Sommerloch?

Zugegeben, die Sommerausgabe der Datenschleuder liess heuer etwas auf sich warten – aber das tut der Sommer ja auch, zumindest hier in Deutschland. Wie selbiger es dann doch noch geschafft hat, ein solches Vakuum zu erzeugen, ist uns allen ein Rätsel.

Trotz dieser widrigen Umstände trudelten aber auch dieses mal wieder fleissig Beiträge in der Redaktion ein.Soviele sogar, dass wir uns kurzerhand entschlossen, anstatt zu kürzen oder gar Bildmaterial wegzulassen, einfach noch vier Seiten dranzuhängen.

Einer weiteren Expansion stehen dann allerdings deutlich höhere Druck- und Portokosten im Wege – es sei denn natürlich, ihr wärt bereit, für eine fettere Schleuder auch ein oder zwei Mark mehr hinzulegen. Was meint ihr?

Auch wenn wir dieses mal unbedingt den Urlaubsschnappschuss eines Aufklärers von Dennis abdrucken mussten: schickt uns Kabelknotenbilder! Je fieser und verknoteter, umso besser – den besten winken Abdruck und ewiger Ruhm.

Das gilt aber natürlich auch für jeden anderen konstruktiven Input! Also her mit dem Scheiss!

In diesem Sinne,

Tomster

0 7 1 - 0 0 1

Französische Gesetzeslage stellt anonymes Publizieren unter Strafe

Den gesellschaftlichen Nutzen der Möglichkeiten anonymer Kommunikation haben französische Politiker offenbar überhaupt nicht begriffen. Als Reaktion auf den vom französischen Künstler Valentin Lacanbre betriebenen Dienst altern.org, der anonym erstellte Websites ermöglichte, wurde laut Telepolis mit dem Multimediagesetz "Loi sur la communication audiovisuelle modifiant la loi" unter Androhung eines Strafgeldes in Höhe von FF 50.000 oder bis zu sechs Monaten Gefängniss ISP´s die Pflicht auferlegt, entsprechende Sendefunktionalitäten (Web, Mail, News) nur mit Vollnamen oder Pseudonymen zu betreiben. **<andy>**

Quelle: "Loi sur la communication audiovisuelle modifiant la loi du 30/09/1986". – http:// www.-legalis.net/jnet/2000/loi-audio/projetloi-fin.htm

Telepolis vom 02.07. von Florian Rötzer "Frankreich hat mit der Anonymität Schluss gemacht." – http:// www.heise.de/tp/deutsch/inhalt/te/8313/1.html

ETSI-Policy Gremium wieder aktiv

Das bereits aus Zeiten der globalen Key-Escrow Campagne bzw. der US-Amerikanischen Kryptoregulierungsversuche durch wundersame Vermehrung der britischen Mitarbeiter bekanntgewordene "ETSI-Policy" Gremium ist offenbar wieder aktiv. Nachdem die europäische Telekommunikations-Sicherheit zuletzt durch Errungenschaften wie die einseitige GSM-Authentifizierung unsichere Standards gesetzt hat, sind jetzt verschiedene Standards zur Überwachung von Mobilfunknetzen, des Internets bzw. packetvermittelten Netzen etc. aber auch z.B. des UMTS-Standarts (dessen Protokolle an- und für sich erst seit kurzem vorliegen) aufgetaucht.

Abgesehen von dem notwendigen Hinweis, daß diese europäischen technischen Standards in vielen europäischen Ländern noch gar keine Gesetzesgrundlage haben (in Deutschland z.B. steht die Erstellung / Veröffentlichung / Verabschiedung einer Telekommunikationsüberwachungsverordnung (TKÜV) noch immer aus), spricht vor allem die zmd. bei der für das Internet zuständigen Richtlinie (TR 101 750) inhaltliche Kompatiblität zur jüngst in Kraft getretenen amerikanischen CALEA-Richtlinie (Communications Assistance for Law Enforcement Act). Aufgrund der Komplexität der hier angesprochenen Dokumente steht eine detaillierte Analyse noch aus.

Da die dieses Dokument beschreibenden Bits derzeit unter einem virtuellen Vermehrungsverbot namens Copyright stehen, geben wir hier mal keine URL an. **<andy>**

- ***ETSI TS 101 509*** *Digital Cellular Telecommunications System; Lawful Interception*
- ***ETSI 201 671*** *Telecommunications Security; Lawful Interception (LI)*
- ***ETSI EG 201 781*** *Intelligent Networks (IN); Lawful Interception (LI)*
- ***ETSI ES 201 671*** *Telecommunications Security; Lawful Interception (LI) Handover interface for the lawful interception of telecommunication traffic*
- ***ETSI TR 101 750*** *Telecommunications and Internet Protocol Harmonization over Networks (TIPHON); Security; Studies into the impact of lawful interception*
- ***ETSI TS 133 107*** *Universal Mobile Telecommunication System (UMTS); 3G Security; Lawful interception Architecture and functions*

Zur CALEA-Richtlinie findet sich viel Material bei http://www.eff.org

"Dabei handele es sich nicht um Wirtschaftsspionage, sondern um Aktionen zu Gunsten des wirtschaftlichen Wohls des Landes."

Im Verlaufe des Auftritts von Duncan Campbell im Rahmen einer nicht-öffentlichen Sitzung des Bundestags-Ausschusses für europäische Angelegenheit am Mittwoch dem 05.07. in Berlin wurde abgesehen von erheiternden Formulierungen einiger Vertreter des Innenministeriums auch mal wieder etwas zum Thema Kryptoregulierung assoziiert.

Eine Arbeitsgruppe des Europäischen Rates für Justiz und Inneres, die sich dem Thema widmet, inwieweit Bürger mit Hilfe von Verschlüsselungsmitteln oder anderen Methoden ihre privaten Kommunikation schützen können, die auf Anregung von Bundesinnenminister Schilly eingerichtet wurde, muß nach Ansicht von Schilly dabei auch das Interesse der Strafverfolgungsbehörden berücksichtigt werden.

Auch wenn der brandenburgische Datenschutzbeauftragte Dix zurecht kommentiert, daß damit nicht automatisch die Interessen der Geheimdienste gemeint seien, so muß man allerdings anmerken, daß die derzeitigen Aktivitäten der amerikanischen Regierung ja auch nicht mehr "global key escrow" wie 1997 heißen, sondern nunmehr unter der Formulierung "lawful interception to telecommunication" tituliert werden.

Insofern ist der Hinweis auf die 2001 ablaufende Zwei-Jahres-Frist die in den deutschen Kryptoeckwerten von 1999 festgelegt wurde, sicherlich notwendig. **<andy>**

Quelle: http://www.heise.de/tp/deutsch/special/ech/6895/1.html)

Cybercrime Convention: Überwachungsstaat jetzt

Viel Arbeit wird uns dieses Jahr voraussichtlich noch die vom Europäischen Ausschuss für Strafrechtsfragen (CDPC) bislang in einer "deklassifizierten öffentlichen Fassung" vorliegende Entwurf der "Cyber Crime Convention" (Entwurf eines Übereinkommens über Datennetzkriminalität) machen.

Das grobe politische Konzept zur Bekämpfung der zunehmenden "Computerkriminalität" im Bezug auf die wahrgenommenen Delikte wie Denial of Service Attacks etc. ist dabei ein Gespann aus dem Verbot von Sicherheitsinstrumenten (alle Instrumente, die sich als Angriffswerkzeuge zur Durchführung oder Vorbereitung von Straftaten nutzen ließen) und verschiedenen – im veröffentlichten Dokument nicht spezifizierten – Überwachungsmaßnahmen. Bei den entsprechenden Paragraphen 18 und 28 steht einfach nur "under discussion".

Mittlerweile gibt es eine deutsche Version und die Antwort des Parlamentarischen Staatssekretärs im Bundesministerium der Justiz auf einen Fragenkatalog von MdB Tauss auf die deutsche Einschätzung des Dokumentes. Sie ist erwartungsgemäß inkompetent. Kommt die Tage auf *www.ccc.de/CRD/*. **<andy>**

Quelle: http://conventions.coe.int/treaty/en/projects/cybercrime.htm

Kategorie "Aua!"

```
> telnet mail.surf1.de
Trying 194.25.165.21...
Connected to mail.surf1.de.
Escape character is '^]'.
Dies ist ein Mailserver.

Mit anderen Worten: Unsere Rechtsabteilung findet es
sehr interessant, was Sie so mit unserem Mailserver
machen wollen.

Bis demnächst, vor Gericht

Hochachtungsvoll,
Ihre Silyn-Tek Communications GmbH
```

Subject: Dokumentenschutz

Hab Eure Seiten durchforstet und durchkämmt trotzdem wurde meine Frage nicht beantwortet die klein aber fein ist!! Ich suche einen Rat, wie ich ein HTML Dokument schützen kann, also das man im Browser den Quelltext weder anzeigen lassen, noch abspeichern lassen kann! Ich hoffe auf Eure Hilfe und Ratschläge…

Das dürfte kaum gehen. Da der Browser den HTML Text ja benötigt, um ihn darzustellen und dieser über das HTTP Protokoll angefragt und ausgelierfert wird, müsste sich a) der Browser weigern, den Quelltext anzuzeigen. Dieses "Feature" bieten aber (Gott sei Dank) keine mir bekannten Browser. b) der Server keine HTTP Anfragen von Browsern != a) beantworten. Jede Anfrage per telnet hebelt deinen Schutz sonst aus. Man könnte jetzt natürlich durch Protokoll/Browser/Servermodifikationen versuchen, einen Pseudoschutz aufzubauen. Selbiges ist aber immer Pfusch. Die Daten sind öffentlich, wieso sollte dann niemand den Source sehen? Hast du Angst, dass jemand was aus deinem Javascript lernt? **<Frank Kargl>**.

Real Hackers do it with Security…

hallo, vor kurzem habe ich mir übers Netz eine nette kleine Sache eingefangen und werde sie nicht mehr los. Bei jedem Hochfahren des Rechners erscheint u.a. auch ein "fliegender Penis" der meiner Maus nachjagt. Norton AV findet nichts, ein Scandisk brachte keinen Erfolg, Funktion "Suchen mit Datum" ebenfalls nicht.

Wie werde ich diesen Schwachsinn wieder los???

Ja, gute Frage. Versuchs doch mal beim Urologen… Also na gut, Ernst beiseite, Neuinstallieren hilft. Tut mir jetzt echt leid, daß es dich so böse erwischt hat, aber ich kann da nicht ernst bleiben und verkneifen kann ichs mir auch nicht. Das ist einfach zu lustig. Vielen Dank, du hast einen einfachen Hacker sehr glücklich gemacht. **<Steini>**

Werbegeschenke?

Bestehen irgendwelche Probleme mit der Polizei, Staatschutz oder anderen Behörden wenn ich Mitglied werde im CCC?

Definiere "Probleme". Der CCC ist jedenfalls nicht illegal, falls Du das meinst.

Meine weitere Frage: werden auch irgendwelche Maßnahmen ergriffen um laufend neue Mitglieder zu werben?

Nein. Wir sind kein Konzern und auch keine Partei. Wir wollen nicht expandieren. Wir wollen "Spaß am Gerät".

Ist es erwünscht, öffentlich zu werben für den Club? z.B. durch T-Shirts oder Aufkleber oder anderer Dinge?

Eher nicht. Wozu auch?

Ich würde sofort Mitglied werden, wenn alle meine Fragen konkret beantwortet werden. Ein kleine Spende würde natürlich auch rausspringen, um dann unseren Club zu fördern.

?!? Ich glaube, Du verstehst hier so einiges falsch. Nochmal: wir sind ein Verein und weder Konzern noch Zeitschriftenzirkel noch Sekte. Wir haben auch keine Akquise-Abteilung. Oder hast du schon mal Leute mit CCC Transparenten in einer Fußgängerzone Deiner Wahl gesehen, die T-Shirts und Luftballons verteilen und Leuten Mitgliedsfetzen in die Hand drücken? **<Tomster>**

Nur mit Journalisten...

Auszüge aus dem Telefonat von Prinz Ernst August von Hannover mit der Journalistin Anne-Kathrin Berger, die in der "Bild"-Zeitung behauptet hatte, er habe gegen den arabischen Expo-Pavillion gepinkelt.

Der Prinz: Ich sag das nur, damit sie sich langsam ärgern, mit mir wird nicht rumgefickt, ja? Ihr schweissdreckiger Arsch wird gefickt von mir bis ich nicht mehr lebe. ja?

Die Berger: Reden Sie mit allen Menschen so, Königliche Hoheit?

