die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

ISSN 0930-1054 • 2008
Два Еуро Пятьдесят
Kein Postvertriebsstück mehr ~~€11301F~~

#93

Geleitwort

Ein ereignisreiches Jahr neigt sich dem Ende zu und die Redaktion Datenschleuder freut sich, endlich wieder ein spannendes Heft fertiggestellt zu haben, allen widrigen Einflüssen wie crashenden Festplatten zum Trotze.

Plötzlich und wenig überraschend befindet sich die Welt im Wirtschaftskrisen-Modus. Au weia, denkt sich da der Durchschnittsbürger, was haben wir bloß für einen geldgeilen Raubtierkapitalismus an unserer Brust genährt? Vielleicht ist dies ja die Krise, für die der verdiente Minister und Verfassungsfreund Dr. Wolfgang Schäuble die Werkzeuge der Pöbelunterdrükkung und Volksdisziplinierung zu brauchen meint, falls die Milliardengeschenke an die Zockerbanker nicht helfen. Die Diskussion um BKA-Gesetz, Bundestrojaner und die Aktionen dagegen haben jedenfalls gezeigt, daß es in Deutschland endlich eine – wenn auch knappe – Mehrheit für Freiheits- und Bürgerrechte gibt. Der Hirnfurz mit dem BKA-Datenschutzbeauftragten als Wächter über die Bundestrojanerbeute war aber auch zu dreist.

Das Gefühl, nicht allein zu sein im Streben nach mehr Freiheit, Glück und Demokratie, beschwingt uns durch die frustrierenderen Zeiten. Die entspannte Demo in Berlin im Oktober brachte eine erfreulich bunte und große Menschenmenge auf die Straße, was noch vor zwei Jahren praktisch undenkbar schien. Es bildet sich langsam, aber beharrlich eine umfassende Gegenposition zu den realitätsabgewandten Regierungsansichten. Die Fähigkeit der SPD, selbst aus der Bauchlage noch umfallen zu können, überrascht natürlich niemanden mehr, aber gerade im Bereich Sicherheit und Bürgerrechte zeigt sich die zunehmende geistige Umnachtung des derzeitigen Bestands der uns regierenden Internetausdrucker. Daß die SPD Jörg Tauss abschießt, den einzigen Abgeordneten, für den Internet, Datenschutz und Medienzeugs keine totalen Fremdwörter sind und der einen Browser selbständig bedienen kann, paßt da ins Bild.

Da hebt sich auch die Opposition nicht sonderlich ab. Die Grünen haben nach ein paar Jahren Abwesenheit vom Katzentisch der Regierenden nun auch Bürgerrechte wieder als Thema entdeckt. Allerdings mangelt es an Glaubwürdigen in ihren Reihen, denen man sowohl inhaltliche Kompetenz als auch Charisma unterstellen könnte. Bei den Linken sieht es nicht viel besser aus. Die Berliner Lokalfraktion arbeitet sogar aktiv mit am Ausbau des Überwachungsstaates mit brachialem Polizeigesetz und Schülerzentraldatei.

War da noch was? Achja, die FDP: Bei Burkhard Hirsch und Gerhart Baum muß man sich ob ihrer Beharrlichkeit in Sachen Gang nach Karlsruhe bedanken. Der Rest der „Liberalen“ übt sich dagegen wie immer im Fönfrisurentragen und sieht dabei reichlich alt aus. Dazu gehört seit neuestem auch Sabine Leutheusser-Schnarrenberger, die einmal mehr bewiesen hat, daß Macht korrumpiert. Im trojanergeilen Bayern überrascht das aber weniger als in anderen Regionen der Welt. Immerhin scheinen wenigstens die Jugendorganisationen der Parteien schon in der Jetztzeit angekommen zu sein und sprechen sich gemeinsam gegen das

BKA-Gesetz aus. Mal schauen, ob sie sich noch an ihre Ansichten von früher erinnern, wenn sie dereinst in der Nähe des Kanzleramtes sitzen. Andrea Nahles läßt grüßen.

Zunehmende Nervosität, Unsicherheit, eine intensive Defensivhaltung und geradezu ideologische Verbohrtheit kennzeichnen mittlerweile die Argumentation der „Sicherheits"fanatiker. Seit kurzem wird andauernd mit der These argumentiert, daß „die Bürgerrechtler da" nur das Ziel hätten, Angst und Verunsicherung zu schüren. Yeah, right. Wir haben ja auch sonst nichts zu tun... Aber alleine, daß die führenden Innenpolitiker des Landes bei öffentlichen Veranstaltungen akribisch auf ihre Fingerabdrükke an Gläsern und Tassen aufpassen, erfüllt uns mit Stolz und etwas Häme. Diese Art Verunsicherung schüren wir doch gerne. Das biometrische Sammelalbum von Problempolitikern wird natürlich weitergepflegt (Datenspenden, auch genetische, sind herzlich willkommen), Updates gibt es in einer der nächsten Ausgaben.

Seit längerem betreibt der CCC – aus dem simplen Grunde, zumindest die Chance zu haben, die oben aufgezählten Spaten auch auf demokratisch korrektem Wege in die Produktion schicken zu können – eine Kampagne gegen den automatisierten Wahlbetrug, hierzulande euphemistisch „Wahlcomputer" genannt. In den USA hat es nur acht Jahre gedauert, bis die überwältigende Mehrheit der Wahlbevölkerung auch für die ausgefuchstesten Betrugsschemata zuviel wurde. Die Niederlande ist im Laufe des Jahres aus vernünftiger Einsicht zur Papierwahl zurückkehrt. Nur in Deutschland geht es zu wie in einer rumänische Bergdorfdisko: Die peinlichsten Trends schwappen um Jahre zu spät und dann mit unaufhaltbarer Wucht über das Land, bis am Ende wieder nur die allerletzte Hoffnung bleibt, das Bundesverfassungsgericht wusche den übereifrig modernitätsheischenden Lokalbratzen die Rübe. In Brandenburg konnte man es jüngst live besichtigen: Selbst nach über einem Jahr Computerwahldebatte entschlossen sich ein paar abgelegene märkische Sumpfdörfer zum erstmaligen Erwerb der Nedapschen Risikowahlcomputer. Wir harren sehnsüchtig der Entscheidung aus Karlsruhe und hoffen, daß nicht noch mehr Steuergelder in unförmiger Hollandblech-Althardware versenkt wird.

Ein besonderes Highlight dieser Ausgabe aus der Rubrik „Bürger beobachten Geheimdienste beim Dilettieren" ist eine ausführliche Darstellung zu den IP-Netzen des Bundesnachrichtendienstes. Natürlich fragt sich der geneigte Leser, wie jemand klaren Geistes auf die Idee kommen kann, eine für ihr Versagen im Industriemaßstab weithin gerühmte Firma wie T-Systems mit der Betreuung der Netze des deutschen Auslands"geheim"dienstes zu beauftragen. Wir hatten zwischenzeitlich schon Furcht, daß die Welt nicht von einem schwarzen Loch am LHC, sondern von einer Inkompetenz-Singularität in Pullach vernichtet werden könnte. Es bleibt zu nur hoffen, daß da ein paar Spezialexperten demnächst auf Jobsuche sind. Vielleicht wäre ja Trainer für Bauchatmung ein angemessenes Betätigungsfeld.

Überhaupt, die Telekom. T-Systems ist nun nicht der einzige Konzernbereich, der dieses Jahr durch großzügige Informationsweitergabe und eine dermaßen schlechte Presse auffiel, daß eine neue nach unten offene Mielke-Skala geschaffen werden muß. Der Konzerngeheimdienst T-Com glänzte durch präzise und umfassende Problemkunden-Aufklärung. Ehrlicherweise bezeichnet die Telekom selbst in ihrem Datenschutzportal den hausgemachten Skandal nur leicht beschwichtigend als „Bespitzelungsaffäre". Laut Informationen des Nachrichtenmagazins „Titanic" hat sich der Telekom-Chef René Obermann ausweislich seiner Verbindungsdaten inzwischen persönlich bei den bespitzelten Journalisten entschul-

digt und Maybrit Illner danach jeweils Bericht erstattet.

Die eigentlich für Olympia-Berichterstatter aus der „freien Welt“ gedachten Freedom-Sticks, die der CCC im Sommer dieses Jahres zu tausenden verteilte, werden wir nun an deutsche Internetnutzer ausgeben müssen. Was in China schon nicht funktionierte, soll hierzulande nämlich in reverser Transrapidlogik Bürger vor schädlichen Einflüssen wie ausländischen Lottoanbietern, feindlich-negativer Propaganda, der Konterkulturrevolution und anderen gesellschaftlichen Problembereichen, für die unsere Politiker keine sinnvollen Antworten mehr haben, behüten.

Unserer prima Familienministerin Ursula von der Leyen würden wir gerne die Anleitung für das Internet zukommen lassen; bedarfsweise auch in ausgedruckter Form, zur entspannten Lektüre beim Kinderwagenschieben. Vielleicht ist ja ihr zahlreicher Nachwuchs helle genug, Mama mal zu erklären, wie das mit dem Internet so funktioniert und wieso ein kleines bißchen Zensur genauso gefährlich ist wie die chinesische Lösung. Wenn sie so weitermacht, bleibt uns allerdings nur noch, ihr statt Dummheit Bösartigkeit zu unterstellen. Zum allgemeinen Demokratieverständnis der Regierung würde das hervorragend passen. Ob da mit Bildung und Erziehung noch was zu reissen ist, darf bezweifelt werden.

Aus ‘Schland kommen nicht nur Internetausdrucker, sondern auch Häusle-Beblinker, und deshalb sind wir stolz, unserem Team Blinkenlights aus der Heimat nach Toronto zuzurufen: Volldampf voraus! Was uns sofort zum Thema Congress bringt, zu dem wir unter dem Motto „Nothing to hide“ auch nach diesem Weihnachten wieder die familien(ministerinnen) geplagten Hacker, Cracker, Phreaker und Bastler einladen, sich von der R(0)ute im localhost zu erholen. Zum nunmehr 25. Mal gibt es die gemessen höchste Nerddichte der Welt – noch vor dem MIT, dem Cern und allen CSU-Ortsvereinen. Das Programm ist dichtgepackt mit großartigen Vorträgen und Workshops und hat das Potential, Wissen, Motivation und Energie für das nächste Jahr im Überfluß zu geben.

Und was wünschen wir uns und euch fürs neue Jahr? Daß ihr verschont bleibt von Verfolgung durch den Hackerparagraphen, von erweiterter Vorratsdatenspeicherung, biometrischen Datenzentrallagern und anderen Personenkennzifferprojekten inklusive Schülernumerierung, Internetzensur, Spionagedrohnen, Wahlcomputern und klagewütigen Wahlstift-Herstellern. *<die redaktion>*

Inhalt

Geleitwort/Inhalt	1
Impressum	4
Leserbriefe	5
WTF is BVOE?	9
Die Welt von morgen: Spreading Democracy	18
Secure Instant Messaging — am Beispiel XMPP	20
Software Distribution Malware Infection Vector	32
Angriffsszenarien auf Microsoft Windows	34
Chinesewall — Internetzensur gibt es nicht nur in China	38
Ronja	39
Das Chipkartenbetriebssystem ECOS	41
21th century digital bikes	43
Atomare Datenkrake	47
Capture the Flag in der IT-Sicherheit	52
Easterhegg 2008	54
Gedanken zum elektronischen Personalausweis	56
slashdot-netstatistik	59
Im Umfragetief	60
14 Years of starting a hacker scene in brazil	62
UniHelp	64
Netsecurify	68

Erfa-Kreise / Chaostreffs

Bielefeld, CCC Bielefeld e.V., Bürgerwache Siegfriedplatz,
freitags ab 20 Uhr *http://bielefeld.ccc.de/ :: info@bielefeld.ccc.de*

Berlin, CCCB e.V. (Club Discordia) Marienstr. 11, (✉ CCCB, Postfach 64 02 36, 10048 Berlin),
donnerstags ab 17 Uhr *http://berlin.ccc.de/ :: mail@berlin.ccc.de*

Bremen, CCCHB e.V., Sophienstraße 6, 28203 Bremen, (✉ CCCHB e.V., Hauffstr. 11, 28217 Bremen),
jeden 2. Dienstag *http://www.ccchb.de/ :: mail@ccchb.de*

Darmstadt, chaos darmstadt e.V. TUD, S2|02 E215,
dienstags ab 20 Uhr *https://www.chaos-darmstadt.de/ :: info@chaos-darmstadt.de*

Dresden, C3D2/Netzbiotop e.V., Lingnerallee 3, 01069 Dresden,
dienstags ab 19 Uhr *http://www.c3d2.de/ :: mail@c3d2.de*

Düsseldorf, CCCD/Chaosdorf e.V. Fürstenwall 232, 40215 Düsseldorf,
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, Lokstedter Weg 72, 20251 Hamburg,
2. bis 5. Dienstag im Monat ab etwa 20 Uhr *http://hamburg.ccc.de/ :: mail@hamburg.ccc.de*

Hannover, Leitstelle 511 e.V., c/o Bürgerschule Nordstadt, Schaufelder Str. 30, 30167 Hannover,
jeden 2. Mittwoch und jeden letzten Dienstag ab 20 Uhr *https://hannover.ccc.de/ :: kontakt@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., Vogelsanger Straße 286, 50825 Köln,
letzter Donnerstag im Monat ab 20 Uhr *https://koeln.ccc.de :: mail@koeln.ccc.de*

München, CCC München e.V., Balanstraße 166, 81549 München,
jeden 2. Dienstag im Monat ab 19:30 Uhr *https://muc.ccc.de/ :: talk@lists.muc.ccc.de*

Ulm, Café Einstein an der Uni Ulm, montags ab 19:30 Uhr *http://ulm.ccc.de/ :: mail@ulm.ccc.de*

Wien, Metalab, 1010 Wien, Rathausstraße 6, jeden Freitag ab 18 Uhr *http://www.metalab.at/*

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, Basel, Bochum, Bristol, Brugg, Dortmund, Frankfurt am Main, Freiburg im Breisgau, Gießen/Marburg, Hanau, Heidelberg, Ilmenau, Kiel, Leipzig, Mainz, Mannheim, Mülheim an der Ruhr, Münster/Osnabrück, Offenbach am Main, Paderborn, Regensburg, Rheintal in Dornbirn, Stuttgart, Trier, Weimar, Wetzlar, Wuppertal, Würzburg, Zürich.

Zur Chaosfamilie zählen wir (und sie sich) die Häcksen (*http://www.haecksen.org/*), den FoeBuD e.V. (*http://www.foebud.org/*), den Netzladen e.V. in Bonn (*http://www.netzladen.org/*) und die c-base Berlin (*http://www.c-base.org/*).

Die Datenschleuder Nr. 93

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 Dirk Engling *<erdgeist@erdgeist.org>*.

Chefredaktion
46halbe und erdgeist

Layout
evelyn, hukl, erdgeist

Redaktion dieser Ausgabe
Gismo, Tim Blazytko, Derneval Cunha, erdgeist, Hans-Christian Esperer, codemonk, Felix Gröbert, Martin Haase, Pallas, Johann Kleinbrenn, Karel Kulhavy, 46halbe, 0042, Philipp Fabian Benedikt Maier, Hannes Mehnert, gøph3r, frank, Frank Rosengart, Markus Schneider, 0023, Martin Wisniowski

Betreff: Bundes-Einbruchs-Trojaner

Nach Einbruch manipulierte Rechner stehen zur Ihrer näheren Untersuchung bereit!

Ab 2001 machte ich auf die damals geheimgehaltene Erforschung und Anwendung von Mikrowellen-Waffen gegen Personen aufmerksam, die jetzt besser bekannt ist.

Bald wurde versucht mich mundtot zu machen. Es wurde auch in meine Wohnung und das Haus meiner Lebensgefährtin (fast) unauffällig mehrmals eingebrochen. Gestohlen wurde nichts, aber die Computer funktionierten danach als wäre die Software plötzlich in mehreren Einstellungen verändert usw. Emails wurden sogar inhaltlich manipuliert. Auch mein Handy, das in meiner Wohnung zur Zeit der Einbrüche war, konnte danach abgehört werden.

Die zwei manipulierten Rechner und das Handy sind noch vorhanden. Falls Sie oder andere neutrale Fachleute auf dem Gebiet diese mal näher untersuchen möchten, ist dies möglich!

Aus Sicherheitsgründen bitte ich um eine kurze Eingangsbestätigung dieses Emails. <*Herr M.*>

Ist angekommen. <erdgeist>

Kein Scherz, die Firma Lidl schreibt uns:

Guten Tag, wir haben Ihre Veröffentlichung zum Thema „Skandal: Schäubles Finger falsch“ gelesen. Das von Ihnen abgedruckte Zitat

„Wir haben den veröffentlichten Fingerabdruck [...], teilte ein Firmensprecher des Lebensmitteldiscounters LIDL am späten Sonntag Abend mit“

entspricht weder den Tatsachen noch stehen wir mit diesem Fakt in irgendeinem Zusammenhang. Wir möchten uns unmißverständlich von dieser Aussage Ihrerseits distanzieren und bitten Sie daher, diese Passage umgehend von Ihrer Seite zu nehmen. <*Freundliche Grüße Lidl Stiftung & Co. KG Petra Trabert Presse + Medien*>

Sehr geehrte Frau Trabert, der Chaos Computer Club hat auf seiner Internetpräsenz http://www.ccc.de/ keinerlei Statement veröffentlicht, welches das von Ihnen erwähnte Zitat verwendet. Vielmehr steht in der aktuellen Pressemitteilung zu lesen, daß der Fingerabdruck von Herrn Schäuble tatsächlich echt ist. (Siehe: https://www.ccc.de/updates/2008/schaubles-finger?language=de)

Wir haben derzeit weder Zugriff auf Ihre Kundendatenbank noch Kontakt mit einem Lidl-Firmensprecher.

Wir möchten Ihnen nahelegen, einen Fortbildungslehrgang für die Benutzung des Internet zu belegen, denn wie leicht herauszufinden war, stammt die Behauptung von der Satire-Webseite „Frankfurter Magazin“:
http://www.frankfurter-magazin.de/?p=294

Vielleicht empfiehlt sich auch eine Image-Kampagne, da der Ruf des Unternehmens Lidl in Bezug auf den Datenschutz offenbar optimierbar ist. Alternativ könnten Sie sich auch entschließen, das Ausspähen Ihrer Kunden und Mitarbeiter zu beenden.

Mit freundlichem Gruß <46halbe>

GEGENDARSTELLUNG

In der DS #89 heißt es im Artikel “Update fürs Herkunftswörterbuch” zu Slashdot, es sei vom Deutschen “schlag tot” abgeleitet.

Auf dem Linux Tag 2001 hat Rob Malda, der Gründer von Slashdot, den Namen allerdings ganz anders erklärt. Sinngemäß sagte er:

“Auch wenn viele das denken, Slashdot ist keine Anspielung auf Dotfiles oder die häufige Verwendung von ‘./’ unter Unix. Es ist viel blöder, als Ihr denkt, nämlich ein einfaches Wortspiel, ein Zungenbrecher. Denn wer kann das schon schnell aussprechen: ‘http:///..org’?” [auf Englisch natürlich]

Die Ableitung aus dem Deutschen hat er mit keinem Wort erwähnt. <*Chris*>

Unser Fingerabdruckkopieren-Video macht auch international Eindruck

Mr frank i see your film on youtube...that was really interesting about fake fingerprint.. is there a real you can fake your fingerprint? so how long can i fake my fingerprint? is there just a few days or forever? and can the police see or understand i fake my fingerprint? after faking my fingerprints what tels the fingerprint? i need more information about fingerprint and how this stuff works ? i can pay money if this is reall.. thanks <*waryaa*>

Dear Mr Waryaa, MY MAIL MAY COME TO YOU AS SURPRISE. I AM REPRESENTATIVE OF CCC ORGANIZATION FROM GERMANY. OUR PRODUCTS GUARANTEE ENLARGEMENT OF NUMBER OF FINGERPRINTS FAKE! FOR MORE INFORMATION CONTACT AT <scam@ccc.de>

Der Freund vom Heinz schreibt:

Guten Tag Liebe Leute vom CCC. Ich habe einen Frage im Betreff Email. Seit fast einem Jahr bekomme ich von einer Person aus dem Internet benachrichtungen das er Emails erhält die auf mich Adressiert sind. Danach haber ich Passwörter und eingangsdaten geändert. Auch meinen Anbieter benachrichtig, der mir lapida mitteilte das es wohl nicht an ihm liegen würde. Auch die Person hat sich bei free gemeldet, auch ihm haben sie nur eine nichts Aussagefähige Antwort geschrieben. Mein Pc ist durch eine Hardwarefirewall und eine Softwarefirewall gesichert, dazu habe ich auch neuste Antivirus,antipishing,usw auf dem Rechner.

Das Problem bleibt bestehen, und die Person schrieb mir wieder mal , das er wohl diverse Softwarepasswörter vom mir besitzen würde, und die auch benutzt. Ich habe keine Ahnung wie ich mich noch da gegen schützen kann. Das er meine Daten mißbraucht!!! Auch eine weitere Email Adresse die ich habe , auch von dort bekam er meine Emails.

Ich hoffe das ihr mir irgendwie helfen könnte wie ich noch vorgehen kann, oder mir hinweise geben könntet wo ich hilfe bekomme. Auch scheint seine Personendaten vom ihm selber angegeben nicht zu stimmen. <*Norbert*>

PS-hallo heinz liest du wieder mit????

DU SPINNER!! Dein Heinz

Nicht schreiben solltet ihr, wenn...

Hallo, ich möchte euch nicht lange aufhalten und habe auch schon die FAQ gelesen(haben geholfen). Meine Frage: Ich möchte endlich weg vom Scriptkiddie status und echter Hacker werden und möchte deswegen programmieren lernen, nur weiß ich nicht mit welcher Sprache ich anfangen soll ??? Bitte um eine nützliche Antwort, denn die ist in fast allen Foren icht zu erwarten. Danke für eure Zeit <*Marco*>

Deutsch <erdgeist@46halbe>

Schleichwerbung... 4 Freikarten gibt's unter ds@ccc.de

Sehr geehrter CCC, wenn Sie die Umstände einer Singlebörse testen möchten, versuchen Sie einfach mal den Harzflirt. Über ein Ergebnis würden wir uns sehr freuen. Hochachtungsvoll C.M. Antolic

Sehr geehrter Herr Antolic, herzlichen Dank für Ihr Angebot, die „Harzflirt"-Singlebörse kostenlos zu testen. Ich möchte Ihnen jedoch mitteilen, daß unsere Mitglieder entgegen den üblichen Vorurteilen gegenüber Computerfreaks durchaus in der Lage sind, ihre Lebens- und Sexualpartner „in real life" zu suchen. Viele Grüße, <Frank Rosengart>

Ehrliche Finder

Sehr geehrte Damen und Herren, ich beziehe mich auf die aktuelle Ausgabe der Datenschleuder.

Als ordentlicher deutscher Staatsbürger stehe ich dem Diebstahl grundsätzlich ablehnend gegenüber. Wie mir über die Medien bekannt geworden ist, haben Sie Herrn Innenminister

Wolfgang Schäuble seine Fingerabdrücke entwendet.

Ich fordere Sie daher auf, dem Innenminister umgehend seine Fingerabdrücke zurückzugeben. Bitte übersenden Sie diesbezüglich dem Innenministerium eine kostenlose Ausgabe der Datenschleuder, die die Fingerabdrücke mitsamt Vorlagen enthält.

Ich gehe davon aus, daß die Entwendung der Fingerabdrücke unabsichtlich erfolgte, weil derzeit völlig unklar ist, ob Daten nun gestohlen werden können oder nicht. Ich verweise auf meine an das Bundesinnenministerium übersandte Email. **[Kopie lag bei – die Redaktion.]**

Bei Rückgabe der Fingerabdrücke hätten sich juristische Schritte seitens des Bundesinnenministeriums dann sicherlich erledigt. <*Bönisch*>

Wir können versichern, daß wir dem BMI den Fingerabdruck mit Zinsen zurückerstattet haben.

Ferner wurden mehrere tausend Sicherheitskopien bei vertrauenswürdigen Bürgern hinterlegt, sollte das Original im Ministerium bei einem Brotschneideunfall verlorengehen. <erdgeist>

Was so ein MCSE wert ist...

Hallo liebe Freunde, seitdem ich bei Euch Mitglied geworden bin und beim foebud so ein lustiges T-Shirt bestellt habe, ist mein PC Angriffen ausgesetzt:

```
IP-Adresse des Angreifers: 224.0.0.252
Protokoll: UDP
Anwendung: svchost.exe
Lokaler Port: alle 65.536 Ports werden systematisch seit Sonntag, 13.01.2008 durchprobiert!
Richtung: -> (ausgehend)
Entfernter Host: 224.0.0.252
Entfernter Port: llmnr(5355) link local multicast name resolution
```

Ich vermute ganz stark, dass hier irgendwelche Überwachungsbehörden am Werk sind.

Deshalb meine Frage an Euch: könnt ihr mir zu dieser statischen IP-Adresse irgendetwas sagen? <*Dipl.-Kfm. (FH) XXX. Microsoft Certified Systems Engineer*>

Eingedenk solcher Anfragen fürchte ich, Schäuble hat erreicht, was er wollte. <erdgeist>

Spiegel-Cover-Star

Nicht schlecht gestaunt

haben wir, als wir die Fotostrecke zum Test eines Fotoapparats der Firma Panasonic auf Spiegel Online, *http://www.spiegel.de/netzwelt/tech/0,1518,590135,00.html* gefunden haben.

Das Makro wurde offensichtlich mit einem uns sehr vertrauten Motiv getestet. Die Fotostrecke findet ihr unter *http://www.spiegel.de/fotostrecke/fotostrecke-37086-4.html*

Die Mail zum Sonntag

Ich hab gerade von Jesus gemeint bekommen, daß man wohl doch was tun kann gegen Pornografie im Netz, weil jeder weiß (wie ich hoffe), was das für Zeug ist.

Frauen werden gezwungen Sex mit Männern zu haben, die nicht die ihren sind, vergewaltigt, eingesperrt, gefoltert, unter Drogen gesetzt und erpresst und auch deren Angehörigen. Welche Mittel gibt es das zu unterbinden?

Ich habe bereits eine Mail an die Polizei geschrieben, daß Jesus meint, daß Prostitution und Pornografie genau das sind, was es vermutet zu sein. Die Inhalte dazu habe ich oben geschildert, alles andere ist die Angst vor Schlimmerem und der Lügen, die daraus entstehen und:

Du sollst nicht begehren deines Nächsten Haus noch Weib. (noch Mann). *Das scheint in jeder wahrhaften Religion als Grundsatz zu stehen.*

Ich kann so was leider nicht selbst rausprogrammieren, aber was sollen die ganzen Bilder und Vids im Netz? Was sagt Ihr dazu? Kann man da nicht was machen?

In meiner Vorstellung war vorhin der Gedanke, wenn diese Sachen einfach nicht mehr da wären, sozusagen in die große Löschmaschine geschluckt werden ein guter. Der Gedanke hat mir nicht wehgetan. Nur die Frage, ob das alles Rechtens ist, ob das alles Rechtens sein darf? So wäre es doch nur die Angst vor den Anderen, die dieses Handeln vorzubringen wissen wollen. Alles andere müßte jeder dieser Leute als Übel und Böses erfahren haben..das Mannsbild, das sich nicht mehr selber weiß..vor lauter Mannsseins..eine Frau wird im Bewußtsein des Geschenkes der Geburt von Gott wohl kaum außerhalb von Furcht in der Lage sein anderes zu behaupten, behaupten zu wollen..oder haben diese Menschen (Männer) vor lauter Lüge, vor lauter Geld sich selber, ihre Mütter vergessen? Die anderen..die, die selber nicht gesehen haben, was das eigentlich ist, derer einer war ich selber und kann mich dafür nicht sonderlich leiden, daß ich so lange gebraucht habe das zu erkennen, daß das nicht einfach nur Bilder sind. Ich schäme mich dafür.

So what to do? In Namen Jesu, in meinem Namen und im Namen Gottes, macht was draus. Wir alle sind daran beteiligt, daß der Staat, wie er in der Bibel steht, wie er auch vermutlich in jeder anderen wahren Religionsauslegung steht etwas gutes wird, etwas zum Mitmachen ist. Die Zehn Gebote heiligen, die geheiligten Zehn Gebote ernst nehmen..auf die Engel verweißen und darauf, daß staatliche Grenzen in der Wahrung unseres Glaubens, unseres Glaubens, den uns Gott geschenkt hat unsere Erde verlassen können.

Gegen Waffen, gegen ein Aufschieben von Abrüstung des Geldes wegen, gegen Folter, Prostitution, Pornografie und Gewalt, gegen die Verbreitung von Angst.

In all meiner Liebe,im Vertrauen auf Gott und seinem wiedergeborenen Sohne Jesus Christus, *<Thomas S.>*

Vielleicht solltest Du besser darüber mit (D)einem Pfarrer sprechen. <padeluun>

Da die Mail in Cc: auch an information@bundesnachrichtendienst.de ging, bin ich sicher, daß sich schon jemand darum kümmert. Vielleicht erklärt dies auch das plötzliche Erwachen der Frau von der Leyen. <erdgeist>

DAS ist mal ein Kessel

WTF is BVOE?

von 0023 und 0042 <ds@ccc.de>

Mit der Veröffentlichung der oder einiger IP-Netzbereiche des Bundesnachrichtendienstes im November 2008 auf wikileaks.org [WL08] und der dadurch ausgelösten Befassung diverser Blogs mit diesen Netzen sind diese einer breiteren Öffentlichkeit bekanntgeworden. Um weitere Erkenntnisse in die Diskussion einzubringen, möchten die Autoren aus gelegentlicher, aber über mehrere Jahre andauernder Beobachtung berichten.

Diese Netzbereiche existierten teilweise seit zehn Jahren. Das ist nicht weiter verwunderlich, schließlich ist der BND ein Nachrichtendienst, und Nachrichtendienste leben von Informationen. Daß der BND im dritten Jahrtausend auch am Internet teilnimmt, ist ergo selbstverständlich. Merkwürdig daran ist hingegen, daß diese Netze bei gezielter Suche problemlos gefunden werden konnten. So leicht, daß die Autoren lange Zeit von einer Veröffentlichung absahen, weil sie die Netzbereiche für einen sogenannten Honigtopf [Provos] hielten.

Für die Vergabe von IP-Adreßbereichen im europäischen Raum ist das RIPE-NCC [RIPE-NCC] verantwortlich. Diese Organisation führt eine Datenbank, in der zugewiesene Netzwerke eingetragen sind. Das ist in etwa mit einem Handelsregister für Firmen vergleichbar, nur eben für Netzwerke. Die Autoren wurden 2003 auf die erwähnten Netze aufmerksam. Eine Suche in Kopien der RIPE-NCC-Inetnums (den Netzobjekten der Datenbank) [RIPE] etwa in den Jahren 2003/2004 nach „Pullach" erbrachte unter anderem das Netzwerk BVOE-MANAGEMENT--PULLACH-NET mit der Beschreibung „BVOE Management". Neben Netzen einer bekannten Autovermietung aus Pullach und einigen mittelständischen Unternehmen fand sich eine Vielzahl weiterer Netze mit dem kryptischen Namen „BVOE" und der Beschreibung „TSI fuer LVP". Die Anzahl der Netze war auffällig hoch, und eine Suche im Internet nach diesen Kürzeln brachte demgegenüber recht wenig zutage. Weitere Netznamen wie LVP-INFO-BROKING-NETWORK werteten wir als weitere Indizien dafür, daß die Netze vom BND genutzt werden – bereits der Gründer des Dienstes, General Reinhard Gehlen, legendierte sich als Patenthändler. Das älteste Netz, welches in den Daten der RIPE-NCC zu finden war, war das bereits genannte LVP-INFO-BROKING-NETWORK. Ende 1997 wurde es durch Mitarbeiter der Deutschen Telekom AG eingerichtet. 2004 wurde es in BVOENET4 umgenannt.

Wir haben damals umfangreich Telefonbücher und das Internet durchsucht, um Verbindungen zwischen den Netzen und dem BND herzustellen und unsere Hypothese vom Honigtopf zu bestätigen oder zu widerlegen. Die Netzwerke, die vom Namen her auf die Bundesstelle für Fernmeldestatistik wiesen, existierten noch nicht. Im Jahre 2003 war uns auch noch nicht bekannt, wofür LVP steht. Wir sind zwar auf

Idylle am Lage- und Informationszentrum

das „Betreuungswerk D. LVP Pullach" gestoßen, das als Tennisverein aufgelistet wurde. Außer der Postfachadresse 20 04 31 in 80004 München und einer Telefonnummer aus Pullach gab es dazu jedoch keine weiteren Informationen. TSI hingegen, so wurde uns gewahr, war das Kürzel der T-Systems International GmbH – der Großkundentochter der DTAG.

