die datenschleuder.

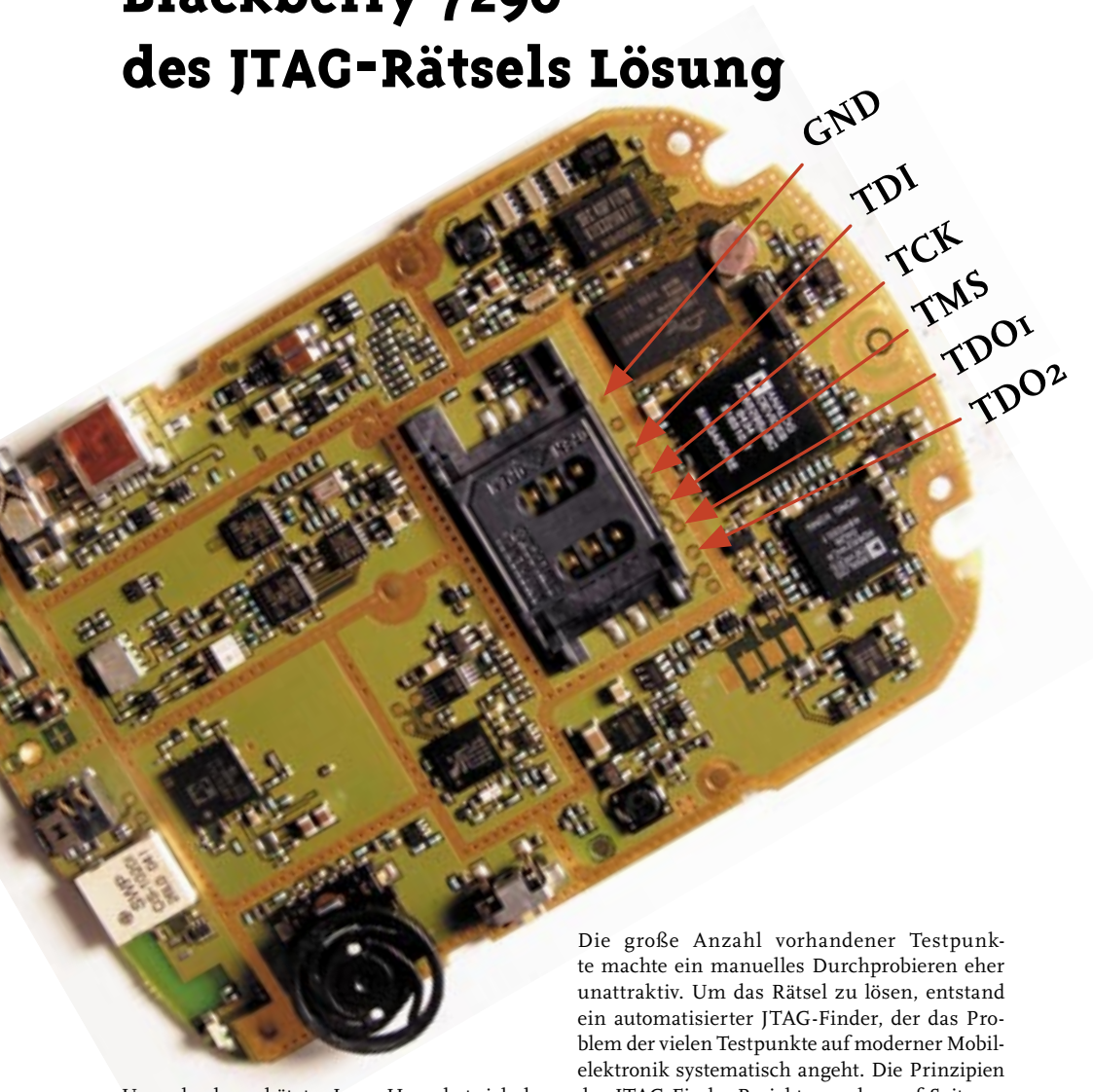
das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

Pragmatismus in Thailand: GSM-Basisstation mit Palmenantenne.
Photo aufgenommen von David Bank auf Koh Phi-Phi / Thailand

ISSN 0930-1054 • 2006
€2,4999999999999999999
Postvertriebsstück C11301F

#90

Blackberry 7290 – des JTAG-Rätsels Lösung



Unser hochgeschätzter Leser Hunz hat sich des Blackberry-Testpunkt-Rätsels aus der letzten Datenschleuder angenommen und es erfolgreich gelöst. Detaillierte Forschungsergebnisse zum JTAG am Blackberry 7290 gibt es unter

http://www.c3a.de/wiki/index.php/Image:Bberry-7290.jpg

Die große Anzahl vorhandener Testpunkte machte ein manuelles Durchprobieren eher unattraktiv. Um das Rätsel zu lösen, entstand ein automatisierter JTAG-Finder, der das Problem der vielen Testpunkte auf moderner Mobilelektronik systematisch angeht. Die Prinzipien des JTAG-Finder-Projekts werden auf Seite 20 dieser Ausgabe der Datenschleuder erläutert. Ausführliche Doku und mehr JTAG-Pinouts von verschiedenen Geräten, die mit Hilfe des Finders gefunden wurden, gibt es unter

http://www.c3a.de/wiki/index.php/JTAG_Finder

Ein Licht am Ende des Tunnels macht Mut. Man weiß zwar nicht, ob es vielleicht doch nur der entgegenkommende Zug ist, aber es gibt zumindest so etwas ähnliches wie Hoffnung. Die Gerichte erweisen sich als unsere letzte Hoffnung bei der Zähmung marodierender ProblemPolitiker.

Der Europäische Gerichtshof erklärt die Übergabe der Flugpassagierdaten an die USA für illegal, das OLG Frankfurt befindet, „Online-Demonstrationen" seien keine Gewalt. Das Bundesverfassungsgericht kippt das Gesetz zum Abschuß vollbesetzter Passagiermaschinen und die Rasterfahndung. Und das OLG Düsseldorf entschärft das Risiko für Betreiber von Internet-Foren. Es scheint, als ob der Rechtsstaat noch ein bißchen funktionierte. Die nicht geführte gesellschaftliche Debatte über die Balance zwischen „Sicherheit" und individuellen Freiheiten wird hilfsweise durch Gerichtsurteile ersetzt.

SchadPolitiker aller Couleur finden, daß diese aufsässigen Richter sich gefälligst aus dem Alltagsbetrieb der Demokratur heraushalten sollen. Flugpassagierdaten werden weiter übermittelt, weil die USA sonst einseitig mit dem Entzug der Landerechte drohen. Die angemessene Antwort darauf wäre die Drohung mit einer Sperre für US-Fluggesellschaften, analog zu den beliebten USA-EU-Handelskriegen.

Unser Kriegsminister schwadroniert derart vom übergesetzlichen Passagiermaschinen-Abschuß-Notstand. Es stellt sich die Frage, warum er nicht vom Verfassungsschutz beobachtet wird. Es ist nun also Bürgerpflicht, die Umsetzung von Gerichtsurteilen durchzusetzen. Als Schmankerl soll die Bundeswehr ganz offiziell die Aufgabe erhalten, uns gelegentlich einen schönen neuen Strand dazuzuerobern, vorzugsweise mit ein paar ergiebigen Ölquellen. Da kommt doch Freude auf.

Der Mangel an Respekt der Regierenden vor den Grundpfeilern der Gesellschaft zwingt wohl oder übel dazu, sich mit den Basics der Demokratie zu befassen. Mit „Sicherheitsüberprüfungen" von Hobbypiloten und WM-Würstchenverkäufern wird eine Kultur der Furcht etabliert, die politsche Opposition schnell zur „feindlich-negativen Grundeinstellung" stempelt, die diskriminiert werden muss. Wahlmaschinen gehören ganz sicher auf unsere Zielliste für dieses Jahr. Wenn wir diese PolitikerProblemFälle irgendwann wieder loswerden wollen, dürfen sie nicht die Gelegenheit erhalten, sich auch noch die Wahlen unter Machterhaltsgesichtspunkten zu „optimieren".

In diesem Sinne wünscht die Redaktion unseren Lesern einen hackfreudigen Sommer.

Inhalt

Dear Datenschleuder,

in der Ausgabe 87, die ich ansonsten sehr informativ fand, hat mich die Seite 35 sehr verärgert. Beim meist zum Scheitern verurteilten Versuch, kapitalistische Prozesse zu visualisieren, wählte Ihr ausgerechnet eine Heuschrecke, hippes Symbol für die bösen Kapitalisten und Aktiengesellschaften, die plagenmäßig alles leerfressen würden.

Dafür, dass ihr ansonsten gern genauer hinschaut wie die Dinge funktionieren, ist das ein ärgerlicher Bezug auf eine populäre wie populistische, oberflächliche und gar gefährliche Sicht auf das Funktionieren der Verhältnisse. Ich habe mal ein wenig herumgesucht, ob ich was kurzes finde, in dem dazu einige Aspekte drinstehen, ihr könnt bei Interesse ja mal hier drauf schauen: *http://www.jungle-world.com/seiten/2005/20/5517.php* <Sascha>

Beschwer Dich bei Münte! – Nein, im Ernst: Du argumentierst mit ein paar Totschlagargumenten, die Dir genausowenig gut anstehen, wie der Gebrauch der Parabel, die Du uns vorwirfst. Allein daraus, daß die Heuschreckenmetapher holzhammermäßig gegen alle Kapitalisten gebraucht wird, kann man nicht ableiten, daß dieses Bild nicht doch vereinzelt zutrifft.

Unseres Erachtens gibt es eine zentrale kritische Infrastruktur, zu der neben Geld, Wasser, Strom, Straßen und Netzwerk natürlich auch Identifikationskarten gehören, die nicht wie andere Geschäftsfelder dem freien Spiel des Marktes überlassen werden dürfen. Zuweilen müssen dort langfristige und nicht immer lohnende Investitionen getätigt werden, Entscheidungen, die der Markt nicht zwingend goutiert.

Eine Privatisierung dieses Geschäfts, mit dem immamenten Versprechen, nicht pleite gehen zu können (schließlich geht es um eine kritische Infrastruktur), lockt nun genau **die** *Finanzinvestoren an, die man auch ohne schlechtes Gewissen als Heuschrecken beschimpfen kann. Mit Unterstützung der Politik werden ihnen nun per Dekret Zwangsumsätze zugeschachert.* <erdgeist>

Sinn der ganzen Sache

Moin, ich habe da mal so eine Frage. Man hoert immer, dass ein Hacker wieder ein System gehackt hat oder aehnliches.

Ich höre sowas zwar eher selten, kann aber einfach damit zu tun haben, daß ich nicht wirklich in Script-Kiddie-Kreisen verkehre. Was hört man denn da zum Beispiel so?

Macht ihr das aus freien Stuecken, gibt euch jemand einen Auftrag, oder macht ihr das aus Spass–das ist natuerlich immer dabei, klar–um es allen zu demonstrieren, das es nicht sicher ist.

Ähm, was meinst Du genau mit "das"? Und nein, Aufträge zur "Prüfung" bestimmter Systeme übernimmt der CCC nicht, warum, steht sogar auf unserer der Website.

Wenn ihr soetwas nicht ankuendigt, habt ihr dann schon mal etwas auf die Muetze bekommen, oder sagen alle, toll danke, da muessen wir wohl mal was tun.

Was tut ihr?

Das wissen wir leider manchmal selbst nicht so genau, aber wir schauen dann einfach mal, ob und was dabei rauskommt. Aber so ist das halt mit kreativen Ideen... ;)

Wo steckt euer Sinn?

Wir sind. Ist das nicht Sinn genug? ;)

Warum macht ihr es?

Es? Meinst Du, warum wir "sind"? Darauf hat leider nicht mal unser Haus-Theologe eine Antwort.

Werdet ihr dafuer bezahlt?

Leider nein. Aber wenn Du das ändern möchtest:

```
Chaos Computer Club
Konto 59 90 90-201
BLZ 200 100 20
Postbank Hamburg
```

Nein, im Ernst: Ich glaube, Du hast ein völlig falsches Verständnis vom CCC. Möglicherweise einfach geprägt von den Massenmedien, das kann ich persönlich leider nicht beurteilen. Aber allein die Tatsache, daß Du nachgefragt hast, ist sehr sympathisch.

Wenn Du wirklich wissen willst, was der CCC ist und tut, komm doch einfach mal in einer der lokalen Treffs vorbei und rede mit den Leuten, die da so rumlaufen, da beißt (fast) keiner: https://www.ccc.de/regional?language=de

Das Kreuzverhör geht weiter...

Es muss doch eine Grundidee geben, oder ein Hauptziel, Grund der Bildung des CCCs etc.

Das ist einfach: Allgemeines Interesse am kreativen Umgang mit Technik.

Gibt es einen Oberhacker bei Euch.

Wie überall sind natürlich die Leute mehr oder weniger aktiv und prägen daher auch unterschiedlich stark die Arbeit des CCC aber es gibt hier weder Titel noch Hierarchien, weil sowas den Grundsätzen des CCC entgegensteht.

Ich habe einfach nur Interesse und möchte ein klein bisschen mehr mit meiner Mühle machen. Wo ich nun so langsam hinter das System meiner Suse steige will ich auch mehr.

Was ist "mehr"?

Sollte ich tatsächlich ein paar Cuxhavener finden die Lust hätten, einen CCC-Kreis zu gruenden, dann sollte ich wenigstens wissen worum es geht.

Wenn Du etwas tust, sollte das etwas sein, was **Du** *tun willst. Wenn es sich dann noch mit den Zielen von anderen (z.B. CCC) deckt, ist es ja umso besser, aber das sollte nicht Bedingung für Dein Tun sein.*

Die Fragen stellte Martin L., für die Datenschleuder antwortete Martin G.

Badeschleuder

Habe ein Abo bei euch und mir ist die Ausgabe 89 in der Wanne baden gegangen. Würde Sie deshalb gerne nachbestellen.

Wunderschönen guten Tag, wir könnten die nächste Ausgabe in einer wasserdichten Spezialedition herausbringen, dann kann man damit auch baden gehen... vorerst klickst Du hier:

https://berlin.ccc.de/index.php/Konsum <erdgeist>

Mäusejagd revisited

Ok, das kommt bisschen spät, da die DS#88 schon mehr als ein halbes Jahr zurückliegt, aber ich dacht mir: Das musst du probieren, ob das wirklich geht!

Gesagt, getan: Da ich selber keine M$ Maus besitze, bin ich einfach in den nächsten E-Markt gefahren und hab mir die Seriennummer, die ja angeblich bei der Hotline verlangt, wird abgeschrieben. Im übrigen gar nicht so einfach, weil Logitech wohl mittlerweile sowas wie ein Monopol hält was Mäuse und Tastaturen angeht. Naja, kein Wunder, die M$ Dinger sind auch ganz schöner Schrott, ich musste mir ernsthaft überlegen, ob ich das hier überhaupt durchziehe, was mach ich denn mit so einer häßlichen Maus wenn das wirklich klappt?!

Daheim hab ich die Hotline angerufen und so wie bei euch beschrieben versucht eine Laser Funkmaus von M$ zu reklamieren, obwohl ich gar keine besaß, ich Schelm. :P Nunja, das Ergebnis war das der Herr am anderen Ende eine Produkt-ID (kurz PID) haben wollte die wohl am unteren Ende der Maus sitzen sollte. Da wurde es natürlich etwas heikel für mich, habe mich aber mit "das muß wohl durch vieles Benutzen abgescheuert worden sein" nochmal rausreden können!

Mein Fazit: entweder Ihr hattet nur Glück, weil eure alte Maus noch keine solche PID hatte oder die haben mittlerweile das Loch in ihrem Support gestopft!

Bleibt mir nur, noch euch viel Spaß mit euren "ergaunerten" M$ Mäusen zu wünschen, ich hätte den eh nicht gehabt, die Mäuse sind schrecklich unergenomisch und unkewl! ;P

<Fabian>

Aus der „öfter mal im Briefkasten"-Abteilung

ich bin schon lange bei euch mitglied aber habe immer noch keine Datenschleuder bekommen, heißt das jetzt ich habe den Beitrag umsonst bezahlt????

Ich hoffe ich werde bald man eine oder mehrere bekommen <Alex>

Da sich diese Frage nun doch häuft: Wer Mitglied wird oder ein Abonnement erwirbt, wird in die Adressenliste eingetragen und bekommt ab der **nächsten** *Ausgabe eine Schleuder nach Hause.*

Die kann belastungs- und inhaltsbedingt auch ein wenig länger dauern, einzig garantiert ist, daß 4 Ausgaben jährlich im Briefkasten landen.

Den Phasenprüfer mißverstanden...

ich habe folgendes Problem mit ARCOR. Jeden Abend von 22.00 Uhr bis 0.00 Uhr ist mein Internetzugang gestört.

Ich habe den Verdacht das mein Internetverhalten nicht in die Kalkulation von Arcor passt und man mir deshalb den Zugang in der angegebenen Zeit sperrt. Ein Fehler in meinem Netzwerk scheidet aus da ich selbst der Administrator bin.

Sollten sie Interesse haben, der Sache nachzugehen und meine Leitung zu überprüfen bin ich dazu gerne bereit. <Andreas L.>

Wie sollen wir "die Leitung prüfen"? – Was sagt denn Arcor dazu? – Und was bedeutet "Internetzugang gestört"?

Ein "Administrator" sollte schon eine etwas genauere Fehleranalyse erstellen können... <FrankRo>

Auf eine Nachfrage eines besorgten Mitglieds bei seiner Bank:

Sehr geehrter Herr F.,

vielen Dank für die Zusendung des Artikels. Wir freuen uns, dass Sie als Vorstandsmitglied des CCC e. V. zu unseren Kunden zählen.

Gern kommen wir der Klärung des Sachverhaltes nach.

Die NetBank wurde im Jahr 2005 auf einen Softwarebug hingewiesen. Der Hinweis war aber letztendlich mit dem Versuch einer Erpressung verbunden.

Mit diesem Hinweis sind sicherlich manche Reaktionen der NetBank in diesem Fall leichter nachzuvollziehen.

Der Fehler wurde auch von der NetBank bereits im Vorfeld des Treffens behoben. In diesem Punkt, wie auch bei vielen anderen, möchten wir noch erwähnen, das die Darstellungen des Artikels (Datenschleuder #88) erhebliche Abweichungen mit dem tatsächlichen Fall aufweisen.

Es wäre aus diesem Grund auch wünschenswert gewesen, wenn man sich im Vorfeld der Recherche mit der NetBank in Verbindung gesetzt hätte.

Das Thema IT-Sicherheit hat bei uns geschäftsbedingt einen sehr hohen Stellenwert und wird durch zahlreiche externe EDV-Revisoren und Sicherheitsfirmen begleitet.

Als eine der unabhängigen Security Firmen möchten wir hier nur *www.atsec.com* erwähnen.

Wie gerade Sie sicherlich wissen, ist trotz aller Security-Prüfungen durch externe EDV-Revisoren und Sicherheitsfirmen, vorgegebenen Softwareentwicklungsmethoden, Softwarequalitätsprüfungen und der Ausrichtung nach BSI-Grundschutz, das Thema IT-Sicherheit immer eine Momentaufnahme.

Aus diesem Grund durchlaufen wir jedes Jahr kontinuierliche Security-Prüfungen.

Wir hoffen, Ihnen mit dieser Ausführung geholfen zu haben und verbleiben

Mit freundlichen Grüßen

Gerald Artelt
Prokurist / Bereichsleiter IT-Strategie & Datamining
NetBank AG

Anmerkung der Redaktion:

Daß die Geschichte ein Geschmäckle hat, war der Redaktion natürlich bewußt. Daß die Datenschleuder, wie in einem früheren Falle, als Druckmittel für einen Beratervertrag eingesetzt würde, war hier nicht zu befürchten. Die Hin- und Rückbuchung auf das Konto waren der eigentliche Ausschlaggeber für den Abdruck der Geschichte.

Nichtsdestotrotz räumen wir Versäumnisse bei der Recherche ein, da wir dachten, schon der Artikel allein würde, insbesondere in Hinsicht auf die Rolle des Vaters, den gesamten Sachverhalt in ein korrektes Licht rücken.

Wir geben der NetBank ganz selbstverständlich Raum für eine Gegendarstellung, in der sie ihre Sicht der Dinge schildern kann, bis dato ist eine solche bei uns nicht eingegangen.

Für die Redaktion Datenschleuder <erdgeist>

Erscheinung Ihrer Adresse auf meinem Rechner

Hallo Ihr Pfeifen, in Zukunft bitte von meinem Rechner fernhalten. Thanks <*lifeartist@xxx.de*>

Alter, wenn du Erscheinungen an deinem Rechner hast, ist das dein Ding. Wenn dir unsere Adresse erscheint, ist die Geschichte schlimm – du solltest einen Arzt konsultieren. Wenn du uns „Pfeifen" nennst, wirst du sicher einen Arzt brauchen, deine Punkte in Flensburg nachzählen und mal öfter über deine Schulter schauen müssen. <erdgeist>

Foto: Wolfgang Hilse

Nachruf auf Gerriet Hellwig

Mit einem Lächeln verstarb Gerriet am 7. Juni 2006.

Wir danken ihm für die Zeit, die er bei uns war.

Er hat sich nicht nur mit Computern beschäftigt, sein Interesse galt auch der freiheitlichen Kindererziehung, der Farbtheorie, dem Umgang mit Hunden und Pferden, kreativem Kochen–und so vielem mehr. Seine Art zu diskutieren und zu denken hat uns viel gegeben.

Gerriet war einer der wenigen Menschen, der nicht nur über den Tellerrand hinaussehen konnte, sondern auch als Visionäre neue Wege zeigte und lebte. Er war ein besonderer Mensch, immer voller neuer Ideen und Freundlichkeit, und er teilte beides gerne.

Er war auch ein treuer Freund–so war er regelmäßig bei Wau, als dieser im Koma lag, und kümmerte sich darum, daß er gut versorgt wurde.

Die Welt verliert einen Denker, der die Symbiose zwischen "Bauch" und "Kopf" geschafft hat. Und einen sensiblen, humorvollen und intelligenten Freund.

Gerriet, wir vermissen Dich.

Piratendemonstration

Auf der Demonstration am 03.06.2006 in Stockholm/Schweden, zu der die dort bei den Parlamentswahlen antretende Piratenpartei einlud, hielt deren Anführer, Rickard Falkvinge, eine flammende Rede über philosophische Hintergründe des modernen Netzpiratentums. Hier ein Transkript, unter Zuhilfenahme anderer Übersetzungen aus dem Schwedischen übersetzt von Maha.

Freunde, Bürger, Piraten!

Es gibt nichts Neues unter der Sonne.

Mein Name ist Rickard Falkvinge, und ich bin der Anführer der Piratenpartei. Während der letzten Woche haben wir einige Übergriffe miterleben müssen. Wir haben gesehen, wie die Polizei die ihnen zu Verfügung stehenden Mittel mißbraucht hat. Wir haben gesehen, wie hochrangige Politiker mobil gemacht haben, um die Medienindustrie in Schutz zu nehmen.

All das ist ungeheuer skandalös. Deshalb stehen wir heute hier.

Die Medienindustrie will uns davon überzeugen, daß es nur um Vergütungsfragen geht, also darum, wie eine bestimmte Berufsgruppe bezahlt wird. Daß es um ihre stetig sinkenden Verkaufszahlen geht, um trockene Statistik. Das ist ein Vorwand. Es geht um etwas ganz anderes!

Um die heutige Situation im Licht der Geschichte zu verstehen, müssen wir 400 Jahre zurückgehen – zurück in eine Zeit, als die Kirche das Kultur- und Wissensmonopol hatte. Was die Kirche sagte, hatte zu geschehen. Kommunikation war wie eine Pyramide hierarchisiert: Es gab eine Person an der Spitze, die mit einer gewissen Zahl anderer weiter unten in der Pyramide sprach. Kultur und Wissen hatten eine Quelle, und diese Quelle war die Kirche. Gnade Gott denen, die es wagten, das Kultur- und Wissensmonopol der Kirche in Frage zu stellen! Sie wurden den zu jener Zeit denkbar schlimmsten Mißhandlungen ausgesetzt. Die Kirche erlaubte den Bürgern unter keinen Umständen, selbst Informationen zu verbreiten; sie beherrschte die gesamte Gesetzgebung: Prävention, Verfolgung und Bestrafung.

Es gibt nichts Neues unter der Sonne.

Heute wissen wir, daß die Befreiung des Wissens das einzig Richtige für die Gesellschaft ist. Galileo Galilei hatte Recht; auch er kämpfte gegen das Wissensmonopol. Wir sprechen hier von einer Zeit, in der die Kirche die Meinung vertrat, daß Bürger nicht lernen müßten zu lesen und zu schreiben, denn der Pfarrer würde ihnen ohnehin alles sagen, was sie zu wissen hätten. Die Kirche wußte, was es bedeutet hätte, wenn sie die Kontrolle verloren hätte. Dann kam der Buchdruck. Plötzlich gab es nicht nur eine Wissensquelle, auf die man hören konnte, sondern mehrere. Die Bürger, die angefangen hatten, lesen zu lernen, konnten von unsanktioniertem Wissen profitieren. Die Kirche war wütend. Die Königshäuser waren wütend. Die britische Krone erließ sogar ein Gesetz, daß nur Drucker, die speziell von der Krone zum Buchdruck befugt waren, das Wissen und die Kultur für die Bürger vermehren durften. Dieses Gesetz wurde "Copyright" genannt.

Dann vergingen einige hundert Jahre und die Pressefreiheit wurde geschaffen. Aber überall existierte immer noch dasselbe alte Kommunikationsmodell: eine Person teilt vielen etwas mit. Es gab verschiedene Leute, auf die man hören konnte, aber überall galt: eine Person teilt vielen etwas mit. Das wurde vom Staat benutzt, um das Konzept eines "verantwortlichen Herausgebers" einzuführen.

