Gesellschaftliche Spannungsfelder der Informatik (187.237)

Mitschrift GSI2 2007-05-08

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 (2. VO) fand sich in Folie 2:144 ein Bild von Tim Taylor stand anstelle eine Bildes von Barlow

- Fragenwiki:
  Bis jetzt sind über 25 Fragen eingepflegt, die Richtung stimmt! Es wäre allerdings eine Schande, wenn genau bei 100 Fragen aufgehört wird, und keine neuen Fragen mehr eingepflegt werden.

- Übungsbeispiel:
  Das Beispiel ist diese Woche leicht, näheres dazu im Laufe der VO.
  Bewertung über Arbeitsmappe

Kapitel 2 (Fortsetzung)

Verletzlichkeit der Informationsgesellschaft

Vernetzung

Jede Lösung, egal ob “dummes” oder “intelligentes” Netz hat seine eigenen Einflüsse auf die Informationsgesellschaft.
Die Bush Administration *(besser: Bush Regierung, wieso das immer so schlecht übersetzt wird, ist mir ein Rätlsel, Henry)* setzt nach 9-11 eine “**National Strategy to secure Cyberspace**” fest. Solche Einflußnahmen sind im Endeffekt **gegen den Konsumenten**. Ein höherer Level an Sicherheit schränkt freie Kommunikation & Infrastruktur ein, und ist Hinderlich für Innovation. Hinter der Zuwendung zu intelligenten Netzen stehen auch viele Firmen, wie z.B. **US-Telcos**, Content-Provider, ... Der Nutzen ist auf Seite der Big Player, die bei den Entscheidungen mitreden können.
Bevor wir uns mit dem Streit über **die Zukunft der Netneutrality** beschäftigen schauen wir uns an, wie das Internet z.Z. Organisiert wird:

Wer kontrolliert das Internet?

Technische & organisatorische Grundlage für das Internet bilden 13 'r**oot-server**'. Zehn in den USA, zwei in Euroa und einer in Japan. Server A und J (beide US) halte alle Information, die anderen Server müssen sich innert 24 Stunden syncen. Es gab unlängst eine massive DDoS (darüber später mehr) Attacke auf die root-server in einem bis dato unbekanntem Ausmaß.
Betreiber ist **VeriSign**, Koordinator **ICANN**, eine Non-Profit-Organisation. Letzere vergibt Domains, welce von den root-servern in IP-Adressen umgesetzt werden. An der Spitze der Hierarchie stehen die TLD (Top-Level-Domains), wie .com, .net., .biz, .info, .at, .us, .eu, ...
Die ICANN ist kompliziert aufgebaut, und steht unter starkem politischem Einfluß, vorallem dem **Handelsministerium der Vereinigten Staaten** (Deparment of Commerce). So kommt es immer wieder zu Konflikten da verschiedene Wünsche und Bedürfnisse auf einander treffen. Diese Konflikte bestehen auch bezüglich der TLDs. So existiert z.B. eine TLD für Katalonien *(in der Vorlesung nicht erwäht: .ca ist eine gesponsorte Domain und keine länderspzeifische Domain, Henry)*, aber nicht für Tibet. Diese **Interessenskonflikte** sind auch immer wieder Grundlage für Mißbrauch. So ließ VeriSign alle Anfragen an nicht existierende Domains auf eine eigene Webseite weiterleiten.
Als Lösung für diese Probleme wurde vorgeschlagen, die **Kontrolle über die ICANN** der UNO zu übertragen. Die **UNO lehnte ab**, die USA erklärte, daß sie sie Kontrolle nicht aus der Hand geben wolle, und die EU sprach sich für mehr internationale Kontrolle aus. Dazu wurde 2005 ein “World summit on the information society” ausgerichtet. Ergebnisse:

- **Internet Governance Forum** der UN wird eingerichtet, mit dem

Ziel allen gleiches Recht zu bieten
- **Souveränität nationaler Strukturen** wird festgestellt: So kann China unbeliebte Seiten ausblenden, sowie auch Argentinien (?) keinen youtube Zugang zulässt.
- Es wird anerkannt (nach dem Microsoft es nicht schaffte, diesen Punkt aus der Erklärung heraus zu reklamieren), daß **der Wert des Internets an dessen "Rändern" liegt**

Es gibt schon länger **alternative TLD-Strukturen**: OpenNIC, AlterNIC, ... Verwendet man einen alternativen root-server, sieht man eine anderes Internet. Dabei gibt es auch Probleme: Es sind nicht alle Server in allen TLD-Strukturen eingetragen, daher nicht erreichbar. Oder sie sind nicht gleich eingtragen: so kann es zu Kollisionen kommen. Ausserdem werden die alternativen TLD von google ignoriert. Und heutzutage ist nur noch Internet was von google indiziert wird.