Der Prinz: Nein. Nur mit Arschlöchern wie Journalisten. Nur mit Journalisten. Sie kennen mich ja. Sie wissen, was ihre Scheisszeitung macht. Und wenn Sie ihre Zeitung verkaufen wollen, dann machen Sie das nicht auf meine Kosten […]

Der Prinz: Schneiden Sie mit! Schreiben Sie morgen in der Zeitung: Der Prinz von Hannover ist wütend, weil die Bild-Zeitung wieder mal Scheisse macht. Ja? Scheisse.

Die Berger: Wir berichten über die Ereignisse, wir machen ja keine Ereignisse.

Der Prinz: Es gab keine Ereignisse. Wenn Sie sagen – und ich lese in den Zeitungen, das wird mir zugeschickt aus der ganzen Welt – ich würde einen Rassenhass kreieren in Deutschland wegen Türken und Deutschen, ja? Wissen Sie, was Sie kriegen? Sie wissen garnicht, was ihnen blüht, Frau Berger. Keep your Arsch together. Sie werden seitlich gefickt. [...]

Die Berger: Ich wusste garnicht, dass man so spricht in Königlichen Kreisen. Haben Sie aufgelegt?

Der Prinz: Sie machen alles kaputt in Deutschland.

Die Berger: Machen Sie denn alles richtig?

Der Prinz: Sie mit Ihrem fetten Arsch. [...]

Der Prinz: Wir finden morgen raus, wo das Bild gemacht worden ist. Und dann gibt's *Superaction.*

Die Berger: Was gibt's dann?

Der Prinz: Dann gibt es eine Action, das glaubst Du garnicht. Denn wissen Sie was, wenn die Türken sagen, ich habe ihr Ding bedingst äh... ich weiss nicht, wie beschuldigt, ich habe da reingepinkelt, Frau Berger, Sie wissen garnicht, was für ne Scheisse Sie machen.

Die Berger: Und was dann?

Der Prinz: Wie, was passiert dann? Also schreiben Sie mit, telefonieren Sie mit. Ich muss das noch ganz laut sagen, Ihre Fotze, Ihr dreckiges Arschloch wird so gefickt, das glauben Sie garnicht. Okay? [...]

Die Berger: Vielleicht sollten Sie doch mal mit dem Chefredakteur sprechen. Dazu sollte Ihr Mut reichen. [...]

Der Prinz: Sie haben mir überhaupt nichts zu sagen. Sie sind ein Stück Dreck. [...]

Quelle: Internet

0 7 1 - 0 0 5

Y2HACK - die erste Hackerkonferenz in Israel

Andy Müller-Maguhn <andy@ccc.de>

Der Kontakt kam per E-Mail von der Organisatorin Neora, einer in Tel Aviv ansässigen Journalistin, die sich in Israel um Cyberkultur und ähnliches kümmert. Sie kam durch die europäischen Aktivitäten von HEU, HIP und Chaos Camp auf die Idee, doch einmal die in ihrem Land vorhandene Hacker-Szene etwas zusammenzuraufen.

In einem Land, dessen Wehrpflicht schlicht jedes menschliche Wesen erfasst und das durch einen nicht unerheblichen Militär- und Sicherheitsapparat aufrechterhalten wird, ist das allerdings so eine Sache.

Vorweg: Zum Staatswesen Israel und zu den dortigen Konflikten möchte ich mich mangels detaillierter Kenntnis nicht wirklich äußern. Allerdings ist es aus der Perspektive von außerirdischen oder europäischen Hackern wohl nicht unwichtig, das Staatswesen Israels zu skizzieren, um zu begreifen, warum so viele Computersicherheitsprodukte aus Israel kommen, warum das Hacken von Computern, genauso wie das Ausspähen von Daten aus Computern und die Ausführung systematischer Angriffe auf die Verfügbarkeit von vernetzten Rechnern dort quasi zur militärischen Grundausbildung gehört, die dort Frauen und Männer mit Computertalent genießen.

Der Staat Israel beruht – wenn ich das alles richtig verstanden habe – zunächst einmal

nicht nur aus den israelischen Staatsbürgern, sondern vor allem aus einem gigantischen Militärapparat, der zu einem Großteil von den USA finanziert wird und dazu dient, das Staatsgebiet Israels im Rahmen der lokalen Territorialstreitigkeiten mit Palästinensern bzw. Arabern und den anderen ethnischen Gruppen, die dort ursprünglich wohnten, zu verteidigen bzw. aufrechtzuerhalten.

Dazu gibt es dann noch ein Bündel von Bombenattentaten auf Schulbusse von der einen Seite und Flugzeugbombardierungen auf der anderen, an die man sich offenbar alternativ zu einer Lösung des Konfliktes einfach gewöhnt hat. Das militärische Staatswesen Israels umfasst insofern nicht nur alle BürgerInnen ab 18 Jahren (die, mit Ausnahme von Müttern mit Kindern, regelmässig zu Übungen herangezogen werden), sondern auch den Charakter des Landes, in dem es neben dem Militär dann folgerichtig auch noch die zuliefernde Rüstungs- und Sicherheitsindustrie gibt.

Tel Aviv ist eine schöne, bunte, schnelle und dreckige Stadt, in der man sich - abgesehen von der partiellen Präsenz von Uniformierten mit Maschinengewehren - wie im Westen fühlen kann; die Eingeborenen reden selbst leicht ironisch davon, so etwas wie der 52. Staat Amerikas zu sein. Die Organisatorin Neora entstammt dabei eher aus einem Umfeld, wo man durchaus Leute antrifft, die aus meiner subjektiven Sichtweise einen vernunftbegabten und vor allem halbwegs entspannten Eindruck machen, sich an Elektronik, elektronischer Musik und Naturprodukten erfreuen und sich über ihren Kulturraum auch eher amüsieren als sich an den diversen Konflikten zu beteiligen. Diese Leute schienen mir – auch wenn bzgl. der Konferenz eher die Minderheit waren – durchaus kompatibel zu unseren Teilnehmern auf Congress und Camp zu sein.

Als Neora die Idee zur Organisation dieser ersten Hacker-Konferenz in Israel hatte, suchte sie sich zunächst die notwendigen Ressourcen zusammen. Von Termin und der Location war es sozusagen eine Begleitveranstaltung zur dort gerade stattfindenden Internet World; es handelte sich um eine Art Zeltbau mit Wiese und einem davor aufgebauten Zeltpavillon. Sponsoren aus der Internet- und Sicherheitsindustrie finanzierten nicht nur die Veranstaltung, deren Logistik dann letztlich von einer (halbwegs) professionellen PR-Firma durchgeführt wurde, sondern auch durchgehende Umsonst-Versorgung mit Cola, Pizza und Kaffee für die Teilnehmer, um im Gegenzug Werbeplakate aufzuhängen, Produkte vorzuführen und Personal zu aquirieren ("hire the hacker").

Zwischen Planung und tatsächlichem stattfinden der Veranstaltung gab es dann noch ein größeres Problem, als eine Abgeordnete des israelischen Parlaments das Innenministerium ersuchte, die Veranstaltung zu verbieten. Mit der Begründung "Hacken sei ja schließlich illegal und dementsprechend müsse ja auch eine Konferenz der Hacker illegal sein" und: "Schließlich würde man auch nicht einen Kongress von Dieben zulassen".

Dieser politische Vorstoß kam übrigens von einer Angehörigen der sogenannten "Linken" in Israel und führte zu einer Debatte im Parlament, die Neora zwar nicht besuchen durfte, jedoch mit einem ihr bekannten Abgeordneten während der Sitzung (!) chatten konnte, so daß sie ihm die Argumente für die live im Fernsehen übertragene Sitzung übermitteln konnte; davon wurde auf der Konferenz ein Video gezeigt. Schließlich konnte sie Ihre Argumentation in das Bewusstsein des Parlaments hacken und so die Konferenz zur Förderung von Transparenz und Bewusstsein über Risiken und Chancen von Technologie veranstalten. Für die

Presse wurden dann noch extra Handzettel gereicht: "What are hackers", "The convention objectives" etc. um etwaige weitere Mißverständnisse zu vermeiden, die offenbar in einem Land wie Israel schnell fatale Folgen haben können.

Ich war dort eingeladen, den ersten Tag mit einem Überblick über die Unsicherheit und daraus resultierenden Spannungsfeldern im Internet sowie Lösungsansätzen zu beliefern und am zweiten Tag etwas zur globalen Rolle der Hacker, ihrer Motivationen und vor allem Abgrenzungen zu anderen Gruppen, sowie den daraus resultierenden Differenzen zu referieren.

Durch die unrühmliche Anwerbung mit Todesfolge des Berliner CCC-Hacker Tron durch ein in Israel ansässiges Unternehmen, welches zum Imperium des Medien-Mogul Rupert Murdoch gehört, hatte ich natürlich auch gewisse Sicherheitsbedenken und daraus resultierende Obacht bei dieser Reise. Aus meiner ursprünglichen Planung, mir auch noch einige Tage Tel Aviv, Jerusalem und andere Teile von Israel anzugucken, wurde dann aus merkwürdigen Ereignissen und praktischen Erwägungen ein auf den Besuch der Veranstaltung reduzierter Besuch.

Das Ganze fing an, als ich am Montag morgen im Flughafen Berlin-Tegel via Frankfurt nach Tel Aviv fliegen wollte und das nicht konnte. Die freundliche Dame vom Lufthansa Schalter fragte mich, ob ich mit jemandem zusammen fliegen würde; bis Frankfurt könne sie mich einchecken, aber nicht bis nach Tel Aviv, weil ich von dort eine "combined booking" hätte. Den ersten Flug habe ich daher sausen lassen; soviel Luxus muss sein, daß, wenn man schon berufsbedingt mit Geheimdiensten zu tun hat, man die nicht auch noch im Flugzeug neben sich sitzen haben muss.

Mit einem späteren Flieger kam ich in Tel Aviv in der Nacht an, das Einreisen war problemlos. Auch so eine Eigenschaft von Israel, die man im Hinterkopf behalten sollte: die paranoide Sicherheitskontrolle findet dort nicht bei der Einreise, sondern bei der Ausreise statt. Allerdings ist es aufgrund der bereits erwähnten Umstände wohl auch etwas anderes, ob man bei der Anreise angibt, in Tel Aviv eine Konferenz zu besuchen, oder ob man sich das Land angucken möchte. Letzteres könnte sehr schnell zu Mißverständnissen, Empfindlichkeiten und der Notwendigkeit, sich vor den Grenzbeamten zu entkleiden, führen. Bei der Ausreise wusste ich zum Glück schon, was man falsch machen konnte. Solange man *lückenlos* nachweisen kann, wo man sich im Land befunden hat (und darunter keine Palästinenser-Gebiete etc. sind) schafft man die Sicherheitskontrolle in etwa einer Stunde. Ganz anders verhält sich das allerdings, wenn man z.B. irgendwo privat unterkommt und das nicht nachweisen kann. Ein anderer Berliner Hacker berichtete mir von vier Stunden, die er zum Auspacken seiner Sachen, Erläuterung jedweder schriftlicher Notizen und seiner Aufenthaltsorte etc. benötigte, bevor er zum checkin-Schalter gelassen wurde - und er hatte nichtmal seinen Computer dabei.

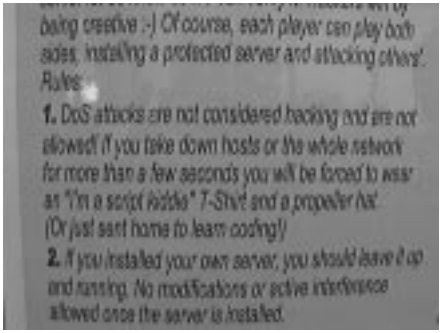
Die Datenleitungen des Landes werden offenbar in ähnlichem Maßstab beobachtet, wenn auch Datenpakete zur Ausreise aus Israel keine Bestätigung der Sicherheitskontrolle benötigen. Verschlüsselung ist für normale Bürger eigent-

lich verboten, de fakto findet aber keine feststellbare Kontrolle statt. Bestimmte mit Kryptographie und anonymem Zugang zusammenhängende Vorträge fehlten trotzdem auf dem Congressprogramm.

John Draper (aka Capt. Crunch, der Mann mit der Cornflakespfeife), war bereits einen Tag vorher angereist und informierte mich beim Frühstück über seine Befragung eines israelischen Anwalts, was er denn im Rahmen eines Vortrage so sagen könne und was nicht. Es sei ganz einfach: man könne in Israel alles sagen; es sei denn, es könne die Stabilität des Staates Israel gefährden. Sollte man dies allerdings ungeschickterweise z.B. durch Erörterung von bestimmten Technologien tun, könne man mit seiner umgehenden Inhaftierung und drakonischen Strafen rechnen. Das konnte ich von Draper zum Glück vor der Konferenz im Hotel erfahren; dort gab es auch praktischerweise gleich neben dem Frühstücksraum einen Atombunker.

