die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

Das Modell wurde großzügigerweise von dexter zur Verfügung gestellt.
Foto von Nadja Ritter.

ISSN 0930-1054 • 2010
Zweihundertundfünfzig Cent

#94

Geleitwort

Wird der Chaos Computer Club arriviert? Sind wir angekommen in den seichten Niederungen des Establishments, in den schattigen Gesprächskreisen an den Lobbyisten-Schnittchenschleudern? Bei flüchtiger Betrachtung kann einem schon der Gedanke kommen. Politiker aller Couleur werfen sich uns mit ausgebreiteten Armen an den Hals oder tun zumindest so, als würden sie beim Grauburgunder unsere fachliche Meinung hören wollen. Selbst der neue Innenminister gibt sich konziliant, erörtert unseren Datenbrief-Vorschlag und macht runde Tische wieder eckig.

Migriert die Mitte der Gesellschaft nun also ins Netz, zusammen mit den Silversurfern aus der Berufspolitikergilde? Fungiert der CCC als eine Art Vermittlungsausschuß zwischen digitalen Zuwanderern und den leicht angenervten Eingeborenen? Ist es also eher so, daß sich die Mitte rein demographisch zwangsläufig auf uns zubewegt? Sterben die analogen Telex-Dinosaurier aus oder müssen sie sich noch im und mit dem Netz arrangieren? Kommen wir in die Rolle des permanenten Erklärbärs oder – schlimmer noch – des Computer-ADAC?

Der Umarmungsdruck von allen Seiten ist gerade groß. Allein, der Club ist etwa so gut zu umarmen wie ein Kaktus. Viele haben es ob der scheinbaren Omnipräsenz in Medien und Gremien vergessen: Alles, was ihr seht, ist reine Freiwilligenarbeit, die von Leuten gemacht wird, die darauf Lust haben. Ob die Congresse, die Datenschleuder, Gutachten fürs BVerfG, die Pressearbeit: Niemand wird bezahlt, niemand gezwungen. Wenn keiner Interesse hat, weil das Thema zu öde ist oder das Gremium zu staubig und unwichtig, passiert auch nichts. Nicht zu müssen, sondern zu dürfen, ist der Kern der Unabhängigkeit des Clubs, nur so können wir unbefangen und unbeeinflußt Stellung nehmen und Expertisen beitragen zu den Themen die uns am Herzen liegen. Stopft also bitte die übersteigerten Erwartungshaltungen zurück in den Schlüpfer!

Nicht zuletzt der Spaß am Gerät und das Zerforschen der Technologie, die unseren Alltag bestimmt, gibt uns Energie, Expertise und Lust, dem im Politzirkus allgegenwärtigen Gemisch aus Unwissen, Proporz, Ignoranz und Stammtischlogik eine rationale, freiheitsliebende Perspektive entgegenzusetzen. Daher freuen wir uns, einige sehr erbauliche Forschungsberichte aus den Randbezirken des erforschten Digitaluniversums präsentieren zu können. Besonders zu empfehlen seien angesichts des dräuenden elektrischen Personalausweises die reich bebilderten Abhandlungen zur Entkleidung und optischen Feinanalyse von Chips und Angriffen auf „sichere Hardware“ mit Seitenkanalmethoden. Die hier erstmals so schön in Schriftform aufbereiteten Erkenntnisse sind das Rüstzeug für die nächste Etappe.

Seit die letzte Datenschleuder aus den Druckerpressen donnerte, hat sich einiges getan im deutschen Digitaldilemma. Das Bundesverfassungsgericht hat uns vorerst von der Vorratsdatenspeicherung befreit und harte Grenzen gezogen, was zukünftige bevorratende Speichergier auf die Daten der Anderen angeht. Organisierte Berufsdatenverbrecher wie Facebook, google und StudiVZ bemühen sich jedoch redlich, die beim Staat gerissene Speicherlücke zu füllen. Wie lange der Respekt vor dem Urteil die Datengier zähmen wird, bevor die gerade noch in ihren Werkzeugen beschnittenen Bedarfsträger sabbernd nach diesen privaten Speicherpfründen langen, kann sich auch ein SchülerVZ-ler an einer Hand ausrechnen.