Wie international ist das Internet?

Der Zugang zum Internet ist stark länder-, alters- und schichtenspezifisch (3. Welt). Der "**digital divide**" trennt die jenigen die Zugang zum Internt haben, vom Rest. Dadurch wird eine neue Ungerechtigkeit geschaffen.

Übungsaufgabe 2:

Bild (Foto) zu "digital divide" *(Details im VO-Blog, Henry)*

Lösungsansätze für den digital divide:
Der indische **Simputer**, der tragbar, energiesparend, hitzebeständig, billig und auch für Analphabeten verwendbar sein soll. Letzteres sollen ein einfaches Interface und Sprachausgabe in verschiedenen indischen Sprachen garantieren.
Ein anderer Ansatz ist das **OLPC Projekt** von Nicholas Negroponte *(MIT Media Lab, Henry)*, mit dem Ziel ein Gerät zu bauen, daß um $ 100 produziert werden kann. Das Gerät soll aber nicht auf dem freien Markt kommen, sondern von Regierungen (der 3. Welt) direkt an Kinder verteilt werden. **An diesem Projekt wird aber auch Kritik geübt**, z.B. sollte statt der Shared Interntaccess (Internetcafes) gefördert werden, was wesentlich besser dazu beitragen würde, den digital divide zu schmälern.

Es stellt sich in **Schwellen- und 3. Welt Ländern** auch die Frage, ob man sich **von einer Firma abhängig** macht. So orientieren sie sich vertärkt an **open-source**. Die betrifft aber nicht nur Schwellenländer, sondern auch US-Bundesstaaten wie Ohio, aber auch München oder Wien.

Monopolisierung & Gegebewegungen

John **Sherman** bringt 1890 ein Gesetz “durch”,das verhindern soll, dass der freie Markt mißbraucht wird (Preisabsprachen, Monopole, ...)

Schäden durch Monopole: Zerstärung der Konkurrenz, Preisabsprachen, Verhinderung von Innovation

Strategien von Monopolisten:

- Erpressung
- Embrace & Change (z.B. übernehmen von freien Standards, die dann angeändert werden, und duch den hohen Marktanteil des Monopolisten wird dann ein neuer, nicht mehr freier Standard geschaffen, z.B.: Java, HTML, ...)
- Leverage (Aushebeln: andere Tecnologien oder Programme werden mittels der Markmacht ausgehebelt. z.B: Internet Explorer <-> Netscape, ...)
- Verdrängung (Entwicklung von eigenen Produkten, freme werden nicht unterstützt)
- Behinderung (z.B. Fotohersteller bekommen keine Schnitstellendaten)
- FUD (Fear, uncertainty and doubt) (es werden Massive Fehlinformationen publiziert, Falschinterpretationen gelifert, Vaporware,...)

Um dies zu Verhindern, gibt es in den USA **Anti-Trust-Verfahren**.

1969 Lyndon B. Johnson vs. IBM
: IBM hät damals ca. 75% der Computermarktes. Das Verfahren wird unter Reagan eingestellt, da sich diese Situation stark Verändert hat

1974 Gerlad Ford vs. AT&T
: AT&T ist damals alleiniger Betreiber des US-Telefonnetzes. AT&T wird 10 Jahre später zerschlagen, wodurch Telefonieren viel umständlicher wurde (spzielle Vorwahlen waren nötig, je nachdem wohin mal telefonierte), Jahre später wurde AT&T mächtiger als je zuvor

1998 Bill Clinton vs. Mircosoft
: Mit diesem Verfahren werden wir uns im Detail auseinandersetzten

Anklagepunkte:

- Netscape (Leverage): Microsoft verdrängt Netscape, nach dem Netscape es ablehnte den Markt aufzuteilen.
- Java (Embrace & Change)
- Multimedia (quicktime & realplayer): Nachdem der Vorschlag den Markt zwischen Apple und PC aufzuteilen, versucht MS die fremden Multimedia-Produkte zu verdrängen
- Druck auf Hardwarehersteller, damit diese nicht die Intel Signal Processint Library mit ausliefern
- Lotus Notes: Druck auf IBM, damit Lotus Notes nicht mehr auf Apple weiterentwickelt wird.

