Proseminar
"Ethische Aspekte der Informationsverarbeitung"

BTU Cottbus
Lehrstuhl Graphische Systeme
Prof. Dr. Winfried Kurth

Die Verwundbarkeit der informationstechnischen Infrastruktur, insbesondere am Beispiel der Luftfahrt

Christian Bendele - 22.01.2008

Übersicht

1. Verwundbarkeit

Die Verwundbarkeit informationstechnischer Infrastruktur heißt einerseits

- Unsicherheit gegenüber Unfällen, zufälligen Ereignissen (einschließlich z.B. Naturkatastrophen) sowie unbeabsichtigter Fehlbedienung, andererseits auch

- Unsicherheit gegenüber bewussten, böswilligen Angriffen jeglicher Art, von innen (eigenes Personal) wie von außen.

Es ist jedoch nicht notwendig, vielleicht sogar gar nicht empfehlenswert, diese beiden sehr unterschiedlichen Gefahrengruppen völlig isoliert zu behandeln:

"Wir beobachten, daß eine große Zahl der Unfälle der Vergangenheit durchaus auch absichtlich hätten hervorgerufen werden können -- und in manchen Fällen auch heute noch böswillig hervorgerufen werden könnten." [Neumann]

Wenn wir von Unsicherheit sprechen, was heißt denn dann Sicherheit?

2. Sicherheit - auf Deutsch und auf Englisch

Safety — Freedom from hazards which could lead to death or injury to people or damage to equipment, property, or the environment[i]

Security — Methods or systems to prevent any event or action that could cause a loss of or damage to computer hardware, software, data and information[ii]

Im Zusammenhang mit Daten und Informationen heißt das insbesondere den Erhalt der drei Grundeigentschaften

- Confidentiality, also Vertraulichkeit
- Accurcy/Integrity, also Genauigkeit und Integrität
- Availability, also Verfügbarkeit

Reliability — The capability of an implementation to maintain its level of performance under stated conditions for a stated period of time.[iii]

"Safety" und "Security" sowie auch Zuverlässigkeit ("Reliability") sind natürlich eng mit einander verknüpft.

3. IT-Infrastruktur

Informationstechnische Infrastruktur im weitestens Sinne sind Rechner und Rechnernetzwerke. Komplexe Rechnernetzwerke und Netzwerkverbunde finden sich heute überall.

Die Ausdehnung kann dabei über die ganze Welt gehen, wie im Beispiel der Luftfahrt (Infrastruktur des Flugsicherungsapparates, Der Fluggesellschaften, ...), oder sich über ein Land erstrecken (Netzwerk der dt. Banken zur Abwicklung des elektronischen Geldverkehrs).

Auch die in ihrer lokalen Ausdehnung sehr kompakte IT-Infrastruktur innerhalb z.B. eines Passagierflugzeuges oder eines modernen PKW ist heute ausserordendlich komplex und verdient der Betrachtung.

Je nach Anwendungsbereich können die Folgen einer Beeinträchtigung solcher Strukturen enorm sein. Im Bereich der Luftfahrt können Unfälle mit hohen Todeszahlen die Folge sein. Auch zur gezielten Entführung von Maschinen mit hochrangigen Passagieren nach vorherigem Einbruch in die Passagierdatenbestände ist es schon gekommen[Neumann].

4. Angriffspunkte anhand von Beispielen aus der Vergangenheit.

4.1. Mangelnde Redundanz der Kommunikationswege

"Twenty air-traffic control centers were downed by a fiber-optical cable inadvertedly cut by a farmer burying his cow (4. May 1991)"[Neumann]

Der dezentral organisierte Apparat der Flugsicherung, auch in Europa, ist in hohem Maße auf seine Kommunikationsinfrastruktur angewiesen. Piloten geben Flugpläne an ihrem Startort (oder heute Online) auf, die später jedem Sektorkontroller auf dem Weg sowie den Controllern am Zielort automatisch vorliegen müssen. Radaranlagen stehen teilweise hunderte von Kilometern von den ATC Centern entfernt, ein Zusammenbruch der Kommunikation hätte einen Wegfall der Luftraumstaffelung und damit je nach Verkehr und Sichtbedingungen (Wetter!) ein hohes Risiko von Zusammenstößen zur Folge.

