die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

Klar: Wirtschaftsverbrechen sind eine schlimme Sache! Besonders die Verbrechen, die die Wirtschaft verübt und dabei so unwichtige Dinge wie freie Meinungsäußerung, informationelle Selbstbestimmung oder Privatsphäre mißachtet.

ISSN 0930.1045 • Sommer 2001
DM 5,– die sich wieder mal lohnen
Postvertriebsstück C11301F

#75

Erfa-Kreise

Hamburg: Lokstedter Weg 72, D-20251 Hamburg,<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/.

Berlin: Club Discordia jeden Donnerstag zwischen 17 und 23 Uhr in den Clubräumen in der Marienstr. 11, Vorderhaus 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

Köln: Chaos Computer Club Cologne (c4) e.V. Vogelsangerstraße 286 / 50825 Köln 50° 56' 45"N, 6°51'02"O (WGS84) / Tel. 0221-546 3953 / http://koeln.ccc.de/ <oeffentliche-anfragen@koeln.ccc.de>. Treffen Dienstags 20:20.

Ulm: http://www.ulm.ccc.de/ Kontakt: Frank Kargl <frank.kargl@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 EMail: 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

Die Datenschleuder Nr. 75

II. Quartal, Sommer 2001

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,
eMail: office@ccc.de

Redaktion:
(Artikel, Leserbriefe etc.)
Redaktion Datenschleuder, Postfach 640236, D-10048 Berlin, Tel +49 (30) 280 974 70
Fax +49 (30) 285 986 56 / eMail: ds@ccc.de

Druck:
Pinguin-Druck, Berlin

CvD, Layout und ViSdP dieser Ausgabe:
Tom Lazar **<tom>**, tom@tomster.org

Mitarbeiter dieser Ausgabe:
Rüdiger Weis, maz&morix, Sebastian Zimmermann, David Burke, Sabine Krüger, Stefan Krecher, Edward Felten et al. sowie Andy Müller-Maguhn und Tina Lorenz

Open Chaos

Es tut sich etwas. Die Datenschleuder bekommt mehr Feedback und Input. Die 75. Ausgabe ist die erste seit langem, wo wir mehr (druckfähiges!) Material bekommen haben, als wir abdrucken konnten. Und das obwohl wir dieses mal bei satten 48 Seiten liegen!

Vielleicht liegt es auch daran, daß derzeit einfach viel mehr zu passieren scheint. "Law & Order" in aller Welt sind im Begriff sich auch in neuen Gebieten durchzusetzen. Koste es was es wolle.

Wenn man sich die aktuellen Geschehnisse anschaut (Skylarov, Genua, TKÜV etc.) braucht man nicht viel Phantasie/Paranoia um sich zu fragen: "Sind die 'demokratischen Regierungen' dieser Welt wirklich im Begriff, den 'Demokratie-Teil' zu opfern, (nur) um den 'Regierungs-Teil' zu retten?"

Fest steht: die Regierungen bekommen Angst. Angst, die Kontrolle zu verlieren. Die zunehmend Überzogenen Maßnahmen (Ausreiseverbot, "Schwarze Listen", absurd hohe Strafen für reine Urherberrechtsverletzungen) erinnern an das wilde Beißen eines in die Enge getriebenen Hundes.

Der Schlüssel im Kampf gegen solche "tollwütige" Macht- und Kontrollgelüste ist Information: nicht nur, daß die Mainstream-Medien bestenfalls zaghaft über bestimmte Themen berichten – diese Themen sind auch i.d.R. sehr komplex und lassen sich nicht in BILD-Zeitungs-Phrasen pressen.

Relevante Entwicklungen aufzeigen und transparent machen wird deshalb immer wichtiger.

Auch diese Datenschleuder will dazu einen Beitrag leisten. *Tom Lazar <tom@tomster.org>*

Widmung

Diese Datenschleuder ist dem Gründungsmitglied des Chaos Computer Club und Erfinder der Datenschleuder, Wau Holland gewidmet.

Wau verstarb am 29.07.2001 infolge eines Schlaganfalls im Alter von 49 Jahren.

In dieser Ausgabe findet sich das letzte Interview mit Wau.

Weitere Informationen zu Wau gibt es unter *http://www.wauland.de*

“Mit Geheimdiensten kann man nicht spielen.”

Die Hacker-Legende Wau Holland über illegales Verhalten, Kontrolle und Staubsauger

Von Oliver Zihlmann http://www.sonntagszeitung.ch / Sonntagszeitung / Schweiz, 06.05.2001

SonntagsZeitung: Wau Holland, Sie haben vor 17 Jahren eine Hamburger Bank gehackt und 135 000 Mark erbeutet...

HOLLAND: ...und wir haben das Geld sofort zurückgegeben.

Das Internet wurde doch erst vor zehn Jahren erfunden.

HOLLAND: Das erste, weltumspannende, frei programmierbare hackbare System war das Telefonnetz.

Ein Telefon lässt sich nicht hacken.

HOLLAND: Der Hacker der 60er-Jahre ging in eine Telefonzelle, steckte 20 Pfennig in den Münzautomaten, drückte ein paar Mal die Gabel und telefonierte stundenlang mit Hawaii oder Kuala Lumpur. Gabelwählen hiess das.

Sie machten sich also strafbar.

HOLLAND: Die Post zeigte mich nicht an. Sie sagte, ich zeige "atypisches Nutzerverhalten". Danach baute die Telefongesellschaft flächendeckend Stossdämpfer in die Münzsprechapparate, um das Gabelwählen zu unterdrücken.

Es scheint, die Hacker passen nicht in das klassische Täter-Opfer-Schema der Kriminalistik.

HOLLAND: Nulla poena sine lege - gibts gegen eine Tat kein Gesetz, kann der Täter nicht bestraft werden. Die ersten englischen Telefonzellen-Hacker wurden deswegen konsequent wegen Stromdiebstahls verurteilt. Dafür gab es ein Gesetz. In England wurde die Auslegung des Gesetzes der sozial gewünschten Richtung angepasst.

Sie sind Gründungsmitglied und Alterspräsident des legendären Chaos Computer Clubs, der grössten und bekanntesten deutschen Hackerorganisation. Sie und Ihre Clubmitglieder hakken seit 20 Jahren Computersysteme von Militär, Forschung und Wirtschaft. Trotzdem sind Sie seit 20 Jahren ein legaler Verein. Wie das?

HOLLAND: Wir Hacker dürfen uns im Vergleich keine illegalen Aktivitäten leisten, sonst werden unsere Clubs sofort verboten. Wir begehen nur Strafbare Handlungen, wenn wir das verantworten und dazu stehen können.

Irgendwo zwischen "atypischem Nutzerverhalten" und Straftat, liegt die vielzitierte Hacker-Ethik.

HOLLAND: Unterhalb der strafbaren Handlung steht die Ordnungswidrigkeit. Unterhalb dieser gibt es noch den groben Unfug. Wir sind aber nicht grob. Wir tippen mit dem Fingerchen auf die Telefongabel, verbinden Modem-Relais, tippen ein paar Befehle in eine Maschine. Wir machen das Gegenteil von grobem Unfug. Wir machen feinen Fug.

Neue Dimensionen erreichte der Fug mit den ersten vernetzten Computern und der Erfindung des Modems.

HOLLAND: Ja. Bloss, ein legales Postmodem kostete 120 Mark im Monat und war nicht kompatibel mit internationalen Standards. Deshalb bauten wir uns ein Daten-Klo. Billiger und praktischer.

Ein Daten-Klo?

HOLLAND: Ein genormter Gummiring, der ein Frischwasserrohr an einer Kloschüssel arretiert, passt exakt auf eine genormte Telefonhörermuschel. Mit diesen Klorohr-Gummiringen befestigten wir das Sende- und Empfangsteil des Modems an den Muscheln des Telefonhörers.

Originell. Und umgingen das vorgeschriebene Datenübermittlungsverfahren?

HOLLAND: Wir nutzten nur das Telefon atypisch. Eingriff in einen Fernmeldeapparat war nach der damaligen Rechtsauffassung eine Straftat. Höchststrafe Fünf Jahre. Das Überstülpen von Klogummiringen über einen intakten Hörer war ein Präzedenzfall, den wir öffneten das Telefon oder den Hörer ja nicht. Ob ich mir den Hörer ins Gesicht halte, reinbrülle, ihn vor die Stereoanlage strecke oder einfach an ein kleines Gerätchen halte, das schnelle Datenpiepser von sich gibt, ist schliesslich meine Sache.

Deshalb durften Sie auch die Baupläne publizieren?

HOLLAND: Die Pressefreiheit ist ein historisch erkämpftes Recht. Wir druckten eine 16-seitige Bauanleitung, die es beim Chaos Computer Club zu kopieren gab. Ganz unverfänglich formuliert. "Diesen Kontakt solltet ihr nicht mit dem Relais verbinden, sonst funktioniert das Ding wie ein Modem." Den Anleitungstext für den Bau des Daten-Klos haben wir mittels Daten-Klos selbst in die Druckerei gesendet. Die Anleitung bewies, dass der Apparat, den wir beschrieben, auch wirklich funktionierte.

Mit derartigen Tricks umgingen Sie auch die teure Hardwarebeschaffung Anfang der 80er-Jahre.

HOLLAND: Ein deutsches Tastatur-Terminal kostete an die 10 000 Mark. Sie haben richtig gehört. Ein guter Bildschirm oder eine 5-Megabyte-Festplatte kosteten ebenfalls gegen 10 000 Mark.

Wie funktionierte der Netzzugriff ohne Internet?

HOLLAND: Es gab Datex-P, einen Datenpaket-Vermittlungsdienst. Eine Art Vorläufer des Internets. Ein beliebtes Ziel war der Computer der "Washington Post". Dort konnten die Hacker Artikel lesen, die noch nicht gedruckt waren. Andere beliebte Ziele waren der Polizeicomputer in der kanadischen Hauptstadt Ottawa oder das europäische Kernforschungszentrum Cern. Das Cern war sozusagen die Fahrschule der Hacker.

Hacken scheint damals einfacher gewesen zu sein als heute.

HOLLAND: Der Zugang zum DEC-Netz, einem der Vorgänger des Internets, war bei der Installation am Rechner auf den Benutzernamen "system" und das Passwort "manager" eingestellt. Schwierig, nicht? Mit diesem Zugang hatte man alle Rechte des Systemmanagers. Als wir auf dem Netz auch Militärrechner fandenm, die noch auf diesen Voreinstellungen waren, bekamen wir die Schlagzeile: "Deutsche Hacker dringen in US-Militärcomputer ein".

Zieht man die Empfindlichkeiten der Geheimdienste und Militärs in Rechnung, war das eine sehr gefährliche Situation.

HOLLAND: Ja. Mit diesen Leuten kann man nicht spielen.

1985 drangen einige Kinder aus dem Dunstkreis des Chaos Computer Clubs in eine französische Militäranlage ein.

«Es kann sehr gefährlich sein, zu hacken. Man lässt sich mit Kräften ein, die man nicht mehr überblickt»: Zu Besuch in Wau Hollands Haus in Ostberlin (oben und rechts).
Holland nach dem Hamburger Sparkassen-Hack im November 1984 (links)

FOTOS: DPA/KEYSTONE, MAURICE WEISS/OSTKREUZ (2)

HOLLAND: Die Kiddies berichteten, sie hätten einen grossen Zentralrechner in einer französischen Zementfabrik gefunden, über den sie gut durchschalten konnten. Wir haben die Brisanz nicht begriffen. Wozu braucht eine Zementfabrik einen derart grossen Rechner? Für normale Plattenbauten reicht ein Taschenrechner. Grossrechner braucht man nur, wenn man Raketensilos, Atombunker und Teile von Atomkraftwerken baut. Die sind aus einem Guss Stahlbeton, damit sie bei einem direkten Treffer nicht brechen. So kamen deutsche Hacker zufällig in eine französische Militärfabrik - wir waren im "Herzen der Bestie".

Das Beispiel des Hackers Tron vom Chaos Computer Club, der unter ungeklärten Umständen zu Tode kam und erhängt aufgefunden wurde, zeigt, wie gefährlich Hacken sein kann.

HOLLAND: Es kann sehr gefährlich sein, zu hacken. Man lässt sich mit Kräften ein, die man nicht mehr überblickt.

Auch auf Technologien, die man nicht mehr beherrscht?

HOLLAND: Der erste Computer, der Z3, hatte etwa 3000 Relais und konnte von seinem Erbauer Konrad Zuse noch allein überblickt werden. Spätere Prozessoren mit rund 6000 Relais konnten nur noch von einem Technikerteam verstanden werden. Anfang der 80er-Jahre hatten wir den Atari ST mit 68000 Transistorfunktionen im Prozessor. Heute sind tausendmal kompliziertere Rechner gemeinsam vernetzt. Übersicht ist nur noch kollektiv möglich.

Verlieren wir nicht nur die Übersicht, sondern auch die Kontrolle?

HOLLAND: Alle 18 Monate verdoppeln sich die Geschwindigkeit der Prozessoren und die Festplattenkapazität. Der Mensch hat in den

letzten Millionen Jahren seine Input-Output-Leistung nur unwesentlich gesteigert. Wir können mit 100 Bit pro Sekunde sprechen und etwa 1000 Bit pro Sekunde lesen. Das stimmt nachdenklich.

Wie sieht Ihrer Meinung nach die Zukunft der Menschheit aus?

HOLLAND: Wir laufen auf den totalen Überwachungsstaat zu, und keiner merkt es. Er ist schon so alltäglich, dass niemand mehr reagiert.

Ach, das klingt doch nach Panikmache und Verschwörungstheorie.

HOLLAND: Die Videokameras in London erkennen Nummernschilder von Autos und können einen Wagen durch die ganze Stadt verfolgen. Installiert wegen der IRA natürlich. Das System schützt sich selber. Wenn Sie in England mit einer Farbpistole für Rindermarkierung eine Kamera zukleben, reagiert das System so, dass mindestens eine weitere Überwachungskamera von Ihnen ein gutes Bild liefert.

Wer ständig auf Kameras achtet, bekommt den Verfolgungswahn.

HOLLAND: Stellen Sie sich vor, man würde überall Hunde beim Verrichten ihres Geschäfts filmen und die Bilder veröffentlichen. Ich bin überzeugt, die Hundebesitzer würden sofort ein Betroffenheitsgefühl entwickeln und die Persönlichkeitsrechte ihres Hundes verteidigen. Die gleichen Menschen, die klaglos an den Schildern vorbeilaufen, auf denen steht: "Hier ist ein Zentrum krimineller Aktivität. Deshalb ist dieser ganze Platz videoüberwacht."

Die zunehme Überwachung könnte sich auch selber aufheben. Wegend der ständig wachsenden Datenströme wird es immer schwieriger für die Überwacher, an Einzelinformationen über einen Menschen zu kommen.

HOLLAND: Zur Zeit von Martin Luther wurde die Schulpflicht mit drei Grundfertigkeiten eingeführt. Rechnen, Lesen und Schreiben. Im kommenden Informationszeitalter ist als vierte Qualifikation Filtern eine zwingende Notwendigkeit. Filtern. Effizienter Umgang mit den Datenmassen. Sei es im Fernsehen, am Computer oder eben auch in Archiven und Datenbanken, die permanent angelegt und erweitert werden. Nachrichtendienste beherrschen den Umgang mit Datenmassen seit zumindest Jahrzehnten.

Der Chaos Computer Club hat sich selber immer als Mahner verstanden. Das Cluborgan "Datenschleuder" beobachtet kritisch die Medienlandschaft, insbesondere auch die Wissenschaftsberichterstattung.

HOLLAND: Es gab und gibt zu viele Pseudowissenschaftler. Horst Herold, seinerzeit Chef des Bundeskriminalamtes schrieb mal von seinem deutschen Sonnenstaat der Zukunft, in dem die Computer für die Verbrechensprävention eingesetzt werden. Die Maschine merkt, wann einer gerade über eine Straftat nachdenkt, und meldet es. 1984 griffen wir einen Artikel des Deutschen Ärzteblattes auf, in dem die "Züchtung von Mensch-Tier-Mischwesen zur Verrichtung einfacher Arbeiten" gefordert wurde. Kritik und Realsatire vermischten sich. Im Online-Magazin "Bildschirmtext" kommentierten wir eine medizinische Dissertation über "Penisverletzungen bei Masturbationsversuchen mit Vorwerk-Staubsauger". Vorwerksauger hatten den Ventilator vorne am Absaugrohr. Vorwerk wollte uns auf eine halbe Million Mark wegen Rufschädigung verklagen, doch wir konnten den Doktorvater auftreiben und sogar ein Opfer. Darauf baten wir Vorwerk uns nicht zu nötigen, die Boulevardpresse einzuschalten.

Und?

HOLLAND: Die Sauger zogen die Klage zurück.

Feiner Fug?

HOLLAND: Feiner Fug.

Echelon I

Wir bedanken uns für die Beachtung aller Sicherheitsmaßnahmen...

```
Royal  Signals and Radar Establishment (NET-RSRE-EXP)
St. Andrews Road  Great Malvern
Worcestershire, WR14  3PS
GB
Netname:  RSRE-EXP
Netblock: 25.0.0.0 -  25.255.255.255
Coordinator:
Andrews,  John  (JA168-ARIN)   J.Andrews@cs.ucl.ac.uk
+44 71 387 7050  ext. 3691
Domain System inverse mapping  provided by:
NS1.CS.UCL.AC.UK  128.16.5.32
RELAY.MOD.UK   192.5.29.50
Record last updated on  01-Dec-2000.
Database last updated on  30-May-2001 23:00:23 EDT.
The ARIN  Registration Services Host contains ONLY
Internet Network  Information: Networks, ASN's, and
related POC's. Please use  the whois server at rs.
internic.net for DOMAIN related Information  and
whois.nic.mil for NIPRNET  Information. <andy>
```

Echelon II

Am Dienstagabend (3.7.) hat der Echelon-Ausschuss des Europäischen Parlaments über seinen Abschlussbericht abgestimmt. Dazu hat Ilka Schröder, MdEP (Deutschland, Grüne) zusammen mit den grünen Abgeordneten Alima Boumediene-Thiery (Frankreich) und Patricia McKenna (Irland) die folgende Minderheitenposition eingereicht:

"Es ist wichtig, das dieser Bericht betont, dass Echelon existiert. Er weigert sich jedoch, daraus politische Schlussfolgerungen zu ziehen. Heuchlerisch ist, dass das Parlament die Echelon-Abhörpraxis kritisiert, während es die Planungen eines europäischen Geheimdienstes befürwortet.

Weltweit gibt es kein Beispiel für eine funktionierende Kontrolle von Geheimdiensten und ihren undemokratischen Praktiken. Es liegt in der Natur von Geheimdiensten, dass sie nicht kontrollierbar sind. Deswegen müssen sie abgeschafft werden. Dieser Report trägt dazu bei, einen europäischen Geheimdienst zu legitimieren, der in gleicher Weise wie Echelon gegen Grundrechte verstoßen wird.

Für die Mehrheit des Parlaments steht die Industrie im Mittelpunkt, deren Profitinteressen angeblich durch Wirtschaftsspionage gefährdet sind. Das zentrale Problem ist jedoch, dass niemand mehr über Entfernungen vertraulich kommunizieren kann. Politische Spionage ist eine wesentlich größere Bedrohung als Wirtschaftsspionage.

Dieser Bericht spielt diese Gefahren von Echelon systematisch herunter, während er zur ENFOPOL-Abhörplanung der EU schweigt. Es ist für jede Gesellschaft eine grundsätzliche Entscheidung, ob sie unter permanenter Überwachung leben will. Mit der Annahme dieses Berichts zeigt das Europäische Parlament, dass ihm am Schutz von Menschen- und Bürgerrechten nicht viel gelegen ist."