Die Netzsperren haben sich für uns als langlebiges Kleinod erwiesen. Selbst die ansonsten als Steh-auf-Weibchen bekannte, stets grinsende Zensursula wurde dabei verschlissen. Ihre Nachfolgerin mit den häufig wechselnden Allerweltsnamen hat sich gleich gar nicht mehr des Themas angenommen. Etwas einsam an dieser politischen Front kauert nur noch die Christenunion, um von der Realität unerschüttert die nichtsnutzigen Zugangshemmnisse zu promoten. Nebenbei schlich sich – quasi wie zum Test der Beißreflexe – in fast schon erfrischender Dreistigkeit eine neue Volkszählung in die politische Arena: Ein vorprogrammiertes Debakel, geradeso als ob uns die Möglichkeit gegeben werden soll, in Zeitlupe beim Gedei-

hen eines Datenskandals zuzugucken. Dem widmen wir uns auf Seite 45 ausgiebig.

Wir hatten die einmalige Gelegenheit, einem kulturellen Wandel beizuwohnen: Neuerdings gehört es sich für jeden gestandenen Politnachwuchs, mangelnden Berufsethos durch Netz-Anschleimerei zu kompensieren. Zufällig mischt man ein paar technische Fachwörter in jede Rede, was sie bedeuten, spielt dabei weniger eine Rolle. Bei Nachfragen wird betont, daß das sicher die Experten erklären könnten. Ein klitzekleines bißchen Lob spendet man hernach für die Segnungen des Netzes, nur um dann auf die entsetzlichen Abgründe zu verweisen, welche die „Datenautobahn“ (Wtf?) mit sich brächte. Keine Rede ohne den strunzblöden Verweis auf unter allen Umständen zu vermeidende „rechtsfreie Räume“. Dies müssen wir ihnen noch abgewöhnen.

In anderen Ländern – wie etwa Brasilien – ist schon seit vielen Jahren selbstverständlich, daß bei Parlamentsdebatten die E-Mail-Adresse des Redners in der Fernsehübertragung eingeblendet wird. Bis wir in Deutschland soweit sind, wird es wohl noch dauern: Die Konservativen konnten sich in der Enquête-Kommission des Deutschen Bundestages, die explizit das Internet zum Thema hat, nicht mal durchringen, durchgehend öffentlich zu tagen. Das Antwortverhalten auf Abgeordnetenwatch kann jedenfalls kaum als Maßstab für eine transparente Regierung herhalten.

In Deutschland hingegen haben viele Politiker erst kürzlich wirklich Selberklicken gelernt. Doch sogar Wiefelspütz hat jetzt seinen eigenen Computer – und schweigt dankenswerterweise seit dem Alltagskontakt mit der vernetzten Realität beharrlich. Selbst Frau Zypries mußte auf die harte Tour erlernen, was ein Browser ist. Die Internetausdrucker drucken jetzt nur noch heimlich, wenn sie glauben, daß keiner zuschaut. Sie twittern bisweilen und vereinzelt sogar selber, eventuell hat ein Social-Media-PR-Beratersimulant ihnen dazu geraten. Zu echten Online-Wahlkämpfen reichte es allerdings noch nicht, dafür brauchen sie wohl noch ein Jahrzehnt. Ein paar sinnvolle Inhalte und Antworten würde das vielleicht beschleunigen. Daß **wir** uns noch einmal brasilianische Verhältnisse wünschen würden ...

Nerds, Hacker, Netzbewohner, Blogger haben sich fast ans helle Sonnenlicht beim auf der Straße Demonstrieren gewöhnt – und mit ihnen demonstriert der vielgespriesene Querschnitt der Bevölkerung mit passenden Parolen-Nickis und Kinderwagen. Zum dritten Mal schon kamen wir zu Tausenden zum Revolutionstraining in der Mitte Berlins zusammen. Aufgrund immer wieder an die Redaktion herangetragener Fragen bezüglich mißverständlicher Spielregeln für das Demo-Adventure publizieren wir daher auf Seite 48 ein nutzbringendes Regelbuch, das am 11. September dieses Jahres praktisch eingesetzt werden kann.

Zu den erfreulichsten Nachrichten der letzten Erscheinungspause der Datenschleuder gehört die Verleihung der Goldenen Nica 2010 des Prix Ars Electronica an den CCC. Der renommierteste Preis, den es in puncto Digitales in Europa so zu gewinnen gibt, wurde uns in der Kategorie „Digitale Gemeinschaften“ verliehen. Dankeschön! *<die redaktion>*

Inhalt

Aufgrund einiger mysteriöser Vorgänge auf meinem Rechner (gesperrte Tastatur, deaktivierter Mauszeiger, eingefrorenes System) vermute ich einen Einbruch in mein System. Ich arbeite mit einem PC unter Suse Linux,

Lieber Bo, die mysteriösen Vorgänge auf Deinem Rechner nennt man in der Fachwelt schlicht „Suse Linux". Hier sind eingefrorene Systeme und dysfunktionale Peripherie an der Tagesordnung.

und bin über einen Router mit dem Netz von T-Systems verbunden.