Die Eintragungen in der RIPE-Datenbank waren von betonter Unauffälligkeit und paßten ins Bild. Es stellte sich nunmehr die Frage, ob diese Netze nachweisbar dem BND zuzuordnen seien. Das Dokument auf *wikileaks.org* nennt zu den Netzen aus dem „Projekt BVOE für die LVP" ein Netz der Fernmeldestelle Süd. Damit ist die Fernmeldestelle Süd der Bundeswehr in Gablingen gemeint. Bis 1994 wurde die dortige Wullenweber-Anlage als Field Station Augsburg vom amerikanischen Militär als SIGINT-Station genutzt. Der BND durfte die Anlage mitbenutzen [W07]. Seit dem Auszug der amerikanischen Streitkräfte 1994 ist der BND Betreiber der Anlage unter dem Decknamen „Drehpunkt", auch wenn die Fernmeldestelle Süd namentlich als Bundeswehreinrichtung ausgewiesen wird.

Trotz des Machtkampfes zwischen BND und Bundeswehr, der in der Auflösung des Zentrums für Nachrichtenwesen der Bundeswehr (ZNBw) und damit der weitgehenden Unüberprüfbarkeit von BND-Meldungen gipfelte [Richter], tarnt sich der BND weiterhin unter Bundeswehrlegende. So werden alle beim BND eingesetzten Soldaten formal in das Amt für Militärkunde (AMK) versetzt [Juretzko]. Darüberhinaus gibt es eine Parallele zum Augsburger Fall, in der von den amerikanischen Streitkräften aufgegebenen Satellitenabhörstation der National Security Agency (NSA) in Bad Aibling, die heute vom BND unter der Tarnbezeichnung „Fernmeldeweitverkehrsstelle der Bundeswehr" (FmWVStBw) – Deckname Seeland – betrieben wird.

LVP ist das Kürzel der Liegenschaftsverwaltung Pullach. Entsprechend benannte Netze, beispielsweise LIEGENSCHAFTSVERWALTUNG-PULLACH-PULLACH-NET [sic!], das etwa zwischen 2005 und 2007 existierte, hatten als administrativen und technischen Ansprechpartner Gerhard Zucht eingetragen. Dessen Personeneintrag wies die Adresse der Liegenschaftsverwaltung Pullach in der Heilmannstraße 30 aus. Das ist auch die offizielle Anschrift der Zentrale des Bundesnachrichtendienstes.

Das Netz mit dem Namen BVOENET hieß vor Januar 2007 BUNDESSTELLE-FUER-FERNMELDESTATISTIK-GAUTING-NET. Die Bundesstelle für Fernmeldestatistik ist seit Jahrzehnten die Legendierung für die (bisherige) Abteilung 2 des BND. Diese BND-Abteilung betreibt technische Aufklärung. Die Zentralstelle der Bundesstelle für Fernmeldestatistik – Deckname Stellwerk – ist in der Wanneystraße 10 in Stockdorf, einem Ortsteil der Gemeinde Gauting. Es besteht kein Zweifel, daß diese Netze vom Bundesnachrichtendienst verwendet wurden.


Lage- und Informationszentrum

Sämtliche Personen aus den Personenobjekten, so vermuten wir zumindest, sind Telekom- bzw. T-Systems-Mitarbeiter, auch wenn sie etwa mit „BVOE Management" beschrieben sind. Für Gerhard Zucht ist zwar als Adresse die LVP in der Heilmannstraße angegeben, Mailadresse und Telefonnummer stammen aber von T-Systems.

Das Postfach 80 01 03 in 81601 München gehört der Deutschen Telekom AG. In der Sonnenstr. 24-26 in 80331 München befindet sich eine Geschäftskundenniederlassung der DTAG sowie eine Filiale der Deutschen Post AG.

Bis zur Austragung der Netze aus der RIPE-NCC-Datenbank konnten wir zuletzt etwa drei Dutzend registrierte IP-Adreßbereiche ausmachen, die in bundesweit verteilte Ballungszentren geroutet wurden. Die Anzahl der Netze wuchs stetig. Die Netzwerke BVOENET26 bis BVOENET28 wurden sogar erst binnen der letzten drei Monate eingerichtet. In den letzten Jahren gab es einige Abschaltungen, Umbenennungen und kleinere Konfigurationsänderungen.

Zu diesen ominösen BVOE-Netzwerken gibt es eine passende Domain: *bvoe.de*. Herbert Schunk ist dafür als administrativer und technischer Ansprechpartner eingetragen, ebenso wie für diverse BVOE-Netze.

Ein weiterer Ansatz für die Recherche nach den BVOE-Netzen bildeten die IP-Adressen aus den gefundenen Bereichen. Wenn man Google mit einer IP-Adreßnummer in Anführungsstrichen befragt, zeigt es Seiten, in deren Text die IP-Adresse steht. Für nur wenige IP-Adressen aus diesen Netzen findet man auch Einträge im WWW. Bei der Beurteilung der Ergebnisse muß man darauf achten, ob die IP-Adressen auch wirklich einem der BVOE-Netze zuzuordnen sind. Es kann z. B. sein, daß das BVOE-Netz bereits abgemeldet wurde und lediglich dessen Nachmieter elektronische Spuren im Web hinterlassen hat. Die Suche nach IP-Adressen bringt Foren-Postings, Hostnamen und IP-Adressen in Mail- und NNTP-Headern und unzählige Zugriffszähler und Webserver-Logfiles ans Licht. Webseiten aus allen Teilen der Welt wurden aufgerufen, darunter natürlich auch einige aus dem nahen und mittleren Osten.

Anhand von Zugriffsstatistiken, dem Wikipedia-Scanner und angezeigten IP-Adressen aus Webforen konnten wir feststellen, daß Webseitenabrufe von 62.156.187.234 (*www1-1.bvoe.de*, BVOENET5, München), 195.243.248.226 (*www2-1.bvoe.de*), 195.243.248.228 (*www2-2.bvoe.de*), 195.243.248.231 (BVOENET10, Berlin) und 217.89.74.221 (BVOENET13, Frankfurt) erfolgten. Von *www1-2.bvoe.de* (62.156.187.236) sind uns keine Zugriffe auf das WWW aufgefallen. Es ist vorstellbar, daß www1-2 und www2-2 als Ersatzgateways dienen.

Bei der Recherche stellten wir fest, daß die Aktivitäten aus den Netzen nicht unbemerkt blieben. So schrieb im August 2005 ein User proc113:

I wondered if anybody had any information regarding massive use of their sites from this domain, usually from www1-1 or www2-1.bvoe.de. When I search google (or any other major engines) to track who he might be, I get a number of live awstats traffic reports that other people have left open.

It doesn't appear to be anything terribly malicious, but he is taking an incredible amount of bandwidth (in comparison to our regular traffic). Of the 6gb of monthly traffic for regular web users, he is taking half, regularly, almost always in the late night/early morning time.

Does this seem familiar to anybody else? Is it a spider, or something different? Any advice? [Pro5]

Im April 2006 schrieb ein Fred:

Yesterday's outage was courtesy of bvoe.de (195.243.0.0/16 and 62.156.0.0/15), in Munich, who decided to send a continuous stream of queries to Thugburg for Abu Musab Zarqawi. Give them a big ~~finger~~ hand. Another nominee for the Richard Cranium Award. [Fro6]

Dies klingt so, als hätte der BND unausgereifte Skripte losgelassen, um Webseiten nach Informationen abzugrasen. Das ging wohl schief.

Bereits im Jahr 2000 müssen sich die Nutzer der Netze auffällig verhalten haben. Man findet unter [Cho0] eine traceroute-Ausgabe auf die Adresse 62.156.187.234 und die Frage *„Have [you] any idea where the host 62.156.187.234 is located? Drop me a line."* Die IP-Adresse gehörte damals noch zum 1998 eingerichteten LVP-

INFO-BROKING-NETWORK-2. Das Netz wurde 2004 in BVOENET5 umbenannt.

Die Adressen 62.225.71.254 (BVOENET7, Frankfurt) und 217.89.74.221 (BVOENET13, Frankfurt) fanden sich als NNTP-Serveradressen in Usenet-Postings zum Thema Ruby aus den Jahren 2004 und 2005 wieder. Die Absenderadresse der Postings verweist auf einen Mitarbeiter namens A. H. des Ionosphäreninstituts Rheinhausen. Dessen Mailadresse endet auf *@ionosinst.de*. Zu der Domain findet man via Google-Groups weitere Postings eines Mitarbeites namens M. S. zum Thema Windows. Das Ionosphäreninstitut Rheinhausen gehört zun BND. Der BND hat es in den 50er Jahren vom französischen Militär übernommen und nutzt es laut dem Geheimdienstexperten Erich Schmidt-Eenboom für die Satellitenaufklärung. [ESE93]

Eine ganze Weile fand man die Hostnamen *www1-1.bvoe.de* und *www2-1.bvoe.de* als Zeichenkette in Dateinamen, z. B.:

http://www.ind.homeoffice.gov.uk/ind/en/home/0../country_information/country_reports.Maincontent.0004.file.tmp/GGTSPU-www2-1.bvoe.de-3581-1417300-DAT/old3648.tmp

http://www.workingintheuk.gov.uk/ind/en/home/0/country_information/country_reports.Maincontent.0004.file.tmp/GGTSPU-www2-1.bvoe.de-3581-1417300-DAT/

http://www-elec.enst-bretagne.fr/equipe/berrou/GGTSPU-www1-1.bvoe.de-1689-4266501-DAT/Near Shannon Limit Error.pdf

Artikel der Wochenzeitung „Die Zeit" wurden mehrere Jahre auf dem Server *hermes.zeit.de* gespeichert. Der Webserver gab Verzeichnis-Listings aus, und auch da traten die BND-Hostnamen in Erscheinung – zwischen Dateien, die reguläre Artikel beinhalteten. Diese Verzeichnis-Links ließen sich nicht weiter öffnen. Die folgenden Links sind den Ausgaben 02/1997, 23/2004 und 43/2004 zuzuordnen:

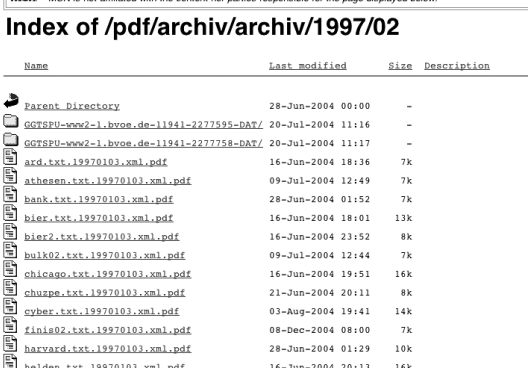
http://hermes.zeit.de/pdf/archiv/archiv/1997/02/GGTSPU-www2-1.bvoe.de-11941-2277595-DAT/

http://hermes.zeit.de/pdf/archiv/2004/43/GGTSPU-www2-1.bvoe.de-6365-1586699-DAT/

http://hermes.zeit.de/pdf/archiv/2004/23/GGTSPU-www2-1.bvoe.de-10681-3435951-DAT/

http://hermes.zeit.de/pdf/archiv/2004/23/GGTSPU-www2-1.bvoe.de-10681-3436222-DAT/

Die GGTSPU-Adresse, die *bvoe.de* enthalten, sind mittlerweile aus dem Internet verschwunden. Der nachstehende Bildschirmausdruck zeigt den Cache der MSN-Suchmaschine mit dem Stand Mai 2005. Auch wenn die Artikel einer Ausgabe aus dem Jahr 1997 zuzuordnen sind, datieren die Einträge im Verzeichnis auf Juli 2004. Unter [AO] findet man das Verzeichnis-Listing für die Ausgabe 23/2004 noch in der Wayback-Maschine von *archive.org*.



This is a version of http://hermes.zeit.de/pdf/archiv/archiv/1997/02/ as it looked when our crawler examined the site on 5 version in our index that was used to rank this page in the results to your recent query. This is not necessarily the most most recent version of this page, visit the page on the web.

msn MSN is not affiliated with the content nor parties responsible for the page displayed below.

Index of /pdf/archiv/archiv/1997/02

Name	Last modified	Size	Description
Parent Directory	28-Jun-2004 00:00	-	
GGTSPU-www2-1.bvoe.de-11941-2277595-DAT/	20-Jul-2004 11:16	-	
GGTSPU-www2-1.bvoe.de-11941-2277758-DAT/	20-Jul-2004 11:17	-	
ard.txt.19970103.xml.pdf	16-Jun-2004 18:36	7k	
athesen.txt.19970103.xml.pdf	09-Jul-2004 12:49	7k	
bank.txt.19970103.xml.pdf	28-Jun-2004 01:52	7k	
bier.txt.19970103.xml.pdf	16-Jun-2004 18:01	13k	
bier2.txt.19970103.xml.pdf	16-Jun-2004 23:52	8k	
bulk02.txt.19970103.xml.pdf	09-Jul-2004 12:44	7k	
chicago.txt.19970103.xml.pdf	16-Jun-2004 19:51	16k	
chuzpe.txt.19970103.xml.pdf	21-Jun-2004 20:11	8k	
cyber.txt.19970103.xml.pdf	03-Aug-2004 19:41	14k	
finis02.txt.19970103.xml.pdf	08-Dec-2004 08:00	7k	
harvard.txt.19970103.xml.pdf	28-Jun-2004 01:29	10k	
holden.txt.19970103.xml.pdf	16-Jun-2004 20:11	16k	

Wir nennen dies das GGTSPU-Rätsel, denn bisher konnten wir keine Erklärung finden, warum Computernamen des BNDs in Verzeichnisnamen auftreten, die auf ganz anderen Servern gehostet wurden. Das GGTSPU-Rätsel steht im Zusammenhang mit der Application-Level-Firewall namens GeNUGate der Firma Gesellschaft für Netzwerk- und UNIX-Administration mbH (GeNUA). GeNUGate ist eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach CC EAL4+ zertifizierte Firewall und wird allem Anschein nach vom BND eingesetzt. In der „Liste aktueller Patches zu GeNUGate 5.0" heißt es: „Das WWW-Relay leitete im Transferstatus GGTSPU-URLs weiter, wenn er diese nicht als selber generiert erkannte. Das

Problem ist behoben." [GG] Wahrscheinlich hat das mit den von uns aufgefundenen BVOE-URLs zu tun.

Webbrowser übertragen mitunter die Information, welche Seite der Benutzer vorher angesehen hat. So erfahren Webserver regelmäßig, mittels welcher Suchworte der Benutzer eine Seite gefunden hat. Im ungünstigen Fall werden aber auch Informationen über interne Netzwerke preisgegeben. In zahlreichen öffentlich zugänglichen Webserver-Statistiken finden sich diese sogenannten Referrer, die Nutzer aus den BND-Netzen übertragen haben, z. B.:

http://osintb.bvoe.de/Osint/pane/bookmark/BMController

http://osintb/Osint/pane/bookmark/BMController?action=changeFolderState&id=213680&open=false&currentBMUserId=V857990

http://osintb/vivisimo/cgi-bin/query-meta

http://osintb/vivisimo/cgi-bin/query-meta?v%3aproject

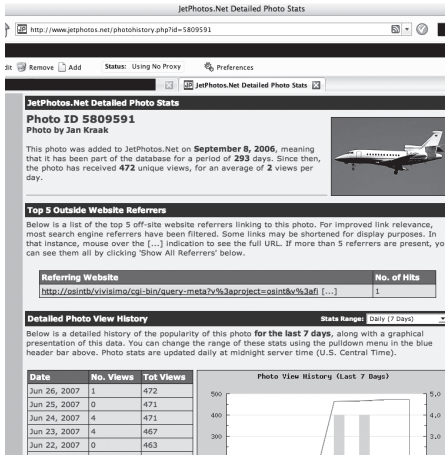
*http://osintb/vivisimo/cgi-bin/query-meta?v%3aproject=osint&v%3afile=viv_u9xKvW&&query=%22Zeman%20Flugtechnik%22&plainquery=%22Zeman%20Flugtechnik%22&num2=7020&fromdate=-1&todate=0&amindate=-30&amaxdate=-0&timeout=10000&stem=depluralize&stoplist=core&aut_*

http://srvsdm16.bvoe.de/mail/ltg.nsf/($Inbox)/D3E12332874DE4F9C125722C003928D7/

http://srvsdm16.bvoe.de/mail/ltg.nsf/($Inbox)/BBDFAB979332A773C1257218004C1D21/

Diese Referrer geben nicht nur Informationen über interne Hostnamen preis. Man kann daraus auch ableiten, was für webbasierte Softwaresysteme eingesetzt werden. Offensichtlich steht BND-Mitarbeitern Webmail zur Verfügung. Möglicherweise handelt es sich um ein IBM Lotus Domino Web Access.

Osintb ist ein Server, der den Bereich Open Source Intelligence – also der Auswertung offener Quellen, z. B. Zeitungen – beim BND unterstützen soll. Neben einer Bookmarkverwaltung ist auf dem Server ein Suchinterface für die intern verwendete Suchmaschinensoftware Vivisimo installiert. Das Suchinterface wurde laut Referrer nach „Zeman Flugtechnik" befragt. Das Ergebnis führte zu einer Seite von *jetphotos.net*.



Das im Screenshot dargestellte Foto zeigt die Dassault Falcon 900EXE mit der Registrierungsnummer D-AZEM. Die Maschine ist auf die Zeman Flugtechnik und Logistik München GmbH (HRB 148243) registriert. Laut Medienberichten handelt es sich um einen Dienst-Jet des BNDs.

Wie mittlerweile in den Medien zu lesen ist, wurden aus den Netzbereichen des BNDs Änderungen in der Wikipedia vorgenommen. Besondere Aufmerksamkeit wurde dem Artikel zum Bundesnachrichtendienst zuteil, in dem der Satz *„Außerdem ist es ein offenes Geheimnis, dass viele der Auslandsniederlassungen des Goethe-Instituts als inoffizielle Residenturen des BND dienen"* durch die Formulierung *„Auslandsniederlassungen des Goethe-Instituts dienen jedoch nicht als inoffizielle Residenturen des BND"* ersetzt wurde. [WP05] Der Geheimdienstexperte Erich Schmidt-Eenboom schreibt zur Legendierung mittels des Goethe-Instituts:

Parallel zu den offiziellen Kontakten [des BND zu Ägypten] lief die illegale Arbeit weiter. Jeweils einen hauptamtlichen BNDler orteten die Geheimdienste der Staaten des Warschauer Vertrags, die über ihre bis 1971 gewachsenen Verbindungen zum ägyptischen Dienst auch später noch über gute Kontakte

verfügten, im Deutschen Archäologischen Institut in Kairo und im Goethe-Institut. [ESE95]

Es ist also wenigstens ein Fall bekannt, in dem das Goethe-Institut als Legendierung genutzt wurde. Wir haben keine weiteren Fälle in der einschlägigen Fachliteratur gefunden. Möglicherweise rechtfertigt das nicht die ursprünglich getroffene Pauschalisierung. Die Änderung aus dem BND-Netz stimmt aber ebenfalls nicht ganz. Im allgemeinen begrüßen wir jedoch ausdrücklich, wenn BND-Mitarbeiter ihr Wissen und ihre Dienstzeit nutzen, um an der Wikipedia mitzuarbeiten.

Im Rahmen dieser Recherche sind wir auf einige Personen aufmerksam geworden, die aus den BND-Netzen das Internet benutzt haben. Die Informationen waren bzw. wären brauchbar, um Klarnamen zu ermitteln. In einem Fall stand die Vermutung im Raum, daß die betroffene Person eine Attaché-Funktion in einer deutschen Botschaft in Südeuropa übernommen hat. Wir möchten aber davon Abstand nehmen, an dieser Stelle über Mitarbeiter des BND zu schreiben.

Die vom BND genutzten IP-Adreßbereiche haben wir 2008 mit der Liste der Tor-Knoten abgeglichen. Dabei konnten wir keine Hinweise darauf finden, daß der BND eigene Tor-Knoten betreibt. Allerdings müßte selbst dem Bundesnachrichtendienst klar sein, daß für das Anzapfen von Tor-Ausleitungen besser ein Root-Server angemietet wird [CCC08].

In der Nacht vom 14. auf den 15. November sind die Netze aus der RIPE-NCC-Datenbank wohl anläßlich der Veröffentlichung auf *wikileaks.org* verschwunden. Die Autoren konnten diese Änderungen verwundert und amüsiert live mitverfolgen. Unter [WL08] haben die Betreiber von wikileaks nunmehr die Bitte des T-Systems CERTs veröffentlicht, die Datei mit den aufgelisteten Netzwerken zu entfernen.

Gleichfalls sind auch die vier Adreßbereiche zu SCHWAIGER-NET verschwunden, von denen wir lediglich die Vermutung hatten, daß sie zum BND gehörten, weil Herbert Schunk als Kontakt eingetragen war. Dafür, daß die Netze jahrelang einsehbar waren, hätte diese Nacht- und Nebelaktion auch entspannter angegangen werden können.

Wir möchten darauf hinweisen, daß sämtliche hier zusammengetragenen Informationen öffentlich sind. Das ist vergleichbar mit der Recherche in Telefonbüchern. Es bestand keine Notwendigkeit, in Computer-Netzwerke einzudringen. Am Rande ist uns der eine oder andere offene Port aufgefallen. Wir haben das jedoch nicht weiter verfolgt.

Ausgangspunkt für die Nachforschungen waren die Daten der RIPE-NCC, die auch unabhängig von den BVOE-Netzen durchaus interessant sind **(Hint!)**. Daß diese Daten brauchbar sind, sollte auch Behörden bekannt sein. Immerhin empfiehlt das BSI zum „Verdeckte[n] Abfragen von Netzwerkbasisinformationen" die „Abfrage von öffentlichen Datenbanken (Whois, Ripe, Arin)". Der Aufwand sei „gering". Wir können uns dieser Aussage vollumfänglich anschließen.

Das BSI ist in den 90er Jahren aus der Zentralstelle für Chiffrierwesen (ZfCH) des BND – dort damals Unterabteilung 62 – hervorgegangen. Entsprechende Informationen über Netzwerkrecherchen sollten also auch dem BND bekannt sein. Um so mehr verwundert es, daß die Registrierungen in der RIPE-Datenbank so panikartig ausgetragen wurden. Diese Reaktion des Bundesnachrichtendienstes auf die Veröffentlichung in *wikileaks.org* halten wir für ein Stück weit überzogen, zumal es die bis dato angefallenen Datenspuren nicht entfernt und Verdachtsmomente erhärtete.

Wir können nicht abschätzen, welche Konsequenzen sich aus der Veröffentlichung auf *wikileaks.org* ergeben. Das hängt nicht zuletzt davon ab, was Organisationen und Dienste anderer Staaten an Logfiles aufgehoben haben. Ob dadurch Vorgänge transparent oder sogar Quellen enttarnt werden, man weiß es nicht. Der BND muß im schlimmsten Fall lernen, daß auf Vorrat angelegte Datenberge gegen ihn verwendet werden können. Vor diesem Hintergrund

beobachten die Autoren gespannt den geplanten Umbau des deutschen Telefonnetzes vom ISDN auf Basis des Elektronischen Wählsystems Digital (EWSD) der in diesem Bereich BND-nahen Firma Siemens [SPIEGEL] auf ein IP-basiertes Netz (sog. NGN) [Heise08] unter Einsatz auch von Geräten ausländischer Anbieter – so z. B. der chinesischen Firma Huawei, die nach Medienberichten eng mit den chinesischen Nachrichtendiensten verzahnt ist.

Zu jeder guten Geschichte gehört auch eine Portion Verschwörung. Bestandteil einer Verschwörung sind Menschen, die sich verschwören, aber auch welche, die die Verschwörung aufdecken. So gehen wir davon aus, daß die BVOE-Netze lediglich eine Sollbruchstelle darstellen, um etwas viel Größeres zu kaschieren. Wir bitten daher die Netzgemeinde, weiterhin wachsam zu sein. Vigilia pretium libertatis.

Quellen

[RIPE] Snapshots der RIPE-Datenbank, *ftp://ftp.ripe.net/ripe/dbase/split/*

[RIPE-NCC] Réseaux IP Européens – Network Coordination Center, *http://www.ripe.net/*

[WL08] German Secret Intelligence Service (BND) T-Systems network assignments, 13 Nov 2008, *http://wikileaks.org/wiki/German_Secret_Intelligence_Service_(BND)_T-Systems_network_assignments%2C_13_Nov_2008*

[Provos] Niels Provos: A Virtual Honeypot Framework *http://www.citi.umich.edu/u/provos/papers/honeyd.pdf*, abgerufen am 15. November 2008

[Richter] Alexander Richter: Verschwundene Geheimdaten, aufgelöste Dienststelle ZNBw *http://www.bits.de/public/gast/2007richter-1.htm*, abgerufen am 15. November 2008.

[Juretzko] Norbert Juretzko, Wilhelm Dietl: Bedingt dienstbereit. Im Herzen des BND – die Abrechnung eines Aussteigers. Ullstein, 1. Auflage, 2004.

[Pro5] *http://www.webmasterworld.com/forum39/3631.htm*, abgerufen am 15. November 2008.

[Fro6] *http://rantburg.com/index.php?D=04/07/2006&HC=1*, abgerufen am 15. November 2008.

[Cho0] Luojian Chen, Route to 62.156.187.234, *http://www.cs.utk.edu/~lchen/stats/routes/62.156.187.234.html*, abgerufen am 15. November 2008

[W07] Günther K. Weiße, Geheime Funkaufklärung in Deutschland, Motorbuch Verlag. 1. Auflage 2005.

[ESE93] Erich Schmidt-Eenboom, Schnüffler ohne Nase: Der BND – die unheimliche Macht im Staate, Econ-Verlag, 3. Auflage, 1993, S. 227.

[ESE95] Erich Schmidt-Eenboom, "Der Schattenkrieger – Klaus Kinkel und der BND", Econ-Verlag, 1995.

[AO] *http://web.archive.org/web/20050222091651/http://hermes.zeit.de/pdf/archiv/2004/23/*, abgerufen am 15. November 2008.

[GG] Gesellschaft für Netzwerk- und Unix-Administration mbH, Liste aktueller Patches zu GeNUGate 5.0, *http://www.genua.de/support/ggc/patches/patches_5_0_html*. Unter der URL ist das Dokument nicht mehr zu finden. Der Archivierungsdienst *archive.org* hat jedoch noch Kopien, z. B. *http://web.archive.org/web/20050223192428/http://www.genua.de/support/ggc/patches/patches_5_0_html*, abgerufen am 15. November 2008.

[WP05] *http://de.wikipedia.org/w/index.php?title=Bundesnachrichtendienst&diff=prev&oldid=8557599*

[CCC08] CCC, Bayern will Trojanereinsatz zum Skype-Abhören, *http://www.ccc.de/updates/2008/bayerntrojaner-wg-skype*. Aus dem verlinkten Dokument geht hervor, daß im Falle einer Skype-Abschnorchelung nach Empfehlungen der Firma Digitask ein „anonymer Proxy-Server" verwendet werden soll. Um den unverschlüsselten Teil der Tor-Kommunikation abzufangen, würden Behörden nicht anders vorgehen.

[BSI] Durchführungskonzept für Penetrationstests, *http://www.bsi.bund.de/literat/studien/pentest/index.htm*, abgerufen am 15. November 2008.

[SPIEGEL] Siemens eng mit BND verflochten – Ex-Manager packen aus, *http://www.spiegel.de/wirtschaft/0,1518,547022,00.html*, abgerufen am 15. November 2008.

[Heise08] Telekom plant Netzumbau zu Lasten der Konkurrenz, *http://www.heise.de/newsticker/meldung/114356*, abgerufen am 15. November 2008.