Die eigentliche Konferenz bestand neben dem offiziellen Programm (siehe *www.2600.org.il*) und den informellen Gesprächen bei Pizza und Cola am ersten Tag aus einem erheblichen Presseansturm, denn die Konferenz stellte aufgrund der erwähnten gesetzlichen Rahmenbedingungen eine Sensation bzw. eine mutiges Unterfangen für dortige Begebenheiten dar.

Bei 25 Grad im Schatten (das ist dort der so genannte Frühlingsanfang) waren dann im besagten Zeltbau ungefähr 250 Menschen versammelt; ein Drittel zwischen 14 und 18 (zu erkennen daran, daß sie noch nicht dem militärischen Drill unterworfen waren), etwa ein Drittel zwischen 18 und 30 (das sind wahrlich keine Chaoten, eher alles Jungs, die schon in der Industrie oder für die Dienste schaffen) und ein Drittel mehr oder weniger ältere Onkels, die entweder von Unternehmen oder von den


being creative :-) Of course, each player can play both sides: installing a protected server and attacking others!
Rules:
1. DoS attacks are not considered hacking and are not allowed! If you take down hosts or the whole network for more than a few seconds you will be forced to wear an "I'm a script kiddie" T-Shirt and a propeller hat (Or just sent home to learn coding!)
2. If you installed your own server, you should leave it up and running. No modifications or active interference allowed once the server is installed.

Diensten auf Personal- und Informationsaquise unterwegs waren. In der mittleren Gruppe waren sogar ein paar Hacker mit gesellschaftlichem Anliegen, auf die ich aber nicht weiter eingehen möchte, weil sie sich dort zwangsläufig als eine der genannte Gruppen tarnen mußten und ihre Anliegen nur unter sehr vorgehaltener Hand diskutieren konnten.

Da die israelischen Hacker selbst ja noch nicht organisiert sind, mußte ich daher als Vertreter der Hacker-Szene am ersten Tag eine Unmenge von Interviews für die israelische und internationale Presse geben, so daß ich dem Konferenzprogramm kaum lauschen konnte. Für die lokale Szene war es wichtig, die Presse gut zu behandeln und sich mit einer offenen Herangehensweise zu präsentieren; auch wenn das ursprünglich geplante Kameraverbot am ersten Tag darunter *deutlich* litt. So schanzten Sie mir etliche Fernsehteams und Zeitungsreporter zu. Den Veranstaltern war es offenbar sehr recht, daß ich Ihnen die nicht unheikle Aufgabe der Kommunikation mit der Presse zum Teil de fakto abnahm.

Pressearbeit für eine Hackerkonferenz in Israel als Deutscher zu machen erfordert allerdings echtes Fingerspitzengefühl, auch weil einige Journalisten natürlich irgendeine Stellungnahme zur Sichtweise des Landes u.ä. vor laufender Kamera wollten, was ich angesichts

0 7 1 - 0 0 9

meines Überlebenstriebes mit der gebotenen Sensibilität freundlich aber bestimmt wegreden mußte. Ich habe es bevorzugt, nur Angaben zur Sache mit latenter Betonung auf europäische bzw. globale Sichtweise zu tätigen.

Vom ersten Tag habe ich zumindest einen umfassenden Eindruck von der Diskussion gewonnen, die als Anschluss zu meinem Vortrag über die Notwendigkeit von überprüfbaren Sicherheitsprodukten durch Open Source u.ä. entstand. Dabei teilte sich die Meinung in Unterstützer dieser Herangehensweise und solche, für die der Gedanke nach Offenlegung zwar interessant, aber doch deutlich gewöhnungsbedürftig war. Diese Mentalität kennt man in unseren Breitengraden eigentlich eher von den Vertretern der Sicherheitsindustrie; aber die Differenzierung zwischen "Hackern" und "Industrie" bzw. Regierung steht in Israel wohl noch aus.

Diese Differenzierung war auch das Thema des Vormittags-Panels am zweiten Tag, daß ich mit einer etwas ausführlicheren Gedankensalat-Präsentation zum Thema "Hacker, Motivationen und andere Gruppen" eröffnen durfte. Anwesend während des "Hackers vs. Industrie vs. Government" Panels war dabei ein Vertreter eines auch als Sponsor der Konferenz auftretenden ISP´s sowie der bereits erwähnte internetphile Abgeordnete des israelischen Parlaments (dem es - offenbar gegenüber der anwesenden Presse - wichtig war, zu betonen, daß er mit offizieller Erlaubnis des israelischen Innenministeriums anwesend war).

Neben der Abgrenzung von Hackern zu Kriminellen, Terroristen, Spionen und Kriegern (die alle durch die Benutzung des Computers nicht zu Hackern werden) ging es mir hier vor allem um die Ansätze, die Entwicklung mit einer eigenständigen Rolle im Sinne von Informationsfreiheit, Beschäftigung mit Restrisiken und Technologiefolgen zu begleiten.

Der Parlamentsabgeordnete (Michael Eitan) schlug daraufhin vor, die Tätigkeit von Hackern doch durch eine staatliche Lizenz zu regulieren, um so die gesellschaftliche Nützlichkeit sicherzustellen. So könne man dem Konflikt zwischen "Privacy" (Privatsphäre) und "Full Disclosure" (volle Transparenz) entschärfen. Dazu muß man allerdings auch sagen, daß Herr Eitan (wie wir es in Deutschland auch kennen) nur zu seinem Panel kam und insofern hier m.E. einen Konflikt beschreibt, den es nur sehr partiell gibt (vgl. "Private Daten schützen, öffentliche Daten nützen", Chaos Communication Congress 1987? Ergänzung zur Hackerethik).

Trotzdem war die Diskussion aufschlußreich, gerade weil auch viele der Teilnehmer sich eine unabhängige Rolle vom Arbeiten für die Regierung in Form von Militär, Geheimdienst oder Sicherheitsindustrie wünschten, dies aber offensichtlich unter den gegebenen Umständen nicht unbedingt selbst postulieren konnten.

Richtig spannend wurde es dann in der Mittagspause vor der Vorstellung des Internet Auditing Projektes. Dies lag zum einen an der minütlich steigenden Nervosität der Organisatoren, hatten Sie doch in den letzten Tagen vor der Konferenz noch einmal den gesamten (!) israelischen IP-Domainbereich mit einem dreistufigen Scan (grob, fein, haargenau) nach bekannten Sicherheitslücken gescannt. Die ursprüngliche Planung, das Ergebnis inklusive der Details anlässlich der Konferenz hier der Öffentlichkeit vorzustellen (nach dem Motto "Israel hat ein Sicherheitsproblem") sorgte anlässlich der mittlerweile aufgetauchten juristischen Bedenken für heftige Diskussion, da in Israel bereits der Versuch eines Computereinbruchs strafbar ist. Nun war man sich angesichts mangelnder Erfahrung des offensiven

Auftretens noch nicht über etwaige Konsequenzen bzw. Reaktionen im Klaren.

Die im Rahmen dieser Auseinandersetzung geführten informellen Gespräche möchte ich aus Rücksicht hier nur grob und anonymisiert wiedergeben. Es gab im wesentlichen zwei Fraktionen bei der Diskussion, die mich netterweise in Ihre Ansichten mit einbezogen. Die einen machten sich keine strafrechtlichen Sorgen - weil sie ja sowieso für die Regierung arbeiteten und solche Scans schließlich zum Arbeitsalltag der israelischen Regierung bzw. des Militärs gehörten (!) - und zwar nicht nur im Bezug auf den israelischen IP-Raum. Sie fragten sich allerdings, inwieweit etwaige betroffene Firmen etc. den Scan als Vorbereitung eines Angriffs werten können und zivilrechtlich für Streß sorgen könnten, hatte man doch kein Spoofing o.ä. verwandt, sondern zuordnungsbare IP-Nummern.

Die andere Fraktion fasste Ihre Ansicht über das Projekt mit den Worten "I am not impressed" zusammen. Das sei doch schließlich Kinderkacke und würde keine wirklichen neuen Informationen zutage fördern, wenn man mit den Ergebnissen der Öffentlichkeit erzählt, das Internet sei unsicher. Mit der Fraktion habe ich mich dann noch über die Frage unterhalten, was sie denn beeindrucken würde. Da kamen dann ein paar interessante Geschichten, wie z.B. der Einbruch in das Intranet eines weltweit bekannten Firewallherstellers in Israel, dessen Computer dann auf einmal nachts damit beschäftigt waren, bestimmte IP-Nummern mit mehr oder weniger Agenten Tools abzuscannen. Die dabei gefundenen Werkzeuge würde man wohl als intelligente Agenten bezeichnen, die keinen Eindruck zivilen Ursprungs machten. Da gibt es wohl die Tage noch etwas mehr Informationen.

Insgesamt kann man die Situation in Israel wohl mit den Worten "arbyten unter erschwerten Bedingungen" zusammenfassen. In einem Land, in dem es keinen Datenschutz gibt, staatliche Überwachung eine Selbstverständlichkeit und die allgemeine Wehrpflicht eine latente Einbindung aller Menschen in das militärische Staatswesen mit sich bringt, mußte ich über die Frage der Organisation von Hackern auch erst einmal nachdenken. Ich habe dort echt nette Jungs kennengelernt, leider reicht nur meine Sympathie nicht für die Organisationen, für die sie arbeiten. Immerhin haben mich auf dieses Problem etliche von sich aus hingewiesen.

Letztlich habe ich Neora zur Organisation einer Hackerszene empfohlen, vielleicht erstmal mit einer Gruppe von Frauen mit Kindern und den unter 18 jährigen anzufangen um so die Konflikte mit staatlichen Strukturen einzugrenzen.

0 7 1 - 0 1 1

VCFe 1.0 - "Vintage Computing Festival Europe"

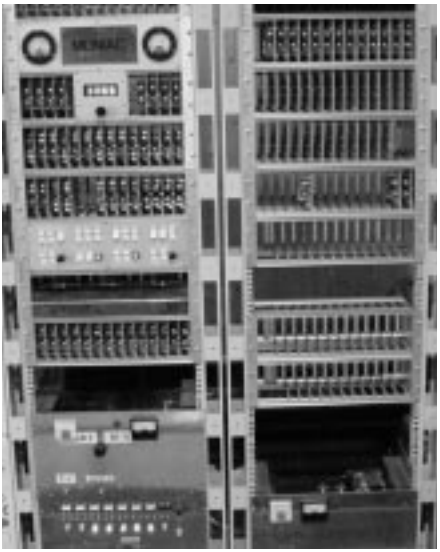
von Hans Hübner <hans@berlin.ccc.de>

Unter diesem Titel trafen sich im April 2000 etwa hundert Computer-Enthusiasten eher fortgeschrittenen Alters in München und zeigten die erfüllten und unerfüllten Träume ihrer Jugend. Die VAXbusters konnten bei so einem Ereignis nicht fehlen und reisten mit einem Haufen Hardware an.

Aus fast jedem Dorf der einst so vielfältigen Computergemeinde der 80er Jahre waren würdige Vertreter anwesend. ZX81, TI99/4A und VC20, Robotron und Sinclair, CP/M, Apple, Cyber und VAX waren einträchtig und außer Konkurrenz vereint und ihre Besitzer voll Schwärmerei und Spass am Gerät.

Für die meisten der alten und öffentlich ausgestorbenen Rechner-Arten scheint es irgendein Völkchen von unentwegten Liebhabern zu geben, die sich um Ihren Kultgegenstand kümmern und ihn weiter hegen und pflegen. Am kuriosesten war in dieser Hinsicht der Vertreter des ZX-Clubs, der in einem vierstündigen Auftritt eine schöne Kollektion von Original-Sinclair-Exponanten, mehrere Ausgaben eines seit den 80er Jahren bis heute erscheinenden Fanzines und Geschichten von FPGA-basierten ZX-81-Reimplementationen mit LCD präsentierte.

Zum Höhepunkt und Abschluß der ansonsten zur vollen Zufriedenheit der Teilnehmer verlaufenden Veranstaltung wurde ein Nerd-Quiz



Der MUNIAC ist ein röhrenbasierter Computer, der auf einem vollständigen Neudesign basiert. Sämtliche Logikfunktionen werden durch Röhrengatter implementiert. Die digitalen Leistungsdaten sind nur akademisch Interessant, das diskret aufgebaute, längsgeregelte Röhrennetzteil gebietet jedoch Ehrfurcht.

Konsole einer Control Data Cyber. Cyber war als Number Cruncher in den 70er Jahren unter Mathematikern sehr beliebt. Programme wurden üblicherweise auf Lochkarten zugeführt. Grafische Ausgaben erledigte ein Plotter oder diese Vektorkonsole. CDC-Systeme waren auch unter den ersten, die in Berlin über Modem-Pools verfügten und so Hackern zur Kommunikation dienten.

