Mit dem Finger

Von Ralf Isau

„Digital aufpoliert gefallen mir die beiden Bs viel besser. Einfach exorbitant! Was hältst du davon, Humunculus?“

„Schwärmst du gerade von Brigitte Bardot oder von Boris Becker, mein Lieber?“

„Weder noch, sondern von Ingrid Bergmann und Humphrey Bogart. Hab letztens mit Ingeborg die digitale Bearbeitung ihres Kultstreifens *Casablanca* angesehen. Einfach genial: keine Kratzer, kein Knistern – und alles so schön bunt!“

„Aber digital bedeutet doch ‘mit dem Finger’. Willst du mir sagen, wenn eine kultige Aktrice und ihr starrgesichtiger Lover auf der Leinwand fluoreszieren, als hätte ein Dreijähriger sie mit Fingerfarben aufgepeppt, dann sei das ‘exorbitant’?“

„Von wegen Finger! Nichts da manuell. Das ist Hightech in Reinkultur. Alles mit elektronischen Hochleistungsrechnern gemacht. Computer arbeiten, wie du eigentlich wissen müsstest, digital.“

„Der einzige mir bekannte Rechner, der mit dem Finger bedient wird, ist der Abakus.“

„Ich rede nicht vom lateinischen ‘digitus’, dem Finger, sondern vom englischen ‘digit’, der Ziffer also. Mit denen, genauer gesagt mit Nullen und Einsen, werkeln Digitalcomputer. Und das äußerst effektiv. Durch die Digitaltechnik geht alles schneller, genauer, schöner, besser ...“

„Und warum fluchst du dann unentwegt, wenn du vor deinem neuen PC kauerst?“

„Weil ich ihn noch nicht so gut kenne.“

„Frisch verliebte Paare schreien sich auch nicht ständig an.“

„Ich fluche ja nur, wenn er sich aufhängt.“

„Was tut er? Schöne neue Welt! Suizidgefährdete Maschinen treiben ihre Bediener in psychotherapeutische Behandlung. Und das nennt sich dann Fortschritt.“

„Das sind nur Kinderkrankheiten. Der Fortschritt steckt im unglaublichen Potenzial der Maschinen. Sie krempeln unser ganzes Leben um. Sogar den menschlichen Körper wird die Digitaltechnik bald perfektionieren. Künstliche Sinnesorgane wie Augen und Ohren sind bereits im Experimentierstadium. Irgendwann gibt es den individuell konfektionierten und bedarfsgerecht umfunktionierbaren Body. Dann werden wir zu einer neuen Daseinsstufe aufsteigen, den Cyborgs. Ist das nicht aufregend!“

„Ich bekomme gerade das große Zittern. Der Mensch hat seine Werkzeuge zu entsetzlichen Waffen perfektioniert – was wird erst entstehen, wenn er sich an der Schöpfung vergreift? Da ziehe ich die Ingeborg doch jedem Cyborg vor.“

„Du kannst nicht alles mies machen, Homunculus. Nimm doch nur das digitale Haus. Geräte schalten sich auf Zuruf ein. Alles funktioniert automatisch. Demnächst, wenn nach der Geburt jeder seinen Chip ins Hirn gepflanzt bekommt, genügt schon ein Gedanke, und das Haus, das Auto, der Fahrkartenschalter – jeder weiß sofort, was du willst.“

„Wie wahr! Dein Arbeitgeber, die Polizei, der Geheimdienst ...“

„Natürlich müsste man die Computer so programmieren, dass weder Missbrauch noch Fehlfunktionen möglich sind.“

„Mach dir doch nichts vor, mein Lieber. Abgesehen vom verkabelten Grips bist du doch heute schon eine digitale Persönlichkeit. Deine Blaupause ist in Computern abgelegt, zur gefälligen Bedienung durch jedermann. Und was die Fehlertoleranz dieser Systeme betrifft, darf ich dich nur an den Wortlaut des Lizenzvertrages für dein neues Programm erinnern, das du dir kürzlich aus dem Internet geladen hast: ‘Es wird darauf hingewiesen, dass nach dem Stand der Technik es nicht möglich ist, Computersoftware so zu erstellen, dass sie

in allen Kombinationen und Anwendungen fehlerfrei arbeitet.' Mit anderen Worten: Es gibt keine fehlerfreie Software. Wir vertrauen unser Leben fehlerbehafteten Maschinen an. Wir lassen sie Nuklearwaffen und Atomkraftwerke überwachen, den Straßen-, Schienen- und den Luftverkehr, Geräte der Intensivmedizin und vieles mehr. Mit jeder neuen Version der Programme vervielfacht sich noch deren Komplexität. Der Terminus 'fehlerfreie Software' ist ein Widerspruch in sich, mein Lieber. Genauso gut könntest du auf einen dunklen Blitz warten. Dann allerdings suche ich mir eine neue Bleibe."