Netz	Description	IP-Range	Raum	Last Hop (letzter bekannter)
BVOENET	TSI fuer LVP	212.185.184.224-231	München	0111246-1-1-gw.M.DE.net.DTAG.DE (62.154.31.14)
BUNDESSTELLE-FUER-FERNMELDESTATISTIK-GAUTING-NET	Bundesstelle fuer Fernmeldestatistik	212.185.184.224-231		
BVOENET1	TSI fuer LVP	62.225.74.128-135	München	068062-1-1-gw.M.net.DTAG.DE (62.154.29.197)
BVOENET2	TSI fuer LVP	217.7.155.168-175	Braunschweig	068062-2-1-gw.BS.net.DTAG.DE (62.154.99.164)
BVOENET2	T-Systems Business Service GmbH fuer BVOENET (war: TSI fuer LVP)	62.153.65.32-39	Braunschweig	80.148.106.127
BVOENET2	T-Systems Business Service GmbH fuer BVOENET	62.157.194.32-39	Braunschweig	80.148.106.127
BVOENET2	T-Systems Business Service GmbH fuer BVOENET	62.159.60.144-151	Braunschweig	80.148.106.127
BVOENET3	TSI fuer LVP	194.25.184.16-23	München	00510-3-1-gw.M.net.DTAG.DE (62.154.29.180)
BVOENET4	TSI fuer LVP	195.145.31.252-255	München	00510-3-2-gw.M.DE.net.DTAG.DE (62.154.29.193)
LVP-INFO-BROKING-NETWORK	LVP / Muenchen	195.145.31.252-255		
BVOENET5	TSI fuer LVP	62.156.187.232-239	München	00510-3-2-gw.M.DE.net.DTAG.DE (62.154.29.193)
LVP-INFO-BROKING-NETWORK-2	LVP / Muenchen	62.156.187.232-239		
BVOENET6	TSI fuer LVP	195.145.182.96-111	Frankfurt	068062-3-1-gw.F.DE.net.DTAG.DE (62.154.21.240)
BVOENET7	TSI fuer LVP	62.225.71.248-255	Frankfurt	068062-4-1-gw.FR.net.DTAG.DE (62.153.182.154)
BVOENET8	TSI fuer LVP	62.153.59.192-223	München	194.25.184.20
BVOE-MANAGEMENT--PULLACH-NET	BVOE Management	62.153.59.192-223		
BVOENET9	TSI fuer LVP	62.157.193.128-223	Frankfurt	068062-3-1-gw.F.DE.net.DTAG.DE (62.154.21.240)
BVOE-MANAGEMENT--FRANKFURT-NET	BVOE Management	62.157.193.128-223		
BVOENET10	TSI fuer LVP	195.243.248.224-231	Berlin	80.148.83.171
BVOENET11	TSI fuer LVP	195.145.57.176-191	München	62.225.74.134
BVOENET12	TSI fuer LVP	195.243.157.184-191	München	80.148.110.50
BVOENET12	TSI fuer LVP	62.154.211.152-159	München	80.148.110.50
BVOENET12	TSI fuer LVP	195.145.128.56-63	München	80.148.110.50
BVOENET12	TSI fuer LVP	193.159.228.32-39		
BVOENET13	TSI fuer LVP	217.89.74.208-223	Frankfurt	80.148.134.29
BVOENET13	TSI fuer LVP	62.159.19.208-215	Frankfurt	80.148.134.29
BVOENET14	BVOE Management Sued	80.146.198.88-95	Augsburg	0101347-1-1-gw.A.DE.net.DTAG.DE (62.153.183.11)
BVOENET15	TSI fuer LVP	62.153.80.208-215	Augsburg	a-ag4.A.DE.net.DTAG.de (62.154.126.110)
BVOENET16	TSI fuer LVP	62.157.194.32-39	Braunschweig	80.148.106.12
BVOENET17-NET	TSI fuer LVP	212.185.191.128-135	München	0102597-1-1-gw.M.DE.net.DTAG.DE (62.154.30.70)
BVOENET18	BVOE Management	62.157.136.64-95		80.148.203.180
BVOENET19	TSI fuer LVP	195.145.163.64-127	München	80.148.111.175
BVOENET19-NET	HS1172-RIPE [sic!]	62.159.104.128-175		80.148.146.214
BVOENET20	TSI fuer LVP	62.157.144.0-63	München	0111246-1-1-gw.M.DE.net.DTAG.DE (62.154.31.14
BVOENET21	TSI fuer LVP	193.159.238.168-175		
BVOENET22	T-Systems Business Services GmbH f"FC"r BVOENET (war: TSI fuer LVP)	194.25.42.232-239	Flensburg (Husum?)	0120571-1-1-gw.FL.DE.net.DTAG.DE (62.154.116.238)
BVOENET23	T-Systems Business Services GmbH f"FC"r BVOENET (war: TSI fuer LVP)	62.225.139.248-255	Berlin	0134609-1-1-gw.B.DE.net.DTAG.DE (62.154.48.50)
BVOENET24	T-Systems Business Services GmbH f"FC"r BVOENET (war: TSI fuer LVP)	62.159.63.72-79	München	0127669-1-1-gw.M.DE.net.DTAG.DE (62.154.29.177)
BVOENET25	T-Systems Business Service GmbH fuer BVOENET [sic!]	62.159.21.152-159		80.148.203.180
BVOENET26	T-Systems Business Services GmbH fuer BVOENET [sic!]	62.159.209.144-151	München	80.148.233.85
BVOENET27	T-Systems Business Services GmbH fuer BVOENET [sic!]	62.159.209.152-159	Mainz	80.148.180.31
BVOENET28	T-Systems Business Services GmbH fuer BVOENET [sic!]	62.153.87.0-15	Traunstein? Übersee?	62.153.87.1
FW-EXTENSION-2-DMZ	TSI fuer LVP	193.159.228.32-39		
LIEGENSCHAFTSVERWALTUNG-PULLACH-PULLACH-NET	Liegenschaftsverwaltung Pullach	62.225.102.248-255	München	80.148.111.175
LIEGENSCHAFTSVERWALTUNG-PULLACH-PULLACH-NET	Liegenschaftsverwaltung Pullach	62.153.60.16-23	München	80.148.111.175
LIEGENSCHAFTSVERWALTUNG-PULLACH-NET	TSI fuer LVP	62.153.75.48-55		80.148.113.185
LIEGENSCHAFTSVERWALTUNG-PULLACH-NET	TSI fuer LVP	62.153.82.136-143		80.148.111.17
LIEGENSCHAFTSVERWALTUNG-PULLACH-NET	Liegenschaftsverwaltung Pullach	217.89.49.176-183		217.89.49.177
LIEGENSCHAFTSVERWALTUNG-PULLACH-NET	TSI fuer LVP	62.159.95.72-79	München	80.148.111.175
FERNMELDESTELLE-SUED-DER-BW-GABLINGEN-NET	Fernmeldestelle Sued der BW	62.159.104.160-175		
SCHWAIGER-NET	T-Systems Business Services GmbH f"FC"r Schwaiger	193.158.63.224-239	Frankfurt	80.148.134.173
SCHWAIGER-NET	T-Systems Business Services GmbH fuer Schwaiger	62.154.226.64-127		80.148.203.168
SCHWAIGER-NET	T-Systems Business Services GmbH fuer Schwaiger	212.185.19.160-175	Braunschweig	80.148.106.87
SCHWAIGER-NET	T-Systems Business Services GmbH fuer Schwaiger	212.185.19.192-207	München	0130097-1-1-gw.m.de.net.dtag.de (62.154.31.116)
SCHWAIGER-NET	T-Systems Business Services GmbH fuer Schwaiger	212.185.19.240-255	Augsburg	0130104-1-1-gw.a.de.net.dtag.de (62.154.126.226)

Last Hop - 1	Letzter Admin-C	Letzter Tech-C	Ältester Change	Abschaltung	Kommentar
m-ag1.M.DE.net.DTAG.DE (62.154.27.114)	HS1172-RIPE	HS1172-RIPE	23.01.2007	14.11.2008	war BUNDESSTELLE-FUER-FERNMELDESTATISTIK-GAUTING-NET
	HS1172-RIPE	HS1172-RIPE	18.10.2005	20.05.2007	wurde zu BVOENET
m-ag5.M.net.DTAG.DE (62.154.27.138)	HS1172-RIPE	HS1172-RIPE	20.09.2004	14.11.2008	
	HS1172-RIPE	HS1172-RIPE	05.08.2002	14.11.2008	
bs-ag4.BS.DE.net.DTAG.DE (62.154.99.102)	HS1172-RIPE	HS1172-RIPE	16.11.2005	14.11.2008	
bs-ag4.bs.de.net.dtag.de (62.154.99.102)	HS1172-RIPE	HS1172-RIPE	25.07.2008 ?	14.11.2008	war BVOENET16
bs-ag4.bs.de.net.dtag.de (62.154.99.106)	HS1172-RIPE	HS1172-RIPE	25.07.2008	14.11.2008	
m-ag2.M.net.DTAG.DE (62.154.27.118)	HS1172-RIPE	HS1172-RIPE	05.07.2004	14.11.2008	
m-ag3.M.DE.net.DTAG.DE (62.154.27.126	HS1172-RIPE (WW208-RIPE)	HS1172-RIPE (LB670-RIPE)	06.07.2004	14.11.2008	war LVP-INFO-BROKING-NETWORK
	WW208-RIPE	LB670-RIPE	05.12.1997	-	wurde zu BVOENET4
m-ag3.M.DE.net.DTAG.DE (62.154.27.126)	HS1172-RIPE (WW208-RIPE)	HS1172-RIPE (LB670-RIPE)	06.07.2004	14.11.2008	war LVP-INFO-BROKING-NETWORK-2
	WW208-RIPE	LB670-RIPE	26.11.1998	-	wurde zu BVOENET5
f-ag5.F.DE.net.DTAG.DE (62.154.18.62)	HS1172-RIPE	HS1172-RIPE	05.07.2004	14.11.2008	
fr-ag1.FR.net.DTAG.DE (62.154.124.50)	HS1172-RIPE	HS1172-RIPE	05.07.2004	20.05.2007	
00510-3-1-gw.M.net.DTAG.DE (62.154.29.180)	HS1172-RIPE	HS1172-RIPE	05.07.2004	14.11.2008	war BVOE-MANAGEMENT--PULLACH-NET
	HS1172-RIPE	HS1172-RIPE	23.04.2003	-	wurde zu BVOENET8
f-ag5.F.DE.net.DTAG.DE (62.154.18.62)	HS1172-RIPE	HS1172-RIPE	05.07.2004	14.11.2008	war BVOE-MANAGEMENT--FRANKFURT-NET
	HS1172-RIPE	HS1172-RIPE	23.04.2003	-	wurde zu BVOENET9
b-eb1.B.DE.net.DTAG.DE (62.154.46.190)	HS1172-RIPE	HS1172-RIPE	05.07.2004	14.11.2008	
068062-1-1-gw.M.net.DTAG.DE (62.154.29.197)	HS1172-RIPE	HS1172-RIPE	05.07.2004	14.11.2008	
m-ea20.M.DE.net.DTAG.DE (62.154.28.110	HS1172-RIPE	HS1172-RIPE	20.07.2004	14.11.2008	
m-ea20.M.DE.net.DTAG.DE (62.154.28.106	HS1172-RIPE	HS1172-RIPE	06.03.2006	14.11.2008	
m-ea20.M.DE.net.DTAG.DE (62.154.28.106)	HS1172-RIPE	HS1172-RIPE	14.12.2004	14.11.2008	
	HS1172-RIPE	HS1172-RIPE	27.04.2006	14.11.2008	war FW-EXTENSION-2-DMZ
fr-ag4.FR.DE.net.DTAG.DE (62.154.124.122)	HS1172-RIPE	HS1172-RIPE	20.09.2004	14.11.2008	
fr-ag4.FR.DE.net.DTAG.DE (62.154.124.118)	HS1172-RIPE	HS1172-RIPE	06.11.2006	14.11.2008	
a-ag4.A.DE.net.DTAG.DE (62.154.126.110)	HS1172-RIPE	HS1172-RIPE	30.07.2004	14.11.2008	
	HS1172-RIPE	HS1172-RIPE	30.07.2004	14.11.2008	
bs-ag4.BS.DE.net.DTAG.DE (62.154.99.106)	HS1172-RIPE	HS1172-RIPE	16.09.2004	25.07.2008 ?	wurde zu BVOENET2
m-ag3.M.net.DTAG.DE (62.154.27.126)	HS1172-RIPE	HS1172-RIPE	22.09.2004	14.11.2008	
217.5.66.34	HS1172-RIPE	HS1172-RIPE	06.09.2006	14.11.2008	
m-ea2.M.DE.net.DTAG.DE (62.154.28.46)	HS1172-RIPE	HS1172-RIPE	06.09.2006	14.11.2008	
217.5.68.82	HS1172-RIPE	HS1172-RIPE	20.05.2005	20.05.2007	
m-ag1.M.DE.net.DTAG.DE (62.154.27.110)	HS1172-RIPE	HS1172-RIPE	06.09.2006	14.11.2008	
	HS1172-RIPE	HS1172-RIPE	18.08.2006	14.11.2008	remarks: INFRA-AW / keine Route
fl-ag1.FL.DE.net.DTAG.DE (62.154.116.50)	TPSR1-RIPE (HS1172-RIPE)	TPSR1-RIPE (HS1172-RIPE)	05.10.2006	14.11.2008	
217.5.72.178	TPSR1-RIPE (MS15854-RIPE)	TPSR1-RIPE (MS15854-RIPE)	15.06.2007	14.11.2008	
m-eb3.M.DE.net.DTAG.DE (62.154.28.98)	TPSR1-RIPE (MS15854-RIPE)	TPSR1-RIPE (MS15854-RIPE)	15.06.2007	14.11.2008	
217.5.66.38	TPSR1-RIPE	TPSR1-RIPE	08.11.2007	14.11.2008	
m-ea5.M.DE.net.DTAG.DE (62.154.27.146)	TPSR1-RIPE	TPSR1-RIPE	29.07.2008	14.11.2008	
mz-eb1.MZ.DE.net.DTAG.DE (62.154.40.174)	TPSR1-RIPE	TPSR1-RIPE	29.07.2008	14.11.2008	
ts-eb1.TS.DE.net.DTAG.DE (62.154.101.50)	TPSR1-RIPE	TPSR1-RIPE	30.09.2008	14.11.2008	
	GZ978-RIPE	GZ978-RIPE	27.04.2006	02.10.2006	wurde zu BVOENET12
m-ea2.M.DE.net.DTAG.DE (62.154.28.46)	GZ978-RIPE	GZ978-RIPE	21.11.2005	20.05.2007	
m-ea2.M.DE.net.DTAG.DE (62.154.28.42)	GZ978-RIPE	GZ978-RIPE	06.10.2005	20.05.2007	
217.5.70.34	HS1172-RIPE	HS1172-RIPE	16.11.2005	20.05.2007	
m-ea2.M.DE.net.DTAG.DE (62.154.28.42)	GZ978-RIPE	GZ978-RIPE	16.11.2005	20.05.2007	
hh-ea2.HH.DE.net.DTAG.DE (62.154.33.70	HS1172-RIPE	HS1172-RIPE	06.09.2005	20.05.2007	
m-ea2.M.DE.net.DTAG.DE (62.154.28.46)	GZ978-RIPE	GZ978-RIPE	27.04.2006	20.05.2007	
	MW2010-RIPE	MW2010-RIPE	20.07.2005	15.11.2008	
fr-ea2.fr.de.net.dtag.de (62.154.124.158)	HS1172-RIPE	HS1172-RIPE	26.09.2007	14.11.2008	
217.5.66.222	TPSR1-RIPE	TPSR1-RIPE	24.10.2007	14.11.2008	
bs-ea1.bs.de.net.dtag.de (62.154.99.158)	HS1172-RIPE	HS1172-RIPE	26.09.2007	14.11.2008	
217.5.66.222	HS1172-RIPE	HS1172-RIPE	26.09.2007	14.11.2008	
a-eb1.a.de.net.dtag.de (62.154.126.154)	HS1172-RIPE	HS1172-RIPE	26.09.2007	14.11.2008	

Die Welt von morgen: Spreading Democracy

von maha

Aus dem Verkaufsprospekt der Firma Spreading Democracy (SD), dem führenden Hersteller von Wahlcomputern (3. Auflage vom 23. Mai 2012, deutsche Fassung).

Wählen mit NuVote

[Da sich die vorliegende Fassung des Verkaufsprospekts an Regierungen wendet, sind keine Preise enthalten. Diese sind vom Einzelfall abhängig und müssen mit SD ausgehandelt werden.]

Machen Sie sich keine Sorgen mehr um die Durchführung von Abstimmungen und Wahlen. Sicher haben auch Sie die Erfahrung gemacht, daß Wahlcomputer, wie sie seit langem bei Ihnen in Gebrauch sind, die Wahlleiter und Wahlausschüsse wie auch die Wähler überfordern. Daher bieten wir Ihnen jetzt das integrierte Wahl-Paket NuVote [1]: Spreading Democracy stellt Ihnen nicht nur die Computer, sondern auch das gesamte Personal für die Durchführung der Wahl. Sie können damit den gesamten Wahlvorgang outsourcen: Sie teilen die für die Wahl nötigen Daten mit und erhalten von SD unmittelbar nach Schließung der Wahllokale das Ergebnis übermittelt. Außer den von SD in Rechnung gestellten und vorher vereinbarten Gebühren fallen keine Kosten an. Da SD die ordnungsgemäße Durchführung der Wahl garantiert, fällt auch die für alle Beteiligten aufwendige Möglichkeit der Wahlanfechtung weg.

Die Durchführung einer Wahl durch ein privates Unternehmen bringt den Vorteil mit, daß Wahlbetrug weitgehend ausgeschlossen werden kann, denn eine renommierte Firma wie SD garantiert, daß alle Kundenwünsche erfüllt werden. Sollten Sie mit unserer Leistung nicht zufrieden sein, können Sie einfach den Anbieter wechseln oder zu kostspieligen traditionellen Wahlverfahren zurückkehren. Sollten Sie sich jedoch gegen das ökologisch zertifizierte NuVote-Paket entscheiden, müssen Sie bei der herkömmlichen Wahlmethode einen unvertretbar hohen Papierverbrauch in Kauf nehmen – von den übrigen Kosten und dem hohen Betrugsrisiko einmal abgesehen!

Das Outsourcen von Wahlen schafft Arbeitsplätze, weil statt freiwilliger Wahlhelfer (die

unzuverlässig und schlecht geschult sind) unser Fachpersonal tätig wird: SD beschäftigt als freie Mitarbeiter zahlreiche Absolventen von BA-Studiengängen wie Politik und Gesellschaft, Politische Wissenschaften bzw. Absolventen der darauf aufbauenden MA-Studiengänge wie Politische Wahlen und Abstimmungen, Wahlhilfe oder Wahlleitung (akkreditiert an der Volkshochschule Wüsterhausen).

Das kostengünstige Basismodul ermöglicht es, Wahlen in vollem Umfang bei höchster Kundenzufriedenheit durchzuführen. Zusätzlich zum Basismodul werden jedoch zahlreiche Zusatzmodule angeboten, die auf die Bedürfnisse verschiedener Abnehmerländer zugeschnitten sind und dort auch schon erfolgreich erprobt wurden. Hier eine Auswahl der wichtigsten Zusatzmodule:

Optional module Athens

Da in vielen westlichen Demokratien die Volksparteien hinsichtlich ihres Programms kaum unterscheidbar sind, empfehlen wir hier das Modul Athens. Hier ergibt sich das Wahlergebnis zufällig zugunsten der einen oder anderen großen Volkspartei. Die Zufälligkeit beruht auf dem erprobten Zufallszahlengenerator einer frühen Debian-Distribution, ersatzweise können die Zufallszahlen auch einer Liste entnommen werden.

Optional module Evolution

Viele Schwellenländer befinden sich gerade auf dem Weg der Demokratisierung. Hierfür sind schwankende Wahlergebnisse typisch, jedoch auch kontraproduktiv, insbesondere weil immer wieder radikale antidemokratische Kräfte an die Macht kommen und Unruhen ausgelöst werden. In diesem Fall empfehlen wir das Modul Evolution. Hierbei wird das Wahlergebnis gerade so langsam in Richtung neu entstandener Parteien und Gruppierungen verschoben, daß das Gesamtgefüge der bisherigen Ordnung nicht ins Wanken geraten kann. Nach ausgiebiger Erprobung in verschiedenen osteuropäischen Ländern wird das Modul auch von älteren Staatsmännern in Afrika sehr geschätzt. Zahlungen von Schweizer Konten werden gern entgegengenommen.

Optional module Transparency

Bei diesem Modul stellt SD nicht nur das gesamte Personal für die Durchführung der Wahl, sondern auch die Wahlbeobachter, die sich vom ordnungsgemäßen Zustand der Wahlcomputer überzeugt haben und gleichfalls überzeugend darüber Auskunft geben können. Gegen Aufpreis werden auch Journalisten gestellt, welche die positiven Prüfberichte medial verbreiten.

Optional module Florida

Dieses Modul ermöglicht es, das Ergebnis automatisiert neu auszuzählen und verläßlich bei jeder Neuauszählung ein anderes Ergebnis zu erzielen. Ein Ergebnis kann dann durch den Wahlleiter oder ein Gericht zum amtlichen Ergebnis erklärt werden. Eine nicht-automatisierte Überprüfung erübrigt sich und ist durch den Einsatz von Wahlcomputern selbstverständlich auch nicht möglich.

Optional module Suspense

Dieses Modul ermöglicht es, vorab automatisch Hochrechnungen zu veröffentlichen, die geeignet sind, ein Fernsehpublikum (und zunehmend auch die Blogo- und Podosphäre) stundenlang in Atem zu halten. Dabei nähert sich das Ergebnis nach diversen vorher einstellbaren Ausreißern in die eine oder andere Richtung schließlich dem Endergebnis an, was zu einem festgesetzten Zeitpunkt bekanntgegeben wird. Das Endergebnis kann nach Wunsch auch vollkommen von den Hochrechnungen abweichen.

[1] In einer ersten Fassung dieser Dystopie hieß das Paket in Anlehnung an George Orwell: NewVote; leider wurde die Dystopie durch die Wirklichkeit überholt, denn die niederländische Firma Sdu (!) bietet schon jetzt einen Wahldienst namens NewVote an, der gewisse Ähnlichkeiten mit dem hier karikierten Dienst zeigt. Diese sind jedoch zufällig und waren nicht beabsichtigt.

Secure Instant Messaging – am Beispiel XMPP

von Hannes Mehnert <hannes@berlin.ccc.de>

Instant Messaging wird viel benutzt. Dabei wird auch immer wieder behauptet, es sei „sicher". Dieser Artikel versucht, diese weitverbreitete These mit Fakten zu unterlegen, in welchen Fällen welche Sicherheitseigenschaften gewährleistet sind. Betrachtungsgegenstand ist das Instant Messaging Protokoll XMPP (früher: Jabber), da dieses frei und offen ist. Es werden verschiedene Verschlüsselungsmöglichkeiten diskutiert. Des weiteren wird anonymes Instant Messaging mit Hilfe von TOR und XMPP vorgestellt.

Kurze Übersicht über XMPP

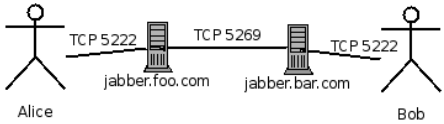
XMPP ist ein offener Standard, der XML zum Austausch sämtlicher Daten benutzt. Die Infrastruktur für XMPP ist ein dezentrales Netzwerk. Eine XMPP-ID ist wie eine E-Mail-Adresse aufgebaut: `$user@$host`. Optional wird noch eine Komponente `/$ressource` verwendet, um mehrere gleichzeitige Sessions zu unterstützen. Als Beispiele werden in diesem Artikel `alice@jabber.foo.com/somewhere` und `bob@jabber.bar.com/somewhere-else` benutzt.

XMPP ist flexibel, da es durch sogenannte XEPs (XMPP Extension Protocols) erweitert werden kann. Auch die Integration von anderen Instant-Messaging-Protokollen ist mit Hilfe von Transports möglich.

Kommunikation

Es gibt Client-Server- und Server-Server-Kommunikation. Die Client-Server-Kommunikation findet über TCP-Port 5222 bzw. 5223 (SSL), die Server-Server-Kommunikation findet allgemein über TCP-Port 5269 statt. Die hier genannten Ports sind die normal konfigurierten und von der IANA vergebenen, es können aber via DNS SRV records andere Ports benutzt werden.

Wenn `alice@jabber.foo.com` eine Nachricht an `bob@jabber.bar.com` mit dem Inhalt „Hello, world" versenden will, verschickt der Client von Alice diese erstmal an den Server `jabber.foo.com`, der die Nachricht an den Server `jabber.bar.com` weiterleitet. Dieser schickt die Nachricht an Bobs Client, falls dieser online ist. Falls nicht, speichert der Server die Nachricht, bis Bobs Client online kommt – genauer: online mit einer Priorität >= 0. Eine Priorität kann von einem Client gesetzt werden. Prioritäten kleiner 0 sind primär für Bots gedacht.



XMPP ist „sicher"

Es kann nicht per se gesagt werden, ein Protokoll sei sicher, da zumindest die Bedrohung (bzw. das Angriffsszenario), vor der das Protokoll sicher sein soll, genannt werden muß. Wenn eine Angreiferin im lokalen Netz als größte Gefährdung ausgemacht wird, reicht eine verschlüsselte Verbindung vom Client zum Server. Wenn allerdings die Angreiferin Zugriff auf den Server hat, reicht die verschlüsselte Verbindung nicht mehr aus, sondern dann ist End-to-End-Encryption notwendig.

Bei XMPP sind prinzipiell folgende Daten schützenswert:

- Nachrichten – Inhalt der Nachricht,
- Verbindungsdaten – Metadaten der Nachricht,

- Presence – Statusänderung eines Accounts,
- Roster (Buddy List) – Liste der Accounts, mit denen kommuniziert wird (Speicherung auf dem Server),
- vCard – angegebene Daten der Accountinhaberin oder des Accountinhabers.

In der Kryptographie werden verschiedene Eigenschaften der Verschlüsselung unterschieden:

- Vertraulichkeit: Niemand außer Alice und Bob kann die Nachricht lesen,
- Integrität: Niemand kann die Nachricht auf dem Weg von Alice zu Bob verfälschen, ohne daß Bob dies entdeckt,
- Authentizität: Bob kann überprüfen, daß die Nachricht tatsächlich von Alice kam,
- Verbindlichkeit: Alice kann nicht abstreiten, die Nachricht verschickt zu haben.

In den folgenden Abschnitten werden zunächst die beiden erwähnten Szenarien analysiert.

Angreifer im lokalen Netzwerk

Zuerst wird das Szenario, daß Alice mit Bob kommunizieren will, ohne daß eine mögliche Angreiferin Eve mithören kann, betrachtet. In diesem Szenario hat Eve nur Zugriff auf das lokale Netzwerk von Alice oder Bob und keinen Zugriff auf den Server. Den Servern (sowohl den Personen mit Zugriff auf diese als auch installierten Betriebssystemen sowie laufenden Services) wird somit vollständig vertraut.

Die zu schützenden Daten sind die Nachrichten sowie die Verbindungsdaten und die Presence. Da diese alle über die gleiche Verbindung verschickt werden und den Servern vertraut wird, ist eine detaillierte Betrachtung der verschiedenen Daten nicht notwendig. Um gegen dieses Angriffsszenario sicher zu sein, muß die Client-Server-Kommunikation die beschriebenen kryptographischen Eigenschaften erfüllen. Auf diese wird im Folgenden eingegangen.

Anschließend wird das Szenario erweitert, sodaß Eve Zugriff auf das Netzwerk zwischen den beiden Servern hat. Daher wird die Server-Server-Kommunikation kurz untersucht.

Vertraulichkeit, Integrität & Verbindlichkeit der Client-Server-Kommunikation

Der Client muß (laut 5.1, Use of TLS) das Zertifikat validieren. Die Validierung muß in mehreren Schritten ausgeführt werden. Zunächst sollte das Zertifikat gegen die erwartete Identität geprüft werden. Falls dies nicht erfolgreich ist, muß die Benutzerin notifiziert werden. Im zweiten Schritt sollte das Zertifikat und die gesamte Kette von Zertifikaten der Benutzerin zur Bestätigung gezeigt werden, falls es nicht anhand der bereits vertrauten Certificate Authorities verifiziert werden kann. Der Client muß das Zertifikat speichern, um bei der nächsten Verbindung zum gleichen Server überprüfen zu können, ob es sich geändert hat.

Die Validierung muß durchgeführt werden, falls das Zertifikat in einem Vertrauensanker (trust anchor) terminiert, also falls es irgendeinen Weg von Root-Zertifikaten, denen vertraut wird, zu dem vorliegenden Zertifikat gibt. Falls das Zertifikat von einer nicht bekannten Certificate Authority signiert wurde oder ein self-signed-Zertifikat ist, sollte die Validierung ausgeführt werden.

Certificate Authorities sind Teil eines zentralistischen Konzeptes, bei dem definiert wird, welchen Trust Center vertraut wird. Dieses paßt gut zu hierarchischen Strukturen, wo die oberste Hierarchieebene bestimmt, was vertrauenswürdig ist; nämlich alles, was von ihr kommt. Auf chaotische Strukturen, die meist hierarchiefrei sind, läßt sich sowas nicht abbilden. Wieso sollte die Benutzerin delegieren, wem sie alles vertraut? Auch der CACert-Ansatz ist hier nicht sinnvoll, da nicht detailliert spezifiziert werden kann, wem vertraut wird. Möglicherweise will ich nur meinen drei besten Nerdfreunden vertrauen und denen, den sie vertrauen, aber nicht dem gesamten CACert, da unklar ist, wie diese Leute den entsprechenden Trustlevel erreicht haben.

Angriff: Person in the middle

Bei einem Person-in-the-middle-Angriff (PITM) täuscht Eve Alice vor, der Server zu sein. Falls der Server nicht hinreichend authentifi-

ziert wird, also hier das Zertifikat nicht hinreichend überprüft wird, kann Eve Benutzernamen und Paßwort von Alice abfangen, falls der Client eine Klartext-Authentifizierung zuläßt. Da die gesamte Kommunikation über Eve läuft, kann diese von Eve gelesen und nach Belieben geändert und gefiltert werden.

Um ein PITM zu verhindern, muß das Zertifikat also validiert werden. Zumindest das Speichern des Zertifikates ist eine gute Idee, da damit nur die erste Verbindung ohne PITM durchgeführt werden muß, um eine spätere PITM zu erkennen, ähnlich wie bei ssh mit den known_hosts. Falls ein PITM erfolgreich durchgeführt wird, sind Eve Benutzername und Paßwort bekannt, und Eve kann sich somit als Alice einloggen und ausgeben.

SSL/TLS in der Praxis

Betrachten wir nun die eigene Client-Server-Verbindung, die vom lokalen Client zu einem offenen XMPP-Server wie `jabber.ccc.de` oder `jabber.berlin.ccc.de` besteht. Da fällt auf, daß diese keine Zertifikate haben, die von einer allgemein als vertrauenswürdig angesehenen CA signiert wurden.

Server: Das Zertifikat von `jabber.ccc.de` ist ein CAcert, somit muß der CA vertraut werden, um die Validierung vorschriftsgemäß durchzuführen. Das Zertifikat von `jabber.berlin.ccc.de` ist von der CA des CCCV signiert, deren Zertifikat via *http://jabber.berlin.ccc.de/cccv_ca.pem* erhältlich ist.

Client: Nun zur Integration der Zertifikate in verschiedene Clients. Getestet wurden Psi 0.10, AdiumX 1.2.1, Pidgin 2.2.1 und Gajim 0.11.2.

Psi: Die geteste Version 0.10 speichert die vertrauenswürdigen Zertifikate in der Datei `~/.psi/certs/rootcert.xml`. Falls das Server-Zertifikat nicht validiert werden kann, wird eine Warnung angezeigt, die in den Optionen allerdings abgeschaltet werden kann. Für die Verbindung mit SSL ist das Plugin Qt Cryptographic Architecture (QCA) erforderlich.

Eine aktuelle Version von Psi (0.11 oder eine Revision 1065 aus dem Subversion) bietet die Möglichkeit, einfach das Zertifikat im PEM-Format in `~/.psi/certs` zu hinterlegen. Somit ist keine manuelles Editieren der XML-Datei notwendig.

Es muß allerdings darauf geachtet werden, daß „Ignore SSL warnings" in den Connection-Einstellungen ausgeschaltet ist. Andernfalls werden SSL-Warnungen ignoriert, und ein PITM ist möglich.

Adium: Seit Version 1.2 (Januar 2008) bietet auch Adium die Möglichkeiten, Zertifikate zu überprüfen. In der aktuellen Version (1.2.3) gibt es bei den Account-Einstellungen „Require SSL/TLS" und „Do strict certificate checks". Beides sollte eingeschaltet sein, damit das Zertifikat des Servers validiert wird. (Allerdings hat Adium Probleme bei der Hostname-Zuordnung, falls SRV records existieren.) Falls dieses unbekannt ist, erscheint ein Popup-Fenster mit der Frage, ob das Zertifikat akzeptiert werden soll (und in die Keychain hinzugefügt werden soll).

Pidgin: Bei Pidgin (früher Gaim) findet keine Verifizierung des Zertifikates statt. Nur wenn „Force old (port 5223) SSL" eingeschaltet ist, wird SSL gesprochen. „Require SSL/TLS" in Pidgin macht einfach eine unverschlüsselte Verbindung zum Server auf, wenn „Force old SSL" ausgeschaltet ist und der Server kein TLS unterstützt.

In Pidgin kann für die SSL/TLS-Unterstützung sowohl Network Security Services (NSS) als auch GnuTLS verwendet werden, standardmäßig wird NSS benutzt. Im Quellcode ist für GnuTLS die Validierung des Zertifikates weiter implementiert als für NSS, wo einfach OK zurückgegeben wird:

```
static SECStatus ssl_auth_cert ( void *arg, PRFileDesc
*socket, PRBool checksig, PRBool is_server) {
  return SECSuccess;
#if 0
 ...
#endif
}
```

Somit werden alle Zertifikate als vertrauenswürdig angesehen. `pidgin-2.3.1/libpurple/plugins/ssl/ssl-gnutls.c`:

```
catic void ssl_gnutls_verified_cb
PurpleCertificateVerificationStatus st, gpointer userdata) {
    PurpleSslConnection *gsc = (PurpleSslConnection *) userdata;
    if (st == PURPLE_CERTIFICATE_VALID) {
        /* Certificate valid? Good! Do the connection! */
        gsc->connect_cb(gsc->connect_cb_data, gsc, PURPLE_INPUT_READ);
    } else {
        /* Otherwise, signal an error */
        if(gsc->error_cb != NULL)
            gsc->error_cb(gsc, PURPLE_SSL_CERTIFICATE_INVALID,
                          gsc->connect_cb_data);
        purple_ssl_close(gsc);
    }
```

Hier wird die Verbindung abgelehnt, falls das Zertifikat nicht validiert werden kann.

Gajim: Bis einschließlich zur Version 0.11.2 gab es keine Unterstützung zur Verifikation von Zertifikaten in Gajim. Dort konnte mittels „Use SSL (Legacy)“ SSL eingeschaltet werden.

Der aktuelle Gajim (Revision 9342 aus dem Subversion) bietet die Möglichkeit, Zertifikate zu verifizieren. Der Client versucht automatisch, zuerst eine TLS-Verbindung aufzubauen, falls dieses nicht erfolgreich ist, eine SSL-Verbindung zu etablieren; falls beides fehlschlägt, wird eine unverschlüsselte Verbindung aufgebaut. Einstellbar ist dies über „Advanced Configuration Editor“, dann beim entsprechenden Account durch Setzen von „connection_types“. Auch das Überprüfen und Speichern des Fingerprints (für die nächste Verbindung zum gleichen Server) ist vorgesehen, funktioniert allerdings gerade nicht.

Fazit: Bei keinem der Clients wird das Zertifikat für eine nächste Verbindung gespeichert. Somit sind aus Vertraulichkeitsgründen Psi, Adium und Gajim aus dem Subversion (oder ≥ 0.12) zu empfehlen, jeweils mit sorgfältig überprüften und eingepflegten CA-Zertifikaten.

Authentifizierung

XMPP spezifiziert die Benutzung von SASL, dem Simple Authentication and Security Layer. Es wird mindestens DIGEST-MD5 gefordert, was einer Challenge-Response-Authentifizierung, in der als Hashalgorithmus MD5 verwendet wird, entspricht. MD5 ist in den letzten Jahren durch einige Angriffe ins Gespräch gekommen, diese lassen sich aber nicht auf die Verwendung im Challenge-Response-Verfahren anwenden.

Im XEP78 wird die Authentifizierung, die früher verwendet wurde, erläutert. Hier handelt es sich um eine Plaintext- oder Digest-Authentifizierung. Bei Plaintext wird das Paßwort in Klartext übermittelt. Bei Digest-Authentifizierung wird `SHA1(concatenate(Stream-ID, Passwort))` zurückgegeben.