Quelle: *Presseerklärung Nr. 17/2001, Berlin 04.07.2001 "Geheimdienste: Echelon-Ausschuss des Europäischen Parlaments Minderheitenvotum"*

Mehrheit der Amerikaner für Internetüberwachung

Die Mehrheit der US-Amerikaner hat sich in einer Umfrage für eine Kontrolle des Internets ausgesprochen. Mehr als die Hälfte der Befragten würden sich im Internet weniger sicher als im "richtigen" Leben fühlen und befürworteten deshalb eine solche Kontrolle, heißt es in einer neu veröffentlichten Studie der gemeinnützigen Merkle Foundation.

60 Prozent der Befragten sprachen sich dafür aus, dass Unternehmen oder gemeinnützige Organisationen die Regulierung des Internets übernehmen. Als Kandidaten für eine mögliche Web-Regierung wurden auch der Microsoft-Gründer Bill Gates und Papst Johannes Paul II. genannt.

Trotz ihrer Bedenken hatten die meisten Befragten eine positive Einstellung zum Internet. 63 Prozent aller Befragten und 83 Prozent der Internet-Nutzer sagten, sie hätten eine gute Meinung vom Internet. 47 Prozent aller Befragten sagten dagegen, das Internet mache ihnen eher Sorgen - vor allem wegen der dort verbreiteten Pornographie und Gewalt sowie wegen mangelnder Privatsphäre für die Nutzer. Die Studie basiert auf mehreren Telefon- und Online-Umfragen sowie ausführlichen Interviews mit ausgewählten Bevölkerungsgruppen.

Quelle: kurier.at/apa/reuters/stp 11.07.2001

Kleine Überraschung in der Neuen Frequenzzuteilungsverordnung – IMSI-Catcher jetzt legal?

In der neuen Frequenzzuteilungsverordnung (FreqZutV), veröffentlicht im Bundesgesetzblatt Jahrgang 2001, Teil 1, Nr. 20 (ausgegeben zu Bonn am 08.05.2001) findet sich eine kleine Überraschung. Besagt das Kapitel "Allgemeine Voraussetzungen der Frequenzzuteilung" (§4) an- und für sich, daß

(1) Frequenzen werden zugeteilt, wenn

1. Sie für die vorgesehene Nutzung im Frequenznutzungsplan ausgewiesen sind,
2. sie verfügbar sind und
3. die Verträglichkeit mit anderen Frequenznutzungen gegeben ist.

Dann kommt es:

"*Frequenzen, die von Behörden zur Ausübung gesetzlicher Befugnisse benötigt werden, werden auch abweichend von Satz 1 zugeteilt, wenn keine erheblichen Störungen anderer Frequenznutzungen zu erwarten sind. Der Antragsteller hat keinen Anspruch auf eine bestimmte Einzelfrequenz.*"

Letzterer Absatz bietet nun hinreichend Spielraum für Assoziationen verschiedenster Art.

Da nun gerade die GSM-Netzbetreiber von einer sogenannten Sicherheitsbehörde auf diesen Absatz hingewiesen wurden, kann es sich sowohl um den Versuch der Legalisierung eines IMSI-Catchers als auch um eine Generalgenehmigung von digitalen Burst-Wanzen im GSM-Frequenzbereich handeln.

Der IMSI-Catcher kämpft derzeit mit dem Problem, eben genau erhebliche Störungen bei den GSM-Netzen zu verursachen, weswegen der Betrieb in der BRD an- und für sich illegal ist. Die Netzbetreiber finden das auch überhaupt nicht lustig, daß mehrere dieser Geräte offenbar in der Bundesrepublik Deutschland aktiv im Einsatz sind, haben aber das Problem trotz der Ihnen bisher zugestandene Frequenzhoheit nicht durchsetzen zu können. Zur Durchsetzung fehlt Ihnen nach wie vor die sichere Detektierbarkeit eines IMSI-Catchers, da die von Ihnen produzierten Netzstörungen sich nur bedingt online nachvollziehen und vor allem von anderen "normalen" Netzstörungen (witterungsbedingten Antennenausfällen, Funkstörungen etc.) nicht unterscheiden lassen. Ihnen fehlt bislang also ein IMSI-Catcher-Catcher um die Charakteriska des IMSI-Catchers klar zu erkennen und dann die Strafverfolgungsbehörden darauf aufmerksam zu machen. Wobei es gerüchteweise ein innerbehördlicher Vorgang sein soll, das Gerät dann zu aktivieren.

Die andere Möglichkeit wäre die Unterbringung von digitalen Burst-Wanzen im GSM-Frequenzbereich, die z.B. als spread-Spektrum Modell eine Detektierbarkeit gerade aufgrund der Vielzahl von anderen Sendern im GSM-Frequenzbereich reichlich schwer machen dürften.

Wer mehr dazu weiß möge sich melden... Input bitte wie immer an an *crd@ccc.de*.

Echelon III: USA schließen Abhörstation Bayern - BND übernimmt ?!

zunächst die offizielle amerikanische Meldung:

US Army Intelligence and Security Command (INSCOM), INSCOM POC: Shirley Startzman, (703) 706-1283

Bad Aibling Station to close

FORT BELVOIR, VA. May 31, 2001 - The U.S. Forces stationed at Bad Aibling Station (BAS), Germany, will be consolidated and realigned according to an announcement today. The Department of Defense made the decision at the request of the Director of the National Security Agency/Chief, Central Security Service (NSA/CSS). Current operations at the U.S. Government facility at Bad Aibling will cease on Sept. 30, 2002, with return of the facility to the German Government to be completed by fiscal year 2003. The U.S. personnel currently stationed at BAS will gradually be reassigned to other operational units. Bad Aibling Station is an integral part of the Department of Defense communications network and provides support to U.S. and allied interests. There has been a U.S. presence in Bad Aibling since 1947.

The U.S. Army took command of the station in 1952. In 1971, the station became a predominately civilian operation managed by NSA. In 1972, its name was changed to the current Bad Aibling Station. In 1994, BAS management was transferred from NSA to the U.S. Army Intelligence and Security Command (INSCOM). Bad Aibling Station is located in the village of Mietraching and is approximately two miles from the center of the town of Bad Aibling, Germany. Bad Aibling is a Bavarian resort town located about 35 miles southeast of Munich.

Und dann noch ein interessanter Halbsatz aus einer DPA-Meldung vom 01.06.2001, die um 13:44 unter der Überschrift "USA schließen Abhörstation Bayern" berichtete:

"*Die USA wollen nach Angaben des "Münchner Merkur" ihre Abhörstation im oberbayerischen Bad Aibling aufgeben. [...] Nach Informationen der Zeitung wird in deutschen Sicherheitskreisen darüber spekuliert, der Bundesnachrichtendienst (BND) werde die US-Anlage übernehmen, wenn das Areal Ende 2003 an die Bundesrepublik zurückfällt.*"

Bleibt zu resümieren: wäre ja auch verwunderlich, wenn der Bundesnachrichtendienst die am selben Tag der Verkündigung der Bad-Aibling Schließung ihm zugewiesenen Ausweitungen im Zusammenhang mit der Novellierung des G10-Gesetzes (siehe *http://www.ccc.de/CRD*) nicht in Anspruch nimmt.

From: Andreas Bogk <andreas@berlin.ccc.de> Date: Wed Jul 25, 2001 05:55:08 PM Europe/Berlin To: intern@lists.ccc.de Cc: debate@fitug.de

Subject: Re: [Telepolis] Die Privatkopie - vom Aussterben bedroht

Telepolis schreibt[0]:

Nahezu unbemerkt von der Öffentlichkeit hat der EU-Ministerrat im April die Richtlinie zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft verabschiedet. Diese wird zu einer erheblichen Ausweitung der urheberrechtlichen Monopolrechte führen - auf Kosten des "free flow of information".

Also ich weiß ja nicht, wie es euch so geht, aber ich kriege langsam echt genug.

Daß die USA ein faschistischer Polizeistaat ist, in dem die verfassungsmäßigen Rechte der

Bürger weniger wert sind als die Gewinne der Medienkonzerne, wissen wir nicht erst seit der Verhaftung von Skylarov. Aber jetzt ist es so sichtbar, daß ein Blinder es sieht, und die Konsequenzen so drastisch, daß ich dieses Land nicht mehr besuchen kann.

Daß die Gesetze in Europa hauptsächlich durch Lobbyarbeit und Bestechung zustandekommen, ist ja auch nicht neu. Aber langsam wird sichtbar, in welchem Ausmaß das passiert, und wie wenig die demokratische Kontrolle ueber diesen Prozess funktioniert. Jetzt kriegen wir ein Gesetz, daß das Recht auf Privatkopien abschafft, und Umgehungswerkzeuge unter Strafe stellt. Toll.

Ist euch eigentlich klar, was das bedeutet? Demnächst wird es nicht mehr möglich sein, private Archive aufzubauen. Das bedeutet, daß die Geschichtsschreibung zentralisiert wird, und der Manipulation der Geschichte Tür und Tor geöffnet werden. Wer 1984 gelesen hat, darf an dieser Stelle eine Gaensehaut kriegen.

Was mir Angst macht, ist die weitgehende Ignoranz gegenüber der Gefahr des Zusammenbruchs der Demokratie. Offensichtlich sind viele Leute der Meinung, da ja alle diese Gesetze auf demokratischem Wege (mehr oder weniger, siehe Bestechungsskandal) zustandegekommen sind, wird uns die Demokratie auch erhalten bleiben. Wie schnell die Abschaffung von Demokratie und Rechtsstaat gehen kann, zeigen aber die aktuellen Ereignisse in Italien, wo Journalisten willkürlich verhaftet und gefoltert werden, Hunderte von Demonstranten ohne rechtliche Grundlage festgehalten werden. [1]

Und währenddessen deckt in Deutschland die neue Regierung die Verbrechen der alten Regierung, werden Demonstrationsteilnehmern von der Polizei die Radios abgenommen, den Geheimdiensten mehr Rechte zur Bespitzelung der eigenen Bürger eingeräumt, und die Reisefreiheit abgeschafft.

Ich weiß, daß es vor allem für Wessis, die in ihrem Leben noch keinen Wechsel des Gesellschaftssystems erlebt haben, schwierig ist, den Verlust der Demokratie als reale Bedrohung wahrzunehmen. Tja, wir haben damals in der DDR zwar gehofft, aber auch irgendwie nicht geglaubt, daß sich etwas ändern wird. Dann ging plötzlich alles sehr schnell.

Und eins muß man den letzten Machthabern in der DDR zuerkennen: sie haben den Anstand besessen, die Leute, die auf die Straße gegangen sind, nicht zu erschiessen.

Es ist an der Zeit, die Demokratie in diesem Lande, in Europa und auf der Welt zu verteidigen, mit dem nötigen Ernst und mit den nötigen Mitteln. Momentan können wir vielleicht noch etwas erreichen, indem wir auf die Meinungsbildung und Gesetzgebung einwirken, diese Chance sollten wir nutzen. Aber es sollte jedem klar sein, daß wir möglicherweise bald einen Punkt erreichen, an dem das nicht mehr geht.

Im Grundgesetz, Artikel 20 steht: "Alle Staatsgewalt geht vom Volke aus". Und da steht auch: "Gegen jeden, der es unternimmt, diese Ordnung zu beseitigen, haben alle Deutschen das Recht zum Widerstand, wenn andere Abhilfe nicht möglich ist." [2]

Vielleicht ist es an der Zeit, diese Rechte in Anspruch zu nehmen.

Gruss Andreas

[0] http://www.heise.de/tp/deutsch/inhalt/te/9123/1.html

[1] http://www.heise.de/tp/deutsch/inhalt/co/9161/1.html

[2] http://www.rewi.hu-berlin.de/Datenschutz/Gesetze/gg.html

Wave-LAN: Wireless Encryption Placebo

von Rüdiger Weiss, Amsterdam <ruedi@cryptolabs.org>

Wave-LAN ist was Feines. Die Möglichkeit an einem entspannten Ort in der Sonne zu sitzen und trotzdem über akzeptable Bandbreite zu verfügen, erfüllt ohne Zweifel einen uralten Hackertraum. Und der Dilettantismus mit dem die meisten Wave-LAN Nutzer vorgehen, öffnet sogar noch weitere Spielwiesen.

Bisher war ja alles ganz witzig. Clevere Junghacker kümmerten sich rührend um kommunikationsbegierige Expo-Roboter. Auf der Cebit war es ein nicht unerhebliches Problem angesichts der vielen mit großer Power sendenden unverschlüsselten Wave-LANs, die Linuxtreiber zum Einloggen in das eigene verschlüsseltes Netz zu bewegen. Und schliesslich glauben einige Universitäten , dass frei wählbare MAC Adressen eine ausreichende Authentifizierung darstellen (Thanks to SK).

Nicht mehr lustig ist die Sache natürlich, wenn Krankenhäuser aus Kostengründen auf die aufwendige Verkabelung verzichten und ihre Patientendaten unverschlüsselt übertragen oder man hören muss, dass ein grosser EDV-Dienstleister am Potsdamer Platz die DEBIlität (Sic!) besitzt, sich von der Straße aus hinter die Firewall hupsen zu lassen.

Der CCC hat mit Recht unter anderem das Einschalten Wired Equivalent Privacy(WEP) Verschlüsselungs- und Authentifizierungsprotokoll angemahnt. Leider taugt WEP weder für Vertraulichkeit noch für Zugangsschutz. Wobei hier sogar das Kunststück fertig gebracht wurde, die Sicherheit von normalen 40 Bit Kryptographie nochmal zu unterbieten. Wegen der hohen Praxisrelevanz soll trotzdem zunächst nochmal auf das 40-bit Problem eingegangen werden.

40-bit Verschlüsselung: Unsicher gegen fast alle Angreifer

WAVE-LAN Systeme, welche 40-bit Karten ("Silber") einsetzten sind für praktisch alle Angreifer unsicher. Hersteller, welche von 64 bit WEP sprechen, beweisen im Übrigen lediglich mangelnde kryptographische Kompetenz. 24 bit des 64 bit RC4 Schlüssels werden der verschlüsselten Nachricht als Klartext vorangestellt, woraus sich die effektive Schlüssellänge auf 40 bit verkürzt. Da die Nutzlosigkeit derartig schwacher Kryptographie schon unzählige Male auseiandergesetzt wurde hierzu nur ein Satz:

Ein Angriff auf 40-bit RC4 verschlüsselte Nachrichten wurde bereits mehrfach erfolgreich

demonstriert, für die nötigen Anpassungen bekommt man an den meisten Unis nicht mal einen Praktikumsschein für das Informatik Grundstudium, und auch der konkrete Rechenaufwand dürfte jedes Wochenende ungenutzt in jedem mittleren Fakultäts-Rechnerpool rumidlen.

Die einzig gute Nachricht für 40-bit Kartenbesitzer: um die Sicherheit der teureren 128 bit Karte ("Gold") ist es auch nicht wirklich viel besser bestellt. Wobei es sich übrigens eigentlich wiederum um 104 bit Karten handelt.

Solides Halbwissen reicht nicht für Protokolldesign

Das ganze Design des WEP Protokolls erinnert an einen Studienanfänger, welcher aus religiösen Gründen nur jede zweite Vorlesung der Kryptographie-Einführung besucht hat. Das ist nicht weiter verwunderlich, da viele, insbesondere auch in der deutschen Computersicherheitsgemeinde, der Meinung sind, Kryptographie sei ausreichend verstanden und könnte problemlos nebenherlaufen. Immerhin kann man einen Fortschritt attestieren. Bisherige Industrieprotokolle erinnerten eher an Entwürfe von Leuten, welche nur jede 5. Kryptographievorlesung besucht haben. Was umgekehrt allerdings sehr lobenswert ist, ist daß die Autoren derart viele Anfängerfehler eingebaut habe, dass man die ersten 5 Vorlesungen einer Kryptographieeinführung damit problemlos bestreiten kann.

Es gibt einen gemeinsamen Schlüssel, welcher sicher an alle Teilnehmer gesendet werden muss ("Shared Secret"). An diesen Schlüssel (40 bzw. 104 bit) werden weitere 24 bit zur Erzeugung des Paketschlüssels angehängt. Dieser wird dann zu Verschlüsselung eines Datenpaketes verwendet. Die 24 bit IV werden als eine Art Initial Vektor (IV) bei jedem Paket im Klartext übertragen und sind daher allgemein lesbar. Als Prüfsumme wird CRC-32 verwendet. Diese wird ebenfalls mitverschlüsselt.

RC4 statt Selbsgestricktes

Das Leben eines Kryptoforschers ist manchmal ganz schön hart. Fast alle akademischen Verfahren erfordern eine harte, lange Analyse, um dann – und das ist dann schon oft das höchste der Gefühle – eine wissenschaftliche Veröffentlichung zu erhalten, die meist so beginnen könnte:

> "Zuerst zerstören wir all die überflüssigen Planeten der benachbarten Galaxien um Platz für Speicher zu schaffen, anschließend füttern wir und unsere Ahnen das Verfahren einige Milliarden Jahre mit fein ausgewählten Klartext/Ciphertext Kombinationen, und schon haben wir eine leichte statistische Schwäche einer reduzierten Variante des Verschlüsselungsverfahrens gefunden".

Da sind doch die handgemachte Verfahren der Industrie, die schon durch schiefes Hinschauen die Schlüssel herausrücken (DVD, GSM, ...) eine echte Erholung.

Immerhin diese Lektion hatten die Protokollentwickler gelernt. Allerdings trafen sie zielsicher unter den wirklich zahlreichen von der Forschungsgemeinde als hinreichend sicher geltenden Algorithmen die wohl schlechtest mögliche Wahl. RC4 ist ein patentiertes Verfahren von RSA Security Inc. Es ist so elegant und schnell, dass sich absolut kein gutes kryptographisches Gefühl einstellt. Und in der Tat wurden in der letzten Zeit wiederholt statistische Probleme aufgezeigt. Ein Blick in die CCC Datenschleuder hätte übrigens genügt (http://cryptolabs.org/ arcfour/ WeisDatenschleuderSummer2000arcfour.txt) um auf dem Laufenden zu bleiben.

Übrigens, wenn das Protokoll insgesamt nicht so katastrophal schwach wäre, würde es sich vielleicht auch lohenen nachzusehen, ob die ersten Bits des Ausgabestromes von RC4 verworfen werden. Die haben nämlich einige unschöne Eigenschaften.

Das Hauptproblem ist jedoch, dass RC4 ein Stomchiffrierer ist, und sowas sollte man nur verwenden, wenn man sich damit auskennt.

Problematisch: Bausteine falsch kombiniert

Man kann Stromchiffrierer als Black-Box betrachten in die man einen kryptographischen Schlüssel steckt und der darauf hin einen beliebig langen Strom von Schlüsselbits erzeugt, welche mit dem Klartext zum Verschlüsselten Text XOR verknüpft werden. Also

```
Ciphertext = Klartext XOR Schlüsselstrom(Key)
```

die Entschlüsselung ist genauso einfach:

```
Klartext = Ciphertext XOR Schlüsselstrom(Key)
```

Zwei Dinge sind recht offensichtlich. Erstens hängt der Schlüsselstrom nur vom Schlüssel und in keiner Weise vom Klartext ab. Wenn man also 2 Nachrichten mit dem selben Schlüssel verschlüsselt hat man ein Problem:

```
Ciphertext1 = Klartext1 XOR Schlüsselstrom(Key)
Ciphertext2 = Klartext2 XOR Schlüsselstrom(Key)
```

Kennt man nun den Klartext1, so kann man auch den Klartext2 lesen, denn:

```
Ciphertext2 XOR Ciphertext1 XOR Klartext1
= (Klartext2 XOR Schlüsselstrom(Key))
(XOR Klartext1 XOR Schlüsselstrom(Key))
XOR Klartext1 = Klartext2
```

Und es kommt sogar noch übler, es gilt nämlich

```
Ciphertext1 XOR Ciphertext2 = Klartext1 XOR Klartext2
```

Da die Klartexte meist eine erratbare Struktur haben, reicht meist also auch das passive Abhören.

