

die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club



Biometrie ganz praktisch: das kapazitative Gummibärchen
AES: Advanced Encrypting (Supposedly)
VPN: Dig Your Tunnel!
Kurzgeschichte: Die Gedanken sind frei...
Gimmick: Open-Source Mischpult zum Selberlöten!

Erfa-Kreise

Bielefeld	im Café Parlando, Wittekindstraße 42, >> jeden Dienstag (außer feiertags) ab 18h	http://bielefeld.ccc.de/ <mail@bielefeld.ccc.de>
Berlin, CCCB e.V.	Marienstr. 11, Berlin-Mitte, Briefpost: CCC Berlin, Postfach 640236, D-10048 Berlin >> Club Discordia jeden Donnerstag zwischen 17.00 und 23.00 Uhr in den Clubräumen.	http://berlin.ccc.de/ Fon: +49.30.285.986.00 Fax: +49.30.285.986.56
Düsseldorf, CCD/ Chaosdorf e.V.	"zakk", Fichtenstr. 40 >> jeden 2. Dienstag im Monat ab 19.00 Uhr	http://duesseldorf.ccc.de/
Frankfurt am Main, cccffm	Club Voltaire, Kleine Hochstraße 5, >> donnerstags ab 19 Uhr	http://www.ffm.ccc.de/
Hamburg (die Dezentrale)	Lokstedter Weg 72 >> jeden Dienstag ab ca. 20.00 Uhr in den Clubräumen. Der jeweils erste Dienstag im Monat ist Chaos-Orga-Plenum (intern). An allen anderen Diensten ist jede(r) Interessierte herzlich willkommen. Termine aktuell unter http://hamburg.ccc.de/bildungswerk/	http://hamburg.ccc.de/ Fon: +49.40.401.801.0, Fax: +49.40.401.801.41, Voice: +49.40.401.801.31.
Hannover, Leitstelle:11	Kneipe "kleines Museum" in Linden, >> am Mittwoch der zweiten Woche des Monats ab 20h	https://hannover.ccc.de/
Karlsruhe, Entropia e.V.	Gewerbehof, Steinstraße 23, >> jeden Sonntag ab 19:30h	http://www.entropia.de/
Köln, Chaos Computer Club Cologne (C4) e.V.	Vogelsanger Str. 286, 50° 56' 45" N, 6° 51' 02" O (WGS84), >> jeden letzten Donnerstag im Monat um 19:30h	Fon: +49.221.546.3953 <oeffentliche-anfragen@koeln.ccc.de>, http://koeln.ccc.de/
München, muCCC	Blutenbergstr. 17, >> jeden zweiten und vierten Dienstag im Monat ab 19:30h	http://www.muc.ccc.de/
Ulm	Treffen Montags ab 19.30 Uhr entweder im 'Café Einstein' an der Uni Ulm oder beim Internet Ulm/Neu-Ulm e.v. (am Besten vorher per Mail anfragen!). Regelmäßige Vorträge im 'Chaos Seminar': http://www.ulm.ccc.de/chaos-seminar/	http://ulm.ccc.de/ <mail@ulm.ccc.de>

Chaos-Treffs

Aus Platzgründen können wir die Details aller Chaos-Treffs hier nicht abdrucken. Es gibt aber in den folgenden Städten Chaos-Treffs mit Detailinformationen unter <http://www.ccc.de/regional/>: Bochum, Bremen, Darmstadt, Erlangen/Nürnberg/Fürth, Freiburg i. Br., Gießen / Marburg, Trier, Kiel, Münster / Osnabrück, Saarbrücken, Stuttgart, Emden

Friends & Family

Zur näheren Chaosfamilie zählen wir (und sich) den/der Beinaheerfakreis Häcksen (<http://www.haecksen.org/>), den/der "Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V." - FoebUD (<http://www.foebud.de/>) und die C-Base Berlin (<http://www.c-base.org/>).

Die Datenschleuder Nr. 80

Viertes Quartal 2002 <http://ds.ccc.de/>

Herausgeber

(Abos, Adressen, Verwaltungstechnisches etc.)
Chaos Computer Club e.V., Lokstedter Weg 72, D-20251 Hamburg, Fon: +49.40.401.801.0, Fax: +49.40.801.401.41, <office@ccc.de>

Redaktion

(Artikel, Leserbriefe, Inhaltliches, etc.)
Redaktion Datenschleuder, Postfach 640236, D-10048 Berlin, Fon: +49.30.285.997.40, <ds@ccc.de>

Druck

Pinguindruck, Berlin; <http://pinguindruck.de/>

Layout, ViSDP und Produktion

Tom Lazar, <tom@tomster.org>

Redakteure dieser Ausgabe

Tom Lazar <tomster> und Dirk Engling <erdgeist>

Autoren dieser Ausgabe

Andreas, cryx, docx, erdgeist, fefe, roh, ruedi, sill, soundjunkie, starbug, tomster.

Eigentumsvorbehalt

Diese Zeitschrift ist solange Eigentum des Absenders, bis sie dem Gefangenen persönlich ausgehändigt worden ist. Zurhabenahme ist keine persönliche Aushändigung im Sinne des Vorbehaltes. Wird die Zeitschrift dem Gefangenen nicht ausgehändigt, so ist sie dem Absender mit dem Grund der Nicht-Aushändigung in Form eines rechtmittelfähigen Bescheides zurückzusenden.

Copyright

Copyright © bei den Autoren. Abdruck für nicht-gewerbliche Zwecke bei Quellenangabe erlaubt.

Das Phänomen Microsoft

von tomster <tom@tomster.org>

Was nützt es, Recht zu haben, wenn Dir niemand zuhört? Nicht nur fanatische Microsoft-hasser, sondern auch moderate Kritiker, ganz ohne Schaum vorm Mund, stossen mit unschöner Regelmäßigkeit auf taube Ohren oder gläserne Augen, wenn sie Windows-Usern ihre Bedenken ob Monopolmißbrauch, Security und Datenschutz nahebringen. Was also tun? In diesem Artikel geht es weniger darum, bessere Argumente zu liefern, sondern vielmehr darum, diese überhaupt anzubringen.

Denn eins ist klar: an dieser Stelle Munition gegen den Einsatz von Microsoftprodukten aufzulisten wäre sinnlos. Kaum jemand im Chaosumfeld benutzt Windows oder Office. Ein Rundgang auf dem 19C3 z.B. hat mir subjektiv den Eindruck vermittelt, dass Windows dort ungefähr den selben Marktanteil hat, wie Linux oder Apple Macintosh "draussen in der realen Welt"...

Aber genau dort sieht es ja bekanntermassen viel düsterer – nämlich umgekehrt – aus. Die Monopolstellung von Windows in der 95%-Region hat zusammen mit einem drastischen Anstieg an PCs innerhalb der letzten Jahre dazu geführt, dass für die meisten Menschen die Begriffe *Betriebssystem* und *Windows* synonym sind. Auf einem PC Windows und Office vorzufinden ist für den durchschnittlichen User genauso selbstverständlich, wie dass Wasser aus dem Hahn kommt wenn man ihn aufdreht – und wird entsprechend auch genausowenig thematisiert oder hinterfragt.

"You're either part of the problem, part of the solution or part of the scenery."

Was das für Konsequenzen haben kann möchte ich zunächst mit einigen Beispielen aus eigener Erfahrung erläutern um anschliessend mögliche Lösungen zu diskutieren.

Da wäre z.B. die hochintelligente Zufallsbekanntschaft, die nach einem kurzen Gespräch "weitere Informationen" zu ihrem tollen Projekt per email schickt – und selbige mit einer geradezu naiven Selbstverständlichkeit als Word-Dokument anhängt. Die Idee, dass jemand, der eine email Adresse (und somit auch einen Computer) hat, kein Word benutzt (oder gar ein Betriebssystem, auf dem Office läuft) kommt ihr einfach nicht in den Sinn.

Oder auch Softwarehersteller, die mit keiner Silbe erwähnen, für welche Systeme ihr Produkt erstellt wurde, sondern kommentarlos eine .exe Datei zum Download anbieten [1]. Oft sogar in einem zip-Archiv verpackt, so dass der schlimme Verdacht, sich erst *nach* dem Download bewahrheitet. Als ob es kein Betriebssystem ausser Windows gäbe...

Dann gibt es da noch eine Beamtin aus meinem Bekanntenkreis, die aus "ethisch-moralischen" Gründen keine Nestlé-Produkte kauft oder IKEA-Möbel besitzt – aber unreflektiert Windows XP Home Edition benutzt und ein Hotmail-Account besitzt. Hotmail, der erste (grosse) Free- und Webmail Provider, wurde von Microsoft aufgekauft und setzt seither die Verwendung von Microsofts umstrittener Passporttechnologie voraus.

Die Liste liesse sich fast beliebig ergänzen. Die Frage hier ist aber: Was macht man mit solchen Leuten? Wie eingangs erwähnt, verlaufen Gespräche, die ausschliesslich die Absicht haben, den Gegenüber seinen/ihren Irrtum erkennen zu lassen, in der Regel so wie alle Konvertierungsversuche: bestenfalls erfolglos, oft genug katastrophal.

Ohne Thema kein Dialog

Vielleicht kennt der eine oder andere Leser das auch: man bemüht sich redlich, bleibt sachlich, führt Vor- und Nachteile an und trotzdem bleibt am Ende ein schaler Nachgeschmack. Der Gesprächspartner kommt sich irgendwie bevormundet vor und man selbst hat das Gefühl, irgendetwas gründlich falsch gemacht zu haben. Ich selbst hatte lange keine Ahnung, was es sein könnte und hatte immer vermutet, dass meine Argumentation wohl zu radikal sei und war deshalb immer peinlich darauf bedacht, möglichst ausgewogen zu argumentieren. Weniger "Microsoft is evil", dafür mehr Vernunftgründe. Genützt hat es aber nichts. Im Gegenteil, wie wir gleich sehen werden...

"Ist doch klar! Wer hört schon gerne, dass er was falsch macht? Du musst die Botschaft besser verpacken, wenn sie heil ans Ziel kommen soll!" Das kann aber auch nicht gut gehen, denn letztendlich halte ich es ja tatsächlich für *falsch*, Microsoftprodukte einzusetzen und damit eine Firma zu unterstützen deren Geschäftsprinzipien auf eklatante Art und Weise gegen so ziemlich alle meine ethisch-moralischen Prinzipien verstoßen! Verdammst nochmal ;-) Da helfen auch keine Samthandschuhe...

Bis ich es neulich dachte, es endlich erkannt zu haben: die sind nicht beleidigt sondern *gelangweilt!* Du! Eigentlich eine ganz einfache Übung: Du versetzt Dich in die Lage Deines Gesprächspartners... Was dabei herausgekommen ist? Sagen wir mal so: Ich vermute stark, dass für die meisten "Normal-User" da draussen alles, was mit Betriebssystemen, Softwarestandards und Monopolpolitik ungefähr genauso spannend und relevant ist, wie die Frage, ob Märklin oder Fleischmann die bessere Wahl bei Modellbaueisenbahnen ist. "Ist Apple besser als Windows? Ist HO besser als Spur N? Lass mich doch in Ruhe. Ich frag' Dich doch auch nicht, ob Deine Unterhosen von Schiesser oder C&A sind!"

Dabei ist es überhaupt nicht so, dass Computer und Internet *an sich* kein Thema für den Normaluser darstellen. Ein Blick auf die Computer-Ecke beim Zeitschriftenhändler genügt, um das festzustellen. Die Leute sind regelrecht verrückt danach. "Volkssport MP3". DivX-fähige, digitale Videorecorder bei ALDI. URLs und eMail Adressen auf alles und jedem. Internetcafés an jeder Ecke. Herrgott, es gibt sogar ne Computer-BILD!!

Das Problem ist also keinesfalls, dass die Leute nicht über Computer sprechen wollen. Im Gegenteil. Wenn Du Pech hast und Dir das Prädikat "kennt sich mit Computern aus" anhaftet, kannst Du Dich in der Regel garnicht davor retten, dass Dich Bekannte aller couleur unaufgefordert mit Ihren (Windows-) Computer-Wehwehchen belästigen.

Mein Fazit: Der normale User betrachtet Computer eben aus einer phänomenalen Perspektive ("Mein Computer druckt nicht.", "Das Internet ist kaputt.") wohingegen Nerds die Sache eher aus einer kausalen Perspektive sehen ("Der CUPS-Dienst startet aufgrund unzureichender Zugriffsrechte nicht und deshalb kannst Du nicht drucken.", "Das Netzteil Deines Modems hat einen Wackelkontakt.")

Zwei Welten prallen aufeinander. Aua.

Eigentlich ist damit ja alles wieder beim Alten: Macht stützte sich doch schon immer gerne hauptsächlich auf passive Gleichgültigkeit und weniger auf aktive Unterstützung seitens der Massen. Und denen ist es nun mal offensichtlich scheissegal, wem welche Software gehört, hauptsache sie können schön klicken.

Sollte das alles sein? Ich glaube nicht. Ich glaube vielmehr, dass es – und ich spreche jetzt wirklich nur für mich – noch einen weiteren Grund gibt, weshalb die obengenannten Gespräche so unerfreulich verlaufen. Unterschwelliger Hass. Denn wenn ich ganz, ganz, ganz ehrlich bin: wenn es etwas gibt, dass mich mehr ankotzt als Microsoft (und die Geisteshaltung derer, die dort verantwortlich sind) dann doch wohl die blöden User da draussen, die sich den Scheiss gefallen lassen!

So jetzt ist es raus. Ich fühle mich besser. Immer dieses schleimige "Ach, Du hast Probleme mit deinem Internet Explorer/Outlook/Windows XP/Office? Das tut mir aber leid. Da kann ich Dir aber leider wirklich nicht helfen, weil ich mich mit sowas garnicht mehr auskenne. Aber hast Du schon mal daran gedacht, es mit Mozilla/Linux/MacOS/OpenOffice zu probieren?" Das kann auf die Dauer nicht gutgehen, wenn ich in Wirklichkeit denke "Du bist doch echt selbst Schuld, Alter. Die Gedanken, die Du Dir aus Bequemlichkeit bei der Anschaffung deines blöden Windows PCs nicht machen wolltest, soll ich mir jetzt machen, um den Schlamassel wieder gerade zu biegen? My ass!"

Microsoft ist unschuldig: Gelegenheit macht schliesslich Diebe...

Ja, das wäre doch mal ein ganz anderer Ansatz. Da sich niemand den schweren Jungs in Redmond entgegenstellt, kann man ihnen auch keinen Vorwurf machen, dass sie das weidlich ausnutzen. Oder? Also bleiben ja wohl nur noch die *Microsoftuser* übrig...

Ich gehe jetzt jedenfalls direkter in solchen Gesprächen vor. Ich sage den Leuten ruhig, aber ehrlich, dass ich glaube, dass sie mit der Verwendung von Microsoftprodukten mehr als nur eine technische Entscheidung getroffen haben. Gut, einigen muss ich überhaupt erst erklären, dass (ich glaube, dass) sie damit eine Entscheidung getroffen haben. Nämlich für eine ganze Plattform und Firmenphilosophie und nicht – wie vermeintlich – nur für oder gegen „das Modell mit oder ohne DVD-Laufwerk“. Und dass ich glaube, dass diese Entscheidung schlicht und ergreifend falsch ist. Und dann... lasse ich es darauf beruhen...

Die Folgen sind verblüffend: die Leute wissen wonan sie bei mir sind und können damit umgehen. Kein schaler Nachgeschmack mehr. Aber das beste: der Ball ist damit jetzt sozusagen in ihrer Hälfte des Spielfeldes. Aus ihren Rechtfertigungen haben sich schon manche interessante und fruchtbare Diskussionen entwickelt. Weil der Motor dafür jetzt nicht mehr bei mir lag, sondern bei ihnen.

Und meine Meinung über die "dummen Windows-User" habe ich mittlerweile auch ändern dürfen: die meisten hinterfragen ihre Entscheidung nämlich doch bereitwillig und aufrichtig. Ich muss sie nur lassen...

[1] <http://www.musicmatch.com/home.htm>

OpenELSTER?

von Andreas Bogk

Ich habe mich neulich mal ein bißchen drüber beschwert, daß man in Deutschland zwar eine Steuererklärung übers Internet abgeben kann, aber nur mittels einer Windows-DLL. Folgende, durchaus zufriedenstellende Antwort habe ich erhalten.

Hallo Herr Bogk,

mit dem Projekt "Elektronische Steuererklärung - ELS-TER" verfolgen Bund und Länder das Ziel, die Abgabe und Bearbeitung von Steuererklärungen durch den Einsatz moderner Kommunikationsmittel bürgerfreundlicher und weniger verwaltungsaufwendig zu gestalten.

Zentraler Bestandteil dieses Verfahrens ist die als bundeseinheitliche Software entwickelte ELSTER-Client-Software (TeleModul), welche die Entwickler von Steuer-, Finanz- oder Lohnbuchhaltungsprogrammen beim Einhalten von Schnittstellenspezifikationen unterstützt und Transaktionen mit den Rechnern der Steuerverwaltung ermöglicht. Sie wird allen interessierten Anwendungsentwicklern kostenlos zur Verfügung gestellt.

Da kommerzielle Steuererklärungsprogramme derzeit fast ausschließlich für Windowsbetriebssysteme angeboten werden, haben die Referatsleiter Automation (Steuer) der obersten Finanzbehörden des Bundes und der Länder entschieden, in der ersten Entwicklungsphase zunächst die marktbeherrschenden (Windows32-)Betriebssysteme zu unterstützen.

Diese Entscheidung wurde getroffen, um eine größtmögliche Zielgruppe kurzfristig zu erreichen, und berücksichtigt damit die Grundsätze der wirtschaftlichen und zielgerichteten Verwendung von Steuermitteln.

Mit der Erweiterung des Angebots von ELSTER zur Datenübermittlung für den Bereich der Unternehmenssteuern ist eine Anpassung der ELSTER-Client-Software vorgesehen. Sie trägt dem erklärten Ziel der Bundesregierung, den Einsatz von Open-Source-Software zu fördern, Rechnung, in dem die u.a. im betrieblichen Bereich üblichen Betriebssysteme (Mac-OS, LINUX, UNIX, MVS, BS2000) unterstützen werden sollen.

Die hierzu erforderliche Neuentwicklung unter Verwendung der Java-Technologie wird jedoch noch einige Zeit in Anspruch nehmen.

Aktuell kann ich Ihnen hierzu sagen, dass neben der Bereitstellung eines Java-API's auch die Möglichkeit geboten wird, selbst mit unserem Server zu kommunizieren. Hierzu wird es demnächst eine Spezifikation geben. Im Groben werden dies sein:

- XML-Datenstrukturen mit XML-Schema
- http
- Verschlüsselung nach PKCS#7
- Signatur nach XML-DSig

Eine Offenlegung des Quellcodes ist leider nicht möglich, da einige Komponenten zugekauft sind und - anders als bei herkömmlichen Open Source Projekten - unser API fast ausschließlich von anderen kommerziellen Steuer- oder FIBU-Softwareherstellern implementiert und i.d.R. nicht von freischaffenden Entwicklern genutzt wird. Die Verwaltung einer OpenSource-Community für die wenigen interessierten Steuersoftware-Entwickler würde unsere Kapazitäten sprengen.

Ich denke aber auf Basis der oben angedeuteten Spezifikationen wird es jedem Entwickler freigestellt, seine eigene Clientapplication für ELSTER zu entwickeln. Der Aufwand wegen der geforderten Sicherheitskomponenten darf aber nicht unterschätzt werden, so dass es unter Umständen einfacher sein wird unser kostenloses Java-API zu benutzen.

Mit freundlichen Grüßen Roland Krebs

Oberfinanzdirektion München

- IT-Bereich - Anwendungsentwicklung

Projektleiter ELSTER

Hallo, Ich bin in einen Counter-Strike Clan..

und wollte fragen ob sie uns einen Server dazu sponseren können. Wir machen dafür auf unserer Homepage Werbung für sie und lassen alles im Server zeigen was sie für Produkte oder sonstiges haben !! Wenn die einen Werbe Banner haben stelle wir den auch gern auf unserer homepage zur verfügung !! Ich würde mich sehr freuen wenn es klappen würde !! Meine e-mail adresse ist <cedric_lichte@msn.com> !!!

weitergeleitet. Nur falls jemand... :) <erdgeist>

Benötige dringendst einen tip

von euch bzw. einen rat an wen ich mich wenden kann oder was zu tun ist: Hänge mit meinem pc am server im netz der firma. Wie kann ich wirksam meine surfspuren beseitigen?

1. Sicher surfen, dort wo es angeboten wird, auf den Prefix <https://> achten, damit kann niemand an den zentralen Übergabepunkten deiner Firma den Netzwerkverkehr, und damit den Inhalt deiner Surferei, mitlesen

2. Deinen Browsercache löschen, beim IE:

tools->internet options->Temporary internet files-> delete files
tools->internet options->history->clear history
bei den anderen Browsern sollte es nicht so schwer zu finden sein.