„Schlag dir das aus dem Kopf, Homunculus. Der Fortschritt ist eine Epidemie, gegen die nur wenige immun sind. Vielleicht wird das Gemeinwesen der Zukunft so gewaltig wie Fritz Langs Metropolis sein, nur dass es Digitalis heißt und genauso kalt und unpersönlich. Vielen Dank, da bleibe ich doch lieber ein rückständiger Nonkonformist, lasse die herzlose Elektra links liegen und spiele mit Ingeborg Dame. Und was dein Digitalis anbelangt, das gibt's unter dem Namen 'Fingerhut' schon lange. Bewährtes Herzmittel. Vielleicht wirst du's mal dringend brauchen, wenn du aus deinem digitalen Zukunftstraum erwachst. Man nimmt es übrigens mit den Fingern."

Recherchequellen

Brute Force-Angriff; ein Angriff auf einen verschlüsselten Datenbestand durch einfaches Ausprobieren aller Kombinationsmöglichkeiten. 1997 hat man gesehen wie sicher die Verschlüsselungen sind, die die NSA dem Rest der Welt (außerhalb der USA) aufgrund der Exportbeschränkungen zugestehe. Zu Jahresbeginn habe die amerikanische Sicherheitsfirma RSA zum Brute-Force-Angriff auf Verschlüsselungsverfahren aufgerufen. Gemäß den US-Exportbeschränkungen dürften nur Verfahren für Schlüssel mit bis zu 40 Bit länge ausgeführt werden. Aufgrund des RSA-Aufrufes schaffte es eine vorwiegend europäische Internet-Initiative in nur 313 Stunden einen 48 Bit langen RC5-Code zu knacken. Ein 40-Bit-Schlüssel war sogar schon 3,5 Stunden nach Beginn des Wettbewerbs gefallen. Selbst ein allgemein als recht sicher angesehener 56-Bit-Schlüssel war am 18. Juni enttarnt. Dabei handelte es sich fatalerweise sogar um ein Datenpaket, das mit dem DES-Algorithmus verschlüsselt worden war, der von Banken eingesetzt wird und an dessen Entwicklung die NSA selbst in Teilen beteiligt gewesen war. Dazu hatten mehrere tausend Anwender ihre PCs über das Internet verbunden und seit Februar gemeinsam an der Lösung rechnen lassen. Das Glück spielte zwar mit – es musste nur ein Viertel der 72 Billiarden Möglichkeiten durchprobiert werden. Aber die NSA wisse schon, warum sie sicherere Verschlüsselungsverfahren als „Waffen“ unter Exportverbot stelle. So könne sie viel leichter den Datenverkehr anderer Personen, Firmen, Organisationen und Länder abhören (was sie, wie jeder inzwischen wisse, ja auch ausgiebig täte).

CIA angreifbar, weil hochtechnisiert; siehe Artikel in *Konr@d,* Nr. 1/97, Seite 32 ff

Clipper Chips der NSA; (siehe c’t 8/94, S. 24) Titel „Die NSA und der Clipper-Chip“ — Mit dem Clipper-Chip und seinem individuellen `Unit Key´ glaubte die →NSA den Weg gefunden zu haben, eine sichere Verschlüsselung verbreiten und doch bei Bedarf auf den Klartext zugreifen zu können: Mit diesem Schlüssel, der per Gerichtsbeschluß bei einer Hinterlegungsstelle einzuholen ist, werden dubiose Clipper-Anwender belauschbar. Der fast gänzlich geheimgehaltene Clipper-Algorithmus `**Skipjack**´ gilt ansonsten als sehr sicher; er verwendet einen 80-Bit-Schlüssel und 32 Iterationen (zum Vergleich: DES basiert auf einem 56-Bit-Schlüssel und 16 Runden). Seit die NSA im April 1993 mit dem offiziellen Vorschlag des `Escrowed Encryption Standard´ (EES) an die Öffentlichkeit ging, laufen Datenschützer in den USA Sturm gegen die Familie der Clipper-Chips. (un)

Titel „Hintertür zugeschlagen – Ein AT&T-Forscher blamiert die NSA“ Ein äußerst umstrittenes Kryptographieprojekt der US-Regierung, die EES-Verschlüsselung der `Clipper´-Chips, ist erneut ins Gerede gekommen. Matthew Blaze von den Bell Labs zeigte, wie sich der behördlich vorgesehene Lauschangriff auf EES-verschlüsselte Informationen umgehen läßt. — Matt Blaze stand neben spärlichen Informationen über interne Clipper-Funktionen für seinen Angriff ein Prototyp der Clipper-PCMCIA-Karte `Tessera´ zur Verfügung. In einer Vorabveröffentlichung beschreibt er detailliert, wie er das für den Zugriff seitens autorisierter Dritter vorgesehene `Law Enforcement Access Field´ (LEAF) mit unsinnigen Daten füllen und Clipper trotzdem nutzen konnte. Das LEAFenthält im Normalfall eine - wiederum verschlüsselte - Kopie des aktuellen Anwenderschlüssels. Blaze kam der Umstand zu Hilfe, daß das LEAF lediglich durch eine 16-Bit-Prüfsumme geschützt ist. — Die Ergebnisse des Kryptoanalytikers zeigen, daß es für Spezialisten möglich ist, Clipper zur unauffälligen und