Zweitens sind Stromchiffrierer empfindlich gegen Manipulationen des Ciphertextes. Wenn man ein Bit im Ciphertext umkippt, kippt genau dasselbe Bit im Klartext nach der Entschlüsselung.

Wenn man darüber hinaus wie in WEP auch noch eine lineare Prüfsumme verwendet, kann man problemlos gefälschte Pakete mit gültiger Prüfsumme erzeugen.

Eine goldene Regel ist also, daß wenn man schon Stromchiffrierer einsetzt, dringlichst eine Vermeidung von Schlüsselwiederholungen zu erzwingen und für die Integrität der Daten sorgen sollte. In beiden Anforderungen versagt WEP kläglich.

Professorale Hacker/die üblichen Verdächtigen zertrümmern WEP

Nikita Borisov (UC Berkeley), Dr. Ian Goldberg (Zeroknowledge) und Prof. Dr. David Wagner (UC Berkeley) - keine Sorge, dass sind immer noch dieselben geschätzten Hacker und Party-Animals - warfen in Februar 2001 einen kurzen Blick auf den WEP Standard. Dieser kostet ärgerlicherweise echt Kohle und wurde daher vorher wohl nicht ausreichend öffentlich analysiert. Und das ist auch deswegen ärgerlich, weil die ganze Konstruktion so grottenschlecht ist, daß diese Angelegenheit eine schwer entschuldbare Verschwendung von Ressourcen einer der besten Forschergruppen der Welt darstellt. Da die Gruppe die jeweiligen Angriffe ausgezeichnet dokumentiert hat (http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html), gebe ich nur einen kurzen Abriss.

Implementierung: Realwelt Problem Nummer 1

WEP ist auch bei einer klugen Implementierung katastrophal unsicher. Da in der Praxis auch mit der schnellstmöglichsten, standarkonformen Implementierung gerechnet werden muss, sollte man auch, wenn es in diesem Fall wirklich an das Erschiessen eines Fischstäbchens erinnert, dies bei der Analyse berücksichtigen. Untersuchen wir jetzt unter welchen Umständen eine gefährliche Wiederholung des IV und damit des Stromchiffriererschlüssels auftreten.

Der WEP Standard "recommends" nicht requires" den Wechsel von IV bei jedem Paket. Dies bedeutet, dass auch eine Implementierung, welche immer den selben Schlüssel verwendet vollständig standardkonform ist. Auch setzen einige Implementierungen den IV zu 0 bei jeder Initialisierung. Und dann könnten einige ganz Clevere IV auf die Idee kommen, alle IVs mit einem starken Zufallsgenerator erzeugen. Dann allerdings beginnt es wegen des Geburtstagsparadoxons schon nach 2^{12}= 4096 Paketen heftig zu kollidieren.

Auch die bestmögliche Implementierung ist unsicher

Aber selbst, wenn man richtigerweise den ersten IV zufällig initialisiert und bei jedem Paket den IV inkrementiert, nutzt man zwar den ganzen jeweiligen Schlüsselraum, doch dieser hat lediglich die Mächtigkeit von 2^{24}. Es ist eine einfache Rechenaufgabe, daß in diesem Falle, wenn man eine Paketgrösse von 1500 byte und die verwendete Übertragungsbandbreite von 5-11 Mb annimmt, nach einigen Stunden IV Wiederholungen eintreten.

Zudem gibt es auch bei einer 104-bit Karte nur 2^{24} verschiedene Schlüsselströme. Verfügt man über eine 24 GB Platte (soll ja vorkommen) kann man versuchen eine Art vollständiges Codebuch erzeugen, mit welchem man ohne Kenntnis des eigentlichen Schlüssels jedes Paket entschlüsseln kann.

Authentifizierung versagt u.a. wegen Linearität der Prüfsumme

Wer nun aber annimmt, es könnte nicht mehr schlimmer kommen, irrt leider. Die Authentifizierung ist noch weit schlechter als die Verschlüsselung.

Als Prüfsumme verwendet WEP das bekannte CRC-32 Verfahren. CRC-32 ist schnell zu implementieren, gut im zufällige Bitfehler aufdekken und beliebt als mathematische Übungsaufgabe für Informatiker. Als kryptographische Prüfsumme ist es schlicht und einfach ein Alptraum. Wie der Name sagt, erzeugt das Verfahren gerade mal eine 32 bit Ausgabe. Selbst bei der Verwendung einer starken kryptographischen Hashfunktion (z.B. SHA) würden 32 bit in gar keiner Weise ausreichen. Aber es kommt noch dicker. CRC ist linear. Linearität einer Prüfsumme ist eine Eigenschaft, die jedem Kryptographen eigentlich den Schlaf rauben sollte. Scriptkiddy-einfach wird es aber wenn man CRC-32 in "Zusammenarbeit" mit einem Stromchiffrierer verwendet. Stromchiffrierer sind auch linear, also kann man beliebig Ciphertext manipulieren und die Prüfsumme anpassen.

Sei `IP-EC` die IP Adresse der ReallyEvilCorporation.com und `IP-NH` die Adresse von PrettyNiceHackers.org, so findet ein verschlüsseltes Pakete `IP-EC XOR UnbekannteSchluesselstrombits|| ....|| CRC-32(Paket) XOR AndereUnbekannteSchluesselstrombits` nach einer leichten Anpassungen `IP-EC XOR UnbekannteSchluesselstrombits {XOR IP-ECXOR IP-NH}||...|| CRC-32(Paket) XOR AndereUnbekannte-Schluesselstrombits {XOR CRC-32(IP-EC XOR IP-NH)}` mit gültiger Prüfsumme die richtige Adresse.

Praktische Angriffe

Im Originalpaper sind dann noch weitere praktische Angriffe aufgelistet. Das Einzige was man braucht um, WEP zu überwinden, ist ein schwachbrüstiger Handheld mit Wave-LAN Karte und eine kooperative Firmware, welche sich in einen promiscuren Modus schalten lässt. Da einige Karten netterweise über updatebare Firmware verfügen, entfällt auch die lästige Rumlöterei. Die gute Nachricht ist, daß zwei Gruppen, die meines Wissen daran arbeiten, aus philantrophen Anarchisten bestehen.

Problemlösung

Kryptographie ist schwierig. Offensichtlich ist nicht einmal die IEEE in der Lage ohne Review der Wissenschaftsgemeinde ein halbwegs brauchbares Protokoll zu designen. Konsequenz sollte daher der Einsatz von von ausführlich analysierten kryptographischen Protokollen sein. Als kurzfristige Lösung sei der Einsatz von IPSEC angeregt. Die elementaren Maßnahmen das Wave-LAN zu verstecken (vielleicht sogar ohne lerratbarem Namen) und trotz der Unzulänglichkeit WEP einzuschalten, sind als kryptographische Notversorgung natürlich auch weiterhin zu empfehlen.

All your base...

von maz & morix

"Aha", dachte man sich, als die erste große Halle der Cebit 2001 von den grade angekommenen Hacksportlern betreten wurde. Die Akkus waren frisch aufgeladen, man war gespannt. Erste Halle, ein Elsa-Accesspoint bestrahlte die Athleten mit einer Standardkonfiguration. Schnell ein flauschiges Plätzchen auf einer Treppe zur IBM-Lounge gesucht und das WaveLAN einmal näher angeschaut...

Das Thema WaveLAN, IEEE 802.11, ist schon seit längerer Zeit ins Gerede gekommen. Nach dem Einsatz dieser komfortablen Technik auf der Expo-Weltausstellung im Jahre 2000 müssten jedoch die verantwortlichen Techniker damit rechnen, daß ein Accesspoint, der nicht ausreichend konfiguriert ist, für jeden zugänglich ist. Ein Sportler entdeckte auf der Expo einen Accesspoint für sich und zwar genau den Accesspoint, über den zahlreiche Roboter mit ihrer "Zentrale" kommunizierten, während sie scheinbar autonom durch die Gegend fuhren und Besucher anquatschten.

Aber keiner hat dazugelernt. Was denkt ein Systemadministrator, wenn er eine neue Basestation in das Firmennetz hängt und auf der grafischen Oberfläche die Konfiguration zusammenklickt?

Da werden Punkte wie "Sicherheit anschalten" einfach erstmal ignoriert. Was heißt denn "Sicherheit anschalten"? Die Sicherheit, die eine Basestation bieten kann, ist trivial – kein größeres Hindernis für jemanden, der alles darum geben würde, in dieses und jenes Netzwerk zu gelangen. Zwei Punkte erhöhen die Sicherheit jedoch fürs Erste ungemein:

+ Aktivieren eines "hidden network"
+ WEP Encryption anschalten.

Ein als "hidden" bezeichnetes Netzwerk gibt den Namen des WaveLANs vorerst nicht allen vorbeischlendernden Leuten preis. Jedes WaveLAN hat einen Netzwerknamen und bei einem "versteckten" Netzwerk muss jeder, der sich da einklinken will, diesen Netzwerknamen kennen. WEP steht für "Wired Equivalent Pricacy" und bedeutet nichts anderes, als "Sicherheit in dem Maße, wie sie ein verkabeltes Netzwerk bietet". Die Verschlüsselung ist relativ schwach und ohne mittleren/größeren Aufwand zu knacken. WEP setzt auf einen Key, der immer gleich bleibt und der sowohl dem Accesspoint als auch der Station bekannt sein muss, die sich dort einloggen will. Dabei gibt es unterschiedliche Hardware: Die billige Variante setzt auf 40

bit (so gewählt wegen den Restriktionen des US-Governement, was den Export harter Kryptographie angeht), die andere teure auf "sogenannte" 128bit Verschlüsselung, die eigentlich nur 104bit Schlüssel verwendet. Dieser secret key wird nun von den Kommunikationspartnern genutzt, um den "body" des Daten-frames zu verschlüsseln. Dazu wird zuerst eine Checksumme des Klartextes gebildet und an den Klartext angehängt (dies dient lediglich der Integritätsprüfung der übermittelten Daten). Als nächstes wird ein "initialization vector" gebildet, aus dem mittels RC4 und dem secret key ein keystream aus pseudozufälligen Bytes erzeugt wird. Als letztes wird der Klartext plus Prüfsumme mit dem keystream "geXORt" und mit dem Initialisierungsvektor über den WaveLAN-Link übermittelt.

Na, und neben "hidden network" und "WEP" gibt es noch Zugriffsbeschränkungen über die Hardware (MAC) Adressen der Karten, was allerdings nicht wirklich sicher ist, da die Mac-Adressen auf den WaveLAN-Karten jederzeit geändert werden können.

Aha-Erlebnis Nummer Eins folgte auch gleich das Zweite: während man sich noch auf der Treppe der ersten besuchten Halle lümmelte, drangen Mitarbeiter des "großen Blauen" zu den Sportlern vor und schauten interessiert über deren Schulter. Man sei ja nicht unschlau und bemerkte sogleich treffend, daß es sich doch um ein offenes WaveLAN handelt - "Bei uns," warf eine Person des IBM-Standpersonals ein, "ist alles sicher. Wenn ihr hier in unser Netz eindringt, rollen Köpfe. Wir haben hier nämlich das gesamte Intranet von IBM mit diesem WaveLAN verbunden."

Soso. Das "IBM Intranet" ist mit diesem WaveLAN auf der Cebit verbunden. Den Vorurteilen zum Trotz, Nerds würden sich jeglicher verbaler Kommunikation verschließen, wurden die Sportutensilien gut in den Taschen verstaut und ein paar Meter weiter ein Stand mit kleinen WaveLAN-tauglichen IBM Notebooks besucht. Ja, mit dem Gedanken ein wenig mit der netten Dame zu plauschen, die das Notebook bewachte. Als sie das mitgebrachte z50 erblickte, sagte sie auch gleich "das ist aber niedlich." – und schon waren zwei in der Regel gesellschaftlich hermetisch voneinander getrennte Lebensformen im Gespräch. Es wurden Notebooks hin- und hergereicht, Gewichts- und Größenvergleiche angestellt und man kam letztlich auch auf WaveLAN zu sprechen. Oh, ob man sich das nicht einmal ansehen könnte, wie die WaveLAN-Konfiguration auf einem Windowsrechner aussieht - *klick* *klick* *klick* - Aha, alles da: Netzname (hidden), Key in der Registry...

Nun nochmal die Notebooks aufklappenderweise auf den Fussboden zwischen das IBM-Personal gesetzt um wenige Minuten später schnell wieder zuzuklappen und sich schleunigst zu entfernen.

Es kamen noch viele Hallen, in denen einige Zeit verbracht wurde. Man wurde so ziemlich überall mit IP-Adressen, Nameserver- und Gateway Adressen beworfen - größtenteils sogar offizielle IP-Adressen größerer Konzerne. Überall hatte man Spaß mit Accesspoints, Ciscos, und den Rechnern im Netzwerk.

Eigentlich hätte man ja erwartet, daß die Leute wissen, wie man am besten einen Acesspoint einrichtet... Aber gut, vielleicht hat das ja auch ein wenig mit den hektischen Vorbereitungen auf so einer Messe zu tun. Und was tut man, wenn man eh keine Zeit für Kleinigkeiten hat? Ja, man gibt der Basestation vielleicht nur 'ne andere IP und das reicht. Der Name bleibt: SCHNUCKEL, ELSA, SUN1,... Als die Sportsfreunde jedoch ihr Gerät aufklappten und sieben vorhandene offene WaveLANs die Entscheidung schwer machten, entschieden sie

sich, das Netz mit dem äußerst interessanten Namen "OFFICE" näher anzusehen.

Zählen wir zusammen: Fehler Nr.1: kein "hidden network", Fehler Nr.2: keine WEP-Verschlüsselung und Authentifizierung, Fehler Nr.3: DHCP mit offiziellen IP-Adressen, Fehler Nr.4: Das Netz OFFICE zu nennen...

Zufällig gab es dort auch noch Strom und die schon recht matten Akkus konnten sich ein wenig regenerieren, während die Sportler begeistert breitbandiges Internet naschten und... Fehler Nr.5: Wie kam dieser Regionalmanager der Tiscali/Nacamar GmbH eigentlich auf die Idee, von dort aus über eine unverschlüsselte Verbindung seine Mails zu poppen??

Da ging dann wohl doch etwas in die Hose... nachdem 10MB geschäftsinterne Unterlagen, Bilanzen, Angebote und Bewerbungen samt Bewertung und Jahreseinkommen den Weg in die Luft fanden, fand sich im Nachhinein erstmal kein "Verantwortlicher". Man entschloss sich nämlich, die Herren beim zweitgößten Europäischen Internetprovider mal darauf hinzuweisen, daß mit persönlichen Unterlagen eher unsensibel umgegangen wurde.

In jedem Fall, so wurde berichtet, gab es einige interessante Internas die dem einen oder anderen viel Zeit und Mühe ersparen könnte ;)

Leider nahmen die Veranstalter der Cebit keine Rücksicht auf nacht- und abendliebende Menschen und so mussten die begeisterten Sportler den Ausgang suchen.

Aber das soll nicht das Ende gewesen sein.

Man nehme: eine handvoll Nerds, die sich in engen PKWs wohl fühlen, ein paar Laptops, ein paar Antennen und ein paar PDAs. Diese stecke man in ein Auto und lasse sie ein wenig durch die Ortschaft fahren... Nachdem diverse "Security-Consulting Unternehmen", Buchhandlungen und div. andere mittelständige Unternehmen so frei waren, die umliegenden hundert Meter mit Internet und IP zu bestrahlen, stieß man im Vorbeilaufen auch auf größere Unternehmen aus der KFZ- und Waffenproduktion. Wow! Ein /8 Netzwerk, viele Ciscos (die nichtmal ein admin-Passwort gesetzt hatten), eine “Netzwerkanalysespielwiese” wie aus dem Regelbuch. Näheres braucht nicht erläutert zu werden. Man verbrachte Nächte und Tage in umliegenden Cafes und PKWs.

Um auch einmal lobend auf den Sportseiten diverser Zeitschriften erwähnt zu werden, traf man sich mit einem Reporter vom Spiegel, um ihm Spielregeln und Spielorte zu erklären. Der Hintergrund der Turniere sollte einmal klar ausgesprochen und bekannt gemacht werden: Der gemeinen Bevölkerung verständlich zu machen, daß es mit ihrer Privatsphäre nicht all zu ernst genommen wird.

Den Leuten auch beizubringen, wo immer es technisch möglich ist, Verschlüsselungstechniken einzusetzen, da auch ihr WaveLAN oder andere, auf die sie vielleicht einmal angewiesen sein könnten, theoretisch zum Austragungsort sportlicher Wettkämpfe auserkoren werden könnte. Reporter mögen es anscheinend, live dabei gewesen zu sein und so schlug auch der Reporter, mit dem sich die Sportler trafen vor, einmal nachts loszuziehen, um ihm das mal zu demonstrieren. Er meinte, man könne ja mal die Straße XY runterfahren, da wäre es ja gut möglich, daß man Erfolg hätte. Fehlanzeige. Aber: durch Zufall stieß man dann auf ein eher weniger lustiges WaveLAN. Voller Tatendrang und Frohsinn tappsten die Sportler durch einschlägiges, von "New Economy" durchdüngtes Gebiet, bis auf den mitgebrachten iPAQs plötzlich der Netzname "Meoclinic_Funklan" auftauchte, einer noblen Luxusprivatklinik mit Hotelathmosphäre im Zentrum von Berlin. Multicast Video, "die Operation live und unge-

schnitten". Die MS SQL Server waren da auch schon etwas älter...

Tags drauf, den Spiegelreporter an der Seite, surfte man mit ihm durch das Krankenhausnetz. Er fotografierte den Bildschirm, um alles ordentlich zu dokumentieren. Warscheinlich hatte der Reporter letztlich Angst vor Schiedsrichterschelte und war der Meinung, den Namen der Klinik auch nach Benachrichtigung des Krankenhauses nicht zu nennen.

Die Sportsfreunde waren erschrocken. Man stelle sich einmal vor man geht mit einer Sportverletzung in ein Krankenhaus und die draussen sitzenden Sportskollegen erzählen einem anschließend, was der Arzt einem nicht gesagt hat! Oder ganz anders: Ein anderer Sportsfreund will sich aufgrund der Flucht vor dem BKA die Nase umdrehen lassen um ohne weiteres durch die Grenzkontrollen zu kommen. Und nun ihm wird statt dessen der Blinddarm herausoperiert, weil es so in der Datenbank geschrieben stand... Er hätte somit Pech gehabt und würde an der nächsten Grenzkontrolle festgenommen.

Da wurde also im höchsten Masse gegen Datenschutz verstoßen, flogen sensible Patientendaten von der Stippvisite mit Laptop durch die Luft. Der Begriff "wardriving" kam ins Gespräch. Man fuhr ein Krankenhaus nach dem anderen ab. Teilweise wurde einem ganz schummrig bei den vielen offenen WaveLANs in den Krankenhäusern. Der Rekord lag nach offiziellen Schätzungen bei 31 offenen Accesspoints, Gratulation.

Die Netze hatten auch teilweise zu eindeutige Namen; Eines nannte sich "<krankenhausname>_SECURE". Letzteres wurde zusammen mit dem Datenschutzbeauftragen und den EDV-Verantwortlichen von bzw. mit den Sportlern gemeinsam abgeschaltet. Super, es geht doch! Also mal eine Stelle höher anklopfen: Der Landesdatenschutzbeauftragte hatte wider Erwarten spontan Zeit für die mittlerweile zu Leistungssportlern gewordenen Laptop-Träger.

Man war erstaunt – es tat sich wieder etwas. Über die bundesweiten Krankenhausverteiler gingen entsprechende Meldungen raus. Die Krankenhäuser haben nach "bestem Wissen" ihr Netz dicht gemacht.