Auch T-Systems ist nicht für wirklich hochqualitative Services bekannt, hat aber mit Deinem Problem eher nichts zu tun.

Wie kann ich den Eindingling dingfest machen, bzw. in einer Fangschaltung/Log aufspüren. Könnten Sie mir dazu ein paar Tips oder Informationen geben. Über Ihre Message würde ich sehr freuen. <*boXXX@arcor.de*>

Was genau sollte der Angreifer damit bezwecken, Deinen Rechner zum Stehen zu bringen? Die üblichen Gründe für einen Angriff auf PCs, nämlich das Installieren von Trojanischen Pferden, machen auf einem Linuxrechner viel zu viel Aufwand: Die frieren nämlich ständig ein, und die Maus geht nicht, und dann werden sie rebootet. ;) <erdgeist>

Sehr geehrter Computerclub! In großer Not und Bestürzung schriebe ich Euch. [...] Es ist dringend! Und eilt sehr. Die Problematik hier nur ganz in Kürze, ich müßte mit euch [...] direkt und persönlich sprechen.

Hier worum es geht: Ich wurde gehackt vor nunmehr 3 Jahren, seither werde ich massiv gestalkt. Zuerst wurde ich am Telefon von meiner Arbeit abgehalten, dann verlor ich die Heimarbeit/ich bin Frührentnerin. Dann wurde in meine Wohnung eingebrochen, es wurden Daten gestohlen usw, Veränderungen am PC vorgenommen usw.

Ich mußte mehrfach umziehen, immer wieder hatte man mich ausfindig gemacht, und weiter massiv gestalkt und gemobbt. Inzwischen wurden mir am Auto zwei mal die Reifen zerstochen, die Antenne runter gebogen usw...

Inzwischen schon über ein Jahr lang auch am Handy [...]. Ich bin absolut am Boden zerstört, weil mir nicht klar ist, wie dies gemacht wird, und wie ich mich dagegen schützen kann.

Bitte mailt mir, am besten wäre es aber, ihr ruft an, oder versucht es, wobei ich am Telefon nicht viel reden kann, es wird ja alles mitgehört. Am besten wäre es, ich könnte euch treffen, oder einen von euch, der sich auch der Sache annimmt. Ich hoffe sehr, von euch bald zu hören! <*R.*>

Ich bekomme häufiger Briefe wie Deinen. Ich habe es mir aber zur Regel gemacht, die Anfragenden stets zu bitten, sich erst mit einem Psychologen zu besprechen und sich attestieren zu lassen, daß man nicht an einer Wahrnehmungs- oder Bewertungsstörung leidet.

Erst wenn der Arzt einen negativen Befund ausstellt, wäre ich bereit, mich mit so einer Geschichte zu beschäftigen. Sei mir nicht böse, aber solche Geschichten kosten regelmäßig unendlich viel Kraft, die ich nur dann investieren will, wenn die Chance besteht, daß es sich nicht um gesundheitliche Störungen handelt. <padeluun>

R. ist empört

Wer ist bitte „padeluun"?? Ich soll ein psychologisches Gutachten vorlegen? Das schlägt dem Faß den Boden aus, an Entwürdigung und Ent-Menschlichung. Ist dies die Ethik des ccc? Ich werde diesen Vorfall nunmehr an die Medien weiterleiten.

Selbstredend, daß ich Polizei (Strafanzeigen) und die Staatsanwaltschaft längst eingeschaltet habe. Aber bis bei Cyberstalking die Bürokratie in die Hufe kommt, dauerts und dauerts... Aber diese E-Mail habe ich in einem Internetcafe geschrieben, möglich daß sich hinter padeluun gar nicht der ccc verbirgt? Sondern ein neuer Trittbrettfahrer, hähähähä, wenns nicht so traurig wär.

Ja, es ist die Ethik des CCC, offensichtlich hilfebedürftigen Menschen nahezulegen, professionelle Hilfe in Anspruch zu nehmen.