Hatte z.B. Stuttgart vor einigen Jahren noch eine eigene Flugsicherung, so werden An- und Abflüge dort heute von Frankfurt aus kontrolliert. Die Radaranlagen, und auch die Funktechnik, befinden sich jedoch auch heute noch in Stuttgart. Die Abhängigkeit von verwundbaren Kommunikationswegen nimmt heute also, teilweise aus wirtschaftlichen Erwägungen, eher noch zu.

4.2. Elektromagnetische Interferenz

Melbourne Airport berichtet von ernstzunehmenden Störungen ihrer Funkkommunikation die letztenendes auf einen "strahlenden" Videorekorder in der Nachbarschaft zurückgeführt werden konnten.[Neumann]

> CE und FCC Bestimmungen werden oft nicht ernst genommen, wieviele der im Raum anwesenden Studenten betreiben regelmäßig ihren PC mit geöffnetem Gehäuse?

Bei einer Boeing 737 kam es während des Reiseflugs zu einem unerklärlichen oszillieren der Höhensteuerung des FMC (Flight Management Computers). Der Flugkapitän bittet per Durchsage alle Passagiere noch einmal zu überprüfen ob ihre Handys ausgeschaltet sind. Kurz darauf verhält sich der FMC wieder normal.[iv]

Anekdoten dieser Art häufen sich unter Piloten, Einflüsse elektromagnetischer Strahlung auf die Elektronik eines Flugzeuges sind noch immer unzureichend erforscht.[4]

4.3. Mängel an der Schnittstelle zwischen Mensch und Maschine

Seitdem Computer an Bord moderner Flugzeuge eine zunehmend wichtigere Rolle Spielen entstehen immer wieder Unfälle weil der oder die Piloten an Bord physisch/mechanisch gegen die Steuereingaben des Computer "kämpfen" anstatt zu ergründen warum der Autopilot nicht so steuert wie erwartet, diesen korrekt zu programmieren, oder auch einfach nur zu deaktivieren.

Als Beispiele seien nur genannt:

- China Airlines A300-600 in Nagoya 1994[v]

- Airbus A320 der Air France 1988 in Habsheim

Unglücklicherweise wird der Fehler in solchen Fällen sehr häufig bei den Piloten gesucht ("human error"), obwohl Probleme im Design der Mensch-Maschine Schnittstelle offensichtlich sind.[auch: Neumann]

Machtungleichgewicht Einzelperson (Pilot) gegen Großkonzern (Systemhersteller?)

4.4."Risks inherent in developing complex systems

"Software complexity ist the largest contributing factor to the [un]reliability of software."[vi]

Probleme bei der Entwicklung komplexer Systeme sind allgegenwärtig und nicht auf die Informationstechnologie beschränkt.

[Neumann] nennt als Beispiel die Entwicklung des C-17 Militärtransporters den McDonnell Douglas in den 80ern und 90ern des vorigen Jahrhunderts für die US Streitkräfte entwickelt hat. Als Luftfahrtrelevante Beispiele aus heutiger Zeit bieten sich die Airbus Modelle A380 und A400M oder der Boeing Dreamliner an. Bei all diesen Beispielen spielen unter anderem auch Schwierigkeiten bei der Entwicklung zuverlässiger und sicherer Software eine Rolle.

Auch Softwarehersteller welche die Release Dates ihrer Produkte über Jahre vor sich herschieben sind heute eher die Regel als die Ausnahme. Und trotzdem fühlt sich so mancher Kunde danach immer noch als Beta Tester mißbraucht.

Auch [Steinmüller] beschäftigt sich intensiv mit der "endogenen Verletzlichkeit" hochkomplexer Systeme:

"Sie entsteht nicht nur [...], sondern vor allem wegen der undurchschaubar großen *immanenten* Komplexität der Informationssysteme"[Steinmüller]

Er fühlt sich leider nicht dazu bemüßigt hierfür ein konkretes Beispiel zu nennen.[1]
Er fährt fort:

"IT-Großtechnologie ist bereits wegen ihres prinzipiell unvorhersehbaren Verhaltens [!] gefährlich, noch vor und unabhängig von dem Hauptstörfaktor, dem leichtsinnigen externen Eingriff sich kompetent fühlender Experten (Ingenieure und Informatiker);"