Alle getesteten Releases der Clients haben noch immer mit der alten Authentifizierung gearbeitet, wobei zumindest Digest und nicht Plaintext benutzt wurde. Angeblich sollen die Clients aber auch SASL unterstützen. Die Sicherheit beider Mechanismen ist in etwa gleich, jeweils wird dem Client etwas Zufälliges vom Server mit dem Benutzerpaßwort zusammengesetzt und danach der Hash davon zum Server zurückgesendet.

Der Zufall vom Server sollte schon kryptographisch zufällig sein, ansonsten kann mit Hilfe von mitgeschnittenen Authentifizierungsvorgängen offline ein Wörterbuch-Angriff gemacht werden (falls der Zufall beispielsweise von der Serverzeit abhängt). Eine Untersuchung der Stream-ID in verschiedenen Serverimplementationen, die in dem obsoleten, aber noch benutzten XEP78 als Nonce verwendet wird, brachte folgendes:

- jabberd-2: (`trunk/sx/server.c:143`)

```
random wurde mit srand(time(NULL)) geseeded
for(i = 0; i < 40; i++) {
    r = (int) (36.0 * rand() / RAND_MAX);
    id[i] = (r >= 0 && r <= 9) ? (r + 48) : (r + 87);
}
```

- jabberd1: Version 1.4.4 (`jabberd/lib/xstream.c:236`):

```
sprintf(id,"%X",(int)time(NULL));
```

- jabberd1: Version 1.6.1.1 (`jabberd/lib/xstream.cc:356`):

```
der PRNG wird mit srand(time(NULL)) geseeded
snprintf(id, sizeof(id), „%08X%08X%08X%08X%08X%08X“,
        rand(), rand(), rand(), rand(), rand());
shahash_r(id, id);
/* don‘t let them see what our rand() returns */
```

- ejabberd: (src/randoms.erl:53):

```
seed vom random mit now()
get_string() ->
    random_generator ! {self(), get_random, 65536*65536},
    receive
        {random, R} ->
            integer_to_list(R)
    end.
```

Dieses benutzt das Random-Modul aus Erlang.

Somit haben zumindest aktuelle Server-Implementationen (außer Jabberd1-1.4.4, der aber schon zwei Jahre alt ist) keine kryptographisch hochwertigen zufälligen Stream-IDs, da die benutzten Pseudo-Random-Number-Generators mit der Zeit des Server-Startups initialisiert werden. Mit der „Last Activity"-Erweiterung kann die Server-Startup-Zeit sekundengenau angefragt werden. Diese eröffnet zumindest die theoretische Möglichkeit, die Stream-ID vorherzusagen. Beim ejabberd werden als Seed auch die Mikrosekunden benutzt.

Server-Server-Kommunikation

Auch bei der Server-Server-Kommunikation sollte sowohl SASL als auch TLS benutzt werden. Zusätzlich gibt es noch „server dialback", das gegen domain spoofing schützen soll. Eine Server-Server-Verbindung sieht also wie folgt aus: jabber.foo.com stellt eine Verbindung mit jabber.bar.com auf Port 5269 her. jabber.bar.com kontaktiert dann jabber.foo.com, um zu überprüfen, ob jabber.foo.com auch tatsächlich der Rechner ist, von dem aus die Verbindung aufgebaut wurde. Anschließend passiert das gleiche für den Rückkanal, also fängt jabber.bar.com an, die Verbindung zu initiieren.

Die verschiedenen Server-Implementationen können wohl untereinander via TLS kommunizieren. Eine genauere Untersuchung fand nicht statt, da eine Benutzerin den Status der Verbindung von einem Server zu einem anderen Server nicht nachprüfen kann. Aus Sicherheitsgründen muß davon ausgegangen werden, daß die Verbindung nicht verschlüsselt wird.

Fazit

Falls dem Server vertraut wird, ist für eine Benutzerin unklar und nicht überprüfbar, ob die Server-Server-Kommunikation verschlüsselt wird oder nicht. Somit kann möglicherweise jeder Rechner im Netzwerk Daten von Server jabber.foo.com zu Server jabber.bar.com mitlesen.

Das einzige, wo man sich sicher sein kann, ist die eigene Client-Server-Kommunikation, falls das Zertifikat erfolgreich verifiziert wurde. Die Client-Server-Kommunikation des Gegenübers muß nicht zwingend verschlüsselt sein. Hier muß je nach Expertise und geistigem Zustand des Gegenübers abgewogen werden.

Bei TLS/SSL wird die Kommunikation zwischen den einzelnen Komponenten verschlüsselt, also vom Client zum Server, dann vom Server zu Server, dann vom Server zum Client. Die einzelnen Server haben die kompletten Kommunikationsdaten unverschlüsselt vorliegen. Falls die Empfängerin momentan nicht online ist, wird die Nachricht auch unverschlüsselt auf dem Server des Empfängers gespeichert.

Eigener Server vertrauenswürdig

Falls nur dem Server von Alice vertraut wird, nicht aber dem von Bob, bleiben weiterhin sowohl die Nachrichten als auch die Verbindungsdaten und die Presence für den Server von Bob unverschlüsselt. Auch der Eintrag von Alice in Bobs Roster ist für den Server von Bob nachvollziehbar.

Der besondere Schutz der Nachricht wird im nächsten Szenario detailliert behandelt.

Server nicht vertrauenswürdig

Als nächstes Szenario wird wieder betrachtet, daß Alice eine Nachricht an Bob schicken will. Diesmal wird allerdings dem Server nicht vertraut. Dieses kann verschiedene Gründe haben: Der Anwenderin unbekannt, wer Zugriff auf die Server hat; ob die Zugriffsberechtigten möglicherweise mit Angreiferinnen oder Insti-

tutionen (Strafverfolgungsbehörden) zusammenarbeiten; oder ob das Betriebssystem und die laufenden Dienste auf dem Server unsicher sind, sodaß sich andere Personen dadurch Zugriff zum Server verschaffen können. Es soll also verhindert werden, daß Eve, die Zugriff auf einen Server hat, die Kommunikation mitlesen kann.

Hierzu ist also Verschlüsselung von Alice zu Bob nötig, ohne daß die Nachricht auf den Servern entschlüsselt und wieder verschlüsselt wird. Dies wird End-to-End-Encryption genannt. In den nächsten Sektionen wird auf zwei unterschiedliche Mechanismen der End-to-End-Encryption eingegangen (PGP und OTR).

Bei der End-to-End-Encryption werden nur Nachrichten verschlüsselt, also keine Verbindungsdaten oder Presences. Somit hat Eve schon die Informationen, daß Alice mit Bob kommuniziert (Verbindungsdaten). Diese können nicht geschützt werden, da sie auf den Servern dafür benötigt werten, um die Nachricht von Alice an Bob entsprechend weiterzuleiten.

Auch weiß Eve, daß Alice online ist (Presence). Die Presence kann nicht geschützt werden, da sie an alle Kontakte im Roster gesendet wird. Falls sie also verschlüsselt werden sollte, müßte sie an jeden Kontakt einzeln verschlüsselt werden; dazu müßte jeder Kontakt Verschlüsselung unterstützen.

Zusätzlich kann Eve durch bestimmte Erweiterungen die Jabber-Client-Version, das Betriebssystem, die Zeit des letzten Logins, die Zeit der letzten Nachricht, die Geolokation, die aktuell gehörte Musik in Erfahrung bringen. Auch die „Freunde“ von Alice kennt Eve schon anhand des Rosters – möglicherweise gruppiert nach Themengebieten oder anhand der Sortierung von Alice. Falls Alice persönliche Daten in die vCard eingetragen hat, weiß Eve auch diese, da diese auch auf dem Server gespeichert werden.

End-to-End-Encryption

Die Eigenschaften der Verschlüsselungsmethode sollten hier auch wieder Vertraulichkeit, Integrität, Authentizität sowie Verbindlichkeit sein. PGP wurde zur Verschlüsselung von E-Mail „erfunden“. Es basiert auf öffentlichen und privaten Schlüsseln. Öffentliche Schlüssel sind für alle Teilnehmerinnen via Keyserver erhältlich. Deren Echtheit mußüberprüft werden (durch die Überprüfung des Fingerprints über einen sicheren Kommunikationskanal wie persönliches Treffen, Telefon o. ä.), damit die Authentizität gewährleistet ist. Es bietet alle geforderten Eigenschaften: Vertraulichkeit durch Verschlüsselung, Integrität, Authentizität und Verbindlichkeit durch digitale Signaturen.

Alle Nachrichten werden mit dem öffentlichen Schlüssel des Empfängers verschlüsselt, sodaß nur dieser die Nachricht entschlüsseln kann. Meist werden die Nachrichten auch zusätzlich mit dem öffentlichen Schlüssel des Senders verschlüsselt, damit dieser die Nachrichten später nochmal lesen kann. Der Sender kann

mit seinen privaten Schlüssel die Nachricht zu signieren.

Somit können alle Nachrichten auch zu einem späteren Zeitpunkt von einer Inhaberin des privaten Schlüssels entschlüsselt werden. Falls also zu einem späteren Zeitpunkt der private Schlüssel in die Hände von Eve gelangt und die Nachrichten aufgenommen wurden, können diese entschlüsselt werden. Wenn die Nachrichten auch eine Signatur enthalten, was für Authentizität unerläßlich ist, kann sogar „kryptographisch" nachgewiesen werden, daß Alice zum Zeitpunkt X eine bestimmte Nachricht an Bob geschickt hat (unter der Voraussetzung, daß an diesem Zeitpunkt nur Alice ihren privaten Schlüssel hatte).

Daher haben sich einige Wissenschaftler Gedanken über private Konversationen und Anforderungen gemacht. Sie haben das Off-the-record-Protokoll (OTR) entwickelt. Auch dieses basiert auf öffentlichen und privaten Schlüsseln. Es gibt aber pro Sitzung spezielle Sitzungsschlüssel, die unabhängig von den öffentlichen Schlüsseln sind. OTR bietet zusätzliche Eigenschaften:

- Perfect forward secrecy: Ein Sitzungsschlüssel ist nicht abhängig vom vorherigen Sitzungsschlüssel,
- Malleable encryption: Die Änderung eines Bits im verschlüsselten Text provoziert die gleiche Änderung des Bits im entschlüsselten Text.

Perfect forward secrecy bietet somit die Eigenschaft, daß, wenn ein Sitzungsschlüssel von Eve herausgefunden wird, nicht sämtliche mitgeschriebene Kommunikation entschlüsselt werden kann, da der nächste Sitzungsschlüssel unabhängig vom vorhergehenden ist. Dieses wird dadurch erreicht, daß immer kurzlebige Schlüssel (beispielsweise für jede Nachricht ein neuer Schlüssel) erzeugt werden, die mit Hilfe eines Authenticated Diffie-Hellman-Key-Exchange zwischen den Kommunikationspartnern ausgetauscht werden.

Malleable encryption wird durch ein XOR des Schlüsselstroms mit dem Klartext erreicht. Somit wird, falls ein Bit im verschlüsselten Text geändert wird, auch der Klartext bei gleichen Schlüsselstrom verändert. Dieses hat folgende nützliche Eigenschaft: Es kann nicht nachgewiesen werden, daß Alice einen bestimmten Nachrichtentext an Bob geschrieben hat. Dieses führt zu plausible deniability, später kann Alice also plausibel machen, nicht die entsprechende Nachricht an Bob gesendet zu haben.

Prinzipiell wird auch auf mögliche Angriffe gegen diese Methoden eingegangen. Dazu werden sowohl die Speicherung der privaten Schlüssel und das Verhalten, falls ein Benutzer gerade offline ist, im Detail betrachtet.

Im „Freiheitblog" gibt es eine Serie von Artikeln zur Konfiguration von End-to-End-Encryption verschiedener Clients.

PGP Encryption

Wie PGP in XMPP benutzt wird, ist in XEP 27 spezifiziert. Jede Nutzerin hat einen privaten und einen öffentlichen Schlüssel. Der Schlüssel der Kommunikationspartnerin muß vorher verifiziert worden sein.

PGP-Schlüsselaustausch
Der Austausch der öffentlichen Schlüssel wird durch Key-Server vollzogen, die Vertrauenswürdigkeit kann anhand des PGP Web of Trust geprüft werden. Das Web of Trust ist das Vertrauen, das man den Personen gibt, deren öffentlichen Schlüssel signiert wird. Diese Signaturen der öffentlichen Schlüssel werden zusammen mit den öffentlichen Schlüsseln auf Key-Servern gespeichert. Um einen Schlüssel zu signieren, muß der Fingerprint des öffentlichen Schlüssels auf einem authentifizierten Kommunikationskanal überprüft werden. Wenn Bob und Carol sich schon länger kennen und einander vertrauen, haben sie gegenseitig ihre Schlüssel signiert. Alice und Bob kennen sich auch schon länger und vertrauen sich. Wenn Alice nun Carol kennenlernt, kann Alice anhand der Signatur von Bob auf Carols Schlüssel und dem Vertrauen zu Bob verifizieren, daß

Carols Schlüssel tatsächlich Carol gehört, ohne den Schlüssel auf einem gesicherten Kommunikationskanal zu überprüfen.

Das Web of Trust ist eines der ersten Social Networks. Es beinhaltet die Informationen, wer welchen Schlüssel wann signiert hat. Dieses kann beispielsweise als Kennenlernen der Personen gewertet werden. Aus Datensparsamkeitsgründen muß man sich genau überlegen, ob beziehungsweise welche Informationen von ihr publik sind. Natürlich funktioniert das Web of Trust am besten, wenn jede die Schlüssel der Leute unterschreibt, denen sie vertraut und die sinnvoll überprüft worden sind, indem die Identität der Schlüsselinhaberin sinnvoll überprüft wurde. Wenn der Schlüssel für eMail benutzt wird, also die Validität der E-Mail-Adresse und ob die Inhaberin E-Mails and diese Adresse empfangen kann. Bei Nutzung von XMPP muß dementsprechend analog die XMPP-ID überprüft werden. Natürlich kann man auch ohne Überprüfung des Finger- prints den Schlüssel signieren. Der Signatur ist nicht anzusehen, wie sehr die Identität der angeblichen Besitzerin und der Fingerprint überprüft worden sind.

Discovery
Jede Presence-Nachricht wird kryptographisch signiert, damit wird zum Ausdruck gebracht, daß die Benutzerin PGP-verschlüsselte Nachrichten empfangen und entschlüsseln kann und welche KeyID sie benutzt. Hier sind Replay-Attacken möglich. Das heißt, eine empfangene Presence von Alice kann von Eve gespeichert und zu einem späteren Zeitpunkt nochmal versendet werden, so daß Bob denkt, Alice wäre online und würde gerade diese Presence verschicken. Hierzu muß es Eve allerdings möglich sein, diese Presence als Alice zu verschicken, dazu benötigt sie entweder das Paßwort von Alice oder Zugriff auf den XMPP-Server von Alice oder Bob. Auch Zugriff auf das Netzwerk zwischen Alices und Bobs Server ist ausreichend, um eine Replay-Attacke durchzuführen.

Key Storage
Der private PGP-Schlüssel ist meist durch eine passphrase geschützt auf der Festplatte gespeichert. Die Benutzerin muß sie beispielsweise beim Start des Chat-Clients angeben, diese wird im RAM gespeichert.

Verschlüsselung von Nachrichten
Die Nachrichten, die Alice und Bob austauschen, werden verschlüsselt, aber nicht signiert. Auch hier kann Eve, bei Zugriff auf einen der XMPP-Server, Nachrichten, die mit Alices bzw. Bobs öffentlichen Schlüssel verschlüsselt sind, einschleusen, falls der öffentliche Schlüssel bekannt ist. Also können weder Alice noch Bob sicher sein kann, daß Bob bzw. Alice die entsprechende Nachricht versendet hat. Eve kann nicht lesen, worüber Alice und Bob kommunizieren, wenn sie nicht im Besitz des privaten Schlüssels von Alice oder Bob ist. Somit kann sie auch nur Nachrichten, die möglicherweise kontextfrei sind, einschleusen.

Offline Storage
Die Nachrichten, die Alice an Bob schickt, während Bob offline ist, sind auch verschlüsselt und werden somit verschlüsselt auf dem Server gespeichert.

Geteste Clients
Von mir getestete Clients, welche die PGP-Verschlüsselung unterstützen, sind Gajim und Psi; außerdem noch Jarl (nicht mehr aktiv in Entwicklung). Sowohl bei Gajim als auch bei Psi muß die Zuordnung zwischen Benutzer und Schlüssel von Hand gemacht werden, hier wird nicht anhand der signierten Presence der richtige Schlüssel ausgesucht.

Fazit
Alle abgefangenen Nachrichten können, falls einer der privaten Schlüssel zu irgendeinem Zeitpunkt abhanden kommt, vollständig entschlüsselt werden. Wenn die einzelnen Nachrichten zusätzlich noch signiert wären, könnte auch kryptographisch bewiesen werden, daß Alice die Nachrichten an Bob geschickt hat, indem die Signatur der Nachrichten überprüft wird. Natürlich nur, wenn bewiesen werden kann, daß Alice zum Zeitpunkt des Sendens die Einzige war, die ihren privaten Schlüssel kannte. Auch nicht außer Acht zu lassen sind die Replay-Attacken auf Presence-Nachrichten

und die Einspeisung neuer verschlüsselter Nachrichten. Bob kann aufgrund fehlender Signatur nicht nachprüfen, ob tatsächlich Alice gerade die Nachricht geschrieben hat.

Off-the-Record Messaging

Beim Off-the-Record Messaging hat jeder Benutzer einen öffentlichen und einen privaten Schlüssel. Auch der initiale Austausch des Fingerprints muß durch einen authentifizierten Kommunikationskanal geschehen, beispielsweise durch eine PGP-Signatur des Fingerprints des Schlüssels, falls Alice und Bob schon PGP-Schlüssel von dem jeweils anderen validiert haben.

Discovery
Bei Off-the-Record werden die Nachrichten nicht signiert. Dafür wird die erste herausgehende Nachricht um verschiedene Whitespaces erweitert, die angibt, daß OTR unterstützt wird. Außerdem kann in den Clients explizit angefordert werden, daß eine Session verschlüsselt werden soll, dann wird der Schlüsselaustausch gestartet.

Session Initiation
Falls beide Clients OTR unterstützen, kann mit Hilfe eines Authenticated Diffie-Hellman Key Exchange eine Nonce ausgehandelt werden, die nicht abhängig von den privaten und öffentlichen Schlüssel der Chatteilnehmer ist, aber durch einen Dritten nicht abgehört werden kann, da nicht alle Parameter kommuniziert werden. Somit wird ein Session Key ausgehandelt, mit dem die Nachrichten verschlüsselt werden können.

Verschlüsselung von Nachrichten
Nachrichten werden verschlüsselt und mit einem signierten Authentication Code (HMAC) versehen. Somit kann Bob überprüfen, daß Alice tatsächlich die entsprechende Nachricht verschickt hat.

Client State
Ein OTR-Client muß somit Informationen über den Status der Session haben, ob diese aktuell verschlüsselt ist mit einem Session Key; oder ob gerade der Session Key ausgehandelt wird, etc. Dieses kann zu Problemen führen, wenn die States der beiden Clients nicht kompatibel sind, also der eine Client denkt, sie wären gerade am Neuverhandeln eines Session Keys und der andere noch einen alten Session Key hat.

Auch wenn Pakete nicht in der richtigen Reihenfolge ankommen, kann dieses den Client verwirren, sodaß Nachrichten mit einem neueren Session Key zuerst eintreffen, diese nicht entschlüsselt werden können. Später, nachdem der Session Key upgedatet wurde, können ältere Nachrichten nicht mehr entschlüsselt werden.

Dieses ist nur rudimentär gelöst, indem die zuletzt versendete Nachricht zwischengespeichert wird, und, falls der andere Client einen Fehler zurücksendet, der Session Key neu ausgehandelt wird und die Nachricht mit dem neuen Schlüssel verschlüsselt ein weiteres mal versendet wird.

Key Storage
OTR speichert den privaten Schlüssel unverschlüsselt auf der Festplatte. Falls Eve Zugriff auf diesen bekommt, können ab dann verschlüsselte Sessions von Eve initiiert werden, ohne daß dieses entdeckt werden kann.

Offline Storage
Wenn Bob gerade nicht online ist, können, falls der Client von Alice noch eine Session mit Bobs Client hat, weiterhin verschlüsselte Nachrichten verschickt werden, die dann auf dem Server gespeichert werden. Falls Bob allerdings seinen Client beendet und somit die Session geschlossen hat, kann dieser die Nachrichten von Alice nicht entschlüsseln, da der Session Key nicht mehr vorhanden ist.

Clients
Clients, die OTR unterstützen, sind Pidgin und AdiumX. Auch psi-0.11 mit einem Patch kann OTR unterstützen. Leider kann mit diesem nur entweder mit allen Kontakten via OTR kommuniziert werden oder mit keinem, und er hat kein Benutzerinterface im Chatfenster. Diese Benutzungsprobleme wurden mit dem selbstgeschrieben Patch *http://berlin.ccc.de/~hannes/psi-otr-socks.diff* und dem Plugin *http://berlin.ccc.de/~hannes/psi-otr-0.3-hacked.tar.gz* gelöst.

Fazit
Sowohl PGP als auch OTR haben noch Probleme: die Netzwerkinstabilität (packet loss, out of order), die zur Verwirrung der States der OTR-Clients führen können; das nicht wirklich gelöste Problem von OTR sind die offline-Nachrichten; die nicht signierten Nachrichten, die ein PGP-Client verschickt. Dies kann auch irrelevant sein, beispielsweise wenn aus dem Kontext klar hervorgeht, worüber Alice und Bob reden und Eve nur unsinnige Nachrichten einstreut (da Eve ja die Nachrichten von Alice an Bob nicht lesen kann).

Anonymes Instant Messaging

Im Folgenden wird vorgestellt, wie Instant Messaging mit Hilfe von TOR anonym betrieben werden kann. TOR ist ein Anonymisierungsnetzwerk, daß Onion Routing benutzt. Somit wird jedes Paket, das verschickt werden soll, in mehreren „Zwiebelschalen“ verpackt und an den ersten Router geschickt. Dieser kann die äußerste Zwiebelschale entfernen (entschlüsseln) und schickt den Rest des Paketes an den nächsten Router. Somit ist nicht nachvollziehbar, von wo nach wo das Paket verschickt wurde (es sei denn eine Entität hat Zugriff auf viele Router). Bei TOR gibt es Hidden Services, diese sind nur über TOR zu erreichen und haben einen Namen, der aus 16 Zeichen (ein Teil des Fingerprints des public keys) und .onion besteht, beispielsweise `ww7pd547vjnlhdmg.onion`. Diese haben also keine öffentliche IP, sondern sind nur über das TOR-Netzwerk erreichbar, da der Hostname indirekt auf TOR-Router zeigt, die bestehende Verbindungen vom Hidden Service haben. Durch einige Verbindungen vom TOR-Client zu mehreren TOR-Routern ist somit eine anonyme Verbindung möglich, wo weder der Server noch der Client wissen, mit welcher IP sie kommunizieren.

Da diese Verbindung schon verschlüsselt ist, ist es nicht mehr notwendig, zwischen XMPP-Client und XMPP-Server mit SSL/TLS zu verschlüsseln.

Anfallende Daten und notwendiges Vertrauen

Wenn nun ein XMPP-Server als TOR Hidden Service betrieben wird, kann nur noch die Betreiberin sehen, wer mit wem chattet. Für beispielsweise den Internet Provider einer Nutzerin ist nicht einsehbar, daß gerade ein XMPP-Dienst, geschweige denn welcher, genutzt wird. Somit fallen auch bei der Vorratsdatenspeicherung keine interessanten Daten beim Internet-Provider an. Entweder muß der Betreiberin des Servers vertraut werden oder ein eigener Server installiert werden. Die Betreiberin sieht, welche Daten auf dem Server hinterlegt wurden sowie welche Kontakte im Roster vorhanden sind. Aber immerhin kann die Betreiberin nicht mehr adressiert werden, diese ist anonym, da der TOR Hidden Service nicht lokalisiert oder zu einer realen Person zugeordnet werden kann.

Im allgemeinen kann nicht davon ausgegangen werden, daß alle Server vollständig anonym sind, einige können möglicherweise auch aus dem öffentlichen Internet erreicht werden. Sowohl Server-Server-Kommunikation zwischen anonymen und nicht-anonymen Servern ist denkbar und möglich als auch, daß ein Transport existiert, der zwischen dem anony-

men und dem nicht-anonymen Netzwerk kommuniziert.

Die Server-Server-Kommunikation gestaltet sich etwas komplizierter, da der XMPP Hidden Service keine Netzwerkverbindung in das Internet haben sollte, sondern Verbindungen nach außen nur über den SOCKS-Proxy von TOR herstellen soll.

In bestimmten Szenarien, falls beispielsweise eine Nutzerin nur Accounts eines anderen, öffentlichen XMPP-Servers in dem Roster hat, ist die Anonymität nicht mehr gewährleistet, da aufgrund der Einträge in den anderen Rostern unmittelbar auf die Benutzerin geschlossen werden kann. Somit kann es passieren, daß die Anonymität einer Nutzerin aufgehoben wird.

Patch für ejabberd

Nicht-anonyme XMPP-Server, die eine öffentliche IP-Adresse besitzen, müssen, falls sie mit anonymen XMPP-Servern kommunizieren wollen, verändert werden, sodaß sie für .onion-XMPP-Server den TOR-SOCKS-Proxy benutzen. Auch wenn zwei anonyme Server kommunizieren wollen, muß die Serversoftware den SOCKS-Proxy von TOR benutzen.

Hierzu wurde ein Patch entwickelt, der dem ejabberd die Nutzung von SOCKS-Proxies ermöglicht, und durch eine Konfigurationsoption kann gesteuert werden, welcher SOCKS-Proxy benutzt wird, ebenso welche Verbindungen über den SOCKS-Proxy aufgebaut werden sollen. Hier kann man zwischen all, none (default) und dot_onion_only wählen.

Ein TOR Hidden Service, der die Option auf dot_onion_only gesetzt hat, kann somit nur mit anderen TOR Hidden Services reden. Dieses ist sicherheitstechnisch auf den ersten Blick das „sicherste“, da somit verhindert wird, daß von dem Server an einen öffentlichen Server Daten geschickt werden. Falls allen anderen Hidden Services, mit welchen Nachrichten ausgetauscht werden, vertraut wird, daß sie vollständig anonym sind, ist dies auch so. Solange also jede Einzelne einen eigenen XMPP-Server als reinen TOR Hidden Service betreibt, sind die jeweiligen Daten am besten geschützt.

Praktische Tests

Der Verbindungsaufbau zu einem Hidden Service ist deutlich langsamer als zu einem öffentlichen Server, da das TOR zuerst einen Circuit zum Lookup-Server aufbauen muß. Dort muß ein Introduction Point des Hidden Service gesucht werden, zu diesem muß wieder ein Circuit aufgebaut werden. Zusätzlich braucht man noch einen Rendezvous Point, und die Daten des Rendezvous Point müssen dann via Introduction Point an den Hidden Service übermittelt werden. Der Hidden Service muß daraufhin eine Verbindung zum Rendezvous Point aufbauen. Insgesamt müssen also vier verschiedene TOR Circuits aufgebaut werden, was eine deutliche Latenz bewirkt. Nachdem die Verbindung zum Hidden Service erfolgreich aufgebaut wurde, hat die Kommunikation auf dem gleichen Server etwa vier Sekunden Latenz. Die Server-Server-Kommunikation muß insgesamt vier dieser Verbindungen aufbauen, da eine Verbindung von Server `ww7pd547vjnlhdmg.onion` zu `3khgsei3bkgqvmqw.onion` erst nach einem

erfolgreichen Dialback von 3khgsei3bkgqvmqw.onion zu ww7pd547vjnlhdmg.onion erfolgreich aufgebaut ist. Diese ist dann nur für Nachrichten von ww7pd547vjnlhdmg.onion zu 3khgsei3bkgqvmqw.onion. Für die Rückrichtung werden somit nochmal zwei TCP-Verbindungen aufgebaut. Für die initiale Verbindung zwischen zwei Servern können somit durchaus fünf Minuten vergehen. Das ist auch der Grund, wieso im Patch zu ejabberd der FSMTIMEOUT deutlich erhöht werden mußte.

Ab dann ist eine Latenz von meist weniger als acht Sekunden von Nachrichten von einer Benutzerin des Servers 3khgsei3bkgqvmqw.onion zu einer Benutzerin des Servers ww7pd547vjnlhdmg.onion.

Client Support

Bei allen benutzten Clients war es möglich, einen SOCKS-Proxy einzutragen. Leider machen sowohl Adium als auch Psi DNS-Anfragen des Hostnames über den normalen Resolver, statt den Hostname an den SOCKS-Proxy weiterzugeben. Somit wird der Hostname des XMPP-Servers, zu dem verbunden werden soll, an den eingetragenen Nameserver unverschlüsselt via Netzwerk übermittelt. Für Psi gibt es einen Patch, sodaß Psi keine DNS-Anfragen mehr versendet, falls ein SOCKS-Proxy eingetragen ist.

Bei Pidgin und Adium funktionierte die Einstellung eines SOCKS-Proxy out of the box. Bei Gajim wird Version aus dem Subversion benötigt. Zusätzlich muß in dem „Advanced Configuration Editor“ bei den „connection types“ der entsprechenden Verbindung „tls“ und „ssl“ gelöscht werden, sodaß nur noch plain da steht. Ansonsten verschluckt sich der Gajim an dem SSL Handshake.

Ausblick

Die Entwicklung eines Transports, der zwischen anonymen und öffentlichen XMPP-Accounts Kommunikation ermöglicht, steht noch aus. Dieses ist wie beschrieben nicht ganz ungefährlich, da dieser Transport eine zentrale Stelle darstellt, an der Kommunikationsdaten gesammelt werden. Somit gehen auch sämtliche Presence sowie Nachrichten durch diesen Transport, was Begehrlichkeiten wecken könnte, um anonyme Chatterinnen zu deanonymisieren. Multi-User Chat benutzt eine Subdomain des Hostname, also conferences.jabber.ccc.de oder auch conferences.3khgsei3bkgqvmqw.onion. TOR kann diese allerdings nicht auflösen, somit ist MUC nur innerhalb eines Hidden Servers möglich. Eine Lösung wäre, in TOR alle *.foo.onion an foo.onion zu schicken.

Server-Server-Kommunikation zwischen anonymen und öffentlichen Servern sollte mit SSL/TLS verschlüsselt werden, da ansonsten die TOR Exit Nodes die unverschlüsselten Nachrichten sehen.

Fazit

Es wurden sowohl Client-Server- als auch Server-Server-Kommunikation untersucht. Es gab zwei Angriffsszenarien: Dem Server wird vertraut bzw. nicht vertraut. Beim letzteren Szenario wurden zwei verschiedene End-to-End-Encryption-Systeme erklärt. Beide sind nicht frei von Fehlern; sie bieten verschiedene Eigenschaften. Je nachdem, welche kryptographischen Eigenschaften von einer Person angestrebt sind, sollte entschieden werden, ob PGP oder OTR verwendet wird. Jedes der kryptographischen Verfahren ist besser, als unverschlüsselt zu kommunizieren

Anonymes Chatten ist durch die Installation eines XMPP-Servers als TOR Hidden Service möglich. Auch hier muß beachtet werden, wieviel Sicherheit notwendig ist, um dann Abstriche bei den Kommunikationsmöglichkeiten zu machen (beispielsweise ein reiner TOR Hidden Service Server). In einer geschlossenen Benutzergruppe, die viel Kommunikationsdisziplin an den Tag legt, und einen oder mehrere eigene Server betreibt, kann somit anonym und sicher kommuniziert werden.

Der Artikel inklusive aller Referenzen kann im Internet unter *http://berlin.ccc.de/~hannes/secure-instant-messaging.pdf* abgerufen werden.

Software Distribution Malware Infection Vector

von Felix Gröbert <felix@groebert.org>

Wer kennt es nicht? Frisches Windows installiert, getfirefox.com angesurft: Softwareverteilung über das Internet ist ein integraler Bestandteil bei der Neuinstallation von diversen Betriebssystemen. Während dieser Weg sehr effizient für Free- und Open-Source-Software ist, birgt er auch Gefahren, auf die dieser Artikel eingeht.

Als 2007 das Thema des Bundestrojaners heiß in der Presse diskutiert wird, arbeitet bereits ein bayerisches Entwicklungsbüro an Software zum Mitschnitt von Skype-Telefonaten. Die Software entschlüsselt jedoch keine Skype-Netzwerkkommunikation, sondern nistet sich auf dem Rechner des Opfers ein und speichert die Audioeingänge des Mikrofons. Außer dem Installer gibt es keinen vorgesehenen Weg, um die Software auf den Rechner des zu überwachenden Opfers zu bringen. Also wie könnte die Exekutive eines Staat solche Malware nun unbemerkt installieren?

