt **sichern**
4. Statt vollkommenen Verlass auf eine Lösung: **Redundanzen schaffen**.
5. Statt vollkommener Abhängigkeit von einem Hersteller: **zeitliche, räumlich, technische und organisatorische Vielfalt**
6. Statt Zentralisierung: **entkoppelte, transparente und dezentrale Lösungen**
7. Statt Totalausfall: **stabiler Zustand bei teilweisem** oder ganzem **Versagen**.
8. Statt Überraschunge: **Systematische Notfallplanung** (äußerst

schwer!)
9. Statt Fremdbestimmung: **Gestaltung der Technik** und der Sicherheitssysteme **mit Zustimmung der Betroffenen** und der Öffentlichkeit
10. **Verzicht auf ökonomischen Vorteil** und Komfortgewinn, wenn das Schadenspotential hoch ist

Praxistipps:
- Verzichten Sie auf Internetexplorer & Outlook!
- Verlassen Sie sich nicht auf nur ein Betriebssystem!
- Backups! Backups! Backups!
- Schalten Sie zweifelhafte Features sofort ab!
- Immer für all (mehrere) Browser probrammieren!
- Sichere Verbindungen (VPN) nutzen!
- Kein HTML-Mail nutzen!
- Firewall & Monitoring

3 Thesen (stehen am Ende jede Kapitels):
- Schäden durch Malware werden weiter zunehmen und auch durch drakonische Strafen nicht einzudämmen sein
- In punkto Security Management sind das Bewusstsein und die Praxis von Usern, vor allem aber von Herstellern unter aller Sau.
- Durch eine bessere Entwicklungspraxis ließen sich manche Schäden vermeiden, aber die inhärente Komplexität der Informationsgesellschaft macht sie notwendigerweise verletzlich.

Kapitel 3 Privacy

Was ist Privatsphäre?

Die Idee der **Privatsphäre** ist **nicht so alt**, wie man glauben wollte. **Ludwig der XIV hatte keine Privatsphäre**. Er hatte Audienzen währen er sich ankleiden ließ. Es gab sogar eine eigene Audienz, deren größtes Glück es war, dem Sonnenkönig der Allerwertesten abwischen zu dürfen.
Privatsphäre **kommt erst mit der technischen Entwicklung auf**. Nämlich mit der der des **Fotoapparats**.
Warren & Brandeis schreiben „**The right to privacy**“, worin sie darlegen, dass die Verletzung der Persönlichkeitsrechte durch Fotos schlimmer sein kann, als physische Gewalt. „Right to be left alone“
Jahre später (1967) findet sich (fast) dieselbe Definition, nur prokativ, bei Westin („Privacy and Freedom“). Und bis heute finden sich die Begriffe „Right to be let alone“ bzw. „informationelle Selbstbestimmung“ im Zusammenhang mit Privatsphäre.
Informationelle Selbstbestimmung finden wir sowohl im deutschen, als auch im österreichischen Datenschutzgesetz. Dabei schließt das österreichische Datenschutzgesetz Daten aus, die aufgrund „mangelnder Rückführbarkeit auf den Betroffenen“ oder „infolge ihrer allgemeinen Verfügbarkeit“ nicht als schützenswert erscheinen, z.B. Adressdaten, da sie im Telefonbuch stehen (allg. verfügbar). Das Recht hat verfassungsrang, ist Menschenrecht (gilt alle, auch nicht österreichische Staatsbürger) und ist ein Recht mit Drittwirkung (d.h. Es gilt auch im privaten Bereich).

Staatliche Angriffe auf die Privatsphäre

Dem Staat war die Unverletzlichkeit der Privatsphäre nie „recht“, so gab es **immer Versuche, die Kommunikation der Bürger einzuschränken**. In Diktaturen ist es üblich, in die Privatsphäre ein zu dringen. In Demokratien ist es „eher unüblich“. Neue Technologien wecken dabei alte die Begehrlichkeiten.