“Cross platform APIs werden von MS als Bedrohung angesehen”

Rechtfertigung für viele dieser Dinge war “**maximizing the Shareholdervlue**” (wozu Unternehmen in den USA gesetzlich verpflichtet sind). Das ganze mündete in einem “**Findings of Facts**” Dokument von Richter Thomas Penfield, in dem klar festgestellt wird, daß MS seine Monopolsituation ausnützt. Bemerkenswert ist der (letzte?) Punkt 412 (s. Folie), der auch feststellt, **dass MS Innovation verhindert**.
MS wird zur **Zerschlagung in zwei Unternehmen** (OS, Applikationen) verurteilt. Microsoft legt **Berufung** ein. Ab 2001 regiert Bush, der einen neuen Richter für das Berufungsverfahren einsetzt. Ergebnis der Berufung war nur eine “Vorschrift für zukünfiges Verhalten”, Offenlegung der APIs, Verpflichtung zu einheitlichen Lizenzbedingungen, Verpflichtung zur Offenlegung von kommunikations Protokollen. Letzer Punkt gilt nicht für sicheheitsrelevante Protokolle, wobei zu bemerken ist, daß sicherheitsrelevanz sehr großzügig ausgelegt werden kann.
Ist das Ergebnis gut oder schlecht? Der Aktienkurs macht nach dem Urteil einen Sprung nach oben, Zivilklagen (SUN) sind folgen, ein (millardenschwere) EU Klage ist anhängig. Andererseits führt MS eine “offenes” Dateiformat (ist das wirklich offen? Oder nur eine Finte von MS?) ein und startet ein Shared Source Programm.

Gegenkulturen

Community Networks, lokale wireless Networks. So gibt es in Wien immer mehr Lokale die gratis WLAN anbieten.
Open-Source: interessant ist dabei, wie man mit OSS Geld verdienen kann (dazu später mehr). Im Halloween Dokument stellt MS fest, dass OSS auf Entwickler einen spziellen Reiz hat, der mit MS-Lizenzen nicht generiert werden kann. Zudem “denkt” MS über embrace & change “nach”. Protokolle integrieren, verändern, zum Quasi-Standard erheben. FUD von MS, das damit OSS Befürworter einschüchtern möchte. MS erkennt aber gleichzeitig, dass FUD gegen OSS nicht eingesetzt werden kann, da es glaubwürdiger ist.
Peer-to-Peer: ursprünglich war die Idee, die Last von einem Server zu nehmen und zu verteilen.
“**Gegenöffentlichkeiten**”: der Versuch Gegenpositionen zur Industrie zu beziehen.

Gefährdungen & Schäden

... die erst durch die Informationsgesellschaft entstanden sind.
Am 12. Dezember 1986 **fällt ARPANET in Neu England aus**, weil ein Bagger 7 gemeinsam vergrabenen Leitungen kappt. Pikanterweise sollen die 7 Leitungen eigentlich der Redundanz (Ausfallsicherheit) dienen, da sie aber gemeinsam vergraben wurden ... Ein Bagger war auch im

November 1989 an 150 000 ausgefallenenn Telefonanschlüssen in Chicago schuld. Beim Pflanzen von Bäumen wird eine Hauptverbindung durchtrennt.
Der “**Code Red**” Wurm breitet sich aber dem 13. Juli 2001 aus, in dem er eine IIS Sicherheitslücke ausnützt, und damit eine DDoS-Attacke auf whitehouse.gov startet.
25. August 2000 ist der Tag des **Emulex Hoax**: eine gefälschte Presseerklärung an den den News-Dienst “Internet-Wire”, der diese ungeprüft veröffentlicht. Die Pressemeldung berichte von reealuiertem Firmenergebnis und dem Rücktritt des CEO. Das bedingt das Sinken der Aktien von emulex um 61%. Dies wollte der Täter durch Ver- und Wiederinkauf der Aktien ausnützen. Der Täter wird innert 24h gefasst.

Obiges sind Beispiele für die **Arten von Attacken**:

- **physische**: Angriffe auf Hardware, Infrastruktur
- **syntaktische**: Angriffe gegen Software: Schwachstellen, Bugs, DDoS
- **semantische**: Angriffe gegen den Menschen, bzw. Das Verstädnis von Information, und die Art wie sie verarbeitet wird.