Manuelle Installation

Eine manuelle Installation, auf welche sich das BKA teilweise bezieht, setzt einen physikalischen Zugang zum Zielsystem voraus. Dies bedeutet, daß ein Ermittler unbemerkt in die Wohnung des Opfers eindringt und dabei mögliche Zugangssperren und Detektoren überwindet. Dann müssen lokale Sperren des Zielsystems überwunden werden, wie zum Beispiel Login- und BIOS-Paßwörter. Ein Ausbau und direkte Installation auf der Festplatte wäre möglich, falls das Opfer kein 24/7 Integrity Monitoring und verschlüsselte Dateisysteme verwendet. Eine technisch versierte Zielperson hätte genügend Wege, um sich gegen einen solchen Angriff zu schützen.

Social Engineering

Eine weitere, vom Innenministerium nicht ausgeschlossene, Möglichkeit ist die Übergabe von USB-Sticks oder CDs sowie der Versand von E-Mails, um das Opfer zur Öffnung der Medien und Installation der Malware zu bewegen. Eine trickreiche Aufforderung zur Überzeugung des unvorsichtigen Opfers ist meist notwendig. Eine solche Aufforderung kann unter Umständen aufgrund einer Telekommunikationsüberwachung und der Kenntnisse von sozialen Strukturen des Opfers konstruiert werden.

Backdoor

Häufig wurde in den Medien eine Hintertür in legitimer Software zur Sprache gebracht. Während dieser Infektionsweg bei Open-Source-Software erst gar nicht möglich ist, würde eine Hintertür in **legitimer** Software eine massive Diskreditierung bedeuten. Eine Detektion der Hintertür, durch Verwendung

seitens der Ermittler oder durch Reverse Engineering, könnte bei falscher Konstruktion den Mißbrauch der Hintertür durch Dritte ermöglichen. Daher ist dieser Infektionsweg unwahrscheinlich.

Client/Remote Exploits

Auch der gern genutzte Begriff von Zero-Days scheint eher unwahrscheinlich, da Zero-Days für gängige Software wie Betriebssysteme, E-Mail-Clients und Browser selten sind und dementsprechend einen hohen Marktwert haben. Eine periodische Entwicklung eines solchen Exploits ist unproportional aufwendig bei einer Halbwertszeit von sechs Monaten.

Download-Infektion

Betrachtet man die 270000 Firefox-Downloads pro Tag oder die 100000 VLC- Downloads, eröffnet sich hier ein völlig neuer Infektionsweg. Ist es einem Angreifer möglich, eine ausführbare Datei (Win32 PE `.EXE`, Mac OS `.APP`, Linux Makefile im `.TAR.GZ`) während des Downloads zu modifizieren, ist eine Infektion des Zielsystems möglich. Dazu muß das Opfer die ausführbare Datei über einen kryptographisch ungesicherten Weg, als Update oder via Browser, herunterladen und ausführen.

Der Voraussetzungen sind also:

1. Kontrolle über Paketübertragungswege durch den Angreifer.

Die Debatten über Internet-Teilhabe der Regierungen, diverse SINA-Boxen bei ISPs und Techniken der Deep-Packet-Inspection (DPI) in Großbritannien haben gezeigt, daß die Exekutive sehr wohl die Möglichkeiten haben kann, Internet-Traffic umzuleiten.

2. Keine kryptographische Integritätsprüfung im Übertragungsprotokoll und keine Integritätsprüfung durch das Betriebssystem (z. B. Signed Executables) beim Opfer.

Zwar werden Microsoft- und Firefox-Updates auf Integrität überprüft, jedoch sind Erst-Installation, wie FirefoxInstaller.exe und Linux `.ISO`s weiterhin ein Problem.

3. Keine Erkennung durch Antivirus- oder Intrusion-Detection-Systeme beim Opfer.

Diese Annahme ist sowohl von der Qualität der letztendlich genutzten Malware als auch vom Infektionsweg abhängig.

Ein simpler Proof-of-Concept konnte mit einem modifizierten Privoxy und einem Win32 PE/COFF-Prepend-Binder in einer Woche realisiert werden. Der Privoxy-Teil erkennt Win32-EXE-Downloads anhand den Bytes MZ und injiziert den Binder (18665 Bytes umkomprimiert) mit einem regulären Ausdruck `s-^MZ-\x4d\x5a\x00… MZ-`. Wird der (134 SLOC C++) Binder aufgerufen, sucht der Algorithmus nach der angehängten Malware sowie der originalen Software und führt beide aus.

Somit ist Download-Infektion ein effektiver Infektionsvektor, der den Anforderungen und Ressourcen einer Exekutive genügt. Um dem entgegenzuwirken, müssen weiter sichere Übertragungskanäle für Software Distribution überprüft, entworfen und implementiert werden. Die Open-Source-Gemeinschaft ist mit den GPG-Signaturen von Softwarepaketen wie `.DEB` in diesem Bereich Vorreiter. Kurzfristig kann einer Download-Infektion mit einem VPN oder mit HTTPS verhindert werden, jedoch müssen sich langfristig Code-Signaturen zur Integritätsprüfung in Betriebssystemen etablieren.

Angriffsszenarien auf Microsoft Windows

von Tim Blazytko

Ein Betriebssystem sollte einen bestimmten Grad an Sicherheit gewährleisten. Es sollte zum Beispiel über eine sichere Authentifizierung verfügen, das heißt, daß unter anderem eine vernünftige Paßwortsicherheit existieren sollte. Es werden nun Angriffsszenarien vorgestellt, welche ohne Exploits auskommen, die also Designschwächen in der Betriebssystem- und Netzwerkarchitektur von „Windows NT 5“ ausnutzen.

"Windows NT 5" Systemarchitektur

Ein wichtiger Bestandteil der Architektur der Betriebssysteme Windows 2000 (Version NT 5.0), Windows XP (Version 5.1) und Windows Server 2003 (NT 5.2) der Firma Microsoft ist die Windows-Registrierungsdatenbank (Registry). Für die folgenden Untersuchungen wird lediglich der Registry-Pfad `HKEY_LOCAL_MACHINE` benötigt, welcher in den Dateien im Ordner `%windir%\System32\Config`, genauer in den Dateien `SAM` (Security Account Manager), `SECURITY`, `software` und `system`, gespeichert ist. Es sind hier einzig die Dateien `SAM` und `SECURITY`, welche die sicherheitsrelevanten Einstellungen, wie lokale Benutzerkonten, deren Gruppen, Berechtigungen sowie Systemrechte beinhalten, und `system`, welche die beim Systemstart benötigten Hardware-Informationen von Bedeutung. In der `SAM`-Datei sind alle Benutzer und Paßwörter in durch Hashfunktionen verschlüsselter Form abgelegt.

Hashfunktionen bei "Windows NT 5"-Systemen

„Windows NT 5“-Systeme haben zwei Hashfunktionen implementiert, die LM (LAN-Manager)- und die NTLM (NT LAN-Manager)-Hashfunktion, welche beide standardmäßig aktiviert sind. Der LM-Hash ist lediglich aus Gründen der Abwärtskompatibilität zu früheren Windows-Betriebssystemen implementiert. Der LM-Hash weist bei seiner Berechnung einige Schwächen auf: Erstens wird jeder Buchstabe des eingegebenen Paßwortes in einen Großbuchstaben transformiert. Zweitens wird dieses Paßwort mit Nullen gefüllt oder gekürzt, damit der String 14 Byte groß ist. Drittens wird das Paßwort in zwei 7-Byte-Hälften aufgeteilt und jede Hälfte für sich selbst gehasht.

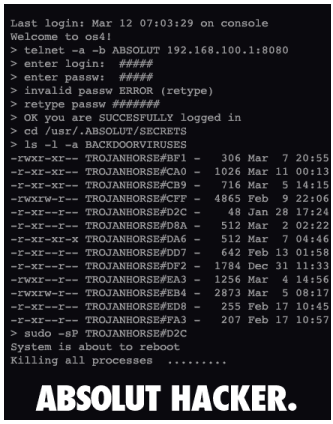
Der NTLM-Hash weist einige Verbesserungen auf: Er verwendet als Zeichensatz den Unicode, ermöglicht folglich die Benutzung einer größeren Anzahl an Zeichen und verzichtet auf die Umwandlung in Großbuchstaben. Des Weiteren teilt er den Input nicht auf, sondern hasht ihn vollständig, sodaß der Aufwand bei einem starken Paßwort bei einem Brute-Force-Angriff wesentlich höher ist. Ähnlich der LM-Hashfunktion wird das Paßwort mit Nullen gefüllt oder gekürzt, damit der String 16 Byte groß ist.

Getting the Hash

Ein Zugriff auf die in der `SAM`-Datei abgelegten Hashes ist während der Laufzeit des Betriebssystems nicht möglich. Die liegt an der Verwendung der Dateien durch das System, genauer, durch die Datei `lsass.exe` aus dem Ordner `system32`, wodurch für alle Benutzergruppen jegliche Zugriffsmöglichkeiten und -berichtigungen entfallen. Weil die `SAM`-Datei nicht in Gebrauch ist, wenn es Windows nicht ist, ist es möglich, durch das Booten eines anderen Betriebssystems auf das Dateisystem zuzugrei-

fen und die SAM zu kopieren bzw. auszulesen und aus ihr die Hashes zu exportieren.

Seit dem Service Pack 3 für NT 4.0-Systeme hat Microsoft eine Datei namens syskey.exe in dem Ordner system32 implementiert. Laut Microsoft „bietet [diese Datei] starke Verschlüsselung der Kennwortinformationen in der Registrierung", das heißt, daß ein Auslesen der SAM nicht zum Erfolg führt, weil die Hashes zusätzlich mit dem system key (auch: bootkey) decodiert werden müßten. Außerdem sagt Microsoft, daß der „Systemschlüssel unter Verwendung eines komplexen Verschlüsselungsalgorithmus im lokalen System gespeichert wird". [1] Daraus kann man schließen, daß man den Systemschlüssel auslesen kann, sofern man weiß, wie er berechnet wird bzw. wo er abgelegt ist, und anschließend die aus der SAM exportierten Inhalte entschlüsseln kann (security by obscurity). Bei detaillierterer Betrachtung des Algorithmus erkennt man, daß die „starke Verschlüsselung" einzig eine Permutation aus vier speziellen Registry-Schlüsseln ist.



Das Programm Bkhive von Nicola Cuomo [2] greift auf die Datei system (im gleichen Ordner wie SAM) zu, liest aus ihr die Schlüssel aus der Registrierungsdatenbank aus und vertauscht diese, bis es den bootkey berechnet hat, und gibt ihn aus. Es gibt auch eine Möglichkeit, die Inhalte der SAM zur Laufzeit zu exportieren. Eine ist zum Beispiel, die Hashes aus dem Arbeitsspeicher auszulesen und auszugeben.

Dies ist möglich, weil Windows die SAM zur Laufzeit in Benutzung hat und bei der Authentifizierung des Benutzers das eingegebene Paßwort gehasht und mit dem Inhalt der SAM verglichen hat, somit der Inhalt der SAM im RAM (Random Access Memory) gespeichert wird. Für den Zugriff auf diesen Teil des Arbeitsspeichers sind administrative Rechte erforderlich. Ist ein Benutzerkonto nicht nur lokal, sondern auf der gesamten Domäne mit administrativen Rechten ausgestattet, hat es Zugriff auf den Speicherbereich, in dem die Hashes abgelegt sind, für jeden einzelnen Computer innerhalb dieser Domäne. Das Programm PwDump4 des Autors bingle [3] führt diese Schritte aus.

Angriffsszenarien auf die Hashfunktionen

Die drei Berechnungsschritte des LM-Hashs ermöglichen neue Angriffsformen: Es wird nicht wie oben die Hashfunktion angegriffen, sondern es werden die sicherheitstechnisch kritischen Schritte der Implementierung ausgenutzt. Der erste Schritt macht die Verwendung von Groß- und Kleinbuchstaben nutzlos und erhöht somit die Wahrscheinlichkeit eines erfolgreichen Angriffs, bei dem alle möglichen Zeichenkombinationen als Paßwort nacheinander eingegeben, anschließend gehasht und mit dem Hash des gesuchten Paßworts verglichen werden, bis eine Übereinstimmung erfolgt (brute force), weil sich die Zeichenanzahl um die der Kleinbuchstaben reduziert. Der dritte Schritt reduziert die maximale Länge aller Kombinationen bei dem Brute-Force-Angriff auf sieben Zeichen, da jeder Teil des LM-Hashs separat angegriffen und das endgültige Paßwort aus beiden Teilen anschließend zusammengesetzt wird.

Obwohl der NTLM-Hash in der Theorie mehr Sicherheit gewährleistet, ist dies in der Praxis nur relativ der Fall. Weil standardmäßig beide Hashfunktionen aktiviert sind, hebt der LM-Hash bei Paßwörtern mit weniger als oder genau 14 Zeichen die Verbesserungen des NTLM-Hashs auf. Sobald ein Angriff auf den LM-Hash erfolgreich war und das Paßwort in Großbuchstaben (und eventuell Zahlen bzw. Sonderzeichen) bekannt ist, müssen die Zei-

chen des Paßwortes lediglich noch per Brute-Force-Angriff auf den NTLM-Hash auf Groß- und Kleinschreibung überprüft werden. Dies dauert in der Praxis meist wenige Sekunden.

Aber auch wenn der LM-Hash deaktiviert ist, gibt es einige Methoden, den NTLM-Hash zu brechen. Weil viele Paßwörter weniger als 16 Byte groß sind, werden diese mit Nullen gefüllt. Deswegen kann ein reiner Brute-Force-Angriff hier ziemlich effizient sein, er benötigt unter Umständen nur wesentlich mehr Zeit. Aufgrund dessen, daß die Hashfunktionen nicht salted sind, das heißt, daß den Paßwörtern vor dem Hashen keine Zufallswerte hinzugefügt werden, sondern entweder mit Nullen aufgefüllt, gekürzt oder mit den Originalzeichen gehasht werden, ist es theoretisch möglich, alle möglichen Kombinationen zu berechnen und in einer Datenstruktur zu speichern, sodaß der Hash des gesuchten Paßworts mit den Hashes in den sogenannten rainbow tables verglichen werden kann und das dazugehörige Paßwort bei erfolgreichem Vergleich ausgegeben wird.

Rainbow tables

Der Einsatz von rainbow tables ist eine weitere effiziente Methode, entwickelt von Philippe Oechslin, um Hashes zu brechen. Rainbow tables sind im voraus berechnete Hash-Tabellen. Zwei verschiedene Algorithmen sind für diese Datenstruktur bedeutsam: zum einen der für die Generierung, zum anderen der zum Finden des Klartextes (lookup).

Der erste Algorithmus arbeitet wie folgt: Ein möglicher Klartext wird durch die Hashfunktion (zum Beispiel die LM-Hashfunktion) zu einem Hashwert transformiert. Anschließend wird dieser durch eine Reduktionsfunktion zu einem neuen Klartext mit der gleichen Länge abgebildet. Dieser Schritt wird n-mal wiederholt. Man nennt dies eine Kette (chain).

Von jeder Kette wird der Anfangs- und Endwert gespeichert. Auch dies wird n-mal wiederholt, sodaß es n Ketten gibt (die Länge aller Ketten ist konstant). Jeder einzelne Schritt der Ketten hat eine eigenständige Reduktionsfunktion, wobei jede Reduktionsfunktion bei dem gleichen Schritt aller n Ketten gleich ist. Auf diese Weise wird die Wahrscheinlichkeit einer Verflechtung der Ketten (Kollision) vermindert, weil die Reduktionsfunktionen nicht einheitlich sind und deshalb eine Übereinstimmung der Endwerte der Ketten wesentlich unwahrscheinlicher ist, weil eine Verflechtung theoretisch überall, praktisch aber nur bei den gleichen Reduktionsfunktionen auftreten kann.

Beim Finden des Klartextes zu dem gegebenen Hashwert passiert Nachstehendes: Der gegebene Hash wird mit der letzten Reduktionsfunktion auf einem Klartext abgebildet, welcher mit den Endwerten aller Ketten verglichen wird. Wenn keine Übereinstimmung erfolgt, wird der gegebene Hash, um eine Gleichheit mit dem vorletzten Klartext der Ketten zu überprüfen, mit der vorletzten Reduktionsfunktion reduziert, gehasht, mit der letzten Reduktionsfunktion auf den Endwert abgebildet und wieder mit den Endwerten aller Ketten verglichen. Dies wird so lange wiederholt, bis die Kette am Anfang angelangt ist oder bis eine Gleichheit gefunden wird.

Beim ersten Fall ist ein erfolgreicher lookup fehlgeschlagen und wird beendet, beim zweiten Fall wird die Kette, bei der die Übereinstimmung mit dem Endwert gefunden wurde, mit Hilfe des Startwerts dieser bis zu der letzten von dem gegebenen Hash verwendeten Reduktionsfunktion neu aufgebaut (zur Laufzeit neu berechnet). Der vorhergehende Klartext ist der Gesuchte. [4]

Ophcrack ist ein von Philippe Oechslin geschriebenes Programm [5], welches Hashwerte mit Hilfe von rainbow tables bricht. Die Ophcrack-LiveCD basiert auf der Linux-Distribution SLAX6 und beinhaltet sowohl Ophcrack als auch alphanumerisch vorberechnete rainbow tables.

Bootet man von der CD, startet SLAX6 automatisch Ophcrack. Letzteres liest die Hashes ähnlich wie PwDump4 aus und extrahiert sie, liest die rainbow tables ein und startet den Angriff auf die LM-Hashes. Nach kurzer Zeit sind die

alphanumerischen Klartexte gefunden und es wird per Brute-Force-Angriff die Art der Buchstabenschreibung überprüft, damit eine Übereinstimmung mit dem gegebenen NTLM-Hash besteht.

Schutzmaßnahmen

Bei einer Deaktivierung der Verwendung des standardmäßig aktivierten LM-Hashs wird eine Schwäche der Windows NT 5-Systeme abgeschaltet. Durch Verwendung starker Paßwörter wird ein Bruch des NTLM-Hashs erschwert. Viele Linux-Distributionen wie zum Beispiel Debian haben mehrere Hashfunktionen zur Speicherung des Paßworts implementiert, sodaß der User frei wählen kann, welche er bevorzugt, und fügen standardmäßig einen salt hinzu, sodaß Brute-Force-Angriffe erschwert und rainbow table attacks verhindert werden. Eine Vollverschlüsselung der Betriebssysteme, zum Beispiel durch AES17, verhindert jegliche Zugriffsmöglichkeiten auf das System außerhalb der Laufzeit.

MAC-Spoofing

Softwareseitig läßt sich die Quell-MAC-Adresse bei Windows NT 5-Systemen beliebig verändern. Der Treiber des Herstellers einer Netzwerkkarte liest zur Laufzeit die MAC-Adresse der Netzwerkkarte auf der Sicherungsschicht aus und übergibt sie der Network Driver Interface Specification (NDIS) von Windows, welche die MAC-Adresse in der Registry speichert. Die Programme changemac-win von Robbe De Keyzer [6] und MACAddressChanger von Nishant Sivakumar [7] ändern den Registry-Wert der MAC-Adresse und starten den Netzwerkadapter neu. Dies kann man auch ohne die Hilfe eines Programms machen. Beim Versenden eines Datenpakets wird diesem nun die gefälschte MAC-Adresse als Quell-MAC-Adresse eingetragen.

IP-Spoofing

Winsock ist eine API für Programmierer, welche es ermöglicht, auf den raw socket zuzugreifen. Ein raw socket ist eine spezielle Art des Sockets, welcher es ermöglicht, Pakete auf der Transport- und der Vermittlungsschicht zu verändern bzw. zu erzeugen. Deshalb kann man die Quell-IP-Adresse beliebig verändern. Weil nach der Veränderung die Header Checksum des IP-Headers nicht mehr übereinstimmt, muß dieser neu berechnet und in jedem gefälschten IP-Paket ausgetauscht werden.

Zusammenfassung

Alle demonstrierten lokalen Angriffsszenarien auf Microsoft Windows NT 5.0-, 5.1- und 5.2-Systeme zeigen, daß eine starke Paßwortsicherheit nicht gegeben ist. Die implementierten Hashfunktionen sind nicht sicher, die weniger sichere ist aus Gründen der Abwärtskompatibilität standardmäßig aktiviert. Die Hashes werden nicht salted, wodurch ein Angriff durch einen Brute-Force-Angriff erleichtert und durch rainbow tables ermöglicht wird.

Wie jede Art der Information kann man die vorgestellten Methoden dazu nutzen, um Schaden anzurichten, aber auch, um die Funktionsweise zu verstehen und daraufhin Präventionsmaßnahmen einzuführen. Sicherheit ist kein Zustand, sondern ein Prozeß.

[1] Microsoft: Windows NT-Systemschlüssel erlaubt starke Verschlüsselung des SAM, *http://support.microsoft.com/?scid=kb%3Bde%3B143475&x=22&y=6, 9.11.2004.*
[2] Cuomo, Nicola: Bkhive, *http://www.studenti.unina.it/~ncuomo/syskey/Bkhive.zip, 28.3.2004.*
[3] bingle: PwDump4, *http://www.mirrors.wiretapped.net/security/host- security/john/contrib/win32/pwdump/pwdump4.zip, 25.9.2003.*
[4] Oechslin, Philippe: Making a Faster Cryptanalytic Time-MemoryTrade-Off, *http://lasecwww.epfl.ch/pub/lasec/doc/Oech03.pdf, 26.5.2003.*
[5] Oechslin, Philippe: Ophcrack, *http://ophcrack.sourceforge.net, 2.8.2007.*
[6] De Keyzer, Robbe: changemac-win, *http://packetstormsecurity.org/Win/changemac-win.c, 31.12.2005.*
[7] Sivakumar, Nishant: MACAddressChanger, *http://www.codeproject.com/KB/applications/MacIdChanger/MACAddressChanger_Src.zip, 25.05.2005.*

Chinesewall – Internetzensur gibt es nicht nur in China

von gøph3r

Kurz vor den Olypmpischen Spielen in China veröffentlichte der CCC die national und international wahrgenommene Kampagne chinesewall.ccc.de.

Hinter der Kampagne stand eine Idee: Wir wollen Sportlern und Journalisten, die nach Peking fahren, Hilfe anbieten, um die Internetblockade zu umgehen.

Das Internationale Olympische Komitee hatte den Journalisten bei der Vergabe der Spiele an Peking vollständige Freiheits- und Pressefreiheit eingeräumt. Nun ruderten die Funktionäre in ihren Aussagen zurück – Grund für uns, praktische Hilfe anzubieten.

Wir sprachen mit Journalisten und Sportlern; auch ein Augenzeugenbericht aus Vietnam war ein Hinweis auf funktionierende Zensur in einem weiteren asiatischen Regime. Die technische Zensur findet in China durch die sogenannte „Great Firewall“ statt, die aus einer Reihe von Filter- und Blockiertechnologien besteht, die von US-amerikanischen und europäischen Firmen geliefert werden. Sie verhindern den Zugriff oder ändern den Inhalt abgerufener Webseiten wirkungsvoll.

Für die Informationsverbreitung und Aufklärung zu diesem Thema sollte eine leicht verständliche Webseite dienen; gleichzeitig lief die Pressearbeit an. Wir beantworteten die Anfragen und gaben Hilfestellung – nicht nur für von Zensur Betroffene in China. Durch die breite mediale Empörung über die Zensur des Internet in China rollte eine Welle von E-Mails über uns. Journalisten und Sportler konnten wir USB-Sticks anbieten, welche die Software TOR-Browser enthalten: der Freedom Stick.

Der Erfolg der Kampagne zeigte sich nach einem Monat: Wir hatten ca. 100.000 Downloads der Software von unserem lokalen Server zu verzeichnen.

CHINESEWALL.CCC.DE

Ronja

by Karel Kulhavy <twibright@hispeed.ch>

Ronja is a device that personifies both technological freedom and independency from potentially corruptible authorities. It is a DIY, garage-grade technology wireless optical Ethernet link 10 Mbps full duplex over 1.4 km. However, garage grade are only the material requirements for the manufacture. The typical bit error rate is better than one corrupted bit in a billion (10^-9) and the link works in heavy rain or snow, just doesn't work in fog.

Whereas radio spectrum up to the order of gigahertz is prone to interference and resulting disputes with neighbours, shifting the carrier five orders of magnitude higher – namely to 480,000 GHz – frees us from these nuissances. We also gain another advantage: This frequency is visible to the naked eye, which makes aiming the wireless link much easier.

Everyone is familiar with 480,000 GHz from brake lights of cars. The LED used to transmit information in Ronja is exactly the same as in the brake lights. While brake lights flash maybe few times per second, Ronja circuits are designed to flash the LED up to ten million times per second. This simple on/off modulation then carries binary data stream, for example a realtime DVD quality video.

After the light is created, it has to be delivered to the target place without wasting too much energy around. The pinnacle of optical technology, chinese die-cast window glass loupe lenses perform this task surprisingly well.

The received signal is detected with a very cheap, but very good performance silicon photodiode and amplified with an extremely sensitive broadband electronic amplifier. This amplifier and other circuits must be enclosed in tin-plated steel casing to keep electromagnetic waves away. This casing can be easily soldered from tin-plated metal boxes from IKEA.

It doesn't matter if the mechanical chassis looks crappy, but it must be watertight and keep its shape precisely stable over many years on the weather. Chimney flues and bathroom silicone sealant seem to be the household items of choice. Silicagel, little white balls from shoe boxes, is used to remove traces of humidity trapped inside the optical head.

One of the two most technologically difficult part of the whole system is the mechanical holder. It must withstand gale force winds without flexing and letting the beam away from the alignment axis and allow comfortable aiming adjustment with milliradian precision. The cur-

rent holder is made of drilled solid steel sections, but a new spaceframe construction welded from light thin steel pipes has been already developed. In both cases the alignment mechanism is based on screws and rubber blocks and offers a 1:300 gear ratio.

And what is the second most technological difficult part? It is the first stage of amplifier which is critical for sensitivity. A MOS tetrode (cascode), a transistor used at the input of TV receivers, is used here together with the photodetector in a very unusual configuration to get minimum noise. Electrical engineering people usually have serious problems understanding the idea behind the noise reduction, claiming that it cannot work.

Factory manufacture can afford expensive and hazardous processes and one-purpose tools. This is not possible when you are working in your cellar. Nevertheless, some methods had to be developed to reduce the complexity of the building process.

Drilling steel parts precisely according to a plan is pretty annoying, therefore the Ronja website offers drilling templates for download. Glue this template on a piece of steel and suddenly there is nothing easier than manufacturing a complicated steel part.

Complicated assemblies are complicated to understand. Therefore Ronja offers rotating 3D model videos modelled with U. S. Army BRL-CAD. BRL-CAD has been developed for already thirty years and is now free software.

Soldering many parts without making a mistake can be difficult. But the printed board contains sector codes printed on the edge and the same code is in the population partlist. This speeds up the population process tremendously, reducing error rate at the same time.

Shopping is an important part of the building process and it has been made easier with automatically generated partlists in spreadsheet format, where order numbers can be filled in and the file sent to the electronic parts shop. To

make sure parts are available as easy as possible worldwide and in small quantities, the whole electronics has been designed from low intelligence parts: discrete transistors, a simple video amplifier, individual logical counters and shift registers etc.

What if it doesn't work after building? Most people don't have an oscilloscope at home and have only rudimentary knowledge of electricity from the primary school. Therefore testing procedures have been developed to identify correctly or incorrectly working parts of Ronja using only a multimeter.

Building a Ronja is a very lengthy process, much more than going to a shop and buying a WiFi card. It takes about 70 hours. Fortunately, it's not boring: „It was very amusing for the whole course of building work. First I was afraid of it, but as soon as I started, it fascinated me immediately." (Filip Nemec)

At the end we have a carefully assembled medley of ridiculously cheap components that can connect our home to the Internet with optical wireless, a technology more modern than electromagnetic radio: „The feeling when the medley of components started to work and the first packet was transferred, cannot be compared to anything else." (Petr Sadecky)

Ronja is or was running on 153 registered installations worldwide. More information can be found at *http://ronja.twibright.com*

Das Chipkartenbetriebssystem ECOS

von Philipp Fabian Benedikt Maier

Wie in der Datenschleuder bereits angekündigt, habe ich für die geekKarte und eine breite Palette anderer Karten ein passendes Betriebssystem geschrieben. Der Name ECOS steht für Experimental Card Operating System. Daß es sich um ein experimentelles Betriebssystem handelt, heißt aber noch lange nicht, daß man es nicht auch produktiv einsetzen könnte. Es ist vielmehr auf die besonderen Bedürfnisse von Hackern zugeschnitten. ECOS ist vollständig in Assembler geschrieben und erschließt sich dadurch auch für Anfänger sehr leicht, da nicht erst eine komplexe Hochsprache erlernt und – schwieriger noch – ein Gefühl für den Bezug von der Hochsprache zur realen Maschine erlernt werden muß.

Der Programmierer findet im Repository ein recht reichhaltiges Angebot von Modulen und Programmen. So ist zum Beispiel schon ein Programm mitgeliefert, welches eine T=0 Smartcard (byteorientiertes Protokoll) ist. Dieses Programm ist standardmäßig aktiviert. Ohne weitere Einstellungen vornehmen zu müssen, baut make das Betriebssystem zusammen.

Es existieren noch weitere Programme bzw. Modi, diese sind aber experimentell und daher weniger interessant: Ein T=0 Memory-Card-Programm (für Karten mit kleinem Flash z. B. Jupiter1) sowie ein Telefonkarten-Programm, welches versucht, das 3-Draht-Protokoll der Telefonkarten (read-only) abzubilden. Es hat sich allerdings gezeigt, daß Prozessorkarten für diese Art von Anwendung völlig ungeeignet sind. Ein CPLD oder FPGA würden hier bessere Dienste leisten.

Außerdem gibt es noch ein Programm, welches lediglich einen ATR ausgibt, den man vorher selbst festlegen kann. Übrigens: Wer ECOS

Hacken ist...

nur mal kurz testen möchte, ohne sich gleich mit der kompletten Toolchain, AVR-Controllern und ASM auseinandersetzen zu wollen, findet im Paket auch schon fertig assemblierte Binärdateien, die direkt startfähig sind. Einfach flashen und los geht's!

Wer ECOS mit den Standardeinstellungen assembliert, wird eine Karte erhalten, die einen PIN-gesicherten EEPROM-Speicherbereich (bzw. read-only-Flash) hat. Drei fehlgeschlagene PIN-Eingaben führen zum Zerstören des EEPROM-Inhaltes. Ein Security-Watchdog ist auch eingebaut, dieser versucht sogenannte Glitch-Attacken zu detektieren. Dies geschieht dadurch, daß in sensiblen Bereichen die Bearbeitungszeiten der Abfragen verzögert und die Karte in einen „instabilen Modus" gebracht wird. Falls es nun zu einer Spannungsunterbrechung bzw. einem Reset vor Beenden der Abfrage kommt, wird die EPROM-Zerstörungsroutine ausgelöst.

Der Security-Watchdog bringt uns zum nächsten Thema: ECOS ist ein experimentelles Chipkartensystem und läuft auf Prozessoren der Firma Atmel. Von der Tatsache einmal abgesehen, daß ECOS „am Küchentisch" entwickelt wurde und dementsprechend mit Sicherheit irgendwo noch Softwarefehler aufweist, die sicherheitskritisch werden könnten, sind die Standard-Atmel-Prozessoren (Atmega, AT90S,...) keineswegs Security-Pozessoren, die man in sicherheitskritischen Anwendungen einsetzen sollte. Auch den Fusebits sollte man nicht unbedingt uneingeschränkt vertrauen.

Beim Programmieren habe ich übrigens die sehr interessante Erfahrung gemacht, daß sich immer wieder eklatante Sicherheitslücken eingeschlichen haben, von denen ich immer glaubte: „Das kann dir nicht passieren." Es handelte sich um die klassischen Lücken, die in der Welt der Chipkarten immer wieder zu Problemen geführt haben: Overflows durch falsche Längenbytes, ungültige Anfragen usw. Viele dieser Lücken habe ich gefunden, indem ich mir Angriffsszenarien für meine eigene Karte ausgedacht habe.

Ich persönlich habe mir mit ECOS einen kleinen Hackertraum erfüllt: In dem Ultrabay meines Notebooks und an meinem Rechner zu Hause befindet sich ein Towitoko Chipdrive. Zur Sicherung meiner Daten verwende ich EncFS. Meine Schlüssel habe ich auf einer ECOS-Karte, die ich stets bei mir trage. Wenn ich jetzt eine mit EncFS verschlüsselte Festplatte, USB-Stick, CD oder DVD mounten will, wird meine Karte und meine PIN verlangt und das Medium eingebunden. Wie im richtigen Hackerfilm!