Auf der Symmetric 375 konnte man sich sogar per telnet einloggen. Ein login auf einer Maschine mit BSD 4.2 war so etwas wie eine Unix-Zeitreise.

Im Gegensatz zur VAX 11/750 bootete die HalfVAX ordentlich und ging mit ihrem 4.2 BSD im lokalen Ethernet online.

veranstaltet, bei der sich vier durch eine Vorausscheidung qualifizierte Teilnehmer einer Kollektion von Fragen aus der Vintage-Computing-Welt stellen durften.

Die Auswertung des Spiels erfolgte dabei durch ein eilends in Ermangelung eines funktionierenden Diskettenlaufwerks live in Maschinen-

Computertechnik "Made in GDR". Deutlich ist zu sehen, daß klassische Funkamateur- und Computertechnik in der DDR eng beieinander lagen.

Detailfoto der durch einen Sharp MZ80 betriebenen Eierbemal- und -köpfmaschine. Ein in die Maschine eingelegtes Ei wird überprüft, ob es gekocht ist, bemalt, geköpft und zusammen mit Salz und einem Eierlöffel dem Benutzer präsentiert. Spektakulär.

0 7 1 - 0 1 3

sprache programmiertes "Wer drückte die Taste als erster?"-System auf Apple II-Basis.

Die VAXbusters hatten eine bunte Kollektion von QBUS-VAXen und VAXstations am Start, von denen gegen Ende der dreitägigen Veranstaltung acht Systeme gleichzeitig in ein Local Area VAXcluster gebooted waren. Dabei spielte eine VAXstation 4000 VLC den Boot Server. Die auf den Fotos abgebildete VAX 11/750 meldete sich auf der Konsole, sie war jedoch vermutlich aufgrund von Hardwarebeschädigungen nicht in der Lage, das auf den Platten befindliche VAX/VMS 5.2 vollständig zu booten.

Eine Neuauflage der Veranstaltung im nächsten Jahr war dank der guten Stimmung Konsens.

Unten eine VAX 11/750, oben eine Symmetric 375. Letztere hiess im Hacker-Volksmund "HalfVAX", teilweise wegen ihres Namens, teilweise, weil sie auf einer VLSI-VAX-Lookalike-Architektur mit 16 statt 32 Bit Busbreite basierte.

Ein Hackertraum wird wahr. Unten im Gehaeuse die PDP11, die das oben eingebaute Halbzoll-Bandlaufwerk steuert. Die luftdruckgedämpfte Führung des Bandes ist links oben zu erkennen. Die PDP11 bootete klaglos und zog mehrfach erfolgreich unter erheblicher Geräuschentwicklung ein Band ein.

Abreise der Commodore-Familie. Mit der Sippschaft vollständig angereist, sorgte sie für sentimentale Gedanken.

First International GIMP Developers Conference

by Mitch <mitch@gimp.org>

Vom 2. bis zum 4. Juni fand in den Chaos-Räumen in der Berliner Marienstraße die erste internationale GIMP-Entwicklerkonferenz statt [1]. GIMP, das GNU Image Manipulation Program [2] ist ein mächtiges Retuschier- und Kompositionswerkzeug für Pixel-basierte Bilder, das in seiner Funktionalität mit Adobe Photoshop vergleichbar ist.

Unter den 20 Teilnehmern der GimpCon war ein Großteil der derzeitigen Core-Entwickler sowie einige Power-User und GIMP-Veteranen.

Ziel der Konferenz war es, das Design der zukünftigen GIMP Version 2.0 zu spezifizieren bzw. sich darüber klar zu werden, was man sich davon eigentlich erwartet.

Der Stand der Dinge (GIMP 1.2):

Die (bald) aktuelle stabile Version 1.2, deren Release diesen Sommer erwartet wird, weist im Vergleich zum größten "Konkurrenten", Photoshop, einige Stärken, jedoch auch Schwächen auf. Das größte Manko, nämlich die fehlende Unterstützung für den CMYK Farbraum, soll nicht verschwiegen werden. Jedoch erweist sich GIMP als Meister des RGB Farbraums und es ist wohl nicht übertrieben zu sagen, daß GIMP *das* Werkzeug zum Erstellen von WEB-Grafiken ist.

Ein GIMP-Dokument besteht aus Layers (Ebenen), einer optionalen Maske je Layer sowie einer beliebigen Anzahl von zusätzlichen Schmuckfarbenkanälen. Desweiteren gehören eventuell vorhandene Bezier-Pfade sowie die aktuelle Auswahl (Selection) zu den persistenten Informationen. Zum Bearbeiten dieser Bilder bietet GIMP etliche Retuschier- und Zeichenwerkzeuge, Farbkorrekturtools sowie verdammt viele Plug-Ins. Die Palette der Plug-Ins umfaßt zahlreiche Datei Import- und Export-Filter, einfache Pflicht-Effekte wie Weichzeichnen oder Rauschen, mächtige Tools zum Erstellen von Animationen, Clickable Imagemaps etc. Viele Plug-Ins erzeugen Bilder "from scratch" aus Fraktalen, iterativen Funktionssystemen oder genetischen Algorithmen genauso wie aus Rauschen oder anderen einfachen Operatoren, deren Resultate oft überraschend sind. GIMP ist voll über seine Plug-In Schnittstelle steuerbar, auf die verschiedene Scripting-Interfaces aufsetzen: Teil von GIMP 1.2 ist Script-Fu, das Scheme-Syntax verwendet und eine Perl-Schnittstelle, die die direkte Manipulation von Pixel-Daten zuläßt.

Den Kern von GIMP 1.2 möchte man nicht wirklich als "High Tech" bezeichnen. Schicke Dinge wie CMYK oder 16 Bit Farbtiefe sind einfach nicht vorgesehen und auf dieser Codebasis weiterzuprogrammieren wäre eine Qual. Dieser Teil wird also den Sprung nach 2.0 nicht überleben und komplett neu programmiert.

Am User Interface hat sich jedoch seit den Tagen von GIMP 1.0 (was nun immerhin schon fast zwei Jahre her ist) einiges getan: So gut wie alles ist Drag'n'Drop-bar (Layers, Brushes, Farben etc.), das Interface hat ein konsistentes "Look and Feel", Längeneinheiten (cm, inches, ...) werden durchgehend unterstützt, es gibt eine Undo-History (und übrigens beliebig viele Undo-Schritte), einen Navigations-Dialog und ein eingebautes Hilfe-System. GIMP macht ausgiebigen (aber inzwischen konsistenten) Gebrauch der Modifier-Tasten und aller drei Maus-Buttons, was die Lernkurve zu Beginn recht steil macht, jedoch dem geübten Benutzer ein sehr zügiges Arbeiten ermöglicht.

Das Hauptprogramm sowie die meisten Plug-Ins verwenden vorgefertigte Widgets (so heissen die UI-Elemente des GIMP Toolkit (Gtk+ [3]) aus der "libgimpui", so daß auch hier Konsistenz gewährleistet ist. Leider ist Vorhandensein und Qualität eines Previews der Willkür des einzelnen Plug-In Autors überlassen.

The Future (GIMP 2.0):

GIMP 2.0 wird kein monolithisches Programm mit einer einzelnen Plug-In Bibliothek mehr sein, sondern eine ganze Reihe von Libraries für die verschiedenem Funktionalitäten des Kerns, der Interface-Elemente und der Plug-In-Kommunikation, für die die eigentliche Anwendung "nur" noch ein ein schönes gemeinsames Interface bereitstellen muß.

Den Umgang mit Bilddaten wird die "Generic Graphics Library" (GEGL) [4] übernehmen. GEGL abstrahiert vom verwendeten Farbmodell und der Farbtiefe (8 Bit, 16 Bit, float, double) und stellt generische Datentypen wie "Channel" oder "Color" zur Verfügung. Aus den mit diesen Typen implementierten Algorithmen erzeugt ein Code-Generator den eigentlichen C-Code, also eine Vielzahl von an die verschiedenen Datenformate angepaßter Funktionen. Auf dieser Ebene wird es auch möglich sein, Optimierungen z.B. für MMX oder AltiVec einzubauen *ohne* sie für jeden Algorithmus von Hand hacken zu müssen.

Was in GIMP 1.2 ein einfacher Layer-Stack ist, der über "Layer Modes" (Normal, Combine, Difference, ...) zusammengerechnet wird ist, wird mit GEGL zu einer Rendering-Pipeline, die man sich wie einen Baum von Layers vorstellen kann, auf dessen Wurzel man blickt. Die Knoten des Baums sind "Operatoren", die beliebig viele Ein- und Ausgänge haben können. Die Ein- und Ausgänge der Operatoren greifen auf rechteckige Regionen von Pixeldaten zu, den Kanten des Baums. Jede Kante (mit den bisherigen Layers vergleichbar) kann ihre Daten intern als Pixel, Vektoren, Text oder was auch immer vorhalten und muß nur ein Interface zum Einfügen in die Rendering-Pipeline bereitstellen.

Genauso wie man seine Layer-Typen nach Belieben implementieren kann, wird das auch mit den Operatoren möglich sein. Einfache Funktionalitäten wie Farbkorrekturen oder Weichzeichnen sind ebenso möglich wie affine Transformationen oder was-auch-immer für komplexe Bildveränderungen.

Aufbauend auf diesem Kern wird die "Core" Bibliothek Objekte wie Images, Tools, Brushes etc. implementieren. Die Interfaces all dieser "High Level" Objekte sind in einer Bibliothek definiert, und haben im Core und auf der Plug-In-Seite jeweils eigene Implementierungen.

Die Implementierung dieser Objekte in der Plug-In-Bibliothek wird aus Objektbeschreibungen komplett autogeneriert. Plug-In Programmierer erhalten auf diese Weise eine vernünftige objektorientierte Schnittstelle und nicht wie bisher ein rein prozedurales Interface. Als netten Nebeneffekt ermöglicht diese Architektur auch die Wiederverwendung von UI-Elementen in Plug-Ins und eine saubere Trennung von "Model" und "View".

Durch die Exportierung der inneren Objektstruktur an die Plug-Ins wird es möglich sein, Operatoren, Werkzeuge oder komplette Layer-Typen als Plug-Ins zu implementieren. Das Design von Layern und Tools ermöglicht es, Tools speziell für eigene Layer-Typen zu konzipieren (schließlich möchte man auf einer Vektor-Layer spezielle Vektorgrafik-Werkzeuge benutzen).

Die Kommunikation zwischen der Applikation und den Plug-Ins erfolgt über CORBA, wobei die Schnittstelle zwischen den den eigentlichen Objekten und dem ORB ebenfalls aus den Objektbeschreibungen generiert wird. Der Programmierer hat also nur Gtk-Objekte vor sich und muß sich nicht mit den Untiefen von CORBA auseinandersetzen. Der Begriff "Plug-In" hat also eher historische Bedeutung, da GIMP 2.0 ein netzwerktransparentes Client-Server System sein wird. Ein weiteres Highlight ist die Parallelisierung der eigentlichen Rechenarbeit. Schließlich will man sich nicht nur eine schicke Rendering-Pipeline zusammenbauen und abspeichern, sondern die Projektion des ganzen (den Blick auf die Wurzel des Baumes) auch sehen. Wann immer ein Update der Projektion oder eines Zwischenschritts nötig ist, wird das System automatisch alle benötigten Ressourcen locken und die Operation an den Batch-Renderer weitergeben, der in einem eigenen Thread läuft. So bleibt das ganze System stets "responsive".

Zu guter letzt wird GIMP 2.0 seine Konfigurations-Daten und Bild-Eigenschaften (außer den eigentlichen Pixel-Daten) als XML abspeichern, das Undo-System wird ein Baum und kein Stack sein (man kann also auch "Undo" rückgängig machen), alle Undo-Schritte werden persistent sein und natürlich wird es alle Features haben, die die aktuelle Version 1.2 bietet.

Auf diesem Berg von Komponenten sitzt die eigentliche GIMP-Applikation und hält alles zusammen. Der Implementierung anderer GIMP-Interfaces wie einem Video-Editing System oder der Darstellung der Rendering-Pipeline als editierbaren Graph wie man es aus der wissenschaftlichen Bildbearbeitung kennt steht also nichts im Wege.

Nicht zu vergessen... GimpCon was FUN!

Mail und IRC sind ja schön und gut, aber *eigentlich* will man die ganzen Leute, mit denen man jeden Tag kommuniziert auch mal persönlich treffen. Schließlich macht das Hacken mehr Spaß, wenn man seine Kollegen kennt.

Abgesehen von diesem zwischenmenschlichen Nebeneffekt hätte es auch verdammt lange gedauert, all dies übers Netz zu spezifizieren, was wir nun in drei Tagen hingekriegt haben, und ein besonders gutes Design wäre dabei wohl auch nicht 'rausgekommen.