3. präventiv: genau auswählen, welche Seiten man in einem nicht vertrauenswürdigen Netzwerk auf deinem Betriebssystem (ich weiß nicht, wie sehr du dem vertraust) du besuchst

ist es jemandem möglich nachzuvollziehen, auf welchen seiten ich war?

Ja. Unter anderem dem Seitenbetreiber, dem Administrator am Gateway oder Proxy, jedes anderen Computers, der während deiner Surferei direkt an deinem Netzwerk angeschlossen war, jedem, der Zugriff auf deinen Computer hat und in der Browserhistory nachschaut. Zudem munkelt man von staatlichen Bedarfsträgern, die beim Internet Service Provider deiner Firma ein Auge auf die von dir besuchten Seite werfen, genau, wie auch beim Anbieter derselben oder IRGENDWO auf dem Netzwerk-Weg zwischen euch beiden, immer mal jemand lauschen kann.

Was der inhalt meiner e-mails an eine gmx-adresse war?

Siehe oben. Zudem kann der Empfänger deiner email und alle Hände, durch die die email gegangen ist (sein ISP, sein Admin, nochmal der Staat, vielleicht noch eine Mailweiterleitung, jemand, der im Netzwerk des Empfängers den Verkehr beim Abholen der Mail mitgelesen hat...) Auf deinem Rechner wahrscheinlich eher nicht.

was ich dort gelesen habe?

Das weiß keiner. Dazu hätte man dich beobachten müssen... aber wo wir doch schonmal so paranoid sind: welche Seiten auf deinem Bildschirm waren, kann man auch über Abstrahlung deines Monitors feststellen. Du mußt dich nur immer fragen, ob der Aufwand all dessen durch die Brisanz des Vorgangs gerechtfertigt wäre. Wenn du mit Lesen aber Heruntergeladen meinst, dann befindet sich eine Kopie dessen in deinem Browsercache.

Bitte helft mir...BALD <defef>

Hmm. Gern geschehn. Wenn du dafür in deinen nächsten emails ein klein wenig auf Satzzeichen, Gross- und Kleinschreibung und all die Winzigkeiten achten könntest, die einem das Lesen deiner Mail erfreulicher machen, dann auch gern immer wieder. <erdgeist>

guten tag...wer auch immer das liest...

ich hab eine frage die nicht mir dienen soll sondern allen anderen denen noch nichts passiert ist...vor kurzem ist mir ein trojaner untergekommen welcher sich aktiviert hat und dann halt verbindung aufgenommen hat... das gegenstück hatte sich dann einen moment später in meinem rechner eingehackt welches nicht schlimm ist weil ich keine daten auf dem rechner habe(extra eine platte fürs internet)nachdem ich nicht das machte was er wollte hat er kurz mal eben so meine platte zerschossen(die reg gekillt).da er nebenbei den fehler machte und mit einer pn über den yahoo messenger reinkam der bei mir nebenbei läuft hatte ich ein yahoo id von ihm...ich habe also von einer anderen platte kurz ein neues system copiert und bin sofort wieder ein ins net und hab ihn über den messi angequatscht...mit dem erfolg das ich nun 3 namen von ihm habe...das sein freund trojaner programmiert...er die hps macht wo die raufkommen...sie an guten tagen 40 leute wie mich haben...und eine copie von der zerschossene platte...die frage lautet nun was kann man gegen solche leute tun... mfg <xxx@yahoo.de>

could not decode data stream <erdgeist>

Ich habe gehört, dass sie die Macht haben

meinen Computer zu überprüfen von Ihrem Standort aus. Mein Neuer Rechner ist zwar erst ein paar Wochen alt, aber ich glaube, das er irgend wie spinnt. Also wenn das wirklich geht, das Sie meinen Computer, wenn er online ist überprüfen können das wär ja stark. <xxx-0001@T-Online.de>

Sehr geehrter Herr xxx.

Vielen Dank für ihren Auftrag. Wenn sich die Konzentration der Macht bei uns wieder dem nötigen Level annähert, werden wir unsere Seher losschicken, die Computronendichte in ihrem Rechner zu erfühlen. Dazu müssen sie aber 5 Kerzen im Pentagramm um ihn herum aufbauen.



Aber im Ernst: wir könnten theoretisch Schwächen in der Programmierung des Betriebssystems auf deinem Computer ausnützen, um Kontrolle über die Funktionen des Rechners zu erlangen. Sowas machen wir aber auch nicht üblicherweise zum Frühstück, hat rechtliche Implikationen und liefert uns deutlich weniger Informationen, als der Händler, der dir den Rechner verkauft hat, durch Aufschrauben erlangen kann. Wende dich bitte an ihn. <erdeigt>

QSC Teil 1: IP-Adresse / Network Address Translation (NAT)

Das Produkt Q-DSLmax beinhaltet die Zuteilung einer offiziellen, festen IP-Adresse. Die Verwendung von NAT (Network Address Translation) und die damit verbundene Uebersetzung der Netzwerk-IP-Adressen auf die offizielle IP-Adresse ist einerseits ein Security Feature, da die Netzwerk-Adressen nach aussen hin nicht mehr sichtbar und damit angreifbar sind. ... Auf besonderen Wunsch des Kunden kann alternativ zur Verwendung von NAT auf einer festen IP-Adresse auch ein ganzer statischer IP-Netzbereich (bis zu 32 Adressen) gegen gesondertes Entgelt durch QSC AG bereitgestellt werden.

Gegen mehr Geld, schalten wir das Feature auch aus! <Cryx>

<http://www.qsc.de/de/produkte/q-dslmax/leistungsbeschreibung/index.html?qscrelaunch=89ed43f2a3d5b8cae2e0714d7d0663c6>

Liebe Redakteure und Redakteurinnen

(auch wenn ich gerade keine bei euch sehe :-)), jedesmal, wenn ich die 'Schleuder durchblättere, bekomme ich so ein Gefühl, dass es eigentlich schade ist, nicht bei eurem Projekt mitzuhelfen. Andererseits kann man jedoch nicht an allen Fronten kämpfen, oder?

Jedenfalls möchte ich euch nur sagen, dass ich das sehr wichtig finde, was ihr macht und ich der Meinung bin, dass ihr es gut macht und ich hoffe, wenigstens mit meinem bescheidenen Mitgliedsbeitrag helfen zu können.

Wer behauptet, nur weil es heutzutage keine Drachen mehr gebe, könne es auch keine Helden mehr geben, der irrt. Denn es gibt viel schlimmere Sachen als Drachen, nämlich Politiker, die sich das Marketingprinzip zu eigen gemacht haben, dass diejenigen, die am besten lügen (die beste Werbung machen), sich am besten verkaufen (d.i. gewählt werden); was dabei herauskommt, ist – wen wundert's – eine käufliche Politik, die Gesetze verabschiedet, bei denen sich vielen von uns – insbesondere denjenigen, denen Freiheit etwas bedeutet – der Magen umdreht; und alles unter dem Deckmantel der Sicherheit. Zu allem Überfluß und um den Fatalismus zu besiegeln sind die Politiker damit auch noch erfolgreich, weil das bei einem Großteil der Leute funktioniert (frei nach dem Motto: weil die Sachzusammenhänge zu kompliziert sind, freuen wir uns, wenn wir von den Politikern

monokausale Erklärungen bekommen, damit wir ruhig schlafen können (bloß wie lange? bis zum nächsten Attentat?); vgl. Bildzeitung, Explosiv usw.).

Bevor diese Mail in ein kleines Manifest ausartet und ihr den Eindruck bekommt, ich sei ein hoffnungsloser Pessimist (was ich m.M.n. nicht bin), möchte ich damit schließen, dass ich den kleinen Helden von heute, die nicht (nur) für das Herz einer Prinzessin oder eines Prinzen kämpfen, sondern für die Freiheit von morgen, mein großes Dankeschön ausdrücke und ich hoffe, dass ihr noch lange so gut weitermacht!

Herzliche Grüße <Stephan Schleim>

TCPA, wie ist da Ihr Standpunkt ?

Inwieweit beschäftigen Sie sich schon intensiv mit dem Problem und welche Lösungen bzw. Gegenstrategien sind Ihnen bekannt ? <xxx@t-online.de>

Uns ist das Problem schon seit längerem bekannt.

So hat sich das Chaosradio Nr. 78 [1] mit dem Thema auseinandergesetzt. Einen Mitschnitt der Sendung gibt es unter [2].

Während unseres jährlichen Congresses in Berlin vor ein paar Tagen, gab es einen Vortrag [3], der sich damit auseinander setzte. Generell kann gesagt werden, dass das Thema dort in aller Munde war. <Lars>

[1] <http://chaosradio.ccc.de/cr78.html>

[2] <ftp://ftp.ccc.de/chaosradio/cr78>

[3] <http://www.ccc.de/congress/2002/fahrplan/event/366.de.html>

Hacker-Kurse???

Gibt es die Möglichkeit einen Hacker-Kurs zu belegen oder ähnliches??? Oder was würden Sie mir vorschlagen? <xxx@t-online.de>

Du hast Glück, unser im Buchhandel erhältliche Kurs "Hacken in dreißig Tagen" ist ausgelassen. Wir bieten jetzt ein neues Präsenz-Seminar "Hacken in drei Tagen" an. Das stellt praktisch eine Verzehnfachung des Wertes dar, obwohl der Preis mit 40 Euro normal / 25 Euro Schüler nur geringfügig gestiegen ist.

Zur Teilnahme an diesem einmaligen Seminar mußt Du allerdings einen Test bestehen: Bediene eine Suchmaschine (z.B. Google) und suche den Geheimcode "19c3". Schon steht die Tür offen zu vielen interessanten Workshops zum Thema Hacken und zu vielen Leuten, mit denen man sich austauschen kann.

Aber Vorsicht, nur solange Vorrat reicht! ;-)
<Sebastian>

Wie kann man das Hobby HÄCKER

als Beruf ausüben ??? Eisbär <xxx@lycos.de>

Indem man Forstwirt wird. <Lars>

Server an den Pranger!

Brauche Hiiiiiiiilfe von euch Profies. Hallo CCC, ein paar Freunde und ich haben ein ersthaftes Problem, und zwar werden wir seit LÄNGERER Zeit von meinem ominösen Server mit Fakemails bombardiert. Das sind diese Art von Mails wo man von imaginären Freunden aufgefordert wird, ihre Hompages zu besuchen, und wie nicht anderst zu erwarten landet man auf Illegalen/Sex Seiten! Das alles wär ja nicht so schlimm, wenn nicht jede 3. dieser Mails einen sich automatisch öffnenden Dealer hätte! Was uns aber am meisten stört, ist dass diese Mails ständig ihren absender ändern und sie zuhauf, manchmal 22mal pro Woche bei uns eingehen! Ich selber habe seit einer gewissen Zeit meine dienste als Hacker erstmal eingestellt, da ich einmal beim ZERHacken eine RechtsradikalenSeite erwischt wurde und glücklicherweise nochmal dank fehlender Beweise mit dem Schrecken davon gekommen bin! Aber ihr habt das Wissen und die Mittel solchen Servern den gar auszumachen! Und ich bitte euch im Namen tausender geplagter User, dieses Ding zu KILLEN! MfG.:<xxx@compuserve.de>

22 Mal pro Woche? Das ist verdammt wenig. Ich beneide euch. <Lars>

Abschlußprüfung

hi leute heute habe ich aus zuverlässiger quelle erfahren das heute nacht die Abschlußprüfung Mechatroniker die in 4 tage oder so statt findet geklaut worden ist könnt ihr mir irgend wie helfen an die prüfung ran zu kommen ?????? bitte <xxx@uboot.com>

http://www.duden.de/index2.html?produkte/nachschlagewerke/komma_punkt.html ... und nein. <ths>

Und später tötet das, was Du als Mechatroniker installierst, meine Tochter? Nö, danke. </padeluum>

frage zur rechtlichen lage...

hi ccc. eine frage hab ich da - wo kann ich artikel bzw. gesetze zur rechtlichen lage beim hacken von wave-lans finden? habt ihr da ein paar nette links für mich? danke, andy *ps: blinkenlight rules !)* <as@xxx.net>

Maximilian Dornseif, Kay H. Schumann, Christian Klein: Tatsächliche und rechtliche Risiken drahtloser Computernetzwerke DuD 4/2002 </Julius>

http://www.datenschutz-und-datensicherheit.de/jhrg2/heft0204.htm#Schwerpunkt

hi ich bin alex

und möchte wissen wie ich eine richtig gute Homepage mache, ich hab es bei aol schon probiert aber so richtig gefunzt hat es nicht <xxx@aol.com>

Hallo, ich bin Volker und ich möchte Dir empfehlen, daß Du Dir mal SelfHTML reinziehst. <Volker>

Sehr geehrte Damen und Herren, liebe Chaoten

Ich habe mir kürzlich zum Aufzeichnen von Lesungen, Rezitationen und Diskussionen einen Sony MiniDisc Recorder Net MD N707 gekauft. An der Überspielung von Musikstücken bin ich weniger interessiert (höchstens als Hintergrunduntermalung aus meinem eigenen CD-Bestand). Der Verkäufer im Promarkt Eschborn wußte von dem Grund des Kaufs. Mit dem Gerät kaufte ich auch ein Stereomikrofon. Er empfahl mir dieses Gerät wegen der USB-Verbindung und dem qualitativ besseren und schnelleren digitalen Datentransfer. Erst zuhause und nach mühsamem Suchen im Handbuch fand ich heraus, daß der Datentransfer beschränkt ist entweder für Daten vom PC auf die MD - oder für Stücke von der MD auf den PC, sofern sie vorher vom PC heruntergeladen wurden. Daten, die durch Aufzeichnung direkt auf der MD erzeugt werden, können nicht auf den PC überspielt werden. Die mitgelieferte Software Jukebox 2.2 verweigert dann den Transfer. Als Grund wird Schutz des Copyrights angegeben. Denn sonst könnte man die wiederbespielbaren MD's sehr leicht von Gerät zu Gerät austauschen, auf einen PC spielen und davon CDs brennen. Nur: auf diese Weise bleibt das Copyright an meinen eigenen Sprachaufzeichnungen auf der Strecke. Meine Frage und Bitte an Sie: Gibt es eine Software, die die Sperre von Jukebox 2.2 aufheben oder umgehen kann? Ich habe mich nicht nur über den Verkäufer geärgert - noch mehr über Sony, die mit irreführender Werbung die Kunden an der Nase herumführen. Ich habe später im WEB ähnlich frustrierte Statements von enttäuschten Käufern gelesen, die selbst etwas produzieren möchten - aber ihr Produkt nicht auf den PC übertragen können. Höchstens analog (mit Qualitätsverlust und langer Laufzeit). Für jede Hilfe, jeden Tip bin ich dankbar. Vor allem in diesem Fall für jeden Hacker, der mir mein eigenes Recht verschafft. Es wäre endlich etwas nützliches als dumme Mailviren! Mit freundlichen Grüßen, Regina Berlinghof

vielen dank fuer dein plastisches beispiel dafuer, wie die industrie ihre eigenen interessen ueber die der konsumenten/buerger stellt.

konkrete hilfe kann ich dir jetzt nicht aus dem sprichwoertlichen aermel schuettern, aber wir werden deine anfrage auf jeden fall in der kommenden ausgabe abdrucken. vielleicht kann dir ja einer unserer leser weiterhelfen. <tomster>

Sicherheit Zonealarm Pro 3.1xxxx

Meine Frage: ist Zonealarm "geknackt" worden und somit unwirksam? Habt Ihr da Infos für mich??? <xxx@gmx.de>

Zonealarm ist ein Programm wie jedes andere auch. Wer es deaktivieren will kann das auch. Wenn du mal einen schoenen Verriss lesen willst: http://www.fefe.de/pffa/ (und die Links da). <Jürgen>

Brauche HILFE !

Hört sich viel. blöd an was ich hier schreibe aber ich finde es gar nicht blöd ! ICH GLAUBE MEINE FRAU GEHT FREMD ! Sie hat das Passwort für unsere gemeinsame E-Mail Adresse ohne mein Wissen ändern lassen ! Gibt es irgend ein Programm um E-Mail Passwörter zu knacken oder kann mir jemand einen Tipp geben was ich tun soll ?

Klar: Red mit deiner Frau. Da war doch so ein Treueschwur, wegen Heirat und so. Nicht wahr? Naja, und wenn du deiner Frau jetzt nichtmal mehr so weit vertraust, dass du sie fragen koenntes warum (oder ersteinmal OB ueberhaupt) sie es getan hat (koennte ja auch ein Fehler bei deinem Mail- anbieter sein), scheide da bei euch doch noch viel anderes im Argen zu liegen, als nur ein bloeder email-account.<erdgeist>

Ich will wieder mit dem Hacken anfangen (private gründe)...

...habe es aber > seit 2 Jahren nicht mehr gemacht. Könntet ihr mir die wichtigsten > Sicherheitslücken und Änderungen per E-Mail mitteilen?

Heee, Christoph (oder soll ich sagen theface?!)

schoen, dass du dich mal wieder meldest, wir haben ja schon wirklich lange nichts mehr von dir gehoert. Und so ein wenig Sorgen haben wir uns auch um dich gemacht.

Naja, aber jetzt, wo du wieder da bist: wir haben in den letzten 2 Jahren ziemlich viele gute Maenner verloren. Die Boesen haben quasi gewonnen. Man, wo warst du nur? Wir mussten in den Untergrund, alles was es heutzutage "da draussen" noch als Meldungen ueber Sicherheits- luecken gibt, ist von DENEN, damit keiner merkt, was sie uns angetan haben. Und du? Ziehst dich einfach aus privaten Gruenden zurueck!?

Vergiss es einfach. Geh besser gaerteln oder Baeume umarmen. Ist nich so gefaehrlich. Ich muss jetzt aufh hoeren, der Waerter macht seine Runde. <erdgeist>

Null-T-arif

Viele Leute meckern immer darueber, dass die Telefon-tarife steigen wuerden. Diese Panik kann ich gar nicht nachvollziehen. Es mag wohl nur daran liegen, dass die meisten Nutzer ortsfester sowie mobiler Fernsprecher die Auswahl der Tarife sowie die Kombination derselben vernachlaessigen.

Daher an dieser Stelle ein wenig Werbung fuer gute Produkte der Fernmeldebranche welche gerade durch Kombination einen symbiotischen Effekt haben, der es nicht nur knausrigen Nerds warm ums Herz werden laesst.

Produkt 1: Genion, das Clevere Festnetz-Placebo von O₂. Man erhaelt eine Festnetznummer, auf der man

in einer sogenannten Homezone zum Festnetz-tarif erreichbar ist. Bei Genion kann man sogar bedingte Rufumleitungen schalten (z.B. nach 5 Sekunden) die, solange man sich in der Homezone befindet und die Umleitung innerhalb des O₂ Netzes laeuft, kostenlos sind.

Produkt 2: LOOP - Die Prepaidkarte von O₂. Diese Karte hat das tolle Feature (sprich: Fiehtschae!) dass man pro vollendeter ankommender Gespraechsminute ganze 2 cent gutgeschrieben bekommt. Dies gilt natuerlich auch fuer Gespraechе, die auf die loop-Karte umgeleitet werden.

Produkt 3: T-ISDN XXL - Mit diesem innovativen Produkt aus dem Hause des rosa - aeh pardon, magenta-farbenen „T“ erhaelt man die Moeglichkeit Sonntag und Feiertags kostenlos beliebige Festnetznummern zu erreichen, sogar die des Konkurrenten O₂.

Ruf doch mal an! <nibbler>

Subject: Höfliche Anfrage!

Sehr geehrte Damen und Herren!

Betrachten Sie diese email als höfliche Anfrage zu einer geschäftlichen Zusammenarbeit. Sie sind über die uns angeschlossene Suchmaschine Google bei uns gelistet. e-business <toppromo@freenet.de>

Hallo Hacker! Seit einem Jahr

gelingt es niemanden den Code zu knacken, mit dem der im Anhang stehende Text generiert wurde. Ich würde mich freuen, wenn sich jemand in einer freien Minute diesem Problem annehmen könnte - vielen Dank!

[... snip Dezimalgruetz...] <Andreas S>

Hallo Andreas, fein, was du geleistet hast. Echt prima. Du bist mein Held, ich kriegs nicht raus. Magst du vielleicht im Gegenzug das hier entschlüsseln: o gfgqco34o81urgf3uO=)Z%POZEW5zuvaTAoqoih dslifueuo(ti/&%=)(o(&\$LDSJF<YDSVFioiure. Danke <erdgeist>

QSC Teil 2:

Auf http://www.qsc.de/de/produkte/q-dslmax/fragen_und_antworten/?qscrelaunch=89ed43f2a3d5b8cae2e0714d7d0663c6#2 unter "Wie wird der Datentransfer abgerechnet?" findet sich dieser grossartige abschnitt:

"Fuer die Feststellung des Datentransfervolumens wird folgende Definition zugrunde gelegt. Ein GB (Gigabyte) entspricht eintausend MB (Megabyte), ein MB eintausend kB (Kilobyte) und ein kB eintausend Byte."