Ich denke also, daß padeluun damit für den Chaos Computer Club spricht, und würde seine Empfehlung unterstützen. <erdgeist>

Die nachfolgenden Zitate kann ich nur unterstreichen und muss fassungslos zur Kenntnis nehmen, wie die Diskussion über „Zensur" im Internet von Ihnen extrem einseitig, undifferenziert und vollkommen unangemessen geführt wird. Schade, daß Sie sich nicht für wirkungsvolle und umsetzbare Maßnahmen gegen Kinderpornograhie einsetzen bzw. hier mit der Politik zusammenarbeiten – das wäre ein echter, bürgerlicher Beitrag.

Vielleicht sollten Sie einfach den Gesetzentwurf lesen, auf den Sie im Internet verweisen?

Ich gehe schon davon aus, daß in diesem (besonderen) Falle die Politiker (ausnahmsweise?) im Interesse der überwältigenden Mehrheit handeln – setzen Sie sich lieber dafür ein, daß das Handeln in wirkungsvollen Kanälen mündet anstatt meiner Meinung nach völlig unausgewogene „Visionen" vom Überwachungsstaat zu entwerfen. *<Oliver Marquardt>*

Hans-Peter Uhl, CDU Die ganze pseudo-bürgerrechtsengagierte Hysterie von Pseudo-Computerexperten, man müsse um jeden Preis ein „unzensiertes Internet" verteidigen etc. – vgl. *www.ccc.de* –, fällt für mich in die Kategorie: juristisch ohne Sinn und Verstand und moralisch verkommen.

Ursula von der Leyen, CDU Und deshalb noch mal vielleicht ein Wort zu denen, die hier heute protestieren. Die dagegen protestieren, daß – ich sag's noch mal: Die Bilder von Kindern, die vor laufender Kamera geschändet werden, wo vor laufender Kamera in Kauf genommen wird, daß diese Kinder an inneren Verletzungen verbluten, das sind genau die Themen die unter „Kinderpornographie" laufen, wenn Sie Ihre Fachlichkeit, Ihre Fähigkeit als Chaos Computer Club im Internet einsetzen würden, um genau dieses zu verhindern, dann wäre Ihr Engagement an der richtigen Stelle.

Wir freuen uns, nun auch in bildungsfernen Schichten wahrgenommen zu werden. Herr Uhl fühlte sich übrigens nur drei Tage nach obiger Aussage ein wenig nach Zurückrudern:

Ich bezweifle nicht, daß z. B. die Angehörigen des Chaos Computer Club grundsätzlich Ernst zu nehmende Computerfachleute sind. Ich bedaure, daß ich einen unnötig polemischen Ton in die Debatte gebracht habe. Schließlich ist es ja richtig, geplante Maßnahmen von allen Seiten zu beleuchten und zu hinterfragen. *Link: http://www.abgeordnetenwatch.de/dr_hans_peter_uhl-650-5550--f173841.html#q173841*

Wahrscheinlich hatte er bloß Angst, daß ihn mal jemand fragt, was ein Browser sei. <erdgeist>

Helfer mit PC gesucht

Starnberg – Die Stadt Starnberg sucht für ihre 21 Wahllokale für die Kommunalwahl am 2. März noch rund 50 Wahlhelfer, die ihren eigenen PC oder ihr Notebook mitbringen und für die Stimmenerfassung zur Verfügung stellen. Das Gerät muss dafür einen Zugang für einen USB-Stick bieten. Die Stadt gewährt für die Wahlhelfertätigkeit ein Erfrischungsgeld in Höhe von 50 Euro und für den mitgebrachten Rechner zusätzliche 30 Euro. Interessenten werden gebeten, sich im Wahlamt der Stadt Starnberg unter der Telefonnummer 08151/772131 zu melden.

sb

Zensurusla, entsetzt.

hi ccc.de, with the present i would like to know why you don't pubblish too in English your zine „die datenschleuder". Deutch is difficult and not have studied Deutch, more other people could be interested, but so it is impossible to know what was written :-(

i am sorry, but i can't read a zine such as „die datenschleuder", why i don't know Deutch :-(*<Paolo B.>*

this is deutschland, so we sprechen deutsch! <guido w.>

Dann war da noch die Signatur des Herrn S.:
Scharfes Auge, sichere Hand - Und ein Herz fürs Vaterland.
Bürgerliche Schützengesellschaft 1776 Markt Nordheim e.V.
Gaukoenig Gruppe A Hefeklasse sitzend getrunken