Die Bürger können zwar selbst am Wissen teilhaben, doch es wird immer jemanden geben, der verantwortlich gemacht werden kann, wenn sie – welch schrecklicher Gedanke – am falschen Wissen teilhaben. Das ist es, was sich jetzt grundsätzlich verändern wird. Denn das Internet gehorcht diesem Modell nicht mehr. Heute laden wir nicht mehr einfach nur Kultur und Wissen herunter. Wir laden gleichzeitig hoch – zu anderen. Wir verteilen Dateien. Wissen und Kultur entziehen sich plötzlich einer zentralen Kontrolle.


Rickard Falkvinge

Das ist der zentrale Punkt meiner Ansprache, deshalb werde ich ins Detail gehen: Downloaden ist das alte mediale Modell zentraler Kontrolle mit einem verantwortlichen Herausgeber, der angeklagt werden kann, dem Mittel gekürzt werden können usw., wo jeder Zugang zu Wissen und Kultur über eine Zentrale kontrolliert wird, die genau die Rechte vergeben kann, die sie für angemessen hält.

Kultur- und Wissensmonopol, Kontrolle:

Filesharing ermöglicht das gleichzeitige Hoch- und Herunterladen durch alle vernetzten Personen, ohne jede zentrale Kontrolle; die gesamte Kultur und Information fließt gleichzeitig zwischen Millionen verschiedener Menschen. Das ist etwas grundlegend anderes, etwas komplett Neues in der Geschichte der menschlichen Kommunikation. Es gibt niemanden mehr, der verantwortlich gemacht wird, wenn falsches Wissen verbreitet wird. Deshalb reden die Firmen so viel von legalen Downloads. Legal. Downloads. Denn sie versuchen, nur das Abholen von einem zentralen Punkt unter ihrer Kontrolle zu erlauben. Downloaden, nicht Filesharing. Und genau das ist der Grund, warum wir das Gesetz ändern werden.

Während der letzten Wochen haben wir gesehen, wie weit einer der Akteure zu gehen bereit ist, nur um nicht die Kontrolle zu verlieren. Wir haben gesehen, wie die Verfassung verletzt wurde. Wir haben gesehen, wie Zwangsmaßnahmen und Angriffe auf die persönliche Integrität von der Polizei durchgeführt wurden – nicht um Verbrechen zu bekämpfen, sondern um die Beteiligten und ihr Umfeld zu belästigen.

Es gibt nichts Neues unter der Sonne, und die Geschichte wiederholt sich immer wieder. Es geht nicht um die Vergütung einer bestimmten Berufsgruppe. Es geht um die Macht über Kultur und Wissen, denn wer diese Dinge beherrscht, beherrscht die Welt.

Die Medienindustrie hat versucht, uns ein schlechtes Gewissen einzureden, indem sie uns sagt, daß das was wir tun, illegal sei, daß wir Piraten seien. Sie versuchen uns zu erdrücken. Schaut euch heute um – schaut, wie sie versagt haben. Ja, wir sind Piraten. Aber wer es für eine Schande hält, Pirat zu sein, hat Unrecht. Wir sind stolz darauf!

Denn wir wissen ja schon, was es heißt, ohne zentrale Kontrolle zu leben. Wir haben ja schon die Freiheit geschmeckt, gefühlt und gerochen, ohne zentrales Wissens- und Kulturmonopol zu leben. Wir haben ja schon gelernt, zu lesen und zu schreiben.

Und wir werden auch nicht vergessen, wie man liest und wie man schreibt, nur weil es den Medien von gestern nicht in den Kram paßt.

Mein Name ist Rickard und ich bin ein Pirat!

Der große Bruder fliegt auch Dich

Zuverlässigkeitsüberprüfung für alle im neuen Luftsicherheitsgesetz

von Otto Groschenbügel und Winston Smith <ds@ccc.de>

Am 18. Juni 2004 beschloß der Bundestag das Luftsicherheitsgesetz (LuftSiG) [1] zum Schutz vor Angriffen auf die Sicherheit des Luftverkehrs. Laut §7 dieses Anfang 2005 in Kraft getretenen Gesetzes muß sich nun neben zahlreichen anderen Betroffenen ausnahmslos jeder fliegende Bürger vom Motorseglerpiloten an aufwärts jedes Jahr einer„ Zuverlässigkeitsüberprüfung" (ZÜP) unterziehen – inklusive weitestgehender Durchleuchtung durch alle deutschen Sicherheitsbehörden und Geheimdienste, nach nirgendwo nachprüfbaren Kriterien, mit potentiell schwerwiegenden Folgen für den Einzelnen – und natürlich kostenpflichtig.

Da der Luftverkehr grundsätzlich nicht anderen Zwecken dient als der Straßenverkehr oder die Schiffahrt, aufgrund der deutlich kleineren Zahl der aktiven Teilnehmer aber ein politisch besonders geeignetes Erprobungsfeld für die Implementierung von (vorgeschobenen oder tatsächlich intendierten) Sicherheitsmaßnahmen auf Kosten einer überschaubaren Zahl von Betroffenen darstellt, soll in diesem kleinen Beitrag versucht werden, kurz exemplarisch darzustellen, was morgen jeden von uns erwarten kann, wenn rechtsstaatliche Freiheiten und Grundsätze allzu bereitwillig aufgegeben werden. Denn: Ist dies der Fall, sind Seesicherheitsgesetz und Straßensicherheitsgesetz nur eine Frage der Zeit.

Die Zuverlässigkeitsüberprüfung: Willkommen, Genosse Mielke!

Zunächst ist es nicht zuletzt vor dem Hintergrund einer potentiellen Ausdehnung auf weitere Lebensbereiche recht interessant, nicht nur herauszustellen, was die Zuverlässigkeitsüberprüfung umfaßt, sondern vor allem auch, auf welche Weise sie zustandekommt und durchgeführt wird. Ihre rechtliche Grundlage, das Luftsicherheitsgesetz, war schon während seiner Entstehung von den Wogen des emotionalen Aktionismus nicht gänzlich unberührt und im Bundestag von vehementen Forderungen bis hin zur Grundgesetzänderung begleitet – der geneigte Leser möge sich anhand der Plenarprotokolle [2] selbst ein Bild machen, in welchem Umfang sich die von ihm gewählten Politiker noch Einigkeit und Recht und Freiheit verpflichtet fühlen. Auf die Entstehungsgeschichte und erlesene handwerkliche Qualität des Gesetzes, insbesondere des §14 Abs. 3, der bei Vorliegen bestimmter Umstände den gezielten Abschuß von Verkehrsflugzeugen durch Entscheid des Verteidigungsministers vorsah, soll an dieser Stelle aber nicht weiter eingegangen werden – zumal nachdem die letztgenannte Passage mittlerweile vom Bundesverfassungsgericht als verfassungswidrig gekippt wurde [3].

Die rechtliche Klärung der im gleichen Gesetz in §7 eingeführten Zuverlässigkeitsüberprüfung steht derzeit allerdings noch aus; so hat u.a. der deutsche Verband der Allgemeinen Luftfahrt AOPA Verfassungsbeschwerde gegen diesen §7 eingelegt. Was umfaßt aber nun die in diesem Paragraphen definierte Zuverlässigkeitsüberprüfung, und wie wird sie durchgeführt? Es geht darum, daß sich jeder (!) Pilot

mit deutscher Lizenz vom Motorsegler an aufwärts jährlich (!) einer solchen Zuverlässigkeitsüberprüfung unterziehen muß. Tut er dies nicht, ist er natürlich per definitionem unzuverlässig und wird in Folge seine Lizenz verlieren. Betroffen sind überdies alle, die beruflich „nicht nur gelegentlich Zugang zu nicht allgemein zugänglichen Bereichen des Flugplatzgeländes eines Verkehrsflughafens“ haben, bis hinunter zu den Reinigungsunternehmen und Warenlieferanten.

Alle werden im Rahmen der Überprüfung fürsorglich und vor allem gründlich durchleuchtet: Neben Anfragen bei den Polizeivollzugs- und den Verfassungsschutzbehörden der Länder werden Bundes- und Zollkriminalamt, das Bundesamt für Verfassungsschutz, der Bundesnachrichtendienst, der Militärische Abschirmdienst und sogar der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR im Gesetz ausdrücklich als in die Zuverlässigkeitsüberprüfung mit einzubeziehende Behörden genannt. Darüberhinaus darf die die ZÜP durchführende Behörde (i.d.R. das für den Wohnort zuständige Regierungspräsidium, d.h. eine einfache Landesbehörde) unbeschränkte Auskünfte aus dem Bundeszentralregister einholen, ggf. das Ausländerzentralregister und die zuständigen Ausländerbehörden konsultieren sowie „Anfragen an die Flugplatzbetreiber und Luftfahrtunternehmen sowie an den gegenwärtigen Arbeitgeber des Betroffenen“ (sic!) stellen.

Der Betroffene ist selbstverständlich darüber hinaus nach §7(3) verpflichtet, an seiner eigenen Überprüfung mitzuwirken. Sämtliche Wohnorte seit der Geburt sind anzugeben und in die Zuverlässigkeitsüberprüfung mit einzubeziehen. Weh' dem, der da einmal zuviel Ärger mit dem Nachbarn hatte oder gar von einem IM aktenkundlich angeschwärzt wurde. Auslandsaufenthalte sind sowieso verdächtig.

Besonders perfide: Da es staatlichen Behörden nach sonst geltender Gesetzeslage ja aus guten Gründen (offiziell noch?) nicht gestattet ist, ohne weiteres beliebige Daten von Polizei, Geheimdiensten usw. über einen Bürger zu sammeln, zu kombinieren, seinen Arbeitgeber und andere Personen aus seiner Umgebung ganz unverbindlich und neutral auszuhorchen und all dies' in einer Akte zusammenzustellen, muß der fliegende Bürger jedes Jahr „freiwillig“ durch Stellen eines dahingehenden Antrags mit seiner eigenen Unterschrift seine Zustimmung zu einer solchen Datensammlung nicht nur geben, sondern sogar selbst beantragen und somit selbst die §1 und §4a des Bundesdatenschutzgesetzes für sich außer Kraft setzen. Logisch folgerichtig sind die Kosten für die aus der Antragstellung resultierende Schnüffelei (je nach Bundesland unterschiedlich, im Gespräch

sind 25 bis hin zu 255 EUR p.a.) selbstverständlich auch vom Antragsteller selbst zu tragen.

„Unsere Juristen müssen begreifen, dass der Staat und das von ihm geschaffene Recht dazu dienen, die Politik von Partei und Regierung durchzusetzen."

Dem geneigten Leser könnten nun bereits erste Zweifel kommen, ob die ZÜP nicht möglicherweise genauso wie der bereits gekippte §14(3) des gleichen Gesetzes zum gezielten Abschuß von Verkehrsflugzeugen schlichtweg verfassungswidrig ist. Warum, so könnte er sich z.B. fragen, werden, wenn die Terrorgefahr solch schwerwiegende Eingriffe denn offensichtlich erfordert, dann nicht alle dieser offenbar ja überall auftretenden potentiellen Terroristen gleichbehandelt? Warum müssen sich nicht z.B. alle Autofahrer (Oklahoma) oder alle S- und U-Bahn-Fahrer (Tokio, Madrid) einer Zuverlässigkeitsüberprüfung stellen? Oder alle Bauarbeiter in Schulgebäuden, Lehrer und Theaterbesucher (Beslan, Moskau)?

Gerade wenn sich der geneigte Leser über das zahlenmäßige Verhältnis von Attentaten mit Autobomben (neben Oklahoma drängen sich u.a. Jakarta, Sharm El-Sheikh, Bagdad, Kerbala u.v.a.m. im Irak, in Israel usw. usf. auf) zu Attentaten insbesondere mit Kleinflugzeugen klar wird, wird er doch einige Verwunderung darüber ausdrücken, warum hier eine bestimmte Bevölkerungsgruppe offensichtlich unter Generalverdacht gestellt wird, ohne daß auch nur vage Anhaltspunkte eines Terrorverdachts bestehen [4]. Dies umso mehr, wenn er weiß, daß diese Maßnahmen gegen tatsächliche und motivierte Terroristen vollkommen wirkungslos sind: Seit 1944 ist im Chicagoer Abkommen über die internationale Zivilluftfahrt („ICAO-Abkommen") verbindlich geregelt, daß jeder Mitgliedsstaat verpflichtet ist, nach bestimmten Regeln seinen Luftraum für ausländische Flugzeuge aus anderen ICAO-Mitgliedsstaaten zu öffnen. Gerüchteweise sollen diese ausländischen Flugzeuge ja nun auch von ausländischen Piloten gesteuert werden. Wahlweise natürlich auch von deutschen Piloten mit ausländischen Lizenzen. Diese brauchen sich der hoheitlich-deutschen ZÜP aber selbstverständlich nicht zu unterziehen. Als ausländischer Pilot, so könnte man meinen, lebt es sich in Deutschland möglicherweise besser und mit mehr Privatsphäre denn als Einheimischer?

Darüberhinaus könnte der geneigte Leser weitere grundsätzliche Bedenken haben, wenn er sich klarmacht, daß die ihm aus grauer verfassungstreuer Vorzeit möglicherweise noch bekannte Unschuldsvermutung in diesem Verfahren fröhlich negiert wird: Die Zuverlässigkeit ist durch den Piloten nachzuweisen, nicht etwa die Unzuverlässigkeit durch die Behörden, auch wenn diese quasi als kostenpflichtige Dienstleister den Bürger bei dieser seiner Pflicht unterstützen.

Der Leser mag sich auch fragen, ob er sich möglicherweise nicht mehr richtig daran erinnert, daß umfangreiche Ermittlungen dieser Art doch nach seinem Verständnis von einem Staatsanwalt nach Vorliegen eines begründeten Anfangsverdachts geführt werden, und daß der Betroffene selbstverständlich die Aussage ver-

weigern kann und in der ganzen Strafprozeßordnung nirgendwo davon die Rede ist, daß der Beschuldigte an Ermittlungen gegen ihn mitzuwirken verpflichtet ist. Er mag sich ferner gegenwärtigen, daß laut Luftsicherheitsgesetz dagegen auch laufende Ermittlungsverfahren in die Beurteilung der Zuverlässigkeit einbezogen werden und sich fragen, inwiefern dies wohl mit dem Verbot der Vorverurteilung in Einklang zu bringen ist.

„Wir haben, Genossen, liebe Abgeordnete, einen außerordentlich hohen Kontakt mit allen werktätigen Menschen, in überall, ja, wir haben einen Kontakt, ihr werdet gleich hören, ihr werdet gleich hören, warum, ich liebe, ich liebe doch alle, alle Menschen, na, ich liebe doch, ich setze mich doch dafür ein."

Wenn nun aber, so beruhigt sich der geneigte Leser, solch weitgehende Ermittlungen zur Feststellung der Zuverlässigkeit durchgeführt werden, so werden diese doch sicher nur unter strengen Auflagen durchgeführt, und es wird anhand eines klar definierten und nachprüfbaren Kriterienkatalogs über die Frage der Zuverlässigkeit entschieden. Stattdessen wird er aber unter anderem feststellen, daß die Kriterien, nach denen über zuverlässig oder nicht zuverlässig entschieden wird, nirgendwo gesetzlich festgelegt sind!

Nun, denkt der geneigte Leser weiter, wenn es nicht im Gesetz steht, wird es sicherlich in der Durchführungsverordnung nachprüfbar festgelegt sein? Der §17 LuftSiG legt ja schließlich ausdrücklich fest, daß die Einzelheiten der Zuverlässigkeitsüberprüfung durch Rechtsverordnung zu regeln sind. Doch welch Überraschung: Eine solche Rechtsverordnung ist bis heute nicht erlassen worden – ebensowenig natürlich eine Gebührenordnung.

Daß die ZÜP dessen ungeachtet bundesweit bereits mit voller Routine im Gange ist, wird da sicherlich keinen stören. Heißt es doch lediglich, daß die Entscheidung darüber, ob jemand als zuverlässig oder unzuverlässig zu gelten hat, im alleinigen Ermessen des Beamten einer einfachen Landesbehörde steht!

Ein unbedarfter Narr, wem sich da das häßliche Wort „Willkürentscheid" aufdrängt.

Eine Widerspruchsmöglichkeit gibt es bei solch unfehlbaren Entscheidungen in wiederum bewundernswerter logischer Konsequenz auch nicht. Wieder wird der geneigte Leser in den Untiefen seines Gedächtnisses suchen und sich vielleicht erinnern, daß nach Art. 103 (2) GG der Bürger doch das Recht haben sollte, die Gesetze, Vorschriften und Verordnungen zu kennen, deren Verletzung für ihn zu Nachteilen führt. Wie soll man nun aber gegen unbekannte Ermessensspielräume selbst beweisen, daß

man kein Terrorist ist? Dies selbstverständlich auch noch kostenpflichtig?

Um zu verdeutlichen, daß es sich hier nicht um abstrakte Sachverhalte handelt, sondern um konkrete Probleme mit weitreichenden Konsequenzen für jeden Betroffenen, sei auszugsweise aus dem offenen Brief [5] eines Professors, anerkannter Spezialist für Flugzeugantriebe, an die für ihn zuständige Luftsicherheitsbehörde zitiert:

"Mit welchen Ausländern darf ich in Zukunft noch Kontakt haben, ohne behördlichen Zweifel an meiner Zuverlässigkeit zu wecken? Ich habe berufliche Kontakte zu US-amerikanischen Kollegen mit iranischem und pakistanischem Pass. Wenn sie mir nicht schriftlich bestätigen, dass diese Kontakte für mich auch potentiell keine negativen Konsequenzen haben können, werde ich diese abbrechen. Dieses Vorgehen zu meinem Schutz ist mir persönlich sehr unangenehm. Ich werde mich bei diesen Kollegen deshalb entschuldigen, ihnen die Gründe schriftlich mitteilen und sie über ihre Botschaften an die deutsche Regierung verweisen. […]"

Das eine oder andere Regierungspräsidium z.B. verlangt seinerseits in den suspekten Fällen, in denen der Antragsteller das Wagnis eines längeren Auslandsaufenthalts einging, regelmäßig den Nachweis der lokalen ausländischen Behörden, daß sich der Antragstellende während seines Aufenthalts dort keiner Straftat schuldig gemacht hat. Je nach Gutdünken selbstverständlich mit Apostille, amtlich beglaubigten Übersetzungen usw. und, wie schon ausgeführt, auf Kosten des Antragstellers. Genauso regelmäßig sehen sich die lokalen Behörden mangels vorhandener Zentralregister außerstande, einen solchen „Persilschein" auszustellen, was wiederum auf das Unverständnis der entsprechenden deutschen Luftsicherheitsbehörde stößt etc. ad infinitum.

Wie lange wird es noch dauern, bis sich der Begriff „feindlich-negative Grundeinstellung" wieder wie in Mielkes Zeiten in den Akten findet und Anlaß genug ist, die bürgerliche Freiheit einschränkende staatliche Maßnahmen zu rechtfertigen? Ist es vielleicht schon so weit? Das zu überprüfen ist selbstverständlich genau so wenig möglich, wie gegen einen negativen Zuverlässigkeitsbescheid Widerspruch einzulegen. Denn wenn der eigene Bürger aufgrund nachrichtendienstlicher Erkenntnisse als unzuverlässig angesehen wird, dann dürfen ebenjenem Bürger diese Erkenntnisse natürlich nicht mitgeteilt werden, denn die sind ja geheim. Catch-22, anyone?

„Die Mauer wird in 50 und auch in 100 Jahren noch bestehen bleiben, wenn die dazu vorhandenen Gründe noch nicht beseitigt sind. Das ist schon erforderlich, um unsere Republik vor Räubern zu schützen."

Zusammenfassend bleibt festzuhalten: Mit der im Luftsicherheitsgesetz festgelegten umfassenden Zuverlässigkeitsüberprüfung wird eine ganze Bevölkerungsgruppe mit nachrichtendienstlichen Mitteln ausgeforscht – mit verfehlter Zweckerfüllung, dafür aber auf verfassungsrechtlich ausgesprochen fraglichen gesetzlichen Grundlagen, nach öffentlich nicht bekannten und nicht nachvollziehbaren Kriterien, unter Preisgabe der gesetzlich geschützten Privatsphäre, auf Kosten von und mit potentiell schwerwiegenden Konsequenzen für das berufliche und private Leben der Betroffenen, ohne

ordentliche Berufungsmöglichkeit – und das jedes Jahr aufs Neue.

Der geneigte Leser sei ein letztes Mal bemüht: Er mag sich überlegen, ob er an dieser Stelle nicht beispielsweise die laufenden Verfassungsbeschwerden z.B. der AOPA unterstützen will oder zumindest beim Abgeordneten seines Wahlkreises Aufklärung über die Durchführung der Zuverlässigkeitsüberprüfung nach dem Luftsicherheitsgesetz verlangt. Was heute nur Piloten und Bodenpersonal betrifft, kann morgen auch für jeden Autofahrer Wirklichkeit werden, wenn Verhältnismäßigkeit, Recht und Augenmaß keinen Eingang mehr in Gesetzgebungsverfahren finden.

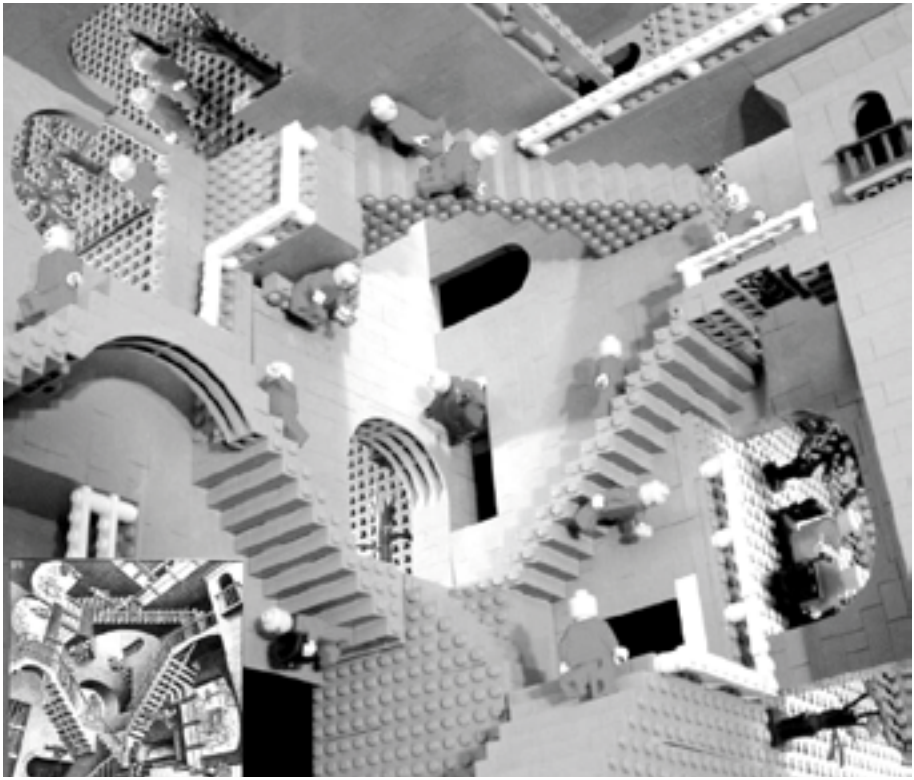
[1] Luftsicherheitsgesetz, verabschiedet als Artikel 1 des Gesetzes zur Neuregelung von Luftsicherheitsaufgaben vom 11. Januar 2005 (BGBl. I 78), am 14. Januar 2005 verkündet und am 15. Januar 2005 in Kraft getreten. Das Gesetz wurde geändert durch Artikel 49 des Gesetzes zur "Umbenennung des Bundesgrenzschutzes in Bundespolizei" vom 21. Juni 2005 (BGBl. I 1818).

[2] Plenarprotokolle des Deutschen Bundestages 15/89 vom 30. Januar 2004, 15/115 vom 18. Juni 2004 und 15/155 vom 28. Januar 2005.

[3] Entscheidung des Bundesverfassungsgerichts vom 15. Februar 2006 (1 BvR 357/05) und Bekanntmachung des BMJ vom 27. Februar 2006 (BGBl. I 486).

[4] Vgl. Verfassungsbeschwerde der AOPA beim Bundesverfassungsgericht gegen die Zuverlässigkeitsüberprüfung nach dem Luftsicherheitsgesetz.

[5] Öffentlicher Brief von Prof. Dr.-Ing. Konrad Vogeler an das Regierungspräsidium Dresden vom 16. Juni 2005.



Hacking routers using Universal Plug and Play

Armijn Hemel <armijn@uulug.nl>

At the SANE 2006 conference in Delft, the Netherlands, I presented a paper about vulnerabilities in many Universal Plug and Play enabled routers. This article is an adaption of that paper, with new updated information and more hacks than described in the original paper.

The Universal Plug and Play protocol (often simply called UPnP) is a network protocol that makes it easy to connect networked devices to a network. Special software on the devices makes it possible that they configure themselves and offer services to other devices or programs on the network, all without any intervention from the user. The ideas behind UPnP are noble, but it clashes hard with reality. In this article I will briefly show what UPnP is and how it works, after which I will show where some of the sub protocols and implementations go awfully wrong, with disastrous consequences.

The history of UPnP starts at one of our favourite inventors of security holes, namely Microsoft. In 1999 the first specifications were released, apparently as a reaction to JINI from Sun. Microsoft founded a seperate entity to govern UPnP specifications and do UPnP promotions, called the UPnP Forum. Quickly a number of companies signed up. On April, 30th 2006 the UPnP Forum had 785 members. In the subsequent years UPnP was quickly pushed.

Windows ME and Windows XP come with UPnP built in, Linksys enables most of its home routers with it and programs like MSN Messenger, X-Box Live, many networked games and bittorrent clients use it extensively.

The UPnP protocol is mostly based on open standards, or adaptions of open standards, including HTTP and SOAP. In the lifecycle of UPnP there are 5 + 1 stages.

The zeroth, optional, stage is addressing. If a device is connected to the network it will first try to get an address via DHCP. If the device does not get an IP address it will fall back to a technique called ``auto-addressing'':

1. randomly pick an IP address from \ url{169.254/16} IP range
2. if IP address is taken, abandon IP address and goto 1
3. else keep IP address

This technique is not specific to UPnP.