Schoen nicht? "Solange dein traffic durch meinen router geht, definiere immernoch ich wieviel ein byte ist!" <Cryx>

Fear, Uncertainty, Consumption, Knowledge... Und Palladium

von Erdgeist <erdgeist@erdgeist.org>

Wir haben vor allem Möglichem Angst. Ist ja auch nur zu natürlich. Bei allem, was man immer so liest und hört. Es ist eine schreckliche Welt da draußen und das Einzige, was uns noch retten kann, ist: viel Geld auszugeben.

Was es genau ist, das uns Angst machen muß? Das ist von Fall zu Fall natürlich unterschiedlich. Aber generell sind es zwei Dinge, die sie verursachen: Unwissenheit und Unsicherheit. Und es gibt genug Leute, die von deiner Angst leben: Politiker, Polizisten, Anwälte, Versicherungsverteter, Potenzpillenhersteller, die Presse, die Rüstungsindustrie, sogar Greenpeace. Also gibt es auch ein vitales Interesse, dir deine schöne Angst nicht wegzunehmen. Man sehe sich nur die RTL-Abendnachrichten an und spiele ein kleines Spiel: versucht einmal, jeden Beitrag in eine der beiden Kategorien Angst oder Konsum einzuordnen. Und dann sagt, wo es die idyllischeren Bilder zu sehen gibt. Und wieviel Hintergrundinformationen vermittelt wurden. Dann schau man sich die darauffolgende Soap an und sage, welche Gestalten gemeinhin als Sympathieträger oder Identifikationsfiguren propagiert werden. Wissen und Intelligenz ist nicht schick, Erfolg nicht mehr Ergebnis von Fleiß. Daß gerade bei der Bildung gespart wird, wenn es nicht um die Elite geht, mag Zufall sein. Der Trend jedoch ist erkennbar: weg vom mündigen Bildungsbürger, hin zum modernen Konsumbürger mit all seinen pflegebedürftigen ngsten.

Was uns das als Hacker interessieren muß, die wir doch größtenteils reflektierte, nicht vom Konsum verblendete Heroen sind? Wir sind das prototypische Feindbild des Konsums. Wir schließen uns meist nicht der Finanzelite an und versuchen nicht einmal, eine berechenbare Gegenelite zu bilden. Unser erklärtes Ziel ist es, Herrschaftswissen zu nehmen und dem Beherrschten zugänglich zu machen, zudem sein privates Wissen vor der zentralen Erfassung zu schützen. Höchste Zeit, dem Hacker ein bedrohliches Image zu verpassen und am besten noch mit dieser neuen Angst Geld

zu verdienen. Hier eine proprietäre Virensan-Software, dort eine Closed-Source Firewall, und natürlich im Fernsehen neben den Bösen, die Bomben auf Unschuldige werfen, der Hacker, der sich deine Festplatte zum Ziel genommen hat, so zwischen Überschwemmung, Lebensmittelvergiftungen und der Werbung. Da, wo die Komplexität des Systems das Verständnis sprengt und darüber hinaus magische, fast religiöse Grenzen ankratzt, findet auch leicht die Überhöhung des Hackers ins Diabolische statt.

Aber auch wenn man die Angst durch Bildung bekämpft, bleibt sie nominal oft gleich: Denn hier führt Beseitigung der Unwissenheit zu einer Zunahme der eigenen Unsicherheit - die zweite Quelle der Angst. Wem zum Beispiel vertrauen wir denn in letzter Zeit unser Weltwissen an? Wir vertrauen darauf, daß in einem Prozessor, dessen Leiterbahnen wir mit bloßem Augen nicht mehr erkennen können, sich Elektronen in gerade der richtigen Anzahl an den richtigen Stellen zusammensammeln, um bestimmte Schwellenwerte zu unter- oder überschreiten. Im Optimalfall kommt dabei die gewünschte Transformation der Daten heraus. Die Ergebnisse werden in Abermilliarden schnell flüchtiger Rückkopplungsgattern (üblicherweise Speicher genannt) abgelegt. Was aufhebenswert erscheint, wird als mikroskopisch kleine Magnetisierungsinsel auf schnell rotierende Metallscheiben gebannt, ständig auf der Furcht vor externen Magnetfeldern. Und wenn wir ernsthaft an das Konservieren für später denken, benutzen wir extrem lichtempfindliche Billigstkunststoffscheiben, in die wir mit starken Lampen Löcher brennen, diese mit weniger starken Lampen wieder abtasten, nur um die Daten kurz darauf dem selben Zyklus zu unterwerfen. (Wie lichtempfindlich die



Scheiben sind, kann man im Experiment mit einer über den Sommer ins Fenster gegangenen CD selbst nachvollziehen.) Alles in allem wohl ein unglaublich fragiler Ablauf, der nur mit Redundanz und dem kontinuierlichen Kopieren und Vergleichen der Daten mit den Zweit- und Drittkopien in stabilen Bahnen zu halten ist. (Versucht doch mal, eine Diskette von vor mehr als 7 Jahren zu lesen. Solltet ihr durch Zufall noch die passenden Laufwerke haben, ist die Wahrscheinlichkeit der Datenintegrität wohl eher gering).

Das bewährte Konzept der menschenlesbaren Papierkopie wird mehr und mehr zurückgedrängt, zumindest für die breite Masse, sie läßt sich zu schwer regulieren. Wissen ist (neben dem politischen) auch ein wirtschaftlicher Vorteil, Information Wirtschaftsgut. Öffentliche Bibliotheken sind finanziell so schlecht ausgestattet, wie schon lange nicht mehr, Tendenz fallend. Aber auch im Elektronischen, wo die Regulierung des Kopierens mittels Kontrolle über das Kopiergerät demnächst leichter fallen soll, sind die Bewegungen in Richtung Informationsverknappung und Mehrfachverkauf deutlich zu erkennen. Dabei geht es mir nicht primär um mp3s und Hollywoodschinken. Bald wird gar das private Pressearchiv urheberrechtlich bedenklich. An zentraler Stelle bleibt die Information natürlich für Geld weiter verfügbar. Ob aber morgen in der selben Zeitung noch dasselbe steht, wie heute, ist fraglich. Dabei muß man nicht gleich mit Orwell argumentieren, eine einstweilige Verfügung bei genügendem politischen/wirtschaftlichen/staatssicherheitstechnischen Interesse ist durchaus im Rahmen des aktuell Wahrscheinlichen.

Selbst Suchmaschinen, respektive deren Caches, haben sich zuletzt nicht als zuverlässig-objektive Archive gegen den Willen der, von den Informationen Tangierten, erwiesen. Eine dezentrale Informations-Vorhaltung und -aufbereitung kostet aber Geld. (Man schaue sich nur die Unordnung in der privaten mp3-Sammlung an. Dann stelle man sich vor, wie die aussähe, wenn irgendeine bezahlte Kraft den ganzen Tag nichts anderes zu tun hätte, als diese zu pflegen und zu erweitern.) Doch wo strukturiertes - und damit erst zugängliches - Wissen viel Geld kostet, muß sich die Akquisition/Aufbereitung auch finanziell lohnen. Sonst bleibt es Luxus, den man sich erst einmal leisten können muß. Aber aufgepaßt: Viel zu schnell droht einem dabei selber der Abrutsch in die Klauen der Finanzeliten, die einen in ihre Unterabteilung Wissenselite einsortieren. Beispiel OpenSource-Projekte: sogar hier findet man das gesamte Muster Fear, Uncertainty, Consumption wieder. Was bleibt, wenn man etwa für eine Textverarbeitung auf proprietäre Datenformate

angewiesen ist, reverse engineering verboten ist? Legal nur noch der Zukauf der Information, was bei einem kostenlosen OpenSource-Programm schlicht nicht finanzierbar ist. Und selbst wenn, bleibt beim potentiellen Benutzer der (auch vom Hersteller der kommerziellen Software gern gepflegte) Rest Unsicherheit, die Angst, die dann nur noch durch Konsum - Kauf der SW - besiegtbar scheint.

Zum Glück wird aber ab demnächst die Entscheidung, welche Software auf welchem Rechner laufen, welche Informationen man sich anschauen darf (und damit: welche aufhebenswert ist), die Wahl, welche zusätzliche Hardware man an seinen Computer anschließen, oder mit wem man kommunizieren will, von Firmen abgenommen, die sich damit ja nun wirklich auskennen müssen. Unter Zuhilfenahme eines Chips (oder gar der CPU) in jedem Computer wird der bestmögliche Schutz der Information vor dem Anwender gewährleistet. Das Kartell, das diesen Kraftakt stemmen will, heißt TCPA. Viele kluge Menschen haben viele kluge Worte dazu zusammengesammelt [1] (oder deutsch) [2], deshalb will ich hier nicht mit meiner laienhaften Interpretation der technischen Abläufe dahinter langweilen.

Die Implikationen sollte man sich aber, den oberen Teil des Textes als Maßstab genommen, vor Augen halten. Erstmals seit Gutenberg wird der Weg, Informationsvervielfältigungstechniken immer mehr zu verbessern, radikal verlassen. Die weltweite Zensur eines Fakts bedarf nichts weiter als der Eingabe einer Nummer in eine Datenbank (die wohl irgendwo auf einem Server in einem kulturellen Entwicklungsland zwischen Kanada und Mexiko liegt). Die redundante Vorhaltung von Informationen wird unglaublich teuer, wo nicht sowie-so technisch unmöglich, die Gefahr von Kollateralschäden ist immens. Kein Geheimdienst, der etwas auf sich hält, dürfte noch Computer benutzen, die Monopolklage gegen Microsoft liesse sich wahrscheinlich nicht wiederholen, da wichtige Beweisdokumente nicht lesbar wären. Es wird wohl Zeit, alle auf seinem Computer befindlichen Dokumente auszudrucken, (möglichst nicht auf "elektronischem Papier"), alle Tageszeitungen zu abonnieren und zu bevorraten. Zudem sollte man sich mit der Funktion einer Schreibmaschine auseinandersetzen. Auf jeden Fall aber: viel Geld ausgeben.

[1] <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>

[2] <http://moon.hipjoint.de/tcpa-palladium-faq-de.html>

AES und Attack

von Rüdiger Weis (cryptolabs Amsterdam) und Stefan Lucks (Universität Mannheim)

Gross war seit Oktober 2000 die Freude endlich über ein standardisiertes und sichereres Verschlüsselungsverfahren zu verfügen. Der neue Chipher Rijndael ist schnell und elegant - vielleicht etwa zu schnell und sehr wahrscheinlicher Weise viel zu elegant. Neue Angriffsmethoden lassen jedenfalls, obgleich noch entfernt von einer praktischen Durchführbarkeit, bei vielen Kryptographen recht ungute Gefühle entstehen.

Der AES (Advanced Encryption Standard) ist der Nachfolger des inzwischen wegen der zu geringen Schlüssellänge völlig unsicheren DES (Data Encryption Standard). Die Wahl des AES ist das Ergebnis eines mehrjährigen, mit großer Sorgfalt vom US-amerikanischen NIST (National Institute of Standards and Technology) betriebenen Prozesses [WL99].

Zentrale Anforderungen waren dabei:

- 128-bit breite Blockchiffre.
- Drei verschiedenen Schlüssellängen 128 bit, 192 bit und 256 bit.
- AES soll mindestens so schnell und sicher sein wie Triple-DES,
- Im Gegensatz zum DES-Verfahren wurden diesmal die Design-Grundsätze veröffentlicht.
- Die Entwickler mussten plausibel machen, dass ihre Algorithmen nicht mit geheimen Hintertüren versehen sind.

Auf der ersten AES-Konferenz 1998 wurden 15 Kandidaten präsentiert. Die Submission der Deutschen Telekom mit dem schönen Namen Magenta wurde übrigens schon während des Vorstellungsvortages gebrochen.

Nach der zweiten Konferenz wurden vom NIST fünf Finalisten ausgewählt.

- Mars
- RC6
- Rijndael
- Serpent
- Twofish

Von diesen Kandidaten wurden Mars, Serpent und Twofish von der NSA hohe Sicherheit bescheinigt und Rijndael und RC6 nur angemessene. Gegen Mars und RC6 gab es von verschiedener Seite Bedenken wegen möglicher Patentbegehlichkeiten.

Nach der dritten AES-Konferenz im Jahr 2000 mit einer eingehenden Diskussion der fünf Finalisten entschied sich das NIST für "Rijndael" als vorläufiger Standard, der Ende November 2001 als endgültiger Standard bestätigt wurde.

Rijndael

Rijndael wurde von den beiden Belgiern Joan Daemen und Vincent Rijmen entwickelt. Rijndael ist eine Weiterentwicklung des SQUARE Algorithmus, der ebenfalls von den beiden Autoren zusammen mit Lars Knudsen entworfen [DKR97]. Rijndael verwendet eine umkehrbare 8x8 bit S-Box und nutzt Berechnungen mit Polynomen über den Körper GF[28], um gute Diffusionseigenschaften sicherzustellen. Die Berechnungen erinnern an fehler-erkennende bzw. -korrigierende Codes (MDS-Codes). Rijndael ist im Gegensatz zu DES kein Feistel-Netzwerk.

Rijndael überzeugte nicht nur durch Effizienz, sondern auch durch seine mathematisch elegante und einfache Struktur. Manche Kryptographen warteten allerdings auch davor, daß gerade diese einfache Struktur ein Einfallstor für Angreifer sein könnte. Und es gab noch weitere kritische Stimmen.

Geringe Sicherheitsmargen

Vielen Kryptographen erschien insbesondere die Rijndael-Variante für 128-bit Schlüssel mit nur 10 Runden und recht einfacher Rundenfunktion als "recht nahe am Limit". So verwendet der Konkurrent Serpent 32 Runden.

Einfache S-Boxen

Als weiterer Kritikpunkt galt die einfache algebraische Beschreibung der S-Boxen, die ihrerseits die einzige nichtlineare Komponente der Chiffre sind. Dieser Punkt ist im Zusammenhang mit den aktuellen Ergeb-



nissen besonders wichtig. Die S-Boxen sind sogenannte "Knudsen-Nyberg" S-Boxen, die optimalen Schutz gegen differentielle und lineare Kryptanalyse bieten. Diese beiden Techniken waren in der Vergangenheit die wichtigsten und erfolgreichsten Methoden für die Kryptoanalyse von Blockchiffren.

Einfacher Key Schedule

Rijndael verwendet einen sehr einfachen Key Schedule. Kryptographisch schön ist insbesondere die Eigenschaft, dass sich aus Kenntnis irgend eines Rundenschlüssels trivial 128 bit des Verfahrensschlüssel gewinnen lassen. Auch konnte die einfache mathematische Darstellung der Rundenschlüssel bei den unten diskutierten Angriffen verwendet werden. Lucks [Lu00] nutzte eine weitere Schwäche für einen erfolgreichen Angriff gegen Rijndael mit reduzierter Rundenzahl.

Mathematische Struktur

2001 gelang es Ferguson, Schroeppel Whiting [FSW01], die gesamte Chiffre als überraschend einfache geschlossene mathematische Formel darzustellen - in Form einer Art Kettenbruch. Entscheidend dabei war die oben erwähnte einfache algebraische Darstellbarkeit der S-Boxen. Fuller und Millian [FM02] sowie Murphy und Robshaw [MR02] veröffentlichten 2002 weitere interessante Ergebnisse.

Das wohl spektakulärste der neuen Resultate ist jedoch der "eXtended Sparse Linearization" (XSL-Angriff von Courtois und Pieprzyk [CP02], der im folgenden Abschnitt ausführlicher dargestellt wird.

Der XSL-Angriff

Für den Kryptographen zählt jedes Verfahren, das eine Chiffre schneller als mit erschöpfender Schlüsseluche bricht, als "Angriff", unabhängig von der Praktikabilität. Denn auch ein unpraktikabler "Angriff" gilt als Nachweis, dass die Chiffre ihr angestrebtes Sicherheitsziel verfehlt hat. Im Fall der AES-Variante mit maximaler Schlüssellänge (256 bit) braucht die erschöpfende Schlüsseluche im Durchschnitt 2255Verschlüsselungsoperationen. Dies ist der Wert, den es mit einem kryptoanalytischen Angriff zu unterbieten gilt.

Der XSL-Angriff liegt nach Angabe der Autoren im Bereich von 2200Operationen und ist damit definitiv nicht praktikabel. XSL ist eine Weiterentwicklung von XL ("eXtended Linearization"), einer heuristischen Technik, mit der es manchmal gelingt ist, große nicht-lineare Gleichungssysteme effizient zu lösen. XL wurde ursprünglich zur Analyse von Public-Key Kryptosystemen entwickelt. Der Einsatz im Kontext der Secret-Key Kryptographie ist eine Innovation von Courtois und Pieprzyk.

Grob kann die Technik und ihre Anwendung auf Secret-Key Kryptosysteme wie folgt beschrieben werden:

- Beschreibe die Chiffre als überspezifiziertes System quadratischer Gleichungen in GF(2). Mit "überspezifiziert" ist gemeint, dass es mehr Gleichungen als Variablen gibt. Eine derartige Gleichung kann z.B. so aussehen:

$$x_1 + x_2x_3 + x_2x_4 = 1 \pmod{2}.$$

Diese Gleichung besteht aus einem konstanten Term ("1"), einem linearen Term (der Variablen "x1") und zwei quadratischen Termen ("x2x3" und "x2x4").

- Erzeuge durch An-Multiplizieren zusätzliche Gleichungen, um ein noch mehr überspezifiziertes System zu erhalten. Aus der obigen Gleichung kann man durch Multiplizieren mit x1, x2, x3 und x4 die folgenden zusätzlichen Gleichungen erhalten:

$$x_1 + x_1x_2x_3 + x_1x_2x_4 = x_1 \pmod{2},$$

$$x_1x_2 + x_2x_3 + x_2x_4 = x_2 \pmod{2},$$

$$x_1x_3 + x_2x_3 + x_2x_3x_4 = x_3 \pmod{2},$$

$$x_1x_4 + x_2x_3x_4 + x_2x_4 = x_4 \pmod{2}.$$

Man beachte, dass jede erfüllende Variablenbelegung der ursprünglichen Gleichung auch eine erfüllende Belegung für jede der vier neuen Gleichungen ist. Die Umkehrung gilt nicht: So ist $x_1=x_2=x_3=x_4=0$ in unserem Beispiel eine erfüllende Belegung für alle vier zusätzlichen Gleichungen, aber keine für die ursprüngliche Gleichung.

- Linearisiere durch Ersetzung jedes nicht-linearen Term durch eine (Hilfs-)Variable. Zum Beispiel kann man im obigen Beispiel jedes Auftreten des Terms x_2x_3 durch eine Variable $x_{[2,3]}$ ersetzen. Das Gleichungssystem muss so stark überspezifiziert sein, dass es selbst nach dem Linearisierungsschritt immer noch mehr Gleichungen gibt als Variablen, einschließlich der neu-geschaffenen Hilfsvariablen.
- Das so erzeugte große überspezifizierte System von linearen Gleichungen kann man effizient lösen.

Theoretisch können dabei Lösungen gefunden werden, denen keine Lösung des ursprünglichen Gleichungssystems entspricht, z.B. $x_2=x_3=0$ und $x_{[2,3]}=1$. Eine solche (Schein-)Lösung wäre für den Angreifer irrelevant. Aber die Wahrscheinlichkeit, dass dieser Fall eintritt, ist dank der Überspezifiziertheit des linearen Gleichungssystem gering.

Für die meisten Blockchiffren ist dieser Angriff unbrauchbar, da das Gleichungssystem, das man im ersten Schritt erhält, riesig wird. Besäße z.B. der AES statt definierter S-Boxen gänzlich zufällige, wäre dieses Gleichungssystem so groß und komplex, dass die XSL-Methode nicht zu einem brauchbaren Angriff führen würde. Die spezielle Wahl der AES S-Boxen erlaubt es jedoch, ein System mit nur 8.000 quadratischen Gleichungen und sogar nur 1.600 Variablen anzugeben. Das Gleichungssystem ist dazu noch dünn besetzt ("sparse"), das heisst von den insgesamt etwa



1.280.000 möglichen quadratischen Termen tauchen nur relativ wenige überhaupt im Gleichungssystem auf.

Für Kryptographen ist es bemerkenswert, dass eine Erhöhung der Rundenzahl keine exponentielle Steigerung der für den XSL-Angriff erforderlichen Rechenzeit mit sich bringt.

Außer Rijndael scheint auch ein zweiter AES-Finalist verwundbar gegen dieses Angriffstechnik zu sein, nämlich "Serpent" - was die Autoren von Serpent allerdings bezweifeln [SeHo].

Das generelle Problem mit diesem Angriff besteht darin, dass man bisher nicht angeben kann, unter welchen Umständen er zum Erfolg führt. Courtois und Pieprzyk geben in ihrer Arbeit einige notwendige Bedingungen dafür an [CP02]: Unter anderem darf das im zweiten Schritt erzeugte nichtlineare Gleichungssystem nicht zu viele lineare Abhängigkeiten enthalten. Leider ist nicht klar, ob die bekannten notwendigen Bedingungen auch hinreichend sind; darauf weisen auch Courtois und Pieprzyk hin.