Happy End? Das bleibt abzuwarten. Die WaveLANs der Krankenhäuser, auf die schlecht verzichtet werden kann, sind nun erstmal sicher geklickt worden. Nur ist es eine Frage der Zeit, wann die Sportler hinter das "Geheimnis des Hermes" gekommen sind, dem von der Firmware gesteuerten Controller, der auf fast jeder WaveLAN Karte steckt. Durch Reverseengineering könnte man eine eigene Firmware schaffen und diese auf die Karte laden. Kann man mit dem Hermes direkt sprechen und hat somit Zugriff auf den untersten Layer, dem "Link-layer", können "hidden-networks" entdeckt werden, kann der komplette mit WEP verschlüsselte Traffic ohne größere Probleme dechiffriert werden, damit wäre alles wieder beim Alten, aktive und passive Attacken gegen WaveLAN Netze ein Kinderspiel. Aber wer von den großen Unternehmen wird schon IPSec über das WaveLAN fahren? Das kostet doch viel zu viel Zeit und außerdem ist ja noch nichts passiert...

weiterführende Literatur:

http://www.isaac.cs.berkeley.edu
http://grouper.ieee.org/groups/802/11/
http://www.wavelan.com
http://www.x-itec.de/projects/tuts/ipsec-howto.txt

Das Phänomen Überlast

von Sebastian Zimmermann

**Neue Verfahren zur Überlastabwehr im Internet:
Active Queue Management und Explicit Congestion Notification**

Stockende Dateiübertragungen, "stalled connections", wohl jeder kennt dieses Phänomen im Internet. Aber wie entsteht es eigentlich? Egal ob kanalorientiertes oder paketorientiertes Netz, es gibt immer dann Probleme, wenn man nicht volle Kapazitäten von jedem Teilnehmer zu jedem Teilnehmer eines Netzes vorsieht. So etwas wäre auch kaum bezahlbar. Betrachten wir das Telefonnetz: Nimmt man an, es könnten theoretisch 1.000.000 Menschen gleichzeitig von Hamburg nach München telefonieren, so wird man noch lange nicht soviel Leitungskapazität vorsehen. Ein Netzbetreiber geht lediglich davon aus, daß statistisch gesehen nur ein sehr kleiner Teil der Anschlußinhaber von Hamburg nach München telefonieren will. Wollen jetzt doch mehr Leute als geplant telefonieren, gibt es ein Gassenbesetztzeichen - nicht zu verwechseln mit dem normalen Besetztzeichen, wenn der Teilnehmeranschluß belegt ist. Man nennt dies Rufannahme ("Call Admission Control"). Im Internet wird - bisher zumindest - vollkommen auf eine Rufannahme von der Netzseite aus verzichtet (bei einzelnen Servern gibt es dagegen sehr wohl eine Rufannahme, z.B. bei einer Beschränkung der maximalen Zahl von simultanen Benutzern eines FTP-Servers). Und noch einen Unterschied gibt es zum Telefonnetz: Da im Internet einzelne (IP-) Pakete vermittelt werden, kann man diese für eine gewisse Zeit zwischenspeichern und so kurzfristige Überlasten ausgleichen. Dazu gibt es in jedem Netzknoten Warteschlangen, in die die Pakete eingestellt werden, bis die ausgehende Leitung frei wird. Hierbei ist wichtig, daß die durchschnittliche Gesamtlast unter 100% liegt, sonst wird das System instabil und die in ihrer Größe begrenzten Warteschlangen laufen über. Dies führt dann zu Paketverlusten.

Das Internet nutzt nun aber keine Rufannahme. Trotzdem muß sichergestellt werden, daß die durchschnittliche Gesamtlast unter 100% liegt. Wie wird das also erreicht? In der Anfangszeit des Internets hat man sich um dieses "Detail" überhaupt nicht gekümmert. Es gab nur wenige Rechner mit langsamen

Anbindungen an das Internet, und allein aus diesem Grund gab es keine wesentlichen Überlasten. Aber als das Internet größer wurde, wurde auch der Handlungsbedarf deutlicher. Also wurde ein Protokoll geschaffen, das die Senderate an den aktuellen Lastzustand im Netz anpassen kann. Das heutige Transmission Control Protocol (TCP) war geboren. Inzwischen gibt es viele unterschiedliche TCP-Varianten. Ihnen gemein ist aber, daß sie auf eine bestimmte Art und Weise versuchen, den Lastzustand im Netz zu erkennen und die Senderate entsprechend anzupassen. Bei allen bedeutenden Varianten wie sie in Windows oder Linux implementiert werden, geschieht dies anhand der Erkennung eines Paketverlustes. Geht man davon aus, daß IP-Pakete so zuverlässig über die Leitungen transportiert werden, daß sie praktisch nie durch fehlerhafte Übertragung verloren gehen, so kann man einen Paketverlust als Überlauf einer Warteschlange im Netz interpretieren. Ergo war die Senderate zu hoch.

Bei Telefongesprächen würde dies natürlich nicht funktionieren - es sei denn, man nimmt eine Verschlechterung der Qualität z.B. durch Veränderung der Kompression in Kauf. In der Anfangszeit gab es im Internet nur Dienste wie Datei-Transfer (FTP), E-Mail oder News. Bei diesen Diensten ist es im wesentlichen egal, ob die Verbindung mal etwas länger dauert oder nicht. Man nennt solche Arten von Datenverkehr auch elastischen Verkehr.

Obwohl das Prinzip recht praktisch zu sein scheint, so stößt es immer häufiger an seine Grenzen. Dies liegt daran, daß sich viele Prämissen geändert haben. So sind immer mehr Verbindungen drahtlos. Drahtlose Übertragungen haben eine deutlich höhere Bitfehlerwahrscheinlichkeit als drahtgebundene. Die Annahme, daß ein Paketverlust durch eine Überlastung entstanden ist, ist bei einer korrupten Übertragung also falsch. Die Senderate wird fälschlicherweise noch weiter heruntergeregelt, und die Qualität verschlechtert sich. Auch gibt es immer mehr Dienste im Internet, die unelastischen Verkehr erzeugen, bei denen es also sehr wohl auf eine konstante Übertragungsrate ankommt. Beispiele sind Internet-Telefonie oder Video-Streams. Diese Dienste benutzen daher in der Regel auch kein TCP, sondern das User Datagram Protocol (UDP). Noch dominiert TCP mit einem Anteil von deutlich über 95% in den großen Backbone-Links, aber der Trend geht in Richtung UDP.

Das grundlegendste Problem ist aber, daß es erst zu einer "katastrophalen" Überlast, nämlich einem Warteschlangenüberlauf, gekommen sein muß, bevor die Sender ihre Raten reduzieren. Häufig geht bei einer solchen Überlast nicht nur ein einzelnes Paket verloren, sondern eine ganze Reihe von Paketen. Dies ist besonders schädlich für TCP; denn während moderne TCP-Varianten einzelne Paketverluste sehr schnell an den Empfangsbestätigungen erkennen können, muß bei mehrfachen Verlusten auf den Ablauf eines relativ langsamen Timers gewartet werden. Die Verbindung gerät ins Stocken. Solche Mehrfachverluste können auch mehrere Verbindungen gleichzeitig betreffen, die dann alle gleichzeitig die Rate reduzieren. Gleichzeitig erhöhen sie dann wieder die Rate, bis es wieder zu Verlusten kommt, worauf alle gleichzeitig ein erneutes Mal die Rate reduzieren. Diesen unglücklichen Kreislauf nennt man Global-Synchronization-Problem.

Was ist also zu tun? Zum einen wäre es sehr praktisch, wenn der Sender eine Überlast auch ohne Paketverlust erkennen könnte. Dies bewirkt die *Explicit Congestion Notification* (ECN), bei der die Pakete einfach markiert werden, wenn ein Netzknoten überlastet ist. Zum anderen wäre es auch sehr vorteilhaft, würden die Sender ihre Rate reduzieren, bevor es zu einer Überlast kommt. Dies bewerkstelligt das Active Queue Management (AQM), indem die ange-

sprochenen Markierungen (Congestion Signals) schon dann generiert werden, bevor die Last den kritischen Bereich erreicht hat. Ein zweites Ziel des Active Queue Managements ist es, das Global Synchronization Problem zu verhindern und möglichst alle Verbindungen gleich zu behandeln. Bei der einfachen Warteschlange konnte es ja sehr leicht passieren, daß eine einzelne Verbindung mehrere Pakete verliert und so deutlich stärker betroffen ist als der Rest.

Explicit Congestion Notification (ECN)

ECN ist neues Verfahren, bei dem ein Router durch eine einfache Markierung eines Bits im IP-Header eine drohende Überlast mitteilen kann. ECN ist sowohl auf der IP-Ebene als auch auf der TCP-Ebene des Netzwerk-Schichtenmodells definiert und benötigt jeweils zwei Bits im IP- und im TCP-Header.

Im IP-Header wurde das ECN-Feld mit zwei Bit Länge im ehemaligen Type of Service (TOS) - Feld untergebracht. Das TOS-Byte ist ein Feld in der ursprünglichen Definition des IP-Headers, das zur Priorisierung von Paketen nach unterschiedlichen Kriterien dienen sollte. Diese Verwendung hat sich nicht durchgesetzt, und deshalb wurde das TOS-Byte von der IETF Differentiated Services Working Group für ein neues und besseres Verfahren in Anspruch genommen, das Gegenstand eines anderen Artikels sein wird. Seitdem besteht das ehemalige TOS-Byte aus einem sechs Bit Differentiated Services Field (Bits 0 bis 5) und einem zwei Bit ECN Field (Bits 6 und 7). Es ist an dieser Stelle noch einmal explizit hervorzuheben, daß es das TOS-Byte nicht mehr gibt, obwohl noch häufig in der Literatur die Rede davon ist. Wer Router oder Firewalls konfiguriert, sollte vor diesem Hintergrund seine Regeln anpassen: Das ehemalige TOS-Byte ist nun zweigeteilt (siehe Bild 1). In alten RFCs findet man auch häufig noch einen widersprüchlichen Sprachgebrauch. So wird manchmal von einem DS-Byte gesprochen oder von einem ECT und einem CE Bit. Die Bezeichnung DS-Byte ist eine Folge eines Mißverständnisses, bei dem davon ausgegangen wurde, daß das gesamte ehemalige TOS-Byte nun für die Differentiated Services benützt werde. Die Bezeichnungen ECT und CE-Bit sind mittlerweile überholt, die zwei Bits sind nun gemeinsam zu interpretieren. ECT steht für ECN-Capable Transport, CE für Congestion Experienced.

Die Werte, die so ein Feld aufnehmen kann, nennt man im technischen Sprachgebrauch Codepoint. Das ECN-Feld kann somit vier verschiedene Codepoints aufnehmen, nämlich 00, 01, 10 und 11. Der Codepoint 00 heißt Not-ECT Codepoint, ist also der Wert für Verbindungen, die noch nicht ECN-fähig sind. Der Codepoint 11 ist der CE Codepoint und wird in der Regel vom Router gesetzt, wenn eine Überlast vorliegt. Die verbleibenden Codepoints 01 und 10 sind die ECT(1) bzw. ECT(0) Codepoints. Sie zeigen an, daß beide Partner der Verbindung ECN anwenden. Im ersten Entwurf von ECN gab es nur einen ECT-Codepoint, nämlich den ECT(0) Codepoint.

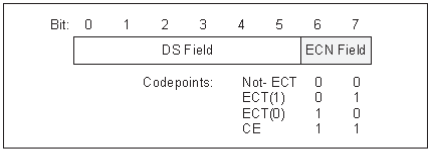


Bild 1: Aufteilung des ehemaligen TOS-Bytes im IP-Header in DS und ECN-Feld

Prinzipiell sind beide ECT-Codepoints gleichwertig, der zusätzliche Codepoint wurde ursprünglich deswegen geschaffen, um überprüfen zu können, ob eine Netzkomponente unerlaubt gesetzte Bits im ECN-Feld löscht. Dies ist in der Tat ein großes Problem, da viele Router das ehemalige TOS-Feld auf Null setzen. Wird nur ein ECT-Codepoint verwendet, sollte ECT(0) verwendet werden.

Beim TCP-Header war die Schaffung von Platz für die zwei neuen Bits zum Glück einfacher. Im 13. und 14. Byte des Headers befinden sich nämlich insgesamt sechs bisher ungenutzte Reserved Bits, von denen jetzt zwei Bits (Bit 8 und 9) für ECN verwendet werden (siehe Bild 2). Diese zwei Bits stellen zwei neue Flags dar, nämlich das Congestion Window Reduced (CWR) Flag und das ECN-Echo (ECE) Flag. Beim TCP-Verbindungsaufbau überprüfen Sender und Empfänger, ob sie beide ECN verstehen. Nicht nur der Sender muß ECN verstehen können, sondern auch der Empfänger, da er die Markierungen der ankommenden IP-Pakete zurück an den Sender weiterleiten muß.

Beim Rufaufbau schickt der Sender ein ECN-Setup SYN Paket mit gesetztem SYN, CWR und ECE-Flag. Der Empfänger antwortet mit einem ECN-Setup SYN-ACK Paket, bei dem das SYN, ACK und ECE-Flag gesetzt sind. Das CWR-Flag ist hier nicht gesetzt, da es inkorrekt implementierte TCP-Versionen gibt, die in den ACK-Paketen einfach die empfangenen Reserved Bits zurücksenden und somit fälschlicherweise ECN-Funktionalität signalisieren könnten. Während des Rufaufbaus darf auf der IP-Ebene noch kein ECT-Codepoint gesetzt sein.

Ist die Verbindung zustande gekommen, kann der Sender in den IP-Paketen einen ECT-Codepoint setzen. Tritt an einem Router eine Überlast auf und ist ein ECT-Codepoint gesetzt,

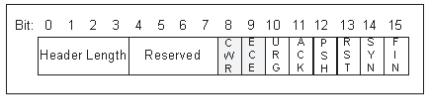


Bild 2: Neudefinition des 13. und 14. Bytes im TCP–Header

so ändert der Router den Codepoint in den CE-Codepoint um. Andernfalls wird das Paket bei Überlast wie bisher verworfen. Der Empfänger des IP-Pakets liest nun den Codepoint aus und informiert mit dem nächsten TCP-ACK-Paket den Sender darüber: Wurde ein CE-Codepoint empfangen, so setzt der Empfänger in den TCP-ACK-Paketen solange das ECE Flag, bis der Sender wiederum den Empfang des ECE-Flags durch ein TCP-Paket mit gesetzten CWR-Flag bestätigt hat. Danach geht das ganze von vorne los.

Der Sender wiederum reagiert auf empfangene ECE-Flags mit einer Ratenreduktion, die Senderate wird halbiert. Dies wäre auch bei einem Paketverlust der Fall gewesen, allerdings hätte in so einem Fall zusätzlich das verloren gegangene Paket erneut übertragen werden müssen. Die Ratenreduktion wird wie beschrieben durch das CWR-Flag dem Empfänger bestätigt. Der Empfänger wird das CWR-Flag allerdings nicht sofort bekommen und in der Zwischenzeit weiter ECE-Flags senden. Der Sender darf nun natürlich nicht auf alle diese ECE-Flags mit der Reduzierung der Senderate reagieren. Dies wird dadurch sichergestellt, daß die nächste Reaktion frühestens nach einer vollen Umlaufzeit (Round Trip Time) stattfinden kann.

ECN im Linux-Kernel 2.4.x

Mit der neuen Generation der Linux-Kernel hat ECN auch in Linux Einzug gehalten. Man muß diese Option bei der Kompilierung des Kernels aber erst noch explizit aktivieren. Sie verbirgt sich in den Networking Options unter TCP/IP Networking und heißt sinnigerweise IP: TCP Explicit Congestion Notification support. Über /proc/sys/net/ipv4/tcp_ecn kann man dann nach Bedarf ECN ein- und ausschalten. Der Vorteil von ECN liegt auf der Hand: unterstützen Empfänger und alle Netzknoten auf dem Weg dieses Protokoll, so werden die eigenen Pakete deutlich seltener verworfen. Man spart nicht nur eine erneute Übertragung, sondern auch die Wahrscheinlichkeit der oben erwähnten Mehrfachverluste mit den damit verbundenen negativen Folgen wird deutlich geringer.

Freud und Leid mit ECN

Allerdings hat ECN einen sehr entscheidenden Nachteil: Viele Administratoren und Netzkomponenten-Hersteller haben die Aufteilung des ehemaligen TOS-Bytes (s.o.) noch nicht mitbekommen. Viele Router setzen dieses Feld einfach zurück auf Null, und manche schlecht konfigurierte Firewalls filtern solche Pakete sogar komplett heraus. Es kommt noch schlimmer: bei einigen Geräten einiger namhafter Hersteller läßt sich dieses "Feature" nicht einmal abschalten. Wer ECN aktiviert muß also leider damit rechnen, an Firewalls und der Unwissenheit einiger Administratoren zu scheitern. Meine bisherigen Experimente haben gezeigt, daß diese Probleme leider auch nicht gerade selten auftreten. Hier hilft nur Aufklärungsarbeit bei den jeweiligen Administratoren. Eine Alternative wäre auch noch ein automatische Fallback auf eine Not-ECN-Verbindung. Diese Option ist allerdings umstritten, da dies auch bedeuten würde, ein empfangenes RST-Flag zu ignorieren.

Ein zweites Problem würde aber auch durch das automatische Fallback nicht gelöst werden: Es gibt da nämlich noch Intrusion Detection Systeme (IDS), die allergisch auf ECN reagieren. Viele Intrusion Detection Systeme verwechseln einen TCP-ECN-Rufaufbau mit einem "Queso"-Scan, also mit einem Versuch, die Art und Version des Betriebssystems auf einem Server aus der Ferne herauszufinden. Und schon löst das IDS "Roten Alarm" aus. So etwas ist nicht nur ärgerlich für die Firma, die das IDS einsetzt: In einem konkreten Fall ergab es sich beispielsweise, daß beim Besuch der Webseiten einer solchen Firma das IDS Alarm schlug. Schon kurze Zeit später gab es eine Beschwerde von Seiten dieser Firma bei unserem Sicherheitsbeauftragten, es seien bei uns "Hacker-Tools" im Einsatz! Natürlich dauerte es einige Zeit und nahm einiges an Personal in Anspruch, bis sich herausgestellt hatte, was die eigentlich meinten. Seitdem wird diese Webseite von uns regelmäßig besucht. ;-)

Wer ECN einsetzen möchte, sei also vorgewarnt. Letztendlich ist es aber wichtig, daß sich dieses Protokoll im Internet durchsetzt, denn viele zukünftige Erweiterungen bauen darauf auf. Noch ist ECN auf das TCP-Protokoll beschränkt, aber auch dies wird sich ändern.

Active Queue Management (AQM)

Bisher haben wir Sender- und Empfängerseite einer ECN-Verbindung besprochen. Aber auch die Netzknoten dazwischen müssen mitspielen und ECN erkennen können. Dafür wird in der Regel eine RED-Warteschlange verwendet. Random Early Detection (RED) ist ein Active Queue Management - Verfahren. Neben der ECN-Problematik soll die RED-Warteschlange auch noch das Problem der Mehrfachverluste und das Global Synchronization Problem lösen (s.o.). Inzwischen hat sich herausgestellt, daß RED noch nicht die ultimative Lösung ist, aber RED ist ein Schritt in die richtige Richtung und inzwischen in vielen Routern implementiert. Es ist auf jeden Fall eine gute Idee, dieses Verfahren im Router zu aktivieren.