Last but not least möchte ich im Namen aller GIMP-Hacker deshalb der Free Software Foundation (FSF) [5] danken, die GimpCon *großzügig* finanziell unterstützt hat. Desweiteren natürlich dem Chaos für die Räume und O'Reilly für die schönen Shirts :) **<tom>**

[1] http://www.gimp.org/gimpcon/
[2] http://www.gimp.org/
[3] http://www.gtk.org/
[4] http://www.gegl.org/
[5] http://www.fsf.org/

0 7 1 - 0 1 7

Security Problems with ARCfour

by Rüdiger Weis <ruedi@cryptolabs.org>

RC4 is a fast software stream cipher designed by Ron Rivest. It is widely used e.g. in the Netscape browsers (SSL), Lotus Notes and included in many cryptographic libraries. RC4 has variable key-length.

RC4 has been published anonymously (thanks to an anonymous writer on the Cypherpunk mailing list). Because RC4 is a trademark we should call it ARCfour.

Since there is no official publication we give a short description of the algorithm *http:www.cryptolabs.orgarcfour*.

The Algorithm uses a S-box S[0],...,S[255] which contains a key dependant permutation of {0,...,255} and two counters i and j. For the initialization we use another 256 byte array K[0],...,K[255]. We fill this array by repeating the key bits. Than we initialize the S-box:

```
FOR i:= 0 TO 255 DO
    S[i]:=i;   j:=0;
    FOR i:= 0 TO 255 DO
        BEGIN
            j:=(j+S[i]+K[i]) MOD 256;
            Swap(S[i],S[j])
        END;
```

To generate a key stream byte we do following:

```
       i:=(i+1) MOD 256;
       j:=(j+S[i]) MOD 256;
       Swap(S[i],S[j]);
       K:=S[(S[i]+S[j]) MOD 256];
```

That's all.

So we can e.g. use export restricted signatures like:

```
 #!/usr/local/bin/perl -0777-- -export-a-crypto-
system-sig-RC4-3-lines-PERL
@k=unpack('C*',pack('H*',shift));
for(@t=@s=0..255){$y=($k[$_%@k]+$s[$x=$_]+$y)%256;&S;}
$x=$y=0;for(unpack('C*',<>)){$x++;$y=($s[$x%=256]+$y)%
256;  &S;
print pack(C,$_^=$s[($s[$x]+$s[$y])%256]);}sub
S{@s[$x,$y]=@s[$y,$x];}
```

Thanks to Adam Back and Malcolm Beattie.

Ok now, but that's basically just screwing around, and of course, we all know, that 40bit strong RC4 (such as used in older browsers) is not such a good idea anyway, so what's new?

Well, the cryptographic feeling says: Ron Rivest ist probably the best designer of symmetrical ciphers, but can crypto be so easy and elegant?

There have been some attacks against RC4 (e.g. Golic, Eurocrypt 97) and statistical observations (e.g. Paul Crowley, *http://www.cluefactory.org.uk/paul/*, pretty cool home-page!-), but until recently no real problems have surfaced. Until recently…

On the Fast Software Encryption 2000 in New York a ''Statistical Analysis of the Alleged RC4 Keystream Generator'' by Scott R. Fluhrer and David A. McGreW (Cisco) has been presented. They show a socalled distinguire attack which needs only 2^{30.8} byte. That‘s less than 2 GB.

What is a distinguire attack?

Somebody gives you a sequence of bits and you have to answer whether these bits are truly random bits, or the result of a stream cipher.

Why is this a good indicator oft the security of an algorithm? Because if an attacker can break a cipher, she can answer the question quite easily. If, on the other hand she does‘t know whether some bits are random or a cipher output, she has no hook to attack at all.

And think of a scenario using a steganographic filesystem. It is not a nice idea to think the friendly government employees with the rubber-hoses have an indication that there are cryptographic bits of information in your wonderful random looking 'SETI' data.

Do not use ARCFour!

RC4 is patented, trademarked, not published. The free crypto community is just starting to understand RC4 and now there is no margin of security left! So let's switch to better and free algorithms.

Netscape Users: Switch off anything except Triple DES in Configure SSL v.2. and Configure SSL menu. (Click Lock, Click Navigator, Click Configure SSL v.2 and Click Configure SSL v.3)

If there is no item for Triple DES, ask your BoH, install a new version with strong cryptography (meanwhile downloadable from Netscape directly) or use Fortify (*http://www.fortify.net/*).

Developers: Additionally to the security problems, there is an open question regarding patents, trade secrets etc. We have very strong, fast and free ciphers. E.g. Blowfish, or the AES candidates Twofish, Serpent (not really fast) and Rijndael (use at least 13 rounds). I think Blowfish is the most secure 64-bit cipher, anyway. If you need a stream cipher just use the Outer Feedback Mode (OFB). **<tom>**

Justizausschuss der EU auf dem Wege der Demokratieabschaffung.

In einem im Internet anonym publizierten eigentlich internen Protokolls der Direction "General Justice and Home Affairs" der Europäischen Kommission, die einen Treff der "Police and Customs Cooperation" vom 13. und 14. Oktober 1999 kommt die aktuelle Strategie zur Abschaffung der Demokratie zum Vorschein.

Unter Punkt C1 - 4 ist notiert zur Erhöhung der Akzeptanz von Überwachungsmaßnahmen für das Internet notiert: "The Commission, whilst noting that its position has not changed, informed delegations that a possible way to break the deadlock could be following a similar strategy as that followed in tackling the issue of Child Pornography in the Internet."**<andy>**

Das vollständige Protokoll ist unter https://www.ccc.de/CRD/CRD1999i013.html abrufbar.

Trusted Clients – the Coming Storm

by Bruce J. Bell <bruce@ugcs.caltech.edu>

While data locked in a proprietary format may be an inconvenience, it isn't a dead end for computer users; hackers can always find a way around software limitations. But what if the limitation is in the hardware?

Introduction: Paranoia strikes deep

Every now and then, I meet somebody with a particular take on the concept of free software – call it the conspiracy theory perspective. It goes like this:

"Free software is a great idea, but it's too radical for The Man. If it ever starts to catch on, the Powers That Be will buy it out. They'll make it illegal. They'll do whatever it takes to kill it."

I'm not a big fan of conspiracy theories. Delusions of persecution are the easy way out; they give us something simple to blame in a complicated world. Spinning theories is easy, hacking reality is hard. But we all have to make sense out of the noise somehow, I guess.

Anyway, free software has caught on. What's The Man gonna do about it?

In all rationality, I think we should worry. The current assaults by the recording and movie industries against MP3 and DeCSS are just the tip of the iceberg; there are bad times ahead for the Open Source community, and for cyberliberties in general.

There's no conspiracy. Nobody has a master plan to keep us from having fun. But there is a basic and irreconcilable conflict of interest between those who see computers as user-programmable devices and those who see them solely as devices for delivering their content to their consumers.

We have a fundamental paradigm shift on our hands, and it's going to get us into trouble. Since computers are user-programmable devices, trying to treat them like just another consumer-electronics device is a recipe for disaster.

The media industries facing the prospect of convergence don't see this conflict yet. They'll find their way to it eventually, though – by sheer instinct, by trial and error, by brute force and ignorance. We have some time, but the

Open Source community needs to prepare now to control the damage to come.

Brave GNU world

Richard M. Stallman (RMS), the free software movement's prophet crying in the wilderness, isn't above speculation; check out his right-to-read story. I don't always agree with RMS, but he's got something important here.

"The Right to Read" is a worst-case scenario in which established commercial interests have instituted comprehensive and Draconian hardware-enforced copy protection for all possible forms of intellectual property. "If this goes on" is a long tradition in science fiction, and the usual hope is that following a trend to its logical conclusion in fiction will help us avoid the problems it would cause in reality.

However, the established interests in question would certainly consider the regulatory regime in the story to be the best case, and dismiss RMS's dystopian presentation as blatant propaganda from a bearded revolutionary.

Not everyone will follow why this worst case is supposed to be so bad, or how we might get there from here. It's hard to explain why without a better example.

Enter The Man

Today, my favorite examples of established interests out to screw us all over are the recording industry and the movie industry.

The players in both industries are old-media cartels, whose members dominate production and distribution in their respective markets. These cartels are wealthy, organized, and thuggish, and have the motive and the means to do real damage. They have a lot of practice screwing people over.

These industries routinely herd national legislatures to do their bidding. The recording industry has managed to tax consumers and funnel the money directly to their companies. When originally faced with the prospect of digital audio, they killed digital audio tape (DAT) as a consumer medium in the US, and they don't see why computers should be any different.

Those nasty technical issues

The crack of Microsoft's Windows Media Audio format (WMA) demonstrates some of the problems awaiting old-media interests in their quest to protect their copyrights. Rather than try to figure out how WMA is encoded, "unfuck.exe" just saves the output of the decoder before it's sent to the sound card.

For any audio format, the media player has to decode the data to plain, uncompressed digital audio before sending it to the sound card, so this attack will work on any proprietary decoder program.

The more recent crack of DVD's Content Scrambling System (CSS) demonstrates the more general problem. A loose association of programmers reverse-engineered a commercial software DVD decoder, re-implemented the decryption algorithm, and broke the lame 40-bit code used by CSS. Jon Johansen, a 15 year old from Norway, wrote the simple playback-enabling utility "DeCSS".

The technical reality is that any software-based copy protection is just security by obscurity, subject to reverse engineering. Any player popular enough to make the effort worthwhile will be reverse-engineered.

If it's not practical to stop individual users from copying media over the net, it won't be any easier to stop distribution of "enabling tech-

nology" – software used for unauthorized conversion, distribution, and performance of digital media. If the Soviet Union couldn't stamp out samizdat when all the underground had was typewriters, what chance do American corporate interests have against networked computers?

It isn't even practical for old-media to ignore computers altogether. Even if computers didn't already have CD and DVD drives, the ever-decreasing cost of hardware is driving convergence of media, communications, and conventional computer functions into general-purpose appliances. If old-media companies want to stay in business in the new millennium, they will deal with computers.

It seems the position of the old-media cartels is to accept computers as media players only if the computers act like other consumer media players, with barriers against unlimited copying and transmission of digital media content. Only then will they be able to protect their legal rights from being violated.

Unfortunately for them, the basic function of computers is to transmit, copy, and process digital data. As long as computers are user-programmable, there will be no effective barrier to copying digital media. It doesn't matter what old-media is willing to accept if their legal rights are unenforceable.

Let me be clear: I do not advocate breaking copyrights just because we can. Although the recording and movie industries don't have much room to talk about economic justice, they raise a moral point that those who create music and movies deserve compensation for their efforts.

However, regardless of what anyone advocates, people will copy anyway, because they can. And trying to enforce the unenforceable is not just futile, it's destructive.

Who are these guys?

The recording and movie industries aren't the only old-media groups with an interest in computers, but they're important because they're the first to make a serious attempt at imposing their will on the Net. Future battles will rely on the precedent, both legal and practical, set by these conflicts.

Who makes the decisions for these industries, and what do they want?

They want money, of course – but more than that, they want control. The old-media cartels are accustomed to controlling their markets, which lets them extract more money.

The RIAA, the MPAA, and their associated ancillary organizations are directed by the head executives of the cartel corporations. To achieve their position, executives in the movie and recording industries must instinctively seek and maintain a position of power. Expect ego to be as important as money in their decisions; it's an adaptive trait in their environment.

These people are not naturally inclined to compromise. It's their way or the highway; you will sign their contract or you'll go begging.

In addition, it seems clear that the people running the cartels aren't technically inclined. In a sense, most of them don't really understand what a computer is. For instance, even if they use MS Office every day, they probably don't distinguish between the application, the OS, and the hardware it runs on. In all fairness, that's not their job – or hasn't been, until recently.

As long as the old-media moguls don't understand the terrain, they'll be incapable of com-

ing up with workable plans, unable to comprehend why their plans won't work, and unlikely to agree to a workable accommodation with computer technology.

The people who run the legal machinery (legislators, enforcers and judges alike) aren't any more technically oriented than old-media execs. They're likely to be sympathetic to outraged complaints about established legal rights and claims of billions in lost revenue.

If current laws and enforcement aren't sufficient to ensure these legal rights, we'll get more enforcement, in the spirit of the "hacker" raids of the past, and more laws to enable such enforcement.

If enforcement continues to fail, the enforcers (both government and industry agencies) may continue to gain more legal and institutional powers for enforcement. The principle here: if it doesn't work, do it more and harder.

Trust and security

In conjunction with legal enforcement, old-media will reach for the technical fix. Every time new technology threatens old-media control, the instinctive reaction of old-media is to "put something" in the technology to stop it. Media execs may not be technically inclined, but there's no shortage of technical companies eager to sell them solutions to their problems.