The first step is discovery. When a device is connected to a network, it will broadcast a packet to the multicast address `239.255.255.250` on UDP port 1900.

This packet is basically just a HTTP header. The protocol is often referred to as HTTPU (HTTP over UDP). A discovery packet can look like this:

```
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: ssdp:discover
MX: 10
ST: ssdp:all
```

All UPnP devices on the network should reply to this by sending a packet back using UDP unicast. This packet, again, consists of HTTP headers and could look like this:

```
HTTP/1.1 200 OK
CACHE-CONTROL:max-age=1800
EXT:
LOCATION:http://10.0.0.138:80/IGD.xml
SERVER:SpeedTouch 510 4.0.0.9.0 UPnP/1.0
(DG233B00011961)
ST:upnp:rootdevice
USN:uuid:UPnP-SpeedTouch510-1_00::upnp:
rootdevice
```

Interestingly, not all UPnP certified devices do this. For example, the Linksys WRT54G and related devices do not send these notifications.

Periodically, devices should also announce that they are alive, again using HTTPU. A notification looks like this:

```
NOTIFY * HTTP/1.1
HOST: 239.255.255.250:1900
CACHE-CONTROL: max-age=180
Location: http://192.168.1.1:5431/dyndev/
uuid:0014-bf09
NT: upnp:rootdevice
NTS: ssdp:alive
SERVER:LINUX/2.4 UPnP/1.0 BRCM400/1.0
USN: uuid:0014-bf09::upnp:rootdevice
```

The second stage is ``description''. What it basically means is that after discovery or notification a device can query the other device to see what functionality it offers. It does so by downloading and parsing the XML file that can be found in the "LOCATION" header of a discovery or notification message. In this XML file you can find a lot of information. The most important elements are ``controlURL'' (used in stage 3), ``eventSubURL'' (used in stage 4) and ``SCPDURL'' (not used, but informative).

You should be aware that there is no fixed URL or even a fixed port for where you can find this XML file. I have seen it vary on the same device after it was rebooted.

The most interesting stage is ``control''. In this stage devices can be controlled using SOAP. SOAP can be seen as a form of RPC over XML. Functions and values are encoded in XML and sent to the device. On the device the XML description is parsed and the function is executed (or not, if it is an invalid function or if function values are not correct). The SOAP packets are sent to the ``control URL'' which can be determined in the previous stage.

The fourth stage is called ``eventing''. Most devices keep state variables which represent some state in the device. This could be whether or not the device is up, if NAT is enabled, and so on. These variables are evented. Clients can subscribe to these events, but sending one or more callback URLs to the event's URL from stage 2. Whenever a variable changes, the new value(s) will be sent to the callback URLs.

The final, fifth, stage is called presentation. Usually this just comes down to the webinterface on the device.

Together a set of state variables and actions form a so-called ``profile''. The UPnP forum has defined various standard profiles. One of the profiles is the Internet Gateway Device profile. This profile was the first to be standardized and is currently the most widespread. The IGD profile defines a few subprofiles, of which WANPPPConnection and WANIPConnection are of particular interest, because these profiles define things like NAT rules.

Sending a request to an IGD is simple. In the example Python code I have used the SOAPpy library:

```
import os
from SOAPpy import *
# Edimax devices often have the control URL here...
control="http://192.168.0.1:49152/upnp/control/WANIPConn1"
namespace = "urn:schemas-upnp-org:service:
WANIPConnection:1"
server = SOAPProxy(control, namespace)
soapaction = "urn:schemas-upnp-org:service:WANIPConnection:
1#GetExternalIPAddress"
print "external IP", server._sa(soapaction).
GetExternalIPAddress()
```

This little command will send a SOAP request to the IGD and ask for its external IP address.

A more interesting piece of code is where you ask the IGD to make a portforward and punch a little hole in the firewall:

```
soapaction2 = "urn:schemas-upnp-org:service:WANIPConnection
:1#AddPortMapping"
server._sa(soapaction2).AddPortMapping(
        NewRemoteHost="",
        NewExternalPort=5667,
        NewProtocol="TCP",
        NewInternalPort=22,
        NewInternalClient="10.0.0.152",
        NewEnabled=1,
        NewPortMappingDescription="evil h4x0r",
        NewLeaseDuration=0)
```

This will forward external port 5667 on the external interface of the IGD to port 22 on my machine (10.0.0.152) on the LAN. This is done without authentication. With a similar request you can delete the portmapping and close the port again.

Hacking the Internet Gateway Device

The portmapping feature of an IGD might be convenient to users and programs such as MSN, but it can of course also be abused by others. At SANE I heard vague rumours that apparently there are already botnets that use the portmapping feature to open more ports to an infected machine. But there are a lot more interesting hacks possible with the IGD profile. The hacks that I will discuss are not a hole in the specification, but are a direct result of unclear specifications and sloppy programming. This nothing new of course.

Some of the bugs that are listed below are just the common ones that we've seen countless times before, for example in CGI programs. What makes it a real problem is the fact that there are literally millions of routers that have these bugs. Gijs Hillenius, the journalist from „Automatisering Gids" that first published about my research checked with Linksys about the amount of routers they ship. He was told that Linksys sells 1.5 million units of the WRT54G family PER MONTH worldwide (he actually had the marketeer repeat this three times just to be sure it was correct).

All hacks that I will describe here can only be launched from the LAN. This is a barrier and if someone has access to the LAN they can already do a lot of other interesting attacks on targets on the LAN. However, I think these attacks are a lot more interesting than others, because they involve reconfiguring the router. A trojaned machine is fairly easy to detect, but a reconfigured routers can go unnoticed for much longer.

The hacks require only a minor tweak to one of the parameters of the AddPortMapping SOAP request, namely NewInternalClient.

Hack 1: Opening other machines on the LAN

It is not clearly defined where NewInternalClient should point to. In the IGD specifications there are several definitions for this. On page 12 of the specifications (available in PDF format on the UPnP Forum website) NewInternalClient is described as:

``This variable represents the IP address or DNS host name of an internal client (on the residential LAN).''

On page 13 of the same document it says:

``Each 8-tuple configures NAT to listen for packets on the external interface of the WANConnectionDevice on behalf of a specific client and dynamically forward connection requests to that client.''

NewInternalClient has been defined to be either a normal IP address or a multicast or broadcast address (so machines behind the IGD can share things like TV streams). It is pretty obvious that a device would only ask for a portmapping on its own behalf, but the specifications are not clear.

In many implementations of the IGD it is possible to specify another machine at the LAN. This is interesting if that other machine is your internal DNS server, mail server or Windows file server.

I wouldn't necessarily want to call this a bug, because the specifications do not explicitely allow it. On the other hand, the specifications also don't mention that it should be possible. Whatever the ``official'' status is, it is at least something that in my eyes is not good.

Hack 2: Turning your router into a proxy

So, the next logical step to take is to see what happens when you change the parameter NewInternalClient from a machine on the LAN to a machine which is not on the LAN. According to the specifications this should not be possible.

The bad news (or good news, depending on your point of view) is that some implementations of IGD will accept it when NewInternalClient is actually not located on your LAN. It will still send all packets through NAT. The headers of the IP packets will be rewritten by the NATing code. This means that you can turn a router into an onion router.

For example, you could ask your router to make a portmapping for port 80, which should be sent to *www.ccc.de* port 80. When someone connects to your router on its external interface on port 80, the packet will be NATed and be sent to *www.ccc.de* port 80. The whole connection will go through the router and never go on the LAN. If you do this a few times it will be very hard to trace you, since no router logs by default.

The solution for router manufacturers is simple, just check whether or not the value of NewInternalClient actually is a machine on the LAN. If it is not on the LAN, you reject the portmapping, otherwise you accept.

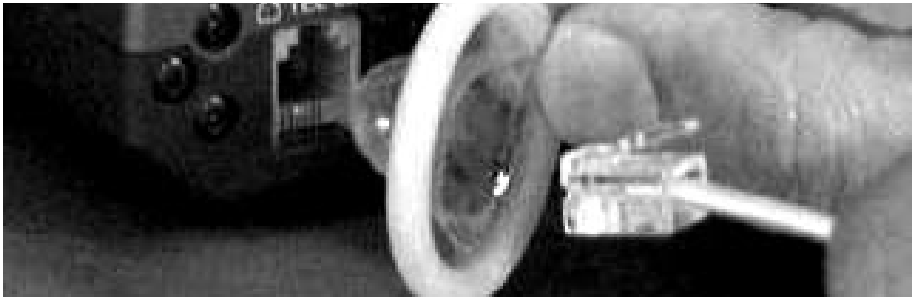
Many devices that use hardware and software from Broadcom (for an extensive list see the OpenWrt website) have this same vulnerability. The only exception is US Robotics, who fixed this in March 2005, but the patch apparently never went upstream.

Hack 3: Executing code on your router

So, what if you actually don't put IP addresses in your SOAP request, but throw in random garbage? One of the devices I looked at in my research was the Edimax BR-6104K (firmware version 3.21). In the GPL tarball Edimax has on their website you can easily find the UPnP code in the `EdiLinux/AP/upnp_adm/IGD` directory. This code is a CVS checkout of the Linux-IGD software (*http://linux-igd.sourceforge.net/*), after they rewrote it to C. In the code for `pmlist.c` you can see the following in the function `AddPortMapping()`:

```
int pmlist_AddPortMapping (
    char *protocol, char *externalPort,
    char *internalClient, char *internalPort)
{
    char command[500];
    sprintf(command, "%s -t nat -A %s -i %s -p %s -m \
mport --dport %s -j DNAT --to %s:%s", g_iptables,
g_preroutingChainName, g_extInterfaceName, protocol,
externalPort, internalClient, internalPort);
    system (command);
```

What happens is that a command is constructed using plain strings, a shell is spawned and the command is executed as a shell command. You can actually insert shell commands here. If you look through the code you will see that internalClient is restricted to 15 bytes (4 octets of the IP address, with the dots inbetween them), which gives you 15 bytes of exploit code. Two backticks for the shell command will eat up two more bytes (semi-colon did not work), so you have 13 bytes for exploit code on the device. This is enough to issue the command `/sbin/reboot`, or `flash default` (the default search path is set to `/usr/bin:/bin`, so it will find the `flash` command



through this path), which resets the device to factory defaults.

```
server._sa(soapaction2).AddPortMapping(
        NewRemoteHost="",
        NewExternalPort=21,
        NewProtocol="TCP",
        NewInternalPort=21,
        NewInternalClient="`/sbin/reboot`",
        NewEnabled=1,
        NewPortMappingDescription="blah",
        NewLeaseDuration=0)
```

I have tried uploading my own custom exploit code to the router (by appending it to a file) and executing that, but that failed. I am confident there are people who are far more inventive when it comes to abusing this.

Not every version of Linux-IGD has this problem. It is used a lot on routers and there are many versions floating around. Some of them have checks in the source code (using functions like inet_aton() to check if `NewInternalClient` is an IP address in the first place), others don't even have the length check built in and you can send arbitrary length strings to the device which will then be executed.

Some devices even use the predecessor of Linux-IGD called Pseudo-ICS, which suffers from the same problem. If you happen to think that only old routers have this problem you are very wrong, because I found it in some routers which had only been on the market for a few months at most. Devices are identified pretty easily, either by inspecting the GPL sources from the vendor website, or (if the company is violating the GPL, which seems to happen quite often) by dissecting firmware and checking if somewhere in the UPnP program there are ``iptables'' commands.

Apart from the code execution, there is also no check if the IP address is on the LAN (because there is no check at all), so devices that suffer from this are also vulnerable for the other hacks. I have seen this code used on many EdiLinux based devices.

Why?? Oh why??

A question I have asked myself a lot during my UPnP research is why manufacturers actually make these mistakes. I have a few explanations.

First of all, the engineers who wrote the code never tested with bogus input, but only with programs that actually work according to the specifications, such as MSN Messenger. If you only test with programs that behave correctly, you will miss the bugs.

Second, the specifications are written in such a way that they never even force someone who implements the specifications to think about what the values of all parameters can be.

Third, many manufacturers don't build their own systems, but instead buy it somewhere else. These companies mostly consist of marketeers and compete on time to market and price. Putting more engineering into a product would cost time and money. A competitor could put a cheaper product, with less engineering, on the market in the meantime. Most companies only care about the amount of units they sell. Support often also stops after a device is no longer on the market. Given the short lifetime of most products (around two years) this means that many devices will never be fixed.

Other profiles

The IGD profile is not the only profile which has been standardized. There are quite a few other profiles, but most of them are not used at all, but seem to be developed mainly for dickwaving purposes to be able to say "Look! We can do this too!" The best example of that is the HVAC profile (Heating, Ventilation and Air Conditioning).

The other profiles that are gaining a lot of support lately are the A/V profiles. Networked audio and video devices are getting more and more popular and there are quite a few vendors that implement UPnP on these devices. I have not yet had time to completely dive into the specifications and see if there are any big holes.

Conclusion

As you have read in this article there are many things wrong with current IGD implementations. Even though what is described here is not

directly a bug in the UPnP IGD profile, it is true that the underlying UPnP mechanisms just make it too easy for an attacker. The complete lack of security in the protocol is astonishing.

Personally I am wondering whether or not exploits for the bugs described here will be released and actively used. Of course, I'm hoping nothing will happen.

List of vulnerable devices

Below is a list of devices that I have tested myself and found to be vulnerable. There are a lot more devices that are vulnerable that I have found through simple code review, but I have not included them. Also not included are devices that are similar or the same, except for the packaging.

You will find a list of devices per manufacturer. Listed are the name of the unit and, if applicable, the hardware revision. Also included is the firmware revision and which bugs are in the device (1: forward to other machines on the LAN, 2: forward to external machines, 3: code execution on the router).

Linksys

name	firmware	1	2	3	comments
WRT54G v2.2	3.03.9	x	x		on by default
WRT54G v2.2	4.20.7	x	x		on by default
WRT54G v2.2	4.20.8	x	x		on by default
WRT54G v1.0	2.09.1	x	x		on by default
WRT54G v1.0	4.70.6	x	x		on by default

For the WRT54GS the bug was fixed in firmware 4.71.1.

ZyXEL

name	firmware	1	2	3	comments
P-335WT	V3.60(J0.3)	x	x		off by default

ZyXEL is aware of the issue, but because UPnP is turned off by default they are not treating it as an urgent bug. It will be fixed in a future version along with other bugs.

Edimax

name	firmware	1	2	3	comments
BR-6104K	3.21	x	x	x	off by default

Previous versions of the firmware are also vulnerable, but I have not tested them. As I write this I am corresponding with Edimax to try to get this issue finally fixed. It was reported to them via various channels about a week before the bug was disclosed, but there was no response initially and I had to try really hard to get them to notice it. To top it off, an unofficial response from one of their support people said he did not see it as a big threat, because UPnP is turned off by default and 90% of the people he mailed with and talked to on the phone had not enabled it later on and that the people who know how to turn it on would know about the risks involved. I did not bother to try and explain ``remote code execution'' to him.

Sitecom

name	firmware	1	2	3	comments
WL-153	1.31	x	x	x	off by default

Sitecom reacted very fast to my report. They have privately sent me new firmware, which solved hacks 2 and 3 and which will be made public soon.

AVM

name	firmware	1	2	3	comments
Fritz!Box Fon WLAN 7050	14.03.91	x	x		off by default

On the Fritz!Box Fon WLAN 7050 UPnP discovery is turned on, but control is turned off by default. AVM does not use one of the Open Source IGD implementations but uses its own. The first hack does not work for all ports. There are special firewall rules on the Fritz!Box that rule out forwards to internal Windows file and printer servers. According to AVM the same firmware is used on all Fritz!Box devices.

AVM has stated that they are very much aware of the problems in UPnP and that they will add routing rules in the new Fritz!Box firmware to disallow this from happening. This firmware should be released within the next few months.

Links

http://www.upnp.org/
http://www.upnp-ic.org/

Finding JTAG

von Hunz <hunz@hunz.org>

JTAG steht für Joint Test Action Group, ein Verfahren mit dem in einer bestückten Schaltung verifiziert werden kann, ob alle Verbindungen ordnungsgemäß verlötet wurden.

Das ist bei ICs nützlich, die keine sichtbaren Pins an der Außenseite, sondern ein Feld von Lötpunkten an der Unterseite haben. Bei diesen Ball Grid Array ICs ist es nicht mehr möglich, alle Verbindungen ohne teure optische Instrumente visuell zu überprüfen.

JTAG erlaubt, die Verbindungen über vier Testpins zu prüfen. An jedem Pin kann ein Low- oder Hi-Pegel angelegt oder der anliegende Wert gemessen werden. Dadurch kann in der Schaltung via JTAG auf Bausteine wie Flash ROMs lesend oder schreibend zugegriffen werden. Ein JTAG-Anschluß auf einer Platine kann mehrere Chips gleichzeitig ansprechen. Die JTAG-Interfaces der einzelnen Chips werden dabei verkettet – man spricht von der JTAG-chain.

JTAG wurde später von Herstellern zu unterschiedlichen Debuggingschnittstellen erweitert. Im laufenden Betrieb können u.a. Speicher und Register gelesen und beschrieben werden. Damit steht dem Auslesen und Modifizieren der Firmware nicht mehr viel im Weg. Zunächst stellt sich die Frage, wie man die vier Testpins lokalisieren kann. Je nach Gerät können unterschiedlich viele Pins divers angeordnet sein. Der Blackberry auf Seite 2 hat z.B. etwa 30 Pins, also `30*29*28*27=657720` mögliche Kombinationen. Diese Zahl weckt Automatisierungsgelüste.

Die Anschlüsse eines JTAG heißen *TCK*, *TMS*, *TDI* und *TDO*. Es besteht aus seriellem Interface und Statemachine, in der man mittels *TMS* navigiert. Daten gelangen via *TDI* in ein Schieberegister, an dessen Ende *TDO* angeschlossen ist. Den Takt macht *TCK*. Bei mehreren Chips in einer Kette sind *TMS* und *TCK* parallel verdrahtet. *TDO* eines Chips ist mit *TDI* seines Nachfolgers verbunden. Ein großes setzt sich aus den kleineren Schieberegistern einzelner Chips zusammen.

Eine bestimmte *TMS*-Sequenz bringt die Statemachine (siehe Wiki) in den Shift-*IR*- oder Shift-*DR*-Zustand, in dem das *IR* oder ein *DR* zwischen *TDI* und *TDO* gelegt werden kann. Während *DR*s unterschiedliche Länge haben, ist die des *IR* pro Chip konstant. Die Sequenz ist vom Zustand der Statemachine abhängig, zum Reset gibt es einen optionalen fünften Pin: *nTRST*. Alternativ gelangt man aus jedem Zustand mit fünf Takten *TMS=1* dorthin.

Ein über *TDI* in das Register geschobenes Bit erhält man an *TDO* wieder, sobald es durch das Register geshiftet wurde. Die nötige Anzahl an Takten entspricht der Länge des Registers in Bits +1. Man kann also ein Muster nach *TDI* hineinschieben, welches nach der entsprechenden Anzahl an Takten wieder aus *TDO* herausgeschoben wird. Von IC zu IC ist die Länge des Instructionregisters aber unterschiedlich, also für das vorliegende Gerät nicht bekannt. Da auch mehrere Chips in derselben JTAG-chain sein können, muß die Anzahl an Takten entsprechend großzügig gewählt werden. Für zwei ICs in einer Kette sollten 100 Takte ausreichen.

Um zu testen, ob die vorliegende Kombination aus *TCK*, *TMS* und *TDI* korrekt und welcher Pin *TDO* ist, wird im Shift-*IR*-Zustand beispielsweise 0x23 zwanzig mal nach *TDI* geschoben. Findet man das Muster auf einem anderen Pin wieder, stehen die Chancen nicht schlecht, daß dieser Pin *TDO* ist und die Kombination korrekt. Zur Sicherheit kann man das Muster 21-mal nach *TDI* schieben. Dann sollte sich das Muster an *TDO* einmal mehr wiederfinden lassen.

Genauere Informationen, Mitmachseiten und die derzeitige Hard- und Softwareimplementierung finden sich im Wiki des Augsburger Chaostreffs: *http://www.c3a.de/wiki/index.php/JTAG_Finder*

Hacktivismus fokussieren

von Sandro Gaycken <sandro.gaycken@iwt.uni-bielefeld.de>

Der bisherige, traditionelle Hacktivismus ist auf dem letzten Congress rechtens als ineffektiv ausgewiesen worden. Dazu wurden auch einige konkrete Ursachen angegeben, wie zum Beispiel der Verlust von Aktivisten an die „dunkle Seite" und die Ineffizienz von Szenepamphleten. Was mir aber fehlte, war eine systematischere, pragmatische Sichtweise. Denn der Mißerfolg scheint mir vor allem grundlegende Ursachen zu haben und weniger auf spezifischen Detailgründen zu beruhen.

Problemidentifikation

Das Hauptproblem ist, daß die Öffentlichkeit nicht in einem Maße erreicht wurde, das öffentliche Aktivität erzeugt hätte, und sicher wurden hier die Szenepamphlete schon ganz richtig identifiziert. Aber das ist, denke ich, nur ein Problem innerhalb einer Gruppe grundlegender Probleme, die insgesamt einen effektiven Kontakt zur Öffentlichkeit verhindert haben. Ein gutes Indiz für diesen schlechten Kontakt ist bereits die öffentliche Wahrnehmung des Clubs als obskurer und verschwörerischer Haufen, von dem keiner so recht weiß, was der eigentlich macht. Natürlich ist hier die Innenwahrnehmung völlig anders, aber aus der Außenwahrnehmung kann definitiv dieses Bild berichtet werden. Ich will hier also einmal grundlegend versuchen, die Ursachen für den Mangel an Öffentlichkeitskontakt zu identifizieren und ein paar Lösungswege vorzuschlagen.

In Bezug auf den Mangel halte ich vor allem drei Problembereiche für verantwortlich:

1. Mangel an inhaltlicher Prägnanz: Das Thema Datenschutz wird wenig wahrgenommen und meist nicht als unmittelbar bedrohlich empfunden. Viele Themen werden sogar als ambivalent aufgefaßt.

2. Schlechte Präsenz: Die bisherige Hauptlinie des Clubs war sachliche Aufklärung über das Netz, die Datenschleuder und gelegentliche Presseauftritte. Allerdings war hier der Output generell gering, fand meist unter den üblichen Verdächtigen in bereits esoterischem Jargon statt und war wenig öffentlichkeitswirksam (längere und mit Zeigefingermentalität geschriebene technische Abhandlungen sind nicht gerade bekannt dafür, daß sie Menschen oder sensationsfixierte Medien in größere Erregung versetzen).

3. Mangel an Angeboten: Der Öffentlichkeit werden nur wenig Mittel zur Verfügung gestellt, um sich selbst zu engagieren. Es gibt keine Konzepte zur aktiven Organisation von Spenden, Abstimmungen, Demonstrationen, Grundsatzklagen etc.

Zusammenfassend kann man also sagen, daß die Themen des Clubs inhaltlich wenig, verzerrt und ambivalent wahrgenommen werden, sie werden vom Club aus methodisch höchst ineffektiv geliefert, und sie lassen eventuell einmal aktivierte Menschen ins Leere laufen, da keine Angebote für weiteres Engagement geliefert werden. Das ist offensichtlich die Grundproblemlage des Aktivismus des Clubs, und sie ist inzwischen stark in den Kommunikations- und Aktivitätsgewohnheiten stabilisiert: es hilft eben wenig, daß die Clubabende weitestgehend daraus bestehen, rumzusitzen, zu surfen, ab und zu mal heimlich was zu hacken und sich ansonsten gegenseitig paranoid zu versichern, wie schlecht alles ist.

Was also kann geändert werden? Ich will einige Ideen entlang der skizzierten Problembereiche entwickeln. Zuerst also zur inhaltlichen Prägnanz.

Prägnanz

Hier gibt es klare Mängel an der Wahrnehmung der Dringlichkeit des Themas Datenschutz. Sporadische Hinweise etwa darauf, daß man ja vielleicht nicht gefilmt werden möchte, liefern auch einfach keinen unmittelbar bedrohlichen Konflikt.

Die Gegenargumente sind ja bekannt. Überspitzt: wer braucht schon Privatsphäre außer Kinderschändern und Betrügern? Hier muß allerdings nicht resigniert werden, denn es gibt ja einen grundlegenden Konflikt mit klarer Prägnanz: es geht um demokratische Werte. Das muß allerdings auch grundlegender präsentiert werden. Es muß hier die allgemeine Bedrohung deutlicher herausgestellt werden, indem man einen zentralen Fokus darauf herstellt.

Eine geeignete Möglichkeit der inhaltlichen Fokussierung besteht meiner Meinung nach in dem technikphilosophischen Begriff der Macht-Medialisierung. Der Begriff spiegelt eine These, die genau das ausdrückt, worum es uns geht. Macht-Medialisierung beschreibt einen Prozeß, in dem Machtbedürfnisse in Technologien materialisiert werden. Ein Beispiel ist das Machtbedürfnis der Kontrolle durch Information, das sich in Überwachungstechnologien, dem ePass und im Data Mining medialisiert hat.

Drei aus politischer Sicht entscheidende Elemente an Macht-Medialisierungen sind dabei, daß sie nicht demokratischen Prozessen unterliegen (die Entscheidungen darüber werden nicht öffentlich getroffen), daß sie Machtmechanismen in Sachzwänge umformen (jeder muß seine biometrischen Daten abgeben, wenn er einen Pass will) und daß sie leicht totalitaristisch mißbrauchbar sind (wenn sie nicht ohnehin schon totalitaristische Züge tragen).

Und an dieser Stelle hat man bereits ein enormes inhaltliches Konfliktpotential aus einem einzigen Fokus. Denn das Prinzip der Kontrolle durch Information ist radikal antidemokratisch, antirechtsstaatlich und spottet dem humanistischen Menschenbild. Im staatlichen Kontrollinteresse basiert es auf dem Gedanken, daß jeder Mensch prinzipiell ein Verbrecher ist, denn warum sonst sollte man Fingerabdrücke von allen Bürgern nehmen. Damit widerspricht der Staat aber inhaltlich dem Gedanken des Rechtsstaats, indem er nicht mehr von der prinzipiellen Unschuld ohne Gegenbeweis ausgeht, sondern vom Gegenteil. Und er widerspricht dem Gründungsgedanken der Demokratie, daß Menschen frei sind und selbst über ihr Leben entscheiden, indem er sie technisch-methodisch in dieser Freiheit überwacht und einschränkt.