im Ernstfall doch unangreifbaren Verschlüsselung ihrer Kommunikationsstrecken einzusetzen. — Die verantwortliche Regierungsbehörde NSA indes gibt sich gelassen und Blazes erfolgreiche Attacke als ein nicht praxisrelevantes Problem aus: `Wer den gesetzlich erzwungenen Zugriff umgehen will, würde höchstwahrscheinlich einfachere Alternativen wählen´, so NSA-Sprecher Michael Smith unter Anspielung auf Sicherheitsprodukte, die nicht von der NSA stammen. Schon deren bloßer Einsatz könnte allerdings das Behördeninteresse wecken, wenn Clipper erst einmal weite Verbreitung finden sollte.(un)

Cyborg; Begriff der sich aus Cybernetic (Kybernetik) und Organism (Organismus) zusammensetzt. Damit werden (nicht nur in der SF-Literatur) biologische Wesen bezeichnet, deren Sinne oder körperliche Leistungsfähigkeit durch technische (kybernetische) Veränderungen gesteigert wurde. Eine Abhandlung darüber, was heute schon geht oder in naher Zukunft (Stand: September 1997) zu erwarten ist, findet sich in *Konr@d,* Nr. 1/97, Seite 101 ff

digital *Adj.;* Bezieht sich auf Ziffern oder die Art und Weise ihrer Darstellung. In der Computertechnik ist »digital« ein Synonym zu »binär«, da die landläufig bekannten Computer Informationen als Kombination binärer Stellen (Bit) verarbeiten.
Quelle: *Computer-Fachlexikon mit Fachwörterbuch (deutsch-englisch/englisch-deutsch);* Microsoft Press

digitus; lat. „Finger“

DVD; digitale Video-Disk

DV; digital Video

DAT; digital audio tape

digitale Kamera

digitales Kaufhaus

Extropianer; Bewegung, die sich dem Ziel verschrieben hat, den Supermenschen zu schaffen. Dabei sind alle Mittel recht: Genmanipulation, „Verbesserung“ des menschlichen Körpers durch technische Implantate oder „Ergänzungen“ usw. Einige Extropianer sehen auch die Zukunft darin, dass jeder Mensch selbst bestimmen kann, wie er aussieht und welche Fähigkeiten er besitzen wird.
Quelle: c’t 1997, Nr. 11, Seite 124 f

Gedankenkraft zur Steuerung von Computern benutzt; bereits heute gibt es erste technische Lösungen und interessante Ansätze zur Nutzung der elektrischen Gehirnaktivität für die Steuerung von Computern. Die Technik ist allerdings noch weit davon entfernt, das Gedankenlesen zu ermöglichen.
Quelle: c’t 1999, Nr. 6, Seite 296–301

Geheimdienste bedienen sich der Informationstechnik; der Verteidigungsfähigkeit durch Informationstechnik auf die Spünge helfen: Zu den Highlights in dieser Richtung zählt das Einschleusen von Computerviren und logischen Bomben in gegnerische Rechnersysteme. Nach Berichten des *Time Magazine* präpariert der amerikanische Geheimdienst Hard- und Softwarekomponenten, um sie „feindlichen Nationen“ zuzuspielen.
Quelle: *c’t* 18/1998, S. 81.

Kriminalität im Internet; Das Internet wird zusehens Schauplatz und Mittel krimineller Handlungen. Fall aus dem Jahre 1998. Die französische Polizei hatte im Februar des Jahres einen Neonazi-Ring ausgehoben, der über das Internet Todesdrohungen gegen prominente Franzosen verbreitet hatte. Die entscheidende Spur konnten die Ermittler aufnehmen, als sie die von Kanada aus verbreitete Internet-Homepage einer Gruppe mit dem Namen „Charlemagne Hamerskin“ entdeckte. Auf dieser Homepage wurde rassistische und antisemitische Propaganda verbreitet.
Quelle: *Stuttgarter Zeitung,* 19.2.1998

>>4

Tamagotchi; siehe Artikel in *c't* 7/1997, Seite 55

Auszug aus **Lizenzvertrag** zum Programm *WebWasher* von webwasher.com (ehemals Siemens AG): "Es wird darauf hingewiesen, daß nach dem Stand der Technik es nicht möglich ist, Computersoftware so zu erstellen, daß sie in allen Kombinationen und Anwendungen fehlerfrei arbeitet."