Software copy protection may be unworkable, but hardware that refuses to transfer copyrighted plaintext in unauthorized ways – what some call "trusted client" devices – is possible. (Of course, this kind of device is exactly what RMS is concerned about in "The Right to Read".)

In the jargon of trusted-client, "trusted" doesn't mean the owner can trust his hardware, it means the manufacturer trusts that it has the exclusive authority to program the device. Also, "security" doesn't mean security for the user, it means security from the user.

The integration of trusted-client copy protection with computers would not benefit the consumers who use them; the constraints on general-purpose copying and processing make trusted-client computers less useful than normal computers. More importantly, it would shift the balance of power completely, from the user to the industries that control the devices. In either case, why would people buy crippled hardware when un-crippled hardware is available?

To be successful at all, trusted-client computers will have to appear first as small, cheap embedded systems, like converged portable cellphone/PDA/media players, or gaming consoles whose functions grow to encompass those of low-end desktop computers. These devices tend to have proprietary hardware and software anyway, and are cheap enough to get away with being crippled.

Vertically integrated conglomerates like Sony, with a finger in every pie, are likely to be the first to try to market trusted-client computers. Although the Playstation is only useful for playing games and CDs, the next generation of game consoles will include Internet access and other capabilities associated with general-purpose computers. Sony is well-placed to make the whole distribution chain proprietary, including music and movie production, consumer-electronics players, computers, and physical storage.

Electronics giant Intel is also well-placed to institute trusted-client hardware. Intel has the capacity to integrate processor, graphics, and support hardware on one chip, stick it on a

board, and sell it cheap. While their processor-ID feature recently went down in flames due to consumer protests (and was in itself comparatively innocuous), their publicly declared intentions were directly aimed at instituting a trusted-client regime. In other words, they're working on it, and there is no doubt they can integrate all the necessary features whenever they think they might succeed.

On the whole, though, the computer industry should be our allies. Most manufacturers don't want to redesign their hardware or their software to accommodate trusted-client copy protection. Even in new products, trusted-client systems increase cost and complexity, while decreasing utility. Wherever competition exists, trusted-client systems will be at a disadvantage.

Enforcement and control

The cartels are raising these legal and technical enforcement issues in terms of traditional copyright practice. The ideal seems to be to force computers to make digital data act like physical objects such as CDs, DVDs, and books. Old-media will accept this behavior because they're used to it, and the legal system will enforce it because that's what existing law and precedent are set up to enforce.

However, the cartels also have an inexhaustible appetite for control. If new technology threatens their current dominance, it also gives them an opportunity to extend it.

If technical and legal tools can make your data act like a physical thing, they can enforce other behaviors also. They can control how you play it, and set any kind of pricing scheme. Limited play, pay-per-play, and DIVX-like schemes are some of the possibilities.

In fact, there seems to be no legal limit on the conditions that can be imposed as requirements to view or perform media products. They could require you to stand on your head during the performance, and if your player could detect and enforce those conditions, you'd have to obey or forego the experience.

If you managed to circumvent the enforcement of these conditions, you'd be breaking the DMCA.

Although the current DVD/DeCSS cases are being carefully couched in terms of piracy, the real issue is control. If computer users can write their own DVD player, they can ignore region codes, skip over ads regardless of the commands encoded on the DVD, and in general exert their own control over how they view their DVD collection.

Truth and consequences

This is all is very alarming from a cyberliberties point of view, but what does it have to do with Open Source?

As a current example, the DeCSS mess will make it harder to develop an Open Source DVD player. At best, development will take longer, as the developers deal with lawsuits and uncertainty. If the industry's arguments aren't soundly refuted in court, it will be impossible to distribute a finished player as a standard package in Open Source operating systems.

Other Open Source projects are on the block also. If DeCSS can be banned, CD ripping programs will be easy to outlaw as "primarily for illegal use". Once they intimidate Napster into submission, Gnutella, Freenet, and other distributed file-sharing programs will be targeted for termination.

Most importantly, if computers with trusted-client copy protection become prevalent in the future, they will be deadly to Open Source. Microsoft may be able to get Windows certified to run on trusted-client hardware, but how will you get approval to run your custom-patched Linux kernel?

For now, the recording and movie industries seem to be taking their threats as they find them. Eventually, though, they may learn to know and loathe Open Source in general.

For one thing, once the corporate legal battles are settled, all that's left will be the Open Source offenders. Open Source projects may well be harder to squash; at any rate, they won't react in ways old-media is prepared to understand or accept.

More generally, Open Source products shift the balance of power back towards the user by providing practical alternatives to crippled products. As long as Open Source systems are widely used, they will blunt old-media copy protection schemes indirectly, in ways they can't legally contest.

So, what do we do now?

Given the nature of the participants, I don't think we can avoid this conflict. No matter how much restraint the free software community shows, I doubt the old-media cartels will change their dedication to having it their way. If they need a legal provocation to act, somebody will provide it. The only course left is to prepare for the storm.

If we act now, we can deny the old-media cartels the opportunity to impose onerous copy-protection on us. We can blunt and eventually repeal the DMCA before it can be used in a truly destructive manner. We can make our side of the story heard in the halls of power, and educate our representatives on the consequences of their actions.

We must do these things because the alternative is to dig in and prepare to be driven underground.

Some things you can do to help:

* *Support Open Source software. Write it, document it, test it, and above all use it. Ask commercial software companies to port their products to Open Source operating systems.*
* *Refuse to buy hardware you can't develop for. Even if you can't write a line of code, proprietary hardware will lock you into proprietary software. Be vocal about it. Ask the manufacturer before you buy.*

  The same goes double for PDAs and other prospects for secure-client techniques. Never, ever buy an actual trusted-client device like DIVX.
* *Write (snailmail, not email) your congressperson to repeal the DMCA. Sound reasonable, and be polite.*

  In the long run, though, what we really need is a political machine. The EFF is fine as far as it goes (join them, and give them money!), but we need more lobbying, better organization, and the ability to mobilize at a moment's notice. If the AARP can do it, we can too. We've got the net; we might as well use it.
* *Finally, spread the word. Post it to (appropriate) forums both on- and off-line. Tell friends, journalists, pundits, and anyone else you think might make a difference. With apologies to Slashdot, this news isn't just for nerds any more.*

Credits

Many thanks to Dan, Jacques, and others on Gale, Jen, Phil, Dan, and the rest at Kaldi's, plus Gavin and everyone else. **<tom>**

EXPO 2000 "Spezial"

von padeluun <PADELUUN@BIONIC.zerberus.de>, Wetterfrosch <wetter@ccc.de> und <expositionstourist@gmx.de>

Auf der EXPO möchte die deutsche Wirtschaft technische Kompetenz auf Weltniveau demonstrieren und dass sie bereits "heute schon" für die Zukunft gewappnet sei. Dass sie aber trotz allem Medienrummel auch nur mit Wasser kocht, belegen unsere drei Berichte...

EXPO Security

Während der EXPO2000 arbeiten Polizei, Feuerwehr und Geheimdienste so eng zusammen wie noch nie.

Die Besucher der ersten Weltausstellung in Deutschland sind gut behütet: Damit bei Unfall, Diebstahl oder technischen Defekten trotzdem alles reibungslos läuft, wird es während der EXPO2000 eine Sicherheitszentrale geben, in der Polizei, Feuerwehr, Rettungsdienste, Verkehrsplaner und Techniker so eng zusammen arbeiten wie nie zuvor. Die Betriebs- und Sicherheitszentrale (BUSZ) der EXPO2000 war schon zu den beiden Großmessen im Februar 2000 einsatzbereit.

Untergebracht sind in der BUSZ auch Beamte von Bundesgrenzschutz, Bundeskriminalamt, Landeskriminalamt und vom polizeilichen Staatsschutz (KFI 4). "Wir wollen, daß jeder den direkten Kontakt zum anderen hat, und alle die gleichen Ausgangsinformationen haben", erklärt der stellvertretende Sicherheitschef der EXPO2000, Hermann Fraatz. Es gibt insgesamt 150 Mitarbeiter, die in der BUSZ rund um die Uhr im Einsatz sein werden.

In den Räumen zwischen den Messeeingängen West 3 und West 4 arbeiten an 32 Arbeitsplätzen Kollegen von EXPO2000, vom Verkehrsleitsystem move, von Polizei, Feuerwehr, Rettungsdiensten, Deutsche Bahn AG sowie von der EXPO beauftragten private Sicherheitsleute gemeinsam zusammen. Auch die Störtrupps von Strom-, Gas-, Wasser und Kommunikationslieferanten werden von hier gelenkt. So sollen Abstimmungswege so kurz wie möglich gehalten werden, damit im Ernstfall alles Schlag auf Schlag geht. Die Kollegen müssen nicht erst herum telefonieren, um den richtigen Ansprechpartner zu finden, sondern sitzen mit ihm an einem Tisch. Jeder Arbeitsplatz ist mit einem Computersystem ausgestattet, auf dessen Bildschirm jederzeit die aktuellsten Informationen gesendet werden. So hat jeder den selben Sachstand, sieht dasselbe Bild

vom Einsatzort und hat die selbe Karte dazu wie sein Kollege.

Um das Geschehen auf dem gesamten Gelände zu überwachen, gibt es während der Weltausstellung ca. 250 Videokameras, die ihre Bilder direkt in die Sicherheitszentrale senden. Dort sind neben 42 Fernseh-Bildschirmen auch drei Großbildleinwände installiert. Kommt es zu einem Unfall, oder gibt es einen Stau, weil eine Rolltreppe ausgefallen ist, dann können die Sicherheitsmitarbeiter das Bild vom Ort des Geschehens auf eine Großbildleinwand schalten, so daß jeder Kollege jedes Detail genau sehen kann. Im Notfall ist dann für Feuerwehr, Polizei und Rettungsdienste jeder Punkt auf dem Gelände innerhalb von drei bis vier Minuten erreichbar.

Das ausgeklügelte Sicherheitskonzept beinhaltet neben der BUSZ auch ein Polizeikommissariat im Nordriegel, eine Polizeistation im Europa-Center und Beamte an jedem Eingang, zwei komplette Löschzüge der Feuerwehr werden direkt auf dem Gelände stehen, Notfallambulanzen wird es in Halle 19 und auf der Plaza geben. Die BUSZ selbst wird zwei Unterstationen in Halle 12 und auf der Plaza haben. Am Flughafen Hannover ist zusätzlich ein Abschiebeknast entstanden.

Der Innenausbau der Zentrale hat zehn Wochen gedauert. Dabei sind insgesamt rund 25 Kilometer Computer- und Telefonkabel und fünf Kilometer Videokabel verlegt worden.

So viele Unwägbarkeiten und Unsicherheiten es bei einer Großveranstaltung wie der Weltausstellung auch geben mag, eines steht für Hermann Fraatz fest: "Die EXPO2000 wird sicher, mit Sicherheit." **<tom>'**

Spass mit WaveLAN

'PIEEP' - Das war der Metall-Detektor am Eingang Ost, "Was ist das denn?" fragte ein lieber Sicherheitsbeamte bei dem Anblick auf mein Notebook "Das ist ein Laptop." entgegnete ich. Mit einem sehr stutzigem Gesicht liess er mich passieren.

Ich hatte nur ein Ziel: 76 Wavelan-Roboter. Sie waren der eigentliche Grund, weshalb ich auf der Expo war. Mit schnellen Schritten eilte ich zu Halle 4: kein einziger Roboter weit und breit. Trotzdem setzte ich mich ersteinmal in ein Treppenhaus und schaute was meine Wavelankarte sagte ... Netz! Irgendwo mussten sie also doch sein...

Nach kurzem Fussweg kam ich in einen grossen, dunklen Raum, in dem dutzende Milchglas-Halbkugeln im Schrittempo dicht an dicht rumkurvten. Sofort setzte ich mich in die nächste Ecke und spielte ein bischen mit tcpdump. "Komisch", dachte ich, "die 168.192.68.92 macht aber eine Menge Traffic, gleich mal portscannen". "Hmm, telnet, ftp, http und ssh offen, das wird bestimmt lustig." Bei einer telnet-Verbindung wurde komischer Weise kein Login abgefragt, stattdessen tauchte ein schönes Menü auf – das Menü des sog. Accesspoints, der Zentralstelle des WaveLAN-Netzes.

Eine kleine Auswahl an Einstellungen, die ich per Zifferndruck vornehmen konnte: Filtern von TCP/IP Packeten bzw. Multicast Adressen, ARP-Packete per Menürsteuerung verschicken, meine eigenen Privilegien ändern uns letztendlich den Accesspoint herunterfahren. Ein Mittschnitt der Telnet-Sitzung und ein paar TCP-Dumps liegen auf [1].