Dies kann schlicht als Grundmißtrauen gegen die Freiheit der Bürger angeklagt werden. Das allerdings ist gerade ein Grundmißtrauen der Demokratie gegen ihre eigene Grundlage. Hinzu kommt nun noch das kapitalistische Kontrollinteresse, das auf dem Grundglauben an die völlige Manipulierbarkeit der Menschen durch „Marketing“ basiert und hier ebenfalls dem Bild vom freien Menschen spottet.

Da dieses destruktive und zweifelsfrei antidemokratische Machtprinzip jetzt in Überwachungstechnologien, ePass und Data Mining medialisiert ist, muß man sich – denn es ist demokratische Pflicht, die Demokratie zu verteidigen – gegen diese Technologien zur Wehr

setzen. Hinzu kommt das Problem, daß Macht-Medialisierungen demokratischen Prozessen nicht zugänglich sind. Es gibt keine öffentlichen Abstimmungen oder direkten Möglichkeiten zur politischen Gegenwehr gegen diese Technologien.

Wir sind also umgeben von Technologien, die direkt Ausdruck und Mittel antidemokratischer und unmenschlicher Machtinteressen sind, ohne daß wir eine Möglichkeit des demokratischen Einflusses darauf hätten. Dieser Grundkonflikt ist natürlich auch als Hintergrund unserer Themen irgendwie bekannt, aber er muß eben stärker und fokussierter in den Vordergrund gerückt werden und sollte meiner Meinung nach die eher ungefährlichen Schlagworte „Privatsphäre“ und „Datenschutz“ ersetzen.

Natürlich muß noch mehr inhaltliche Bearbeitung stattfinden, propagandistische Arbeit sozusagen, um den Grundkonflikt wirklich prägnant in Formeln zu schmieden, etwa wie „Kontrolle ausschalten, Demokratie einschalten“ oder so. Aber nur mit dieser inhaltlichen Klärung und Stärkung hat man überhaupt eine valide Substanz zum Kämpfen in der Hand.

Präsenz

Nach der inhaltlichen Fokussierung folgt der richtige Auftritt. Ein Blick auf die schlechte Präsenz und zuerst auf die Medienwirksamkeit.

Wie kann man in die Massenmedien gelangen? Hier kann die bisherige Strategie des sachlich-ruhigen Aufklärens eben nicht mehr alleinig verfolgt werden, denn die wurde ja legitim als eine Ursache des Mißerfolgs des Aktivismus identifiziert. Es braucht vielmehr den Superlativ-Effekt: Sensationen müssen inszeniert werden.

Das Problem dabei ist, wie man aus der Reaktion eines Datenschützers auf eine Technologie eine solche Sensation macht. Ein Vorschlag von Rop und Frank war ja der Spaß-Guerilla-Aktionismus (vgl. „We lost the war“ auf dem 22C3). Allerdings wird es hier vielleicht schwierig sein, den nötigen inhaltlichen Kontakt zur Problematik der Technik herzustellen.

Ich will deshalb erst noch eine neue Art des Technik-Aktivismus als medienwirksame und speziell für Technik geeignete Methodik vorschlagen. Sie ergibt sich aus einer einfachen Rechnung. Wenn nämlich bisher das sanfte Demonstrieren nicht gereicht hat, um die nötige Aufmerksamkeit zu erreichen, sollte man vielleicht einfach den Maßstab daran ändern.

Und exakt diese Maßstabsänderung hat jetzt im Rahmen von Technik einen eigenen Begriff: Sabotage. Und Sabotage ist für Technik-Aktivismus ein ausgezeichnetes Mittel. Denn im Gegensatz zum normalen Zweck von politischer Sabotage, demonstrativ Mittel zu blockieren, etwa indem man Haken auf Zugstromleitungen wirft bei Castor-Demonstrationen, schaltet im Fall von Technik-Aktivismus Sabotage auch konkret den Gegenstand des Aktivismus aus. Man hat den Demonstrationseffekt gleich gemeinsam mit dem damit angestrebten Resultat. Nicht nur Mittel werden blockiert, auch das konkrete Endziel wird gleichzeitig erreicht, denn die technischen Mittel sind ja unser Ziel.

Der Vorteil dieser Fügung ist, daß Sabotage in unserem Fall ungleich mächtiger ist. Dabei sind verschiedene Formen der Arbeit mit Sabotage denkbar. Zum einen ist die öffentliche Ausgabe von Anleitungen (oder Programmen) zur Sabotage von Kontrolltechnologien mit dem öffentlichen Aufruf zur aktiven Sabotage denkbar – sicherlich eine medienwirksame Aktion und gut als Kampagne lancierbar, wie oben schon erwähnt etwa als „Kontrolle ausschalten, Demokratie einschalten“.

Dann kann man auch in Large-Scale-Operationen selbst Sabotageakte durchführen, etwa in lokal organisierten Gruppen. Man könnte etwa versuchen, Data-Miner mit sinnlosen Informationen zu ruinieren, öffentlich Biometriedaten der Bundesregierung zu hacken und im großen Umfang zu vernichten, alle Schufa-Einträge zu löschen, die auch einwandfrei als Macht-Medialisierung gelten (das wäre übrigens nachgerade eine Heldentat für die zu Großteilen verschufate Öffentlichkeit...) oder man geht öffentlich im Beisein der Presse in Gruppen mit Geräten durch Einkaufspassagen und tötet RFID-Chips oder legt ePässe lahm.

Alle Sabotageakte können anonym stattfinden. Wichtig ist dabei aber, daß man sich eindeutig auf den politischen Hintergrund bezieht, etwa durch Pressemitteilungen oder durch den persönlichen, anonymen, aber inhaltlichen Bezug auf eine größere, übergreifende Kampagne.

Natürlich sind viele dieser Ideen illegal und, wenn man sie eben nicht anonym, sondern vielleicht als Gruppe oder Kampagne öffentlich unternimmt, sicher mit Konsequenzen behaftet. Aber genau das ist ein entscheidender PR-Vorteil. Zum einen garantiert das eine länger dauernde Pressepräsenz, weiter wird diese auch inhaltlich stattfinden, da die Leute ja wissen wollen, warum man das gemacht hat, und man ist in der Verteidigungsposition, da die Anklagen ja von außen kommen. Mit geschickter PR kann man aus dieser Position ganz hervorragend Kampagnen entfalten, da man ja direkt demokratische Grundrechte verteidigt.

Sollten derartige nicht-anonyme Aktionen unternommen werden, muß allerdings vorher intensiv über alle Schritte Abstimmung mit einer auch für die Konsequenzen zur Verfügung stehenden Rechtsabteilung gehalten werden. Das „unrechtliche“ Verhalten muß in jedem Fall – auch bei anonymen Aktionen – sehr präzise sein, um die Anklage richtig zu lenken.

Mir scheint in dieser Richtung wirklich viel denkbar und wenn man sich auf die völlig richtige Grundeinstellung einläßt, daß man bereits illegal mit Kontrolltechnologien unterwandert wurde und man nur die Courage der Verteidigung seiner Grundrechte als Erster übernimmt, ist der vielleicht etwas radikal scheinende Schritt zur Sabotage auch absolut reinen Gewissens empfehlbar.

Aber auch andere Aktionen mit anderen Extensionen der Präsenz sind denkbar. Man kann etwa auch Infomaterial zu Datenschutz in Form von Postern, Präsentationen und Lehrfilmen produzieren, das an Schulen und Universitäten, eventuell sogar offiziell über das Bildungsministerium oder den VDI, ausgegeben werden kann.

Auch könnte man mehr Aktivisten in verschiedene, externe Veranstaltungen schicken oder vielleicht sogar mal einen Stand an einem verkaufsoffenen Samstag aufstellen und Info(- und Sabotage-)material verteilen, etwa über die Zahl der Überwachungen und gesammelten Daten pro Einkauf. Auf jeden Fall kann und muß die Präsenz des Clubs auf verschiedene Arten verbessert werden. Der Kontakt zur breiten Öffentlichkeit muß dauerhaft und bis zu einem knapp enervierenden Maß hergestellt werden und die bisher eher esoterische Kommunikation zwischen verschwörerischen Zirkeln im Netz, in den Clubs, den IT-Abteilungen, Informatikinstituten und auf Fachtreffen ablösen.

Angebot

Zuletzt widmen wir uns dem Angebot an Aktionsmöglichkeiten. Natürlich müssen die einmal durch den klaren Inhalt und die gute Präsenz aufgeschüttelten Menschen auch Möglichkeiten in die Hand bekommen, ihrem Unmut Luft zu machen und eine Änderung zu unterstützen.

Dafür gibt es wieder eine Vielzahl an Möglichkeiten. Eine Möglichkeit ist das Sammeln von Stimmen. So kann man etwa im Rahmen einer umfassenderen Kampagne Gesetzesänderungen konzipieren, die zum Beispiel eine Demokratisierung von Technologien anstreben und dafür Stimmen sammeln. Eine andere Möglichkeit ist das Sammeln von Geld. Banner auf Webseiten etwa können Spenden sammeln, welche die Produktion von Infomaterial ermöglichen oder gezielte, zum Beispiel eben mit

Sabotageakten lancierte Rechtsstreits und Kampagnen finanzieren. Und eine weitere Möglichkeit besteht, wie bereits erwähnt, darin, den Menschen die Bauanleitungen für Sabotagegeräte zu geben, mit denen sie einfach selbst ausschalten können, was sie stört: direkter geht's nicht.

Im Bereich Angebot muß auf jeden Fall noch viel mehr unternommen werden als bisher, denn hier sind Aktionen selten gewesen, und es fruchtet eben nicht, Menschen erst für eine Idee zu gewinnen, nur um sie dann damit ins Leere laufen zu lassen. Und da der Einzelne nicht aus dem Stehgreif wissen wird, wie er sich allein dagegen wehren kann, ist es eben unsere Aufgabe, dafür etwas bereitzustellen.

Das waren jetzt einige pragmatische und grundsätzliche Anmerkungen. Wie gesagt bin ich der Meinung, daß eher hier die Hauptquellen der Ineffektivität zu suchen sind als in Detailursachen. Der Club und das Thema Datenschutz stehen einfach nicht in der breiten Öffentlichkeit und ohne die breite Öffentlichkeit kann nichts verändert werden. Um den Kontakt stärker herzustellen, sollten mehr Aktionen und vor allem heterogene und sensationelle Aktionen stattfinden, die mehr Medienpräsenz garantieren.

Um mit gutem Beispiel voranzugehen, melde ich hiermit mein Interesse an der Gründung einer präzisen und elaborierten Kampagne gegen undemokratische Technologie an – mehr oder weniger unter dem obigen Motto „Kontrolle ausschalten, Demokratie einschalten". Den genauen Fokus können wir dann gemeinsam je nach unseren Möglichkeiten ausarbeiten.

Vor allem möchte ich mal untersuchen, ob und wie man gezielt Sabotage als politisches Mittel für Technik-Aktivismus einsetzen kann. Wenn die oder der eine oder andere Lust hat, da mitzumachen: bitte mich kontaktieren. Und keine Angst: wer nicht will, wird in nichts Illegales verwickelt. Trotzdem brauchen wir dabei vor allem Rechtsberatung – falls jemand einen guten und inhaltlich überzeugten Anwalt kennt. Auch würde ich gerne mit einer Gruppe arbeiten, die Infomaterial für Schulen und Universitäten produziert. Wenn sich da auch jemand interessiert, bitte melden.

Vulnerability Markets

What is the economic value of a zeroday exploit?

Rainer Böhme <rainer.boehme@inf.tu-dresden.de>,
Technische Universität Dresden • Institute for System Architecture

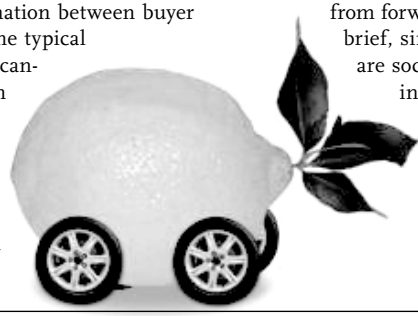
Vulnerabilities are errors in computer systems which can be exploited to breach security mechanisms. Such information can be very valuable as it decides about the success of attack or defense in computer networks. This essay introduces into the economic perspective on computer security and discusses the advantages and drawbacks of different concepts for vulnerability markets, where security-related information can be traded.

Economics and security

What's wrong with today's computer and network security? If you were asked by a journalist to answer this question in just one concise sentence, you'd probably talk tech gibberish. But there is a very elegant answer, which is compelling as well: it's all about people and their motivations – in brief, economics.

Researchers in both fields, computer security and economics, recently found that economic theory can well explain why computer security is so difficult despite the presence of sophisticated security technologies. For a good introduction read Ross Anderson's seminal article[2].

Before discussing the effects of vulnerability markets, let me sketch two examples to illustrate how the market fails in providing computer (or network) security. The first example refers to the supplyside for security technology. Its theoretical background is George Akerlof's famous lemon market problem [1]. Akerlof, meanwhile nobel laureate, studied the rules of a market with asymmetrical information between buyer and seller. For instance, the typical buyer of a second hand car cannot distinguish between good offers and bad ones (so-called "lemons"), because – unlike the seller – he does not know the true story of the car. So he is not willing to pay more than the price of a lemon. As a result, used cars in good condition will be undersupplied on the market. The same applies to computer security: security is not visible, it's a trust good. Since the buyer is unable to differentiate secure from insecure products apart, the market price drops to the level for insecure products. Hence, vendors have little incentive to develop sound security technology and rather prefer to invest in more visible gimmicks.



The second example targets to the demand-side of security. Its theoretical roots lie in the popular "tragedy of the commons", another economic theory published by Garrett Hardin [6]. Consider a computer network and the danger of worms and viruses. If the weakest node gets corrupted then the other nodes face a high risk of contagion and consequently face higher expected loss. Therefore the cost of security incidents is distributed among all nodes. On the other hand, if one node decides to invest in security, then all computers in the network benefit, because the now secure node is less likely to cause harm to others from forwarded malicious traffic. In brief, since both risk and benefits are socialized between all nodes, individuals lack the incentive to unilaterally invest in security. They prefer to remain "free riders" waiting for others to pay in their place (who'll never

do so, because of the same rationale; see [14] for a rigorous analysis).

To sum it all up, the lemon market suggests that vendors under-supply security to the market, whereas the tragedy of the commons tells us that users demand less security than appropriate. That's what we call a market failure. (There are many other approaches trying to tackle computer security problems with economic theory rather than with technology. Among them is the software liability discussion [13], which I omit for the sake of brevity.)

A short typology of vulnerability markets

There are two ways to fix a market failure. At first, regulation–which is least desirable as there are numerous examples where regulation makes things worse. Indeed, good regulation is really difficult since it often implies a trusted third party (TTP) as "social planner", whom to make incorruptible is costly, if not impossible. Second, one can respond to a market failure by establishing new markets with mechanisms that eventually feedback and thus mitigate the problems at their source. In this context, the following overview on vulnerability markets particularly addresses how well the different concepts are suited to solve the security market failure.

Bug challenges

Bug challenges are the simplest and oldest form of vulnerability markets, where the producer offers a monetary reward for reported bugs. There are some real-world examples for bug challenges. Most widely known is Donald E. Knuth's reward of initially 1.28 USD for each bug in his TEX typesetting system, which grows exponentially with the number of years the program is in use. Other examples include the RSA factoring challenge, or the shady SDMI challenge on digital audio watermarking [4].

Depending on the value of the reward, an adversary would have an incentive to report the bug instead of exploiting it or selling it on the black market. The vendor, in turn, can claim that the product is as secure as the amount alloted. This serves not only as a measurable quantity but also as a means to differentiate from competitors–as security becomes measurable, the lemon problem vanishes. Stuart Schechter's thesis [11] on vulnerability markets actually discusses bug challenges in great detail and he coined the term market price of vulnerability (MPV) as a metric for security strength.

Although including a monetary measure, I would not call this concept a genuine vulnerability market, because the underlying market mechanism suffers from a number of imperfections. Rather than resulting from a multi-lateral negotiation process, the market price is set by the demand side (i.e., the vendor, who demands vulnerability reports). Even if the vendor decides to increase the reward over time (and reset it after each report), the price quote is not a timely and reliable indicator for the true security of a product. Consider the case where two vulnerabilities are discovered at the same time. A rational agent would "sell" the first one and then wait with the second release until the reward has slowly climbed back to a worthwhile amount. In the meantime, the mechanism fails in aggregating the information about the security. Hence, prudent users would have to stop using the product in critical environments until the reward signals again the desired level of security. Obviously, this is not very realistic.

Bug auctions

Bug auctions offer a different theoretical framework for essentially the same concept as bug challenges. Andy Ozment [9] first formulated bug challenges in the terms of auction theory, in particular as a reverse Dutch auction, or an open first-price ascending auction. This allowed him to draw on a huge body of literature and thus add a number of efficiency enhancements to the original concept. However, the existence of this market type still depends on the initiative of the vendor. (2 Though not considered in Ozment's work, one can certainly conceive other types of bug auctions independent of the vendor: for example, offering new exploits on E-Bay (see http://archives.neohapsis.com/archives/ dailydave/2005-q2/0308.html). This sort of blackmailing the vendor and all honest users is definitively not a welfare maximizing strategy. And it does not provide any useful information on security strength when there is no vulnerability for sale.) On the one hand, this is an advantage because this market type can easily bootstrap–apart from the need of a trusted third party. On the other hand, the cooperation and financial commitment of the vendor makes it very difficult to use this kind of market mechanisms for small vendors and for open source software in general. (Mozilla Foundation's "Security Bug Bounty" program is a commendable exception: it rewards each remote vulnerability report with 500 USD.) Moreover, it is questionable whether the rewards offered will ever be high enough to provide an appropriate counterbalance to the assets at risk for software with large installation bases in critical environments, such as finance, healthcare, or government agencies. After all, even Professor Knuth opted for an upper limit to his exponential payoff function for bug hunters in TEX ...

Vulnerability brokers

Vulnerability brokers are often referred to as "vulnerability sharing circles". These clubs are built around independent organizations (mostly private companies) who offer money for new vulnerability reports, which they circulate within a closed group of subscribers to their security alert service. In the standard model, only „good guys" are allowed to join the club. The customer bases are said to consist of both vendors, who thus learn about bugs to fix, and corporate users, who want to protect their systems even before a patch becomes available. With annual subscription fees of more than ten times the reward for a vulnerability report, the business model seems so profitable that there are multiple players in the market: iDefense, TippingPoint, Digital Armaments, just to name a few.

If I were to classify CERT (Computer Emergency Response Team) in this typology, I would probably subsume it here. It also acts as a vulnerability broker, albeit on a non-profit basis. It does not pay any reward for reporting vulnerability information and disseminates that information for free. In a recent paper, Karthik Kannan and Rahul Telang [7] compare the social welfare of vulnerability markets (more precisely: vulnerability brokers) and the CERT approach. They conclude that CERT acting as a social planner always performs better than commercial brokers. (Note that the authors come from Carnegie Mellon University, which hosts the headquarters of CERT.)

Exploit derivatives

Exploit derivatives transfer the mechanism of binary options from finance to computer security. Instead of trading sensitive vulnerabili-

ty information directly, the market mechanism is build around contracts that pay out a defined sum in case of security events. For instance, consider a contract that pays its owner the sum of 100 EUR on, say, June 30th 2006 if there exists a remote root exploit against a precisely specified version of ssh on a defined platform. It is easy to issue this kind of contracts, since you would sell it as a bundle with the inverse contract that pays 100 EUR if the ssh program is not broken within the maturity. Then, different parties can trade the contracts on an electronic trading platform that matches bid and ask prices, settles the deals, and publishes the price quotes from the order book. The price is freely negotiable and reflects the probability of occurrence of the underlying event at any time. (5 For simplicity, I refrain from discussing interest rates, which can easily be handled by selling the bundles with a deduction equivalent to the return from a reference interest rate over the remaining maturity.) If ssh is considered as very secure by the market participants, then the first contract would be traded for, say, 1 EUR, whereas the second for 99 EUR.

The accuracy of the price information depends on the liquidity of the market, hence the number of participants. This market, however, attracts far more groups of participants than the previous market types: software users would demand contracts paying on breaches in order to hedge the risks they are exposed to due to their compute network. The same applies for insurance companies underwriting their customers' cyber-risks. Investors would buy the inverse contract to diversify their portfolios. Software vendors could demand contracts that pay if their software remains secure as a means to signal to their customers that thy trust their own system; or contracts that pay if their competitors' software breaks. One could even conceive that software vendors use exploit derivatives as part of their compensation schemes to give developer an incentive to secure programming.

Finally, security experts could use the market to capitalize effort in security analyses. If, after a code review, they consider a software as secure, they could buy contracts on the secure state at a higher rate than the market price. Otherwise they buy contracts that pay off on vulnerabilities and afterwards follow their preferred vulnerability disclosure strategy. As any interaction with the market influences the price, the quotes can be used as reliable indicators for security strength. Note that this concept does not require the cooperations of the vendor, and the number of different contracts referring to different pieces of software, versions, localizations, etc., is solely limited by demand.

The concept requires a trusted third party as well to test candidate exploits at the end of each contract and announce the resul. However, if the TTP is required to publish the exploit together with the announcement, it becomes verifyable and cannot cheat. The job can also be distributed to a number of TTPs. Hence, the assumptions about the TTP are much gentler in this scenario than in other market types.

Cyber-insurance

Cyber-insurance is among the oldest proposals for market mechanisms to overcome the security market failure (see [5, 8, 12, 13, 15]). The logic that cures the market failure goes as follows: end users demand insurance against financial losses from information security breaches and insurance companies sell this kind of coverage after a security audit. The premium is assumed to be adjusted by the individual risk, which depends on the IT systems in use and the security mechanisms in place. Therefore it would be costly to buy insurance coverage for less secure software. This gives users an incentive to invest in security technology. One would even raise the willingness to pay more for secure products if – in the long run – the total cost of ownership including insurance premiums is below the expenses for a less secure product.

However, despite the presence of potent insurance companies, there is surprisingly little supply for cyber-insurance contracts. One of the reasons for this undersupply is the fact that insurance companies hesitate in underwriting cyber-risks, because the losses from virus outbreaks and worms are highly correlated global-

ly. This concentration of risk is contrary to the insurance principle of portfolio balancing (see [3]). Apart from the fear of "cyber-hurricanes", there are other operational obstacles, such as the difficulty to substantiate claims, the intangible nature of cyber-assets, and unclear legal grounds.

Boon or bane?

We have seen that quite a number of possible instances for vulnerability markets is conceivable. So the question to answer is whether we are better off with or without them – frankly, shall we hype or fight them? It is obvious that any claim of a universal answer to this question cannot be serious, so the remainder of this essay tries to collect arguments for and against the markets, and in particular the pros and cons between different market types.

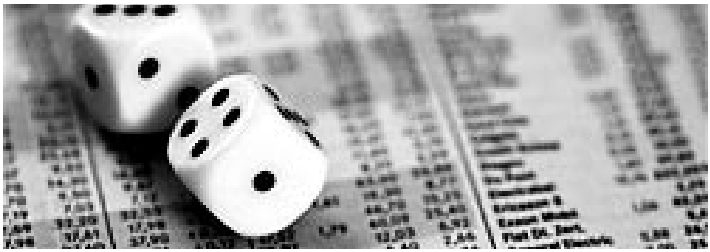
To judge the markets it is useful to define a set of criteria. An ideal vulnerability market fulfills three functions: first, the information function refers to the ability to use market prices as forward-looking indicators of security properties. This is important to counter the lemon effect. Second, the incentive function allows monetary compensation for security research and development. It motivates firms and individuals to give security a higher priority. Third, the risk balancing function means, that the market provides instruments to hedge against large information security risks. This is important to mitigate the financial impact of (occasional) security breaches, which may help firms to survive a virus attack rather than filing for bankruptcy with all its adverse social and economic consquences. Orthogonal to these functions, market efficiency is a criterion under which I subsume other desirable properties, such as low transaction costs, liquidity, transparency (public quotes, fair rules), and accountability (low counterparty risk). Table 1 compares the different types of vulnerability markets along the defined criteria.

Both bug challenges and bug auctions provide vulnerability hunters with an incentive to report and also give developers a motivation to take security more seriously. However, there is no possibility for risk balancing at all, and the information obtained from the market price is only a lower bound, which fails to be accurate when vulnerabilities are reported frequently. As to efficiency, the vendor has to bear most of the burden and the existence of a market depends on his cooperation. Vulnerability brokers (excluding CERT) do worse because they create questionable incentives (i.e., for bad boys to join the circle) and deliver no information to the public at all. It appears that exploit derivatives and cyber-insurance are both acceptable, with exploit derivatives having an advantage as timely indicator whereas cyber-insurance gets a deduction in efficiency due to the presumably high transaction costs. What's more, both concepts complement one another. Please note the limitations of this qualitative assessment, which should be regarded as a starting point for discussion and exchange of views.

There is also room for more general critiques on the market approach. One might question if vulnerability hunting actually leads to more secure products (see[10] for a discussion and evidence for vulnerability hunting), so why bother putting market incentives in place for something allegedly useless? Moreover, we all know that markets tend to err in the short term – but it's still very difficult to outpace existing markets in the long run. Therefore we need to assess the harm a "vulnerability market bubble" potentially causes, and weight it against the welfare gains from better information, more secure products, and the possibility to hedge information security risks. Finally, there remains to be written a chapter on conflicts of interest.

To conclude, we have seen that economic models can well explain the computer security dilemma and that vulnerability markets are a way to tackle the problem. However, there is not one "vulnerability market" but rather a family of different concepts. After regarding their individual mechanisms, it becomes evident that the market types close to reality, namely bug challenges and vulnerability brokers, are not the best possible solutions.