Die Skripte dafür sind im übrigen dem Repository inklusive Beispiel-Cryptovolume zum Testen beigelegt, sodaß es gleich losgehen kann. Man sollte sich die Schlüssel natürlich irgendwo aufschreiben, zum Beispiel auf einem selbstgemachtem Mikrofilm. Doch wie das geht, erzähle ich euch ein anderes mal.

Informationen zu Ecos, der geekKarte und den anderen netten Spielereien findet man auf meiner Web1.0-Homepage: *http://www.runningserver.com/*

21th century digital bikes

von Gismo

Zwanzig Jahre gibt es sie schon, zwanzig Jahre lang führten sie ein stiefmütterliches Dasein. Niemand will so richtig etwas mit Fahrrädern zu tun haben, die mit einem Elektromotor angetrieben werden. So erreichen sie zwar nette Geschwindigkeiten, allerdings durch die Akkus, die man mitnehmen muß, auch ein beachtliches Gewicht. Die letzten Jahre haben nun ein paar bemerkenswerte Neuerungen sowohl bei der Technik der Räder selbst als auch bei den Rahmenbedingungen für solche Fahrzeuge gebracht. Drehen wir eine kleine Runde durch das Hands-on-Department und sehen mal, was der moderne Tüftler und Hacker heute so alles anstellen kann.

Seid ihr schon mal mit einem Elektromotor durch die Gegend gefahren? Mal generell gefragt: überhaupt irgendein Elektrofahrzeug, sei es nun das gute alte Fahrrad, ein E-Roller oder Auto? Wenn ich jetzt noch die Bedingung stelle, daß ein Hybrid-Fahrzeug (Plug-In hin oder her) nicht zählt, wird die Quote sich wohl selbst in den Technikkreisen der Datenschleuder-Interessierten der des breiten Straßenbildes anpassen. Blind geraten, 0,001%? Tausend Benzin-Fahrzeuge und ein E-Mobile. Vermutlich sind es momentan viel weniger, auf die Leserschaft der Datenschleuder umgelegt sind das dann ganze drei Leute. Ein Kreis, klein genug, daß man gerade noch alle persönlich kennt...

Die passende Zeit für mich, ein bißchen von der nahen Zukunft zu schwärmen und den Status Quo der Situation festzunageln. Ein Erfahrungsbericht und Pionierarbeit in einer Szene, die gerade erst anfängt, sich ihres Potentials bewußt zu werden. Die Bestandteile der Fahrzeugtechnik selbst, im Gegensatz zum Verbreitungsgrad von Elektrofahrzeugen, haben sich tatsachlich massiv weiterentwickelt. Gemeint ist nicht der letzte Stand der Entwicklung bei Einspritzdüsen und Gemisch-Regulatoren, sondern die Verfügbarkeit von modernen Elektromotoren und eine noch viel spannendere Entwicklung diverser Akkumulationstechniken für einen fahrzeugtauglichen Energieträger.

PWM – Pulsweiten-Modulation auf dem Radweg

Was ist mit den Motoren passiert? Was haben wir neues in der Hand? Bisher war der klassische Gleichstrom-Elektromotor mit seinen Schleifkontakten (Bürsten) in E-Bikes verbaut. Dieses Design ist wohl hinlänglich bekannt, wird im grundlegenden Physikunterricht ausschweifend behandelt und ist mit seinem Erfindungsjahr 1832 ein echter Klassiker.

Prinzipbedingt ist hier eine gewisse Drehzahl notwendig, die Kontaktbürsten sind Verschleißteile und der direkte Einsatz an einem Fahrzeugrad ist nur in Ausnahmefällen möglich. Die Kraft der Motoren wird meist aus der Drehzahl gewonnen und dann über ein weiteres mechanisches, verschleißendes Bauteil – nennen wir es Kupplung – erst auf die Antriebsräder übertragen. Kurz und gut: eine ganz alte Kamelle. Der moderne Ansatz verlangt – wie könnte es anders sein – einen Mikrocontroller und ein bißchen Code. Aber langsam, erstmal die Fachbegrifflichkeiten: Es geht um den bürstenlosen Außenläufer-Motor. Dieser bringt das passende Prinzip für das Konzept Elektrofahrrad. Was ist anders? Nun, so ziemlich alles, doch die zugrundeliegenden Funktionen des Elektromagnetismus werden natürlich nicht verändert. Ab dann wird aber alles ganz anders gemacht. Im Namen steckt schon, daß die alten Graphitschleifer, die meistens als Bürste einge-

setzt werden, ausgedient haben. Mechanische Kontaktflächen und somit Verschleißteile des Motors werden so auf die beiden Achsenlager reduziert. Der gesamte Motor wird als Nabenmotor in das Fahrzeugrad direkt eingebaut. Bei Fahrrädern sieht das dann aus wie eine riesige Trommelbremse. Ein weiterer Unterschied zum klassischen E-Motor ist die Kupferspule selbst. Sie ist fest an der Radgabel montiert und somit der Stator des Motors, gedreht wird nicht das Spulengewirr selbst, sondern der auf den Achsen gelagerte Magnetring des Motors.

So, und wie bekommt das Teil jetzt Feuer, sprich einen Drehimpuls? Die Spule des Motors wird an eine Verstärkerendstufe angeschlossen, genau wie bei der Soundanlage zu Hause. Hier kommt nun der Mikrocontroller ins Spiel, der die Endstufe ansteuert. Dort, wo bei dem alten System die Schleifer dafür sorgten, daß sich der Rotor immer im Wechselfeld weiterbewegt, wird das Wechselfeld nun von unserem kleinen Computer generiert und über die Endstufe in die Spule gepulst. Diese Pulsweiten-Modulation gibt dem Motor zusätzlich auch noch den Namen PWM-Motor. Der Dreheffekt ist derselbe, nur ist es möglich, den Motor wesentlich präziser anzusteuern. Anstelle der hohen Drehzahl beim Klassiker ist es mit der PWM möglich, dem Motor eine gewünschte Drehzahl zu geben bzw. ihn sogar gezielt an eine bestimmte Stelle zu drehen. CD-Rom und Festplattenmotoren arbeiten zum Beispiel mit demselben Prinzip, am Elektrorad darf es natürlich gerne etwas mehr Leistung sein.

Volle Kraft

Die Leistung und damit die notwendige Baugrösse des PWM-Motors ergeben sich, zumindest für alles, was am europäischen Strassenverkehr teilnehmen darf, aus den zuständigen Richtlinien des Gesetzgebers. Also eiskalt von der schönen und weitreichenden Technik rüber zu den Regularien, die einem im Weg stehen, besser gesagt: vorgegeben sind. Die EU-Richtlinie 2002/24/EC erlaubt seit 2002 den zulassungsfreien Betrieb sogenannter Pedelecs. Ein Elektrofahrrad gilt dann als Pedelec, wenn es nicht mehr als 25 km/h fährt, die Motorleistung nicht über 250 Watt geht und ein Tretsensor an den Pedalen angebracht ist, der das Gasgeben nur dann freigibt, wenn der Fahrer auch wirklich in die Pedale strampelt.

Nicht gerade viel Schwung, aber ein Anfang. Dafür bleibt das Pedelec versicherungsfrei, man braucht keinen Führerschein und kann trotzdem am Straßenverkehr teilnehmen und Radwege benutzen. Helmpflicht gibt es auch keine, ist also alles wie beim normalen Fahrradfahren. Promillegrenze und Verkehrstauglichkeit bleiben natürlich wie gehabt. Weiterer Vorteil ist ein extrem leises Fahrgeräusch, kein Knattern und Stinken, was es erlaubt, auch ohne Probleme mal über den Bürgersteig abzukürzen oder durch den Park zu rollen, ohne daß jemand mitbekommt, daß man gerade motorisiert unterwegs ist.

Ein kleines, aber gerade für den Ampelstart interessantes Luftloch in der Regelung zur Leistung des Motors ist es, daß bis zu einer Geschwindigkeit von 6 km/h keine Leistungsbeschränkung vorgeschrieben ist. Es ist also möglich, für das Anfahren den Motor auf weit über 0,25 kW zu fahren. 1 bis 3 kW wären je nach Motor für den Schnellstart legal, und man fühlt sich wie vom Gummiband abgeschossen. Das kostet zwar ordentlich Akkuleistung, die auf gerader Strecke mehreren Kilometern Reichweite entsprechen kann, ist es aber gerade im Stadtverkehr wert, Stop and Go mit Fun-Faktor, ohne anstrengendes Pedale quälen.

Fahrzeugbau

Nun aber los. So ein E-Bike will erstmal gebaut werden, Massenware aus China ist zwar vorhanden, da die ganze Sache aber noch so weit

in den Kinderschuhen steckt, empfiehlt es sich, ein modulares System, also einen Motorbausatz an ein vorhandenes Fahrrad zu verbauen. Als Grundlage dient ein normales Fahrrad, alles, was nicht älter als 15 oder 20 Jahre ist, sollte hinsichtlich der Achsen, Pedalen und Lenkergriffe standardisiert sein. Ob es nun ein Mountainbike, Cityflitzer oder Tourenrad ist, spielt keine Rolle. Alles mit Rädern von 20 bis 28 Zoll läßt sich in wenigen Stunden motorisieren.

Was kommt alles in den ersten Bausatz rein?

Nabenmotor (20" bis 28")

Zur besseren Verteilung des Gewichts am Fahrrad wird bei den meisten E-Bikes der Nabenmotor in das Vorderrad verbaut. Je nach Leistung und Hersteller wiegen diese zwischen drei und acht Kilogramm. Die Akkus kommen dann mittig oder hinten auf den Gepäckträger, was einen gewissen Gewichtsausgleich schafft.

Controller (beinhaltet die digitale PWM-Steuerung und eine Leistungsendstufe)

Das Herzstück des ganzen Pedelec-Bausatzes ist ein digitaler Mikrocontroller, der die angeschlossene Leistungsendstufe befeuert. Das für die Motordrehung notwendige PWM-Signal wird von dem Mikrocontroller generiert und über eine (z. B. 20 A) Leistungsendstufe aus MOSFETs in die Spule des Nabenmotors gepulst. Dabei ist mit einiger Hitzeentwicklung zu rechnen, und die thermische Ableitung am Controller spielt eine wichtige Rolle. Es ist zu überlegen, diese Abwärme als Akkuheizung zu nutzen.

Tretsensor (aktiv oder passiv)

Das wichtigste Bauteil, um den gesetzlichen Regelungen eines Pedelecs zu entsprechen, ist der Tretsensor, der die Motorleistung nur dann freigibt, wenn der Fahrer auch wirklich in die Pedale tritt. Hierfür ist nicht entscheidend, mit welcher Kraft dies erfolgt: Ein leichtes Drehen an der Kurbel – und nach knapp einer Umdrehung ist die volle Motorleistung freigegeben.

Unterschieden wird zwischen passivem und aktivem Tretsensor. Der passive gibt lediglich das Handgas frei, sodaß erst dort die Motorleistung geregelt wird. Bei aktiven Tretsensoren wird abhängig von der Trittfrequenz direkt die Motorleistung mit zugeschaltet, ein extra Gasgeben entfällt damit, und es ist auch möglich, komplett ohne Gasgriff zu fahren. Dieses Modell wird gern „Fahren mit Rückenwind" genannt.

Die meisten Controller geben bei fehlendem Tretsensor das Gas direkt frei und riegeln nicht etwa die Motorleistung total ab. Erfahrungsgemäß kann es häufiger – und gerade im Stadtverkehr – passieren, daß das Kabel vom Tretsensor rausrutscht.

Gasgriff (Drehgriff, Daumenhebel)

Wie früher auf dem Mofa wird der Gasgriff als Drehgriff am rechten Lenker montiert: runterdrehen, und los geht es. Wie oben beschrieben natürlich nur, wenn man vorher den Tretsensor bedient. Optional, aber sehr angenehm, ist es möglich, die Gasgriffe mit Tempomat zu bekommen, was ein sehr angenehmes Fahren erlaubt. Zur Sicherheit sind dann aber Bremsgriffe mit Mikroschalter notwendig, die den Tempomaten abschalten, wenn man die Bremse bedient.

Und nochmals volle Kraft!

Tja, die Leserschaft wird's gemerkt haben, das ist hier alles triviale Technologie. Betrachtet man den Motor und die PWM-Technik, sind es alles Techniken der letzten Jahrzehnte: ausgereift und – bis auf den Nischenmarkt Elektrofahrrad – auch in der Massenproduktion. Nach vielen Gesprächen und Diskussionsrunden mit Technikern, Hackern und Bastlern rutscht ein Thema nach nur kurzer Zeit zum aktuell wunden Punkt der ganzen Sache: die Akkus. Kommen wir also zum heißesten Teil in der Debatte Elektrofahrzeug: Wie nehmen wir die Kraft mit an Bord? Zu den Rahmendaten: Wir fahren unsere Testfahrzeuge mit 36/48 Volt. Je nach Hersteller und Motortypen geht die Spanne noch weiter: 12/24 Volt bei den kleinen Baumarkt-Bikes, bis 72 Volt für Lasten und Dreiräder sind auf dem Plan.

Mit der Akku-Debatte befindet man sich mitten in der Zwickmühle zwischen a) Kapazität b) Gewicht c) Haltbarkeit (Ladezyklen) und d) Preis. Gleich vorweg: Alle Akku-Probleme lassen sich mit Punkt d) lösen, das ist aber wegen der Wirtschaftlichkeit eines E-Fahrzeuges und dem vorhandenen Budget nicht das Allheilmittel.

Ein Beispiel aus der Praxis: Mein kleines Klapprad mit Vorderradmotor (ein Crystalyte 4011) fährt mit 48 Volt. Ich hab ein Bleigel-Akkupack mit 7,3 Ah an Bord. Dieser hat dann das stattliche Gewicht von zehn Kilogramm, was nochmals etwa die Hälfte des gesamten Fahrzeuggewichts ausmacht. Das Akkupaket ist mit unter hundert Euro noch die günstigste Lösung. Allerdings ist Bleigel wohl die ungeeignetste Akkutechnik für unsere E-Bikes, nach nur ein paar hundert Ladezyklen geht die Kapazität um ein Drittel bis die Hälfte flöten. Bei Temperaturen unter zehn Grad hat man selbst mit frischen Akkus denselben Effekt: Die Leistung der Packs bricht zusammen.

Eine warme Verpackung für das Akkupaket wird also zusätzlich erforderlich, thermisch isolieren hilft, da die Akkus bei Belastung eine gewisse Temperatur entwickeln. Bei größeren Paketen – gerade in Elektroautos – rentiert sich eine Akkuheizung schnell. Das bißchen Energie, das man braucht, um ein gut isoliertes Paket bei zwanzig Grad zu halten, steht in keinem Verhältnis zum Verlust durch unterkühlte Akkus.

Noch ein Punkt, der gegen die für uns aktuell einzig bezahlbare Lösung Bleigel-Akku spricht, ist die Belastung, die der Motor produziert. Peakströme über 20 Ampere sind keine Seltenheit, und Dauerbelastungen bei 10 Ampere sind die Regel. Wo eine Starterbatterie 100 Ampere Pulse locker abkann, bringt man die Bleigel-Akkus mit solchen Belastungen schnell an ihr Ende. Leider sind sie dann nicht nur leergefahren, sondern nach kurzer Zeit schon kaputt. Lithium-Ionen-Akkus und ein großer Pufferkondensator werden für uns die Zukunft sein, allerdings mit dem entsprechenden Preis, ein erstes Testpaket mit der neuen Technik und der gleichen Kapazität (7,3 Ah) wird über 400 Euro kosten. Mit Heizung und Puffer kommt ein solches Paket noch eine Ecke teurer. Das ganze Ding wiegt dann zum großen Vorteil vier anstelle von zehn Kilogramm, was bei dem Gesamtgewicht des Fahrzeuges zwanzig Prozent Unterschied macht. 12 oder 20 Ah Akkupacks wären dann hinsichtlich des Gewichts an einem normalen Fahrrad auch realistisch.

Atomare Datenkrake

von Johann Kleinbrenn (3bornjohn@gmail.com)

Ein etwas tieferer Blick in Apples „DRM-freie“ Musik-Downloads

Am 2. April 2006 kündigte der CEO des Plattenlabels EMI, Eric Nicoli, in einer kurzfristig anberaumten Pressekonferenz an, EMI-Musik werde im Download künftig ohne die bis dato bei kommerziellen Quellen üblichen Restriktionen erhältlich sein. Special Guest bei dieser Veranstaltung: Steve Jobs. Apple begann dann am 30. Mai damit, im firmeneigenen iTunes Music Store (iTMS) Titel aus dem EMI-Katalog ohne Kopierschutz zu verkaufen. In der Presse wurde dies ausgiebig als das „Ende von DRM“ gewürdigt. Steve Jobs, der vorher in einem flammenden Plädoyer auf den sich bereits abzeichnenden Niedergang von DRM öffentlichkeitswirksam aufgesprungen war, wurde voller Bewunderung als Retter der Musik, der Konsumenten und Visionär im allgemeinen gefeiert.

Im quasi-religiösen Jubelwahn, der bei solchen Gelegenheiten insbesondere in der Apple-affinen Presse und Nutzerschaft regelmäßig ausbricht, ging dann einigermaßen unter, daß diese offenbar in einem Anfall von Neusprech „iTunes-Plus“ benannten Musikdateien zwar keinen harten Kopierschutz mehr besitzen, aber mitnichten frei von DRM-Mechanismen sind. Zunächst wurde verschiedentlich ([0],[1]) darauf hingewiesen, daß die schon in kopiergeschützten iTMS-Dateien eingebetteten Metadaten über den Käufer auch in den PlusGut-Dateien vorhanden sind.

Die EFF beschäftigte sich noch etwas näher damit und weist darauf hin, daß wohl weit mehr käuferspezifische Daten vorhanden sein könnten. [2] Sie berichtet unter anderem von erheblichen Größenunterschieden zwischen mittels unterschiedlicher Accounts erworbenen Dateien des gleichen Songs. Sie halten auch die Einbettung von Wasserzeichen für möglich; das eigentliche Audiosignal sei zwar nach der Konvertierung in ein anderes Format identisch, aber die Wasserzeichen könnten auch in den internen Tabellen des AAC-Formats versteckt sein. Eine detailliertere Untersuchung findet sich bei der EFF aber nicht, hierfür würde es an „in-house expertise on MPEG codecs“ mangeln. Wie sich herausstellt, bedarf es dieser aber auch nicht unbedingt...

Analyse

Musik wird im iTMS als AAC-codiertes Audiosignal, eingebettet in einen MPEG4-Container, verkauft. MPEG4-Container bestehen aus „Atome“ genannten Blöcken. Ein Atom besteht (in dieser Reihenfolge) aus einer 32 Bit breiten Längenangabe, einem FourCC-Code für den Typ des Atoms und den eigentlichen Daten; die Längenangabe schließt die 8-Header-Bytes mit ein. Atome können wiederum Atome enthalten, sodaß eine hierarchische Struktur entsteht. In den Werkzeugkasten zur Analyse dieser Struktur gehören spezialisierte Atom-Parser und -Manipulatoren wie AtomicParsley [3] und Dumpster [4] ebenso wie der persönliche Lieblings-Hexeditor.

Auf „atomarer Ebene“ enthält eine PlusGut-Datei zwei Hauptzweige: eine Audio-Spur mit den AAC-Daten sowie einen applikationsspezifischen „UserData“-Zweig, welcher die Metadaten enthält. In den Metadaten lassen sich relativ leicht Atome identifizieren, welche direkt oder indirekt auf den Käufer verweisen; bei den untersuchten Vergleichsdateien (gleiche Songs, unterschiedliche Käufer) unterscheiden sich die Werte der Atome `apID` und `purd`.

Ersteres enthält den iTMS-Accountnamen im Klartext, letzteres das sekundengenaue Kaufdatum. Diese Daten sind auch in den kopiergeschützten iTunes-Dateien enthalten und werden von iTunes im Info-Bereich angezeigt. Die PlusGut-Dateien unterscheiden sich aber auch in dem der AAC-Spur zugeordneten Bereich der Datei. Apple bettet hier relativ tief in die Atom-Hierarchie ein proprietäres, undokumentiertes Atom ein, das den Typ `pinf` hat und bei allen untersuchten Dateien exakt 32 KB groß ist. Unspezifizierte Atome sind für Player kein Problem, solange sie keine für die Wiedergabe benötigten Daten enthalten; durch die Längen- und Typangaben im Header können sie beim Parsen übersprungen werden.

Der Datenteil des `pinf`-Atoms ist zwar (afaik) nicht öffentlich dokumentiert, ein Blick auf die Binärdaten legt aber die Vermutung nahe, daß es sich wiederum um eine Atom-Struktur handelt. Folgt man dieser Hypothese, ergibt sich die in der Abbildung dargestellte Struktur von Kind-Atomen.

Der Datenteil des `righ`-Atoms scheint keine vollwertigen Atome zu enthalten, es fehlt jeweils die Längenangabe. Stattdessen scheint es sich um bis zu zehn „Pseudoatom“-Paare aus einer FourCC-Feldbezeichnung und einen 32-Bit-Datenteil zu handeln. Nicht alle dieser Pseudo-Atome sind immer vorhanden; das `mode`-Pseudoatom findet sich beispielsweise nur bei bestimmten Werten des `tool`-Pseudoatoms. Der nicht benutzte Rest der 80 zur Verfügung stehenden Bytes ist mit Nullen aufgefüllt.

Bei allen untersuchten Dateien war der Datenteil der `frma`, `schm`, `cert`, `veID`, `plat`, `aver`, `medi` und ggf. `mode`-(Pseudo-)Atome mit den in der Abbildung gezeigten Werten belegt; aus Sicht der Frage, welche käuferspezifischen Daten eingebettet werden, sollten sie folglich nicht weiter interessant sein. Über den Inhalt einiger anderer Atome lassen sich – auch durch die Art, wie sie variieren – zumindest qualifizierte Vermutungen anstellen:

`user`: Ist bei allen mit einem bestimmten Account erworbenen Dateien identisch, variiert aber von Account zu Account; scheint eine eindeutige Benutzer-ID zu sein,

`tran`: Ist identisch für alle zusammen gekauften Dateien, auch für unterschiedliche Alben/Künstler; wahrscheinlich eine Transaktions-ID,

`song`: Ist jeweils für einen bestimmten Song identisch, auch über verschiedene Käufer hinweg, und entspricht dem Inhalt des `cnID`-Atoms im Metadatenzweig. Möglicherweise eine eindeutige ID des Musikstücks,

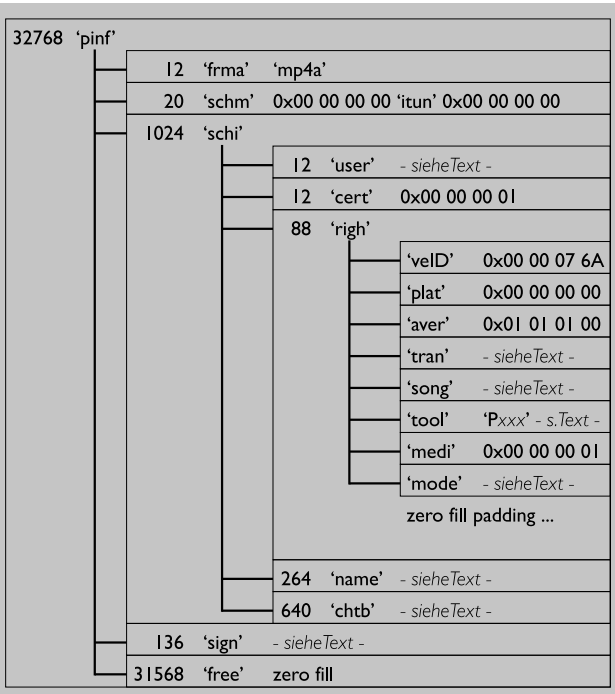
`tool`: Enthält offenbar einen FourCC, typischerweise der Form `Pxxx`, wobei xxx eine dreistellige Nummer ist. Könnte eine Art Versionsnummer der erzeugenden Software sein,

`name`: Enthält den Namen des Käufers im Klartext, der Rest der 256 Bytes ist mit Nullen gefüllt,

`sign`: Enthält zufällig aussehende Binärdaten, die in jeder Datei – also auch bei gleichem Käufer, Kauf, Künstler, Album etc. – unterschiedlich sind. Der FourCC und die Länge legen nahe, daß es sich um eine Signatur handelt.

Die große Unbekannte ist das `chtb`-Atom; der FourCC entzieht sich einer naheliegenden Interpretation. Der Datenteil ist bei allen untersuchten Dateien ähnlich dem `sign`-Atom mit zufällig wirkenden Binärdaten gefüllt, die sich, ebenso wie beim `sign`-Atom, von Datei zu Datei unterscheiden.

Neben diesen „direkt“ personenbezogenen Daten gibt es ein weiteres Merkmal, welches zumindest indirekt auf den Käufer einer Datei weist. In verschiedenen Atomen sind Zeitstem-



Aufbau des 'pinf'-Atoms (Größe / Typ / Inhalt)

pel für Erzeugung und Veränderung vorgesehen, die sich beispielsweise mittels Dumpster auslesen lassen. Das Einbetten der `pinf`-Daten in den Soundtrack ist eine Modifikation, und das Tool, das dies erledigt, setzt offenbar (und korrekterweise) das Modifikationsdatum der betroffenen TrackHeader-(`tkhd`) und MediaHandler-(`mdhd`)Atome der Tonspur.

In den untersuchten Dateien entspricht dieser Zeitstempel nach Auflösung der Zeitzonenzuordnung mit wenigen Minuten Abweichung dem in den Metadaten abgelegten Purchase Date und mit wenigen Sekunden Abweichung dem Zeitpunkt des Downloads; wahrscheinlich wird die Spur „on the fly“ beim Download mit dem `pinf`-Atom versehen. Mit diesem Zeitstempel könnte es Apple bzw. allen, die einen Zugriff auf die iTMS-Kundendatenbank haben, möglich sein, eine „in the wild“ gefundene PlusGut-Datei einem Käufer zuzuordnen oder zumindest den Kreis der in Frage kommenden Personen stark einzugrenzen. Dies gilt natürlich um so stärker, falls nicht nur eine einzelne Datei, sondern zum Beispiel ein ganzes Album untersucht werden kann.

Und schließlich gibt es noch eine weitere Merkwürdigkeit, dieses mal wieder im Metadaten-Zweig. Dieser enthält u. a. auch ein MediaHandler-Atom, das gemäß Längenangabe 34 Bytes groß ist. Es enthält aber nur 33 Bytes spezifizierte Daten; das letzte Byte ist undefiniert. Eine naheliegende Erklärung wäre ein Padding, aber das Byte ist weder Null, noch scheint es einen rein zufälligen Wert zu haben.

Alle in einer einzigen Transaktion gekauften PlusGut-Dateien enthalten hier jeweils den gleichen Wert; mit verschiedenen Accounts gekaufte Dateien eines bestimmten Titels hingegen unterschieden sich. Der Wert bleibt in manchen Fällen über mehrere Transaktionen (und unterschiedliche Werte des `tool`-Pseudoatoms) hinweg gleich, manchmal wechselt er um kleine Differenzen.

Es liegt natürlich nahe auszuprobieren, ob und wie iTunes auf eine Manipulation all dieser Daten reagiert. Weder das Überschreiben der Datenbereiche der diversen diskutierten Atome (inklusive des `sign`-Atoms) noch ein Verändern der Zeitstempel oder das völlige Entfernen des Metadaten-Zweigs veranlassen die untersuchten iTunes-Versionen zu irgendeiner erkennbaren Reaktion; lediglich das Löschen des `pinf`-Atoms führt dazu, daß iTunes die Datei nicht mehr als „purchased“ listet.

Zusammenfassung und Bewertung

Apple bettet in die PlusGut-Dateien also Daten ein, die offensichtlich personenbezogen bzw. Account-spezifisch sind und die für die Wiedergabe der Audiosignale – dem eigentlichen Zweck der Dateien – nicht benötigt werden. Besonders kritisch ist, daß Apple offenbar nicht gewillt ist, offenzulegen, um welche Daten es sich konkret handelt. [4] Kommt eine PlusGut-Datei, beispielsweise durch Diebstahl eines iPods, abhanden, so ist derzeit unklar, welche persönlichen Daten damit ebenfalls in falsche Hände gelangt sind. Dies ist keineswegs eine Bagatelle, schließlich verfügt Apple im iTMS zum Beispiel über Informationen wie die Kreditkartendaten der Käufer.

Es stellt sich die Frage, wie Apple seinen Kunden gegenüber einen solchen Umgang mit deren Daten rechtfertigen will. Erwirbt man beispielsweise ein Buch, egal ob online oder in einer Buchhandlung, stempelt der Händler ja auch nicht zwangsweise den Namen des Käufers, Kaufdatum, Kundennummer etc. hinein. Und dieser Vergleich trifft die Situation noch nicht einmal wirklich: Tatsächlich entspricht Apples Gebaren eher dem Einkleben eines versiegelten Umschlags mit persönlichen Daten des Kunden, ohne daß für diesen erkennbar ist, um welche Daten es sich handelt, ob sie korrekt sind und wer den Umschlag öffnen und die Daten lesen kann. Apple scheint das Grundrecht auf informationelle Selbstbestimmung nicht sonderlich ernstzunehmen – oder zumindest nicht bei iTMS-Kunden...

Notwehr

Wie das mit Grundrechten so ist, sie fallen weder vom Himmel noch weisen sie die Persistenz von Naturgesetzen auf. Sie müssen (meist bitter) erstritten werden, und wenn sie nicht aktiv genutzt werden, tendieren sie dazu, zu vaporisieren.

Als Grundrechtselbstverteidigungswerkzeug eignet sich `AtomicParsley`. Es besitzt mit ‚`--manualAtomRemove`' die Fähigkeit, gezielt Atome zu löschen.

Damit sich dies auf das `pinf`-Atom anwenden läßt, ist zusätzlich die Option `--DeepScan` als zweiter (!) Parameter zu verwenden. Das zu entfernende Atom muß als vollständiger Pfad der FourCC-Types des Atom-Pfades zu diesem angegeben werden; dieser läßt sich ebenfalls mit AtomicParsley ermitteln (`-T`). AtomicParsley löst auch das Problem der Modification Dates in der Tonspur, da es diese beim Entfernen des `pinf`-Atoms korrekt updatet.

Think different!

Ein nicht trivial zu lösendes Problem bildet das „mysterious byte“ im Metadaten-Handler, da beim Löschen des entsprechenden Atoms auch alle Metadaten verlorengehen. Will man sich dieses Bytes entledigen, muß man die sinnvollen Metadaten (Author, Title etc.) zunächst auslesen und nach dem vollständigen Löschen der Metadaten (`--metaEnema`) wieder einfügen.

Vorsicht ist übrigens bei vielen im Netz kursierenden Anleitungen zur „Entpersönlichung“ von PlusGut-Dateien geboten: Die einfacheren beschränken sich auf das Entfernen einiger Metadaten-Atome und ignorieren u. a. das `pinf`-Atom völlig. Die Autoren haben sich offenbar nicht einmal die Mühe gemacht, an den Resultaten den einfachen, schon in [0] erwähnten strings-Test durchzuführen, bevor sie diese „Anleitungen“ veröffentlicht haben. Die besseren erwähnen immerhin noch das `pinf`-Atom und verweisen auf im Umgang mit diesem geeignete Werkzeuge, eine Erwähnung der Modification Dates oder des „mysterious bytes“ fand sich aber nirgends.

Nach einer entsprechenden Kur und einem manuellen Angleichen der Modification Dates (z. B. mittels Dumpster) sind mit unterschiedlichen Accounts erworbene Dateien des gleichen Songs auf Bitebene identisch. Dies zeigt, daß keine weiteren käuferspezifischen Daten z. B. in der Art der Belegung der Sample-Tabellen versteckt sind; dahingehende Vermutungen bestätigen sich also (zumindest für die untersuchten Dateien) nicht. Dies muß aber nichts heißen: Das MP4-Format bietet hinreichend Möglichkeiten für einen solchen versteckten Kanal, und Apple könnte dies jederzeit implementieren, ohne damit die Formatspezifikation zu verletzen oder die Dateien prinzipiell für andere Player ungenießbar zu machen.

Fazit

Diese Analyse muß letztlich unvollständig bleiben: Es konnte natürlich nur ein verschwindend kleiner Teil der möglichen Kombinationen aus Musikstücken, länderspezifischer iTMS-Version und den offenbar vorhandenen zeitlichen Formatvariationen untersucht werden; keine der untersuchten Vergleichsdateien wies beispielsweise die von der EFF beobachteten Grössenunterschiede auf.