Naja, ich finde es sehr blamabel, dass _jeder_ diese Einstellungen vornehmen konnte. Bevor ich aber das ganze meldete, wollte ich noch

einen Freund anrufen, und ihn fragen was noch so interessant wäre. Als ich dann zu wählen begann, machte mich eine Frau darauf aufmerksam, dass telefonieren in dieser Halle verboten sei. Während im Hintergrund mein Laptop mit der Wavelankarte weiterblinkte, erklärte sie weiter, dass das die "Motorik der Funk-Roboter stören könnte."

Nun wollte ich auch wissen, was denn die Verantwortlichen dazu sagen. Also fragte ich eine nette Dame von der Halle 4, ob sie denn wüsste wen ich da aufsuchen müsste. Sie war gleich so freundlich und hat mich zu den Leuten vom Fraunhofer Institut gebracht.

Dort angekommen hielt ich eine kleine Vorführung vor ca. sechs Leuten. Mittendrin ging einer der Anwesenden (ja, einer im Anzug) schnell mit seinem Handy ein paar Meter weg und telefonierte sichtlich nervös. Während dessen zeigte ich dem Rest der Gruppe wie simpel das doch alles war. Danach kam der Herr im Anzug wieder auf mich zu und sagte, dass das Fraunhofer Institut in Dortmund mittlerweile Bescheid wüsste und, dass sie gerade herausfänden, von wem der Accesspoint stamme. Er erklärte weiter, dass an diesem Projekt fünf Firmen und Instituionen (neben dem Fraunhofer) beteiligt wären, und die Koordination untereinander nicht sehr gut klappen würde.

Danach liess ich mir ein bischen die Technik zeigen. In so einem Roboter (ca. 50 cm bis max. 2 m gross) befindet sich ein Steuerrechner mit Lucent Wavelan Orinoco Silver Karte, ein grosser IR-Sensor um Hindernisse zu erkennen, ein Hardware MPEG-Decoder, ein Sony-Beamer und zwei bis vier Akkus. Der Roboter empfängt via 802.11 kurze MPEG-Clips von einer Windows-Maschine, decodiert diese und wirft sie mit dem Beamer an die Milchglasscheibe.

Gesteuert wurden die Roboter mit einen gewöhnlichen SuSE-Linux, auf der eine Software zum Steuern lief. Das Programm lief nach dem Prinzip: Klicken - ziehen - los lassen. Mit zwei gut steuerbaren Überwachungskameras konnte man den ganzen Raum überwachen.

Zu dem Problem mit dem Accesspoint nahm man sinngemäss wie folgt Stellung: "Wir konnten ja nicht wissen, dass jemand mit Laptop und Wireless-LAN hier auftaucht und rumspielt." Auf Nachfrage sicherte man mir zu, dass ich gerne mir Freunden wieder herkommen könnte.

[1] http://www.fnordhausen.de/projekte/expo/

Radio HANNO

Das hannoversche RADIO HANNO hat zur EXPO 2000 weder Kosten noch Mühen gescheut, um den geschätzten Besuchermassen ein interessantes und informatives Programm zu bieten.

Wie in jedem Jahr gestalten die flotten Damen und Herren in grün/weiss auf über vierzig Funkkanälen ein packendes und unterhaltsames LIVE-PROGRAMM rund um die Uhr!

Dieser kleine Leitfaden soll es Ihnen, liebe Hörerin, lieber Hörer erleichtern, den Spass an RADIO HANO erheblich zu steigern...

Allerdings möchten wir hier auf einige rechtliche Sachverhalte hinweisen:

1. *der besitz sogenannter "Scanner" ist grundsätzlich erlaubt, solange dass gerät ein "CE"-zeichen trägt.*
2. *verboten ist das gezielte abhören des BOS-funks. (polizeifunk) ein gerät, das bei der beschlagnahme durch die polizei die*

Name	Frequenz	Bemerkung
n.b.	**173.64**	Auf diesem Kanal funken die "zivilen Aufklärer". Sehr interessant und informativ.
n.b.	**86.995**	der Lotsen-Kanal. Die VIP-Eskorten melden hier fortlaufend ihre Position.
n.b.	**173.34**	Einsatzkanal für Demos etc.
n.b.	**173.10**	Einsatzkanal für Demos etc.
n.b	**172.66**	Einsatzkanal für Demos etc.
n.b.	**85.515**	der allgemeine RADIO HANO Kanal – sozusagen das Informationsprogramm für den Alltag. Hier ist immer was los... .
"drei"	**86.135**	Der zweite allgemeine HANO Kanal. Wird genutzt, wenn der erste HANO-Kanal überlastet ist. Dient auch als Schnittstelle zum EXPO-Funkkreis.
"zwo"	**86.255**	Der Privatchat der eifrigen MitarbeiterInnen von RADIO HANO. Ob einer mal zu "Macdoof" fährt oder wer das verdammte Protokoll gemacht hat oder auch wann endlich Feierabend ist – alles hier zu hören.
n.b.	**85.555**	Der sogenannte EDV-Kanal. Namen, Geburtsdaten, Kennzeichen.
"fünf"	**85.935**	Ausweichkanal für die HANO-Einheiten. Wird auch als Einsatzkanal genutzt.
n.b.	**173.94**	das "kleine Gerät" der HANOS.
n.b.	**172.70**	zweiter 2m-Funkkreis der HANO-Funker.
n.b.	**173.84**	Der EDV-Kanal für das kleine Gerät. Personenüberprüfungen,Kennzeichen…
n.b.	**172.76**	Reservekanal für Kripoeinsätze, Beschattung, Observation.
xxx	**000**	Die Kanäle für das EXPO-Gelände
n.b.	**87.155**	die EXPO-Wache! Hier immer das neuste vonner Weltausstellung!
n.b.	**87.115**	der EXPO-Wachschutz.
n.b.	**85.875**	Ausweichfrequenz für EXPO-Raumschutzkräfte.
n.b.	**171.57**	der EXPO-Geländefunk.
n.b.	**86.055**	RADIO DEISTER. Zuständig für den Landkreis Hannover.
n.b.	**85.455**	HILDE – die Freunde und Helfer aus Hildesheim.
n.b.	**85.375**	HILDE.

frequenzen der BOS-funkdienste eingespeichert hat, kann dann auch beschlagnahmt werden.

3. *sollte zufällig BOS-funk empfangen werden, so ist es verboten, die inhalte des BOS-funk an dritte zu verbreiten.*

Frequenzen

Um das Abhören von Radio Hanno zu erleichtern, haben wir hier alle gebräuchlichen Frequenzen zusammengestellt.

Gelegentlich wechseln unsere unermüdlichen Reporter in Uniform mal die Frequenz für die Live-Berichterstattung. Dabei bedienen sie sich einer internen Kanalbezeichnung.

Grundsätzlich unterscheiden sich der 2-meter ("kleines Gerät", Frequenzen 172 bis 174 MHz) und der 4-meter ("grosses Gerät", 84 bis 88 MHz).

Zur EXPO wurden mehrere Funkkreise gebildet. So wird der normale Funkverkehr der hannoverschen Polizei auf anderen Frequenzen als der Funkdienst für EXPO-Aufgaben abgewickelt. Zusätzliche Frequenzen werden als Reserve vorgehalten. Zur Logistik der Polizei gehören auch Handys, verschlüsselte Textübertragung und verschleierte Funkaussendungen. Auch tummeln sich einige andere interessante Funkdienste im Äther. Die Tabelle links verschafft eine Übersicht.

Codes

Die flinken Reporter von RADIO HANNO bedienen sich im Funkverkehr gewisser Codes zur Bezeichnung häufiger Begriffe. Dies soll das Abhören des hannoverschen Lokalradios interessanter machen. **<tom>**

code	bedeutung	code	bedeutung
015	dienststelle	**081**	festgenommene person
023	ausländer	**082**	feuerwehr
031	verletzte person	**091**	verrückt
032	fahrerflucht	**098**	hilfeleistung
033	unfall	**099**	hilflos
036	verdächtig (person o. kfz)	**104**	kfz
038	raub	**105**	krankenwagen
041	täter	**107**	leiche
044	standort	**116**	drogendelikt
048	selbstmord	**118**	ruhestörung
053	alarmauslösung	**119**	schlägerei
058	bedrohung	**121**	schusswaffe
064	alkoholisiert	**226**	überprüfung
070	diebstahl	**235**	wieder einsatzbereit
072	einbruch		
076	fahndung		

0 7 1 - 0 2 9

Wir haben uns alle lieb...

Felix von Leitner <fefe@fefe.de>

Viren können sich nur auf unsicheren Betriebssystemen selbständig verbreiten. Heute trifft das ausschließlich auf Windows zu, wobei Netscape die Probleme mit Javascript in Mail und News theoretisch auch nach Unix gebracht hat.

Nachdem mal wieder ein Virus die üblichen Verdächtigen heruntergefahren hat (Microsoft, die NATO, das EU-Parlament und diverse Landesregierungen und Verlage in Deutschland) ist das Geschrei immer groß. Sofort finden sich in den Medien diverse Experten, die den Schaden auf mehrere Millionen oder gar Milliarden schätzen (natürlich ist diese Zahl frei erfunden und entbehrt jeder Grundlage, sie wird auch nicht weiter hergeleitet oder begründet).

Aber richtet denn so ein Virus überhaupt Schaden an? Geht auch nur ein einzelner Rechner kaputt? Nein. Sinken dadurch Aktienkurse? Im Gegenteil! Aktien von Security-Firmen treiben jedesmal die Aktienmärkte um mehrere Prozentpunkte nach oben.

Der Schuldige

Microsoft hat es geschafft, das Bewusstsein der Massen so zu manipulieren, dass Viren heute als etwas dastehen, das nicht verhinderbar ist, das eben ab und zu kommt und Daten kaputt macht. Folgerichtig liegt die Schuld natürlich in den Augen der Bevölkerung bei dem Autoren der Viren, nicht bei Microsoft.

In Wahrheit ist aber Microsoft schuld, nicht der Virenautor. Um sich dessen bewusst zu werden hilft ein kleines Gedankenexperiment. Nehmen wir an, die Bundesregierung baut einen Todesstern im Weltraum, der die Erde pulverisieren kann. Nehmen wir weiter an, dass die Bodenstation dazu direkt auf einem frei zugänglichen Autobahnparkplatz steht und draußen ein großer roter Knopf ist, der mit "Selbstzerstörung" beschriftet ist.

Nehmen wir weiter an, dass ein Auto mit einer Familie auf dem Parkplatz parkt und ein Kind herum turnt und den Kopf sieht. Kinder drükken gerne auf Knöpfe. Nehm en wir an, das Kind drückt auf den Knopf und der Todesstern explodiert und stürzt auf Nordamerika, wobei Kanada und die USA im Meer versinken.

In diesem Fall ist doch nicht das Kind schuldig, sondern der Idiot, der den Knopf da frei zugänglich angebracht hat! Und bezogen auf die Virenproblematik ist Microsoft schuld. Mein Vorschlag ist es daher, Microsoft für die gesammelten Milliardenschäden haftbar zu machen, die durch ihre Software auf der Welt entstanden sind, und das betrifft wie oben gesagt nicht nur die Viren.

Nochmal zum Schaden

In einzelnen Institutionen fällt gewöhnlich für ein paar Tage die Arbeit aus. In diesem Fall kann man natürlich von einem Schaden sprechen. Nur - wem entsteht dieser Schaden? Leuten, die Windows einsetzen. Wer einen Blick in die Tagespresse wirft, stellt schnell fest, dass alle paar Tage in allen möglichen PC-Publikationen von Unsicherheiten und Unstabilitäten von Windows die Rede ist. Jeder weiß das. Wenn jemand einen PC mit Windows kauft, obwohl er das weiß, dann ist das grob fahrlässig.

Ich betrachte diese Situation gerne unter dem Gesichtspunkt der natürlichen Auslese. Wer schlechte Software einsetzt, der überlebt eben nicht im Geschäftsleben. Normalerweise finde ich das, wenn es dann geschieht, nicht erwähnenswert, aber das laute Geschrei nach der Strafverfolgung des "Täters" (d.h. des Autors) ist absolut nicht angebracht, und dagegen richtet sich dieser Artikel auch hauptsächlich. Wenn wir uns überhaupt darauf einigen, jemanden haftbar zu machen, dann sollte es Microsoft sein, nicht irgendein 15jähriger Junge aus einem Schwellenland.

Wie kann das sein?

Die Hauptfrage an der ganzen Angelegenheit ist für mich: Wie kann es sein, dass unsere Infrastruktur überhaupt funktioniert, wenn doch offensichtlich fast nur Luschen am Werk sind? Beispiele für extreme Kompetenz am Arbeitsplatz:

• FEMA, die "Federal Emergency Management Agency" der USA. Diese Experten haben an der Firewall die Email-Größe auf zehn kByte limitiert, weil sie gehört hatten, dass ILOVEYOU 15 kByte groß ist. Äh, hallo? Was ist, wenn jemand für die Beschreibung seines Notfalls mehr als zehn kByte brauche? Z.B. weil er auch ein Idiot ist und das ganze als Word-Attachment schickt?