Es gibt auch begründete Zweifel, ob der geschilderte Angriff auf den AES tatsächlich funktioniert [M02]. Der wohl prominenteste Zweifler ist Don Coppersmith, einer der Autoren des DES [C02]. Weil der Angriff mit einem Aufwand von 22000 Operationen nicht praktikabel ist, kann man ihn auch schwerlich experimentell verifizieren.

Was nun?

Die Arbeit von Courtois und Pieprzyk ist ohne Zweifel hoch interessant aus theoretischer Sicht. Die spezifische Bedeutung der Frage, ob der XSL-Angriff nun funktioniert oder nicht, und wie aufwändig der Angriff tatsächlich ist, wenn er denn funktioniert, sollte jedoch aus praktischer Sicht nicht überschätzt werden: Der Angriff (Komplexität ≥ 22000) ist im Moment weit davon entfernt, praktikabel zu sein.

Insgesamt sollte man trotzdem beim Einsatz des AES bis auf weiteres eher zurückhaltend sein, unabhängig davon, ob der XSL-Angriff funktioniert oder nicht. Es ist klar, dass Courtois, Pieprzyk und andere Autoren bestimmte Schwächen des AES aufgedeckt haben. Dieses Warnsignal sollte nicht ignoriert werden.

Für Hochsicherheitsanwendungen raten viele Kryptographen, für den Fall, dass bereits Triple-DES verwendet wird und es sich keine Probleme aus der Blockgröße von 64 Bit ergeben, noch einige Jahre mit der Migration zu warten und sich über den aktuellen Forschungsstand (z.B. [W02]) auf dem Laufenden zu halten.

Alternativen

Die Uralt-Chiffre Three-Key Triple-DES bietet für die kommenden Jahre eine Alternative, bei der das Risiko unliebsamer Überraschungen geringer ist. Der bes-

te bekannte Angriff aus Three-Key Triple DES erfordert eine Rechenzeit von etwa 2108 Verschlüsselungsoperationen [Lu98]. Obwohl die Einschätzung über die tatsächliche Sicherheit von Triple-DES selbst unter den Autoren leicht unterschiedlich ist, sprechen noch zwei ganz pragmatische Gründe für Triple-DES: "Nobody will be fired for using Triple-DES" und "Wenn Triple-DES gebrochen wird, dann haben wir ganz andere Probleme".

Leider ist eine Blockgröße von 64 Bit, wie DES und Triple-DES sie bieten, oftmals problematisch. Der Einsatz einer 64-bit Blockchiffre erfordert besondere Sorgfalt seitens des Anwendungsdesigners. Bei 64-bit Blöcken können sich signifikante Sicherheitsprobleme ergeben, wenn etwa 232 Blöcke, was gerade mal 32 GB entspricht, unter dem selben Schlüssel verarbeitet werden (matching ciphertext Angriffe im CBC-Modus, Probleme bei der Verwendung DES-basierter MACs, etc.).

Als DES-basierte und Triple-DES ähnliche 128-Bit-Chiffre mit 128-bit Blöcken gibt es DEAL [Kn98]. DEAL verwendet den DES als Rundenfunktion und setzt auf die Feistel-Struktur, d.h. auf seit langem bekannte, gut untersuchte und bewährte Komponenten. DEAL bietet nicht die Sicherheit, die vom AES erwartet wurde und erhofft wird, und gelangte deshalb mit Recht als AES-Kandidat nicht in den Kreis der Finalisten [Lu99].

Auch die von den Autoren dieses Beitrags entwickelte DEAL-Variante mit einem verbesserten Key Schedule [LW00] hätte beim AES-Wettbewerb, insbesondere wegen der im Vergleich zu den anderen Kandidaten geringeren Geschwindigkeit, sicherlich keine Chance gehabt. Doch das Risiko eines großen kryptanalytischen Durchbruchs ist bei DEAL vergleichsweise geringer als bei einer noch jungen Chiffre.

Abschliessend sei noch mal auf Twofish hingewiesen. Viele Kryptographen halten diesen mit für den sichersten Cipher im Wettbewerb. Zudem war an der Entwicklung von Twofish Dr. David Wagner, inzwischen Prof in Berkeley, massgeblich beteiligt - Itere kennen ihn noch als Netscape-GSM-WEP-...-Hacker!(-)

Literatur

- [C02] Coppersmith, "Re: Impact of Courtois and Pieprzyk results", 19.09.2002, <http://aes.nist.gov/aes/> [1]
- [CP02] Courtois, Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations" Asiacrypt 2002, <http://eprint.iacr.org/2002/044/> [2]
- [DKR97] Daemen, Knudsen, Rijmen, "The block cipher Square", Fast Software Encryption 1997.
- [F+00] Ferguson, Kelsey, Lucks, Schneier, Stay, Wagner, Whiting, "Improved Cryptanalysis of Rijndael", Fast Software Encryption 2000.



- [FM02] Fuller, Millian, "On Linear Redundancy in the AES S-Box", <http://eprint.iacr.org/2002/111/> [3]
- [FSW01] Ferguson, Schroepel, Whiting, "A simple algebraic representation of Rijndael". Draft, 2001/05/16, <http://www.macfergus.com/niels/pubs/rdalgeq.html> [4]
- Lucks, Weis, "How to Make DES-Based Smartcards fit for the 21th Century", Cardis 2000.
- [LW02] Lucks, Weis, "Neue Erkenntnisse zur Sicherheit des Verschlüsselungsstandards AES", DuD 12/2002.
- [M02] Moh, "AES is NOT broken", <http://www.usdsi.com/aes.html> [5]
- [W99] Weis, "AES", Datenschleuder 66, <http://ds.ccc.de/066/aes> [6]
- [W02] Weis, Cryptolabs AES Page, <http://cryptolabs.org/aes/> [7]
- [WL99] Weis, Lucks, "Advanced Encryption Standard", DuD 10/1999.
- [WL00] Weis, Lucks, "Die dritte AES Konferenz in New York", DuD 7/2000.
- [SeHo] Serpent Homepage: <http://www.cl.cam.ac.uk/~rja14/serpent.html> [8]

- [1] <http://aes.nist.gov/aes/>
- [2] <http://eprint.iacr.org/2002/044/>
- [3] <http://eprint.iacr.org/2002/111/>
- [4] <http://www.macfergus.com/niels/pubs/rdalgeq.html>
- [5] <http://www.usdsi.com/aes.html>
- [6] <http://ds.ccc.de/066/aes>
- [7] <http://cryptolabs.org/aes/>
- [8] <http://www.cl.cam.ac.uk/~rja14/serpent.html>

„Es sei Aufgabe der Politik, das Bedrohungsgefühl zu stärken, sagte Merkel am Montag im Anschluss an Sitzungen von Vorstand und Präsidium der CDU in Berlin.“

Angela Merkel, amtierende Vorsitzende der Christlich Demokratischen Union Deutschlands (CDU) in Partei und Fraktion

<http://www.netzeitung.de/servlets/page?section=110&item=225317> am 03.02.2003.

What follows is quoted from the book "Nuremberg Diary", by Gustave Gilbert, who interviewed Goering in prison.

„We got around to the subject of war again and I said that, contrary to his attitude, I did not think that the common people are very thankful for leaders who bring them war and destruction.“

“Why, of course, the people don't want war,” Goering shrugged. “Why would some poor slob on a farm want to risk his life in a war when the best that he can get out of it is to come back to his farm in one piece. Naturally, the common people don't want war; neither in Russia nor in England nor in America, nor for that matter in Germany. That is understood. But, after all, it is the leaders of the country who determine the policy and it is always a simple matter to drag the people along, whether it is a democracy or a fascist dictatorship or a Parliament or a Communist dictatorship.“

“There is one difference,” I pointed out. “In a democracy the people have some say in the matter through their elected representatives, and in the United States only Congress can declare wars.“

“Oh, that is all well and good, but, voice or no voice, the people can always be brought to the bidding of the leaders. That is easy. All you have to do is tell them they are being attacked and denounce the pacifists for lack of patriotism and exposing the country to danger. It works the same way in any country.“

<http://www.heggen.net/government/politics/goering.htm>

inspired by the slieve-quote in the Winter 2002 / 2003 issue of 2600



Hacking biometric systems

von Lisa <lisa@berlin.ccc.de> und Starbug <starbug@berlin.ccc.de>

Biometrische Systeme halten langsam aber sicher Einzug in unser Leben, sei es aus Gründen der Sicherheit oder der Bequemlichkeit. Dass diese Systeme aber nicht so sicher sind, wie von den Herstellern gern behauptet, wissen viele nicht. Dieser Artikel soll das am Beispiel von kapazitiven Fingerabdruckscannern dokumentieren.

Es gibt die unterschiedlichsten Techniken, Fingerabdrücke aufzunehmen. Die am häufigsten genutzte ist die Kapazitive. Der Sensor besteht aus einem Array von kleinen Kondensatoren (ca. 40x40µm). Diese messen die Kapazitätsänderung, die auftritt, wenn man den Finger in Kontakt mit dem Sensor bringt. Das aufgenommene Bild wird dann zur Verarbeitungseinheit übertragen, dort mittels Bildverarbeitungsalgorithmen aufbereitet und die Minutienposition und Ausrichtung extrahiert. Um solche Systeme zu überwinden, braucht man lediglich einen Abdruck des Fingerbildes einer berechtigten (eingelernten) Person.

Da die Haut mit einer schützenden Fettschicht überzogen ist, hinterläßt der Finger praktisch überall Abdrücke seines Rillenmusters, also auch auf dem Sensor selbst. Solche Rückstände bezeichnet man als Latenzabdruck. Gelingt es, diesen zu reaktivieren, kann man dem Rechner vortäuschen, ein berechtigter Nutzer melde sich gerade an. Dazu verändert man die Kapazität der Kondensatoren, auf denen sich die Fettrückstände der Haut befinden.

Eine Möglichkeit, dies zu tun, ist, durch Anhauchen zusätzliche Feuchtigkeit einzubringen - eine andere, feinen Graphitstaub aufzutragen, der an den Rückständen haften bleibt und somit die Änderung der Kapazität bewirkt.

Da die Hersteller um dieses Problem wissen und die Erkennung solch einer Latenzbildreaktivierung relativ einfach zu detektieren ist, sind die meisten Systeme so nicht mehr zu täuschen. Abhilfe schafft hier normales Klebeband. Wird das am Fett haftende Graphitpulver mit Klebeband abgezogen und leicht versetzt wieder aufgelegt, funktionieren die Algorithmen zur Latenzbilderkennung nicht mehr. Auf die gleiche Art und Weise können auch Abdrücke von anderen Gegenständen genommen und dem System als echte Finger vorgespielt werden. Besonders gut eignen sich hierfür glatte Flächen wie z.B. Glas oder Hochglanzpapier.

Aber auch wenn man nur im Besitz eines Fingerabdruckbildes (z.B. aus der Datenbank des BKAs o.äe.) ist, gibt es Möglichkeiten der Überwindung. Hierbei kommen Techniken des Platinenätzens zum Einsatz. Zur Herstellung einer dreidimensionalen Fingerabdruck-

ckatrappe druckt man das Fingerbild in Originalgröße (600 dpi sollten bei Kondensatorlängen von 40µm gerade so ausreichen) mit einem Laserdrucker auf Folie aus. Diese wird auf den Fotolack einer handelsüblichen fotostrukturierbaren Leiterplatte gelegt und mit einer UV Quelle bestrahlt. Nach dem Entwickeln und tzen existiert eine Negativ-3D-Form der Fingerfläche.

Für die Fertigstellung der Fingeratrappe muss die Form noch mit einer möglichst hautähnlichen Substanz ausgefüllt werden. Gelatine scheint sich hierfür besonders gut zu eignen, da Konsistenz und Wasseranteil ähnlich wie bei einem echten Finger sind. Die Attrappe wird dann auf dem Sensor plziert. Wenn man gut gearbeitet hat, wird man vom System als berechtigter Benutzer akzeptiert. Und selbst wenn die Authentifizierung unter Beobachtung stattfindet, sollte es keine Probleme geben, da sich Gelatine zu sehr dünnen Folien verarbeiten läßt, die man fast unsichtbar unter den Finger kleben kann. Fazit ist, dass kapazitive Fingersensoren zwar klein und billig herstellbar sind aber wohl auf absehbare Zeit überwindbar bleiben werden. Brücke zwischen Komfort und Sicherheit - Statement zur Sicherheit von Biometrie-Produkten: Siemens sieht die Biometrie als eine Brücke zwischen Komfort und Sicherheit, wobei die Sicherheit biometrischer Produkte gegenüber PINs und Passwörtern deutlich höher sein kann. In verschiedenen Medien wird über erfolgreiche Angriffe auf biometrische Systeme berichtet. Hierbei handelte es sich um Laborversuche, die mit realen Bedingungen wenig gemein haben. [1]

Nach Redaktionsschluss erreichte uns noch diese Meldung der Autoren: Wie neueste Forschungen ergaben, kann man sich den aufwendigen Schritt des Platinenätzens sparen. Zur Überwindung der kapazitiven Sensoren genügt es schon, den digital vorliegenden Fingerabdruck mit einem Laserdrucker bzw. Kopierer auf eine Folie zu bringen. Da sich die Tonerpartikel auf der Folie anlagern, entsteht so eine dreidimensionale Attrappe. Mit etwas Feuchtigkeit versehen (auch hier hilft wieder Anhauchen) ähnelt sie einem echten Finger so ausreichend, um vom System erkannt zu werden.

[1] <http://www.fingertip.de/index/index.html>



Mini-Mischpult-Inputdevice

von roh <ds-roh@hyte.de>

Mit diesem Artikel soll eine kleine Serie (wieder?) eröffnet werden. Er richtet sich an jeden, der einen LötKolben benutzen kann, ohne sich und Andere zu gefährden ;) Wenn ihr also am Ende dieser Anleitung Ideen, Vorschläge oder auch gleich einen kompletten Artikel (am besten mit Fotos) habt dann mailt mir einfach.

Wie schon im Titel beschrieben, wollen wir uns heute ein kleines Mischpult zum Anschluss an den Computer bauen. Da es eigentlich nur aus 4 Schiebereglern besteht, kann man es natürlich auch ganz anders benutzen, z.B. um eine Scrollbar in einer Text-liste oder den Zoomfaktor in der Lieblings-Grafiksoftware einzustellen... das ist aber alles Softwaresache und daher euch und eurer Phantasie überlassen. In diesem Artikel soll es aber erst einmal um die Vorstellung der Hardware gehen, in den folgenden kommt dann ein Software-Beispiel, mit dem man den normalen Mixer der Soundkarte bedient, an die Reihe.

Als Schnittstelle hab ich den alten gameport ausgesucht, da er am einfachsten zu beschalten ist. Für diejenigen, welche keinen solchen Port mehr am PC/Mac/Sonstwas haben: eine Isakarte oder einen USB-Gameport Konverter kaufen (gibt es so groß wie ein Sub-D15 im Handel).

Aber jetzt zur Schaltung, welche schön einfach gehalten ist, damit sie auch wirklich jeder verwirklichen kann: Man/Frau nimmt 1-4 Schieberegler (ja Drehregler gehen auch, sind aber nicht so hübsch ;)) und schließt diese mit der Widerstandsbahn an die Versorgungsspannung (aus dem Gameport: 5V Gleichspannung) an. Der Abgriff stellt jetzt je nach Reglerstellung eine Spannung von 0-5V zur Verfügung. Diese variable Spannung wird nur an einen der 4 Eingänge des Gameports angeschlossen, die für die Joystickpotis gedacht sind. Mittels 4 Potis haben wir damit den Gameport 'voll', da dieser nur 2 Joysticks mit jeweils 2 Achsen unterstützt und dafür 4 Analogeingänge zur Verfügung stellt.

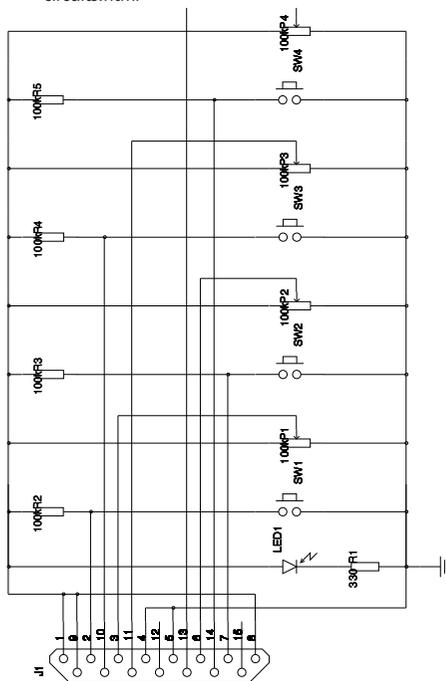
Wer will, kann jetzt noch 4 Schalter oder Taster an die Eingänge, welche für die Buttons des Joystick vorgesehen sind, anschließen. Dafür braucht man dann allerdings, außer den 4 Tastern/Schaltern, noch 4 Widerstände mit ca 100kOhm. Diese schaltet man vom Eingang des jeweiligen Tasters nach 5V und die Taster vom Eingang nach Masse. Zusätzlich habe ich hier einfach noch eine LED mit Vorwiderstand vorgesehen... ist einfach hübsch, so eine Betriebsanzeige.

Zum Testen benutzt man ein beliebiges Programm zum Joysticks kalibrieren. Bei 4 Potis und 4 Tastern müßte man, wenn alles korrekt verschaltet ist, nun mit jedem Poti eine Achse der 2 möglichen Joysticks bewegen können und mit den Tastern oder Schaltern die Buttons 'drücken' können. Die Achsenreihenfolge von P1 zu

P4 müßte X1 Y1 X2 Y2 sein, die Reihenfolge der Taster SW1-SW4 Feuertaste1, dann Feuertaste2 bei Joystick1 und dann bei Joystick2. Passende Testprogramme sind z.B. die im Windows-Treiber eingebaute Kalibrierfunktion für Generic-Joysticks oder jedes andere Kalibrierprogramm.

Weiterführende URLs:

- Pinbelegung des gameports: <http://www.electronic-engineering.ch/microchip/datasheets/pinout/pinout.html#gameport>
- Basteleien am gameport: http://www.epanorama.net/documents/joystick/pc_circuits.html



Die Gedanken sind frei

von sill

“ich kann gar nicht so viel fressen wie ich kotzen moechte. diese idioten.”

athena entered the chat
 athena joined channel 0
 athena he homer, ich muss dir was erzaehlen. Channel -51176.
 athena left channel 0
 homer joined channel -51176
 <homer> was gibts?
 <athena> ich nehme mal an du wirst mich jetzt gleich fuer verrueckt halten...
 <homer> ?
 <athena> dieser wurm von dem ich dir erzaehlte, du weisst schon, “Crunch”...
 <homer> was ist mit dem? ist der fertig? kann ich den code sehen?
 <athena> ja, er ist fertig. und ich glaube ich benenne ihn in “Goettlicher Atem” um.
 <homer> hae? bist du jetzt religioes geworden oder was?
 <athena> nahe dran. ich vermute, dieser wurm war der funke, der bewirkt hat, dass das netz ein bewusstsein entwickelt hat.
 <homer> willst du mich verarschen?
 <athena> ich dachte mir dass du nicht glaubst.
 <homer> wieso sollte ich so eine abgefahrene scheisse glauben?
 <homer> wie aeussert sich denn bitte dieses “bewusstsein”? hats dich beim pr0n klicken erwischt und das bildchen durch ein bild von roland koch ersetzt? *g*
 <athena> sehr witzig. es hat mit mir kommuniziert. emails, defacade webseiten, irc.
 <homer> ich verstehe. haehae. was treibst du dich auch im irc rum? soll ich dir was sagen? da hat dich jemand ordentlich verarscht. du bist irgendeinem spassvogel von einem kiddie aufgesessen.
 <athena> ja, toll. was glaubst du eigentlich, du spinner? ich bin doch keine anfaengerin.
 <homer> ist ja gut. aber das ist eine ziemlich abgefahrene geschichte. du willst mir erzaehlen du hast das erste kuenstliche bewusstsein geschaffen?
 <athena> ich weiss nicht. ich glaube das war zufall. wie mit der ursuppe und den blitzen und den ersten kohlenstoffverbindungen. irgendwas ist jedenfalls passiert. und jetzt betrachtet er mich als seinen schoepfer.
 <homer> er?