In einer RED-Warteschlange werden zwei Schwellen, die untere und die obere definiert. Ist der durchschnittliche Füllstand der Warteschlange unterhalb der unteren Schwelle, werde alle Pakete unverändert durchgelassen. Ist der durchschnittliche Füllstand oberhalb der oberen Schwelle, werden alle Pakete markiert bzw. verworfen (manche Implementierungen verwerfen in diesem Fall immer, auch wenn ECN verwendet wird). Der interessante Bereich ist dazwischen: befindet sich der durchschnittliche Füllstand der Warteschlange zwischen den beiden Schwellen, so werden die Pakete mit einer gewissen Wahrscheinlichkeit markiert bzw. verworfen. Diese Wahrscheinlichkeit steigt dabei in erster Linie linear in Richtung zur

oberen Schwelle an (siehe Bild 3). Die Markierungswahrscheinlichkeit ist an der unteren Schwelle also Null, an der oberen Schwelle maximal (ein einstellbarer Wert). Allerdings ist das Gesagte nicht ganz richtig, denn in einem zweiten Schritt wird die Wahrscheinlichkeit modifiziert, damit der Abstand zwischen zwei markierten/verworfenen Paketen möglichst gleich bleibt und so die Congestion Signals auf möglichst viele Verbindungen durch den Router verteilt werden.

Die Vorteile von RED sind offensichtlich: bereits bevor es zu einer so starken Überlast kommt, so daß der Speicherplatz in der Warteschlange nicht mehr ausreicht, werden Überlast-Signale generiert, die die Sender veranlassen, die Raten zu reduzieren. Auf diese Art und Weise kann man auch relativ große Warteschlangen in den Routern verwenden, ohne daß diese fast immer voll sind. Denn eine volle Warteschlange bedeutet natürlich auch eine entsprechend große Verzögerung für die einzelnen Pakete. Gerade für zeitkritische Anwendungen wie beispielsweise die Internet-Telefonie sind Verzögerungen nachteilig.

Literatur

Sowohl ECN als auch AQM sind zur Zeit Gegenstand intensiver Forschung. Die aktuellste Literatur wird man daher in wissenschaftlichen Konferenzpapieren finden. Über ECN gibt allerdings auch einen RFC mit der Nummer 2481 (z.B. ftp://ftp.isi.edu/in-notes/rfc2481.txt). RFC 2481 ist der Kategorie Experimental zugeordnet und ist auch so aufzufassen. Viele Angaben in ihm sind bereits überholt. Bis zum Erscheinen dieser Ausgabe der Datenschleuder sollte aber auch ein neuer RFC erschienen sein, der die neuesten Entwicklungen von ECN berücksichtigt und vermutlich bereits zur Kategorie Standards Track gehören wird. Damit ist er dann mehr oder weniger verbindlich für Entwickler. Unter http://www.rfc-editor.org

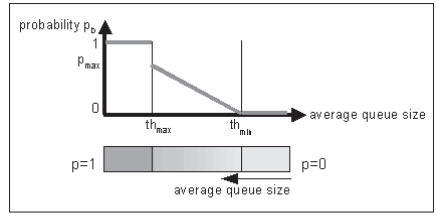


Bild 3: Änderung der Markierungswahrscheinlichkeit in Abhängigkeit des durchschnittlichen Füllstands in einer RED–Warteschlange

gibt es die aktuellsten RFCs. Bis zum Erscheinen des RFCs ist der zur Zeit aktuellste Stand in einem Internet-Draft nachzulesen. Internet-Drafts sind äußerst kurzlebige Dokumente, die den derzeitigen Entwicklungsstand beschreiben. Zur Zeit ist bzgl. ECN der Internet-Draft mit dem Dateinamen draft-ietf-tsvwg-ecn-04.txt aktuell.

Zu RED-Warteschlangen gibt es leider keine RFCs. Aber Sally Floyd, eine der Autoren, stellt den wissenschaftlichen Artikel zum Download zur Verfügung, in dem die Mechanismen genau beschrieben werden:

Floyd, S., und Jacobson, V.: Random Early Detection gateways for Congestion Avoidance, IEEE/ACM Transactions on Networking, V.1 N.4, August 1993, p. 397-413 (http:// www.aciri.org/ floyd/papers/red/red.html).

Außerdem hat Sally Floyd auf Ihrer Homepage (http://www.aciri.org/floyd/) mehrere Verweise auf Folgeveröffentlichungen sowohl zu ECN als auch zu AQM.

"Don't talk to the Press about this!"

by David Burke

White Dot infiltrates itv Industry Trade Body.

Part One: Privacy at the Yale Club

The subject on the email was "Media Privacy Gang-Rape". But he seemed sane enough. For instance, he remained good-natured when I told him he was paranoid, especially in this paragraph:

"I am absolutely convinced" he wrote to me, "that televisions are already capable of acting as cameras which enable the media industry and their clients to observe and listen to everyone and everything within line of sight of the screen." What sounds more crazy than saying "I think my TV set is watching me?" He might as well have signed his message Napoleon@AOL.com. But few people understand this subject, and I'm glad the man found our website. I know how hard it is to choose the right words and anticipate what is possible, without losing all credibility. For three years now, I have been studying the privacy issues surrounding digital interactive television, and I was able to reassure my correspondent that I hadn't heard anything about cameras when I snuck into the Addressable Media Coalition Luncheon at the Yale Club in New York. If those people don't know about surveillance gadgets in television sets, nobody does.

The Addressable Media Coalition (AMC) is a division of the Association for Interactive Marketing (AIM), which has recently been made a part of the Direct Marketing Association (DMA), a lobbying group for junk mailers, cold callers and market researchers. The AMC was established to realize the dream of addressable advertising - a new way to profile and target people based on their viewing behavior, or as it is now known, their "telegraphics". Prominent among the Coalition's 34 members are Nielsen Media Research, the advertising giant Young and Rubicam, WebTV, which is owned by Microsoft, and NDS, which is owned by Rupert Murdoch's News International. The group I work for was not invited to join. I serve as British Director of White Dot, a small, but nevertheless international, campaign against television. I was so disorganized that day, that when I got to the Yale Club, I

didn't have business cards for my fictitious company. My suit looked nice.

"You don't have a business card?" – "Uh, no."

But the young man on the door couldn't make too much fuss. I had missed the food, and walked straight into the AMC's Privacy Subcommittee meeting. The oak paneled room of 20 people sat quietly around their plates of cookies and china cups of surprisingly bad coffee, listening to a speakerphone, out of which the CEO of BeyondZ Interactive passed on what she knew of the lobbying situation in Washington. She emphasized how important it was to negotiate something at the federal level, before individual states could pass their own privacy bills. Discussion turned to their narrow escape in California. That bill had gone so far as to require viewers' permission before monitoring could begin, and was only killed after intensive lobbying by Microsoft and AOL. Everyone agreed they were lucky. State Senator Debra Bowen had been too far ahead of the curve.

"May I ask who you are?"

I looked up, at Art Cohen, Senior Vice President of Advertising and Commerce for ACTV, and Chairman of the Coalition. I recognized him from the SpotOn promotional video he gives to advertisers.

Zoom right in - to a little street of identical houses. Are the happy people inside them identical as well? Oh no! They all have different skins, different numbers of children, make different money and want different things. Every time the old white couple with the poodle click on their remote control, it is recorded in a database on their set-top box. The same is true for the young black family with the Labrador. SpotOn software gathers this data, analyses it, and sends each of them targeted advertising or programs aimed at their unique behavior. The secret: artificial intelligence algorithms! "See that box?" SpotOn's head of sales in Denver asked me at a trade show, "That box can hold 64,000 bits of information about you!" And that was just the General Instruments 2000 box, not even the GI 5000 everyone was talking about. "I'm a programmer" I said, "I'm just beginning to work with interactive TV." Why did I give my real name? That was so stupid. I had asked Mr. Cohen for an interview months ago, and he had turned me down.

"I've got to be careful about what I say," he told me on the phone, "because what I say could end up in a book, and I'll be sorry about it." He looked at my registration form, then looked at me.

"You're not the press are you?" – "No" I said. (a long pause.) – "Okay."

I shook his hand. It was fleshy and strong, like his face. The fashionable, narrow lens glasses made a nice contrast. He looked good.

Art Cohen is very concerned about people listening in on what he says. With the Addressable Media Coalition, he is determined to offer a place where industry leaders can speak in confidence, agreeing how to proceed before saying anything in public. "You don't want to talk to the press about any of this," he told us over and over. "If some bad PR got out, whether it's true or not, it might take us a year to make it up." Everyone nodded. They all agreed they couldn't afford to make the same mistakes they had on the internet - rushing into a medium they didn't control, without a strategy in place, a back-up plan, just in case users found out about all those cookies. Companies who make interactive television are keen to talk about "the coming digital revolution", hoping viewers will forget about the one that has already happened. Interactive TV is really a digital counter-revolution, walling in the content that viewers can see, and handing control of their news and leisure time back to broadcasters. DoubleClick, the internet advertising firm, got into big trouble when they tried to connect internet surfing data with offline records from Abacus, a mail-order catalog company. But tele-

vision service providers won't have to improvise this way. Digital set top boxes connect on and offline data as soon as they are installed. That is what the machine was designed to do. A number of companies now hope to connect the commercials you see to the products you buy using a supermarket loyalty card. There is no end to this convenience.

In Europe interactive TV is a big success. But the American industry requires visionary leaders to overcome the skepticism of advertisers and viewers. Art Cohen is running for Steve Jobs. And he might win; he talked tough and interrupted people. He moved around the room behind the CEOs, lost in thought one second, commanding our attention the next. We were all impressed.

I've interviewed dozens of executives in this industry, on the phone, in their "homes of the future" and at conferences on interactive TV and one-to-one marketing. These are people you will never meet, but who will soon know a great deal all about you. David Byrne, Senior Manager of Business Development at Microsoft was happy to talk about the warehouse of data that is being collected by WebTV, waiting for some future use. Other salesmen and women were young and excited to be part of the next big thing. They weren't sure how to handle privacy questions, but their repeated hope was in today's "media-savvy youth". Apparently, the younger kids are, the less they worry about privacy.

At one conference, Kirt Gunn of the advertising consultancy Cylo had a whole room laughing when he speculated why this might be: "I don't know whether it's how many people read 1984 or what piece of the puzzle it is." Indeed, Orwell's book is about to lose much of its rhetorical power. The real experience of interactive television will soon take its place. When consumers discover that their TV sets are recording what they do in their living rooms and bedrooms, they will either stand up and demand protection, or, conversely, they will learn to love it. "Big Brother," our children may laugh someday, "Some old guy worried about that in the last century. But see - now they record everything I do, and I can order a pizza without dialing my telephone!"

The data analysts I've met were brilliant. I couldn't think of any use for this technology that was not already being studied or already in development. Neal Muranyi of the Database Group is the man who first coined the term "telegraphics" to describe the data you and I will produce each evening. He has already seen how the insurance industry could save millions of dollars: "Such systems would allow, say insurers to differentiate risk-averse conservatives from high-living show-offs, and then tailor both marketing messages and risk scoring systems accordingly."

Pat Dade of Synergy Consulting told me about his psychographic "value groups", people he has surveyed and interviewed until he is able to categorize the emotions that make them act. Here he describes how your television data will be used as a digital fingerprint, linking you into one of them:

"Let's say that the hypothesis is that an inner-directed person, if they watched da-da-da, would react in such and such a way. Now you can test that. You can test that at the end of each time, because you're starting with the question 'Can we change or reinforce behavior based on this information?'"

Control. That's the slogan used to sell interactive television. But what really excites these people is the way it creates experimental conditions in the home. Your TV set will be able to show you something, monitor how you respond, and show you something else, working on you over time until it sees the desired behavior. But who nicer to push the buttons? Pat Dade spoke like the gentle, self-help author he could so easily have been, and he had a nice sense of humor. When I found out that he had worked on Echelon, the US military's worldwide electronic eavesdropping system, he laughed.

"Oh yeah" he said, "We spied on everybody."

That's why the AMC Luncheon was such a surprise. These guys were so hard and aggressive, like big business baddies in a cartoon strip. Poor Jerome Samson, the French data analyst working for Nielsen, was openly ridiculed for talking too long, and a running joke about "career terminating statements" was thrown back and forth between tough young sales reps. Except for Karen Lennon of BeyondZ, none of the women dared say anything. And when some namby-pamby suggested explaining to viewers about the unique identifier and what we did with their data, Jack Myers of the Myers Report shot him down. "Listen," he said, "There really is no such thing as privacy, unless you're..[Unabomber] Ted Kaczynski or something. There is no privacy. It's all public relations. It's all perception."

At the top of the pecking order stood Art Cohen. And he made it clear there would be no telling viewers anything:

"Right now you're being targeted by Nielsen," he said, dismissively, "This is just better data. Nobody's getting permission now."

But then, it's like he had to go on:

"The difference is" he said, totally contradicting himself, "this box has a unique identifier, so you're able to poll boxes individually. The Cable Acts and things that were written years ago don't really deal with that."

It was then that I began to have the strangest feeling of sympathy for Art Cohen. I began to see how much we have in common. Oh sure, before congressmen he can play casual, and say the profiling he does is no different from the way people know their local grocer.

But in front of these advertisers, like Wes Booth of Grey Advertising, or Tim Hanlon of Starcom Worldwide, who was listening somewhere on that speakerphone, Cohen had to lay out his vision of the coming, irrevocable change to the way human beings live. He had to predict the unthinkable. He had to make people listen, but not in any way that could appear, let's say, too far ahead of the curve. "This is going to happen" he was saying again, "Nothing is going to stop it. The technology is so powerful! It's not just interactivity; it's targetability and accountability All the data is digital."

Would he find the right words? How do you describe a future that already takes up your entire present, that you have studied in the smallest detail, so that you are already living it - without sounding crazy?

"Television is projections!" he was insisting, "Nielsen is projections! This will be based on actual counts! Instead of an unreal world of projected data, we're entering a real world of actual data, census data. That differentiates all these things from everything that's gone before."

What did he say? That was good. I scribbled it down. Census data! Why didn't I think of that? I've been so hung up on the experimental conditions thing. Cohen is a genius! That's the perfect way to describe it. This could bring the right-wingers on board! Anyway, I wish my email correspondent had been there. There's nothing like being with people who finally understand what you're talking about.

Part Two: e-Trussed

In the following months, I took part in the AMC's Privacy Subcommittee Meetings. These were chaired by Karen Lennon, a very nice woman whom I would call a privacy dove. That is, she thinks everything will be fine as long as the consumers are told that their civil liberties are being spit on. But both she and the privacy hawks, who were against raising such issues in public, agreed on one thing: a privacy seal was urgently needed. The AMC have published a Privacy Guideline document about this matter, explaining that an industry run system of self regulation had to be in place before legislators

themselves understood what interactive TV was and how it would affect citizens' lives. The cornerstone of any such effort is to be a new Privacy Compliance Seal, that the Coalition hopes to announce with fanfare this Autumn. The rest of the Guideline document is written in vague language about respect and trust, although these two sentences do stand out:

Such security measures will vary depending on the configuration of the systems handling the data and the purpose of the data collected. Financial information, medical information, VOD/PVR/viewing information mapped to PII will require greater levels of security than anonymous information regarding clicks, viewing or purchases. I suppose it is nice of them to fret over the security of viewers' financial and medical information, but what right do they have to all that data in the first place? Anyway, these meetings were held mostly by conference call, so I will skip the witty personal observations and get right to the issues. What follows are the matters that were important to members of the AMC Privacy Subcommittee, the group that will be creating this new Privacy Compliance Seal. When consumers see this seal appear on their TV screens, reassuring them that the highest standards are being met, they should know what went on in these meetings where the Seal was created.

Goal: Persuade Legislators to Scrap the Cable Act

An anomaly exists between the privacy regulation of cable and satellite. The 1984 Cable Act is far stricter. Both privacy advocates and broadcasters want to "level the playing field", except in different directions. Members of the Coalition were specifically advised to copy language that Cox cable had written up for their subscription contract. It was considered a good first step towards freeing interactive TV from the Cable Act.

Goal: Keep Legislation Away from the States

It came up a number of times that state legislatures might propose their own privacy legislation. Debra Bowen's proposed opt-in legislation was discussed a number of times. Repeatedly, it was agreed that if legislation was to be changed, it was best done at the federal level, where the various media lobbyists had more influence.

Goal: Create a Privacy Seal Before Government Regulates

Or, as Art Cohen said, "bites us in the ass". One of the earliest conversations of the Privacy Subcommittee contained a humorous moment. Everyone had been agreeing that speed was of the essence and that the process of creating a Seal could not be allowed to bog down. A lawyer on the call offered to take the initiative and draw up a quick list of privacy principles. That's when there was a silence, followed by a bit of laughter. Of course he couldn't draw up such a list of privacy principles! We hadn't sent out our Privacy Audit, asking all our member companies what practices they already had in place! We had to ask them what data they gathered, where it was stored, whom it was shared with, everything!

The Privacy Audit was every question that I, investigating these companies, could ever want to ask. But it was more important for the AMC's Privacy Subcommittee, because the last thing we all wanted to do was put out rules that might "cut somebody out". So there is the first lesson in how you create a Privacy Compliance Seal: Make sure it embodies the lowest common denominator of what everyone is already doing anyway.

Goal: Avoid Permission, Concentrate on Suitable Content

The Privacy Guideline document was written by Karen Lennon and a man named Jim Koenig of something called the ePrivacy Group, which turns out to be a wholly owned subsidiary of a

company called Postiva. So one would assume he is very strong on things like viewer permission.

But in the meetings, he claimed it was not important. He said that with education, viewers could be made to see that "suitable content" was more important than "permission."

In other words, if a television collects data and uses that data to provide programming that the viewer likes, and the user doesn't notice or sees no reason to complain, then there is no problem.

"There is no privacy problem if content gets 100% acceptance," said Koenig. "If we can go towards relevance, that is ultimately where we want to go." This argument is seductive, and has a lovely libertarian ring to it. But think again about what he is saying. First of all, there is such a thing as the principle of privacy. And reasonable people can argue about where to draw lines around it. But whatever your definition, privacy is a principle of human rights. It must be defined somewhere and respected.

What principle has Jim Koenig defined that the AMC can then respect? Absolutely none. When he says the AMC should move away from permission and towards "relevance", he implies that no principle is at stake that would require a viewer's agreement. In fact, his advice to his fellow iTV producers is not "give consumers what they want", but "do to consumers whatever they let us get away with".

And here is a second way that Koenig's comment betrays his industry's disrespect for its customers:

The viewers he is describing, who meekly accept his scrutiny, are not told the truth about what he does in their homes, or what he will do with the data he gathers. Every month new interactive systems are launched, and each arrives with two sets of promotional literature: one set for the viewers and another for the advertisers. Viewers are told how they will be able to order pizzas through their TV sets, advertisers are told about psychographic marketing and links to huge third party data services. Who would knowingly 'opt in' to that? No one. And Jim Koenig knows it. Yes, iTV producers and privacy advocates share a fondness for overblown rhetoric. But if the people in this industry refuse to be restrained by any principle you could discuss calmly, then we on the outside must continue to imagine that they will follow Koenig's advice, and do whatever they want until somebody complains.

Goal: Just Get A Birthday and ZIP Code!

Now that the Center for Digital Democracy has published its report exposing interactive television, Ben Issacson has been very busy. He is the Executive Director of the Addressable Media Coalition's parent body, the Association for Interactive Media (AIM) and he has been offering himself to any news organization covering the story, rushing to assure viewers at home that nothing is wrong.

"The industry plans are to collect aggregate information for advertising," he told WIRED magazine, "but not to collect information without user knowledge and consent." Notice his emphasis on the word aggregate, the implication being that even if your data finds its way into a database, it would never be connected to you personally. But that is not what Ben was saying when the Addressable Media Coalition met behind closed doors to discuss data collection issues and their new "Privacy Compliance Seal". At that meeting, Ben was reassuring his fellow interactive programmers that individuals could always be identified.