Nach Schneier sind die semantischen Attacken das neue Gefährungspotenzial.

Die **Verletzlichkeit** berechnet sich aus der Wahrscheinlickeit des Schadens multipliziert mit der Schadenshöhe. So haben Atomkraftwareke eine hohe Verletzlichkeit. Ein Schaden ist zwar unwahrscheinlich, der Schaden jedoch immens.

Risikofaktoren: Sicherheitsschwachstellen, Dimensionierung, Geschwindigkeit, Irrtumsanfälligkeit, Verauensseligkeit, Komplexität

Ursachen der Gefährdung: Mißbrauch, Fahrlässigkeit, Denkfehler, systemische Bedingungn, mangelndes Sicherheitsbewusstsein, schlampiges Sicherheitsmanagement

Ursachen: Mißbrauch, böse Absicht

Malware ist der Begriff für “Software die böses will”, eine Einteilung von Malware in die Kategorien Virus, Trojaner, Wurm ist schwierig, da sich diese Kategorien oft überschneiden. Hauptverbreitungsweg von Malware ist das Internet. Ein (frischer) Windows XP Rechner ist durchschnittlich nach 20 Minuten am Internet mit Malware infiziert. Nach SP2 verbessert sich diese Survivaltime kurzzeitig.

Fallbeispiel “Sober”, eine semantische Attacke. Sober verschickt sich, über einen eigenen SMTP-Server selber, fälscht den Absender mit Adressen aus dem Adressbuch, genriert zeitbasiert (nicht existente) URLs, über welche der Hacker (der diese URLs ja vorausberechnen kann) Malware zur verfügung stellt, die Sober dann läd. Malware ist mittlerweile zum Businessmodell geworden, die Autoren und Verbreiter damit Geld (z.B. Verkauf von persönlichen Daten).

Andere **Arten von Malware**

- **Trojanische Pferde**: Passwortdialog wird gefälscht. User gibt PWD ein, wird nach der Eingabe zum korrokten Dialog weitergleitet. Der Benutzer nimmt an, dass er sich vertippt hat, und arbeitet nach nochmaliger Passworteingabe weiter. Der Trojaner hat das Passwort zu diesem Zeitpunkt schon gespeichert.

- **Phishing**: Ist oft schon am Stil erkennbar (schlechtes Deutsch, falsches Layout, ...). Aber wie eine eine Diplomarbeit (Theresia Pinter) ergab, werden auch echte Internetseiten für Phishing versuche gehalten. Das Problem ist also nicht von der Hand zu weise, zu dem Phishing im Moment starke Steigerungsraten vor zu weisen hat.
- **DDoS-Attacken**: Distributed Denial of Service: Eine Demo ist z.B. eine DdoS Attack auf Autos, die dann nicht mehr fahren könne.

Funktionsweise von DdoS: “Irsinnig” viele Rechner stellen gleichzeitig eine Anfrage an einen Server, und versuchen ihn durch die schiere Last außer Gefecht zu setzen. Ist der Server schnell genug (was man nicht wissen kann), kann er auch DDoS abwickeln. Daher werden unbeantwortbare Anfragen geschickt, z.B. kaputte Pakte (malformed packets, **malicious packet**s) mit falschem Absender.
Der Server will sich das kaputte Paket bestätigen lassen, was er aufgrund des falschen Absenders nicht kann. Bis zum Timeout (üblich: 30 Sekunden) wartet der Server auf Antwort. Die hohe Anzahl an Anfragen legt den Rechner, der irgendwann nur noch bis zum Timeout auf Antwort wartet, lahm.
Aber wer verschickt DDos Attacken? Per Malware infizierte Rechner schicken (ohne Wissen des Besitzers) DDoS Pakete.
Ablauf eine DDoS Attacke: Der Hacker hat kontrolle über eine Master Computer und über diese über viele sogenannte Zombies, weche die DDoS Pakete verschicken. Verschleirt der Hacker noch zusätzlich mit Anomyzer, etc., ist er nur schwer zu identifizieren. Daher sind die Urheber von DDoS of nicht eruierbar.
Forgeschrittenes DDoS: Damit die attackierte Organisation nicht den Server gegen das Internet adreht, intern aber weiter verwendet, hat der Hacker auch firmeninterne Rechner infiziert.
“The Gibson Research Group”, die sich mit DDoS beschäftigt, wird 2002 eine DDoS Attacke von einem 13jährigen. Der Begriff “**Script Kiddies**” kommt auf. Diese verwenden Hacker Toolkits um Malware “zusammen zu klicken”.
Ein Grund für die Häufung von DDoS war der “schlechte” Netzwerkstack von XP, es war nämlich der Zugriff auf raw-sockets war möglich. SP2 verbesserte dies, Vista wird die Situation noch weiter entschärfen.