Besonders unbefriedigend ist natürlich die Erkenntnislage bzgl. des chtb-Atoms, da dieses personenbezogene Daten unbekannter Art zu enthalten scheint. Hier besteht die Notwendigkeit zu weiteren Forschungsanstrengungen engagierter Datenreisender. Diesbezügliche Auskünfte von Apple selbst, was sie mit den persönlichen Daten ihrer Kunden anstellen und was sie diesen auf deren Datenträger schreiben, sind, obwohl eigentlich selbstverständlich, offenbar nicht zu erwarten.

[0] *http://www.tuaw.com/2007/05/30/tuaw-tip-dont-torrent-that-song/*
[1] *http://arstechnica.com/news.ars/post/20070530-apple-hides-account-info-in-drm-free-music-too.html*
[2] *http://www.eff.org/deeplinks/2007/05/apples-drm-free-aac-files-contain-more-just-names-and-email-addresses*
[3] *http://atomicparsley.sourceforge.net/*
[4] *ftp://ftp.apple.com/developer/Quicktime/Tools/Programmers_Tools/Dumpster.dmg*
[5] *http://www.heise.de/newsticker/meldung/90666*

Capture the Flag in der IT-Sicherheit

von Hans-Christian Esperer

Im Zeitalter der globalen Kommunikation ist der Punkt Sicherheit bei der Softwareentwicklung nicht mehr wegzudenken. Nicht nur durch das Internet ist unsichere Software ständigen Gefahren durch Angriffe ausgesetzt: USB-Sticks, CD-Rs und mobile Festplatten sind heute Massenware und ermöglichen einen regen Datenaustausch auch „offline". Auch bei Anwendungen wie beispielsweise einem MP3-Player muß auf Sicherheit geachtet werden – eine manipulierte MP3-Datei sollte nicht zum Absturz des Players führen und schon gar nicht zur Ausführung von Programmcode. Dieses Szenario ist allerdings gar nicht weit hergeholt; gerade Autoren von Software, die nicht direkt mit dem Internet zu tun hat, achten oftmals nicht so sehr auf Sicherheit.

Aber auch mit neuen Technologien wie beispielsweise dem Trusted Platform Module (TPM) kommt man ohne fundierte Kenntnisse zum Thema sichere Software nicht sehr weit. Man kann zwar heute durch die sogenannte „Remote Attestation" und das „Platform Sealing" feststellen, ob ein Computer und die auf ihm installierte Software manipuliert wurde. Doch auch nicht-manipulierte Software hilft nicht viel, wenn sie Sicherheitslücken enthält.

Ein wichtiger Punkt beim Schreiben sicherer Software ist das Erkennen, wo überhaupt Probleme auftauchen können. Genau darum geht es bei einem Capture-the-Flag-Wettbewerb (CTF).

In einer simulierten Umgebung wird bewußt unsicher geschriebene Software betrieben. Diese Umgebung wird vom Veranstalter eines CTF bereitgestellt – meist in Form eines Images für eine virtuelle Maschine wie vmware, qemu/kvm oder XEN. Auf diesem Image befinden sich Programme, die über das Netzwerk verwendet werden können (sogenannte Dienste), inklusive Source-Code. Meist gibt es auch ein oder zwei „Binary-Only"-Dienste, bei denen der Source Code nicht beiliegt; dies ist jedoch die Ausnahme.

Das fertig präparierte Image wird an die CTF-Teilnehmer verteilt, die in Teams organisiert sind. Die Teams müssen jeweils einen Internetserver mit Hilfe des bereitgestellten Images betreiben. Die Teams sehen sich die Software an und suchen nach Sicherheitslücken und Stabilitätsproblemen. Gefundene Probleme werden auf dem

eigenen Rechner behoben. Gleichzeitig werden sie auf den Rechnern der anderen Teams ausgenutzt. Dies ist solange möglich, wie die entsprechenden Schwachstellen von den anderen Teams noch nicht behoben wurden.

Die Bewertung der Teams erfolgt durch den sogenannten Gameserver. Dieser simuliert einen normalen Benutzer, der die angebotenen Dienste nutzen möchte. Er hinterläßt dabei seine privaten Daten (sogenannte Flags). Später schaut er, ob diese Daten noch vorhanden sind. Falls ja, bekommt das entsprechende Team einen Defensivpunkt. Falls ein anderes Team durch Ausnutzung einer Schwachstelle an die Flags gelangt, die der Gameserver abgelegt hat, kann dieses Team die Flags an den Gameserver schicken – als Beweis für einen erfolgreichen Angriff (daher der Name Capture the Flag); hierfür gibt es Offensivpunkte.

Je nach CTF gibt es auch noch Punkte für Advisories – standardisierte Fehler- und Exploitbeschreibungen – sowie für regelkonformes Verhalten.

Bei großen CTFs wie dem von der University of California in Santa Barbara organisierten USCB CTF, dem CIPHER CTF der RWTH Aachen und Uni Siegen oder dem von der TU Darmstadt organisierten da-op3n treten meist Teams von Universitäten aus aller Welt an. Bei kleineren CTFs, die meist auf Kongressen und anderen Veranstaltungen, wie beispielsweise dem Easterhegg oder den Meta-Rhein-Main-Chaostagen stattfinden, treten die Teams vor Ort gegeneinander an.

Auch auf dem 25c3 wird es dieses Jahr einen CTF geben. Wer also schon immer mal bei einem CTF mitmachen wollte oder einfach nur mal schauen will, wie sowas abläuft, sei an dieser Stelle herzlich eingeladen teilzunehmen! Große Vorkenntnisse braucht man nicht dafür, im Gegenteil: Man lernt viel durch die Teilnahme.

Interesse? Dann suche Dir ein Team oder bilde selbst ein neues. Wenn Du eh auf den Congress kommst, braucht Du nichts außer einem Laptop; wir kümmern uns um alles weitere. Sag' uns vor Ort einfach bescheid, daß Du teilnehmen möchtest. Wenn Du von außerhalb teilnehmen willst, brauchst Du eine schnelle Internetverbindung und mindestens zwei Rechner. Einer dient als sogenanntes VPN-Gateway. In diesem Fall mußt Du Dich auch im voraus registrieren, das geht hier: *http://ctf.hcesperer.org/25c3ctf/register.py* Auf dieser Seite gibt es auch weitere Informationen.

Wir hoffen auf rege Beteiligung.

Easterhegg 2008

von Pallas & maha

Das Easterhegg ist eine CCC-Veranstaltung mit Teilnehmerzahlen um die 250 Leute. Wie der Name nahelegt, findet das Easterhegg jedes Jahr über die Ostertage statt. Die Ortsangabe ist nicht so einfach, denn der Ort wechselt. In den ungeraden Jahren steht die Antwort fest: Hamburg. In den geraden Jahren „wandert" das Easterhegg. Veranstalter waren schon die CCC-Gruppen in Düsseldorf, München und Wien. Dieses Jahr reiht sich Köln ein. Ein schöner Grund, Deutschland und seine Nachbarstaaten zu bereisen.

Laut älteren Clubmitgliedern ist das Easterhegg heute so, wie die Congresse früher mal waren: entspannt, eher familiär, man kennt sich. Der Nostalgiefaktor wird dadurch unterstützt, daß die Hamburger Easterheggs in demselben Gebäude stattfinden, in dem von 1984 bis 1997 die Congresse stattfanden. So haben auch Nachwuchs-Chaoten die Chance, den Congress-Anfängen nachzuspüren.

Die CCC-ler MiGri, Pirx und sz hatten die Idee zum Easterhegg Mitte 2000. Die drei waren nicht nur im CCC, sondern auch als Funkamateure aktiv. Da sich der Congress von „eher Workshops" zu „viele Vorträge" entwickelt hatte, war der passende Rahmen für ihre Funk-Workshops weggefallen. Funkwissen läßt sich schlecht als Vortrag vermitteln.

Der Hamburger Erfa, dem sie angehörten, hatte schon länger über eine „Family-Party" nachgedacht, nachdem 1998 der Congress nach Berlin umgezogen war. Die Idee des Easterheggs fiel also auf organisationsfreudigen Boden. Schon im nächsten Frühjahr war es soweit: 2001 fand das allererste Easterhegg statt – Fokus: Funken und WLAN.

Schon diese Veranstaltung hatte Features, welche die Easterheggs bis heute auszeichnen:

- Die Betonung liegt auf Workshops, nicht auf Vorträgen.
- Es gibt ein Frühstücksbuffet, welches im Eintrittspreis enthalten ist. Das „früh" in „Frühstück" wird sehr großzügig ausgelegt.

Photo: Der PoCSascha

- Jeder Gast bekommt eine Easterhegg-Tasse. Mit dieser nutzt man während der Veranstaltung die Kaffee-Flatrate. Nach der Veranstaltung hat man eine schöne Erinnerung und vielleicht eine neue Lieblingstasse.

Das Easterhegg war zunächst als einmalige Veranstaltung geplant. Der Erfolg war jedoch so groß, daß von mehreren Seiten eine Wiederholung gewünscht wurde. Als dann noch der Düsseldorfer Chaot Pylon fragte, ob das Easterhegg in Hamburg bleiben würde oder vielleicht auch woanders stattfinden könnte, wurde prompt Düsseldorf als nächstjähriger Veranstalter auserkoren. Aufgrund guter Zurede durch Wau Holland nahm Düsseldorf an. Heute ist das Chaosdorf schon lange Erfa-Kreis, aber damals war es noch ein Treffen Interessierter. Insofern hatte das Easterhegg vereinsstiftende Wirkung.

Noch immer wird der Veranstaltungsort der geradjahrigen Treffen auf der Abschlußveranstaltung der Hamburger Easterheggs bekanntgegeben. Allerdings muß man sich inzwischen bewerben, wenn man ein Easterhegg austragen möchte.

Für 2008 bekam Köln den Zuschlag und lud vom 21. bis 24. März zum Easterhegg in die Domstadt ein.

Veranstaltungsort war das Bürgerzentrum Stollwerck, früher eine Schokoladenfabrik, im Süden der Kölner Innenstadt, also leicht erreichbar. Dort konnte erfolgreich die nötige Infrastruktur errichtet werden, die bisweilen den Internetprovider etwas überforderte, weshalb zwischenzeitlich mit UMTS ausgeholfen werden musste. Zahlreiche Arbeitsgruppen und Vorträge füllten die kleineren Veranstaltungsräume: Neben technischen und gesellschaftlichen Themen gab es sogar praktischen Erfahrungsaustausch für Stricker und solche, die es werden wollten, und über den Anbau von Pflanzen mit Hightech-Methoden im heimischen Hobbykeller.

Der große Saal des Stollwercks war ein riesiges Hackcenter, das gleichzeitig als zentraler Kommunikationsraum diente. Hier konnte man immer wieder alte und neue Freunde antreffen oder etwas abseits vom Trubel auf den Emporen chillen (und trotzdem nichts verpassen). Hier fand sich auch die zentrale Getränkeversorgung und das immerwährende Frühstück. Insgesamt erinnerte das Easterhegg in Köln schon sehr an einen Congress, zwar noch familiär, aber schon in einem größeren Rahmen. Köln ist sicher ein weiterer Meilenstein in der Entwicklung nerdspezifischer Veranstaltungen. Vielleicht treffen wir uns ja in Zukunft öfter in der Domstadt.

Link: *http://eh2008.koeln.ccc.de*

Da jedes EH sein eigenes Logo hat, erhält man eine interessante Zeitleiste: Im allerersten Logo ist noch deutlich der Funkbezug in Form einer Antenne enthalten. In diesem wie auch im nächsten Logo taucht noch kein Hase auf. Erst ab 2003 wird ein Hase das bestimmende Motiv. Dessen Varianten bilden zum Teil aktuelle Strömungen ab, wie z. B. das Barcode-Bunny (2003) oder das Semapedia-Bunny (2005).

Da die Schreibweise des Event-Namens nicht festgelegt ist, gab es kreative Varianten, wie „./easter -h -egg" (2002) oder „EAST erh, egg" (2006). Anfangs wurde noch das „H" als Einschub besonders betont. Dies verlor sich später.

Mag das der Grund sein, aus dem sich der Artikel von ursprünglich „der" (Easter-Hack) zu „das" (Easterhegg) verschoben hat? Sicher ist, sowohl „der" als auch „das" Easterhegg ist okay.

Gedanken zum elektronischen Personalausweis

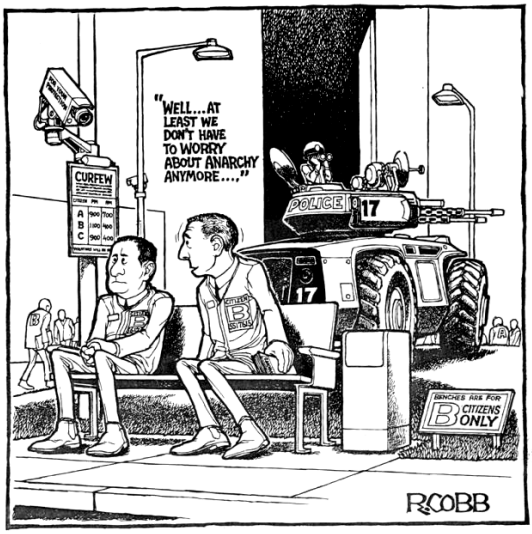
von Frank Rosengart und Martin Haase

Nach der Einführung eines biometrischen Reisepasses mit RFID (ePass) steht nun die Einführung des elektronischen Personalausweises (ePA) vor der Tür.

Fingerabdrücke

Am meisten öffentlich diskutiert wurde die Aufnahme des Fingerabdrucks, bis es schließlich zu einem faulen Kompromiß kam: Die Abgabe des Fingerabdrucks ist freiwillig. Das bringt eine „Zwei-Klassen-Gesellschaft“ mit sich: Inhaber von Ausweisen mit Fingerabdruck werden beim Grenzübergang vermutlich anders behandelt als solche ohne. Zudem ist die Infrastruktur für die zwangsweise Erfassung aller Fingerabdrücke bereits aufgebaut. Technisch möglich ist, daß bei jeder Kontrolle mit Fingerabdruckabnahme diese nachträglich auf dem Personalausweis gespeichert werden.

Innenminister Schäuble hat außerdem angekündigt, daß man für die zwangsweise Erfassung von Fingerabdrücken (und sogar für die Einrichtung einer zentralen Datenbank) wieder auf die EU setzen will, also über EU-Vorschriften sowohl die Erfassung der Fingerabdrücke als auch die Einrichtung einer zentralen Datenbank in Deutschland notwendig machen will. Außerdem fällt auf, daß die Bekanntgabe des Kompromisses zeitlich mit dem Verkauf der Bundesdruckerei zusammenfällt. Es scheint, als ob hier der Preis in die Höhe getrieben werden soll, damit der Bund endlich an die 300 Millionen Euro aus der damaligen Privatisierung kommt.



Biometrisches Foto

Ein biometrisches Foto ist natürlich nur sinnvoll, wenn damit auch biometrische Anwendungen geplant sind – hier sollte die Bundesregierung darüber Auskunft geben, was sie in Zukunft damit vorhat (Abgleiche auf Demos etc.). Das Argument, daß es für die Grenzkontrolle erforderlich sei, ist wie schon beim Reisepaß unsinnig, da es kein Land gibt, in dem solche Systeme bereits erfolgreich eingesetzt werden. Außerdem könnte hier klar zwischen den Anforderungen an einen Personalausweis und denen an einen Reisepaß getrennt werden.

Qualifizierte elektronische Signatur

Als Argument für den neuen Personalausweis wird immer wieder auf die qualifizierte elektronische Signatur verwiesen. Im Signaturgesetz werden der Rechtsgültigkeit der Signatur jedoch keine Grenzen gesetzt. Laut Bundesministerium des Inneren kann die Signatur einen Notar ersetzen – damit wäre es sogar möglich, ein Testament zu unterschreiben oder ein Haus zu (ver-)kaufen...

Für den Bürger ergibt sich ein dramatisches Risiko, denn wenn etwas schiefgeht, also die Signatur gefälscht und mißbraucht wird, liegt die Beweislast ähnlich wie bei der ec-Karte beim Inhaber des Ausweises. Bei der Frage der Haftung bewegt sich die elektronische Signatur praktisch im rechtsfreien Raum.

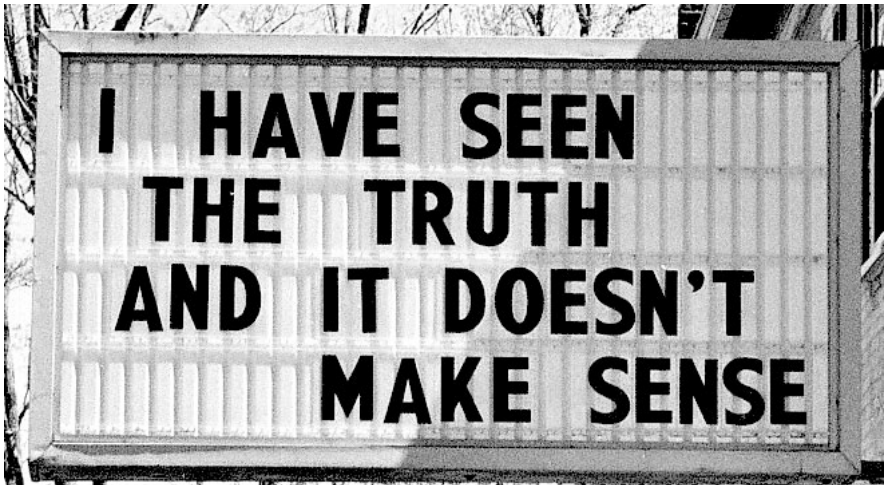
Elektronische ID (eID)

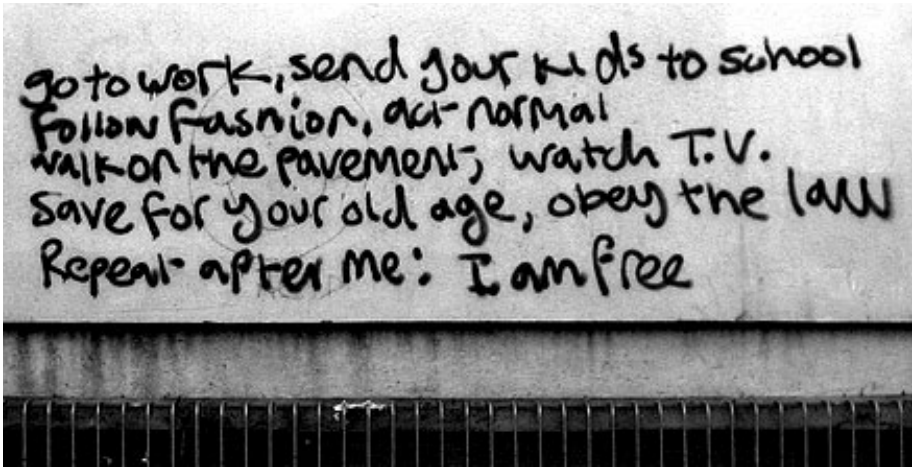
Es muß eine neue Bundesstelle geschaffen werden, bei der sich Anbieter akkreditieren müssen, um Zertifikate für die Anforderung der eID-Daten der Bürger zu erhalten. Diese Zertifikate sind dann für drei Jahre gültig (bzw. werden drei Jahre lang alle drei Tage erneuert). Die große Frage ist, was diese Bundesstelle prüft, was also deren Policy ist und welchen Rechtsanspruch man auf so ein Zertifikat hat.

Hier ein einfaches Beispiel: Ich hole mir ein Zertifikat für die GeldParkBank GmbH und werbe dann unter vielgeldparken.de für hohe Zinsen, wenn man dort Geld parkt. Die Leute eröffnen dort fleißig Konten, und nach ein paar Wochen löst sich alles in Luft auf. Dann wird der betrogene Bürger Ansprüche gegenüber dem Bund geltend machen, der die ominöse Parkbank zertifiziert hat.

Die eID wird vor allem dazu führen, daß elektronische Dienste nicht mehr anonym benutzt werden können. Bereits bei der Nutzung eines öffentlichen WLANs wird man sich mit seiner eID ausweisen müssen. Nach und nach werden immer mehr Dienste auf die eID zurückgreifen und ganz nebenbei die mit der eID validierten Daten sammeln. Die Voraussetzung für die komplette Abschaffung der Anonymität durch die eID wird mit dem elektronischen Personalausweis geschaffen. Dann haben wir Zustände wie in China.

Jede Website wird nach der eID fragen, und der Bürger wird gezwungen, sich überall mit seiner echten Identität – staatlich zertifiziert – auszuweisen. Ein Paradies für Phisher, Identitätsdiebe und Datensammler. Interessanterweise wird gerade Phishing als Argument für den elektronischen Personalausweis angesehen, obwohl er hier eher Probleme schafft als löst.





Wie ein Mantra wird von den Befürwortern immer wieder behauptet, der elektronische Personalausweis mache das Online-Banking sicherer; das ist natürlich Unsinn, denn schon längst gibt es Verfahren wie HBCI, die jedoch kaum genutzt werden, zum Beispiel weil die Kartenleser zu teuer sind und immer da stehen, wo man gerade kein Online-Banking machen will. So dürfen die Mitarbeiter in einer Firma meist keinen Leser an ihren Arbeitsplatzrechner anschließen.

Die Bundesregierung verspricht das Paradies bei elektronischen Transaktionen, aber es ist offensichtlich, daß dies so nicht eintreten wird. Der elektronische Personalausweis löst keines der aktuellen Probleme.

Angebliche Kostenersparnis

Die Kostenrechnung der Bundesregierung (100 Millionen Euro Einsparung) ist ein Taschenspielertrick, denn sie verschweigt, wo diese Kosten eingespart werden: bei der ohnehin völlig veralteten Erfassung von Meldedaten bei Pflegeheimen und Unterkünften. Diese Gelder werden im Rahmen der Melderechtsreform gespart, nicht mit dem elektronischen Personalausweis. Seriöse Zahlen zu den Kosten liegen nicht vor.

RFID

Signaturen auf RFID-Chips bergen nochmal ein ganz neues Risiko. Über die neuen Sicherheitsfeatures wie das Password Authenticated Connection Establishment (PACE, übrigens eine sehr deutsche Bezeichnung) wissen wir leider noch zu wenig.

Links

Bericht über den Kabinettsbeschluß zur Einführung des ePA: *http://www.spiegel.de/politik/deutschland/0,1518,567502,00.html*

Ausmaß der ePA-Nutzung: *http://www.heise.de/newsticker/Elektronischer-Personalausweis-Wenn-das-Web-den-Ausweis-sehen-will--/meldung/108208*

Informationen des BMI: *http://www.bmi.bund.de/Internet/Content/Themen/PaesseUndAusweise/Listentexte/elPersonalausweis.html*

ePA soll Phishing verhindern: *http://www.stern.de/politik/deutschland/:Daten-Klau-BKA-Verbraucherschutz/637441.html*

Bundesdruckerei: *http://www.ccc.de/epass/bundesdruckerei?language=de*

PACE: *http://www.heise.de/security/PACE-fuer-die-schnelle-Authentifizierung--/news/meldung/85024*

slashdot-netstatistik

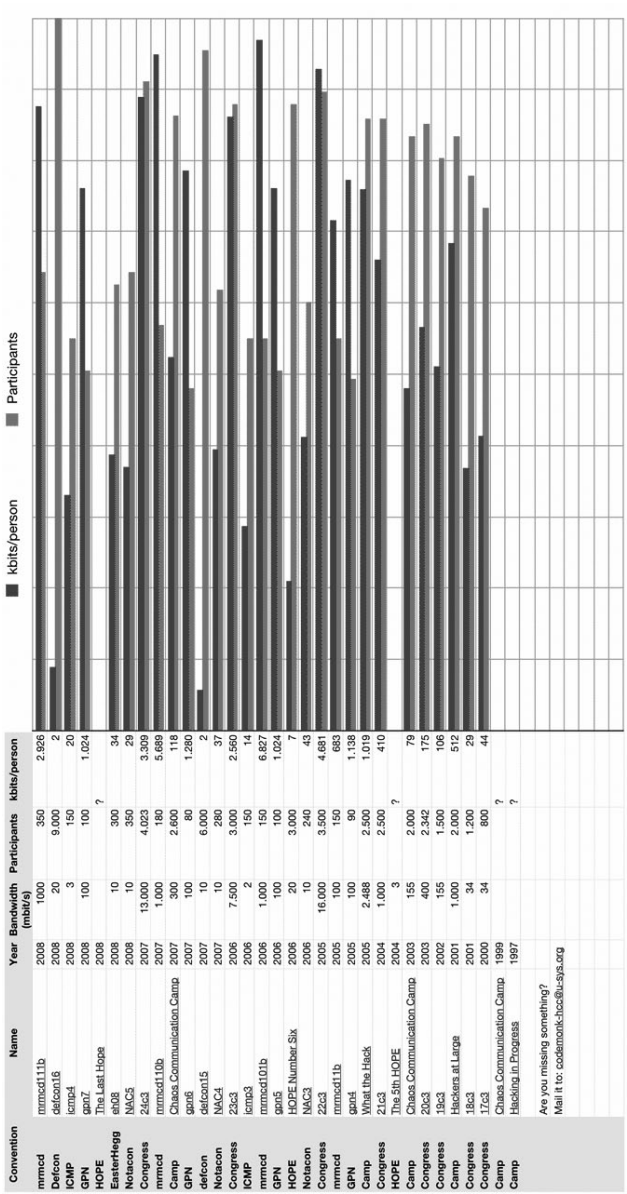
von codemonk

Ein nicht unwesentlicher Bestandteil von Hackerveranstaltungen ist ein vom Veranstalter zur Verfügung gestellter Internetzugang. HC und Codemonk haben sich die Mühe gemacht, eine möglichst umfassende Übersicht über bisherige Hackerveranstaltungen und die verfügbare Bandbreite zu erstellen.

Vorne liegen die mrmcd 101b, die mit einer Gigabit-Anbindung und 150 Teilnehmern jedem anwesenden Nerd knappe 6 MBit/s zur Verfügung stellten, dicht gefolgt von den mrmcd 110b mit 180 Besuchern, aber ebenfalls nur einer Gigabit-Anbindung. In absoluten Zahlen stellte der 22c3 einen Rekord mit einer Außenanbindung von insgesamt 16 GBit/s auf, dicht gefolgt vom 24c3 mit nur 13 GBit/s.

Weit abgeschlagen auf den letzten Plätzen finden sich verschiedene DEFCONs, die jeweils jedem Teilnehmer etwa nur 2 kBit/s zur Verfügung stellten. Selbstverständlich entscheidet selten die Internetanbindung über den Erfolg oder Mißerfolg einer Veranstaltung, trotzdem stellt man sich als Europäer die Frage, wie man mit 2 kBit/s auf einer solchen Veranstaltung auskommen kann.

http://u-sys.org/HCC/



Convention	Name	Year	Bandwidth (mbit/s)	Participants	kbits/person
mrmcd	mrmcd111b	2008	1000	350	2.926
Defcon	defcon16	2008	20	9.000	2
ICMP	icmp4	2008	3	150	20
GPN	gpn7	2008	100	100	1.024
HOPE	The Last Hope	2008		?	
EasterHegg	eh08	2008	10	300	34
Notacon	NAC5	2008	10	350	29
Congress	24c3	2007	13.000	4.023	3.309
mrmcd	mrmcd110b	2007	1.000	180	5.689
Camp	Chaos Communication Camp	2007	300	2.600	118
GPN	gpn6	2007	100	80	1.280
defcon	defcon15	2007	10	6.000	2
Notacon	NAC4	2007	10	280	37
Congress	23c3	2006	7.500	3.000	2.560
ICMP	icmp3	2006	2	150	14
mrmcd	mrmcd101b	2006	1.000	150	6.827
GPN	gpn5	2006	100	100	1.024
HOPE	HOPE Number Six	2006	20	3.000	7
Notacon	NAC3	2006	10	240	43
Congress	22c3	2005	16.000	3.500	4.681
mrmcd	mrmcd11b	2005	100	150	683
GPN	gpn4	2005	100	90	1.138
Camp	What the Hack	2005	2.488	2.500	1.019
Congress	21c3	2004	1.000	2.500	410
HOPE	The 5th HOPE	2004	3	?	
Camp	Chaos Communication Camp	2003	155	2.000	79
Congress	20c3	2003	400	2.342	175
Congress	19c3	2002	155	1.500	106
Camp	Hackers at Large	2001	1.000	2.000	512
Congress	18c3	2001	34	1.200	29
Congress	17c3	2000	34	800	44
Camp	Chaos Communication Camp	1999		?	
Camp	Hacking in Progress	1997		?	
	Are you missing something? Mail it to: codemonk-hcc@u-sys.org				

Im Umfragetief

von erdgeist <erdgeist@erdgeist.org>

Einige Fehlerklassen – so sollte man meinen – wurden in der großen Softwarerevolution von 1999 ausgemerzt. Trotzdem lächeln sie einen von komplett unerwarteter Stelle wieder an. Wie selbstverständlich benutzt jedes Kreditinstitut fürs Onlinebanking eine verschlüsselte Verbindung, jedes schlechtere Wiki ist paßwortgeschützt, hie und da sind selbst PHP-Datenbankanwendungen gegen SQL- und XSS-Attacken gewappnet, und Paßwortkontrolle in JavaScript im Browser waren eine kurze Modeerscheinung Anfang der neunziger Jahre.

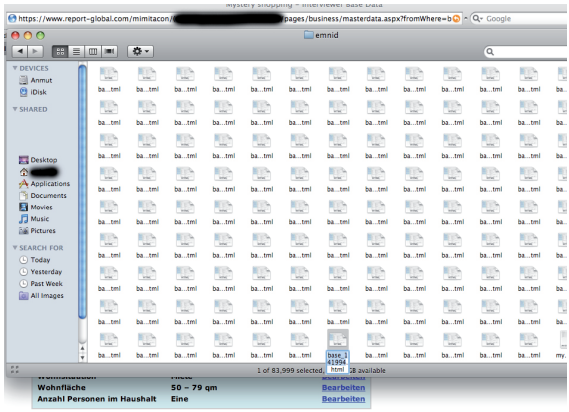
Umso überraschter war die Redaktion, als in einem unmarkierten braunen Umschlag ein Stück Papier mit der URL *https://www.report-global.com/mimitacon/*, einer Kundennummer und dem dazugehörigen Paßwort eintrudelte. Nichtsahnend loggten wir uns durch eine Tor-Kaskade ein.

Auf der Seite prangte groß das Logo der TNS Infratest, einem Marktforschungsinstitut, darunter die Kundenstammdaten des Informanten. Name, Geburtsdatum, Adresse, Telefonnummer, E-Mailadressen, Bankverbindungen – das ganze Programm. In einem zweiten Tab auf der Seite, mit der vielsagenden Bezeichnung „Attributes“ überschrieben, schlackerten dann selbst uns hartgesottenen Datenmüllpanschern die Ohren: Ausbildung, Beruf, Monatseinkommen, Wohnsituation, Mobilfunkverträge, Krankenversicherungen, Autos, Wertgegenstände im Haushalt (Plasmabildschirm, DVD-Spieler, etc.), Kunden- und Kreditkarten – das ganze Wohlfühlprogramm für Datenverbrecher.

Bloß – warum sollte uns jemand so großzügigen Einblick in seine Lebensverhältnisse gewähren? Wir klickten ein wenig auf der Seite herum und staunten nicht schlecht, als wir in der Adreßzeile ein wenig nach rechts wanderten. Dort winkte uns fröhlich folgende URL (Kundennummer durch XXXX ersetzt) zu:

https://www.report-global.com/mimitacon/(kkpadc2olxlev5qcbvgvq3u4)/pages/business/masterdata.aspx?fromWhere=base&id=11XXXX

Der geübte Datenschleuderleser weiß schon, was jetzt kommt. Für zufällig ausgewählte XXXX gab es immer mehr unglaublich offenherzige Portalbenutzer, die bereitwillig Auskunft über die intimsten Lebensumstände gaben. Die sechsstellige Kundennummer ließ nichts Gutes erahnen, und so ertasteten wir einen Bereich gültiger IDs von 100001 bis 141003, also rund 41.000 Datensätze. Und weil das händische Eintippen so mühsam erschien, half uns ein kleines python-Script beim Sicherstellen der Stammdaten.