•



Back to the journalist's question at the beginning, how would you answer in, say, 20 years when computer security is so important that it has entirely melted into finance? You would probably mention the New York Stock Exchange having closed with a 5.23 % decline in the Standard & Poor's composite kernel hardness index. So it's only a matter of time when the next big kernel exploit hits the cyber-world . . .

The author gratefully acknowledges the valuable comments he received from Thorsten Holz and Gaurav Kataria.

Literature

[1] George A. Akerlof. The market for 'lemons': Quality, uncertainty and the market mechanism. Quarterly Journal of Economics, 84:488-500, 1970.

[2] Ross J. Anderson. Why information security is hard – an economic perspective, 2001. Online *http://www.cl.cam.ac.uk/~rja14/econsec.html*

[3] Rainer Böhme. Cyber-insurance revisited. In Workshop on the Economics of Information Security (WEIS), Cambridge, MA, 2005. Online *http://infosecon.net/workshop/pdf/15.pdf.*

[4] Scott Craver et al. Reading between the lines: Lessons from the SDMI challenge. In Proc. of the 10th USENIX Security Symposium, Washington, DC, 2001. USENIX Association. Online *http://www.usenix.org/events/sec01/craver.pdf*.

[5] Lawrence A. Gordon, Martin P. Loeb, and Tashfeen Sohail. A framework for using insurance for cyberrisk management. Communications of the ACM, 46(3):81-85, 2003.

[6] Garrett Hardin. The tragedy of the commons. Science, 162:1243-1248, 1968.

[7] Karthik Kannan and Rahul Telang. An economic analysis of markets for software vulnerabilities. In Workshop of Economics and Information Security (WEIS), Minneapolis, MN, 2004. Online *http:// www.dtc.umn.edu/weis2004/kannan-telang.pdf*.

[8] Jay P. Kesan, Ruperto P. Majuca, and William J. Yurcik. The economic case for cyberinsurance. In Workshop on the Economics of Information Security (WEIS), Cambridge, MA, 2005. Online *http://infosecon.net/workshop/pdf/42.pdf*.

[9] Andy Ozment. Bug auctions: Vulnerability markets reconsidered. In Workshop of Economics and Information Security (WEIS), Minneapolis, MN, 2004. Online *http://www.dtc.umn.edu/weis2004/ozment.pdf*.

[10] Andy Ozment. The likelihood of vulnerability rediscovery and the social utility of vulnerability hunting. In Workshop on the Economics of Information Security (WEIS), Cambridge, MA, 2005. Online *http://infosecon.net/workshop/pdf/10.pdf*.

[11] Stuart E. Schechter. Computer Security Strength & Risk: A Quantitative Approach. PhD thesis, Harvard University, Cambridge, MA, 2004.

[12] Bruce Schneier. Hacking the business climate for network security. IEEE Computer, pages 87-89, April 2004.

[13] Hal R. Varian. Managing online security risks. New York Times, June 1st, 2000. Online *http://www.nytimes.com/library/financial/columns/060100econscene.html*.

[14] Hal R. Varian. System reliability and free riding. In Workshop on Economics and Information Security (WEIS), Berkeley, CA, 2002. Online *http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/*.

[15] William Yurcik and David Doss. Cyberinsurance: A market solution to the internet security market failure. In Workshop on Economics and Information Security (WEIS), Berkeley, CA, 2002. Online *http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/*.

Chaosradio Podcasting

von Tim Pritlove <tim@ccc.de>

Seit November 2005 ist das Chaosradio auch als Podcast zu empfangen. Dem seit über 10 Jahren laufenden Format wurde dazu noch ein reiner Podcast unter dem Namen Chaosradio Express hinzugefügt. Podcasting ändert die Medienlandschaft – und Chaosradio.

Der gemeine Nerd reagiert mithin genervt, wenn man ihn mit dem Hype der Woche konfrontiert, und in gewisser Hinsicht ist dieser Selbstschutz verständlich, um sich nicht von den wirklich wichtigen Dingen ablenken zu lassen. Doch hin und wieder ist der aktuelle Trend auch ein wichtiger Baustein für eine digitale Welt, wie wir sie uns wünschen. Podcasting ist einer davon.

Als das Web erfunden wurde, lautete die ursprüngliche Vision, daß hier jeder lesen und publizieren könne. Es dauerte einige Jahre, bis das Web auch den zweiten Teil dieser Verheißung liefern konnte. In den letzten Jahren wurde das Veröffentlichen der grundlegenden Datenarten (Text, Ton und Bild) Schritt für Schritt für jedermann beherrschbar; in Form von Weblogs, Podcasts und Video Podcasts.

Man mag zu Recht einwenden, daß das reine Publizieren dieser Inhalte schon länger möglich gewesen ist, im Prinzip von Anfang an. Doch waren eine zu geringe Bandbreite, mangelhafte oder ganz fehlende Werkzeuge und ein Formatwirrwarr lange Zeit hinderlich. Was aber noch viel wichtiger wog: es fehlte ein akzeptierter und den modernen Konsumgewohnheiten entgegenkommender Standard, um die Inhalte zu beziehen. Weblogs haben hier mit RSS eine populäre und brauchbar skalierende Lösung gefunden.

Das Abonnement

Während das wilde Herumklicken im Netz seinen Reiz hat, ist es für einen stukturierten Bezug von Informationen ungeeignet. Dinge lassen sich im Netz schnell finden, aber um so schwieriger wiederfinden. Hat man einmal eine aufschlußreiche Quelle gefunden, die auch in Zukunft Aufschlußreiches verspricht, möchte man “dranbleiben”. Die Subkription der Inhalte liegt nahe, und in den Jahren wurde viel mit Push- und Pull-Methoden experimentiert. Verschiedene Lösungen kamen und gingen.

Die simple Struktur von Weblogs führte schließlich zur Entwicklung von RSS, welches sich letztlich als “good enough” und “simple

enough" herausstellte, um breiten Anklang zu finden. Die schiere Zahl von Blogs (ca. 35 Millionen, wenn man „Technorati" Glauben schenken darf) und die hohe Beteiligung der Leser in Form von Kommentaren und Trackbacks zeugt von dieser Akzeptanz.

1994 darf als das Jahr gelten, in dem Blogs sich als führende Kommunikationsform für Textinhalte etabliert haben. In der Folge wurde RSS als technische Basis schnell durch Browser und spezialisierte Leseprogramme zum De-Facto-Standard für Text Broadcasting (interessanterweise wird der "Push" auf Basis einer Pull-Technologie durchgeführt).

Nach einem eine Weile währenden religiösen Krieg in der RSS-Szene konnten sich die Pragmatiker gegen die Anhänger des semantischen Webs technisch durchsetzen. Spricht man heute von RSS, meint man RSS 2.0. Mit Atom 1.0 gibt es auch schon eine W3C-Variante zur mittel- und langfristigen Migration. For the time being ist RSS allerdings das Maß der Dinge.

Podcasting

Die Idee, RSS als Distributionsmedium für große Mediendateien zu verwenden, fand schon recht früh Einzug in den RSS-Spezifikationen. Eine "Enclosure" ist nicht viel mehr als ein Link auf die entsprechende Datei, der dem Empfänger die Möglichkeit bietet, diese ggf. automatisch herunterladen zu lassen. Im Prinzip war die Vision der Verbreitung von Radio- und Fernsehsendungen in Form einfacher Dateien auf Abonnementbasis damit bereits auf dem Tisch. Es dauerte aber eine Weile, bis diese Methode auch Anwendung erfuhr und auf breites Interesse stieß.

Die Gründe dafür sind vielfältig. Zunächst war es nötig, daß RSS selbst die nötige Akzeptanz fand. Internet Flatrates und die Verbreitung portabler Abspielgeräte legten dafür in der Folge die Grundlage. Mit der Veröffentlichung des ersten dedizierten Podcast-Clients (iPodder), der die automatisierte Übermittlung der Inhalte von der Quelle (dem Webserver) zum portablen Abspielgerät sicherstellte, war das System komplett. Nun konnten selbst produzierte Sendungen mit dem Komfort von Radiosendern mithalten und boten darüberhinaus durch die Möglichkeit des zeitversetzen Anhörens zusätzliche Vorteile. Das Abo-Prinzip von RSS tat sein Übriges, den heutigen Bedarf nach individualisiertem Medienkonsum zu bedienen. 2005 war schließlich das Jahr, in dem Podcasts ihren Durchbruch feiern durften.

Chaosradio

Mit dem Format Chaosradio hatte der Chaos Computer Club schon seit Jahren ein alternatives Sendeformat, das dank der Unterstützung durch den Sender Fritz im Raum Berlin/Brandenburg per UKW und via Satellit in ganz Mitteleuropa zu empfangen war. Schon früh haben wir zusätzlich den Live-Empfang durch die Einrichtung eigener Streaming Server im Internet ermöglicht; Aufzeichnungen der Sendungen fanden stets ihren Weg ins Netz und erfreuten sich dort großer Nachfrage.

Podcasting war für Chaosradio ein naheliegender Technologiesprung und im November 1995 war es soweit, daß die Sendungen nun auch via RSS abonniert werden konnten. Binnen kürzester Zeit wurde das Angebot von tausenden Hörern angenommen.

Die Bindung an die Hörer wurde dadurch deutlich verstärkt, zumal der notwendige Aufwand, den Aufzeichnungen der Sendungen habhaft zu werden, deutlich sank. Die Reichweite von Chaosradio wurde dadurch schlagartig erweitert, und man darf sich fragen, ob die Hörerquote aus dem Internet nicht sogar die der klassischen Broadcast-Technologien spürbar übersteigt.

Chaosradio Express

Podcasting ist zunächst nur eine Technologie, die aber wie soviele neue Kommunikationsformen in Kürze auch ihre eigene Kommunkationskultur hervorbrachte. Ein Podcast ist im Vergleich zum klassischen Radio spürbar persönlicher und interaktiver. Die Einbeziehung von Feedback der Hörer, ein grundsätzlich entspannterer Stil und die hohe Experimentier-

freude der Podcaster war von Anfang deutlich wahrnehmbar und führte binnen kürzester Zeit zu einer kulturellen Vielfalt, die man im Radio schon immer sträflich vermißte.

Dieses Maß an Interaktivität ließ sich auch im Chaosradio immer schwer erreichen. Gebunden durch die vorgegebene Sendedauer (3 Stunden) und Sendefrequenz (einmal im Monat) war diese Interaktivität nicht so ohne weiteres herstellbar. Dazu kam, daß Chaosradio nur wenige feste Teammitglieder hat und die Besetzung von Thema zu Thema wechselte. Darüber hinaus gibt auch das Sendeformat "Blue Moon" - der tägliche "Talk Radio" Slot von Fritz - in gewisser Hinsicht einen Rahmen vor. Zwar ist die Einblendung von stündlichen Nachrichten, Radio Jingles und das Ziel, die Hörer stets zum Anrufen in der Sendung zu motivieren, an sich nichts Dramatisches. Doch eignen sich nicht immer alle Themen in dem Maße zum Dialog mit Hörern, wie es vielleicht wünschenswert wäre. Es war klar, daß sich Chaosradio selbst durch den Einsatz von Podcasting nicht stark weiterentwickeln würde.

Das brachte mich auf die Idee, dem bekannten Format ein zusätzliches, auf die Möglichkeiten des Podcastings zugeschnittenes Programm hinzuzufügen, daß in einem höheren Maße das Feedback der Hörer einbindet und seine Themen noch flexibler wählen kann, da auch der Zwang zum Dreistünder entfällt. Chaosradio Express war geboren und hat in rund einem halben Jahr etwa 24 Sendungen produziert.

It's Feedback Time

Die Rückmeldung auf die Einführung eines reinen Podcasts waren reichhaltig. Binnen eines halben Jahres hat das Chaosradio-Team mehr E-Mail erhalten, als in den letzten zehn Jahren zuvor, und die Bereitschaft, die Themen durch Kommentare und Vorschläge mitzugestalten, ist deutlich zu erkennen.

Das Aufkommen des Phänomens des Audiokommentars gibt dem Ganzen nun noch eine neue Ausrichtung. Durch die kürzeren Publikationszyklen (Chaosradio Express versucht, ca. eine Epsiode pro Woche zu veröffentlichen) kann man Themen über einen längeren Zeitraum von Sendung zu Sendung tragen und quasi einen Dialog eröffnen, der aber immer noch durch die Moderation getragen ist. Es ist absehbar, daß diese Diskussionsform weiter an Popularität gewinnt und sich am Ende vielleicht zu einer Art Audio-Usenet entwickelt. Wo man bislang nur dem geschriebenen Wort eine Chance bot, wird dann mit klaren, gesprochenen Worten diskutiert.

Hörer sind keine Leser

Ein interessantes Phänomen des Podcastings ist, daß die Zielgruppe sich nur partiell mit der von textbasierten Medien wie reinen Weblogs überschneidet. Hörer sind keine Leser und umgekehrt. Natürlich gibt es auch hier den fortgeschrittenen Mediengeek, der sich an Quel-

len aller Art nicht sattlesen/hören/sehen kann, doch ist dies sicherlich nicht die Regel. Die einfache Erkenntnis ist, daß Podcasts eine neue Gruppe der Gesellschaft erschliessen, der das textlastige Internet bislang zu schwierig zu ergründen schien.

Dazu kommt die Qualität des gesprochenen Wortes, die gegenüber Text doch zahlreiche Vorteile bietet. Wer kennt sie nicht, die Flame Wars auf Mailinglisten, Foren und Kommentarzonen, die sich meist um Nichtigkeiten drehen und ihre Kraft aus Mißverständnissen ziehen – vorsätzlichen oder ungewollten. Hier verpufft viel Energie, die sich besser nutzen ließe.

Der Klang der Stimme erlaubt es, auf Smileys zu verzichten. Der Mensch ist in der Lage, Ironie und Gefühlslage ohne technische Hilfsmittel aus dem gesprochenen Wort herauszufiltern. Dies macht es einfacher, Einblick in Sachverhalte zu verschaffen, und birgt große Chancen, komplexe Themen in einer Kompaktheit zu vermitteln, wie es mit Text kaum machbar wäre. Dies gilt noch vielmehr für Interviews und Gesprächsituationen, in denen man sehr dynamisch hinterfragen, erklären und variieren kann. Einem solchen Gespräch eine halbe Stunde zu lauschen, erfordert zwar ein gewisses Zeitinvestiment, doch ist die Vorstellung, dem selben Gespräch in Form eines Transkript zu folgen, geradezu absurd. Nicht jeder hat die Gabe, wie ein professioneller Schauspieler einen Wortwechsel in geschriebener Form so zu erfassen, daß man danach noch weiß, welche Akteure sich in welcher Art geäußert haben. Wer glaubt, Podcasts würden zuviel Zeit kosten, sollte hier kurz innehalten – in vielen Situationen kann ein Podcast vielmehr als effektive Zeitersparnis dienen, vorausgesetzt, die Diskutanten sind in der Lage, ihr Wissen oder ihre Meinung auch klar zu formulieren. Dies gilt aber für Textkommunikation im gleichen (wenn nicht noch größeren) Maße auch.

Podcasten Sie!

Für eine Bewegung wie den Chaos Computer Club ist der Podcast ein starkes Instrument in der Unterstützung seiner Ziele. In den letzten Jahren haben sich Chaosradio-artige Projekte nur dort entwickelt, wo auch ein Zugriff auf UKW-Frequenzen bestand. Durch Podcasting fällt dieses Bedürfnis weg. Der technische Produktionsaufwand ist gering und der für die Publikation ebenfalls. Ideale Voraussetzungen für den Revolutionär von morgen.

Ich möchte Euch daher ermutigen, über Podcasts nachzudenken und es im Zweifel einfach mal zu versuchen. Trial and Error haben hier die gleiche Bedeutung, und es ist immer wichtiger, es versucht zu haben, als nur darüber nachzudenken. Das Müßte-Man-Mal-Syndrom ist des Aktivisten Feind auf allen Ebenen. Wer eine Stimme haben will, muß sie erheben, und nie war es einfacher als heute, dieses auch zu tun.

Setzen wir mal ein Wiki auf

von Philipp, Paul und Philip

Es ist noch ein wenig surreal, das Gefühl. Ich sitze hier tatsächlich im Metalab, und ich meine damit nicht "ich habe die Wikiseite offen und lese über die Visionen". Böse Zungen behaupteten ja, nach einem halben Jahr Wiki(-only) Aktivität ohne echte Aussicht auf Real-World-Implementierung, der Name sei gut gewählt: Meta.

Aber nun ist es soweit:

Hier in der Rathausstraße 6 des 1. Wiener Gemeindebezirkes, gleich hinter dem Rathaus und ein paar Gehminuten von der Uni Wien, ist ein leuchtend Loch in der Wand. 200 qm, wie die Wikiseite behauptet, "für meta-disziplinäre Magier und technisch kreative Enthusiasten".

Ja, Pathos laß nach, aber nach den ersten Blicken durch die verstreuten Reihen von Hackern, dem Ambiente, dem Schmuck an den Wänden geurteilt – vielleicht doch nicht so fern von der Realität, wie es sein könnte.

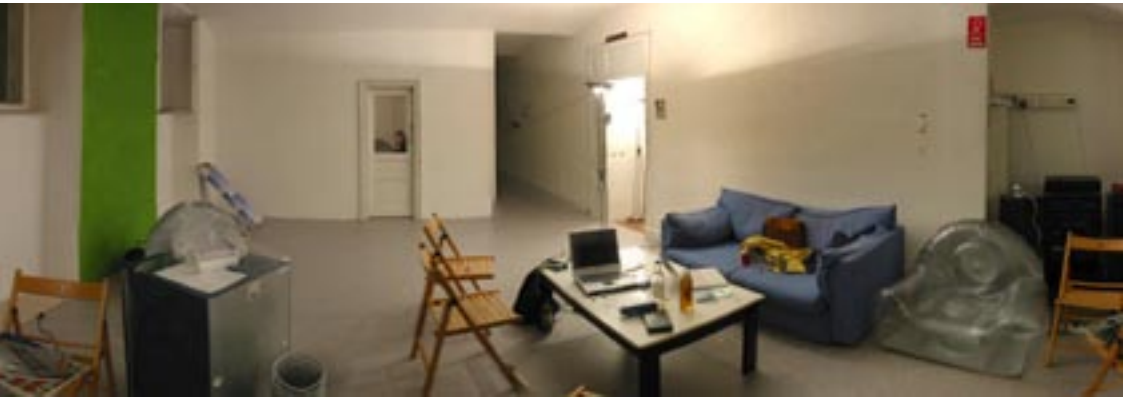
Vor mir sitzen Paul Böhm - manchen als typo von der Gruppe Teso bekannt - und Philipp Tiefenbacher alias wizard23. Jene zwei, die zu Recht von sich behaupten können, die erste Wikiimmobilie in Wien gegründet zu haben. Ihnen stelle ich, repräsentativ für die vielen Mitwirkenden, einige Fragen zum Werdegang und Selbstverständnis dieser Institution in spe.

Q: Was war die Motivation für die Gründung des Metalabs?

Philipp: Es hat's noch nicht gegeben. Aber es hat schon gefehlt.

Paul: Weil's in Wien bereits viele Leute gegeben hat, die coole Projekte gemacht haben, aber sich gegenseitig nicht kannten. Hauptsächlich hat da eigentlich der Platz gefehlt, und damit ist nicht das Beisl beim Stammtisch gemeint. Und natürlich waren wir neidisch auf gewisse andere Plätze in Europa, wo wir bereits die Erfahrung machten, daß Projekte von einem nicht virtuellen Treffpunkt profitieren.

Philipp: Ein Beispiel: Ich hab seit einigen Monaten einen Borland C Compiler gesucht, und hätte auch keinen gefunden. Meine alten Disketten kaputt, sonst auch nichts hilfreiches zu finden. Aber hier find ich plötzlich einen "Borland C++ in 21 Tagen" Band. Und einen Compiler. Und jetzt kann ich meine alten Sourcen wieder compilen...



Q: Wer hatte die ursprüngliche Idee zum Metalab? Und wann?

Paul: Wer ... es gab schon mehrfach Bestrebungen, in Österreich so etwas zu starten. Die Leute rund um die Chaos Nahe Gruppe Wien (CNGW) haben das auch schon versucht, waren aber anscheinend zu klein. Die Idee von Philipp und mir für ein Vorgängerprojekt gibts auf Wikiseiten seit zwei Jahren. Der jetzige Name und das jetzige Projekt ist vor einem Jahr bei einem Treffen von Funkfeuer entstanden, wo es um Ideenfindung zu so einer Location ging. Einen Monat später gab's dann ein initiales Treffen mit ca. 30 Leuten, von denen immer noch viele dabei sind, viele andere kamen später noch dazu. Der Vorstand etwa lernte sich auch erst durch reale Treffen kennen.

Q: Wieviel von der anfänglichen Vision hat den Weg zur Realität gefunden?

Philipp: Erstaunlich viel!

Paul: Es ist besser gelaufen als geglaubt, wir dachten, wir müßten viel kleiner starten. Aber wir haben jetzt auch viele Privatpersonen angesprochen, die überhaupt noch nicht von einer anderen Szene oder Gruppierung eingesammelt wurden.

Philipp: Ich bin sehr überrascht, daß es so läuft wie es läuft. Ich denke, dadurch daß das schon als rein virtueller Platz sehr gut funktioniert hat, war der Übergang in den realen Raum so reibungslos. Es kommt mir vor wie gelebte Open-Source-Kultur, aber aus mehr Bereichen als nur Computer*. Schön wo reinzukommen, wo ein Monkey Island Zitat nicht verständnisloses Schweigen auslöst.

Paul: Fragt sich nur, wie oft der durchschnittlicher Metalab Besucher Sex im Monat hat?

Philipp: Fragt sich bevor oder nachdem es das Metalab gab ...

Q: Welche Personen und Vereine haben maßgeblich beigetragen?

Philipp und Paul: Zuviele zum auflisten. Aber wirklich wichtig waren Funkfeuer für schnelles Netz, CNGW für das Easterhegg und die Mitarbeit, und viele, viele Einzelpersonen.

Q: Wie ist Euer Verhältnis zur CNGW, dem Wiener Erfakreis des CCC? War Euer Projekt nicht ursprünglich ein Ansinnen der CNGW?

Philipp: Öhh ...

Paul: Ääh ... wir zielen auf Infrastruktur ab. Wir fänden's wichtig, daß der CCC hier Projekte macht, und zum Beispiel camdome wieder aufleben läßt. Und natürlich auch, daß wir Leute anziehen, die vorher noch nichts mit dem CCC zu tun hatten. Wir sind keine CCC-Mitglieder, aber auf jeden Fall gerne im Dunstkreis zu finden. Aber bestimmt ist jetzt eine Neuausrichtung der CNGW nötig.

Q: Wieviel vom Vereinszweck der CNGW ist, nicht zuletzt durch die starke Personalunion, im Metalab aufgegangen?

Paul: Das Metalab ist per Vereinsstatut ein reiner Infrastrukturanbieter.

Q: Es stehen Kisten von Club Mate in Frucadekisten (österreichisches Erfrischungsgetränk, Anm.) herum, viele Elemente, Schmuck und Projekte erinnern an C-Base, FoeBuD und Konsorten. Weite Teile Eurer Identität scheinen also noch nach deutschen Vorbildern zu leben. Wie seht Ihr das?

Paul: Wir haben, um das Projekt umzusetzen, Kultur importiert. Kultur, die teilweise für uns normal ist. Aber es wird sicher eine große Herausforderung, unsere eigene Identität zu finden...

Philipp: ... aber das ist ein normaler Prozeß.

Q: 20EUR/Monat Mitgliedsbeitrag, 1600EUR/Monat Miete. Auch zusammen mit der Förderung der Stadt Wien scheint die Finanzierung lediglich mittelfristig gesichert zu sein. Wie gedenkt Ihr, Euch weiter zu finanzieren? Wie steht Ihr zu Leuten, die diesen Mitgliedsbeitrag nicht zahlen wollen oder können?

Philipp: Wenn Leute sich das nicht leisten können, gibt es vereinzelt die Möglichkeit, daß sie trotzdem kommen können.

Paul: In der C-Base liegt der Mitgliedsbeitrag auch bei 17 EUR. Hätten wir mit einer kleineren Location begonnen, wär's schwieriger gewesen, und hätte vielleicht nicht zur Verwirklichung geführt. Und diese Location bietet einiges für's Geld. Aber wir planen, es zu senken, wenn wir es uns leisten können.

Philipp: Wär die Location nicht so zentral gelegen, wär's nicht annähernd so lebendig wie im Moment, die Anforderungen sind also voll erfüllt. Die Einstiegsdroge muß leicht erreichbar sein.

Q: Wie seht Ihr den Wirkbereich des Metalab? Eher politisch oder technisch?

Philipp: Technisch.

Paul: Sozial, eher nicht politisch.

Q: Was sind die aktuellen Projekte, worüber freut Ihr Euch?

Philipp: Das Metaschild, mit 64 einzeln steuerbaren LEDs ... die Hardware ist schon fertig, wir basteln nur noch an der Software und den Algorithmen. Auf die Roboter freu ich mich, und zelluläre Automaten sind hier auch schon (weiter) entwickelt worden.

Paul: Diverse Softwareprojekte, darunter eine P2P-Filesharing-Applikation (quaffler), einige google-maps-Hacks, Spielereien mit GIS-Daten, und einige, die ich nicht nennen will, weil sie noch in Entwicklung sind.

Philipp: Und ein Einsteins "game of gravity" aka Gravitationsloch für Spendengelder.

Q: Was wollt Ihr den Leuten sonst noch sagen?

Paul: Das Metalab ist ja eigentlich nur Infrastruktur. Schaut vorbei, und bringt eure Projekte mit. Das Metalab lebt ja erst durch die Mitglieder und Projekte, die hier umgesetzt werden.

Philipp: Damit das Mögliche entsteht, muß immer wieder das Unmögliche versucht werden, das ist aber nicht von mir. Wir haben eine Menge anzubieten: Eine komplette Hardwarebastelwerkstatt mit u.a. Oszilloskop, Labornetzteil, Lötstation und allem, was man zum Roboterbasteln so braucht; sowie eine ausgerüstete Küche, eine coole Bibliothek, einen Wutzler und space invaders an der Wand.