In Frankreich (ab 1791) gab es den „**Tachygraphen**“ zwischen Paris und Lille. Eine Übertragungstechnik, die ähnlich wie Flaggensignale arbeitet (s. Folie). Auf einem Turm gab einer das Signal weiter, das ihm der andere (mit einem Fernglas ausgestattet) ansagte. Um Missbrauch zu verhindern, waren die ersten Stationen bewacht, weiter im Land liegende aber nicht mehr. Dies wurde auch missbraucht, in dem die Übermittler bestochen wurden, falsche oder zusätzliche Nachrichten zu übertragen *(wenn ich mich recht erinnere wurde die Niederlage Napoleons für spektakuläre Börsengewinne genutzt, Henry) (In „Der Graf von Monte Christo“ wird solch ein Mißbrauch geschildert, Henry)*. Aufgrund dieses Mißbrauchs wurde **in Frankreich ein Gesetz erlassen, daß die private Kryptographie verbietet**. Dieses Gesetzt bleibt bis 1999 in Kraft.

In den USA ist **Kryptographie gleichgestellt mit Munition**, d.h. Es besteht ein **Exportverbot**. Die USA versuchte auch mit dem **Clipper Chip** die **Verschlüsselung in staatliche Hände** zu bekommen. Dabei sollte es für jeden verbauten Chip einen Schlüssel geben der hinterlegt wird und mit dem die Exekutive (Regierung?) sämtliche verschlüsselten Daten entschlüsseln kann.

Es gibt Individuen und Institutionen in der Gesellschaft, die von „berufswegen" paranoid sein müssen. Durch neue **technische Möglichkeiten** entstehen auch immer **neue Begehrlichkeiten** (so wie die Datenspeicherung bei Providern), und zu einer Vermischung der verschiedensten Dienste (Polizei, Geheimdienste, Militär).

Ausgelöst durch 9/11 ist es sehr leicht geworden, solche Dinge um zu setzten. „**Patriot Act**" in den US, **biometrische Daten in EU-Reisepässen**. Nach 2001 wurden in den USA viel mehr Dinge als zuvor als terroristischer Akt definiert. Die Anklagen und Verurteilungen sind eklatant gestiegen, die durchschnittliche Haftdauer ist aber stark gesunken, da die Gesetzte nun auch auf vollkommen unterroristische Verbrechen eingesetzt wurden (z.B. Glücksspiel).

Es gibt weltweit eine Reihe von technischen Sytemen, um zu überwachen. Z.B. „**echelon**": **Abhören von Satellitenkommunikation**, entstanden aus einem Abkommen zwischen den USA und GB, ausserdem nehmen Neuseeland, Australien und Kanada teil. Ehemalige US-Militärs und Geheimdienstleute (CIA-Chef James Woolsey)geben zu, ausländische (Frankreich) **Industriegeheimnisse**, die über echelon **abgehört** werden, an US-Unternehmen weitergegeben zu haben.

Überwachungskameras

Ein ganz alltägliche Bedrohung sind Überwachungskameras. 2001 gab es in Wien **mehr als 200 000 Überwachungskameras** in Wien. Jeder wird mehr als hundert Mal pro Tag aufgenommen.

Was bringen sie? **Befürworter behaupten**, die **Kriminalität sinkt** „nur weil jemand zuschaut", die Angst der Bürger sinkt.
CCTV (Überwachung in London) und ähnliche Dienste werden (weltweit) von privaten Firmen betrieben. Um das **Vorhandensein** dieser Kameras **zu rechtfertigen**, und das eigene Geschäft zu schützen, werden hauptsächlich **„kleine Delikte" gemeldet**: Urinieren, Mist wegwerfen, Gehsteigparken, ... Jede neue Meldung unterstützt das Argument für das CCTV System.
Eine Studie hat aber ergeben, dass eine Überwachung nur auf Parkplätzen die Kriminalität verringert hat. Damit Kameras Parkplätze überwachen könne, müssen diese ausgeleuchtet werden. So bleibt die Frage, ob die Kameras ober das Licht Verbrechen verhindern. Eine andere Studie stellt fest, dass **die Kameras keinen Einfluss auf die Zahl schwerer Delikte (Gewaltverbrechen) haben**.
Probleme:

- keine Überwacher der Überwacher (Vorurteile, so kann z.B. Rassismus

ausgelebt werden)
- Mißbrauch:
  - Verkauf der Aufzeichnungen an private („Dümmste Einbrecher (...) der Welt“). Ohne Einverständnis der Dargestellten -> illegal!
  - „Unwanted Category of People“ (z.B. Sandler) werden Zielscheibe
- Unklar, wessen Interssen verfolgt werden
- Nachlassende Wirkung: 12-18 Monate nach der Einführung tritt ein Gewöhnungseffekt auf
- Verdrängung in benachbarte, nicht überwachte Gebiete
- Normierender Einfluß auf das Verhalten.
  Beispiel: Jemand filmt in der Vorlesung mit -> das Verhalten ändert sich. Jeder versucht wie ein „Wanted Category of People“ zu sein.
- alternative, vielleicht bessere Systeme werden verdrängt: mehr Licht, mehr Personal, ...