<athena> mein suesser. das netz.
 <homer> bwahaha. ohmann, du hast einen an der waffel, echt mal.
 <homer> ich muss los. cu.
 homer left channel -51176
 homer left the chat

5 Jahre später

Internationale Allianz von Regierungen beschliesst umfassende Sperrmassnahmen im Internet zum Schutz der Zivilbevoelkerung dpa/ Bruessel. Eine internationale Allianz, bestehend aus den USA, Kanada, Deutschland, Frankreich, Grossbritannien, Italien, Japan, Australien und Neuseeland beschloss gestern Richtlinien fuer umfassende Sperrmassnahmen im Internet zum Schutz der Zivilbevoelkerung, die unter dem Namen “Towards a Safe World for our people” zusammengefasst wurden. Wie ein Sprecher der Bundesregierung erklarte, sollten damit die Buerger der freien Staaten vor gefaehrlicher staatsfeindlicher, insbesondere islamistischer, rechts- und linksextremistischer Propaganda, sowie moralisch untragbaren Inhalten geschuetzt werden. Wie die Sperrungen genau erreicht werden sollen, ist bislang unklar, eine Task-Force von Experten aus den beteiligten Staaten soll zur Klaerung dieser Frage innerhalb eines halben Jahres Vorschlaege vorlegen. Jochen Bossel, Leiter der Bezirksregierung Darmstadt, der wegen seiner einschlaegigen Erfahrung auf diesem Gebiet in die Task-Force berufen wurde, aeusserte sich dazu nur soweit: ‘Zur sozialen Isolation dieses gefaehrlichen Gedankenguts in der Gesellschaft soll nun auch die voellige netztechnische Isolation im Internet kommen.’

‘Wir erreichen damit nicht nur eine neue Dimension des Jugendschutzes, sondern auch eine ganz neue Qualitaet im Schutz der Personenrechte aller Buerger.’, so Bundeskanzler Gerhard Schroeder, der sich persoendlich an den Verhandlungen beteiligt hatte, da, wie er sagte “in dieser Sache alle, die am Wohle



ihrer Buerger interessiert sind, an einem Strang ziehen" mussten. Die Staaten einigten sich darauf, die Richtlinien innerhalb eines Jahres in nationales Recht umzusetzen. Dies sei genuegend Zeit, Gesetze zu entwerfen und absegnen zu lassen, sowie die dafuer noetigen Verfassungsaenderungen vorzunehmen. Auf den Protest verschiedener Buergerrechtsorganisationen hin, die den massiven Eingriff in die Verfassung und die Unverhaeltnismaessigkeit der Massnahmen bemaengelten, erwiderte ein Sprecher des Weissen Hauses: 'Wir duerfen nicht zulassen, dass die Verfassung uns dabei im Wege steht, unsere Buerger zu schuetzen'."

athena entered the chat

athena joined channel 0

<juhle> "neue Qualitaet im Schutz der
Persoenlichkeitsrechte aller Buerger!"

<athena> tag *

<homer> he athena!!1!

8 users in channel 0

Nickname	From	Idle
boss	p380263d-dip.t-dial	1m
firebody	firebody.datenfrei	5m
gar	nowhere	30s
homer	homer.dyndns.org	20s
juhle	rz2.uni-koeln.de	1m
kaefer	pulse.eeg.de	20m
athena	141.20.193.64	25s
Tolstoi	ipv6.fire.de	15m

<juhle> ich kann gar nicht so viel fressen wie ich kotzen moechte. diese idioten.

<juhle> athena.

<kaefer> athena!

<athena> kaefer! welche freude! :)

<boss> athena!

<firebody> pr0mi3th3u5!

homer he athena, wie gehts?

athena ich mach mir sorgen wegen dieser sperrmassnahmen.

homer tun wir alle

athena nein, du verstehst nicht. bisher hat er nur gespielt, aber ich glaube er fuehlt sich durch diese massnahmen bedroht und hat angefangen, sich zu wehren.

homer scheisse, du hast recht.

homer dieser boersencrash - meinst du das war ... hat er eigentlich einen namen?

athena ja. er nennt sich seit einiger zeit "wintermute". hat wohl irgendwo "neuromancer" gefunden :)

athena zu dem boersencrash: die boersianer sind ja durchgedreht wegen dieser ap-ente.

homer yeah. "EU verhaengt Handelsembargo gegen die USA". Total unklar, wie darauf ueberhaupt jemand reinfallen konnte...

athena Naja, von den Journalisten ist ja auch keiner auf die Idee gekommen, mal in Brussel nachzufragen, die haben erst mal fleissig abgeschrieben und ihre sensationsmeldung rausgehauen. morons.

athena ne ap-ente zu lancieren traue ich ihm auf jeden fall zu. die behoerden suchen jedenfalls gerade intensiv nach dem hacker der das gewesen sein soll: "wintermute". ich glaube die verschwendend ihre zeit.
fg

homer und was machen wir jetzt?

athena keine ahnung. abwarten nehme ich an.

Ihr taten sich in diesen Tagen ganz neue Blickwinkel auf das Thema Sterben und Tod auf. Diese Jemands hatten ohne Zweifel jahrhundertalte Erfahrung darin, Menschen und Tiere zu toeten - qualvoll, schmerzlos, schnell, langsam, einzeln oder in Massen. Aber wie toetet man ein Bewusstsein, das nichts mit dem zu tun hat was es bisher auf der Erde gab? Wintermutes Bewusstsein befand sich nicht auf einem einzelnen Computer irgendwo im Internet - eswardas Internet.

Als letztes tauchten auf den weltgroessten Nachrichtenseiten eine groessere Zahl von Dokumenten auf, die, einmal veroeffentlicht, eine verheerende Wirkung zeigten. Diese Dokumente waren Dossiers, angefullt mit der Dreckwaesche saemtlicher wichtiger Regierungsmitglieder der "Towards a Safe World for our People"-Staaten, die sich an besagter Initiative beteiligt hatten.

Tags darauf fiel aus unerfindlichen Gruenden in saemtlichen groesseren Staedten der Welt der Strom fuer mehrere Stunden aus - wie saemtliche Betreiber von Rechenzentren feststellen mussten, deutlich laenger als die leistungsfahigste USV, die in Benutzung war, ueberbruecken konnte.

Einen weiteren Tag spaeter konnte man in den Zeitungen lesen, dass der mysterioese Hacker "wintermute", der "die Welt in Atem gehalten hatte", bei seiner Festnahme erhebliche Gegenwehr geleistet hatte und von den Sicherheitskraeften in Notwehr erschossen worden war.

athena entered the chat

athena joined channel 0

athena he homer

homer he. hast du die nachrichten gelesen? was meinen sie damit? seit wann kann man netzwerke erschliessen?

athena das war ein fake. sollen sie in die zeitungen schreiben "ki geloescht, menschheit kann wieder in frieden leben"?

homer ?

athena sie haben ihn geloescht. die schweine.

homer aber genutzt hat es ihnen nichts mehr. die dokumente sind draussen, die haelfte der typen, deren widerliche geheimnisse so ans licht gekommen sind haben bereits abgedankt, sich umgebracht oder sind spurlos verschwunden. und von den richtlinien redet niemand mehr. man munkelt dass sich keiner traut. die haben scheinbar immer noch angst vor irgendeinem allmaechtigen hacker der ihnen auch die leichen aus dem keller zerrt.

athena das nuetzt ihm aber nichts mehr.

From: nobody@nowhere.net

To: athena@odem.org

Subject: ... kein Jaeger erschliessen ...

Bewusstsein - Gedanken. Und die Gedanken sind frei...
http://www.radiostation5.org/ -- fuer dich:)

Now playing MPEG stream from "Wintermute - Cracking the Ice.mp3"



SQL-Injection

von Stefan Krecher <stefan@ccc.de>

SQL-Injection ist eine Technik, die wenn man sie einordnen müsste, irgendwo zwischen Cross Site Scripting (XSS) und CGI-Vulnerabilities liegt. Kurz gesagt geht es um die Infiltration von SQL-Queries um deren Verhalten abzuändern. Dieser Artikel soll einen Überblick über unterschiedliche Arten von Angriffen liefern und anhand eines kleinen Beispiels die praktische Anwendung demonstrieren. Als Anschauungsbeispiel müssen Dienste die auf Rechnern der Bezirksregierung Düsseldorf laufen erhalten.

Die Grundlagen

Wie wir alle wissen werden Datenbankinhalte meist mit SQL-Queries abgefragt, aktualisiert, gelöscht bzw. hinzugefügt (SQL = Structured Query Language). Und da das WWW zu einem großen Teil aus dynamisch erzeugten Seiten besteht, liegt es nahe, das gerade bei größeren Angeboten eine Datenbank die Inhalte bereitstellt. Der Zugriff auf die Datenbank kann dann via SQL-Queries stattfinden, die mit Datenbank-APIs von z.B. PHP, Perl, JSP, ASP usw. implementiert werden.

Die generelle Unsicherheit bei solchen Systemen kommt nun dadurch zustande, das die SQL-Queries häufig dynamisch zusammengebastelt werden. So werden z.B. aus Benutzereingaben oder Aufrufen von Scripten Strings erzeugt, die dann unter Umständen ungeprüft an das Datenbank-Managementsystem geschickt werden. Gelingt es diese Strings geschickt zu manipulieren kann man man das Abfrageergebnis beeinflussen, und z.B. auf Inhalte zugreifen, auf die man nicht zugreifen dürfte. Sogar eine Manipulation der Daten ist möglich, die Auswirkungen können verheerend sein.

Unterschiedliche Arten von Angriffen

Gegenstand dieses Artikels sind SQL-Injection-Angriffe, bei denen SQL-Statements erweitert werden und ihr Verhalten sich ändert. Der Vollständigkeit halber will ich eine andere Variante nur kurz anreißen: bei einigen Datenbankmanagementsystemen ist es möglich, in einer Query zwei Statements unterzubringen. Das funktioniert dann, wenn das Semikolon als Trenner zwischen Statements zugelassen ist. Beispiel: der URL `http://webserver/cgi-bin/find.cgi?ID=23` ruft das CGI-Script `find.pl` auf, die Variable `ID` wird mit dem Wert `23` übergeben. Das Script konstruiert eine SQL-Query, setzt diese an die Datenbank ab und präsentiert das Ergebnis. Das SQL-Statement könnte dann z.B. so aussehen: `SELECT NAME FROM PERSONS WHERE ID=23`

Wenn der Aufruf von `find.cgi` nun z.B. nicht aus einem Web-Formular heraus passiert, und deshalb vergessen wurde, der übergebene Parameter durchzuparsen, kommt bei dem Aufruf

```
http://webserver/cgi-bin/find.cgi?ID=23&3BUPDATE%20PERSONS%20SET%20NAME%3D%22malacLypse%22%20WHERE%20ID%3D23
```

der String

```
SELECT NAME FROM PERSONS WHERE ID=23;
UPDATE PERSONS SET NAME="malacLypse" WHERE ID=23
```

heraus. Effektiv werden zwei Statements an die Datenbank abgesetzt: ein `SELECT`- und zusätzlich noch ein `UPDATE`-Statement, das Daten in der Tabelle `PERSONS` manipuliert. Man hat also die Möglichkeit ein beliebiges SQL-Statement auszuführen, Daten zu manipulieren, ggf. je nach Rechtevergabe und mangelnder Admin-Paranoia sogar in Systemtabellen.

Doch nun zu der anderen Variante – hier der Aufruf eines CGI-Scripts, das aus einer Datenbank eine Liste mit allen Personen extrahiert, die den Status `ANGESTELLT` haben:

```
http://webserver/cgi-bin/list.cgi?STATUS='ANGESTELLT'
```

Das SQL-Statement würde so aussehen:

```
SELECT * FROM PERSONEN WHERE STATUS='ANGESTELLT'
```

Durch entsprechendes Anpassen des URL könnte man das SQL-Statement abändern:

```
SELECT * FROM PERSONEN WHERE STATUS='ANGESTELLT' OR NAME LIKE '%x%'
```

...und hätte eine Liste aller Personen aus der Datenbank – unabhängig vom Status, bei denen ein `x` im Namen vorkommt. Häufig läuft der Angriff auf die Manipulation einer `WHERE`-Klausel hinaus. Ein einfaches Beispiel, wie man eine Authentifizierung durch Eingabe von Nutzernamen und Passwort umgehen kann – die URL:

```
http://webserver/cgi-bin/login.cgi?USER=admin&PASS=xyz
```

ruft ein login-Script auf, das überprüft, ob in der Datenbank ein Nutzer mit dem Namen "admin" und dem Passwort "xyz" vorhanden ist (`SELECT COUNT(*) FROM USERES WHERE USER='admin' AND PASS='xyz'`). Wenn die `WHERE`-Bedingung zutrifft und die Anzahl der gefundenen Datensätze `!= 0` ist, wird der Nutzer eingeloggt. Erweitern wir den URL:

```
http://webserver/cgi-bin/login.cgi?USER=admin&PASS=xyz%20OR%201=1
```

ergibt sich als SQL-Statement:

```
SELECT COUNT(*) FROM USERES WHERE USER='admin' AND PASS='xyz' OR 1=1
```



Da wg. 1=1 die WHERE-Klausel immer erfüllt ist, ist das eingeebene Passwort egal – der Nutzer wird eingeloggt. Bei Scripten, die via INSERT-, UPDATE- oder DELETE-Statements Daten einfügen, ändern oder löschen funktioniert das Ganze natürlich analog.

SQL-Injection für Fortgeschrittene

Wenn ein SQL-Statement manipulierbar ist und komplexere Statements möglich sind, hat ein Angreifer im Falle eines SELECT-Statements lesenden Zugriff auf alle Spalten einer Tabelle bzw. sogar auf Daten aus anderen Tabellen. Voraussetzung dafür ist, das ein UNION möglich ist, und das Namen und Typ der Spalten bekannt sind. Da die Konstruktion eines entsprechenden URL im vorigen Abschnitt besprochen wurde, soll hier nur noch die Konstruktion des SQL-Statements untersucht werden. Die Beispiele sind an Tabellen/ Spaltennamen der SAMPLE-Datenbank von IBM DB2 angelehnt und können dort auch nachvollzogen werden.

Mal angenommen wir haben eine Abfrage, die aus einer Tabelle mit dem Namen EMPLOYEE Vor- und Nachnamen gemäß einer vorgegebenen Nummer ausgibt:

```
SELECT FIRSTNAME, LASTNAME, EMPNO FROM EMPLOYEE
WHERE EMPNO=1
```

Der Vergleichswert für EMPNO wird aus einer Formulareingabe übernommen – wenn die Eingabe ungeprüft in das SQL-Statement übernommen wird, können wir folgendes Statement konstruieren:

```
SELECT FIRSTNAME, LASTNAME, EMPNO FROM EMPLOYEE
WHERE EMPNO=123 UNION SELECT 'XYZ', JOB LASTNAME, 123
FROM EMPLOYEE WHERE LASTNAME='MaLaclypse'
```

Hier werden per UNION zwei SELECT-Statements aneinandergehängt und mit der WHERE-Klausel des ersten Teils auch im Ergebnis des zweiten Teils gesucht. Das zweite SELECT liefert als FIRSTNAME immer den String 'XYZ', es wird der Job aus der Spalte JOB abgefragt – die Spalte erhält aber den Namen LASTNAME und in der dritten Spalte steht immer die ganze Zahl 123. Angenommen der Wert 123 für EMPNO ist fiktiv und nicht in der Datenbank vorhanden, liefert obiges Statement in der (Web-) Bildschirmausgabe im Feld für den Nachnamen den Beruf des Angestellten mit dem Nachnamen Malaclypse. Ganz einfach eigentlich. Es ist aber noch mehr möglich, z.B. das Ermitteln von Daten aus einer andern Tabelle. Nehmen wir an es gibt eine Tabelle SALES, in der für jeden Mitarbeiter die getätigten Umsätze gespeichert sind (Spalte SALES). Mit dem SELECT-Statement:

```
SELECT FIRSTNAME, LASTNAME, EMPNO FROM EMPLOYEE WHERE
EMPNO=456 UNION SELECT 'XYZ', CHAR(SALES) LASTNAME, EMP-
NO FROM SALES...
```

wird bei bekannter EMPNO (die Spalte existiert in beiden Tabellen) der Umsatz (SALES) in einen String umgewandelt (Funktion CHAR bei DB2) und in der Spalte LASTNAME ausgegeben.

Die Bezirksregierung Düsseldorf

Die Bezirksregierung Düsseldorf hat eine hübsche Webseite, bei der Seiten aus Datenbankinhalten generiert werden. Die verantwortliche Software mit dem Namen SilverStream fällt zwar offensichtlich einem Relaunch zum Opfer ist aber noch auf dem Server vorhanden und betriebsbereit.

Via CGI werden Datenbankabfragen generiert und von Java-Servlets an eine Oracle-Datenbank weitergereicht. Wenn man nun ein wenig umherklickt gerät man an URLs wie: http://193.159.218.178/cat/SilverStream/Pages/AUFGABEN_ecq.html?query=ANSPRECHPARTNER.ID%3d507 [1], die den Datensatz eines Ansprechpartners bei der Bezirksregierung ausgibt. Angezeigt werden u.a. Name und E-Mail-Adresse des Ansprechpartners. Im obigen Fall wird via CGI die Variable query mit dem Inhalt ANSPRECHPARTNER.ID=507 übergeben – es liegt nahe, das query an ein WHERE-Klausel angehängt wird. Nach einem bißchen herumprobieren stellt man fest, das zwar ein UNION nicht möglich ist, die WHERE-Klausel aber doch angepasst werden kann.

Das SQL-Statement wird im Programm ungefähr so kreiert: SELECT irgendwas FROM irgendwo WHERE \$query. Eine der evtl. mehreren Tabellen, die abgefragt werden heißt ANSPRECHPARTNER, es gibt eine Spalte mit dem Namen ID und eine mit dem Namen EMAIL. Um nun wahlfrei in der Datenbank zu suchen, kann folgender URL konstruiert werden: http://www.bezreg-duesseldorf.nrw.de:8080/cat/SilverStream/Pages/AUFGABEN_ecq.html?query=ANSPRECHPARTNER.EMAIL%20LIKE%20'%25a%25 [2] Das SQL-Statement sieht dann so aus: SELECT irgendwas FROM irgendwo WHERE ANSPRECHPARTNER.EMAIL LIKE '%a%' und zeigt den ersten Ansprechpartner an, der ein "a" in der E-Mail-Adresse hat.

In diesem speziellen Fall ist die Schwäche zwar wahrscheinlich relativ ungefährlich, da nur Daten angezeigt werden, die ohne frei verfügbar sind, ich weiß aber nicht wie das bei anderen Tabellen im System aussieht. Es wurde jedenfalls nicht versucht nicht für die Öffentlichkeit bestimmte Informationen auszuspähen. Die Bezirksregierung wurde vor Erscheinen dieses Artikels informiert.

Wie kann man sich schützen?

Es gelten die allgemeinen Sicherheitshinweise, die auch für die Entwicklung von sicheren CGI-Scripten gelten: alle Eingaben ordentlich durchparsen! Dann sollte im Datenbankmanagementsystem eine vernünftige Rechtevergabe organisiert werden – so sollte der DB-User der Webanwendung nur Zugriff auf bestimmte Tabellen haben, auf keinen Fall jedenfalls Zugriff auf Systemtabellen.

[1] http://193.159.218.178/cat/SilverStream/Pages/AUFGABEN_ecq.html?query=ANSPRECHPARTNER.ID%3d507

[2] http://www.bezreg-duesseldorf.nrw.de:8080/cat/SilverStream/Pages/AUFGABEN_ecq.html?query=ANSPRECHPARTNER.EMAIL%20LIKE%20'%25a%25

[3] <http://online.securityfocus.com/infocus/1644>

[4] <http://www.wiretrip.net/rfp/p/doc.asp?id=42&iface=6>



Offener Brief an info@universal-kopierschutz.de

von Soundjunkie <soundjunkie@firemail.de>

Der folgende offene Brief wurde von "Soundjunkie" in die Newsgroup de.comp.audio gepostet. Die Sicht eines Künstlers auf die Kopierindustrie.

Date: 12 Oct 2002 19:14:52 GMT From: soundjunkie <soundjunkie@firemail.de> Newsgroups: de.comp.audio Subject: Offener Brief an Universal-Kopierschutz.de

Liebe Kopierschuetzer der Universal, die Ihr hier von mir stellvertretend fuer andere Hueter des Rechts am digitalen Klangeigentum angeschrieben werdet: Ihr habt sicherlich nicht erwartet, dass diese Mailadresse fuer Begeisterungsausbrueche genutzt wird. Warum soll man es auch als Fortschritt empfinden, seine Lieblingsband nicht mehr ohne Qualitaetseinbussen im Player seiner Wahl hoeren zu koennen?

Das geschieht selbstverstaendlich in der edlen Absicht, die Interessen Eurer Kuenstler zu schuetzen - eine Tradition der Musikindustrie, fuer die besonders die Majors geschaezt werden. Ich bin geradezu dankbar dafuer, dass der Universal-Kopierschutz ueberhaupt das Abspielen des kostspieligen Silberlings am Computer erlaubt.

Ich weiss, Ihr geht durch harte Zeiten. Umsaetze brechen weg, der Mutterkonzern taumelt. Die Labels werden neu strukturiert und manche haben den Umzug nach Berlin noch nicht verkraftet. Da troestet auch der wunderschoenen Blick ueber die Spree nicht, den Ihr aus Eurem schicken Wasserpalast geniessen koennt. Gestattet mir trotzdem, den Stolz auf Euer hauptstaedisches Firmendomizil mit Euch zu teilen - schliesslich habe ich jahrelang etwas dazugegeben.