Wann und Wo und Wie genau das mit dem Metalab ist, erfährt man im Metalab Wiki unter *http://www.metalab.at/*, das detaillierte Angaben zu Organisationsstruktur, Menschen und Zielen enthält, ebenso wie zu wichtigen Terminen und Projekten.

FIFA WM 1984™

von <Brud3r_H4ck@gmx.net>

Ich bin im IT-Betrieb eines deutschen Konzerns tätig und dabei u.a. für den Einkauf von IT-Services zuständig. Anfang April wurde ich nun von einem unserer Dienstleister zu einer Veranstaltung während der FIFA Fußball-Weltmeisterschaft Deutschland 2006™ eingeladen, um mir die Services, die dieses Unternehmen im Rahmen dieser Veranstaltung erbringt, einmal anzusehen.

Um an dieser Veranstaltung teilnehmen zu können, brauche ich lediglich einige Angaben zu meiner Person machen und mich mit der Datenschutzinformation der Abteilung Akkreditierung der FIFA Fußball-Weltmeisterschaft Deutschland 2006 einverstanden erklären. Ich bin nicht nur ein gesetzestreuer Staatsbürger, sondern auch papyrophil (sprich Papier liebend) und habe aufgrund dieser Eigenschaft die Dokumente vollständig gelesen.

Welche Informationen werden abgefragt?

Abgefragt werden zum einen Informationen, die sich auf das jeweilige „Event" beziehen wie „Event Name", „Event Funktion", „Registrierungsnummer" (in meinem Falle zudem „Rechnungsanschrift für Hotelkosten").

Zum anderen geht es um persönliche Angaben wie Nachname, Vorname, Geburtsort und -land, Geburtsdatum, Nationalität, vollständige Adresse, Bundesland und Ausweisnummer.

Mit meiner Unterschrift in dem Feld „Ich habe die Datenschutzerklärung gelesen und bin damit einverstanden" dürften meine Angaben schon ausreichen, um in/mit meinem Namen im erheblichen Maße für Unfug zu sorgen. Und damit meine ich mehr als nur den fingierten Erwerb einer Kaffeemaschine oder ein Jahres-Zeitschriften-Abo. Aus der Sicht eines alteingesessenen Paranoikers reichen diese Informationen aus, um eine Identität zu fälschen oder einer tatsächlich existierenden Person eine neue, andere, u.a. strafrechtlich relevante Vergangenheit zu geben (z.B. durch Fälschen eines Geständnisses). Aber ich schweife ein wenig ab.

Zuverlässigkeitsprüfung:

„Zu diesem Zweck [der Prüfung, ob Erkenntnisse vorliegen, die aus der Sicht der beteiligten Sicherheitsbehörden einer Zulassung zum Veranstaltungs-ort entgegen stehen] soll ein Auszug aus den mit dem Anmeldungsformular erhobenen Angaben (Nachname, Vorname, Geburtsname oder anderer Name, Geburtsdatum, Geburtsort, Geschlecht, Nationalität wie im Ausweis angegeben, Postleitzahl, Ort, Straße, Hausnummer, Bundesland, Land, Art und Nummer des Ausweises, Event Name, Event Funktion, Registrierungsnummer) dem Landeskriminalamt des Bundeslandes, in dem Sie derzeit Ihren Wohnsitz haben, sowie dem Bundeskriminalamt, der Bundespolizei, dem Bundesamt für Verfassungsschutz und dem Bundesnachrichtendienst (soweit ausländische Staatsangehörige mit Wohnsitz im Ausland die Akkreditierung beantragen) zur Durchführung einer Zuverlässigkeitsprüfung elektronisch zur Verfügung gestellt werden.

Quelle: Datenschutzinformation der Abteilung Akkreditierung der FIFA Fußball-Weltmeisterschaft Deutschland 2006

Wozu werden diese Informationen abgefragt?

„Die im Formular angegebenen Daten werden vom Deutschen Fussball-Bund e.V. [...] ausschließlich dafür verarbeitet und genutzt, um über die Erteilung des Zutrittsrechtes und dessen Umfang zu entscheiden und die Einhaltung der entsprechenden Beschränkungen zu kontrollieren. Die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten dient somit der Gewährleistung der Sicherheit der Veranstaltung."

Quelle: Datenschutzinformation der Abteilung Akkreditierung der FIFA Fußball-Weltmeisterschaft Deutschland 2006

Ich weiß nicht genau, warum mich diese Aussagen nicht beruhigen. Glaubt man wirklich, daß Personen, welche die Veranstaltung stören wollen, sich auf diese Weise akkreditieren und erfassen lassen? Und wenn ja, werden dann nicht eher vermeintlich unbescholtene und bislang nicht auffällig gewordene Personen zu diesem Unterfangen eingesetzt – wie bei den 9/11-Anschlägen?

Nun gut. In dem Prozedere geht es um eine sog. Zuverlässigkeitsprüfung (siehe Box). Dabei werden meine persönlichen Daten verschiedenen Behörden zum „Abgleich" zur Verfügung gestellt. Diese Stellen sprechen dem DFB/der FIFA dann eine Empfehlung aus, ob ich an der geplanten Veranstaltung teilnehmen darf oder nicht. Eine Ablehnung erfolgt ohne die Angabe von Gründen. Doch dazu später mehr. Betrachten wir zunächst den Personenkreis, dem Zugriff auf meine Daten gewährt wird.

Wer hat Zugriff auf die Daten?

Richtig unheimlich wird es, wenn ich mir den Abschnitt Zuverlässigkeitsprüfung (siehe Box) anschaue und sehe, wer auf meine Daten zugreifen darf/wird. So werden LKA, BKA, Bundespolizei, Bundesnachrichtendienst und der Verfassungsschutz gleichermaßen auf die Daten zugreifen. Seitens der Polizeibehörden wird ein „Abgleich" in zweierlei Hinsicht vorgenommen. Zum einen werden die Daten mit jeweils individuell behördlich relevanten Daten/Dateien „abgeglichen". Das Landeskriminalamt, das Bundeskriminalamt sowie die Bundespolizei halten dafür eigene Datenbestände vor. In einem zweiten Datenmodell fließen gewisse Informationen zu Verbunddateien zusammen.

Abbildung 1: „Datenabgleich" der Polizeibehörden

Diese Verbunddateien umfassen Straftäter-/Strafdatendateien (bei denen auch eingestellte oder ohne Verurteilung beendete Verfahren betrachtet werden), Staatsschutzdateien und die Datei „Gewalttäter Sport", auf deren Inhalte ich allesamt nicht en Detail eingehen möchte. Eine Datenlöschung erfolgt im jeweils individuellen Kontext gemäß des jeweils geltenden Rechts.

Das betrifft auch die in dem Nachrichtendienstlichen Informationssystem NADIS bevorrateten Daten, die von den verschiedenen Instanzen des Bundesverfassungsschutzes (BfV) genutzt werden. Hier werden Daten ggf. zwischen fünf und 15 Jahre lang gespeichert, ehe sie gelöscht werden. Meine Daten werden auch hier einem „Abgleich" unterzogen! Ich mag mir gar nicht vorstellen, daß eine den Nahen Osten liebende Person aus meiner Nachbarschaft, ein längst vergessener, heute drogenabhängiger, Freund oder ein entfernter Verwandter mit kommunistischem Persönlichkeitsprofil – aus welchem Grund auch immer – in diesem System erfaßt ist. Das könnten allesamt Referenzen auf/von/mit meiner Person sein. Und wenn derartige Personen aus dem Rande meines sozialen Umfeldes doch erfaßt sind, stellt sich mir sofort

die Frage, ob meine Daten dann „nur“ abgeglichen oder ob sie auch dort abgespeichert werden. Darüber hinaus grübele ich darüber, ob diese Informationen eine negative Entscheidung begünstigen würden/werden.

Anyway. Der Bundesnachrichtendienst ist neben den Polizeiorganen und dem Verfassungsschutz das dritte große Organ, das sich für meine Daten interessiert. Im Normalfall prüft er Personen mit ausländischem Wohnsitz und gleicht die ermittelten Daten mit Dateien zu den Themen Internationaler Terrorismus und Organisierte Kriminalität ab. Ausgewiesenermaßen wird bei Personen mit ausländischem Wohnsitz eine derartige Prüfung durchgeführt. Es bleibt allerdings die Frage offen, ob der Datenabgleich in den anderen Fällen wirklich nicht durchgeführt wird (siehe Toll-Collect; der Umstand, daß wir bislang nur eine LKW-Maut entrichten bedeutet nicht, daß wir in Zukunft nicht eine PKW-Maut bekommen – die dazu relevanten Daten werden von dem System bereits erfaßt, lediglich (noch) nicht ausgewertet).

Wie funktioniert das System? Wohin wandern meine Daten?

Nachdem wir nun einen grundlegenden Einblick darin haben, welche Behörden mit ihren Personalstäben die Daten auswerten, interessiert uns die Art und Weise, wie die Daten transportiert und in welchen Systemen die Daten wie lange gespeichert werden. Ggf. möchten wir des weiteren in Erfahrung bringen, welche Personen diese Systeme betreuen und sichern.

Hierzu läßt sich zunächst keine pauschale Aussage treffen. Lesen wir daher diesbezüglich die Datenschutzinformation noch einmal genau...

Einen ersten Hinweis auf ein elektronisches System zur Datenverarbeitung finden wir hier:

> „Die Erhebung, Verarbeitung und Nutzung Ihrer personenbezogenen Daten erfolgt über ein Akkreditierungssystem, das die FIFA durch Beauftragung Dritter erstellt und bereitgestellt hat.“
>
> *Quelle: Datenschutzinformation der Abteilung Akkreditierung der FIFA Fußball-Weltmeisterschaft Deutschland 2006*

An dieses Akkreditierungssystem ist ein sog. „Event-Server Deutschland“ gekoppelt. Und weiter:

> „Alle im Akkreditierungssystem gespeicherten personenbezogenen Daten werden spätestens Ende September 2006 gelöscht.“
>
> *Quelle: Datenschutzinformation der Abteilung Akkreditierung der FIFA Fußball-Weltmeisterschaft Deutschland 2006*

Das ergibt folgende Grundstruktur...

Abbildung 2: Grundzüge Akkreditierungssystem

... und auch gleich einige Fragen:

Betrifft der beschriebene Löschvorgang auch den deutschen Event-Server? Und wer verbirgt sich hinter dem ominösen Dienstleister? Welche Zugriffe hat er? Werden durch ihn zur Systemsicherheit Backups erstellt? Wo und wie werden diese Backups aufbewahrt? Werden Backups und andere Verbindungs- bzw. Transaktionsdaten des Dienstleisters ebenfalls gelöscht? Welche Service Level wurden für die Datenerfassung, -verwaltung und -bevorratung vereinbart und wie wird das Einhalten dieser Vereinbarungen geprüft?

Die Datenschutzinformation gibt darüber genauso wenig Auskunft, wie sie dem Leser offenbart, wie seine persönlichen und auf das Event bezogenen Daten überhaupt in die Systeme gelangen. Fakt ist, daß ich eingeladen wurde und meine Informationen dem Einladenden übermitteln muß (passenderweise schon einmal per E-Mail unverschlüsselt über das Netz

– sind die Informationen damit nicht schon öffentlich?). Er leitet diese – in seiner Rolle als Event-Manager – wiederum an den DFB weiter.

> „Der Deutsche Fußball-Bund e.V. bedient sich zum Teil externer Dienstleister (insb. Provider, Softwareunternehmen)."
>
> *Quelle: Datenschutzinformation der Abteilung Akkreditierung der FIFA Fußball-Weltmeisterschaft Deutschland 2006*

Mehr kann ich der Datenschutzinformation, bezogen auf meinen Fall, gar nicht entnehmen. Würde ich in die Gruppe derer fallen, die „internationale Medien vertreten oder FIFA-Mitarbeiter sind", würde es (zusätzlich) eine Bewertung der FIFA geben, die in die Akkreditierungsentscheidung einfließt. Für mich bleibt daher nur diese Übersicht:

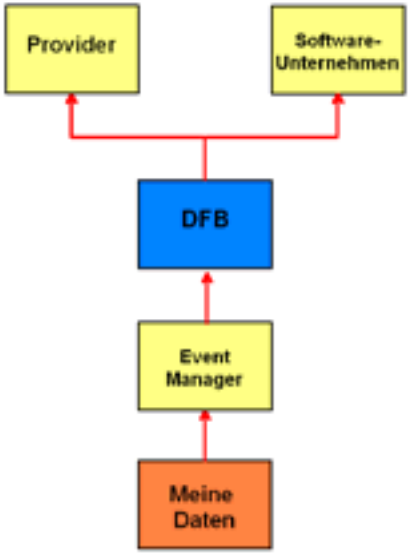


Abbildung 3: Wohin wandern meine Daten?

Es wird bislang weder deutlich dargestellt, wer auf meine Daten zugreift, noch wie diese zwischen den Verantwortlichen transferiert werden. Möglicherweise erfasse ich die Daten selbst, gebe sie an meinen Event Manager weiter, der sie wiederum dem DFB übersendet. Dieser bedient sich wiederum Providern und Softwareunternehmen, um die Daten in den Event-Server Deutschland einfließen zu lassen oder über die FIFA und den Dienstleister in das Akkreditierungssystem zu überführen. Jetzt werden die Daten durch einen weiteren Unbekannten an die Behörden zwecks „Abgleich" übertragen:

Abbildung 4: Das Datenabgleich-Verfahren

Eine mysteriöse Person (vielleicht mit Mantel, Hut, Sonnenbrille und schwarzem Aktenkoffer – nennen wir sie Mr.X) übersendet meine Daten an das jeweilige Landeskriminalamt (LKA), die Bundespolizei (Bpol), den Bundesnachrichtendienst (BND) und das Bundesamt für Verfassungsschutz (BfV) – wobei auch nicht transparent ist, ob die Daten direkt digital übertragen oder auf Datenträgern zwischengespeichert versendet werden.

Im Anschluss werden die Daten beim LKA, der Bpol, dem BND und dem BfV gegen die jeweils individuellen Datenbestände „abgeglichen" (bei den Polizeibehörden gibt es zusätzliche Verbunddateien – siehe Abbildung 1). Die Ergebnisse und Empfehlungen dieser Behörden werden dem Bundeskriminalamt (BKA) überstellt, wo sie letztlich gegen BKA-spezifische Datenbestände abgeglichen werden. Daraus erstellt das BKA als koordinierende Instanz eine „sicherheitsbehördliche Empfehlung", die es dem Organisationskomitee des DFB mitteilt. Vermutlich wird diese Empfehlung dann meinem „Event Manager" mitgeteilt, der mich dann darüber informieren wird, ob ich eine weiße Weste habe oder nicht.

Zunächst fällt mir in diesem Zusammenhang auf, daß Mr. X den Personenkreis, der über meine Daten verfügt, um mindestens fünf weitere Stellen mit einer unbestimmten Zahl an Mitarbeitern erweitert. Dann stelle ich fest, daß in der Datenschutzinformation zwar auf die unterschiedlichen Löschfristen der Datenbestände hingewiesen wird, nicht aber darauf, ob meine Daten oder die neu entstehenden Relationen und Verknüpfungen zu bereits bestehenden Daten ebenfalls abgespeichert werden. Sind diese neuen Relationen dann von der Löschung überhaupt betroffen?

Letztlich wird die Vorgehensweise des Datenabgleich-Verfahrens derart oberflächlich dargestellt, daß es auch an dieser Stelle der Datenschutzinformation mehr Fragen als Antworten gibt. Wer transportiert auf welche Art und Weise meine Daten (Mr.X und weitere)? Wie erfolgt der Datenabgleich? Werden meine Daten in den lokalen Systemen und/oder den Verbunddateien gespeichert? Werden meine Daten manuell erfaßt oder digital über eine Schnittstelle eingegeben? Wer verwaltet die Daten bzw. Schnittstellen? Gibt es Kontrollfunktionen, Koordinierungsinstanzen? Wer überwacht/dokumentiert die ordnungsgemäße Durchführung eines Abgleiches? Verbleiben meine Daten dort oder werden sie gelöscht? Wenn meine Daten wieder gelöscht werden, wer überwacht/überprüft die ordnungsgemäße Durchführung und Vollständigkeit des Löschens...?

Es bleibt in der Tat ungeklärt, was genau – insbesondere aus technischer Sicht – ein „Abgleich“ ist und wie dieser Prozess en Detail reguliert wird. Die Beschreibung hat daher etwas von einer „Black-Box-Dokumentation“:

Input => Black-Box => Output.

Antrag abgelehnt! Was nun?!

Zwar wird in der Datenschutzinformation angegeben, in welchen Fällen die Polizeibehörden, der Verfassungsschutz und der Bundesnachrichtendienst eine Ablehnung der Akkreditierung einer Person empfehlen werden. Aber auch hier bleibt das Dokument schwammig und intransparent, da neben den allgemeinen Zuständigkeiten im Grunde genommen immer auf das Vergehen der „Störung des Rechtsfriedens“ als Kriterium verwiesen wird – und diese Phrase ist gelinde gesagt: schwammig! In diesem Zusammenhang mißfällt mir auch der Passus, daß eine Ablehnung erfolgen kann, wenn „Erkenntnisse vorliegen, die darauf schließen lassen, daß Sie künftig solche Straftaten begehen werden.“ Wenn das nicht an 1984™ erinnert, was dann?

Es kommt erschwerend hinzu, daß die durch das Verfahren erzielte Empfehlung dem Betroffenen ohne die Angabe von Gründen mitgeteilt wird. Sprich: wird das Individuum abgelehnt (ich vermute, der DFB wird den jeweiligen Empfehlungen des BKA folgen), so erfährt es die Gründe hierfür nicht. In meinem Fall wäre eine Absage besonders tragisch, da der mich einladende Dienstleister (beschrieben als „Event-Manager“) vermutlich nicht nur vor mir erfahren wird, daß ich abgelehnt bin, sondern mir dies aller Voraussicht nach auch mitteilen wird.

Wenig nachvollziehbar bleibt auch der Umstand der Möglichkeit, einen Einspruch gegen eine Ablehnung geltend zu machen.

> „Lehnt das Organisationskomitee Ihre Akkreditierung wegen Zuverlässigkeitsbedenken der Sicherheitsbehörden ab, haben Sie [...] die Möglichkeit, sich wegen der Gründe an das Landeskriminalamt Ihres Wohnsitzlandes bzw. – soweit Sie Ihren Wohnsitz im Ausland haben – an das BKA zu wenden."
>
> *Quelle: Datenschutzinformation der Abteilung Akkreditierung der FIFA Fußball-Weltmeisterschaft Deutschland 2006*

Obwohl an anderer Stelle (Datenabgleichverfahren) darüber informiert wird, daß das BKA federführend Daten zusammenführt, die sicherheitsbehördliche Empfehlung erstellt und dem Organisationskomitee des DFB mitteilt, soll man sich zwecks Einspruch an das LKA wenden. Das impliziert, daß das LKA ebenfalls auf die zusammengeführten Daten des BKA zugreifen kann, denn beim LKA „können Sie auch Ihre Einwände geltend machen. Ihre Ein-

gabe wird sodann ggf. an die ablehnende(n) Sicherheitsbehörde(n) weitergeleitet."

Anbei: welche Einwände soll ich geltend machen, wenn ich nicht einmal erfahre, warum ich überhaupt abgelehnt werde?

Wer ist denn nun die koordinierende Instanz: das BKA oder das LKA? Wenn nicht einmal das geklärt ist, wie soll ich da Vertrauen in ein vollkommen diffuses Datenverteil- und Abgleich-Verfahren haben?

Fazit – eine ernsthafte Betrachtung

Es ist mir mulmig zu Mute! Einen technischen „Event" der FIFA Fußball-Weltmeisterschaft Deutschland 2006 besuchen zu dürfen, hat für mich in der Tat einen hohen ideellen Stellenwert, aber es bleibt ein mehr als fader Beigeschmack, wenn ich an die losgetretene Lawine von Personen und Systemen denke, die mit der Erfassung, dem Transport, der Speicherung und Bevorratung meiner persönlichen Daten beschäftigt sein werden.

Es ist mir nicht ersichtlich, wie viele Personen und Systeme allein an dem Transferprozess beteiligt sind. Es ist mir nicht ersichtlich, wie viele Personen und Systeme meine Daten bevorraten und in welchem Zusammenhang sie – wie auch immer – mit anderen Daten abgeglichen werden. Ich kann nicht erkennen, ob meine Daten andere Datenbestände ergänzen und bevorratet bleiben oder ausgetauscht werden.

Daß mir die Datenschutzinformation nicht der Aufklärung darüber dient, nachvollziehen zu können, wo wie lange welche meiner Daten gespeichert werden, kann ich noch verstehen, wenn die Inhalte der Datenschutzinformation wiederum dem Datenschutz unterliegen (mit anderen Worten: das darf mich nicht interessieren und ich soll es gefälligst nicht hinterfragen!) Unerwähnt bleibt in jedem Fall, wie die Daten übermittelt und gesichtet bzw. gesichert und später gelöscht werden.

Es ist ferner in jedem Fall zu bezweifeln, daß eine vollständige Löschung aller mich betreffenden Daten, die aus diesem Vorgang gewonnen werden, nach drei Monaten bzw. einem Jahr gewährleistet ist. Dazu werden die Daten an zu vielen Stellen eingepflegt und „abgeglichen". Ferner ist bei Behörden nicht auszuschließen, daß die Datenübermittlung an einigen Stellen in der Prozeßkette per CD/DVD vorgenommen wird, so daß das ein oder andere Exemplar einer Sicherungs-CD sicherlich den Prozess der „Datenlöschung" überleben wird.

Ich bin mir des weiteren auch nicht sicher, daß die durch die FIFA und den DFB beauftragten „Dienstleister", „Provider" und „Softwareunternehmen" in dem Maße ihre Pflicht erfüllen, wie es die Sensibilität der Informationen gebietet. Leider habe ich keine Kenntnisse über die Unternehmen, die ausgewählt wurden und die Service Level Agreements (SLA) und Vertraulichkeitsverpflichtungen, die zwischen den Parteien (hoffentlich) vereinbart wurden. Ggf. müssen in diesem Zusammenhang verschiedene internationale rechtliche Grundlagen betrachtet werden. Was in einem anderen Land erlaubt ist, kann aufgrund unterschiedlicher Gesetzgebung in diesem Lande verboten sein und umgekehrt.

Und auch für den Fall, daß eine Person abgelehnt wird, finde ich die Darstellung skurril. Es kann einem unbescholtenen Bürger beispielsweise passieren, daß er eine Negativ-Empfehlung erhält, da der Verfassungsschutz einmal gegen eine gewaltbereite und extremis-

tisch auffälligen Person aus seinem Freundes- oder Bekanntenkreises ermittelt hat. Welchen erzieherischen Effekt hätte eine derartige Absage? „Traue Niemandem!“ anstelle von „Ändere Dich!“ Eine Mentalität wie „Du bist durch die Prüfung gefallen – ich sag Dir aber nicht warum!“ sollte im 21. Jahrhundert doch wohl kaum noch Verbreitung finden...!

Fazit II – eine unernste Betrachtung

Ähem. Aber wie gehe ich denn jetzt mit meiner Einladung weiter um? Der Umstand, daß das Schreiben derart komplex und kompliziert aufgebaut ist, daß es entweder gar nicht gelesen und/oder mit dem Kommentar „Ich habe ja nichts zu verbergen!“ belegt wird, nutzen mir konkret nicht weiter. Ich erliege ja einem ziemlichen Druck, da es sich bei der Teilnahme an dem Event um eine im Leben einmalige Gelegenheit handelt („Sie haben doch nichts zu verbergen, oder?“)

Fall 1:

Nehmen wir einmal an, ich unterschreibe die Einverständniserklärung nicht. Kann ich dann überhaupt auf mein Recht nach Datenschutz und Selbstbestimmung pochen – oder leidet die Dienstleister-Kunden-Beziehung darunter („Der hat doch was zu verbergen!“). Ich könnte natürlich auch andere Dinge als Grund vorgeben wie meine plötzliche Hochzeit oder ein Magengeschwür aufgrund akuten Stresses. Dann würde ich allerdings die Unwahrheit sagen, was wiederum aus meiner Sicht die Kunden-Dienstleister-Beziehung nachhaltig beeinträchtigen würde.

Fall 2:

Nehmen wir einmal an, ich unterschreibe die Einverständniserklärung. Das – ernsthaft – mulmige Gefühl des Wartens wird mich beschleichen. Das erinnert mich an die Wartezeit nach der Abgabe einer wichtigen Klassenarbeit bis zur benoteten Rückgabe. Warten auf Godot... Und dann werde ich – ohne Begründung – abgelehnt. Ich werde nicht einmal erfahren, warum. Fakt ist aber, daß der mich Einladende über die Ablehnung unterrichtet wird. Und das wird die Dienstleister-Kunden-Beziehung in der Tat nachhaltig beeinflussen bis hin zu Ansätzen des Denunziantentums und der Rufschädigung meiner Person.

Letztlich müßte meine Person aufgrund derartiger Umstände sowohl in den Qualitäts- und Risk-Management-Prozessen meines eigenen Unternehmens wie auch bei der einladenden Seite kritisch hinterfragt werden. Im extremen Fall könnte eine Ablehnung also eine Geschäftsbeziehung nachhaltig negativ beeinträchtigen und den Ruf des Individuums beschädigen.

Fall 3:

Ich ergebe mich meinem Schicksal, werde nicht abgelehnt (olé olé) und nehme einfach an der Veranstaltung teil – in der Hoffnung, daß mich niemand erkennt... und mich kritisch hinterfragt! Sollte dann allerdings der Veranstalter absagen, MÜSSTEN MEINE DATEN NEU ABGEGLICHEN WERDEN...!

gefunden von einem aufmerksamen Leser in einem McDonalds-Restaurant in Münster (Danke, Philipp)

Nerddaters

46halbe <46halbe@weltregierung.de>,
Florian Holzhauer <fh-ds@fholzhauer.de>

“Ich hab das ja alles für einen Witz gehalten, wie diese Kettenmails eben. Ich kannte so Typen nur von der Mensa in der Uni. Das waren die mit den Shirts mit kryptischen Programmcodes, die immer vor ihren Laptops saßen und irgendwie komisch waren. Meistens haben die nicht so gut gerochen und hatten keine Frisur, die man so nennen könnte.”