Für New York gibt es ein System, das einen weg mit „geringster Kameradichte“ errechnet.

Hierzu auch die **dritte Aufgabe**: Finden und fotografieren Sie Kameras im ersten Bezirk (Details siehe Arbeitsmappe!)

Die Geschichte ist aber nicht ganz so einseitig, wie bisher dargestellt: KH Grasser und Fiona wurden von privaten Touristen fotografiert, und die beiden posierten sogar für sie. Aber als die Bilder dann an die Presse gelangten, war das nicht mehr so easy.
In Anderson County wurde die sog Jailcam (Kameras im Gefängnis) aufgrund von Sicherheitsrisiken (Ausbrüche planen) abgeschaltet.
Die Allgegenwart von Kameras, wer hat kein Handy mit Kamera? *(um mich herum zeigen alle auf, ich brauche ein neues Handy!, Henry)* lässt eine **Gegenöffentlichkeit** entstehen. Eine „**Bottom-Up-Überwachung**“ wird möglich, so wie auch im Fall Rodney King.

Visionen zur Überwachung
Es gibt wie immer Visionen, die über den normalen Rahmen hinausgehen. **Roboterkameras, die die Polizei verständigen**, wenn jemand ein **verdächtiges Verhaltensmuster** zeigt. Was passiert, wenn diese Leute dann gar kein Verbrechen begehen? (s. Minority Report)
De-Fakto bedeutet das eine **Umkehr der Unschuldsvermutung**, welche die bedeutendste Grundlage der Rechtssaatlichkeit ist. Tatsächlich ist dies aber nicht neu: Herlod (deutsches BKA) hatte schon 1984 die Idee künftige Straftaten zu verhindern, in dem Stimme und Bild in Bankcomputern gespeichert werden. John Ashcroft (Ex-US-Justizminister): Zum Verhindern von Verbrechen ist es nötig Daten im vornherein zu speichern und zu analysieren. (-> Umkehr der Unschuldsvermutung).
Wie die Interpretation vorhandener Daten ausfällt, ist aber fragwürdig. z.B. wird nach den Bombenanschlägen in London (solche Dinge passieren gerne im Zusammenhang mit Terror) ein Elektriker von der Polizei erschossen, da sie aus den Daten falsche Schlüsse gezogen hat. Jegliche Interpretation von Daten (so wie Analysen von Verhaltensmustern) kann nicht objetiv sein! Was passiert mit jemandem, der dringen aufs Klo muss, voher aber noch Geld abhebt, und daher Verhaltensmuster wie ein Bankräuber an den Tag legt?

Biometrie
Security Now Podcast: jede Menge Information zu Authentifizierung.

Der übliche „Spruch“ für „sichere“ Authentifizierung: „**Something you know, something you are, something you have**“.
Biometrie ist immer schwierig: Es gibt **Menschen**, die von Biometrie nicht erfasst werden können, da die **biometrischen Merkmale nicht stark genug ausgeprägt** sind. Dies sind vor allem Frauen. Studien zu Biometrieverfahren, die vorwiegende Männer als Testpersonen haben, sollte mit Mißtrauen begegnet werden, das System könnte Probleme mit Frauen haben. Aber es haben auch ca. 4% der Bevölkerung keine (brauchbaren) Fingerabdrücke. Vor allem bei älteren Menschen verschwinden die Fingerabdrücke, und Bauarbeiter haben auch oft keine.

Biometrische Identität ist auch „Subject of Faking“. So gibt es ein Projekt des CCC, welches zeigt, dass auf **einfache Weise Fingerabdrücke gefälscht** werden können. Andere Frage: Wie lange funktioniert ein Auge, das nicht mehr im Körper ist? Laut CCC: 10 min.

Es entstehen immer wieder seltsame Begehrlichkeiten, vorhandene Daten für andere Zwecke zu verwenden. So gibt es in Deutschland den Versuch auf die Daten der Mauterfassung zu zugreifen. In Österreich werden die Section Control Strecken mit Glasfasser ausgestattet (Breitband). Wozu? Die Strafmandate können auch ohne große Datenmengen übertragen werden.