Um mit Heine zu sprechen: Ich fuerchte, ich gleite aus dem suessen Gewaesser des Lobes unversehens ins bittere Meer des Tadels. Verbale Entgleisungen bitte ich a priori zu entschuldigen - Musik ist nun mal eine emotionsgeladene Angelegenheit.

Mein Vorwurf lautet, dass das Lamento um CD-Brenner und Internetauschaechsboersen lediglich ein Vorwand ist, um schlussendlich das Recht auf die private Kopie grundsuetzlich auszuhebeln. "Pay-per-listen" - das ist Euer Wunschtraum: Jeder Abspielvorgang kostet ein

paar Microcent und nach vier Wochen muss die Basislizenz erneuert werden. Die Kundenabspeisung funktioniert vertriebskostensenkend ueber das Internet, waehrend der Preis pro Song sich nur unwesentlich vom anteiligen Verkaufspreis eines Longplayers unterscheidet. Die tauben Tekknokids koennen den Frequenzgang verlustbehafteter Kompressionsverfahren sowieso nicht von der ohnehin eingeschaerzten Samplingqualitaet einer CD unterscheiden. Die Kroenung des Ganzen waere dann eine Copyright Taskforce a la Zollfahndung, die spontan Festplatten und mobile Abspielgeraete nach Tracks ohne Wasserzeichen durchkaemmen darf. Soweit die Unterstellung.

In Wirklichkeit ist die Krise der Musikindustrie hausgemacht und hat mit Hobbybrennern und Netztauschern wenig zu tun. Um es kurz zu machen: Ihr produziert seit Jahren zuviel Schrott mit immer kuerzerer Halbwertszeit zu steigenden Kosten. Massengeschmack statt Innovation, Hochglanz statt Inhalt, Banalitaet statt Werte. Die Abspielgehilfen aus Funk und Fernsehen haben ihre Programme stromlinienfoermig an Eure Vorgaben angepasst und werden mit Interviews, Freixemplaren und Backstage-Paessen bei Laune gehalten. Eine inflationaere Schar von Musikmagazinen rezensiert noch den letzten Schund, weil die betreffende Company Anzeigen oder gar das Cover bezahlt hat.

Gleichzeitig werden von Euren mundfertigen, aber von Fachkenntnissen gaenzlich unbelasteten Wichtigtuern Unsummen bei Produktion und Promotion versenkt. Da werden Tagespauschalen an Tonstudios gezahlt, die laengst nicht mehr marktueblich sind. Es werden suendhaft teure Videos gedreht, die keine Station zeigen will. Mit der Giesskanne werden Promopaeckchen uebers Land verspritzt; begleitet von kryptisch-feuilletonistischen Bandinfos, die offensichtlich von Schulerzeitungsredakteuren morgens nach dem Abi-Ball verfasst wurden. Auf grosskotzig gebuchten Tourneen spielen enttaeuschte Kuenstler vor leeren Hal-



len, verdienen sich gierige Catering-Unternehmen eine goldene Nase, rollen Nightliner zu Mondpreisen und tummeln sich zahllose Mitesser mit glänzenden VIP-Kaertchen am Halsband.

Meist laesst sich Gott sei Dank der komplette Kostenblock vom Einkommen der Kuenstler abziehen. Was aber, wenn man den Hungerleidern nichts mehr abziehen kann, weil der ganze Zirkus floppt? Nur drei Prozent aller Acts verdienen fast hundert Prozent des Firmengewinns, wie wir wissen. Ist das ein Marktgesetz oder ein Ausdruck von Unfaehigkeit?

Nun also liegt Eure Antwort auf den ganzen Schlamassel auf meinem Tisch und ich gebe zu, ich bin nicht amuesiert. Meine zentrale Musikstation ist mein Computer. Wozu einen separaten CD-Spieler kaufen, wenn der Rechner das Laufwerk gleich mitbringt? Statt nach dem genuesslichen Auspacken das volle Klangerlebnis ueber meine hart ersparten Edelboxen zu hoeren, werde ich dazu genoetigt, einer unerwuenschten Software Zugriffsrechte auf meinem Computer einzuraeumen. Was dann ertoent, sind herunterkomprimierte Audio-tracks in mp3-Qualitaet. Die originalen Wavefiles sind unzugaeenglich. Der lausig programmierte Software-Player schluckt selbst im Ruhezustand fuefnmal mehr CPU-Leistung als der genuessame Windows-Standard-player. Apple-Computer, bekanntermassen die Lieblingsgeraete von Musikern auf der ganzen Welt, werden erst gar nicht unterstuetzt.

Werde ich da fuer in Zukunft 17 Euro ausgeben? Nein. Ich fuehle mich bestraft von einer Branche, die ihre Hausaufgaben nicht gemacht hat. Die reformunwillig und reaktionaer und deshalb in ihrer jetzigen Form rechtmassig zum Untergang verurteilt ist. Liebe Musikfreunde in den Verwaltungsetagen der Plattenkonzerne: Falls Ihr es noch nicht bemerkt habt - das Zeitalter der Dampfmaschine ist angebrochen. Segelschiffe und Pferdefuhrwerke werden bald nur noch von Nostalgikern benutzt. Sogar das gemeine Volk kann sich eine Fahrt mit der Eisenbahn leisten. Will heissen: Segelflicker und Kutscher werden nicht mehr gebraucht.

Haette es mp3-Files und CD-Brenner nicht gegeben, haette ich meine achtjaehrige Musikkonsum-Abstinenz nicht beendet. Weil formatierte Radioprogramme laengst nicht mehr als Informationsquelle fuer neue Musik dienen, haben Audiofiles und Kopien von Freunden meine Ohren wieder fuer zeitgenoessische Popmusik geoeffnet. In den letzten vier Jahren habe ich so viele Original-CDs angeschafft wie im ganzen vorhergehenden Lebensabschnitt zusammen. Das war harte Arbeit. Meine Faustregel lautet: Eine Scheibe muss mindestens 12 Tracks haben, von denen die Haelfte mehr als zweimal gehoert werden kann. Wenn man dieser Regel folgt, kann man nur eine von zehn CDs kaufen.

Wenn ich eine CD kaufe, stimme ich ab: Ich will meine Favoriten in den Charts sehen, damit andere auf sie

aufmerksam werden. Aus dem gleichen Grund moechte ich Freunden unkompliziert eine Kopie brennen oder meiner Stammkneipe eine Compilation basteln duerfen. Wenn sich dann nur ein Zuhoerer das Original oder ein Konzertticket kauft, hat sich die Muehe gelohnt. Auf die Art und Weise habe ich schon mehr Leute angefixt als jede Streifenbandanzeige im Stadtmagazin. Ich bin ein Ein-Mann-Streetteam im Auftrag des guten Geschmacks. Naja.

Was soll ich in Zukunft tun? Einen CD-Brenner und ein Crackprogramm beschaffen, das den Kopierschutz ignoriert? Dateien grundsaeztlich aus dem Netz ziehen? Den Minidisc-Recorder an den Kopffoererausgang im Plattenladen anschliessen? Neue Scheiben nicht mehr kaufen, alte da fuer kopieren? Das Radioprogramm auf Festplatte mittelschneiden lassen und hinterher sortieren? Was auch immer ich davon waehle, Plattenfirmen und Kuenstler werden mich als zahlen-den Kunden verlieren.

Eine Armee schieisst in die falsche Richtung, weil der Generalstab keinen Schlachtplan hat - hit by friendly fire. So wird aus Kollateralschaeden ein Totalschaden. Die gewerbsmaessigen Piraten in Russland oder Asien, die es immer gegeben hat, werdet Ihr damit nicht beeindrucken. Aber Ihr werdet da fuer sorgen, dass Musik auf Schulhoefen und in Kinderzimmern noch weniger zum Thema wird als ohnehin.

Eure Umsatzeinbrueche sind Zeitzeichen. Waehrend es Euch noch vor kurzem praechtig ging, spuert Ihr nun die Wirkung von Rezession und Verunsicherung. Zusaetzlich konkurrieren Unterhaltungsformen wie Computerspiele und Spass- / Extremsportarten mit dem Musik hoeren. Funktelefone, Tattoos und Markenklamotten kosten Geld. Bildung und Kultur verlottern pisamaessig, die Aufmerksamkeitsspanne der Kids hat sich dramatisch verkuerzt. Drei Jahre Gitarre lernen? No way. Die Musikindustrie hat es vorgemacht: Sampling und Recycling funktionieren praechtig, wozu fuer eigene Ideen schwitzen? Wer als Erwachsener die Charts beobachtet, fuehlt sich an seine Kindheit erinnert. Coverversions von Elvis, den Bee Gees und Joan Jett loesen einander ab; alte Helden wie Groenemeyer retten die EMI vorm Bankrott, Stones und U2 spielen Rekordsummen ein, ein zipfelbaertiger Peter Gabriel spielt allersmilde laechelnd Jungspunde an die Boxenwand. Der Gipfel der Altstoffverwertung ist das aktuelle Cover vom Lagerfeuerheuler "House Of The Rising Sun".

Eine Industrie mit Zukunft? Schrumpft in Wuerde. Soundjunkie P.S. Ihr werdet mir nachsehen, dass ich meinen kleinen Aufsatz in einschlaegigen Internetforen veroeffentliche. Auch ich bin nicht frei von Eitelkeit und halte oeffentliche Aufmerksamkeit fuer den angemessenen Lohn meiner aufgewendeten Zeit.



Dig your tunnel!

von Cryx <cryx@berlin.ccc.de>

Dieser Artikel erhebt nicht den Anspruch IPSec vollständig zu erklären, noch gibt er konkrete Anleitungen wie man sein OS zu patchen hat oder wie man es genau konfiguriert.

Wer sich tiefer mit der Materie auseinandersetzen will, sollte sich die dicken Bücher kaufen, die es inzwischen mehrfach gibt oder nach "ipsec howto" googeln und sich selber ein Setup aufsetzen.

What, what, what, what, what, what, what, what?

IPSec ist eine IP Erweiterung, die einem Verschlüsselung, Authentifizierung, Integrität und Transparenz bietet. Es gibt einem also die Möglichkeit, auf Netzwerkebene IP-Verbindungen zu Verschlüsseln und/oder zu signieren und das völlig transparent für jegliche Applikationen und IP Protokolle.

Die beiden dazu verwendeten IPSec Protokoll sind AH und ESP. Beide IPSec Protokoll können in zwei verschiedenen Arten angewandt werden, die letztlich nur vom Einsatz Zweck abhängen.

Transport Mode (zB. Host-to-Host)

Dieser Mode ist dazu gedacht, in Situationen eingesetzt zu werden, bei denen ein Tunnel nur zwischen zwei kryptographischen Endpunkten bestehen soll. In diesem Mode wird der IPSec Header zwischen IP Header und TCP bzw. UDP Header platziert.

| IP Header | IPSec Header | TCP Header | Data |

Tunnel Mode (Host-to-Net oder Net-to-Net)

Dieser Mode kann in der gleichen Situation eingesetzt werden, wie der Transport Mode, gibt einem aber noch die weitere Möglichkeit, durch zwei kryptographische Endpunkte, zwei nicht kryptographische Endpunkte zu verbinden, die klassische Implementation eines VPN. Dazu wird das ursprüngliche IP Paket von einem IPSec Header umschlossen und ein weiter IP Header voran gestellt. Die kryptographischen Endpunkte werden im äusseren IP Header referenziert, die



nicht kryptographischen Endpunkte im inneren.

| IP Header | IPSec Header | IP Header | TCP Header | Data |

ESP (Encapsulating Security Payload)

ESP ist ein Protokoll Header, der in ein IP Paket eingefügt wird und Authentifizierung, Integrität, Verschlüsselung und antireplay protection (die sequence number ist teil der checksum) bietet. Bsp. für Transport-Mode:

|<--- Encrypted --->||

| IP Header | ESP Header | Protected Data ||

|<----- Authenticated ----->||



AH (Authentication Header)

AH bietet alles, was ESP kann, bis auf die Verschlüsselung. Was das Processing wesentlich schneller macht und es dadurch als die geeignete Wahl für Verbindungen darstellt die zwar keinerlei "geheime" Daten enthalten, bei denen aber Schutz vor Manipulation gewährleistet sein muß (zB. DNS anfragen).

Bsp. für Transport-Mode:

```
-----
|IP Header | AH Header | Protected Data |
-----
|<----- Authenticated ----->|
```

Der Key!

Die Verschlüsselung oder Authentifizierung wird durch einen Schlüssel sichergestellt, der beiden kryptographischen Endpunkten bekannt ist. Er kann auf mehrere Arten ausgetauscht werden kann. Entweder per statischem pre-shared-key für die Encryption, oder per statischem pre-shared-key für die Authentifizierung, mit oder ohne IKE oder auch durch die Verwendung von x509 Zertifikaten oder RSA Schlüsseln. Man kann auch seine Schlüssel im DNS hinterlegen, wenn man dies seinem z.B. bind vertraut ;).

Weiterführende Features

Als weiterführende Features sind noch Compression und Random-padding zu erwähnen. Ersteres ist nicht weiter erklärenswert, trotzdem leider nicht flächendeckend und Plattform unabhängig verbreitet. Dieses gilt für letzteres allerdings auch, ist aber ein weit interessanteres Feature. Random-padding sorgt dafür, daß an jedes per ESP verschlüsselte Paket, ein Stück Daten mit einer zufälligen Länge angehängt und verschlüsselt wird, um so einem externen Beobachter das Erraten des Inhalts auf Grund von statistisch ermittelten Paketlängen zu erschweren. So gesehen bei dniff und ssh, wo man die Kommandos, die durch eine ssh Verbindung gingen, aufgrund der Paketlänge erraten kann.

Warum will man es benutzen?

Sicherheit, Integrität, Authentifizierung, Verbreitung.

Sicherheit

IPSec gibt einem die Möglichkeit sicher zu gehen, daß niemand den Traffic zwischen zwei Punkten im Klartext mitlesen kann. Im Standard ist nur der Cipher DES festgelegt, was niemanden daran hindert, IPSec mit allen anderen Ciphern zu erweitern. So kann man AES oder auch blowfish benutzen und sich selbst ein gutes Gefühl im Bauch verschaffen wenn mal wieder ein Kryptograph einen Cipher auseinander nimmt.

Integrität

IPSec ermöglicht es einem, sicher zu gehen, daß die Daten beim Versenden zwischen zwei Punkten nicht von Dritten manipuliert wurden. Man-In-The-Middle Attacken kann man so recht gut ein Schnippchen schlagen.

Authentifizierung

IP Pakete können signiert werden, so daß der Andere wirklich sicher gehen kann, wer der Absender ist. Die initiale Authentifizierung lässt sich auch als Zugangsregelung für bestimmte Netzbereiche missbrauchen.

Verbreitung

IPSec gibt es inzwischen auf fast allen Plattformen, sowohl auf freien Unices als auch unter bunt-OSSen wie Windows und MacOSX. Sogar auf mobilen Endgeräten sind inzwischen IPSec-Implementation vorhanden.

Unterscheiden tun sich die Implementationen eigentlich nur in ihrer Fähigkeit, verschiedene Cipher zum Verschlüsseln der Daten zu benutzen und die Initiale Authentifizierung zu erledigen. Unter Windows2000/XP gibt es z.B. in der Standard-Implementation nur DES bzw. 3DES während es unter MacOSX ab Version 10.2. neuere Cipher wie AES, den Nachfolgercipher von DES, oder auch blowfish gibt. Für Microsoft Windows gibt es inzwischen zusätzlich zum eingebauten Stack noch etliche kommerzielle Zusatzprodukte, die mehr Features bieten.

Auch die üblichen großen Firmen haben inzwischen in viele ihrer blackbox Hardware einen IPSec-Stack implementiert, so daß man schon sagen kann, daß IPSec als Standard weit verbreitet ist auch wenn man dort auf Grund von mangelndem Einblick nicht sicher von eingebauten Hintertüren ist.

Konfiguration

Die Konfiguration unterscheidet sich natürlich meist erheblich, weswegen sie nicht Bestandteil dieses Artikels sein soll. Es gibt für die entsprechenden Betriebssysteme viele Howtos und Anleitungen oder entsprechenden Support vom Hersteller. Eigentlich sollte inzwischen eine Welle von "IPSec Konfiguration Schulungen" auf uns einbrechen, bisher scheint sich das allerdings in Grenzen zu halten. Dabei tut das vielleicht wirklich mal Not, denn die Konfiguration ist kaum einheitlich zu nennen.

Während bei NetBSD, FreeBSD und MacOSX die Konfiguration des IKE daemon, racoon, gleich aussieht, ist die Konfiguration des isakmpd unter OpenBSD oder des pluto unter Linux total anders. Unter Windows artet die Konfiguration in wildes rumgeklicke im System-Manager aus, was dazu führt das alle Anleitung zur Konfiguration entweder aus tausenden Screens-



hots oder unverständlichen Klick-Anweisungen bestehen. Generell kann man sagen, daß die einfache Konfiguration von IPSec für die User da draußen noch nicht vorhanden ist, allerdings gibt es auch in diese Richtung schon Ansätze.

Einsatzorte

IPSec wird momentan gerne als zusätzlicher Boos-ter für das Buzzword VPN benutzt. Das ist zwar nicht falsch, IPSec ist natürlich auch dafür gedacht, ein VPN aufzubauen, allerdings lässt sich IPSEC noch auf andere Art und Weise einsetzen.

buzz VPN *buzz*

Als klassischer Einsatzort, lassen sich VPNs mittels IPSec relativ einfach aufbauen. Dazu betreibt man IPSec einfach im Tunnel-mode, das bedeutet, daß ein Paket vom internen Netz einfach vollständig, inkl. IP Header encrypted und mit einem neuen IP Header versehen wird. |Header|Data.. | IPSEC processing |Header|[Header|Data.]| Auf der anderen Seite des VPN wird das Paket entschlüsselt und unverschlüsselt weiter an den Zielhost versendet.

IPSec und Wavelan

Da Wavelan von hause aus keine guten Sicherheitsoptionen hat, WEP ist tot und mac-act's sind Unsinn, aber viele Unternehmen oder private Anwender die Freiheit, die Wireless-LAN einem bietet, nicht mehr missen möchten, ist IPSec eine gute Möglichkeit, das Wavelan weiter zu betreiben und trotzdem den Zugang ins interne Netz nur autorisierten Personen zu gewähren.

Auch hier kommt wieder der Tunnel-mode zu Einsatz, nur daß diesmal der Client selber ein Endpunkt der Verbindung ist. Der andere Endpunkt ist die Firewall die mit einem Interface im Wireless-LAN steht. Auf diesem Interface ist nur ESP erlaubt, der Rest kann beruhigt geblockt werden.

Auf dem Wireless Client wird einfach jeder Traffic der aus dem Wireless Interface raus geht, durch den IPSec-Tunnel zum IPSec-Gateway geschickt, welches diesen Traffic dann in die entsprechende Richtung weitertroutet.

Die Identität des Wavelan Users ist so immer gesichert, was einem auch ermöglicht auf dem Gateway einem User z.B. keinen Zugriff auf den internen Unternehmens Webserver zu ermöglichen ihn aber trotzdem den Unternehmens Kühlschrank per Webinterface neu zu bestücken.

Auch nach dem Verlassen des Unternehmen kann ein Mitarbeiter so relativ einfach der Zugriff aufs Firmennetz entzogen werden, indem sein Key gelöscht oder sein Zertifikat revoked wird.

Remote access

Ein Remote Access über IPSec erlaubt es z.B. einem herumreisenden Mitarbeiter, per IPSec Zugriff aufs interne Netz seiner Firma zu bekommen, um beispielsweise auf den Fileserver zuzugreifen.

Die Implementation ist ähnlich der vom Wavelan-Szenario und auch die Möglichkeit gleichen sich.

Auch hier kommt der Tunnel-mode zum Einsatz, die Endpunkte sind in diesem Fall die Unternehmensfirewall, oder ein Extra-Gateway, und der Rechner des Mitarbeiters. Da man in diesem Fall allerdings nicht die IP-Adresse des Client im vornherein bestimmen bzw. wissen kann, wird hier die Authentifizierung nicht mit Hilfe der Source-IP-Adresse sondern einzig und allein per Zertifikat gemacht. Das heisst: ein Zertifikat ist nicht an eine bestimmte Source-IP-Adresse gebunden sondern die Authentifizierung kann von jeder beliebigen IP-Adresse erfolgen.