Wir sind in Kreuzberg im einem Café, eine Gruppe Frauen sitzt um einen runden Tisch. Miriam erzählt davon, wie sie ihren neuen Lebensabschnittsgefährten Dirk kennengelernt hat. Dirk ist vor einigen Minuten mit seinem Laptop nach drinnen verschwunden, “bei der Sonne erkennt man ja nichts auf dem Display”. Das Café hat ein Gratis-Wlan.

Miriam ist Teil der Nerddaters, ein loser Zusammenschluß von weiblichen Gleichgesinnten, die Nerds als erstrebenswerte Zielobjekte für die Partnersuche erkannt haben. Ein kurzer Text per Mail Anfang letzten Jahres auf Craigslist hat sie hier zusammengeführt. Craigslist ist eine Art Kleinanzeigencommunity in den USA, nett gestaltet und von vielen Singles frequentiert. Eine Frau hatte dort eine Liste gepostet, auf der sie 15 Argumente anführt, warum Nerds und Geeks lohnenswerte Objekte der Begierde seien. “Why Geeks and Nerds are worth it”, so der Originaltitel, ist inzwischen zu einer Netzlegende geworden, übersetzt in viele Sprachen.

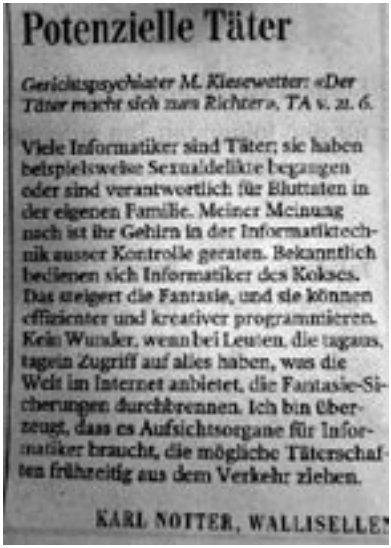
“Mein Ex war ein oberflächlicher, egoistischer Loser mit Oberlippenbart und Schuppen. Irgendwann hat er mal zu mir gesagt, daß ich zu dick sei und was ändern müßte. Er fand auch meine Kochkünste unzureichend, von Sex mal gar nicht zu sprechen. Als dann Schluß war, hat es mich aber doch getroffen.” Die anderen am Tisch nicken. Miriam weist mit dem Kopf Richtung Dirk und lacht. “Was bin ich froh, daß ich nun Dirk kenne.” Sie seufzt.

Der Kellner bringt Kaffee und Tee. Miriam erzählt, wie sie sich kennengelernt haben. “Ich hab´ einfach mal so diesen Typen mit Laptop

angequatscht. Auf Craigslist stand ja auch, man braucht keine Angst vor einem Korb haben. Er hatte mich erst gar nicht wahrgenommen, er war wohl irgendwo anders in Gedanken." Idealer Jagdgrund sind laut Craigslist Cafés und andere Orte, wo es Netz gibt. Miriam hatte es nicht sonderlich schwer, halb Berlin ist voller netter Kaffeeläden mit Wlan. Und ihr reichte ein einziger Versuch. "Er kann nicht nur kochen, man kann auch noch intelligente Gespräche mit ihm führen, und er ist nicht so unglaublich von sich selbst überzeugt. Und er kann jeden Film besorgen. Einfach sexy."

Die Idee, daß es wohl ein paar mehr Frauen geben könnte, die mit einem Nerd als erstklassigem Zeitvertreib gut beraten sein könnten, kam dann beim Essen mit Freundinnen. Die beiden Frauen, die bei ihr zu Gast waren, wollten die Vorzüge eines Nerds nicht recht glauben. "Nerd? Was ist denn ein Nerd?" Miriam weihte sie ein und zeigte das Posting von Craigslist vor. Neid machte sich breit, so einen hätten die beiden auch gern. Miriam empfahl ihnen das Café an der Ecke.

"Die eine ist inzwischen auch in festen Händen und überglücklich – die andere noch nicht, sie legt wohl zuviel Wert auf Äußerlichkeiten." Dabei, so Miriam, seien Nerds ja eigentlich gar nicht unansehnlich oder ungepflegt, nur eben etwas optimierbar. Sie vergleicht Dirk mit einem ungeschliffenen Rohdiamanten. Aber mit ein paar Ratschlägen von erfahrenen Weiblichen würden sich auch Nerds ganz passabel kleiden. "Und wenn sie am Anfang keine Lust auf Einkaufen haben, kann man sie mit kleinen Annehmlichkeiten ködern", sagt sie und lacht leise. Die Waffen einer Frau, wirksames Equipment auch für Nerds.



Potenzielle Täter

Gerichtspsychiater M. Kiesewetter: «Der Täter macht sich zum Richter», TA v. 21. 6.

Viele Informatiker sind Täter; sie haben beispielsweise Sexualdelikte begangen oder sind verantwortlich für Bluttaten in der eigenen Familie. Meiner Meinung nach ist ihr Gehirn in der Informatiktechnik ausser Kontrolle geraten. Bekanntlich bedienen sich Informatiker des Kokses. Das steigert die Fantasie, und sie können effizienter und kreativer programmieren. Kein Wunder, wenn bei Leuten, die tagaus, tagein Zugriff auf alles haben, was die Welt im Internet anbietet, die Fantasie-Sicherungen durchbrennen. Ich bin überzeugt, dass es Aufsichtsorgane für Informatiker braucht, die mögliche Täterschaften frühzeitig aus dem Verkehr ziehen.

KARL NOTTER, WALLISELLEN

Nerddating, in Deutschland noch eine eher verwegene Idee, ist in den USA schon bekannt und schwer im Trend. Gleich mehrere Portale wie *consumating.com* oder *nerddating.net* existieren für die angehende Nerddaterin, sie expandieren inzwischen auch nach Frankreich, Polen oder Finnland. Hierzulande fehlen noch die entsprechenden Angebote, diese Marktlücke wollen die Überzeugungstäterinnen nun nutzen. "Die Nerddater-Webseiten existieren schon. Wir wollen da erstmal eine Sammlung von Tips und Ratschlägen für geneigte Frauen entstehen lassen. Sie sollen auch die berühmte Liste lesen und rausfinden, warum Nerds so sexy sind und wo man sie am besten findet. Danach dann ein Forum, wo man direkt Kontakte anbahnen kann." Miriam bittet nun Dirk hinzu. Er zeigt einige Entwürfe der Webseite, die Frauen sind begeistert.

"Diesen Kontakteteil machen wir so, daß die Mädels gleich klicken können, wen von den Nerds sie interessant finden. Jede kann sich ihre eigene Bestenliste anlegen. Eine Bewertungsskala wird es auch geben." Dirk implementiert das gerade. Er sagt: "Im Prinzip sind so Beziehungsgeflechte ja nichts anderes als ein Graph. Wir haben es hier mit einem Matchingproblem zu tun. Ich schreibe da grade an einem Approximationsalgorithmus, der unglaublich schnell und ausreichend effizient ist. Alles nur ein Optimierungsproblem." Die Frauen nicken, natürlich.

Während Miriam ihm den Nacken krault, erzählt Dirk von Tagging-Features und XMLRPC-Schnittstellen, die er vielleicht noch implementieren will, mit zwei Freunden zusammen. Die Frauen bitten unauffällig, diese beiden Freunde doch mal mitzubringen.

Musings on web applications

von Jane Random Hacker <ds@ccc.de>

Web applications seem to be a big thing right now. To be frank, I cannot quite understand this at a gut-feeling sort of level. But that's not the point, my gut feeling can do whatever it likes. I still want to look at some aspects of the web application hype from a technical and jurisdicational point of view.

How the hell did we get HERE?

A number of years ago, networked software became wide-spread. At some point people noted that somehow the specification and implementation of a certain aspect of the behaviour of networked systems had not been done in a sufficient manner. That aspect is the communication behaviour: Inbound and outbound network activity. Thus, the firewall was invented.

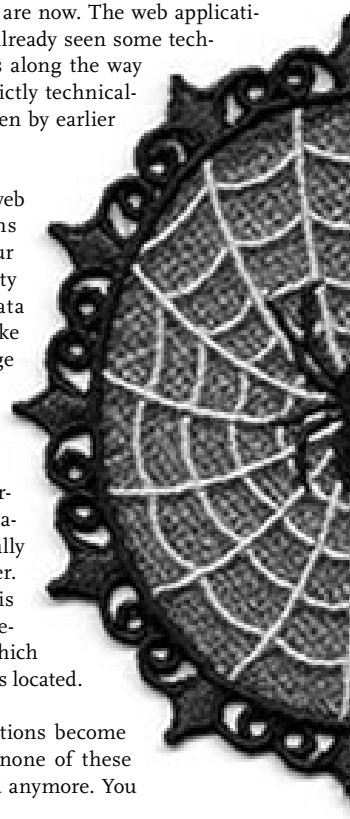
One might regard it as a kind of chewing-gum-and-gaffa-method of specifying a system's network activity: Which kind of input it accepts at its (abstract) network interface and which kind of output it should generate on that interface. Firewalls were either useful or sold well (or both), and so they became widespread. Every administrator then learned that you have to firewall all unnecessary ports. In this process, it became common practice to ideally only leave port 80 and 443 open to the outside, in order to expose minimal attack surface.

But just exchanging formatted text was not enough, either for the people providing content or for those accessing it. And thus began the practice of piping everything over ports 80/443, and not only that, but also piping everything through the protocol associated with these ports: http(s). Note that it is not exactly a light-weight protocol.

But when firewalls were introduced, the problem of properly specifying a system's communicating behaviour had not been essentially solved. And so it popped up again, now that everything was done over port 80. Not all that fancy web-traffic was desired, yet to a classic firewall it all looked alike. And so the idea of the application-level firewall was born, which was yet another gum-and-gaffa-method of constraining the communications behaviour of a system, only at the next level.

Entering web application land

So that's where we are now. The web application rush. We have already seen some technical developments along the way which were not strictly technically sensible but driven by earlier glitches.

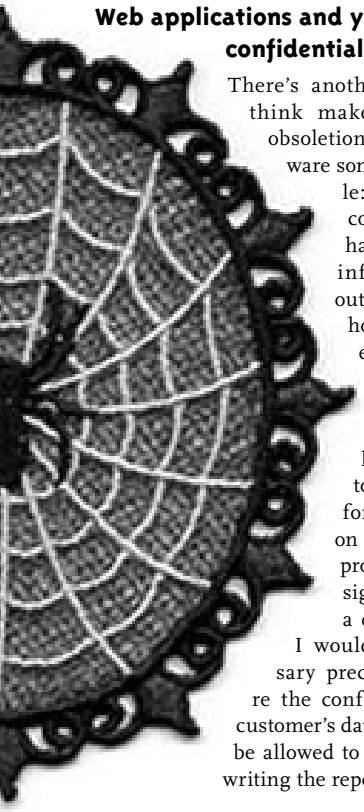


First of all, using web applications means that you entrust your data to a third party entirely. Your data usually doesn't make it onto any storage device you control. It is stored in a database on some server. Ideally you know the person who administrates this server. Ideally you trust him or her. Ideally the server is always the same. Ideally you know in which country the server is located.

But as web applications become more widespread, none of these assertions will hold anymore. You

will probably not know the people who run this web application. You won't know in which country the server is located, and by consequence, under which jurisdiction the content you enter falls. Look out, there's a trap here. What if the web application you're using grows and the maintainers decide to use load-balancing across many servers, possibly across several nations? In this case you can't even ask once under which jurisdiction the server in question is run, because it changes arbitrarily and unpredictably.

Now, of course, that you control your local computer entirely is almost always an illusion. But it still takes both responsibility and freedom away from you if you give away all your data to be stored and maintained and processed elsewhere. To people with whom you probably don't have an established trust relationship.



Web applications and you: confidentiality and trust

There's another aspect that I think makes the complete obsoletion of desktop software somewhat improbable: Which fucking company wants to have all its internal information given out to some webapp hoster and let their employees decide over that? As a security consultant I would have to be crazy to write the reports for my customers on some webapp text processor. Because I signed an NDA and a contract that said I would take all necessary precautions to ensure the confidentiality of my customer's data. I wouldn't even be allowed to use a webapp for writing the report if the hoster of that webapp was a good friend of mine. Could be a very expensive mistake to make.

Of course, companies might at some point enter into trust relationships with hosters of certain web apps. Send in audit teams to make sure the hoster at least adheres to the so-called industry best practice where reliability and security are concerned. Smaller firms may even skip the audit and simply trust the hoster. But again, this latter case is far more likely to happen if that hoster is a well-established and already trusted big player.

Like Microsoft. Google. Yahoo. You name it. Very grass-rootsy, really. And the companies entrusting their data to webapp hosters would not only have to trust these hosters that they are technically reliable. They also have to trust that they won't make use of that position of power that the exclusive physical possession of critical data puts them in.

Whats next

The next great idea of the webapp folks will be to change, no, revolutionize! the way libraries are used. Libraries will become alive, they will no longer be linked into some software but the library functionality will be provided as a Webservice by some hoster. Which raises even more fun issues concerning trust: The user of a "live" library has to entrust a foreign party with possibly sensitive data (the "arguments" to the library call) and has to trust the results coming back from it. This means trusting the foreign party to be both benign in itself and not compromised. We're just not ready yet to provide this level of architectural robustness.

Consequences

So I'd boldly state that using webapps on a wide basis requires the users to grant even more trust to the hosters of webapps. Hey, if it's fun, whatever. I personally am very uncomfortable with that thought. I already feel today that I don't have enough control about my data and my infrastructure, mostly due to a lack of time on my side.

auch eine Netzapplikation

And what is more, I really, really can't understand what's so great about web applications. What's the great benefit of having one big fat huuuuge-ass terminal that's basically able to do anything? But I always have to be connected to the internet to do anything with it at all? (Either that or run a local webserver with the webapp(s) in question, but that is equivalent to running local desktop applications, so there's no point doing that.) I'm sorry, but that concept of one monolithic piece of software, which is then accordingly large, complex, and difficult to handle and maintain from the developer's point of view, does not appeal to me at all. I have to note, though, that one idea behind this whole web application thing is to hide the complexity of software from the user, which is a noble motivation. I just don't think that the path we're taking to reach this goal (webapps! server side blink tags!) is anything good.

The last consquence I want to point out concerns a societal and jurisdictional problem. People investigating security holes in publicly deployed software are in a bit of a problematic position even today. The discussion has cooled off a bit, but remember when politicians were discussing to make the possession and use of "hacker tools" such as nmap and Nessus illegal? Or, as has happened in the USA, make reverse engineering illegal? So there is clearly a drive towards criminalising security research. With web applications, this gets a new and problematic angle. Any webapp that does not publish its source code and anything else that is needed to run it at home will drive the "security researchers" (white hats, call them what you like) and the underground (black hats or whatever, you choose) further apart, since vulnerability research will already violate computer crime laws. You send a malformed packet to a live webapp to search for vulnerabilities, you already run (and accept) the risk of crashing it. Which is, for example, in Germany a violation of paragraph 303b StGB - so vulnerability research of webapps will be punishable with up to 5 years of jail. You know, number (2) of that law: The attempt is liable to prosecution. Our Minister of the Interior, for one, will be delighted.

Thanks & Acknowledgements

I need to hand out credits to FX and Hannes, who both discussed these thoughts with me and thus induced them or helped shaping them. Some things I said here are also outright stolen from FX, I guess.

This text has previously been published on Janes Weblog.

Anonym eingesendete zugefrorene Antenneninstallation, Quelle leider unbekannt

The History of HOPE

by Emmanuel Goldstein

Many people ask us how HOPE began. And I guess if there's anyone to blame for the existence of HOPE, it's the Europeans. That's right. Your fault.

You see, back in the 1980s, we were still amazed that we could somehow manage to publish a hacker magazine and get away with it. As many of you know, 2600 started in 1984 and we adopted our present quarterly format in 1988. It was that new format that actually attracted the interest of bookstores and magazine distributors which gave us access to all kinds of new readers. Until then you would have had to have heard of 2600 somehow and agreed to send us money in order to have us send you a magazine that might get you on a government list. Or at the very least get you in trouble with your parents. So the ability to walk into a bookstore and quietly buy a copy of 2600 without anyone else knowing was as significant a development as the invention of the printing press. At least it was to us.

And it was also in 1988 that the "Off The Hook" radio show began on WBAI Radio in New York City. Now we were suddenly able to project the ideas and stories of the hacker world onto an unsuspecting populace who had no choice but to listen.

Clearly, America was facing a crisis. Apparently we couldn't be stopped.

I would have been happy with this. But anyone who knows me is well aware of the fact that I really hate to cause trouble. And if the government had asked me to stop publishing this obnoxious zine because it was causing them grief, I would have in an instant. I only wanted to help make America a better place. And then I went to Europe for the first time in 1989. I was never the same again. And for that I can never forgive you. Gone was the desire to not cause trouble. I no longer was content to exist quietly in the background. After spending six weeks wandering around Holland and Germany, all I wanted to do was stir things up. I've since sought treatment for this affliction but so far nothing has worked. I fear that I will never be able to stop being a thorn in the side of the establishment. What was it that happened back then? I got my first glimpse of a real hacker conference. It was called the Galactic Hacker Party and it took place in Amsterdam in the summer of 1989. I saw people from all parts of the world come together and learn from each other, sharing all kinds of stories and information. You see, until then I always thought the hacker world was relatively small. We had tiny gatherings in the States like Summercon where a handful of people who all knew each other hung out in a cheap hotel for a weekend. If there were more than a couple of dozen people in attendance, it was a crowd. But in Amsterdam, there were HUNDREDS of people! And, even more amazing, these were people from foreign countries who actually cared about the same things we cared about back home. Phone phreaking. Voice mail hacking. Unix systems. Security holes of all sorts. Launching nuclear missiles from your bedroom. You get the idea. It was cool.

I knew at the time that we could never do something like this in the States. For one thing, we could never get people to work together the way they did over in Europe. We'd never be able to afford a space to have such an event in a decent location. And we'd probably get prosecuted for even thinking about doing it. No, this could never happen in the States.

And then you Europeans did it again. In 1993 the Dutch held another hacker conference that attracted people from all over the world, myself included once again. This time it was an outdoor

camp, which really seemed impossible to pull off. But they did it and they did it well.

Thousands attended. History was made. And I still knew that doing anything remotely similar to this in the States would be impossible. And yet I couldn't stop thinking about it. And I wasn't the only one. We continued to have small gatherings in the States. Summercon, HoHoCon, even Defcon which also started in 1993 with about 75 people. It seemed like this was as far as we could go unless something dramatic happened.

And then something dramatic happened. In the spring of 1994, I got a call from Craig and Randy, the founders of Phrack Magazine and the organizers of the annual Summercon gathering. They weren't going to be able to hold the con this year and wanted to know if 2600 would be willing to host it in New York. By an amazing stroke of luck, I got the call while driving around New York City with Rop, the organizer of the Dutch conferences who just happened to be visiting. We started to plot and scheme and soon realized that this was the chance to actually do something different. It wouldn't be a duplicate of Summercon - it would be modeled instead after the two Dutch conferences. And while I had never been to a CCC Congress, I had heard that they were running annually in Germany since 1984 with smaller crowds but still very well organized and productive. We really had no idea what would happen but it seemed pretty clear that we were the right people in the right place at the right time. And we had nothing better to do.

We still didn't have a name and many of them were flung around. 2600Con – boring. American Hacker Congress - sounded like a political party. CeBit - stupid name that nobody would ever remember.

And then one day it happened. I was driving around with a friend of mine spelling out acronyms in my head and hoping to make them mean something. I hadn't spoken in days. I wanted to call the conference Hackers Around The Earth but I couldn't reconcile being known as the organizer of HATE, tempting as it was. I had just passed through an intersection when suddenly I felt God speak to me. Hackers On Planet Earth. HOPE! There wasn't a bit of doubt that this was the name our conference was meant to be called. And to this day, you can see the skid marks where the name was born.

So we pulled it together in 1994 and had close to 2000 people show up, far more than we had ever imagined. We had two days of a single track which seemed like a lot back then. Ex CIA guy Robert Steele kicked it off on Saturday afternoon with a rousing talk that set the tone for the subject matter we were about to dive into. There were presentations on all forms of computer hacking, blue boxing, and the first social engineering panel, which was also inspired by such a panel at HEU. And best of all, I saw a lot of the same faces that I had seen at the European conferences. The best compliment I received was that HOPE reminded people of HEU and GHP. It was the attitude, the cooperation, the education, and the fun. And, guess what? We did this in the middle of New York Fucking City, something EVERYONE had agreed was completely impossible.

The hacker spirit had really come through. It took a while for us to recover and the last thing I expected was to be able to pull this off a second time. But people were clamoring for another HOPE so we put our heads together and tried to figure out if we could do it again. We knew we didn't want to do this every year because it wouldn't be a special event if we did. The last thing I wanted was to be stuck in a predictable routine. It would be another three years before the next conference took place. And rather than do something lame like call it HOPE 2, we decided to make a whole new name while keeping a link to the past.

And so in 1997, Beyond HOPE came to be. Once again it was great fun and a little bit bigger. Defcon had now gotten big as well but people still told us that HOPE was unique. Maybe it was the large international turnout, maybe it was the fact that we were in the most exciting city in the world. All I knew was that it was magic.

But despite all of the fun and success, one sobering development took place at Beyond HOPE. We lost a ton of money, probably because we only charged $20, which was actually LESS than the first HOPE. Bad move and it couldn't have come at a worse time since we had just lost another ton of money when one of our distributors went bankrupt. That was the year we almost lost 2600.

Despite this near disaster, we knew the conference world happen again. We just had to figure out how to make it work. And so, in 2000, H2K, our third conference – with an acronym in an acronym – was held. We had more space and a much larger speaker program. We got ex-Dead Kennedy's singer and spoken word performer Jello Biafra to deliver a completely different sort of keynote address than what most were expecting. We were always careful to avoid being predictable but at the same time we wanted to remain relevant. Jello opened a lot of eyes that year. This time it all went so smoothly that we decided to start holding these things every two years so that we could alternate with the Dutch and German hacker camps that take place in odd-numbered years.

H2K2 (a name nobody was expecting) followed in 2002. This time we had a tremendous expansion of space as an old department store downstairs had been taken over by the hotel. At times it actually seemed as if we had too MUCH space, a nice problem to have. I decided to get a completely different kind of keynote speaker once again: a cartoonist who had managed to ACCURATELY portray the whole DeCSS lawsuit (which we had been a recent victim of) in a comic strip called "Boondocks." Most attendees had never heard of him. And when he was done, nobody forgot who he was or the words he spoke. (Today his name is a household word and his comic strip has expanded into a successful television show.) H2K2 brought even more people together and the tradition really seemed to be a solid thing. Because of the name, a lot of newcomers thought it was only our second conference. But who cares.

The most recent conference was NOT called H2K4 like everyone seemed to expect but rather The Fifth HOPE since it was, after all, our fifth conference. It had a nice ring to it as well, like the Fifth Amendment or the Fifth Dimension. Once again, we had a huge amount of space and a ton of speakers. We decided to have a different keynote speaker for every day of the conference: recently freed computer hacker Kevin Mitnick on Friday, Apple co-founder Steve Wozniak on Saturday, and returning keynoter Jello Biafra on Sunday. The overwhelming complaint we received was that there was just too much to do and no way to do it all. This is most definitely a big problem for all of us.

And so, it's now 2006. Not only is that an anagram of 2600 but it's also a year ending in six that is the year of our sixth conference! Six is in the air. And so, we present HOPE Number Six. Do I really have to explain why your stay on this planet will be more pleasant if you attend? There is no better feeling than to be in a foreign land and realize that you're amongst friends. For that reason alone you should come. But in addition, you will learn a great deal, make connections that you'll likely have for the rest of your life, and have stories to tell your grandkids when this sort of thing becomes illegal worldwide. So do what you have to do in order to raise the funds to come over here and experience HOPE.

One thing we hear from a lot of people is concern of what it's like to come into our country, now that it's pretty much been destroyed by our leaders. Hey, life is full of challenges and the road to enlightenment isn't always paved. So maybe you'll have to give your fingerprints to the nice customs agent. Maybe you will need to apply for a visa. Perhaps you will grow weary of the American flags flying everywhere which serve to remind us which country we're living in. None of that should matter. Because at the end of the road, there will be HOPE. And if that's not worth a little adventure and perhaps some inconvenience, you may find the claws of conformity catching up to you sooner than you would like.

See you in New York. Resistance is futile.

Hackers on (the other side of) Planet Earth

By B9punk and Villan, support: Dragorn

NOTICE:

Pursuant to U.S. Intellectual Property Law, the American P.A.T.R.I.O.T. Act (2) extension, and, in accordance with Cryptographic Arms & Ammunitions export controls to territories deemed within "Old Europe", the reader is required to consider the following:

- Any and all "Hacking" is both completely illegal and absolutely unacceptable.
- You do not "own" either the software nor hardware you use. Both have been licensed for your own beneficial use, for a limited time only.
- Since cryptography can only be used to hide things, and only criminals hide things, it is hereby understood that only criminals use cryptography.
- Despite our continued economic exchange, it is the official opinion of the U.S. Government that the animal most representative of the fighting spirit of the German people to be DAS WEASEL.

This article MUST include the preceding "Free Speech Authorization" when being reproduced either in part or its entirety. Also note, neither this "Authorization" nor the United States Constitution shall infringe the methods or wishes of the National Security Agency, Department of Homeland Security, or the Republican Party. God bless.

There has never been a better time to come to the U.S.