Doch was nun? Infratest hatten wir schonmal gehört. Bei der Sonntagsfrage in einigen Lokalblättern liest man über die als Umfrage-

institut. Wikipedia half weiter: TNS Infratest/Emnid ist eines der führenden Marktforschungsinstitute der Welt, und das Portal report-global.com scheint Infratest zugeordnet zu sein:

```
Domain name: report-global.com
Registrant:
 TNS Infratest GmbH (TNSINFRA376)
 Landsberger Str. 338
 Muenchen, 80687
 DE
```

Attributname	Wert des Attributs	
Postleitzahl Wohnort	**806**	Bearbeiten
Bundesland	**Bayern**	Bearbeiten
Staatsangehörigkeit	**Deutsch**	Bearbeiten
Anrede	**Frau**	Bearbeiten
Geburtsjahr	**1967**	Bearbeiten
Schulbildung	**Abgeschlossenes Studium (Universität oder FH)**	Bearbeiten
Sprachkenntnisse	**Deutsch**	Bearbeiten
Sprachkenntnisse	Englisch	
Status Krankenversicherung	**Mitglied gesetzlicher Krankenkasse**	Bearbeiten
Krankenkasse / Krankenversicherung	**BEK Barmer Ersatzkasse**	Bearbeiten
Pflicht- oder freiwillig versichert	**Freiwilliges Mitglied**	Bearbeiten
Mitversicherte Personen	**Keine Person mitversichert**	Bearbeiten
Zusatzkrankenversicherung	**Leistungen im Krankenhaus**	Bearbeiten
Fahrzeuge im Haushalt	**PKW**	Bearbeiten
Autos	**1**	Bearbeiten
Marke des/der Autos im Haushalt	BMW	
Modell	BMW Dreier- Reihe	
Baujahre des/der Autos im Haushalt	2004	
KFZ Versicherungsverträge im Haushalt	**Weiß nicht, keine Antwort**	Bearbeiten
Art KFZ-Versicherungsschutz im Haushalt	**Vollkasko**	Bearbeiten
Kundenkarten	**Lufthansa Miles & More (Blau)**	Bearbeiten
Kundenkarten	Payback	
Kunde bei Geldinstitut	**DAB Bank**	Bearbeiten
Kunde bei Geldinstitut	ING-DiBa	
Kunde bei Geldinstitut	Postbank	
Versicherungen im Haushalt	**Hausratversicherung / Haushaltversicherung**	Bearbeiten
Versicherungen im Haushalt	private Haftpflichtversicherung	
Versicherungen im Haushalt	Berufsunfähigkeitsversicherung	
Versicherungen im Haushalt	Rechtsschutzversicherung	
Internetfähigkeit	**Internetzugang vorhanden**	Bearbeiten
Online Provider im Haushalt	**T-Online**	Bearbeiten
Geräte im Haushalt	**Digital-Kamera für Einzelbilder**	Bearbeiten
Geräte im Haushalt	DVD Brenner	
Geräte im Haushalt	DVD Laufwerk	
Geräte im Haushalt	DVD-Player für den Fernseher	
Geräte im Haushalt	Flachbildschirm	
Geräte im Haushalt	Kombigerät (Drucker mit Fax und/oder Scanner)	
Geräte im Haushalt	MP3 Player (Portable)	
Geräte im Haushalt	Spielekonsole (PS 1 oder 2 / X-Box etc.)	
Anzahl Handys im Haushalt	**2**	Bearbeiten
Mobilfunknetz	O2 (Genion / Citypartner) (früher Viag Interkom)	
Art Mobilfunk Handy 1	"Postpaic" / Mobilfunkvertrag abgeschlossen	
Mobilfunknetz	O2 (Genion / Citypartner) (früher Viag Interkom)	
Art Mobilfunk Handy 1	"Postpaic" / Mobilfunkvertrag abgeschlossen	
Status Erwerbstätigkeit	**Vollzeit-erwerbstätig**	Bearbeiten
Beruf	**Sonstiger Angestellter**	Bearbeiten
Persönliches Nettoeinkommen	**Zwischen EURO 3.500 und EURO 4.000**	Bearbeiten
Haushaltsnettoeinkommen	**Zwischen EURO 3.500 und EURO 4.000**	Bearbeiten
Art des Fernsehempfangs	**Kabel**	Bearbeiten
Wohnsituation	**Miete**	Bearbeiten
Wohnfläche	**50 – 79 qm**	Bearbeiten
Anzahl Personen im Haushalt	**Eine**	Bearbeiten

Wir trieben uns in einem Bereich herum, der mit „Mystery Shopping“ gelabelt war. Laut Infratests Selbstdarstellung haben sie hundert Mystery-Tester bundesweit im Einsatz, laut Wikipedia gibt es bundesweit 4.000 Mitarbeiter. Wo kommen also die fast 40.000 Einträge her?

Als wir durch die Datensätze durchblättern, fallen uns spontan mehrere Berufsgruppen ein, die sich über dieses Datenschnäppchen die Hände reiben würden. Kalle Klau könnte eine alleinstehende Zielperson mit gehörigem Monatseinkommen und Vollzeitstelle zu üblichen Arbeitszeiten an der angegebenen Adresse besuchen, überprüfen, ob das bezeichnete Kraftfahrzeug vor dem Haus steht, noch einmal ein Testtelefonat führen, wüßte genau, nach welchen Wertgegenständen er suchen müßte, sogar, welche Taschen er mitzubringen hätte, damit er alles gut verstauen könnte.

Erna Erbschleich und Stefan Stalker könnten Opferprofiling machen. Bestatter Bertram, Ottfried Opelschraub und Olivia Ökostrom sind eh natürliche Freunde solcher Marketingdaten, Richard Radikal hingegen freut sich über die unerwartete Liste von Bonzen in seinem Kiez.

Nina Neidisch kann endlich voller Genugtuung rumerzählen, daß Nachbars Benz nur geleast ist, und Micha Miethai entsorgt vorsichtshalber schonmal den gehaltsgekürtzten Mieter Hans Husten.

14 Years of starting a hacker scene in brazil

by Derneval Cunha

October 1994: The „Hacker and Virus Congress“ in Buenos Aires, Argentina. Went there, knew lots of people, like Goldstein, Mark Ludwig (author of „The Little Black Book of Computer Virus“).

So, what was my goal? Just to get people together, to exchange information. Prepare for a hacker conference. So started by the easy and cheapest way could think of: an electronic publication. South america‘s first in *ftp.eff.org* and Brazilian‘s first Internet publication.

Writing it in ASCII helped it to be uploaded to and downloaded from in BBSes all around the country and abroad, in portuguese speaking places like Portugal and Mozambique. Had nobody to help, wrote most of it alone. Pity I wasn‘t doing Computer Science. Or Journalism.

Barata Elétrica (Electric Cockroach), it spread everywhere like a disease. It appeared in places like the usenet, like 2600 list and *soc.culture.brazil*. My own university didn‘t like, once even suspended my Internet access for a few months (that ruined organizing Brazilian‘s first „hacker“ meeting). Another federal university, UFSC, left at their website for about ten years.

Created a motto: „I login, therefore I am“. But few people in South America had Internet accounts in 1994. Internet wasn‘t easily available those days. Phone modems were not reliable (used 600 bps maybe 1.200 bps, sometimes 2.400 bps modems). In Argentina, everything gravitated around virus writing, BBSes and X-25 network. Most „hacker“ things happened in BBS, Fidonet or the like. Set my eZine to talk about Internet, hacker ethics and computer underground lore. Couldn‘t be arrested for that.

After I started, lots of good (and bad) information started to spread around. Soon people started to write other publications, more aggressive, like the eZine Axur 05, Nethack and a few others, mostly in BBSes. If someone wanted to be known as a hacker, he and his friends would write an eZine – the „Golden years“.

An eZine meant to be something simple grew complex, with sections like history, FAQ, about, better articles (IMHO), a news sections that became a blog. And an eZine t-shirt. Learn from public relations to law and journalism. People began offering help, like how to better eZine‘s html. For free. Said no. Besides, a better eZine would be even more complex. Would have to go corporate. Pay taxes, etc.

Published the first article about Linux in Brazil. Phiber Optik came here, my eZine tipped everybody to ask him to compare Windows NT security versus Free BSD (couldn‘t pay my entrance but people asked). Was also there to give support when an activist from International Amnesty, Fernanda Serpa, started „Free Kevin Mitnick“ movement in Brazil. Once there was a talk to bring Markoff and Shimamura in a US$ 400 a ticket conference. Funny, after my writing, nobody talked about that anymore.

My dream was now real. There was a „hacker scene“ with meetings and people talking about it everywhere. But paper press started to run articles how-to-do-bad-things-for-fun, they wanted blood (to write about). And some guys star-

ted to write best-sellers using material from several underground eZines. Cut and paste jobs. I can trace today's Brazilian electronic vandalism back from those mags and books.

Enrolled in a post-graduation, got a Master degree but nothing to do with computers. Wrote articles to 2600. Most people keep pressing me for writing a book about all my exploits (only one?). Me thinks about a thesis, outside Brazil. Lost some „friends" because they gave up on me writing about them. And changed my writing in order to avoid copy cats (in fact I could sue some people). Got paranoid. People said the author of „Underground", Suelette Dreyfus, wanted to interview me online. Declined.

How could I write a book about „starting a hacker scene" and get a „normal" job anywhere but in computer security? There are „hacker" conferences I don't go to. TV cameras everywhere. E.g. at the same time there was one, I was working right next to an office where people were trying to sue youtube, that Cicarelli thing. Even saw the law people picking up the books to study the case. One exception was last year's „You Shot the Sheriff" conference, YSTS, in São Paulo. Fewer cameras. Another one was the first conference for feds, judges and police related personnel (only). Being anonymous does pay.

The (ex)-chief of Brazilian Intelligence Agency (ABIN), Mauro Marcelo (first Brazilian „Cyber" cop), did know me, though (of course). While he was there, he bothered to answer an email of mine. Almost interviewed him.

Lost early days energy but try to keep on writing the eZine and the blog... why not? And some people really do help. I try to return the favor by writing. Sure, words like „please", „thanks" works wonders. Never had to hack much to get things done, anymore. Sometimes I sing a song like „let me please introduce myself". Many times I sing to myself „Don't you forget about me"... Writing an eZine does get you high.

Once I posted that „need a few memory chips for 486 Computer". I live in Sao Paulo. Marcos Pereira, big fan and friend from Rio de Janeiro read it, asked my mailbox and sent the chips. And about 16 kg of hardware, a complete CPU. He made a party, people brought old hardware pieces, set up a Pentium 233, 30 gig HD and sent it to me, FEDEX like. Couldn't believe it. Sent him some t-shirts for thanks. Recently, he sent me a Pentium 4, 150 big HD, etc... Beautiful.

Someone said: If you don't like the news, go out and make some of your own. My eZine started just like that, a publication for a few people that used a net connected computer lab nearby. Everybody can help change the world. Just interact with your community.

UniHelp

von Markus Schneider <markus.schneider@unihelp.de>

Im vergangenen Jahr gab es viele Diskussionen und einen großen Medienrummel um social networks und sogenannte Studentenportale. Und meistens hatte man den Eindruck, es ginge nur um Userdaten und viel Geld, nicht um die User oder um die Studenten. Die Frage, ob es eine Alternative gibt, möglichst noch quelloffen (open source), wurde ab und zu gestellt, aber eine Antwort gab es bis jetzt noch nicht. Doch ein Projekt aus Magdeburg zeigt, wie Studenten ihre eigene Community für Studenten betreiben können. Seit acht Jahren hat sich das Projekt immer weiter entwickelt, und die Zahl von 12.000 angemeldeten Studenten spricht für die Erfolgsgeschichte. Jetzt wird der Sprung zum Open-Source-Projekt gewagt, um die Idee „UniHelp" außerhalb der eigenen Stadt bekanntzumachen.

Idee „UniHelp"

Die Idee „UniHelp" wurde im Jahr 1999 geboren. Damals fragte sich Karsten Wysk, Student der Volkswirtschaftslehre, warum er sich viele Unterlagen für sein Studium immer bei seinen Kommilitonen zusammensuchen mußte – warum kann man sie nicht einfach über das Internet austauschen? Nach einer Woche Crash-Kurs in PHP und MySQL programmierte er die erste Grundlage für das Portal *UniHelp.de*. Von Anfang an stand das Motto „von Studenten für Studenten" im Mittelpunkt. Schnell waren Mitstreiter gefunden, und im Jahr 2002 wurde der gleichnamige studentische Verein UniHelp e. V. gegründet. Schon zu diesem Zeitpunkt wurde die Vision entwickelt, UniHelp als Open-Source-Projekt zu führen und über Magdeburg hinaus zu verbreiten. Doch bis dahin sollte es noch ein langer Weg sein. Die Meßlatte wurde also hoch gesetzt, doch zunächst war den Entwicklern nicht die schnelle Expansion wichtig, sondern die Qualität und Kreativität des Projektes.

Daß UniHelp nicht so ist wie der Rest der Welt, merkt man schnell. Hinter UniHelp stehen ausschließlich Studenten, ob in der Entwicklung, im Bereich der Nutzerbetreuung oder der Finanzierung. Die Anmeldung als Nutzer erfordert die Angabe der studentischen E-Mail-Adresse. So wird sichergestellt, daß UniHelp tatsächlich eine Studenten-Community ist und bleibt.

UniHelp begreift sich als unabhängig, frei und unpolitisch. Persönliche Daten werden nicht gesammelt. Auch die Moderation in den Foren ist auf das minimal Notwendige beschränkt. Der Nutzer kann seine private E-Mail-Adresse angeben und sie dann über eine Privatsphä-

ren-Option für seine Freunde freigeben – unter Angabe des PGP-Keys.

Der Mittelpunkt der UniHelp-Idee ist jedoch das Studiensystem. Hier findet man zu jedem Fach, das am Standort Magdeburg an der Universität oder der Hochschule angeboten wird, ein Forum und einen Unterlagenbereich. So haben sich über die Jahre schon über 12.000 Unterlagen zu allen Fachbereichen angesammelt! Sie stellen eine wichtige Hilfe für die Vorbereitung der einen oder anderen Prüfung dar, sodaß viele Studenten, die Magdeburg verlassen haben, um an anderen Hochschulen ihr Studium fortzusetzen, an ihrer neuen Hochschule ein UniHelp stark vermissen. Denn nirgendwo sonst findet man schneller eine Lösung für die gestellten Aufgaben.

Im Gegensatz zu anderen Foren einer Fakultät oder manchen privaten Internetseiten, zeichnet sich UniHelp dadurch aus, daß es alle Fachbereiche des Hochschulstandortes zusammenbringt. So nutzen Geisteswissenschaftler, Ingenieure und Wirtschaftswissenschaftler das gleiche Portal und teilen ihr Wissen interdisziplinär.

Auch die angenehmen Seiten des Studentenlebens spiegelt UniHelp wider. So geht es nicht nur um Studieninhalte, sondern man findet die neuesten Party-Infos, welche Restaurants in der Stadt am leckersten sind, im Forum wird über Tages- und Hochschulpolitik diskutiert und auf der Startseite findet man unter anderem die aktuellen News der Fachschaftsräte und anderer Hochschulorganisationen.

Der UniHelp e. V. betreibt die Plattform unabhängig von politischem Einfluß der Hochschulpolitik. Einnahmen werden nur zur Deckung der laufenden Kosten gebraucht. Bleibt doch mal mehr Geld in der Kasse, wird es an die Studenten zurückgegeben, indem im echten Leben Veranstaltungen organisiert werden, wie beispielsweise Spieleabende oder eine Herrentagsrallye.

Entwicklung und Open-Source-Strategie

Die ursprüngliche Version der Portalsoftware, UniHelp 1.x, basierend auf MySQL und PHP, war organisch gewachsen. Nach und nach wurden neue Funktionen in die Software eingestrickt. Mit dem enorm wachsenden User-Zuspruch war schnell klar, daß man die Software von Grund auf neu schreiben mußte, um dauerhaft einen zuverlässigen Betrieb zu ermöglichen. Dafür wurde 2005 der Grundstein gelegt, und eine kleine Gruppe von drei Studenten hat begonnen, Konzepte und Grundlagen zu entwerfen. Im Folgejahr 2006 wuchs die Entwicklergemeinde, trotzdem waren die Fortschritte auf dem Weg zum laufenden Neusystem nur minimal. Ein großes Problem war, daß die Entwickler sich nicht auf die Neuentwicklung konzentrieren konnte, sondern auch das alte System am Leben erhalten mußten. So wurden unzählige Stunden mit dem Flicken von kaputten MySQL-Datenbanken und dem

Fixen von Bugs verbraten, welche technisch im neuen System schon viel sauberer gelöst wurden. Durch die stetig zunehmende Nutzerzahl mußte auch die Performance des Altsystems verbessert werden.

Große Stücke der Arbeit der Neuentwicklung wurden bei Entwicklertreffen in den Wohnstuben der Teammitglieder realisiert. Wenn zehn engagierte Studenten an neun Laptops sitzen und versuchen, die bestehenden Aufgaben zu bewältigen, entsteht eine motivierende Stimmung! Trotzdem gab es immer mehr Aufgaben, als Entwickler Zeit verfügbar hatten. Eines der größten Probleme war die Überarbeitung des Designs und der Usability. Die Schwierigkeit bestand darin, die bestehende Nutzerschaft, die an das Altsystem gewöhnt war, nicht mit Veränderungen zu verschrecken und doch eine zeitgemäße und moderne Lösung zu finden, die es neuen Benutzern ermöglicht, sich auf Anhieb in der Vielzahl der verfügbaren Funktionen des Portals zurechtzufinden. Trotz umfangreicher Verbesserungen des Designs und der Usability – auch der Barrierefreiheit – ist auch das Neusystem unter diesen Aspekten verbesserungswürdig.

Zu Ostern 2007 sollte es dann endlich soweit sein: Das neue System sollte released werden. Doch wie das Leben so ist, machten dem Team einige Schwierigkeiten zu schaffen. Bis in letzter Minute wurde am System geschrieben. Daneben wurde ein weiterer Server benötigt, und der mußte vor allem bezahlt werden. Dazu veranstaltete der UniHelp e. V. die sogenannte Supporter-Party, welche sich zu einer der besten Parties des Semesters entwickelte und etwas Geld in die Kasse spülte. Den Großteil jedoch übernahm dann dankenswerterweise der Studentenrat Magdeburg. Am 25. Juni war es dann endlich so weit, das neue UniHelp erblickte das Licht der Welt. Ungefähr 13,5 Mannjahre und 150.000 Zeilen Quellcode stecken in dem Projekt. Während der Umstellung des Systems ging die Plattform für fünf Tage vom Netz. Die Zeit war nötig, um die Inhalte zu überspielen. So wurde der komplette Stand von acht Jahren UniHelp in ein komplett neues Datenbankdesign migriert.

Nach dem Release kehrte etwas Ruhe in die Gemeinde der Entwickler ein. Man konzentrierte sich auf das Beheben kleinerer Bugs und Verbesserungen im Detail, die während des Betatest niemandem aufgefallen waren. Außerdem konnte nun der Open-Source-Gedanke wieder aufgegriffen werden. Ein modernes und flexibles Framework, in das die Erfahrungen aus acht Jahren Betrieb einer aktiven Studentencommunity flossen.

Die Entwicklung hatte bisher schon nach dem Vorbild von Open Source stattgefunden: Jeder interessierte Student konnte kommen und mit anpacken, sich einbringen und seine Ideen verwirklichen. Leider war nur ein geringes Interesse außerhalb von Magdeburg vorhanden. Zu groß war meist die Skepsis, ob die gesteckten Ziele erreichbar seien. Im Rückblick müssen die Entwickler zugeben, den Umfang des Projektes unterschätzt zu haben. Mit der Inbetriebnahme des neuen Systems jedoch waren die Zweifel beseitigt. Trotz aller noch verbleibenden Baustellen mußte man doch anerkennen, daß in ehrenamtlicher Arbeit ein mehr als konkurrenzfähiges Portalsystem entwickelt wurde. Das Team wuchs demzufolge auch über die Grenzen der Stadt hinaus und war so gezwungen, auch die Arbeitsweise neu zu organisieren. Es ist eben doch ein Unterschied, ob sich eine handvoll Entwickler in der Uni trifft oder sich eine Open-Source-Entwickler-Community aufbaut.

Technischer Überblick

Das UniHelp-Framework ist eine Eigenentwicklung in objektorientiertem PHP5 aufbauend auf einer PostgreSQL-Datenbank und der PHP-Template-Engine Smarty. Das Framework selbst ist modular konstruiert und erlaubt Portalentwicklung gemäß dem Model-View-Controller-Pattern.

Um die Verteilung auf mehrere, auch physikalisch getrennte Standorte zu ermöglichen, ist eine XMLRPC-Schnittstelle zur Datensynchronisation in Arbeit. Die Cross-Authentifizierung läuft über signierte Domain-Cookies. Eine SOA-Beispiel-Implementation, durch die

auch mit anderen Web-Diensten kommuniziert werden kann, existiert für das Bugtrackingsystem Mantis, über das neben der Koordination der Entwicklung auch der gesamte User-Support abgewickelt wird. Hieraus gibt es wiederum eine Integration in das Private-Nachrichten-System des Portals.

Der Zugriff im Code auf sensible User-Daten wird von einem Privacy Manager in Abhängigkeit der User-Einstellungen reguliert. Somit wird Datenschutz schon per Softwaredesign unterstützt.

Smarty wird intensiv als Template-Compiler und Caching-Instanz eingesetzt. Fast alle Seiten können im Cache vorgehalten werden, lediglich Bugs in Smarty und das eingesetzte Dateisystem (im Falle von *UniHelp.de* eine RAM-Disk) begrenzen Cache-Umfang und Lebensdauer. Die Mehrsprachigkeit ist angedacht durch austauschbare Templatesätze, da isolierte Variablen für Sprache zu unflexibel sind. Für die Textausgabe aus PHP gibt es Dateien mit sprachabhängigen Konstanten. Regen Gebrauch findet auch die Plugin-Funktion von Smarty, die für viele Standardobjekte (z. B. UserModel) passende Ausgaben erzeugt (Link zur Userpage, URL des User-Bildes).

Als Datenbank ist PostgreSQL vorgesehen. Durch zahlreiche Constraints und einige Trigger wird Datenkonsistenz forciert. Zur Zeit arbeitet unser Framework auf PostgreSQL 8.0 und höher.

Besonderen Wert wird auch auf die Trennung von Markup und Design gelegt. Hierfür war das Ziel, die Webstandards XHTML 1.0 und CSS 2.0 zu berücksichtigen. Viel Mühe wurde auch auf Barrierearmut gelegt, weshalb Flash gar nicht zum Einsatz kommt und alle JS/Ajax-Features nur Gimmicks sind. Der volle Funktionsumfang der Seite steht dem User auch bei abgestelltem Javascript zur Verfügung. Die Javascript-Bibliothek Behaviour ermöglicht es, den Template-Code selbst frei von Javascript zu halten.

Für die Unterstützung von LaTeX-Ausgabe und Code-Syntax-Highlighting stehen Bibliotheken bereit, zusätzlich einfache Schnittstellen für den E-Mail-Versand und die Ausgabe von RSS-Feeds.

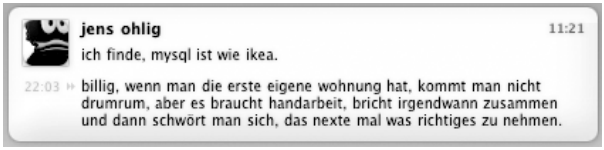
Die kühne Vision für die Zukunft

Die Entwickler und Betreiber von UniHelp blikken optimistisch in die Zukunft: Daß die Idee funktioniert, wird täglich auf *http://magdeburg.unihelp.de/* bewiesen. Nun wird das Framework unter dem Namen xPyrus unter der Gnu Affero General Public License Version 3 veröffentlicht. Der Name xPyrus bezieht sich auf Papyri, das Papier des Altertums, und auf Exchange, also den Austausch, und soll so den Kern der UniHelp-Idee abbilden: den Tausch von Wissen und studienrelevanten Unterlagen. So besteht die Möglichkeit, Studenten-Communities nach dem Muster von UniHelp an beliebigen Hochschulstandorten zu bilden – nicht nur in Deutschland. Jeder Standort wäre unabhängig und könnte trotzdem intensiv mit anderen Standorten kommunizieren sowie studienrelevante Unterlagen tauschen.

Überall dort, wo Studenten bereit sind, eine eigene Community zu betreiben, steht der UniHelp e. V. Magdeburg mit seiner Erfahrung aus Entwicklung und Betrieb gerne zur Seite.

Die Wahl liegt nun bei den Studierenden, ob sie sich einem Marketing-Kanal als Nutzermasse der Spaßgeneration zur Verfügung stellen wollen oder ob sie die Idee von UniHelp übernehmen und ihr Online-Schicksal selbst in die Hand nehmen wollen.

Weiterführende Informationen finden sich unter *http://www.xpyrus.org/*, *http://www.unihelp.org/* und *http://magdeburg.unihelp.de/*



Netsecurify

von Martin Wisniowski
<mw@node3000.de>

Petko Petkov vom Hackernetzwerk GNUCITIZEN stellt deren neues Werkzeug mit dem Namen „Netsecurify“ vor, welches automatisierte Tests von Webprojekten in Hinblick auf deren Sicherheit ermöglicht.

Wisniowski: Hallo Petko. Steigen wir direkt ein. Was genau macht das Tool „Netsecurify“?

Petko Petkov: Netsecurify ist ein Analysetool, mit dessen Hilfe man automatisierte Tests zur Schwachstellenanalyse von Webprojekten durchführen kann. Es folgt dem SaaS-Modell (Software as a Service) und wird dafür die gut skalierbare Computerinfrastruktur von Amazon benutzen. Im wesentlichen führt das Tool unterschiedliche Tests durch, die alle auf Open-Source-Technologien beruhen. Nach den Tests werden Empfehlungen zur Verbesserung der Sicherheit ausgegeben. Dafür haben wir eine sehr flexible „Recommendation Engine“ eingebaut. Das Tool erlaubt es auch Drittanbietern, die Empfehlungen mit eigenen Technolgien zu verbessern.

Netsecurify ist sehr einfach zu nutzen. Alles, was der Anwender tun muß ist, sich in den Service einloggen und einen Test für eine bestimmte Netzreichweite anzumelden. Sobald der vorgesehene Zeitpunkt gekommen ist, wird der Test von uns ausgeführt. Wenn die Überprüfung abgeschlossen ist, bekommt der Nutzer eine E-Mail zugestellt. An anderen Möglichkeiten des Feedbacks arbeiten wir im Moment. Der Nutzer kann sich dann einloggen und den Testbericht runterladen. Aus Sicherheitsgründen wird der Report nach dreißig Tagen automatisch von uns gelöscht.

Wisniowski: Was war eure Motivation, dieses Projekt in die Wege zu leiten?

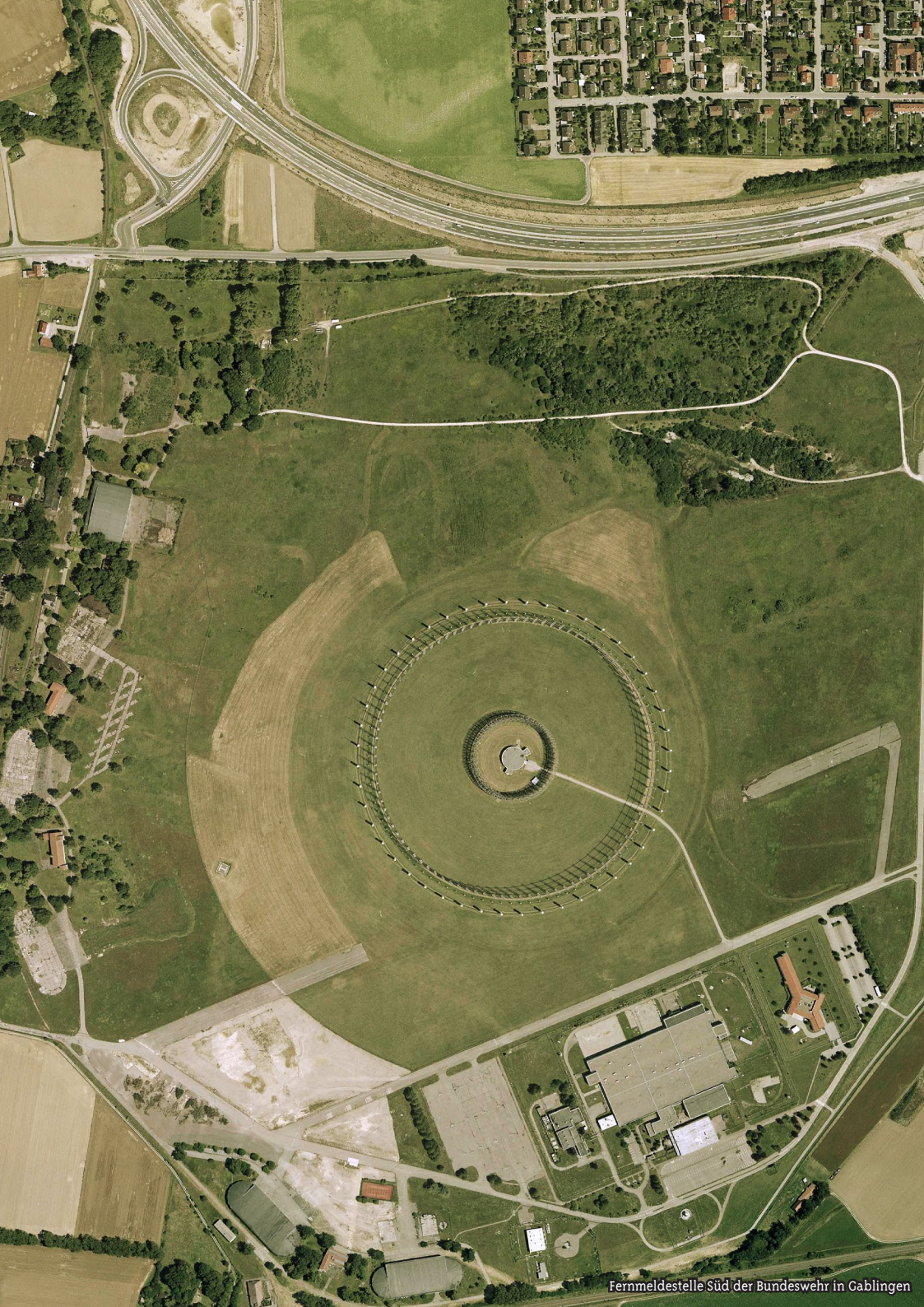
Petkov: Die Hauptmotivation für das Projekt war, ein freies, flexibles, automatisiertes und qualitativ hochwertiges Sicherheits-Testtool zu erschaffen, welches vor allem auch von gemeinnützigen Organisationen, Ländern in der Dritten Welt oder noch allgemeiner Organisationen und Unternehmen genutzt werden kann, die es sich schlichtweg nicht leisten können, Geld für Sicherheit auszugeben. Ein weiterer großer Motivationsfaktor war natürlich auch, daß es bisher noch niemanden gab, der so etwas in dieser Ausprägung gemacht hat. Wir sind also die ersten, die einen solchen Service anbieten.

Wisniowski: Wer sind die Leute, die hinter dem Projekt stehen, und wie habt ihr euch organisiert?

Petkov: Die Leute hinter Netsecurify sind grundsätzlich zunächst einmal GNUCITIZEN. Wir begrüßen aber jeden, der Lust hat, uns bei dem Projekt zu unterstützten, um den Service zu verbessern. Da wir das Projekt aus Open-Source-Technologien zusammengebaut haben, die wir ständig verbessern, planen wir auch, unsere Arbeit irgendwann wieder zurück an die Community zu geben. Wir wollen den Kreislauf der Energie so wieder schließen. Theoretisch also ist die Security-Community ein integrierter Bestandteil des Netsecurify-Projekts.

Wisniowski: Wir seid ihr beim Design der Anwendung vorgegangen? Und in welche Richtung soll es weitergehen?

Petkov: Wir haben ein skalierbares Backend und ein sehr einfach zu nutzendes und flexibles Frontend. Dazwischen gibt es unterschiedlich APIs, die es uns ermöglichen, den Service jederzeit zu erweitern. Wie bereits erwähnt, sind viele Open-Source-Technologien zum Einsatz gekommen – wir haben also nicht bei Null angefangen. Jedoch haben wir von Anfang an eine Menge über das Design und die Architektur nachgedacht, bevor wir anfingen, es in Code zu implementieren. Dabei folgen wir ganz klar dem KISS-Prinzip: Keep It Simple Stupid. Und das klappt hervorragend. In Zukunft wollen wir das einfach fortführen: die Anwendung noch besser und noch einfacher gestalten.


Fernmeldestelle Süd der Bundeswehr in Gablingen

http://events.ccc.de/congress/2008