Stolperfalle sind hier meistens die Firewall in anderen Netzen, die versuchen, IPSec Paket mit NAT zu versehen und dabei die beinhaltete Checksum ungültig machen.

tunnel(tunnel(tunnel))

Eine unkonventionelle Methode IPSec einzusetzen, ist das Tunneln von IPv4 oder IPv6 Netzen zu Standorten, die nur über dynamisch vergebene IP-Adressen Zugang zum Internet haben, zB. TDSL. Über ein Zertifikat, welches nicht an eine bestimmte IP-Adresse gebunden ist wird ein IPSec-tunnel zu einem Tunnel-Server aufgebaut, der durch diesen Tunnel entweder IPv4 direkt oder IPv6 durch einen GRE oder SIT tunnel getunnelt wird.

My name is...

Eine sicherlich sehr sinnvolle Anwendung von IPSec ist die Authentifizierung von DNS requests, bzw. derer die darauf antworten. Hier sind mehrere Arbeitsweisen denkbar. Einmal ein Transport-Mode Setup welches z.B. dem Secondary-Nameserver sichergehen läßt, daß es seine Zone-File Updates vom richtigen Master-Nameserver bekommt. Oder ein Tunnel-Mode-Setup, das vielen Clients hinter einem IPSec-Router ermöglicht, auch wirklich den beim Provider befindlichen Nameserver zu befragen und nicht etwa den inoffiziellen Backup Nameserver von Mr.X.

hnlich lassen sich SMTP Server oder HTTP Proxys untereinander verbinden, wobei man dabei noch Encryption hinzuschalten möchte.

Streaming

Man könnte IPSec-Tunnel auch dazu nutzen, das Streamen von rechtlich eher nicht unkritischen Audio oder Video Daten, zu verschleiern. Zumindest der Beweis, woher die Daten ursprünglich kamen, könnte so



schwerer zu erbringen sein. Hierbei könnten Scheintunnel und Random-padding behilflich sein. Dabei sollte man natürlich sichergehen, daß die Keys zur Verschlüsselung der Daten nicht später einsehbar sind.

mounten

Auch zum Sichern von Filesharing Protokollen wie NFS oder SMB läßt sich IPSec nutzen, eine transport-mode Verbindung zwischen Client und Server kann hier vor im Klartext herumfliegenden Daten schützen. In diesem Fall muß man sich allerdings im Klaren sein, das die Performance hier nicht überragend sein wird.

Performance

Die Hardwareanforderungen von IPSec werden natürlich vom Einsatzort und dem verwendeten Cipher bestimmt. 3DES ist natürlich langsamer als zB. AES oder blowfish.

Ein dynip-IPv6 tunnel z.B. der eh nur über eine 144kbit/s Leitung durchgeht, braucht nicht viel Rechenleistung auf der Tunnel-Server Seite. Auch ein bis zwei Wavelan-Clients die über IPSec mit AES oder blowfish ins interne Netz kommen, brauchen nicht viel Hardware, da reicht auch schon mal ein Pentium 200.

Wer allerdings 1000 Außenstellen mit VPN anbinden will und z.B. nur 3DES benutzen möchte, sollte sich entweder nach Hardwarelösungen von den üblichen Verdächtigen wie Cisco, Nokia etc. umsehen, oder einen schnellen Server mit Hardware-acceleration einsetzen der auch entsprechende Netzwerkklass gleichzeitig trägt. Auch eine übersichtliche Möglichkeit zur Konfiguration tut der Sicherheit keinen Abbruch.

Grenzen der Sicherheit

Die Verschlüsselung mit IPSec ist natürlich nur so stark wie der gewählte Cipher, allerdings kann man über das System IPSec schon behaupten, daß es recht ordentlich durchdacht wurde. Von Fehlern oder Backdoors in der Implementation einmal abgesehen. Auch hilft IPSec nicht gegen schlecht abgesicherte Tunnelendpunkte. Ein System ist eben nur so sicher wie sein schwächstes Glied.

Auch bei IPSec sollte man sich immer fragen, ob die Daten die darüber geschickt werden sollen, nicht doch zu vertraulich sind, um überhaupt in digitaler Form zu bestehen.

Schlusswort

Zum Schuss bleibt noch anzumerken, daß hoffentlich mit IPv6 die Einsatzweite von IPSec zunehmen wird, allein schon deswegen, weil viele auf IPv6 aufbauende Protokolle (zB. BGP-4) vollständig Authentifizierung auf IPSec auslagern. Auch werden lästige Probleme wie NAT (einige IP-Stacks versuchen mit IPSec versehene

IP Pakete mit NAT zu befangern, was der checksum gar nicht gut bekommt) und dynip einfach verschwinden.

Auf jeden Fall kann uns IPSec jetzt schon in Zeiten von TKÜV und ähnlicher Dinge helfen, die schon geschehenen Einschränkungen zu umgehen.

Vielleicht können wir ja bald mit unseren mobilen Endgeräten über IPv6 und IPSec den Füllstand unseres heimischen Kühlschranks überprüfen ohne, daß die ISPs dazwischen die Daten an die nächste Supermarkt Kette verkaufen.

Bis dahin: hoffen wir, daß niemand das Filtern von ESP beschliesst.

URLS

- IPsecEEE802.11 howto [<http://wiki.ash.de/cgi-bin/wiki.pl?IPsecEEE802.11>] [1]
- Electrolux IPv6 enabled Fridge [<http://www.electrolux.com/screenfridge/>] [2]
- NetBSD IPSec FAQ [<http://www.netbsd.org/Documentation/network/ipsec/>] [3]
- OpenBSD using IPSec [<http://www.openbsd.org/faq/faq13.html>] [4]
- Linux FreeS/WAN [<http://www.freeswan.org/>] [5]
- Seminarfacherbeit: Sicherere latenzarme Kommunikationswege mit IPsec von Thomas Walpuski [<http://bender.thinker.de/~thomas/IPsec/>] [6]
- google?ipsec howto [<http://www.google.com/>] [7]
- ISAKMPD using X509 certificates [8]

[1] <http://wiki.ash.de/cgi-bin/wiki.pl?IPsecEEE802.11>

[2] <http://www.electrolux.com/screenfridge/>

[3] <http://www.netbsd.org/Documentation/network/ipsec/>

[4] <http://www.openbsd.org/faq/faq13.html>

[5] <http://www.freeswan.org/>

[6] <http://bender.thinker.de/~thomas/IPsec/>

[7] <http://www.google.com/>

[8] <http://mirror.huxley.org.ar/ipsec/isakmpd.htm>



Virtual Private Networks (VPN)

von DocX <docx@duesseldorf.ccc.de>

Was ist ein VPN?

Ein VPN ist eine Netzwerkverbindung, die durch ein anderes Netzwerk geroutet wird. Diese Verbindung wird auch Tunnel genannt. Warum das? Es geht darum, daß ein Rechner, der weit weg von uns ist und der nur über ein fremdes Netz (d.h. das Internet) mit uns verbunden ist, in unser eigenes Netz integriert werden soll. Dies zu tun hat vier Gründe:

- Der Client hat eine IP-Adresse innerhalb des lokalen Netzes
- Der Client ist "virtuell" innerhalb unserer Firewall angesiedelt
- Der Aufbau der VPN-Verbindung kann authentifiziert werden
- Die Daten, die über den Tunnel laufen, können verschlüsselt wer

Welches Protokoll benutze ich?

Es gibt verschiedene Protokolle, um VPNs zu realisieren:

- Secure Shell Tunnel - Die vermeintlich einfachste Lösung ist der Aufbau eines Secure Shell Tunnel mit SSH. Sie hat jedoch Ihre Nachteile bei verbindungslosen Protokollen.
- VPN mit PPTP - Benutzt ein Protokoll, das vor allem von Microsoft benutzt wurde und sich zum Verbindungsaufbau z.B. mit Win98-Rechnern eignet, hat aber einen Sicherheitsmangel.
- VPN mit IPSec - Wahrscheinlich die beste Lösung, außerdem Teil des IPV6-Standards und damit das Protokoll der Zukunft, leider auch kompliziert zu installieren (benötigt einen Kernelpatch).

Sicherheit

Sicherheitsfanatiker sollten sich statt für PPTP eher für IPSec entscheiden. Probleme mit PPTP können aber soweit ich gelesen habe, nur auftreten, wenn ein Hacker die ersten beiden Pakete der Kommunikation abfangen kann. (Es gibt da z.B. einen Fall an einer Uni, an der ein Funknetz betrieben wurde.)

Die Verschlüsselung bei PPTP wird nicht von PPTP erledigt, sondern von PPP, das letztlich die Verbindung erzeugt. Also kann man die für PPP möglichen Verschlüsselungsalgorithmen benutzen. (Diese sind allerdings aufgrund von Exportbeschränkungen und Lizenzproblemen im Standard-pppd eingewschränkt. Man sollte eine gepatchte Version benutzen.)

Das eigentliche Sicherheits-Problem dürfte jedoch weniger die Authentifizierung des Clients sein als vielmehr die Tatsache, daß ich einen Client in mein Netz lasse, den ich unter Umständen nicht so unter Kontrolle habe wie meine eigenen Rechner. Wenn sich z.B. ein Außendienstler ins VPN einloggt, um seine interne Mail abzuholen und auf dem Intranet-Webserver zu sehen, was es neues gibt, habe ich plötzlich einen Rechner im Netz, auf dem gestern abend noch lustig ohne Firewall im Internet gesurft wurde, auf dem alle möglichen aus dem Netz geholten Spiele ausprobiert wurden und auf dem weisstgottwieviele Viren und Trojaner sitzen könnten. Also ist bei der Firewall darauf zu achten, daß die VPN-Verbindungen immer als unsichere Hosts gelten und bei Diensten, die der Außendienst braucht (z.B. Mailserver) alle Vorkehrungen gegen Mißbrauch getroffen werden.

VPN mit SSH

Zum Aufbau eines Virtual Private Network kann auch SSH benutzt werden. Diese Lösung ist einfach und schnell und man benötigt lediglich zwei Linux-Maschinen, auf denen SSH installiert ist.

Vorteil

Ein Vorteil ist wohl der leichte und schnelle Aufbau der Netzwerkverbindung.

Nachteil

Dieser Tunnel hat jedoch einen entscheidenden Nachteil: Er setzt auf dem bestehenden SSH-Protokoll auf, das auf einer TCP-Verbindung basiert. Das bedeutet, daß TCP-typisch (und im Gegensatz z.B. zum UDP-Protokoll) sowohl der vollständige Erhalt als auch die Reihenfolge der Pakete bei der Übertragung garantiert wird. Falls also mal ein einzelnes Paket in den Wirren des Internet verloren geht, steht das gesamte VPN so lange, bis die beiden SSH-Programme sich wieder synchronisiert haben. Wenn wir ein verbindungsloses Protokoll (wie GRE beim VPN mit PPTP oder ESP



bei VPN mit IPsec) benutzen, bewirkt ein verschwundenes Datenpaket nur, daß genau dieses eine Datenpaket weg ist. Das darüberliegende Protokoll, das das VPN benutzt, kann sich dann wie üblich überlegen, ob es das Paket neu haben will (z.B. bei TCP) oder verwirft (z.B. bei Streamingdaten). Andere Datenpakete und Verbindungen über das VPN werden so lange jedoch nicht gebremst. Ein weiterer Nachteil ist, daß man auf Plattformen angewiesen ist, die ssh unterstützen, d.h. ein Aufbau mit einer Windows-Gegenstation könnte problematisch werden. Ggf. würde ich es jedoch mal mit dem freien Windows-SSH-Programm Putty [1] versuchen.

VPN mit PPTP

PPTP ist ein Protokoll für ein Virtual Private Network, das unter anderem schon lange von Microsoft benutzt wird. Daher ist es relativ einfach, VPN-Verbindungen z.B. zu älteren Win98-Rechnern aufzunehmen.

Was brauchen wir?

Es gibt verschiedene Protokolle, um VPNs zu realisieren. Hiervon habe ich PPTP ausgewählt. Dieses Protokoll soll nicht das allersicherste sein, dürfte aber für den normalen Gebrauch genügen. Es hat dabei den Vorteil, daß ein PPTP-Client serienmäßig bei Windows dabei ist, sodaß auch ein plattformübergreifendes VPN-Netz denkbar ist.

Unter Debian gibt es zwei Pakete zu dem Thema:

- ptp-linux - Dieses Paket enthält ein Client-Programm, das die ppp-Verbindung über den Tunnel aufbaut.
- pptpd - Dies ist ein Daemon, der als Server auf eingehende Verbindungen wartet.

Vorab-Überlegungen

Vorab sollte man sich überlegen, wie das gesamte entstehende Netz nachher aussehen soll. Im Prinzip ist der VPN-Server ein Router, der Verbindungen zu Sub-Netzen herstellt. Dabei ist es durchaus möglich, mehrere verschiedene Clients gleichzeitig zu haben. Im Grunde genommen ist das vergleichbar mit einem Dialin-Server, der ganz viele Eingangsleitungen mit Modems hat. Da alle Clients normalerweise sicherheitstechnisch der gleichen Klasse zuzuordnen sind, sollte man sie in ein eigenes Subnetz packen. Dieses kann man dann z.B. in einer Firewall oder bei anderen Zugriffsbeschränkungen benutzen. Wenn sich ein Client per ppp anmeldet, bekommt er normalerweise eine Nummer aus einem Nummernpool zugewiesen. Man kann jedoch über die Authentifizierung in der Datei /etc/ppp/chap-secrets auch dafür sorgen, daß ein bestimmter Benutzer immer

die Gleiche Nummer bekommt. Dies ist aus Sicherheitsgründen immer zu empfehlen. Außerdem kann man so auch feste Nemeserver-Einträge für die Clients machen. Es ist übrigens möglich, daß die verschiedenen PPP-Interfaces, die im Server erzeugt werden, alle die gleiche IP-Nummer haben. Man braucht also nicht für jede Verbindung zwei IP-Adressen.

Also könnte man in einem gedachten Netzwerk folgenden Plan machen:

- 192.168.1.x - normales, internes Netz
- 192.168.2.x - interne DMZ (demilitarisierte Zone)
- 192.168.3.1 - PPP-Interface des Servers
- 192.168.3.2 - VPN-Client test1
- 192.168.3.3 - VPN-Client test2
- 192.168.3.4-254 - ggf. Nummernpool für Clients ohne feste Nummer

Dann stellt sich die Frage, auf welchem Rechner im Netz man den VPN-Server installiert. Steht hierzu kein eigener, dedizierter Server zur Verfügung, so sollte dringend davon abgeraten werden, "irgendwo" auf einem anderen Server oder einem Client diese zusätzlichen Netzwerkverbindungen zu erstellen. Dadurch wird nur das Routing und damit auch das Sicherheitskonzept unübersichtlicher. Am besten sind die VPN-Interfaces da untergebracht, wo auch ansonsten das Routing erledigt wird, also z.B. am Router zwischen internem Netz und DMZ bzw. Internet. Die Firewall-Einstellungen sollten dann im Prinzip denen der DMZ entsprechen. Man sollte die VPN-Clients auch nicht direkt mit einem Server in der DMZ verbinden. Dann läuft man Gefahr, daß bei einer "Übernahme" der DMZ der gesamte Verkehr mit den VPN-Clients in die falschen Hände gerät.

Server-Konfiguration

Nach Installation des Paketes muss zuerst die Konfigurationsdatei von pptpd erweitert werden. hier habe ich folgendes eingetragen:

- localip 192.168.3.1
- remoteip 192.168.3.2-254

Die angegebenen Remote-IPs werden nur verwendet, wenn in der Datei pap-secrets keine Adresse angegeben ist.

Die eigentliche Verbindung mit Authentifizierung etc. ist eine normale PPP-Verbindung. Deshalb gelten hierfür die normalen ppp-Optionen. Diese stehen global in der Datei / etc/ppp/options und speziell für die pptpd-Verbindung in /etc/ppp/pptpd-options (diese zweite Datei wird pppd auf der Kommandozeile übergeben.)



. Auf jeden Fall kann man keine sicherheitsrelevanten Einstellungen, die in /etc/ppp/options stehen, nachträglich entschärfen. Wenn man also testweise erstmal ohne Authentifizierung arbeiten will, muss man den Eintrag "auth" in dieser Datei auskommentieren. (nicht vergessen, das später wieder einzuschalten!)

Nun zur Datei /etc/ppp/pptpd-options, in der die eigentlichen ppp-Optionen stehen. Für einen ersten Test kann man diese auf folgenden Stand bringen. Achtung! Hier ist jede Authentifizierung und/oder Verschlüsselung abgeschaltet.

```
debug name pptpgate ms-dns 192.168.1.1 # ggf.
anpassen auf eigenen Nameserver netmask 255.255.255.0
nodefaultroute
```

Dann kann man den PPTP-Server neu starten mit:

```
/etc/init.d/pptpd restart
```

Jetzt müsste man eine Testverbindung aufbauen können. Wenn man das geschafft hat, kann man sich daran machen, die Sache sicherer zu machen. Hierzu sollte die Datei /etc/ppp/pptpd-options so aussehen:

```
test1 pptpgate passwort1 192.168.3.2 test2 pptpgate
passwort2 192.168.3.3
```

Jetzt nochmal den pptpd neu gestartet und ab jetzt kann keiner mehr ohne Passwort eine Verbindung aufbauen. Die Clients bekommen automatisch die angegebene IP-Nummer, sodaß man sie sogar in seinen Nameserver aufnehmen kann. Außerdem lassen Sie sich so auch von Diensten im Netz über diese Nummer identifizieren und auseinanderhalten.

Client-Konfiguration

Wenn man das Paket installiert hat, hat man eigentlich schon alles geschafft. Man muss ebenfalls /etc/ppp/options ändern, wenn man vom Server keine Authentifizierung verlangen will. Wie gesagt sollte man später überlegen, das wieder zurückzunehmen!

Jetzt startet man mit

```
pptp server-name.domain.bla
```

die Verbindung. Fertig! Auf beiden Seiten ist ein pppx-Device dazugekommen und der Tunnel steht.

Leider geht das mit dem Debian-pptp-Paket nicht ganz so einfach. Hier wird offensichtlich ein Dateiname bei den Pseudo-TTYs verdreht.

Man kann weitere pppd-Parameter in der Kommandozeile angeben. Insbesondere kann man diese Parameter auch in einer peers-Datei speichern. Sind die Einstellungen in /etc/ppp/peers/vpn2home, so kann man den Aufruf so machen:

```
pptp server-name.domain.bla call vpn2home
```

In dieser Datei kann man dann z.B. mit name den Login-Namen angeben. Man kann auch ein ip-up-Skript angeben, das ggf. den Nameserver, Routing zum internen Netz, etc. richtig einstellt. Der Nameserver wird übrigens nicht automatisch eingestellt, auch wenn

man usepeerdns angibt, da ja bereits ein Nameserver im System eingetragen ist (ohne den würde man den Zielhost ja gar nicht finden). Also entweder die wichtigen Sachen nach /etc/hosts oder ein Startskript, das /etc/resolv.conf anpasst.

Interessant könnte auch sein, bei der Haupt-Internet-Verbindung des Clients ein ip-up-Skript einzurichten, das dann immer sofort und automatisch ein VPN aufbaut. Wen sowas interessiert, kann mich gerne fragen: Bei mir läuft's. :-)

Die häufigsten Probleme, von denen berichtet wird, sind nun übriges Routing-Probleme. Dies hängt vor allem damit zusammen, daß man jetzt im Prinzip zwei Routen zum Zielsystem hat. Eine direkte und eine durch den Tunnel. Man sollte sich also bei Schwierigkeiten genau überlegen, welches Paket wann wohin läuft. Dies wird insbesondere interessant, wenn ich nicht die direkte Gegenstelle der VPN-Verbindung anspreche, sondern hinter dem Tunnel durch den PPTP-Server noch weitergeroutet werden muss.

Windows-Client-Konfiguration

Zuerstmal muss das Device für VPN installiert werden. Dazu geht man so vor:

- Start / Systemsteuerung
- Software anwählen
- Registerkarte "Windows Setup"
- Komponente "Verbindungen" auswählen
- Komponente "Virtuelles Privates Netzwerk" anwählen (Häkchen machen)
- Jetzt zweimal auf OK klicken

Jetzt ist die benötigte Software installiert. Als nächstes muss eine Verbindung eingerichtet werden. Hierzu geht man folgendermassen vor:

- Start / Programme / Zubehör / Kommunikation / DFÜ-Netzwerk
- "Neue Verbindung einrichten" anklicken
- Als Namen gibt man eine Bezeichnung an, unter der man die Verbindung nachher auswählen kann
- Als Gerät muss "Microsoft VPN Adapter" ausgewählt werden
- Als Hostnamen gibt man den Namen oder die IP-Adresse des Servers an, zu dem man Kontakt aufnehmen will

Nach der Grundeinrichtung hat man einen Eintrag im Ordner der DFÜ-Verbindungen. Zu den restlichen Einstellungen klickt man jetzt auf diesen mit der rechten Maustaste und geht im erscheinenden Kontextmenü auf "Einstellungen". Auf der zweiten Registerkarte muss man jetzt noch ein paar Kästchen beglücken:

- Netzwerkverbindung herstellen sollte ausgeschaltet sein. Windows versucht sonst, über das VPN mit einem NT-Domänencontroller Verbindung aufzunehmen, der normalerweise



nicht da ist, wenn die Gegenstation ein Linux-Rechner ist (und Samba nicht speziell dafür konfiguriert ist). Das dauert beim Verbindungsaufbau eine ganze Zeit.