Sick and tired of being "accepted" and "appreciated?" Unhappy that your subculture is "losing its edge" or is "no longer considered a terrorist organization?" I bet! Well, take some time out of your busy schedules of state-funded education and see how the other half lives! Now, we know that a lot of you don't like the U.S. government. This is great, because the majority of us don't either (approximately 68%). That's over 172 million people... so you'll be in good company. There are a lot of changes going on in the U.S. Government, and if that sounds a little scary for the hacker scene, that's because many of them are, but lets take a look and see if we can dispel some concerns.

Don't they take your fingerprints at immigration when you visit?

True. But hold on... First of all, they take your fingerprints on a fingerprint scanner. Aren't we hackers? Aren't we the ones who should know and understand the vulnerabilities of technology like this?

[U.S. GOVERNEMENT NOTICE: DEFEATING FINGERPRINT READERS IS IMPOSSIBLE, SO PLEASE, PLEASE DO NOT TRY TO DO THIS.]

It's our responsibility to voice our concerns about this policy in the first place, and proving to them that their data is unreliable is helpful to that cause. Second of all, if these kinds of policies are continued, and advanced by the state, as they have been exponentially since the 9-11 attacks, it will only get harder and harder to enter. By coming now, you can help us protest the policy, and get a chance to see what we are all about and help us to change these policies before they spread around the world.

What's so cool about the American hacker scene?

The American hacker scene is very large. Our largest gathering is twice as large as the lar-

gest German CCC Congress. We are a really big country and we have many small groups spread throughout. There are new conferences being organized every year (we are currently host to over a dozen annually). There are very active 2600, and other groups doing big things in their areas, and there is a lot of variety across the country as to what people are working on. Although we are constantly looking for ways to unite, bring in new people, and to better explain ourselves to the public, we are now faced with an increasingly strict, rights-infringing, political environment. It is perhaps not so unlike the situation in Germany at the time the CCC was formed. Come, so that we can share our stories and learn from each other.

The Two-For-One

We are very lucky to have two of the most important, largest, and most diverse hacker events within two weeks of each other this year: Hope Number Six and Blackhat/Defcon. This hasn't happened in the last half-decade and is not likely to happen again any time soon, in the future. If the events are farther apart from one another it's less likely to get as many foreign travelers to either event, and when they are too close together it is harder for the locals to attend both events. If you choose to come to both, or just HOPE this year you will see a lot of the hacker culture here, and a lot of America. We will be posting information about how to travel between the two conferences in our wiki, so check back often!

So, What is HOPE All About Anyway?

Traveling to HOPE, from Germany or anywhere else in the world, is easy.

[NOTE: Under the newly passed "Better Safe Than Sorry" Act, the policy of shooting all foreigners at the border is not scheduled to be implemented until 2008, so it's perfectly safe. For now.]

There will be detailed information about this posted in the HOPE wiki, which you can find a bright and pretty link for on the main HOPE website: *http://www.hope.net/*

Here are some reasons why you will want to come:

Location

HOPE is held in New York City, the largest metropolis in the United States, and the 5th largest in the world. Despite rumors to the contrary New York is a very friendly city, especially to visitors, and you will find many Germans and German-speakers here, particularly if you visit the favorite tourist spots. It is held in the Hotel Pennsylvania, one of the most famous hotels with one of the most famous phone numbers ever: Pennsylvania 6-5000.

Directly across the street from the Hotel Pennsylvania, Madison Square Garden was recently the host of the Republican National Convention and serves as the home of many other large events. Beneath Madison Square Garden is Pennsylvania Station, one of the largest passenger train stations in the United States. Hundreds of thousands of travelers emerge from this station every morning, and will be greeted with the artwork of the HOPE conference. This time, the front of the Hotel will be decorated with an interactive light display in the spirit of Blinkenlights. The conference location gives us all the chance to interact with the public and display the creative side of hacking.

Community

HOPE is an international event, despite being across the pond and thousands of miles away

from countries other than Canada and Mexico. HOPE Number 6 is no exception, drawing attendees not only from around the United States but from around the world. This means you.

Content

HOPE Number Six will have many interesting talks this year. One of the keynotes will be given by Richard Stallman, founder of the Free Software Foundation, and other celebrity speakers include Kevin Mitnick, Richard Steele, and Jello Biafra. Talks will cover such diverse subjects as privacy, pirate radio, smart homes, smart cars, biometrics, legalities of network monitoring, hackers in prison, wiretapping, consumer electronics hacking, secure programming, quantum computing, and more. If you are interested in becoming a speaker, please visit the "Call for Participation" page on the *hope.net* website.

In addition to the HOPE offerings, there will be a PallTech seminar, "High Tech and Hardcore Investigative Tactics and Training" held at the conference. Attendees who go to both events will receive discounts for admission. More information about the PallTech seminar is available on the HOPE Number Six blog:
(*http://blog.hopenumbersix.net/)*

There will be an opportunity for other ongoing workshops such as lock picking, and possibly some hands-on RFID fiddling, as well as the chance to do an impromptu talk, a short 4-7 minute "lightning talk", a rap session, etc. You can also bring your computers or hardware to set up and show off in the open network space on the second floor. You don't need to sign up, there is plenty of space and power for everyone, so bring your gear, and share what you do.

Network

The network at HOPE is wholly constructed using equipment donations, and by the efforts of conference volunteers. The function and features of the network continue to improve every conference. In 1994 we supplied 28.8K dial up, and in 2000, a pair of Airport base stations. Today, of course, we can supply broadband and a redundant self-healing wireless network, which sustains a large amount of wireless attacks from the attendees. We also provide a public terminal cluster, A/V streaming to the overflow conference rooms, and private protected VLANs for the infrastructure networks (presentation connections, A/V connections, etc). Some of the challenges the HOPE network faces is running a fiber connection between the conference floor of the hotel and the public computing floor (16 floors away), and keeping these things running and secure with many curious conference-goers, and while there is a large amount of normal New York tourists staying in the hotel.

For the first time HOPE Number 6 will set up a VOIP system setup for both the attendees and others to interact with. Expect mailboxes, voice bridges, and a plethora of interesting services running on the open source asterisk project. We will be incorporating SIP phones at the conference for attendees to use, and possibly even a VOIP gateway for others to connect to from anywhere on the net.

CTF

HOPE will be hosting a "Capture the Flag" game. For the unaware, this is a game that traditionally consists of teams who are challenged to attack a machine or machines that are set up for this purpose. These machines host self-written services with various vulnerabilities that require different skills, and skill levels, to exploit. Each team's hacker prowess is scored based on the difficulty and the efficiency of the exploits they manage to find and defeat. Registration details will be announced closer to the conference.

Atmosphere

Hope Number Six will be host to hacker projects, vendors, and international groups such as the CCC. It is 24-hour/3-day affair, with speakers, panel sessions, and activities late into the night. The second floor of the conference is dedicated to the community: space to talk, socialize, relax in hammocks, watch hacker media in the movie room, and hack on equipment the general public can't usually get access to.

We like to design the hell out of our conferences. Our badges, posters, stickers, flyers, t-shirts, and of course the space itself will provide lots of interesting things to look at and to think about. You can get a taste of this on the back cover of this magazine!

The HOPE conferences are life-changing experiences for most attendees. Who can forget these brilliant moments at previous conferences?

- The Prophet, reading "The Hacker Manifesto"
- Kevin Mitnick, talking about his early social engineering
- Emmanuel Goldstein and others doing a live simulation of their court case, just weeks before the real thing
- Live demonstrations of social engineering, caller-id spoofing, and microwaves

So now that you've decided to come...

We encourage people of all ages, races, creeds, etc. to come to HOPE. As expected, our average demographic is 90% male, between the ages of 17 and 45, but the HOPE conferences do frequently attract teenagers and pre-teens, often in the accompaniment of a parent. Sometimes it's a dad wanting to teach his teen about the ethics of hacking, or to point him/her to the fun of developing technical skills. Other times it's the opposite – a young woman who wants her mother to see that learning and exploring all about the world we live in isn't weird, it's something that all hackers do, for their, and everyone's benefit.

[NOTE: GERMAN ATTENDEES WILL NOT BE REQUIRED TO REGISTER THEIR TECHNICALLY GIFTED CHILDREN UNDER THE "NO HACKER CHILD LEFT UNMONITORED" ACT OF 2006]

Registering for HOPE is both simple and cheap, like the French. You will find a link to our online registration on our main website, *http://www.hope.net/*, and information there about other ways to register. Pre-registration for the event is $60 USD (approximately 48€). The door price has not yet been determined, but it will be as cheap as possible and not more than $75 USD (approximately 59€).

Resources

Though we've mentioned some of these previously in this article, here is your one-stop-shop for all the ways to find out more information about HOPE, the main website can be found at: *http://www.hope.net/* or at *http://www.hopenumbersix.net/*. Constant updates can be found at the HOPE Number 6 blog (which we actually acknowledge as a "blog") *http://blog.hopenumbersix.net/*. You can make comments, suggestions, add pages in your favorite language, and interact with the HOPE coordinators, and attendees on the HOPE Number 6 wiki: *http://wiki.hopenumbersix.net/Main_Page*

More information about the PallTech Seminar to be held during hope can be found here: *http://www.palltechseminars.com/*. Registration Information can be found here: *http://www.hopenumbersix.net/register.html*. If you are interested in becoming a speaker at HOPE, please consult the Call for Participation page at: *http://www.hope.net/cfp.html* and then write to *speakers@2600.com*. Information about people wishing to volunteer to help, at or before HOPE can be found here: *http://www.hopenumbersix.net/volunteer.html* or send an email to *volunteers@2600.com*

Those wishing to bring a lot of equipment, a project, and art piece, be a vendor, etc., should also send an email to *volunteers@2600.com*, and you will be put in touch with an appropriate person to find space for you ahead of time.

So don't miss out. Take the trip and share the experiences, the commonalities, the projects, and the ambitions of Hackers On Planet Earth.

Buchbesprechung: Traveler

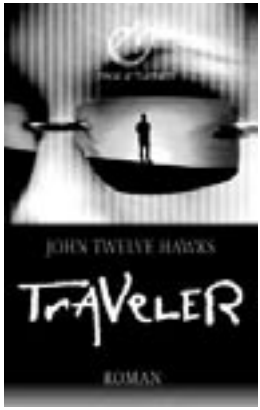
padeluun <padeluun@bionic.zerberus.de>

Eine unglaublich neue Idee, verspricht uns die Verlagsankündigung dieses Buches: „Eine gigantische Verschwörung bedroht die Welt". Guckemaleineran!

„Die weltweite Konspiration einer geheimen Bruderschaft bedroht die Menschheit und nur einige wenige Menschen können das infame Komplott noch stoppen."

So steht es auf der Website des Verlages. Und da steht mehr, das neugierig macht:

„Jede Bewegung wird gefilmt, jedes Telefonat abgehört, jede Spur im Internet verfolgt, jeder Einkauf registriert – mit Hilfe eines Systems der totalen Überwachung versucht eine geheime Bruderschaft, die Herrschaft über die Welt zu gewinnen."



Na, das ist doch mal spannend. Da sind wir doch qua Ehrenamt Spezialisten. Stoff für hunderte von Büchern – und endlich schreibt mal jemand einen hübschen Roman, der so richtig zeigt wo's langgeht? Leider Fehlanzeige. Klar hängen hier und da in der Story Überwachungskameras rum, auch implantierte RFID-Chips spielen eine Rolle, und ein ehemaliger amerikanischer Präsidentenberater ist natürlich einer der Oberbösen. Aber: Gähn. Die Story ist hirnrissig und flach wie Ostfriesland: „Nur wenige Menschen, Traveler genannt, vermögen die Pläne der Bruderschaft zu durchkreuzen. Denn die Traveler haben die außergewöhnliche Gabe, in andere Sphären zu reisen. Und sie stellen sich seit jeher schon jedem Versuch entgegen, die Selbstbestimmung und Freiheit der Menschen zu zerstören." Boah! Da gibt's also besonders begabte Gutmenschen. Wo George Lukas den von ihm geschaffenen „Macht"-Mythos entmystifiziert, indem er die „Die Macht" kleine kribbelnde Tierchen im Blut von Jedies sein läßt, haben hier die Protagonisten Lichter im Hirn. Nur wer von Geburt aus dazu vorbestimmt ist, kann was besonderes sein, bei den anderen reichts höchstens zum ergebenen Jünger: „Die Brüder Michael und Gabriel Corrigan sind, ohne es zu wissen, die letzten Nachkommen der Traveler. Von den Schergen der Bruderschaft gejagt, scheinen sie kaum eine Chance zu haben, deren Machtergreifung noch zu verhindern. Wäre da nicht Maya, die Nachfahrin einer Kriegerkaste, die ihr Leben dem Schwertkampf und dem Schutz der Traveler geweiht hat. Es liegt allein in ihrer Hand, die letzten Traveler vor den Nachstellungen der Bruderschaft zu retten, bevor die Freiheit den Menschen für immer verloren geht." Achja, Schwerter, das ist immer cool. Nagut, das WAR mal cool. Seit Hiro Protagonist, Pulp Fiction und Kill Bill ist es bloß noch blöde. Und der Rest der Ideen nebst Buch ist keinen Deut besser. Der Autor? In Wikipedia steht Stub (eigentlich sollte da gleich ein Löschantrag folgen): „John Twelve Hawks is the mysterious author of the 2005 anti-state novel entitled The Traveler." Aha. Klingt verdächtig autoreferenziell. Und weiter:

„His publishers claim that he is, indeed, a real first-time author, and that he contacts the publishers using an untraceable satellite phone. Not much is known about him except what he himself states. In the beginning of the audiobook version of The Traveler, a garbled, electronic voice states, "This is John Twelve Hawks," and

later, after some introduction to why he wrote the book, he states, "I live off the grid." That last statement basically sums up what is known about this author." Na toll. Kindergarten spielt Überwachungsstaat austricksen.

Wenn schon Bücher zum Überwachungsthema, dann bitte eins, das klarmacht, warum jede und jeder von Überwachung betroffen ist. Ein Buch, das geheimnisvolle Bruderschaften (hier mit den üblichen Anleihen bei den Illuminaten) die absolute Macht erringen lassen will, muß mehr bieten, als Mystik, glückliche Zufälle und ein Minimumwissen über Überwachungsstrukturen und deren Netze.

John Twelve Hawks
Traveler, Roman (Originaltitel: The Traveler - The Fourth Realm)
Gebundenes Buch, 544 Seiten, 13,5 x 21,5 cm,
ISBN-10: 3-442-20300-7
ISBN-13: 978-3-442-20300-0
€ 19,95 [D] / SFr 35,00
Verlag: Page & Turner

Fazit: Das Buch ist „out of the grid". Durchs Raster gefallen. Kürzer: Durchgefallen.

Buchbesprechung: ePass – der neue biometrische Reisepaß

von Thalunil <thalunil@kallisti.de>

Der aktuell ausgestellte Reisepaß in der BRD beinhaltet als erstes biometrisches Merkmal das Gesichtsbild in digitaler Form, und in naher Zukunft (Anfang 2007) soll auch der Fingerabdruck folgen. Dies ist das Ergebnis der deutschen Umsetzung der EU-Rats-Entscheidung zur Integration von biometrischen Merkmalen in Reisedokumenten vom 13.12.2004.

Jöran Beel und Béla Gipp beschäftigen sich in ihrem Sachbuch zum Thema „elektronischer Reisepass" mit der Funktionsweise des Reisepaß, biometrischen Merkmalen, Schutzmechanismen des ePass, Umgehungssicherheit des Reisepaß sowie der Frage nach den Gründen der Einbindung biometrischer Merkmale.

Das Kapitel „Umgehungssicherheit" wurde mit Referenz und in Zusammenarbeit mit dem clubeigenen Kompetenzzentrum für biometrische Angelegenheiten erarbeitet.

Jöran Beel & Béla Gipp
ePass - der neue biometrische Reisepaß
118 Seiten, 13,5 x 21,5 cm,
ISBN: 3-8322-4693-2
€ 29,80
Verlag: Shaker

Der den Bedenkenträgern gewidmete Abschnitt beinhaltet Zuverlässigkeitsaspekte, RFID-Tag-Funkmanipulation sowie kryptographische Sicherheit des Systems.

Das Paßbild wird mittels sogenanntem Basic Access Control-Schema (BAC) gesichert. Die Kenntnis der Behördenkennzahl (BKZ) geht sehr zu Lasten dieses Sicherheitsschemas. Eine gesammelte Liste von BKZ's befindet sich im Aufbau, und gute 10% des Zahlenraums sind bereits gelistet. Die geplante Länder-"Public Key Infrastructure" (Länder-PKI), welche zur wechselseitigen Authorisation (Extendes Access Control) der Biometriemerkmale gegenüber den Auslesegeräten angedacht ist, wird ebenso ausführlich behandelt.

Die rund 100 Seiten sind interessant geschrieben und bieten auch dem Laien einen Einblick in den neuen Reisepaß.

Erfa-Kreise / Chaostreffs

Bielefeld im AJZ, Heeper Str. 132, mittwochs ab 20 Uhr *http://bielefeld.ccc.de/* :: info@bielefeld.ccc.de
Berlin, CCCB e.V. (Club Discordia) Marienstr. 11, (Briefe: CCCB, Postfach 64 02 36, D-10048 Berlin), donnerstags ab 17 Uhr http://berlin.ccc.de/ :: mail@berlin.ccc.de
Dresden, C3D2/Netzbiotop e.V., Lingnerallee 3, 01069 Dresden
dienstag ab 19Uhr *http://dresden.ccc.de/ :: mail@c3d2.de*
Düsseldorf, CCCD/Chaosdorf e.V. Fürstenwall 232,
dienstags ab 19 Uhr *http://duesseldorf.ccc.de/ :: mail@duesseldorf.ccc.de*
Erlangen/Nürnberg/Fürth, BitsnBugs e.V. "E-Werk", Fuchsenwiese 1, Gruppenraum 5
dienstags ab 19 Uhr *http://erlangen.ccc.de/ :: mail@erlangen.ccc.de*
Hamburg (die Dezentrale) Lokstedter Weg 72
2. bis 5. Dienstag im Monat ab etwa 20 Uhr *http://hamburg.ccc.de/ :: mail@hamburg.ccc.de*
Hannover, Leitstelle511 Kulturcafé, Schaufelder Str. 30, Hannover
2. Mittwoch im Monat ab 20 Uhr *https://hannover.ccc.de/*
Karlsruhe, Entropia e.V. Gewerbehof, Steinstr. 23
sonntags ab 19:30 Uhr *http://www.entropia.de/ :: info@entropia.de*
Kassel Uni Kassel, Wilhelmshöher Allee 71-73 (Ing.-Schule)
1. Mittwoch im Monat ab 18 Uhr *http://kassel.ccc.de/*
Köln, Chaos Computer Club Cologne (C4) e.V. Chaoslabor, Vogelsanger Str. 286
Letzter Donnerstag im Monat ab 19:30 Uhr *http://koeln.ccc.de/ :: mail@koeln.ccc.de*
München, muCCC e.V. Kellerräume in der Blutenburgstr. 17
2. Dienstag im Monat ab 19:30 Uhr *http://www.muc.ccc.de/*
Ulm Café Einstein an der Uni Ulm, montags ab 19:30 Uhr *http://ulm.ccc.de/ :: mail@ulm.ccc.de*
Wien, chaosnahe gruppe wien Kaeuzchen, 1070 Wien, Gardegasse (Ecke Neustiftgasse)
Alle zwei Wochen, Termine auf Webseite *http://www.cngw.org/*

Aus Platzgründen können wir die Details aller Chaostreffs hier nicht abdrucken. Es gibt aber in den folgenden Städten Chaostreffs mit Detailinformationen unter *http://www.ccc.de/regional/*: Aachen, Aargau, Augsburg, Bad Waldsee, Basel, Bochum, Brugg, Darmstadt, Dortmund, Dresden, Frankfurt am Main, Freiburg im Breisgau, Gießen/Marburg, Hanau, Heidelberg, Ilmenau, Kiel, Mainz, Mülheim an der Ruhr, Münster/Osnabrück, Offenbach am Main, Paderborn, Regensburg, Stuttgart, Trier, Weimar, Wetzlar, Wuppertal, Würzburg.

Friends & Family

Zur näheren Chaosfamilie zählen wir (und sie sich) die Häcksen (*http://www.haecksen.org/*), den/der "Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V." - FoeBuD (*http://www.foebud.de/*), den Netzladen e.V. in Bonn (*http://www.netzladen.org/*) und die c-base Berlin (*http://www.c-base.org/*).

Die Datenschleuder Nr. 90

Herausgeber (Abos, Adressen, Verwaltungstechnisches etc.)
Chaos Computer Club e.V., Lokstedter Weg 72,
20251 Hamburg, Fon: *+49.40.401801-0,*
Fax: *+49.40.401801-41, <office@ccc.de>* Fingerprint:
1211 3D03 873F 9245 8A71 98B9 FE78 B31D E515 E06F

Redaktion (Artikel, Leserbriefe, Inhaltliches, etc.)
Redaktion Datenschleuder, Pf 64 02 36, 10048 Berlin,
Fon: +49.30.28097470, *<ds@ccc.de>* Fingerprint:
03C9 70E9 AE5C 8BA7 42DD C66F 1B1E 296C CA45 BA04

Druck
Pinguindruck Berlin, *http://pinguindruck.de/*

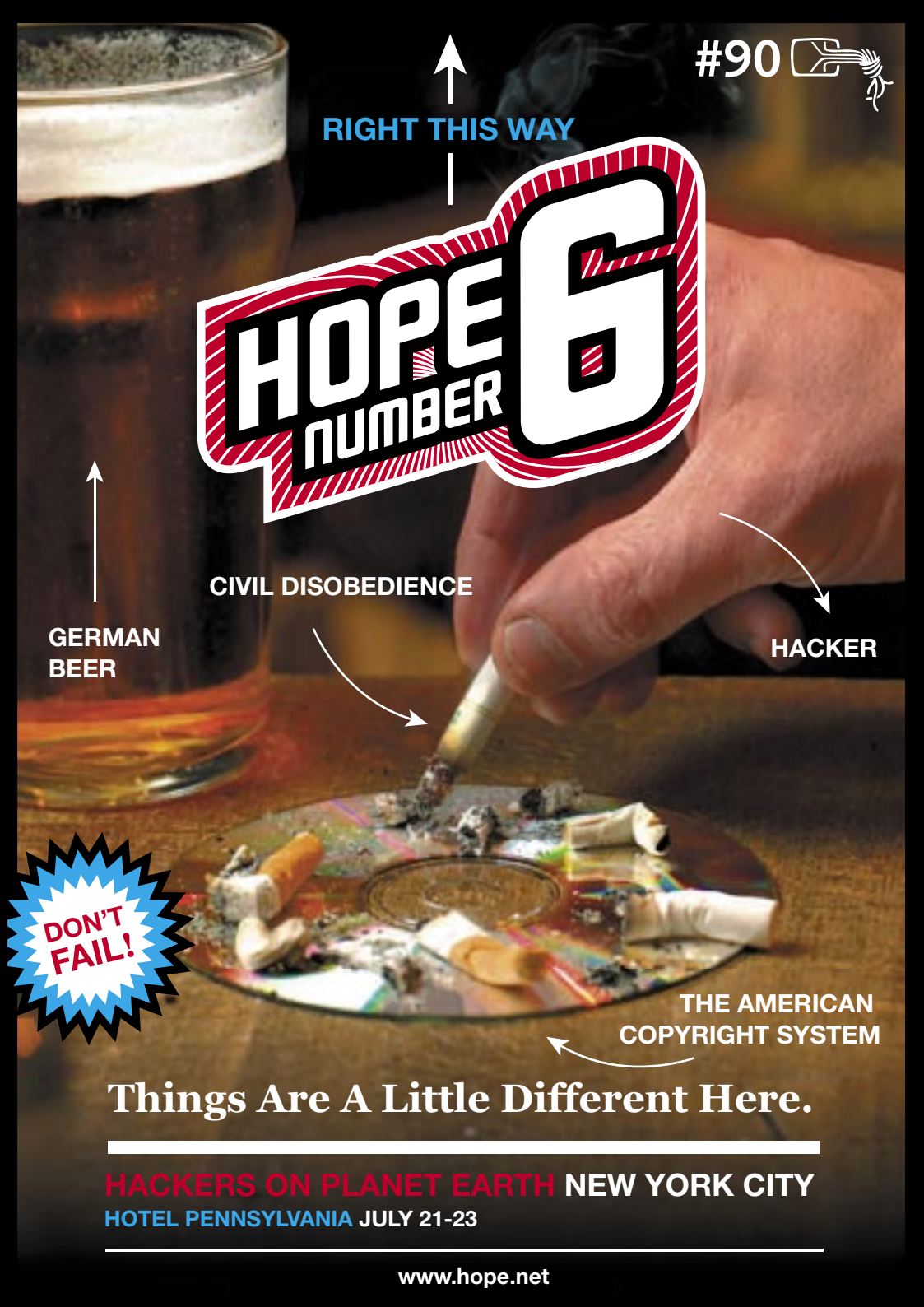
ViSdP und Produktion
Tom Lazar, *<tom@tomster.org>*

Layout
Dirk Engling, b9punk, John Paul Bader <hukl>, Frank

Redaktion dieser Ausgabe
Thalunil, Armijn Hemel, Constanze Kurz, Corinna Habets, Dirk Engling <erdgeist>, McFly, Emanuel Goldstein, Florian Holzhauer, Frank, Jane Random Hacker, b9punk, Philipp Paul & Philip, Rainer Böhme, "Brud3r H4ck", Rickard Falkvinge, Tim Pritlove, Sandro Gaycken, padeluun, Villan

Besonderer Dank
Cover: Tobias, BlackBerry: Maxim, Tempelphone: Andy


1 2 3
4 5 6
7 8 9
* 0 ¤


#90
RIGHT THIS WAY
HOPE NUMBER 6
CIVIL DISOBEDIENCE
GERMAN BEER
HACKER
DON'T FAIL!
THE AMERICAN COPYRIGHT SYSTEM
Things Are A Little Different Here.
HACKERS ON PLANET EARTH NEW YORK CITY
HOTEL PENNSYLVANIA JULY 21-23
www.hope.net