"You have one company that wants information," he told us, "they may ask it directly up front, but they may see a decline in the number of subscribers, because the users feel it's intrusive. On the other end, let's say I want the same information, but jeez, I can't bring myself to ask that, because the decline is percipitous, so I already have their nine digit ZIP code, I'm going to ask them for their birth date, just to confirm it. With a 97 percent accuracy I can then derive that

data of who they are, and go buy all that information." Ben Issacson is deliberately misleading reporters and the consumers who read about this issue. That is not surprizing; Mr. Issacson is a paid spokesman of the interactive advertising industry. What needs attention though is his use of the word "aggregate". He and the programmers he represents are purposely trying to create the impression that "aggregate" data must be "anonymous" data, and therefore protects the viewers who surrender it.

Not so. If the data describes a small enough pool of subjects (individuals with a certain birthdate in a certain ZIP code for instance) then it becomes possible to use that data as if it were personally identifiable. In data wharehousing theory, this is called a dataset's "granularity". And like the granularity of a photograph, it shows a clearer and clearer picture of a crowd, until it is possible to pick out individual faces. Ben Issacson has assured his fellow members of the AMC that he can pick out those faces with 97% accuracy. Shall we then call his data "personally identifiable"? Of course! And it should be regulated as such.

As for the "knowledge and consent" Mr. Issacson mentioned, the Addressable Media Coalition hopes to standardize what viewers everywhere are asked to sign when they subscribe to interactive television. One wording that members liked was "Yes, I want rich personalization!". Who would imagine that little phrase actually gives a cable or satellite company the permission to do so much? If you see these words, watch out.

Goal: Tell Us About Yourself!

It turns out that the moment you sign up for interactive television is the most important 15 minutes in the history of television. Art Cohen, Chairman of the Addressable Media Coalition, was especially keen on this point. Set top boxes are expensive, he told us. And if cable or satellite companies are going to subsedize these boxes, they will want as much information as possible in return, to hold and use for targeting. When you stand there looking over your television subscription form, wondering why there are so many questions to fill out, consider what Cohen told the Coalition: "When you put these boxes out there," he said, "you also want to know who these people are, in addition to what they have in their billing methods, it's very important to these cable operators that the minute they install that cable box, they want to give you a questionnaire."

The checkbox where the user opts-in our opt-out of "rich personalization" is important. But Cohen then described other questions that should be asked, in a standardized way, of every new customer:

"..whatever demographics they can collect because, think about it, if you don't get that, you have to go outside to other sources and it's not as accurate. The whole point being that the cable box is a polling mechanism - the absolute customization, media tool. You have to get as much information as you can on installation and in the follow up." Another member of the Addressable Media Coalition, this august body which is soon to launch its own Privacy Compliance Seal, named Bob Williams, was enthusiastic about the way such information could be used, saying "Once you get their credit card number, you can get their whole history. There's no stopping you!" Chairman Cohen saw a public relations disaster in the making. "Sure" he joked, "we can have DoubleClick make that announcement. And make sure you have plenty of press there."

That's funny. But what is funnier, of course, is that DoubleClick will never have information as complete as the people who provide interactive television. There are no technical obstacles to stop these men and women from collecting the data they want, only the law.

Eins, zwei, drei, viele... Volkszählung

von Sabine Krüger

Ein Gespenst geht um in unserem Land. Unbemerkt schleichen sich in Deutschland anarchistische Zustände ein. Veraltete und nicht vorhandene Zahlen entziehen deutschen und europäischen Politikern die Möglichkeit, das Land zu regieren. Deutschland wird mit Fehlentscheidungen seine Ressourcen ineffizient einsetzen und im unbedeutenden Nirwana versinken.

Die einzige Rettung: die Volkszählung, die wieder Planungssicherheit und Zahlen für soziologische, gesellschaftsanalysierende sowie ökonometrische Modelle bietet, naht unaufhaltsam. Über den Stand der Volkszählung in Deutschland diskutierten im März 2001 Statistiker, Wissenschaftler und Datenschützer auf der Tagung der Johann-Peter-Süßmilch-Gesellschaft in Berlin zum Thema „Volkszählung in Deutschland".

Anarchie in Deutschland

In ganz Europa führen die Länder in den Jahren 2000 und 2001 eine Gesamtzählung der Einwohner, Wohnungen sowie Arbeitsstätten durch. Europa und auch die einzelnen Länder benötigen statistisch legitimierte Zahlen für politische Entscheidungen, Standortentscheidungen privater Investoren und andere Analysen. Einer Großzählung kommt die entscheidende Aufgabe zu, die Grundgesamtheit von bestimmten Merkmalen der Bevölkerung sowie Wohn- und Lebenssituation festzustellen. Die Zahlen sind nicht nur Selbstzweck wissenschaftlichen Erkenntnisdurstes, sondern bedeuten in Deutschland für die Gemeinden bares Geld und Macht. So beruhen beispielsweise der Länderfinanzausgleich und das Stimmengewicht der Länder im Bundesrat auf den Einwohnerzahlen der Gemeinden.

Daten bieten

* Planungssicherheit,
* Datengrundlage gesellschaftlicher Analysen,
* Grundlage verteilungspolitischer Entscheidungen.

Die letzte Volkszählung fand noch im getrennten Deutschland, 1981 in der ehemaligen DDR und 1987 in der Bundesrepublik, statt. Seitdem haben sich die Realitäten stark geändert. Allein aus diesem Grund wird eine Zählung von vielen Seiten gefordert. Fand sonst immer alle 5 bzw. 10 Jahre eine Zählung statt, wird sich für die nächste Zeit gelassen. Nach der zeitlichen Einschätzung von Prof. Krug (Uni Trier, Fachbereich Statistik) wird eine nächste

Zählung erst nach dem Jahr 2007 und nach Dieter Bierau (Statistisches Bundesamt Wiesbaden) auf jeden Fall noch vor 2011 stattfinden.

Die wichtige Frage, wie soll gezählt werden, scheint schon so gut wie beantwortet. Nach den traumatischen Erfahrungen, die mit der Vollerhebung (d.h. ein „Zähler" läuft von Wohnung zu Wohnung) 1987 gemacht wurden, und dem nicht unerheblichen finanziellen Aufwand (Johann Hahlen, Präsident des Statistischen Bundesamtes, schätzt für eine erneute Vollerhebung ca. 1,5 - 2 Mrd. DM) wird in Deutschland ein neues Modell favorisiert: eine registergestützte Datenauswertung. Als datengebende Register sollen das Einwohnermelderegister, das Register der Bundesanstalt für Arbeit sowie Dateien anderer Behörden und Gebietskörperschaften genutzt werden. Zusätzlich werden postalische Befragungen der Gebäudeeigentümer durchgeführt. Dennoch sind die Folgen und die Qualität der Nutzung der Registerdaten unklar. Da Register zunächst ausschließlich für die Verwaltung der Bürger und nicht der statistischen Erfassung des gesellschaftlichen Zustands geschaffen wurden, erwarten die Statistiker einige Probleme bei der Nutzung der Register für einen registergestützte Erhebung. Es wird befürchtet, daß die Register nicht nur fehlerhaft und veraltet sind, sondern auch unterschiedliche Merkmale verwaltet werden.Was ist los in Deutschland?

Registergestützte Datenauswertung

Mit dem Gesetzentwurf vom 26.01.01 wird ein Testgesetz für Deutschland initiiert. In diesem wird der Probelauf eines zur normalen Volkszählung alternativen Modells, der registergestützten Auswertung, vorgeschlagen. Damit werden an einer Stichprobe in Deutschland beide Verfahren, Vollerhebung und registergestützte Erhebung, durchgeführt. Auf diese Weise soll die Fehlerhaftigkeit einer registergestützten Zählung abgeschätzt werden. Das Gesetz sieht vor, am 19. September 2001 und 31. Januar 2002 Personen zu erheben, deren Geburtstag auf 1. Januar, 15. Mai oder 1. September fällt. Ziel ist es, Mehrfachmeldungen in den Registern ausfindig zu machen. Zusätzlich werden in 570 Gemeinden Personen aus max. 38 000 Gebäuden erhoben und befragt, um zu testen, wie korrekt Personen in den Melderegistern erfasst sind. Was liegt bei einer solchen Qualitätskontrolle näher, als die Fehler in den Registern gleich zu beheben? Aber genau das soll und darf nicht geschehen. Gesetzentwurf zum Testgesetz

Die Aufgabe der Statistik ist es, genaue Zahlen über den aktuellen gesellschaftlichen Zustand zu schaffen, ohne daß damit direkte Konsequenzen für den einzelnen Bürger verbunden sind. Ganz im Gegensatz zum Staat, der die Register verwaltet, um den Zugriff auf seine Bürger zu gewährleisten. Der Datenfluss zwischen Verwaltung und Statistik darf aus diesem Grund in Deutschland nur einseitig erfolgen. So wird es aufgrund der "strikten Trennung von Statistik und Verwaltungsvollzug" in Deutschland keinen Abgleich der Registerdaten mit Ergebnissen der Volkszählung, wie es beispielsweise in Österreich geplant ist, geben. Dennoch sind Kontrollen durch den Datenschutz und gesetzliche Regelungen notwendig, um einem „Big Brother is watching you" Empfinden vorzubeugen und somit das Vertrauen der Bürger in die Erhebung aufrecht zu erhalten.

Dazu gehört auch, auf eine Verknüpfung der Datensätze mittels einer personenbezogenen Kennziffer (PKZ) zu verzichten. Diese wird in einigen Ländern, wie Schweden, für Verwaltungsvorgänge sowie auch die Zählung genutzt. In Deutschland ist eine solche Erfassung allerdings gesetzlich verboten. In einem Interview versicherte Johann Hahlen bei einer registerge-

stützten Zählung ohne eine Personenkennziffer auszukommen. Die Datensätze der einzelnen Register werden über bestimmte individuelle Merkmale (Hilfsmerkmale) miteinander verknüpft, um die Individualdaten zusammenzuführen und einzelne Haushalte generieren zu können. In den Häusern der statistischen Ämter werden in der Zeit nach der Volkszählung sehr detaillierte individuelle Datensätze verarbeitet, bevor die aggregierten Statistiken erstellt werden. Vielleicht sollte in dieser Zeit die statistischen Landesämter und das Bundesamtes durch private Sicherungsfirmen verstärkt vor Datenräubern beschützt werden. Dr. Rainer Metzschke (Zensusexperte des Berliner Datenschutzbeauftragten) fordert eine sofortige Löschung der Hilfsmerkmale, nachdem die Erhebungsmerkmale zusammengeführt wurden, sowie Tests der Pseudonomisierungsverfahren. Damit soll sichergestellt werden, daß es nicht möglich ist, aus den einfachen Erhebungsmerkmalen (ohne die gelöschten Hilfsmerkmale) einzelne Personen zu identifizieren.

Trennung von Verwaltung und Statistik unbedingt notwendig.

PKZ - Registergestützte Zählung ohne Schlüssel?

Bei einem solchen Aufwand sollte auch nach den Vorteilen gefragt werden. Ein wichtiger positiver Aspekt einer registergestützten Erfassung ist die geminderte Angst der für die Zählung Verantwortlichen vor unberechenbaren, die Zählung behindernden Massenhysterien, die durch andere gesellschaftspolitische Spannungen entzündet werden. Beispiele hierzu finden sich nicht nur im Vorfeld der letzten deutschen Volkzählung 1982 bis 87, die mit dem Wechsel der Bundesregierung und dem Aufstellen der Pershingraketen politisiert wurde, sondern auch in diesem Jahr in Tschechien, wo die politische Auseinandersetzung um die Besetzung des Fernsehintendanten zu großen Problemen bei der Durchführung der Volkszählung führen.

Für die Bürger bedeutet eine registergestützte Erhebung wesentlich weniger offensichtlichen Stress, da sie einen geringeren persönlichen Anteil an dem Erfassungsaufwand haben. Das bedeutet aber nicht automatisch mehr Vertrauen der Bürger in eine registerbasierte Datenerhebung. Im Zuge der informellen Emanzipation der Bürger wird es zukünftig eine andere Diskussion geben. Dann sollte geklärt werden, welche Daten wirklich benötigt werden, um ein möglichst hohes Maß an gerechter Aufteilung der Ressourcen eines Landes oder einer Region mit einer möglichst geringen Einschränkung der informellen Selbstbestimmung der Bürger zu erreichen.

Heute schon gesqueakt?

von Stefan Krecher

Squeak ist ein Open-Source Smalltalk-Entwicklungssystem, das sich zunehmender Beliebtheit erfreut. Es ist verfügbar für alle möglichen Plattformen, u.a. Linux, Mac, Windows, OS/2, BeOS und NeXT und neben einer PDA-Variante gibt es mit SqueakOS sogar ein eigenes Pseudobetriebssystem.

Smalltalk wurde in den Siebzigern am Palo Alto Researchcenter mit dem Ziel entwickelt, ein dem menschlichen Denken angepasstes Programmiersystem zu konstruieren. Die meisten Smalltalk-Systeme bezeichnen sich selbst als "System", da nicht strikt zwischen der Entwicklungsumgebung und der Sprache zu trennen ist.

Smalltalk-Systeme wie Squeak sind "in sich selbst" geschrieben. Die markantesten Merkmale sind das Vorhandensein eines "Class Hierarchy Browsers (CHB)" zum einfachen Durchstöbern der im sogenannten Image vorhandenen Klassen, und der Möglichkeit u.a. in einem Workspace, der als ein "Schmierzettel" angesehen werden kann, Codefragmente direkt auszuführen. Das Konzept der Sprache ist einfach: Alles was gemacht wird, wird mit Objekten und Methoden gemacht. Der CHB z.B. ist ist eine Instanz der Klasse "Hierarchy-Browser", kann über ein Systemmenü aufgerufen werden, oder per direktem Aufruf aus einer anderen Klasse.

Ein weiteres Beispiel: in der Anweisung "23 + 5 asString inspect" empfängt das Objekt "23" (Instanz der Klasse SmallInteger) die Botschaft "+" zusammen mit dem Argument "5". Das Ergebnis eines jeden Methodenaufrufes ist, wie sollte es auch anders sein, wieder ein Objekt, in diesem Falle das Ergebnis der Addition ("27", Instanz der Klasse SmallInteger). Dieses neue Objekt empfängt dann die Botschaft "asString", es resultiert ein Objekt vom Typ String, das der Konvertierung der Zahl in einen Text entspricht. Dieses Textobjekt empfängt die Botschaft "inspect", was zur Folge hat, das die Inspektorklasse instanziert wird- es öffnet sich ein Inspector-Fenster, welches den Inhalt der, die botschaft-empfangenden Objekte darstellt.

Weitere Konzepte sind: ausschließlich späte Bindung, komplette Untypisiertheit, es existiert ein Garbage Collector. Entwickelt wurde Squeak 1996 von einer Forschertruppe bei Apple, mittlerweile wird Squeak weltweit weiterentwickelt. Das Kernentwicklerteam, zu dem auch noch die Apple-Programmierer zählen,

sitzt bei Walt Disney Imagineering. Die Squeak-Community ist eine weltweite Gruppe von Wissenschaftlern, Programmierern, Hackern, die über diverse Mailinglisten oder den Squeak-Swiki-Server (minnow.cc.gatech.edu/squeak/1) kommunizieren. Der Swiki-Server ist ein Webserver, natürlich implementiert in Squeak (Squeak hat standardmäßig Webserverklassen in der Klassenbibliothek), der nach dem Wiki-Prinzip organisiert ist. Auf reinen Wiki-Servern kann jeder Seiten ändern oder hinzufügen.

Der grundsätzliche Aufbau des Systems ist so wie bei den Meisten Smalltalk-Systemen: es gibt eine virtuelle Maschine, die das sogenannte Image ausführt. In diesem Image befindet sich die Smalltalk-Klassenbibliothek, die Klassen der Entwicklungsumgebung sowie selbsterstellte Klassen des Programmierers. Diese Struktur erlaubt es das System verhältnismäßig einfach an eigene Bedürfnisse anzupassen oder zu erweitern. Wie Smalltalker es gewohnt sind, erwartet den Programmierer eine sagenhaft große Klassenbibliothek, die kaum noch Wünsche übrig läßt. Da der Sprachumfang von Smalltalk sehr gering ist, besteht die Hauptaufgabe des Programmierers darin, sich mit der Struktur und dem Inhalt der Bibliothek auseinanderzusetzen.

Wenn man sich etwas mit der Bibliothek auseinandergesetzt hat wird man aber ziemlich schnell in der Lage sein – erfahrene Smalltalker werden das bestätigen – nahezu prophetische Aussagen über das Vorhandensein bzw. die Funktionalität von Klassen zu machen.

Will man z.B. mal fix einen einfachen Portscanner bauen, sucht man sich als erstes im CHB eine Klasse, die was mit Sockets zu tun hat. Man wird schnell fündigt, es gibt die Klasse "Socket". Darin enthalten, die Klassenmethode "pingPorts: on: timeOutSecs:", der ein Arrayobjekt mit den zu prüfenden Ports, dem zu testenden Host und die Timeout-Zeit übergeben werden. Der Quellcode der Methode liegt ebenfalls vor, dort ist im Kommentar auch gleich ein Beispiel zur Verwendung angegeben. Entsprechend konstruieren wir: "Socket pingPorts: #(21 23 25 80) on: 'www.ccc.de' timeOutSecs: 20" Ergebnis ist ein Arrayobjekt, mit den textuellen Beschreibungen der laufenden Services.

Insgesamt kann man sagen, daß die Netzwerk-Klassen umfangreich und gut dokumentiert sind. Es werden viele Standardprotokolle unterstützt. Das programmieren von Client-Server-Architekturen wird zum Kinderspiel. Standardclients, wie z.B. ein POP3-Client sind per Zweizeiler implementierbar. Diese Möglichkeiten haben natürlich eine gewisse Hackrelevanz, eine Verwendung von Squeak als Attack-Sprache wie NASL bei Nessus wäre denkbar, aber auch im zivilen Sektor hält Squeak noch einiges bereit, ein großer Clou sind die äußerst umfangreichen Multimedia-Klassen, z.B. 3D-Graphik oder Midi-Sounds. Sehr interressant ist auch die Klasse "CCodeGenerator", der Klassenname spricht für sich...

Zusammenfassend kann man sagen, das Smalltalk/ Squeak sicherlich nicht die richtige Wahl ist für zeitkritische und ressourcenschonende Anwendungen, die Vorteile liegen wo anders. Schnelle Entwicklung wird ermöglicht durch umfangreiche Tools und die ausgereifte Entwicklungsumgebung sowie die große, gut strukturierte Klassenbibliothek. Wer genötigt ist mit anderen, hybriden OO-Sprachen zu arbeiten, dem ist viel geholfen, wenn er sich mal ein wenig mit Smalltalk auseinandersetzt. Nicht zuletzt sei erwähnt, daß das Programmieren mit Smalltalk, und im Speziellen mit Squeak, einen hohen Suchtfaktor hat: es ist schnell erlernt und ermöglicht die Bewältigung komplexer Aufgaben durch ein paar einfache Anweisungen. Man kann mit Smalltalk wirklich schönen und vor allem auch sehr eleganten Code produzieren.

Reading Between the Lines: Lessons from the SDMI Challenge

Scott A. Craver[1], John R McGregor[1], Min Wu[1], Bede Liu[1], Adam Stubblefield[2], Ben Swartzlander[2], Dan S. Wallach[2], Drew Dean[3], and Edward W. Felten[4]

[Editor's Note: When Edward W. Felten wanted to publish his findings on the SDMI challenge at a congress on Computer Security, the SDMI's legal team took immediate action – with success. For a while... Initially withdrawing the paper for fear of endangering his employer, the Princeton University, Meanwhile, Felten has gained a partial victory: the SDMI now claims, that they merely 'asked him to not publish the paper' but never actually threatened him with any sanctions. Datenschleuder prints both, Felten's paper and the letter he received.]

Abstract.