- Dialer: Der Klick auf einen Link öffnet einen Installationsdialog. Das installierte Programm verbindet sich auf kostenpflichtige Nummern (z.B. 30 € / Call), Dialer verlieren in Zeiten von Breitbandkommunikation ihre Bedeutung.

Die **Schäden die durch Malware** verursacht werden sind nur **schwer**

abschätzbar, obwohl in den Medien immer wieder konkrete Zahlen verbreitet werden. Wer kann schon den Schanden durch den Betriebsausfall eines Privatcomputers beziffern? Wie groß ist der Schaden durch veröffentlichung geheimer Dokumente? Was kostet ein allgemeiner Internetausfall, wenn niemand ins Internet kann?

Reaktionen der Industrie

- **Schuld auf die Anwender abschieben**, weil diese fahrlässig gehalndelt hätten, oder kein Virenscanner installiert haben. Dazu ist zu bemerken, daß im Falle des iloveyou Virus auch beim Einhalten der üblichen Vorsichtsmaßnahmen nur wenig hilfreich war, da MS immer noch die direkte Ausführung von Attachments erlaubte. Ein Kommolition hat auch richtig bemerkt, daß das verstecken der Dateiendung (per default) kontraproduktiv ist. Virenscanner können ohnehin erst nach ein paar Tagen (im besten Fall Stunden) vor einer Infektion schützen.
- **Schuld auf Administratoren abwälzen**, weil nicht der letzte Patchlevel verwendet wurde. Dazu ist zu bemerken, daß MS (vor dem Patch-Day) ein bis zwei Security Bulletins pro Woche veröffentlicht hat. Für Unternehmen ist es **unmöglich**, zweimal pro Woche zu patchen, da der Arbeitsaufwand, bis die eigenen Programme auf kompatibilität geprüft sind, zu groß ist.
- **Security by obscurity**, z.B. das Verheimlichen von Sicherheitslücken. **Vorgehen gegen diejenigen die Sicherheitslücken veröffentlichen**.
  Stellen sie sich vor, sie entdecken eine Sicherheitslücke in der Onlinebankingsoftware ihrer Bank, und setzen sich mit dem Institut in Verbindung, erzählen von dem Leck, und als Folge werden sie von ihrer Bank geklagt (obwohl sie sonst mit niemandem darüber sprachen, die Sicherheitslücke nicht veröffentlichten). Dieser Fall ist tatsächlich vorgekommen.
  Wann immer der Begriff security by obscurity (Schutzmechnismen nicht offengelegt werden) fällt, sollten bei einem Informatiker **alle Alarmglocken** läuten!
- **Leugnen von Sicherheitsproblemen**

Reaktionen der Politik
Der Europarat verabschiedet ein Cybercrimeabkommen: Speicherung von Verkehrsdaten, Abhörung, ... Die wurde Gott-sei-Dank nich umgesetzt. Es verstößt auch gegen die europäischen Menschenrechtsverträge.

Ursachen: Bugs

14. September 2004: Der **Flugverkehr** über Kalifornien **bricht zusammen**. Auslöser war (ein bekannter Bug in Win95), daß nach dem Wechsel von Unix zu Windows, ein Admin vergaß einen Rechner – wie vorgesehen – regelmäßig neu zu starten.
15. Jänner 1990: AT&T **Ferverbindungen brechen zusammen**: Die neue Release der Telefonvermittlungssoftware hat einen Bug, der nur

selten und unter Vollast auftritt, aber wenn er auftritt, ihn an die benachbarten Stationen “weitergibt”. 70 Millionen Anrufe bleiben unbeantwortet, 9 Stunden bis zur Problembehebung.

Daß derBegriff “Bug” auf einem Tagebucheintrag von Grace Murray Hopper basiert ist nur eine Legende. Zwar eine nette Anekdote, aber nicht wahr. **Der Begriff Bugs wird schon lange für Fehler in Geräten verwendet**.