Nun mag ja die "prinzipielle Unvorhersehbarkeit" etwas überspitzt formuliert sein. Tatsache ist daß viele Systeme heute eine Komplexität angenommen haben die offensichtlich nicht mehr ausreichend durchschaubar ist. Als etwas alltäglicheres Beispiel seien moderne PKW genannt:
"das wuchernde Elektroniknetz moderner Pkw ist inzwischen für jede zweite Autopanne verantwortlich"[vii]

[1] Beispiele weiter unten in [Steinmüller] beschäftigen sich hauptsächlich mit den zusätzlichen Risiken "hybrider" Systeme, d.h. der Verbindung von Großsystemen alter/analoger Technologie mit moderner Informationstechnologie.

5. Der Leichtsinnige Eingriff sich kompetent fühlender Experten?

In der Tat fragt man sich heute als technisch interessierter Verbraucher manchmal, inwieweit die heute praktizierte totale Vernetzung eigentlich unabhängiger Systeme nützlich und wünschenswert ist. Bleiben wir beim Auto:

Eine der Pannen, die die Fachzeitschrift "Auto Motor u. Sport" beim letzten Monat beendeten Dauertest des aktuellen 5er BMW bemängelte, wurde durch den Taster an der Heckklappe ausgelöst, der zum öffnen der Heckscheibe dient. "Der Berührungstaster hatte das Zeitliche gesegnet und brachte das komplette CAN-Bus-System (Controller Area Network) durcheinander."[viii]

Trotzdem gebe ich Herr Steinmüller zu bedenken, daß die "Experten" oft sehr genau wissen wo die Grenzen (und der Sinn) der modernen Technik liegt. Im Alltag unserer Gesellschaft sind es sehr viel häufiger Zwänge durch visionäre Strategen mit eher kaufmännischem Hintergrund oder die Marketingabteilungen die einen Ingenieur oder Informatiker dazu verleiten moderne Technik auf eine Art einzusetzen deren Gefahren ihm durchaus bewusst sind.

6. Lösungsansätze

"We desperately need the ability to develop complex systems -- within budget, on schedule, and with high assurance compliant with their stated requirements"[Neumann]

Mit konkreten Vorschlägen wie dies erreicht werden kann scheinen sich jedoch alle schwer zu tun.

Auch endet manch gut gemeinter Ansatz in einem Teufelskreis:

"In many critical systems, as much as half of the software may be dedicated to techniques for attempting to increase security, reliability and safety."[Neumann]

Akzeptiert man die oben genannte Prämisse des unlösbaren Zusammenhangs zwischen der Komplexität und der erreichbaren Sicherheit/Zuverlässigkeit eines Systems, so sollte man spätestens hier erkennen wo das Problem vieler bisheriger Lösungsversuche liegt.

6.1. Sicherheit a priori, nicht a posteriori

Neumann erkennt einen Ansatzpunkt darin daß bei vielen heute existierenden Systemen Sicherheitsfeatures oft erst am Ende des Entwicklungszeitraumes berücksichtigt wurden. Er fordert daß bei zukünftigen Entwicklungen dieses Thema von Beginn an ("a priori") an wichtiger Stelle stehen muß.

Häufig ist das jedoch nicht so einfach, da Entwicklungen über Jahrzehnte gehen und sich nicht vorherplanen lassen. Bei der Entstehung des Internetvorläufers ARPANet stand Sicherheit und auch Zuverlässigkeit durchaus an erster Stelle. Daß Jahrzehnte später sich das Internet in eine Richtung (und Größe) entwickelt die die damals vorgesehenen Sicherheitsmechanismen als absolut unzureichend erscheinen lassen haben wir schon in einem anderen Referat dieser Veranstaltung gehört, das kann den Ursprünglichen Entwicklern jedoch kaum Vorgeworfen werden.

7. Das Internet als störungssicheres Kommunikationsmittel?

Auch die Redundanz und dadurch die Zuverlässigkeit des Internets ist nicht in früherem Maße gegeben. War das ARPANet mit seinen vielen Querverbindungen anfangs durchaus als störungssicher entwickelt worden, so hat man diesen Schwerpunkt mit zunehmender Kommerzialisierung des Internets zunehmend aus den Augen verloren.