- Passwort-Verschlüsselung sollte eingeschaltet werden. Das kann nie schaden.
- Datenkomprimierung kann eingeschaltet werden, ist bei mir offensichtlich aber nie benutzt worden. Da scheinen sich Linux und Windows nicht auf ein Kompressionsverfahren einigen zu können.
- Die Verschlüsselung funktioniert nicht so einfach (siehe unten), also ausschalten.
- Die Protokolle können bis auf TCP/IP abgeschaltet werden

Auf die Seite mit den TCP/IP-Einstellungen kann man auch mal klicken. Normalerweise ist dort nichts zu ändern. Eventuell ist die Frage interessant, ob das VPN zur Default-Route werden soll. Falls auf dem Client während der Verbindung z.B. gesurft wird, wird das alles über den VPN-Server geroutet.

In der Dokumentation zum pptp-Server stand, daß man, um Passworte und Verschlüsselung mit Windows-Clients zu benutzen, den pptd patchen muss. Passworte (auch verschlüsselt) klappen bei mir jedoch. Vielleicht habe ich ja eine neuere pptd-Version. Verschlüsselung konnte ich allerdings nicht einschalten. Dazu muss man dann ggf. eine entsprechend gepatchte pptd-Version herstellen.

Dynamische IP beim Server

Bleibt noch die Frage, was ich beim Client als Hostnamen des Servers angebe, wenn ich mich z.B. übers Internet in das heimische Netzwerk einwählen will, der heimische Rechner aber über eine preiswerte Flatrate am Netz hängt und daher keine feste IP-Adresse geschweige denn einen Domain-Namen hat.

Die primitivste Lösung ist, bei jedem Verbindungsaufbau automatisch eine Webseite mit der Mitteilung "Jetzt habe ich die IP-Adresse a.b.c.d" auf einen bestehenden Webserver hochzuladen. Dieser Webserver kann von einem Provider für Webspaces wie z.B. tripod, freenet, etc. sein und hat dann eine offizielle, mit DNS zugängliche Adresse. Der potentielle Client nimmt also seinen Webbrowser, öffnet die Seite people.freenet.de/~benutzer, sieht dort die Adresse und trägt sie z.B. in seinen Browser ein, um auf den eigentlichen Server zu kommen.

Eine etwas schönere Lösung ist, direkt eine HTML-Umleitungs-Seite anzulegen. Dann hat man sich einen lästigen Schritt gespart. Nachteil des Verfahrens: Es funktioniert nur für HTML-Seiten. Andere Dienste lassen sich so nicht umlenken.

Und jetzt kommen wir zur schönsten Lösung: Was wäre, wenn es spezielle DNS-Server gäbe, die man bei jedem Verbindungsaufbau permanent umstellen könnte? Normalerweise steht dem das TTL (Time To Live)-

Feld im DNS-Eintrag entgegen, der besagt, daß der Eintrag für z.B. eine Woche gültig ist. Dadurch wird der Eintrag von allen anderen Nameservern im Internet gecached. Wenn man später auf diesen Domainnamen zugreift, bekommt man also die alte Adresse. Nun könnte man theoretisch das TTL-Feld auf z.B. 5 Minuten stellen. Würden das alle machen, würde das ganze DNS-System ewig langsam werden, weil nichts mehr gecached wird, aber für ein paar dynamische IPs sollte das gehen.

Jetzt die gute Nachricht: Es gibt Leute, die solche Nameserver [2],[3] anbieten. Man kann eine Unterdomain der Hauptdomain des Anbieters für sich reservieren und ein kleines Programm, das beim Verbindungsaufbau gestartet wird, sorgt dafür, daß die IP-Adresse richtig eingetragen wird.

VPN mit IPSec

IPSec ist ein Protokoll zum Aufbau eines Virtual Private Network. Es dürfte im Moment die beste Wahl sein, wenn man ein VPN neu aufbaut, da es Teil des kommenden IPv6-Standards sein wird.

Free S/WAN

IDie am besten gepflegte Linux-Implementation von IPSec ist Free S/WAN. Dieses wird auch z.B. von Suse Linux benutzt und es gibt entsprechende Debian-Pakete. Aufgrund der Exportbeschränkungen der USA für Verschlüsselungstechnologien ist Free S/WAN nicht im Linux-Kernel und im normalen Debian-Baum integriert, sondern erfordert die Einbindung des non-us-Debian-Zweiges sowie eine Kernel-Kompilierung.

Installation

Zur Zeit sind die dazu benötigten Debian-Pakete nur in der unstable-Distribution zu finden. Ich habe folgende Files einfach mit wget heruntergeladen und dann mit dpkg -i ... installiert:

- http://ftp.de.debian.org/debian-non-US/pool/non-US/main/f/freeswan/freeswan_1.96-1.2_i386.deb
- http://ftp.de.debian.org/debian-non-US/pool/non-US/main/f/freeswan/kernel-patch-freeswan_1.96-1.2_all.deb

Danach muss der Kernel neu gebaut werden. Wenn der mit Free S/WAN läuft, erkennt man das an entsprechenden Meldungen beim hochfahren.

Außerdem muss in der Datei `/etc/network/options` die Option "spoofprotect" auf "no" gesetzt werden. Sonst beschwert sich ipsec beim hochfahren, dass seine KLIPS-Komponente nicht mit Devices arbeitet, die "route filtering" eingeschaltet haben. (Da spoof protect an sich kein schlechter Gedanke ist, sollte man dieser Frage später nochmal nachgehen.)



Konfiguration

Zuerstmal sollte hier gesagt werden, dass die Dokumentation auf der Webseite sehr ausführlich und umfangreich ist und eigentlich alles erklärt, wenn man nur weiss wo. Gerade weil sie so umfangreich ist, habe ich aber doch lange gebraucht, bis meine Konfiguration so stand, wie sie sollte.

Damit es nicht langweilig wird, habe ich hier einen Fall als Beispiel genommen, den es laut der offiziellen Dokumentation garnicht gibt. :-)

- Eine Verbindung zwischen zwei Rechnern mit fester IP-Adresse ist relativ schnell eingerichtet, wenn man das Grundprinzip verstanden hat. Wichtig im Vergleich zu anderen VPN-Systemen ist die Tatsache, daß nicht eine neue virtuelle Verbindung erzeugt wird, die an beiden Enden jeweils ein neues Interface hat, sondern das neue Interface ipsec0 hat die gleiche IP-Adresse wie das darunterliegende (z.B. ppp0). Die Entscheidung, was wodurch geroutet wird, fällt in der Routingtabelle bzw. im Kernel-Routingcode (den wir ja oben gepatcht haben).
- Eine Verbindung, bei der ein Partner eine dynamische IP besitzt, nennt man "Road Warrior". Auch dieses Thema ist recht ausführlich behandelt. Dieser Fall wird in der Konfiguration daran erkannt, dass anstelle der IP-Adresse der Gegenstelle im Server "%any" steht.
- Für uns arme T-Online-Flatrate-Kunden stellt sich jedoch noch eine ganz andere Frage: Was ist, wenn beide Partner dynamische Adressen haben? Wenn ich zwei Flatrate-Netze verbinden will oder wenn ich mit dem Laptop von unterwegs in meinen heimischen DSL-Rechner will?

Dieser letzte Fall wurde nirgendwo in den Dokus erwähnt. Trotzdem habe ich lange herumgespielt. Natürlich sollten beide Rechner erstmal per dynamisches DNS erreichbar sein. Ininteressanterweise sind es gerade die Sicherheitsmerkmale der Authentifizierung, die zuerstmal die Definition einer einfachen Verbindung, die alle Widrigkeiten wie Verbindungsabbruch durch den Provider übersteht, unmöglich machen. Eine Authentifizierung, die sich auf eine vorhandene Verbindung bezieht, aber auf einmal von einer anderen IP-Adresse kommt, wird geflissentlich ignoriert. :-(Dann habe ich es doch geschafft: Man konfiguriert einfach zwei spiegelbildliche Road-Warrior-Verbindungen. Interessanterweise gibt es kein Problem, weil ja nun zwei Tunnel die gleichen Adressbereiche routen wollen. Es funktioniert!

Schlüssel erzeugen

Grundsätzlich gibt es verschiedene Verfahren der Verschlüsselung, die benutzt werden können. Die Verwendung eines gemeinsamen Schlüssels ist nicht zu empfehlen, da dieser immer gleich bleibt und dadurch ein Angreifer, der ihn irgendwie erbeutet, den gesamten Datenverkehr der Zukunft und auch der Vergangenheit

(wenn er ihn protokolliert hat) entschlüsseln kann. Besser ist da das autokeying-Verfahren. Hier wird der Partner mit einem RSA-Schlüssel (RSA arbeitet mit einem öffentlichen und einem privaten Schlüssel) authentifiziert. Der eigentliche Schlüssel für den Datenstrom wird jedoch regelmässig automatisch ausgetauscht. Als dritte Variante gibt es als Patch noch die Verwendung von X.509-Zertifikaten, die die Bildung einer Trust-Organisation erlauben (letztlich werden auch RSA-Schlüssel benutzt). Da dies für meine Anwendung mit Kanonen auf Spatzen geschossen schien, habe ich mich für RSA-Authentifizierung entschieden.

Bei der Installation des Debian-Paketes fragt das Installationskript, ob ich X.509- oder RSA-Schlüssel erzeugen möchte. Hier wähle ich RSA-Schlüssel. Damit ist schon der erste Schritt getan. Der Schlüssel meines Rechners wird nun in der Datei /etc/ipsec.secrets erzeugt. Mit dem Befehl ipsec showhostkey --left >hostkey.txt (oder right) extrahiere ich ihn in eine Datei. Dabei sollte man auf einem Rechner der Verbindung left und auf dem anderen right angeben. Dadurch wird eine Zeile erzeugt, die direkt in die ipsec.conf eingefügt wird.

Konfigurationsdatei /etc/ipsec.conf

Diese Datei enthält alle Angaben, um IPSec zu konfigurieren. Sie ist in Sektionen eingeteilt. Die erste Sektion config setup enthält globale Einstellungen. Sie sieht bei mir so aus:

```
config setup
# THIS SETTING MUST BE CORRECT or almost nothing
  will work;
# %defaultroute is okay for most simple cases.

interfaces=%defaultroute
# Debug-logging controls: "none" for (almost) none,
  "all" for lots.

klipsdebug=none
plutodebug=none

# Use auto= parameters in conn descriptions to control
  startup actions.

plutoload=%search plutostart=%search
# Close down old connection when new one using same ID
  shows up.

uniqueids=yes
```

Diese Einstellungen sollten eigentlich für alle normalen Anwendungen reichen. Falls der Tunnel nicht auf dem Interface liegen soll, das das Default-Gateway (zum Internet) ist, kann die Zeile interfaces="ipsec0=eth0" oder ähnlich verändert werden.

Jede Verbindung hat nun eine eigene Connect-Sektion. Enthält diese einen Eintrag auto=add oder auto=start, so wird diese Verbindung beim hochfahren automatisch für den Empfang konfiguriert bzw. sogar aufgebaut. Durch das Schlüsselwort also=sektionsname kann eine andere Sektion "eingebunden" werden. Dies nutze ich in meinem Beispiel aus. In der Datei ist immer von "left" und "right" die Rede. Damit bezieht man sich auf die beiden Enden der Verbindung. Ob



der Rechner left oder right ist, stellt freeswan selber anhand der Daten fest.

"linker" Rechner

```
conn horas # Parameter, wenn der Router die
Verbindung initiiert also=stargate left=%defaultroute
right=hal9000.dyndns.org keyingtries=0 auto=start
```

```
conn ares # Parameter, wenn Pommies die Verbindung ini-
tiiert also=stargate left=%defaultroute right=%any
keyingtries=1 auto=add
```

```
conn stargate # Parameter, die fuer beide
Verbindungen auf beiden Rechnern gleich sind:
leftsubnet=192.168.1.0/24 leftid=@firewall.datenstrom.
loc # RSA 1024 bits firewall Mon Dec 16 14:20:37 2002
leftrsasigkey=0SA..... rightsubnet=192.168.2.0/24
rightid=@router.datenstrom.loc # RSA 1024 bits router
Mon dec 16 14:41:02 2002 rightrsasigkey=0SA.....
```

Nun die Unterschiede für den "rechten" Rechner:

```
conn horas left=%any right=%defaultroute keyingtries=1
auto=add
```

```
conn ares left=oscar.evilroot.org right=%defaultroute
keyingtries=0 auto=start
```

Damit findet jeder der beiden Rechner jeweils den anderen und baut eine Verbindung auf. Die angegebene ID wird dabei als "Username" benutzt und der Schlüssel, den wir oben erzeugt haben, als Passwort. Wenn start durch add ersetzt wird, baut sich die Verbindung nicht immer automatisch auf. Dann kann z.B. mit ipsec auto --up horas die Verbindung hochgefahren werden. Fertig!

Falls der Tunnel automatisch hochgefahren werden soll, sollte man dann allerdings noch folgendes nach /etc/ppp/ip-up.d/ipsec schreiben:

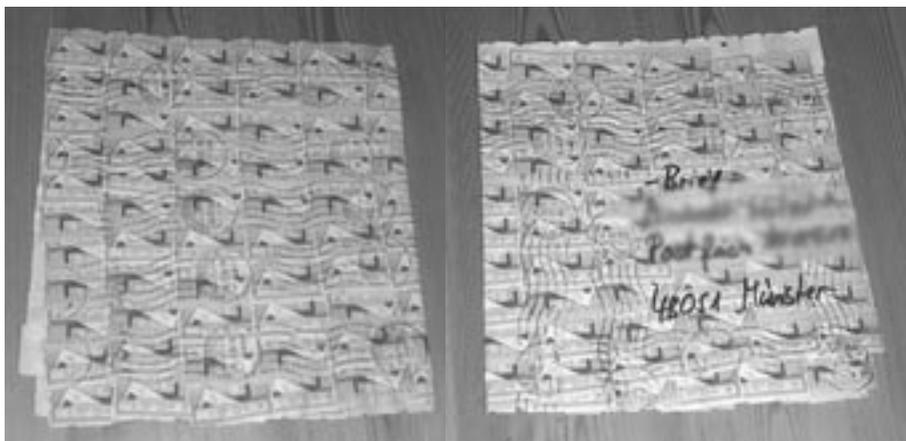
```
#!/bin/bash /etc/init.d/ipsec start
```

Besonderheiten

Zu sagen ist noch, daß nur das Routing zwischen den beiden lokalen Netzen verschlüsselt wird. Pakete, die von einem der beiden Gateway-Rechner kommen, werden nicht geroutet, da sie als Absendeadresse Ihre dynamische IP benutzen (und nicht Ihre IP im lokalen Netz). Zugriff auf das Gateway vom jeweils anderen Netz ist jedoch möglich, da dafür dann das Interface im lokalen Netz benutzt werden kann, ansonsten muss man die IP-Adresse des öffentlichen Interfaces nehmen (also den Namen für dynamisches DNS). Wie das z.B. mit einem Laptop geht, der kein lokales Netz hat, bleibt noch zu erforschen...

Links:

- [1] <http://www.chiark.greenend.org.uk/~sgtatham/putty/>
- [2] <http://www.dyndns.org>
- [3] <http://www.dynip.com>
- [4] <http://www.freeswan.org>
- [5] <http://www.openssh.com/de>
- [6] <http://www.poptop.org/>
- [7] <http://www.linux.org/docs/lp/howto/VPN-HOWTO/>
- [8] <http://www.debian.org/>
- [9] <http://www.freenet.de>



Schutzgeld-Erpressung in der IT-Branche

von Fefe <felix@ccc.fefe.de>

Was ist der Unterschied zwischen der IT-Branche und der Mafia? - Die Mafia zahlt mehr Steuern.

Auf diesen Schluß könnte man kommen, wenn man sich anschaut, mit was für unseriösen Methoden in der IT-Branche gearbeitet wird, insbesondere in der IT-Security. Es ist geradezu erschreckend, mit welcher Bauernfängerei die Unternehmen teilweise vorgehen. Nehmen wir nur mal die halbseitigen Anzeigen in der aktuellen c't. Alle sind glücklich, außer dem Hacker, denn der kommt nicht mehr rein. Alles, was man tun muß, ist diese kleine schwarze Kiste ins Rack stellen. Oder die Pusher-Kolonnen der Virenschanner-Hersteller. Wie sie auf Messen ihre Anfix-Proben unter die vorbeitreibende Schafherde werfen! Oder die Personal Firewalls... aber gegenüber der organisierten Kriminalität der Schutzgeld-Nummer der BIND Company nimmt sich das geradezu wie kleinkriminelle Bagatellen aus.

Die BIND Company hat eine Mailingliste für VIP-Kunden eingerichtet. Der Kunde zahlt, darf auf die Mailingliste, und kriegt dann vor den anderen Mitteilung von neuen Sicherheitslücken in BIND.

Das muß man sich mal auf der Zunge zergehen lassen! Man soll dem Hersteller eines Quasi-Monopol-Produktes auch noch Geld dafür geben, daß er einen über seine ständigen Sicherheitslücken in Kenntnis setzt! So geht nicht mal Microsoft mit seinen Kunden um! Aber bei der BIND Company sind noch einige andere Sachen im Argen. U.a. versuchen die BINDler gerade, eine AXFR Clarification in der IETF zu publizieren. Sie sagen, das sei eine Erläuterung der aktuellen AXFR Implementation. Wer sich das Dokument anschaut, wird feststellen, dass es sich im Gegenteil um eine Protokollrevision handelt, die u.a. alle möglichen Details plötzlich mit MUST und SHOULD zu zementieren versucht, die so genau nur von BIND gemacht werden, nicht aber von djbdns oder anderen DNS Servern. Der Gipfel der Impertinenz ist, dass das Dokument sogar Sachen vorschreibt, die nicht einmal BIND 8 so implementiert -- und das ist der am häufigsten eingesetzte DNS-Server im Internet! Details gibt es hier [1]

Das wäre alles nicht so schlimm, wenn die IETF ein demokratischer Prozeß wäre. Oder zumindest ein offener. Daß ICANN eine korrupte nichtsnutzige Vereinigung von bürokratischen Status-Quo Beibehaltern ist, ist ja hinlänglich bekannt. Aber die IETF ist nicht besser.

Tatsächlich entscheiden da ein paar verkrustete Seilschaften nach Gusto, wer was publizieren darf und wer nicht. Die meisten abgelehnten RFCs verschwinden ungesehen in der Versenkung, aber Herr Bernstein läßt sich von solchen Machenschaften nicht einschüchtern -- dieser Eigenschaft haben wir es übrigens zu verdanken, daß er kürzlich in einer Prozeßserie die Krypto-Exportbeschränkungen der US-Regierung weitgehend zertrümmert hat. Er hat vor Jahren ebenfalls versucht, RFCs zu publizieren, und ist weitgehend ignoriert worden. Dann hat man ihn über Jahre hingehalten und am Ende hat er dann aufgegeben. hnlich ergeht es ihm mit djbdns und seinem Leidensweg mit der IETF und den Mailinglisten dort. Glücklicherweise hat er seinen Leidensweg dokumentiert [2]

Ich weiß nicht, wie es euch so geht, aber mir treiben solche Machenschaften die Zornesröte ins Gesicht. Es wird offenbar Zeit für eine neue Internet-Verwaltung. Wer macht mit? [3]

[1] <http://cr.yo.to/djbdns/axfr-clarify.html>

[2] <http://cr.yo.to/djbdns/namedroppers.html>

[3] <mailto:felix@ccc.fefe.de>



BESTELLFETZEN

Bestellungen, Mitgliedsanträge und Adressänderungen bitte senden an:

CCC e.V., Lokstedter Weg 72, D-20251 Hamburg, Fax +49.40.401.801.41

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

- Chaos CD Blue, alles zwischen 1982 und 1999 EUR 23 + EUR 3 Porto
- Alte Ausgaben der Datenschleuder auf Anfrage
- Datenschleuder-Abonnement, 8 Ausgaben
Normalpreis EUR 32
Ermäßigter Preis EUR 16
Gewerblicher Preis EUR 50 (wir schicken eine Rechnung)
- Satzung und Mitgliedsantrag
EUR 2,50 oder zum Selberausdrucken unter <http://www.ccc.de/club/membership>

Die Kohle

- liegt als Verrechnungsscheck bei
- wurde überwiesen am _____._____._____ an

*Chaos Computer Club e.V., Konto 59 90 90-201
Postbank Hamburg, BLZ 200 100 20*

Name:

Straße / Postfach:

PLZ, Ort

Tel.* / Fax*

E-Mail:

Ort, Datum:

Unterschrift

*freiwillig

First I must sprinkle you with fairy dust!



Chaos Communication Camp 2003
The International Open Air Hacker Meeting
7/8/9/10th August 2003
near Berlin

<http://www.ccc.de/camp/>