The Secure Digital Music Initiative is a consortium of parties interested in preventing piracy of digital music, and to this end they are developing architectures for content protection on untrusted platforms. SDMI recently held a challenge to test the strength of four watermarking technologies, and two other security technologies. No documentation explained the implementations of the technologies, and neither watermark embedding nor detecting software was directly accessible to challenge participants. We nevertheless accepted the challenge, and learned a great deal about the inner workings of the technologies. We report on our results here.

[1] *Dept. of Electrical Engineering, Princeton University*
[2] *Dept. of Computer Science, Rice University*
[3] *Comp. Sci. Laboratory, Xerox Palo Alto Research Center*
[4] *Dept. of Computer Science, Princeton University*

1 Introduction

The Secure Digital Music Initiative (SDMI), a consortium of music-industry companies, is working to develop and standardize technologies that give music publishers more control over what consumers can do with recorded music that they buy. SDMI has been a somewhat secretive organization, releasing little information to the public about its goals, deliberations, and technology.

In September 2000, SDMI announced a "public challenge" in which it invited members of the public to try to break certain data-encoding technologies that SDMI had developed [3]. The challenge offered a valuable window into SDMI, not only into its technologies but also into its plans and goals. We decided to use the challenge to learn as much as we could about SDMI. This paper is the result of our study.[1] Section 2 presents an overview of the HackSDMI challenge. Section 3 analyzes the watermark challenges. Section 4 analyzes the

continued on p. 38

MATTHEW J. OPPENHEIM, ESQ.
[Address illegible]

RIAA April 9, 2001

Professor Edward Felton
Princeton University, Princeton, NJ 08544

Dear Professor Felten,

We understand that in conjunction with the 4th International Information Hiding Workshop to be held April 25-29, 2001, you and your colleagues who participated in last year's Secure Digital Music Initiative ("SDMI") Public Challenge are planning to publicly release information concerning the technologies that were included in that challenge and certain methods you and your colleagues developed as part of your participation in the challenge. On behalf of the SDMI Foundation, I urge you to reconsider your intentions and to refrain from any public disclosure of confidential information derived from the Challenge and instead engage SDMI in a constructive dialogue on how the academic aspects of your research can be shared without jeopardizing the commercial interests of the owners of the various technologies.

As you are aware, at least one of the technologies that was the subject of the Public Challenge, the Verance Watermark, is already in commercial use and the disclosure of any information that might assist others to remove this watermark would seriously jeopardize the technology and the content it protects[1]. Other technologies that were part of the Challenge are either likewise in commercial use or could be utilized in this capacity in the near future. Therefore, any disclosure of information that would allow the defeat of those technologies would violate both the spirit and the terms of the Click-Through Agreement (the "Agreement"). In addition, any disclosure of information gained from participating in the Public Challenge would be outside the scope of activities permitted by the Agreement and could subject you and your research team to actions under the Digital Millennium Copyright Act ("DCMA").

We appreciate your position, as articulated in the Frequently Asked Questions document, that the purpose of releasing your research is not designed to "help anyone impose or steal anything." Furthermore, you participation in the Challenge and your contemplated disclosure appears to be motivated by a desire to engage in scientific research that will ensure that SDMI does not deploy a flawed system. Unfortunately, the disclosure that you are contemplating could result in significantly broader consequences and could directly lead to the illegal distribution of copyrighted material. Such disclosure is not authorized in the Agreement, would constitute a violation of the Agreement and would subject your research team to enforcement actions under the DMCA and possibly other federal laws.

As you are aware, the Agreement covering the Public Challenge narrowly authorizes participants to attack the limited number of music samples and files that were provided by SDMI. The

[1]The Verance Watermark is currently used for DVD-Audio and SDMI Phase I products and certain portions of that technology are trade secrets

specific purpose of providing these encoded files and for setting up the Challenge was to assist SDMI in determining which of the proposed technologies are best suited to protect content in Phase II products. The limited waiver of rights (including possible DMCA claims) that was contained in the Agreement specifically prohibits participants from attacking content protected by SDMI technologies outside the Public Challenge. If your research is released to the public this is exactly what could occur. In short, you would be facilitating and encouraging the attack of copyrighted content outside the limited boundaries of the Public Challenge and thus places you and your researchers in direct violation of the Agreement.

In addition, because public disclosure of your research would be outside the limited authorization of the Agreement, you could be subject to enforcement actions under federal law, including the DMCA. The Agreement specifically reserves any rights that proponents of the technology being attacked may have "under any applicable law, including, without limitation, the U.S. Digital Millennium Copyright Act, for any acts not expressly authorized by their Agreement." The Agreement simply does not "expressly authorize" participants to disclose information and research developed through participating in the Public Challenge and such disclosure could be the subject of a DMCA action.

We recognize and appreciate your position, made clear throughout this process, that it is not your intention to engage in any illegal behavior or to otherwise jeopardize the legitimate commercial interests of others. We are concerned that your actions are outside the peer review process established by the Public Challenge and setup by engineers and other experts to ensure the academic integrity of this project. With these facts in mind, we invite you to work with the SDMI Foundation to find a way for you to share the academic components of your research while remaining true to your intention to not violate the law or the Agreement. In the meantime, we urge you to withdraw the paper submitted for the upcoming Information Hiding Workshop, assure that it is removed from the Workshop distribution materials and destroyed, and avoid a public discussion of confidential information.

Sincerely,

[Signature]

Matthew Oppenheim, Secretary

The SDMI Foundation

cc: Mr. Ira S. Moskowitz, Program Chair, Information Hiding Workshop, Naval Research Laboratory
Cpt. Douglas S. Rau, USN, Commanding Officer, Naval Research Laboratory
Mr. Howard Ende, General Counsel of Princeton
Mr. Edward Dobkin, Computer Science Department Head of Princeton

continued from p. 36

non-watermark challenges. Finally, we present our conclusions in section 5.

2 The SDMI Challenge

The SDMI challenge extended over roughly a three-week period, from September 15, 2000 until October 8, 2000. The challenge actually consisted of six sub-challenges, named with the letters A through F, each involving a different technology developed by SDMI. We believe these challenges correspond to submissions to the SDMI's Call for Proposals for Phase II Screening Technology [4]. According to this proposal, the watermark's purpose is to restrict an audio clip which is compressed or has previously been compressed. That is, if the watermark is present an audio clip may yet be admitted into an SDMI device, but only if it has not been degraded by compression. For each challenge, SDMI provided some information about how a technology worked, and then challenged the public to create an object with a certain property. The exact information provided varied among the challenges. We note, though, that in all six cases SDMI provided less information than a music pirate would have access to in practice.

2.1 Watermark Challenges

Four of the challenges (A, B, C, and F), involved watermarking technologies, in which subtle modifications are made to an audio file, to encode copyright control information without perceptible change in how the file sounds. Watermarks can be either robust or fragile. Robust watermarks are designed to survive common transformations like digital-to-audio conversion, compression and decompression, and the addition of small amounts of noise to the file. Fragile watermarks do not survive such transformations, and are used to indicate modification of the file. For each of the four watermark challenges, SDMI provided three files:

- File 1: an unwatermarked song;
- File 2: File 1, with a watermark added; and
- File 3: another watermarked song.

The challenge was to produce a file that sounded just like File 3 but did not have a watermark -- in other words, to remove the watermark from File 3.

SDMI provided an on-line "oracle" for each challenge. Entrants could email a file to the oracle, and the oracle would tell them whether their submission satisfied the challenge, that is, whether it contained no detectable watermark while still sounding like File 3. Entrants were given no information about how watermark information was stored in the file or how the oracle detected watermarks, beyond the information that could be deduced from inspection of the three provided files.

2.2 Challenges D and E

Challenge D concerned a technology designed to prevent a song from being separated from the album in which it was issued. Normally, every Compact Disc contains a table of contents, indicating the offsets and lengths of each audio track, followed by the audio data itself. Challenge D adds an "authenticator" track (approximately 50ms of very quiet audio,) a digital signature derived from the table of contents, which is supposed to be difficult to compute for an arbitrary CD. Challenge D is discussed in more detail in Section 4.1.

1 The SDMI challenge offered a small cash payment to be shared among everyone who broke at least one of the technologies and was willing to sign a confidentiality agreement giving up all rights to discuss their findings. The cash prize amounted to the price of a few days of time from a skilled computer security consultant, and it was to be split among all successful entrants, a group that we suspected might be significant in size. We chose to forgo the payment and retain our right to publish this paper.

Challenge E involved a technology similar to D, but one which would be immune to the obvious attack on technology D, in which one compiled an unauthorized CD with the same table of contents as an authorized one, for which the authenticator track is given. Unfortunately, this challenge was constructed in a way that made it impossible to even start analyzing the technology. SDMI provided an oracle for this challenge, but unfortunately provided no music samples of any kind, so there was no way to determine what the oracle might be testing for.

Given these facts, we decided not to analyze Challenge E. It is discussed briefly in Section 4.2.

3 The Watermarking Schemes

In this section, we describe our attack(s) on each of the four watermark challenges (A,B,C,F). Our success was confirmed by emails received from SDMI's oracles.

Figure 1 provides an overview of the challenge goal. As mentioned earlier, there are three audio files per watermark challenge: an original and watermarked version of one clip, and then a watermarked version of a second clip, from which the mark is to be removed. All clips were 2 minutes long, sampled at 44.1kHz with 16-bit precision.

The reader should note one serious flaw with this challenge arrangement. The goal is to remove a robust mark, while these proposals appear to be Phase II watermark screening technologies [4]. As we mentioned earlier, a Phase II screen is intended to reject audio clips if they have been compressed, and presumably compression degrades a fragile component of the watermark. An attacker need not remove the robust watermark to foil the Phase II screen, but could instead repair the modified fragile component in compressed audio. This attack was not possible under the challenge setup.

3.1 Attack and Analysis of Technology A

A reasonable first step in analyzing watermarked content with original, unmarked samples is differencing the original and marked versions in some way. Initially, we used sample-by-sample differences in order to determine roughly what kinds of watermark- ing methods were taking place. Unfortunately, technology A involved a slowly varying phase distortion which masked any other cues in a sample-by-sample difference. We ultimately decided this distortion was a pre-processing separate from the watermark, in part because undoing the distortion alone did not foil the oracle.

The phase distortion nevertheless led us to attempt an attack in which both the phase and magnitude change between sample 1 and sample 2 is applied to sample 3. This attack was confirmed by SDMI's oracle as successful, and illustrates the general attack approach of imposing the difference in an original-watermark pair upon another media clip. Here, the "difference" is taken in the FFT domain rather than the time domain, based on our suspicions regarding the domain of embedding. Note that this attack did not require much information about the watermarking scheme itself, and conversely did not provide much extra insight into its workings.

A next step, then, is to compute the frequency response $H(w) = W(w)/O(w)$ of the watermarking process for segments of audio, and observe both $|H(w)|$ and the corresponding impulse response $h(t)$. If the watermark is based on some kind of linear filter, whose properties change slowly enough relative to the size of a frame of samples, then this approach is ideal.

Figure 2 illustrates one frequency response and impulse response about 0.3 seconds into the

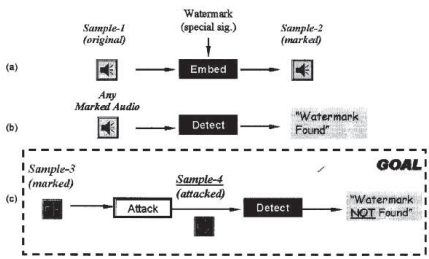


Fig. 1. The SDMI watermark attack problem. For each of the four watermark challenges, Sample-1, sample-2, and sample-3 are provided by SDMI sample-4 is generated by participants in the challenge and submitted to SDMI oracle for testing.

music. These responses are based on FFTs of 882 samples, or one fiftieth second of music. As can be clearly seen, a pair of sinusoidal ripples are present within a certain frequency band, approximately 8-16Khz. Ripples in the frequency domain are indicative of echoes in the time domain, and a sum of sinusoids suggested the presence of multiple echoes. The corresponding impulse response h(t) confirms this. This pattern of ripples changes quite rapidly from frame to frame.

Thus, we had reason to suspect a complex echo hiding system, involving multiple time-varying echoes. It was at this point that we considered a patent search, knowing enough about the data hiding method that we could look for specific search terms, and we were pleased to discover that this particular scheme appears to be listed as an alternative embodiment in US patent number 05940135, awarded to Aris corporation, now part of Verance [5]. This provided us with little more detail than we had already discovered, but confirmed that we were on the right track, as well as providing the probable identity of the company which developed the scheme. It also spurred no small amount of discussion of the validity of Kerckhoffs's criterion, the driving principle in security that one must not rely upon the obscurity of an algorithm. This is, surely, doubly true when the algorithm is patented.

The most useful technical detail provided by the patent was that the "delay hopping" pattern was likely discrete rather than continuous, allowing us to search for appropriate frame sizes during which the echo parameters were constant. Data collection from the first second of audio showed a frame size of approximately 882 samples, or 1/50 second. We also observed that the mark did not begin until 10 frames after the start of the music, and that activity also existed in a band of lower frequency, approximately 4-8 Khz. This could be the same echo obscured by other operations, or could be a second band used for another component in the watermarking scheme. A very clear ripple in this band, indicating a single echo with a delay of about 34 samples, appears shortly before the main echo-hopping pattern begins.

The next step in our analysis was the determination of the delay hopping pattern used in the watermarking method, as this appeared to be the "secret key" of the data embedding scheme. It is reasonable to suspect that the pattern repeats itself in short order, since a watermark detector should be able to find a mark in a subclip of music, without any assistance initially

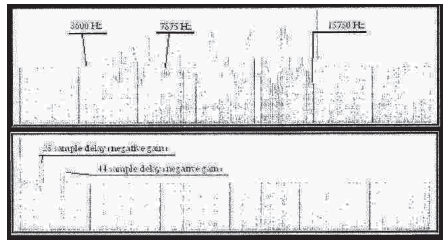


Fig. 2. A short-term complex echo. Above, the frequency response between the watermarked and original music, taken over 1/50 second, showing a sinusoidal ripple between 8 and 16 KHz. Below, the corresponding impulse response. The sinusoidal pattern in the frequency domain corresponds to a pair of echoes in the time domain.

aligning the mark with the detector's hopping pattern. Again, an analysis of the first second revealed a pattern of echo pairs that appeared to repeat every 16 frames, as outlined in figure 3. The delays appear to fall within six general categories, each delay approximately a multiple of 1/4 millisecond. The exact values of the delays vary slightly, but this could be the result of the phase distortion present in the music.

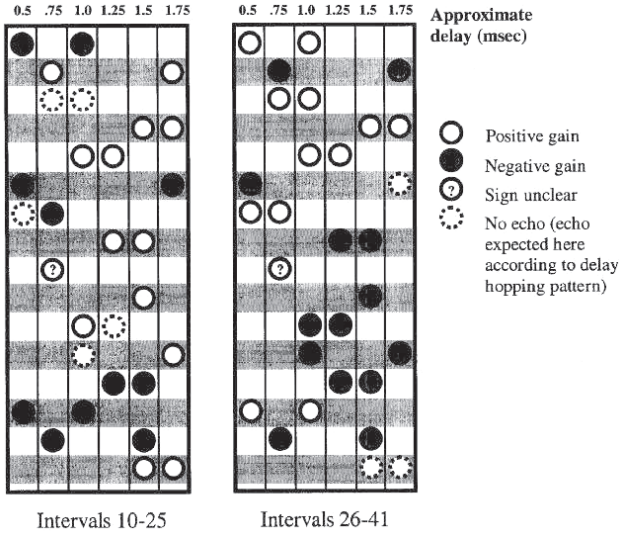


Fig. 3. The hypothesized delay hopping pattern of technology A. Here two stretches of 16 frames are illustrated side-by-side, with observed echoes in each frame categorized by six distinct delays: 2, 3, 4, 5, 6 or 7 times 0.00025 sec. Aside from several missing echoes, a pattern appears to repeat every 16 frames. Note also that in each frame the echo gain is the same for both echoes.

The reader will also note that in apparently two frames there is only one echo. If this pattern were the union of two pseudorandom patterns chosen from six possible delay choices, two "collisions" would be within what is expected by chance.

Next, there is the issue of the actual encoded bits. Further work shows the sign of the echo gain does not repeat with the delay-hopping pattern, and so is likely at least part of an embedded message. Extracting such data without the help of an original can be problematic, although the patent, of course, outlines numerous detector structors which can be used to this end. We developed several tools for cepstral analysis to assist us in the process. See [2] for in introduction to cepstral analysis; Anderson and Petitcolas [1] illustrate its use in attacks on echo hiding watermark systems.

With a rapidly changing delay, normal cepstral analysis does not seem a good choice. However, if we know that the same echo is likely to occur at multiples of 16/50 of a second, we can improve detector capability by combining the information of multiple liftered[2] log spectra.

Three detector structures are shown in figure 4. In all three, a collection of frames are selected for which the echo delays are believed to be the same. For each, the liftered log of an FFT or PSD of the frame is taken. In the first two structures, we compute a cepstrum, for each frame, then either average their squared magnitudes, or simply their squares, in hopes that a spike of the appropriate quefrency will be clear in the combination. The motivation for merely squaring the spectral coefficients comes from the observation that a spike due to an echo will either possess a phase of theta or theta + pi for some value theta. Squaring without taking magnitudes can cause the echo phases to rein-

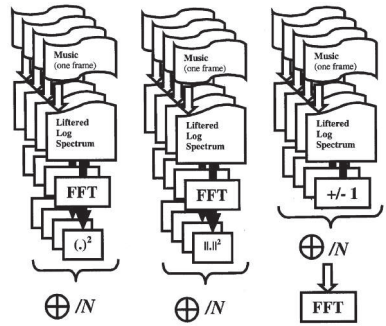


Fig. 4. Three cepstral detector structures. In each case we have a collection of distinct frames, each believed to possess echoes of the same delay. The first two compute cepstral data for each frame, and sum their squares (or squared magnitudes) to constructively combine the echo signal in all frames. The third structure illustrates a method for testing a hypothesized pattern of positive and negative gains, possibly useful for brute-forcing or testing for the presence of a known "ciphertext."

force, whilst still permitting other elements to combine destructively.

In the final structure, one cepstrum. is taken using a guess of the gain sign for each suspect frame. With the correct guess, the ripple should be strongest, resulting in the largest spike from the cepstral detector. Figure 5 shows the output of this detector on several sets of suspect frames. While this requires an exponential amount of work for a given amount of frames, it has a different intended purpose: this is a brute-forcing tool, a utility for determining the most probable among a set of suspected short strings of gain signs as an aid to extracting possible ciphertext values.

Finally, there is the issue of what this embedded watermark means. Again, we are uncertain about a possible signalling band below 8Khz. This could be a robust mark, signalling presence of a fragile mark of echoes between 8 and 16 KHz. The 8-16KHz band does seem like an unusual place to hide robust data, unless it does indeed extend further down, and so this could very easily be hidden information whose degredation is used to determine if music has already been compressed.

Of course, knowledge of either the robust or fragile component of the mark is enough for an attacker to circumvent the scheme, because one can either remove the robust mark, or repair or reinstate the fragile mark after compression has damaged it. As mentioned earlier, this possible attack of repairing the fragile component appears to have been ruled out by the nature of the SDMI challenge oracles. One must wait and see if real-world attackers will attempt such an approach, or resort to more brute methods or oracle attacks to remove the robust component.