"Wenn fünf wichtige Rechner zum Opfer von Terroristen werden, kann das Netz zusammenbrechen"

schreibt die Süddeutsche Zeitung noch vor dem 11. September.[sz]

Wenige extrem frequentierte Austauschknoten, in Europa etwa das DE-CIX in Frankfurt oder das LINX in London bilden das Rückgrat des Internet. Ein genauer Lageplan dieser verwundbaren Stellen des Internet ist sogar im Internet online abrufbar.[sz]

8. Auswege

Tatsächliche Lösungswege fordern zuerst die Erkenntnis dass viele der diskutierten Systeme heute tatsächlich ein Ausmaß an Komplexität angenommen haben in dem sie auch von Experten nicht mehr durchschaubar sind, also auch nicht mit letzter Konsequenz sicher oder zuverlässig zu gestalten sind (vergleiche auch [Steinmüller]).

Jede Entscheidung für oder wider der Verwendung solcher Technologie fordert die unbedingte Einbeziehung dieser Erkenntnis, insbesondere wenn es um Menschenleben geht, wie in der Luftfahrt, oder auch "nur" um die Verarbeitung z.B. hochvertraulicher Daten.

Dort wo eine Abhängigkeit von solchen Systemen bereits besteht muss man sich darüber Gedanken machen wie diese Abhängigkeit zu mildern ist und was getan werden kann damit Ausfälle NICHT zur Katastrophe (d.h. schlimmstenfalls dem Tod vieler Menschen) führen.

Mit der stetigen Zunahme des Luftverkehrsaufkommens bei jedem Wetter, also auch bei schlechten Sichtbedingungen, sind Piloten heute auf die Staffelung der Flugsicherungslotsen an den Radarschirmen angewiesen um Unfälle und Zusammenstöße in der Luft in besonders stark frequentierten Bereichen ,z.B. um Flughäfen, zu vermeiden.

Das Risiko dieser Abhängigkeit wurde durch die FAA (Federal Aviation Administration der USA) und die JAA (neue Joint Aviation Administration der EU) bzw. derer Nationaler Vorläuferorganisationen durchaus erkannt.

Man versucht in den letzten Jahren die Verantwortung deshalb wieder mehr zurück ins Cockpit zu verlegen.

Neuere Gesetzgebung schreibt in Kommerziellen Maschinen den Einsatz moderner TCAS (Traffic Alert and Collision Avoidance System) Systeme vor. In kleineren Maschinen ist mittlerweile zumindest der Einsatz sogenannter "Mode-S" Transponder vorgeschrieben, die eine Radarerfassung erkennen und ein durch TCAS Systeme auswertbares Antwortsignal senden. Aufgrund der hohen Kosten der Umrüstung war und ist diese Gesetzgebung unter Sportpiloten (die hauptsächlich bei gutem Wetter unter Sichtbedingungen fliegen) durchaus umstritten.

9. Anhang

9.1. Quellenangaben

[Neumann] Peter G. Neumann - Computer Security in Aviation: Vulerabilities, Threads and Risks, http://www.csl.sri.com/users/neumann/air.html. Deutsche Zitate in eigener Übersetzung.
[Steinmüller] Wilhelm Steinmüller . Verwundbare Gesellschaft. In: Wilh. Steinmüller - Informationstechnologie und Gesellschaft, Darmstadt 1993. S.540-544.
[sz] "Der verwundbare Datenverbund"", Süddeutsche Zeitung vom 1.8.2000

---

[i] Redmill, Chudleigh, Catmur - System Safety: HAZOP and Software HAZOP, Wiley 1999, p-242
[ii] http://en.wikibooks.org/wiki/SA_NCS_Computer_Application_Technology:Glossary
[iii] http://www.sei.cmu.edu/opensystems/glossary.html#r
[iv] http://www.rvs.uni-bielefeld.de/publications/Incidents/DOCS/Research/Rvs/Article/EMI.html
[v] http://www.rvs.uni-bielefeld.de/publications/Incidents/DOCS/Institution/Risks/COPY/18.33.html#subj5
[vi] Pipkin - Information Security (Pipkin) HewlettPackard Proffesional Books, p40
[vii] http://www.daserste.de/ratgeber/auto_beitrag_dyn~uid,ixgyvwpzoxgfb77r~cm.asp
[viii] Auto Motor und Sport 3/2008, Verlag Motor Presse Stuttgart