• Symantec hat laut diesem Update Usern empfohlen, keine Mails zu öffnen, die "ILOVEYOU" im Subject haben. Und wieder wird es so dargestellt, als ob diese Email das Problem wäre. Einige Administratoren(*) haben daraufhin in ihren Firewalls Mails mit Subject "ILOVEYOU" gefiltert und daher keine Mails von Security-Listen mehr bekommen, die Neuigkeiten zum Virus verbreiteten.

• Das US Defense Department gab an, dass mindestens vier geheime Militärsysteme befallen wurden. Hallo? Geheime Militärsysteme? Unter Windows? Per Email aus dem Internet erreichbar?!

Realsatire: Was Microsoft sagt

Laut [1] sagte Microsoft, dass es sich nicht um einen Fehler, sondern um ein Feature handelt. Schließlich könne man ja das ja alles irgendwo abschalten. Ein Programm-Manager von Microsofts Security Response Team sagte außerdem, Scripting sei nicht das Problem, weil der Virus ja genau so gut als EXE hätte kommen können. Das muss man sich mal auf der Zunge zergehen lassen! EXE-Viren sind natürlich auch ein Windows-Problem!

Aber der größte Hammer, den Microsoft je vom Stapel gelassen hat, ist im Interview mit

Bill Gates [2] dokumentiert, wo er tatsächlich behauptet, dass eine Zerschlagung Microsofts in mehrere unabhängige Firmen es in Zukunft schwieriger machen würde, Viren zu bekämpfen. Als ob Microsoft jemals bei auch nur einem einzigen Virus eine Mitschuld oder auch nur unsichere Grundeinstellungen eingeräumt hätte! Tatsächlich steht Microsoft Security-Dienstleistungen eher im Weg als ihnen zu helfen. Natürlich sagen Antivirus-Produzenten selten schlechtes über Microsofts "Sicherheit", weil sie sich ja dann den Ast absägen würden, auf dem sie sitzen.

Wen hat es denn so alles erwischt?

Man sollte annehmen, dass nur kleine und mittelständische Unternehmen betroffen sind, weil die kein Geld für Sicherheit übrig haben. Man würde vermuten, dass Institutionen, bei denen Security einen wichtigen Teil der Arbeit ausmacht, überhaupt kein Problem mit diesem Virus gehabt haben. Der Artikel unter [3] listet ein paar US-Institutionen, die betroffen waren. Am ironischsten fand ich aber den Bericht, dass die US Präsidentschaftskandidaten Al Gore und George Bush Jr. von dem Virus runtergefahren worden sein sollen, welche sich ja beide Internet-Kompetenz auf die Fahnen geschrieben haben, und besonders Al Gore war dadurch aufgefallen, dass er einmal behauptet hatte, das Internet erfunden zu haben.

Hier ist noch ein schockierter Bericht darüber, dass der Virus praktisch alle US-Regierungsstellen "geschädigt" hat. Und, achtet mal darauf, wieder analysiert der Technologie-Experte als Problem heraus, dass die Leute Email-Attachments von Unbekannten geöffnet hätten. Das ist doch genau die Idee bei Email, dass man mit Leuten kommunizieren und Dateien austauschen kann! Das eigentlich Problem ist, dass bei Windows überhaupt Datenverlust entstehen kann, wenn man Attachments öffnet. Email-Programme, die es erlauben, Skripte oder andere Programme in Emails überhaupt auszuführen, sind das Problem.

Ist das ein isolierter Ausrutscher bei Microsoft?

Nein. Nur ein paar Tage nach ILOVEYOU kam ein neues Sicherheitsproblem im Internet Explorer heraus, bei dem der Browser Programme auf dem Rechner des Users ausführt. Diesen Programmen traut IE, weil sie schon auf dem Rechner sind und nicht aus dem Internet geholt werden. Die Demonstration des Fehlers führte ein Skript aus, das bei der Installation von Netscape installiert wird. Laut dem Bericht [5] hat sich Microsoft tatsächlich getraut, das Problem Netscape in die Schuhe schieben zu wollen.

Abschließende Worte

As you clean up your registry and replace your damaged files, just keep a few things in mind:

1. Microsoft just wants to be free to innovate and to bring great software to consumers.

2. We wouldn't have great software like Windows and Office if Microsoft hadn't violated anti-trust laws. *(von Slashdot)*

(*) Nachzutragen wäre noch, dass der Anbieter Strato auf seinen Mailserver alle E-Mails, die ILOVEYOU im Betreff enthalten, zurückweist. Das heißt, dass kein Strato-Kunde eine Warnung oder Abwehr-Tipps erhalten konnte...

[1] *http://news.cnet.com/news/0-1003-200-1823167.html* [2] *http://ap.tbo.com/ap/breaking/MGID8X25Z7C.html* [3] *http://www.fcw.com/fcw/articles/2000/0501/web-agencies-05-04-00.asp* [4] *http://www.techserver.com/noframes/story/0,2294,500202543-500280338-501496980-0,00.html* [5] *http://news.cnet.com/news/0-1005-200-1820959.html?tag=st.ne.1002.bgif.ni*

Wählen Videokameras SPD?

Die CDU hat zum ersten Mal die Konsequenzen ihrer eigenen Videoüberwachungspolitik zu spüren bekommen: einer ihrer Abgeordneter wurde aufgrund installierter Kameras dabei erwischt, wie er betrunken Auto fuhr.

Kameras sind unparteiisch - das musste vor kurzem auch der baden-württembergische CDU-Politiker Paul Stefan Mauz erkennen.

Bundesweit setzt sich die CDU am meisten für eine stärkere Überwachung durch Kameras ein. Betroffen sind davon überwiegend öffentliche Plätze, öffentliche Verkehrsmittel und sogenannte Gefahrenzonen, wie eben jene Tiefgarage, die dem Mann von der CDU zum Verhängnis wurde.

Erst vor kurzem wurden 13 Kameras in die Landtagstiefgarage eingebaut, weil desöfteren Gegenstände aus den Autos entwendet worden waren. Mauz hatte entweder die Schilder, die explizit auf die Videoüberwachung hinwiesen, nicht gelesen, oder sich einfach keine Gedanken darüber gemacht, dass die Kameras eben doch nicht nur Diebe, sondern alles und jeden filmen.

An diesem Abend jedenfalls torkelte Mauz angetrunken aber nichtsahnend seinem Auto entgegen. Doch schon am Pförtnerhaus wurde er zur Alkoholkontrolle gebeten. Er hatte das Limit weit überschritten.

Daß nun ausgerechnet ein CDU-Politiker erstes Opfer der neuen Überwachungspolitik wurde, sorgt in der Partei vorwiegend für Schadenfreude gegenüber einem Politiker, der nicht besonders beliebt ist, und schon desöfteren dazu neigte, sein Amt auszunutzen (so auch, als er mit einem alkoholisierten Fahrer unterwegs war und versuchte, die Polizei an einer Alkoholuntersuchung zu hindern. Er wurde zu einer Geldstrafe verurteilt).

Eine kritische Diskussion über die Videoüberwachung wird es wohl trotzdem nicht geben: das verhindere die CDU. "Hätte es einen geachteten Architekten getroffen, wäre die Diskussion möglicherweise anders gelaufen", so Sprecher Helmut Zorell von der SPD. **<tina>**

Quelle: BZ vom 11.7.2000

Lexikon der Verschwörungs-theorien

by Robert Anton Wilson

Robert Anton Wilson hat sich wohl mit mehr Verschwörungstheorien auseinandergesetzt, als ein Großteil der restlichen Menschen auf diesem Planeten.

Das Ergebnis ist dieses Buch: fast 400 Seiten voll mit Paranoia und abstrusen Hypothesen. Bei einer solchen Ansammlung von exotischen Gedankenansätzen wird halbwegs deutlich, daß es sich bei dem Autor nicht um einen fanatischen Anhänger von Verschwörungstheorien handelt.

Das Buch ist in vier Teile gegliedert: einer Einleitung, dem tatsächlichen Lexikon ("Verschwörungstheorien von A-Z"), einem Interview mit Wilson und dem Stichwortverzeichnis.

Die geäußerten Gedanken sind nichts Neues, wenn man andere Bücher von Wilson kennt, aber das Lexikon ist wirklich amüsant und birgt eine Menge abgefahrenen Unsinn in sich.

In der Einleitung geht Wilson unter anderem auf das Phänomen Verschwörungstheorie und die Umstände seiner Entstehung ein. Zu den meisten Stichworten gibt es Querverweise auf verwandte Einträge, sowie auf Bücher, oder URLs, von denen viele aber inzwischen wohl nicht mehr aktuell sind.

Wilsons Zusammenfassung von Verschwörungstheorien ist also eher eine kurzweilige Sache zum Blättern und Querlesen. Denjenigen Menschen allerdings, die dieses Buch tatsächlich als Lexikon, sprich Nachschlagewerk benutzen, sollten gute Freunde die Drogen wegnehmen... **<lisa>**

Robert Anton Wilson: ***"Das Lexikon der Verschwörungstheorien"***, DM 44,- Eichborn Lexikon, ISBN 3-8218-1595-7

Anm. d. Red.: *Die Übersetzung ins Deutsche übernahm übrigens kein Geringerer als Gerhard Seyfried u.a. Autor und Zeichner von "Wo soll das alles enden – 1 kleiner Leitfaden durch die Geschichte der undogmatischen Linken", Rotbuch Verlag, Berlin, 1978... Kostprobe, s.u.:*

ECHELON - alter Hut für den VS?

GERMAN SPIES: ECHELON EXISTS For 18 months now, Germany's intelligence service has issued warnings against Echelon's industrial espionage

Dig that. We can now document that the German intelligence service has been warning against Echelon's espionage for at least 18 months. In Denmark, the Military Intelligence Service (FE) states that they know nothing more than what they read in the newspapers. They tackle the situation a little differently in Germany. Germany's national intelligence agency, Verfassungsschutz, openly warns its business and industry community against Echelon. Germany's intelligence agencies do more than just warn against the spying, however. They also instruct German industry in how to protect themselves against the illegal espionage network. Since June 1999, the German intelligence service has been recommending German companies to encrypt all important information, i.e. encode it to prevent Echelon's spies from listening in. And the entire process is very open. Verfassungsschutz has issued its warnings and protection guidelines as folders which they send to German industry.

http://www1.ekstrabladet.dk/VisArtikel.iasp?PageID=44659 – der Onlineartikel enthält die abgebildete Übersichtskarte des Landesamts für Verfassungsschutz: laut Ekstrabladet hatte das Landesamt diese bereits 18 Monate vor offizieller Anerkennung Echelons durch deutsche Behörden angefertigt.

0 7 1 - 0 3 5

DefCon

28. - 30.7.2000, Las Vegas, USA

"DEF CON is an annual computer underground party for hackers held in Las Vegas, Nevada, every summer for the past seven years. Over those years it has grown in size, and attracted people from all over the planet. That's what it is all about. Meeting other people and learning something new.

We are not trying to teach you to learn how to hack in a weekend, but what we are trying to do is create an environment where you can hang out with people from all different backgrounds. All of them interested in the same thing, computer security."
http://www.defcon.org/html/defcon-8-pre.html

Und hier noch ein Hinweis für alle glücklichen Hacker, die sowohl die H2K als auch die DEFCON besuchen wollen: unter http://www.moloch.org/html/defcon_2k.html könnt ihr euch für einen gemeinsamen Flug mit anderen New Yorker Hackern zur DEFCON anmelden.

Hackschiff Cologne - Chaos zwischen Steuerbord und Hackbord

4.8.2000, irgendwo bei, äh, Bonn

"Hacken auf dem Schiff: Am 4. August ist es so weit. Mit der einem Ausflugsschiff kurven wir ab Bonn auf dem Rhein, von 18:00 Uhr bis etwa 3:00 Uhr morgens. Mit einer netten, knackigen Veranstaltung wollen wir der erweiterten Chaos-Familie einen Sommertreffpunkt bieten."
https:/koeln.ccc.de/projekte/hackschiff/

informatica feminale

4.-19.9.2000, Bremen

Die Informatica Feminale ist eine alljährliche Veranstaltung, die zwischen dem 4. und 19. September Frauen mit oder ohne Abitur ein intensives Sommerstudium im Bereich Informatik ermöglicht. Veranstaltet wird die Informatica wie jedes Jahr von der Universität Bremen, die die Räumlichkeiten und den Großteil der Professoren stellt. Kostenpunkt für Nichterwerbstätige ist 25 DM. Informationen über die Informatica gibt's unter:
http://www.informatica-feminale.de/

Hack von http://www.strato.de vom 26.6.2000