Ursachen: Denfehler

Dem Bestrahlungsgerät **Therac-25 fallen drei Menschenleben “zum Opfer”**. Es gibt zwei Operationsmodi, Diagnose (niedirge Intensität) und Behandlungsbestrahlung (hohe Intensität, kurze Dauer). Ein Bug macht hochenergetische Diagnosestrahlung möglich, nur eine Hardware sicherung verhindert ein Disaster. Diese Hardwaresicherung, die vor jeder Behandlungsbestrahlung betätigt werden muß, verhindert aber auch, daß der Bug gefunden wird. Im Nachfolgemodell wird die Hardwaresicherung entfernt, da die Software (so wie so) alles regelt. Die Folge sind drei Tote und mehrere schwere Verbrennungen. Es dauert so lange bis der Fehler gefunden wurde. Grund war, daß die **Softwarefirma nicht getestet** hat.

Die R**aumfähre Challenger explodiert** am 28. Jänner 1986 kurz nach dem Start. Die Gründe für dieses Unglück sind organisatorische und technische Fehler. **Politischer Druck** zwingt zu einem Start bei kaltem Wetter, welches wiederum für das Versagen einer “O-Ring” Dichtung verantwortlich ist. Das traurige dabei: Die Fehleranfälligkeit für den O-Ring bei niedrigen Temperaturen ist **klar** aus den Unterlagen der NASA **ersichtlich**. Die Techniker verwenden jedoch schlecht aufbereitete Unterlagen, und der Zusammenhang war nicht offensichtlich. Hätte man eine andere Visulaisierung, z.B. eine einfach Tabelle verwendet, hätte die Challenger offensichtlich (!) **nicht starten dürfen**. Edward Tuft fordert daher, daß jeder **Techniker auch in der Lage sein muß, Daten zu visualisieren**.

Ursachen: Designfehler

WLAN: Unsicherheit in **WEP** wegen **schwerer Designfehler**. Mittlerweile kann WEP in kürzester Zeit geknackt werden. Leider übertragen viele Protokolle die Daten (auch Passwörter) in **Kartext**, und mit einer einfachen sniffing-attacke könne sensible Daten eruiert werden.

Bush Wahl: Die alten Stimmzettel in Forida hatten zwei Spalten mit Kandidaten und jeweis rechts davon den Bereich “sein Kreuz zu machen” (in wirklichkeit muß mit einem Stif ein Loch gestochen werden). Die neuen Stimmzettel hatten zwar immer noch zwei Spalten mit Kandidaten,

aber die Markierung erfolgte nur noch in der Mitte. Dabei wurde aber die rechte Spalte von der Hand überdeckt.

Robbie cx30 bringt Bart Matthews um. Ein Bug lässt den Roboter ausrasten, Matthews versucht den Roboter zu deaktivieren, muß sich aber durch sechs Untermenüs arbeiten. Fehler war der Bug, T**odesursache ein Designfehler**: der Notstopp war nicht schnell genug erreichbar. Dies ist **nur eine fiktionale Geschichte!**

Y2k Bug basiert auch auf einem **Designfehler**, der noch auf die Lochkartenzeit zurück geht. Damals wurd platz gespart, und es wurden nur die letzten zwei Ziffern der Jahreszahl verwendet. Das rächte sich dann im Jahr 2000. Allerdings konnte große Probleme verhindert werden (obwohl z.B. in einem Staat in Skandinavien (Norwegen?) funktioniert der Feuerwehrnotruf nicht). Der **gute Ausgang** ist einem **immensen Aufwand** der Industrie zu verdanken “Success story”, die die Systeme verbessert, und das Verständnis vertieft hat. Es gibt aber auch Kritik von Peter Neumann, warum im Zuge der Arbeiten am Y2k Bug **nicht auch andere Probleme aus der Welt gschafft** wurden, statt dessen wurde nur (ausreichend?) gepacht. Neumann nennt später auch “das Stiefkind der Y2k Bug” das **buffer-overlow** Problem beim Namen:
Ein Puffer wird über den ihm zugewiesenen Speicherbereich hinaus gefüllt, sodaß Daten im Codespeicherbereicht landen, und ausgeführt werden können (“**Code injection**”). Sei Vist liefert MS eine Execution Protection aus, die aber von Haus aus nicht aktivert ist. Also: **Execution Protection auf Vista aktivieren**! *(Bin ich froh über mein Linux, Henry)*