3.2 Attack on Challenge B

We analyzed samp1b.wav and samp2b.wav using short-time FFT. Shown in Fig. 6 are the two FFT magnitudes for 1000 samples at 98.67 sec. Also shown is the difference of the two magnitudes. A spectrum notch around 2800Hz is observed for some segments of samp2b.wav and another notch around 3500Hz is observed for some other segments of samp2b.wav. Similar notches are observed in samp3b.wav. The attack fills in those notches of samp3b.wav with random but bounded coefficient values. We also submitted a variation of this attack involving different parameters for notch desc-

2 in accordance with the flopped vocabulary used with cepstral analysis, "liftering" refers to the process of filtering data in the frequency domain rather than the time domain. Similarly, "quefrencies" are frequencies of ripples which occur in the frequency domain rather than the time domain.

ription. Both attacks were confirmed by SDMI oracle as successful.

3.3 Attacks on Challenge C

By taking the difference of samp1c.wav and samp2c.wav, bursts of narrowband signal are observed, as shown in Fig. 7. These narrow band bursts appear to be centered around 1350 Hz. Two different attacks were applied to Challenge C. In the first at- tack, we shifted the pitch of the audio by about a quartertone. In the second attack, we passed the signal through a bandstop filter centered around 1350Hz. Our submissions were confirmed by SDMI oracle as successful. In addition, the perceptual quality of both attacks has passed the "golden ear" testing conducted by SDMI after the 3-week challenge.

3.4 Attack on Challenge F

For Challenge F, we warped the time axis, by inserting a periodically varying delay. The delay function comes from our study on Technology-A, and was in fact initially intended to undo the phase distortion applied by technology A. Therefore the perceptual quality of our attakked audio is expected to be better than or comparable to that of the audio watermarked by Technology-A. We also submitted variations of this at- tack involving different warping parameters and different delay function. They were confirmed by SDMI oracle as successful.

4 The Non-Watermark Technologies

The HackSDMI challenge contained two "non-watermark" technologies. Together, they appear to be intended to prevent the creation of "mix" CDs, where a consumer might compile audio files from various locations to a writable CD. This would be enforced by universally embedding SMDI logic into consumer audio CD players.

4.1 Technology D

According to SDMI, Technology D was designed to require "the presence of a CD in order to 'rip' or extract a song for SDMI purposes." The technology aimed to accomplish this by adding a 53.3 ms audio track (four blocks of CD audio), which we will refer to as the authenticator, to each CD. The authenticator, combined with the CD's table of contents (TOC), would allow a SDMI device to recognize SDMI compliant CDs. For the challenge, SDMI provided 100 different "correct" TOC-authenticator pairs as well as 20 "rogue tracks". A rogue track is a track length that does not match any of the track lengths in the 100 provided TOCs. The goal of the challenge was to submit to the SDMI oracle a correct authenticator for a TOC that contained at least one of the rogue tracks.

The oracle for Technology D allowed several different query types. In the first type, an SDMI

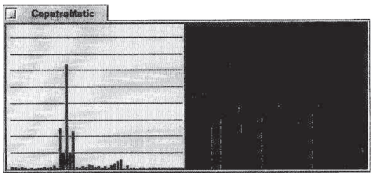


Fig. 5. Detection of an echo. A screenshot of our CepstroMatic utility shows a combination of 4 separate frames of music, each a fiftieth of a second long, in which the same echo delay was believed to exist. Their combination shows a very clear ripple on the right, corresponding to a clear cepstral spike on the left.

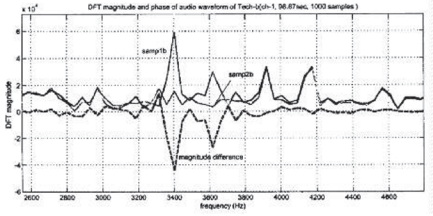


Fig. 6. Technology-B: FFT magnitudes of samp1b.wav and samp2b.wav and their difference for 1000 samples at 98.67 sec.

provided TOC-authenticator combination is submitted so a that user can "understand and verify the Oracle." According to SDMI, the result of this query should either be "admit" for a correct pair or "reject" for an incorrect pair. When we attempted this test a SDMI-provided pair, the oracle responded that the submission was "invalid." After verifying that we had indeed submitted a correct pair, we attempted several other submissions using different TOC-authenticator pairs as well as different browsers and operating systems[3]. We also submitted some pairs that the oracle should have rejected; these submissions were also declared "invalid." Though we alerted SDMI to this problem during the challenge, the oracle was never repaired. For this reason, our analysis of Technology D is incomplete and we lack definitive proof that it is correct. That having been said, we think that what we learned about this technology, even without the benefit of a correctly functioning oracle, is interesting.

Analyzing the Signal Upon examination of the authenticator audio files, we discovered several patterns. First, the left and right channels contain the same information. The two channels differ by a "noise vector" u, which is a vector of small integer values that range from -8 and 8. Since the magnitude of the noise is so small, the noise vector does not significantly affect the frequency characteristics of the signal. The noise values appear to be random, but the noise vector is the same for each of the 100 provided authenticator files. In other other words, in any authenticator file, the difference between the left and right channels of the ith sample is a constant fixed value u[i]. This implies that the noise vector u does not encode any TOC-specific information.

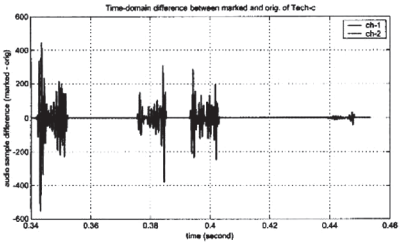


Fig. 7. Challenge-C: Waveform of the difference between samp1c.wav and samp2c.wav.

Second, the signal repeats with a period of 1024 samples. Because the full signal is 2352 samples long, the block repeats approximately 1.3 times. Similarly to the left and right channels of the signal, the first two iterations of the repeating signal differ by a constant noise vector v. The difference between the ith sample of the first iteration and the ith sample of the second iteration differ by a small (and apparently random) integer value v[i] ranging from -15 to 15. In addition, v is the same for each of the provided authenticator files, so v does not encode any TOC-specific information.

Third, the first 100 samples and last 100 samples of the full signal are faded in and faded out, respectively. This is illustrated in Figure 8. The fade-in and fade-out are meaningless, however, because they simply destroy data that is repeated in the middle of the file. We conjecture that this fade-in and fade-out are included so that the audio signal does not sound offensive to a human ear.

Extracting the Data Frequency analysis on the 1024 sample block shows that almost all of the signal energy is concentrated in the 16-20kHz range, as shown in Figure 9. We believe this range was chosen because these frequencies are less audible to the human ear. Closer examination shows that this l6-20kHz range is divided up into 80 discrete bins, each of which appears to carry one bit of information. As shown in Figure 10, these bits can be manually

[3] *Specifically, Netscape Navigator and Mozilla under Linux, Netscape Navigator under Windows NT, and Internet Explorer under Windows 98 and 2000.*

counted by a human using a graph of the magnitude of signal in the frequency domain.

Close inspection and pattern matching on these 80 bits of information reveals that there are only 16 bits of information repeated 5 times using different permutations. Using the letters A-P to symbolize the 16 bits, these 5 permutations are described in Figure 11.

```
ABCDEFGHIJKLMNOP
OMILANHGPBDCKJFE
PKINHODFMJBCAGLE
FCKLGMEPNOADJBHI
PMGHLECAKDONIFJB
```

Fig. 11. The encoding of the 16 bits of data in Technology D

Because of the malfunctioning oracle, we were unable to determine the function used to map TOCs to authenticators, but given an actual SDMI device, it would be trivial to brute force all 216 possibilities. Likewise, without the oracle, we could not determine if there was any other signal present in the authenticator (e.g., in the phase of the frequency components with nonzero magnitude).

For the moment, let us assume that the hash function used in Technology D has only 16 bits of output. Given the number of distinct CDs available, an attacker should be able to acquire almost, if not all, of the authenticators. We note that at 9 kilobytes each, a collection of 65,536 files would fit nicely on a single CD.

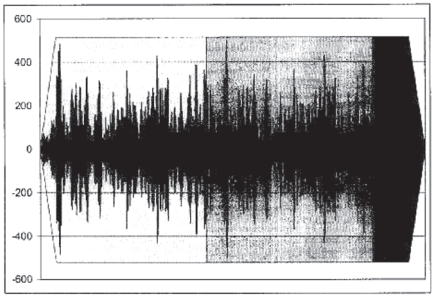


Fig. 8. In a Technology D Authenticator, the signal fades in, repeats, and fades out.

Many people have CD collections of 300+ discs, which by the birthday paradox makes it more likely than not that there is a hash collision among their own collection.

Our results indicated that the hash function used in Technology D could be weak or may have less than 16 bits of output. In the 100 authenticator samples provided in the Technology D challenge, there were 2 pairs of 16-bit hash collisions. We will not step through the derivation here, but the probability of two or more collisions occurring in n samples of X equally likely possibilities is:

$$1-\left(\prod_{i=1}^{n-1}\frac{X+1-i}{X}\right)\left(1+\frac{n^2-3n+2}{2X}\right)$$

If the 16-bit hash function output has 16 bits of entropy, the probability of 2 collisions occurring in n = 100 samples of X = 216 possibilities is 0.00254 (by the above 1.5 equation). If X ~ 211.5, the chances of two collisions occurring is about even. This suggests that either 4 bits of the 16-bit hash output may be outputs of functions of the other 12 bits or the hash function used to generate the 16-bit signature is weak. It is also possible that the challenge designers purposefully selected TOCs that yield collisions. The designers could gauge the progress of the contestants by observing whether anyone submits authenticator A with TOC B to

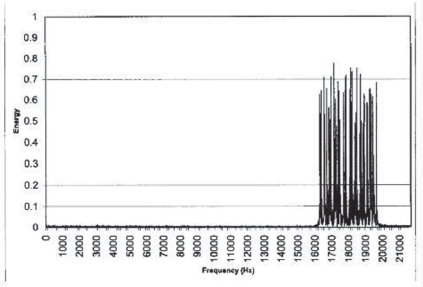


Fig. 9. Magnitude vs. Frequency of Technology D Authenticator

the oracle, where authenticator A is equal to authenticator B. Besides the relatively large number of collisions in the provided authenticators, it appears that there are no strong biases in the authenticator bits such as significantly more or less 1's than 0's.

4.2 Technology E

Technology E is designed to fix a specific bug in Technology D: the TOC only mentions the length of each song but says nothing about the contents of that song. As such, an attacker wishing to produce a mix CD would only need to find a TOC approximately the same as the desired mix CD, then copy the TOC and authenticator from that CD onto the mix CD. If the TOC does not perfectly match the CD, the track skipping functionality will still work but will only get "close" to track boundaries rather than reaching them precisely. Likewise, if a TOC specified a track length longer than the track we wished to put there, we could pad the track with digital silence (or properly SDMI-watermarked silence, copied from another valid track). Regardless, a mix CD played from start to end would work perfectly. Technology E is designed to counter this attack, using the audio data itself as part of the authentication process.

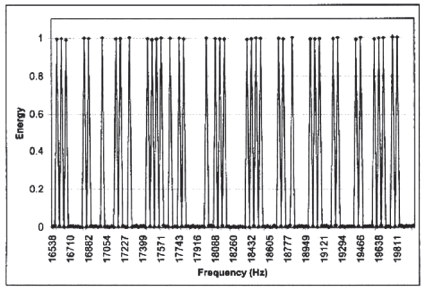


Fig. 10. Individual Bits From a Technology D Authenticator

The Technology E challenge presented insufficient information to be properly studied. Rather than giving us the original audio tracks (from which we might study the unspecified watermarking scheme), we were instead given the tables of contents for 1000 CDs and a simple scripting language to specify a concatenation of music clips from any of these CDs. 'Me oracle would process one of these scripts and then state whether the resulting CD would be rejected.

While we could have mounted a detailed statistical analysis, submitting hundreds or thousands of queries to the oracle, we believe the challenge was fundamentally flawed. In practice, given a functioning SDMI device and actual SDMI-protected content, we could study the audio tracks in detail and determine the structure of the watermarking scheme.

5 Conclusion

In this paper, we have presented an analysis of the technology challenges issued by the Secure Digital Music Initiative. Each technology challenge described a specific goal (e.g., remove a watermark from an audio track) and offered a web-based oracle that would confirm whether the challenge was successfully defeated.

We have reverse-engineered and defeated all four of their audio watermarking technologies. We have studied and analyzed both of their "non-watermarking" technologies to the best of our abilities given the lack of information available to us and given a broken oracle in one case.

Some debate remains on whether our attacks damaged the audio beyond standards measured by "golden ear" human listeners. Given a sufficient body of SDMI-protected content using the watermark schemes presented here, we are confident we could refine our attacks to introduce distortion no worse than the water-

marks themselves introduce to the the audio. Likewise, debate remains on whether we have truly defeated technologies D and E. Given a functioning implementation of these technologies, we are confident we can defeat them.

Do we believe we can defeat any audio protection scheme? Certainly, the technical details of any scheme will become known publicly through reverse engineering. Using the techniques we have presented here, we believe no public watermark-based scheme intended to thwart copying will succeed. Other techniques may or may not be strong against attacks. For example, the encryption used to protect consumer DVDs was easily defeated. Ultimately, if it is possible for a consumer to hear or see protected content, then it will be technically possible for the consumer to copy that content.

References

1. R. J. ANDERSON, AND F. A. P. PETITCOLAS. On the limits of steganography. IEEE Journal of Selected Areas in Communications 16,4 (May 1998),474-481.
2. R. P. BOGERT, M., AND J. W. TUKEY. The frequency analysis of time series for echoes: Spectrum, pseudo-autocovariance, cross-spectrum and saphe-cracking. In Proceedings of the Symposium on Time Series Analysis (Brown University, June 1962), pp. 209-243.
3. R. PETROVIC, J. M. WINOGRAD, K., AND E. METOIS. Apparatus and method for encoding and decoding information in analog signals, Aug. 1999. US Patent No 05940135 http://www.delphion.com/details?pn=US05940135__.
4. SECURE DIGITAL MUSIC INITIATIVE. Call for Proposals for Phase II Screening Technology, Version 1.0, Feb. 2000. http://www.sdmi.org/download/FRWG00022401-Ph2_CFPv1.0.PDF.
5. SECURE DIGITAL MUSIC INITIATIVE. SDMI public challenge, Sept. 2000. http://www.hacksdmi.org.

Und dann noch unser Innenminister…
Bundesministerium des Innern, Pressemitteilung Berlin, 10. April 2001:

"Berichte über 'Hacker-Methoden' sind falsch"

Zu Meldungen über angebliche "Angriffe des Innenministerium mit Hacker-Methoden gegen rechtsextremistische Websites" erklärt der Sprecher des Bundesministeriums:

"Es ist schlichter Unsinn zu behaupten, der Bundesinnenminister habe Hacker-Angriffe gegen rechtsextremistische Web-Sites in die Diskussion gebracht. Davon war nie die Rede. Es geht vielmehr darum, daß Internetangebote mit rechtsextremistischen, neonazistischen, antisemitischen und gewaltverherrlichenden Inhalten eine steigende Bedrohung sind. Allein im letzten Jahr hat sich dies Angebot auf jetzt 800 Seiten verdoppelt. Diese Angebote werden fast ausnahmslos im Ausland ins Netz gestellt, so dass deutsche Gesetze insoweit keine Handhabe bieten. Dennoch muss versucht werden, diese kriminellen Aktivitäten einzudämmen. Dabei darf keine rechtlich oder auch technisch zulässige Möglichkeit außer Acht gelassen werden. Dies ist ein schwieriger Prozess, weil eine Fülle von deutschen, ausländischen und völkerrechtlichen Rechtsnormen zu beachten sind. Bislang sind noch keine Entscheidungen getroffen worden. Das Bundesinnenministerium ist mit ausländischen und übernationalen Sicherheitsbehörden im ständigen Dialog über dies Thema, weil eine nachhaltige Bekämpfung krimineller und extremistischer Internetangebote nur im weltweiten Maßstab möglich sein wird."

(wenn der mal nicht nach Redaktionsschluss noch über seine Stasi-Akte bzw. seine Mandantenverhältniss zu einem DDR-Embargohändler namens Moneten-Müller stolpert…)

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: _____

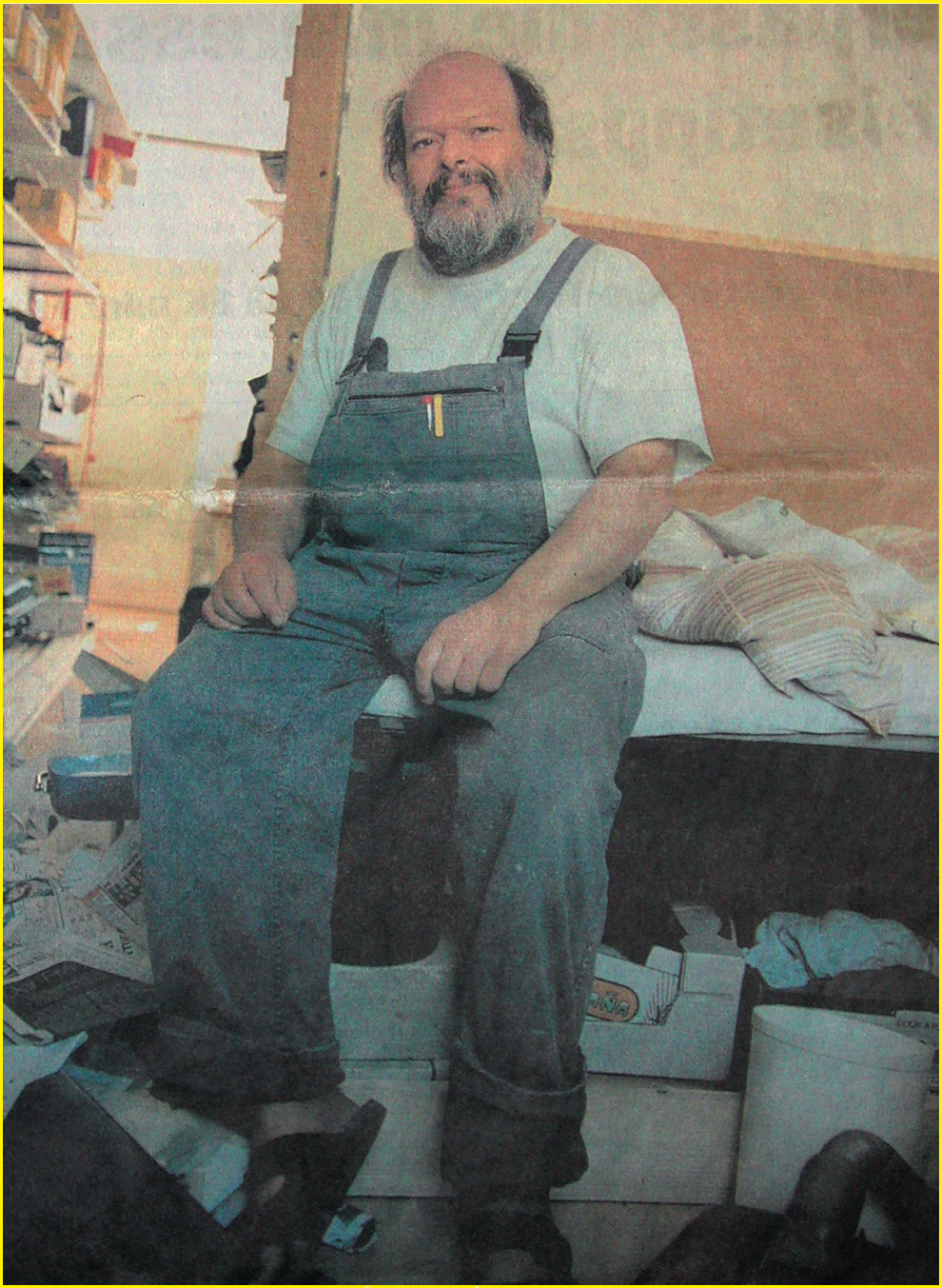
PLZ, Ort: _____

Tel., Fax: _____

E-Mail: _____

Ort, Datum: _____

Unterschrift: _____



*20.12.1951 †29.07.2001