Ich wollte mich einfach mal bedanken für Eure Datenschleuder. Schon seit Langem lese ich Euch. Ich warte immer sehnsüchtig auf die nächste Ausgabe. Da ich zur Zeit mit meinem Fahrrad auf Weltreise bin (*raderfahrung.de*) ist es für mich schwer, etwas Vernünftiges zum Lesen zu bekommen. Eine kleine Bitte hätte ich dennoch. Bitte bringt doch kürzeren Abständen die Datenschleuder raus. *<Gerard P.>*

*Danke für Die warmen Worte. *hust* Die Erscheinungsweise ist stark witterungsabhängig. <erdgeist>*

Mit Interesse lese ich Ihre kritischen Stellungnahmen bezüglich der aktuellen Themen, insbesondere die Netzzensur betreffend. Erlauben Sie mir folgende Anmerkungen:

Das Internet entwickelt sich systembedingt immer mehr zu einer globalen universellen Auskunftei. Dabei spielt es keine Rolle mehr, ob betreffende Personen überhaupt mit einer Veröffentlichung Ihrer Daten in Registern und Suchmaschineneinträgen einverstanden sind.

Beim Googlen nach meinem eigenen Namen fand ich viele Verweise und Veröffentlichungen denen ich nie zugestimmt habe. Alle Bemühungen diese Einträge zu eliminieren waren erfolglos. Aktuell beschäftigt sich ja auch unsrere Bundesregierung mit ähnlichen Auswirkungen, die Verletzungen des Jugendschutzes zur Folge haben. Ich bin der Meinung, daß grundlegende neue Regelungen geschaffen werden müssen.

1) Berichte und Verweise nur durch zugelassene journalistische Institutionen.
2) Bei allen Berichten und Nachrichten muß zwingend die Quelle benannt werden.
3) Alle Veröffentlichungen und Internetseiten erhalten ein Löschungs- oder Verfalldatum, oder werden nach Prüfung und Bestätigung in zugelassene Register eingetragen.
4) Verlinkung auf Internetseiten nur mit Zustimmung des Inhabers und einschgeschlossener rechtlicher Prüfung durch alle zuständigen Stellen.
5) Internetseitenaufruf in Deutschland nur ermöglichen wenn der IP-Nummer ein Impressum des Herausgebers zugeordnet ist.
6) Keine Zulassung mehr für private Suchmaschinen und externe Suchfunktionen auf Internetseiten. Die Internetrecherche kann dann nur noch über die in 3) genannten, behördlich überwachten Registern stattfinden.

Mit anderen Worten: Sie wollen das Internet zu einer Art Mischung aus Fernsehen und Zeitung degradieren, inklusive eingebauter Zensurfunktion.

Diese Maßnahmen erübrigen alle zukünftigen Ärgernisse und Diskussionen in Bezug auf Internet und Informationsfreiheit.

Genau. Die Informationsfreiheit im Internet (ja, die funktioniert hier bidirektional) gibt es dann nämlich nicht mehr.

Eine Zensur kann so nicht mehr stattfinden, vorausgesetzt alle Beteiligte halten sich an die Regeln.

Wenn sich „alle Beteiligten" an „die Regeln" hielten, hätten wir schon ganz andere Probleme wie Krieg, Hunger, Diskriminierung und <hier beliebiges Problemfeld einsetzen> gelöst. De facto werden Regeln gebrochen – auch und gerade wenn sie unsinnig sind. Das wissen Sie so gut wie ich. Ihr Katalog von Forderungen verhindert keine Zensur, er implementiert sie geradezu. Wenn ich nur daran denke, daß ich alles, was ich veröffentlichen möchte, erst bei einer Behörde einreichen und genehmigen lassen soll, wird mir – mit Verlaub – speiübel.

Auf diese Weise ist sichergestellt das unerwünschten Veröffentlichungen wirkungsvoll begegnet werden kann. *<Adolf H.> (We're not kidding you. Aber nicht Hitler. 2x überprüft.)*

*Exakt. Alles, was der „Bundesanstalt für Informationshygiene im Internet" nicht genehm ist, wird zensiert. Dann bleibt natürlich die Frage: Wer bestimmt, was genehm ist und was nicht? Eventuell die aktuellen Machthaber? Könnte es sein, daß diesen gerade jene Informationen nicht genehm sind, die gegen ihre eigenen Interessen gehen? Könnte es – gesetzt den Fall, es wäre so – nicht auch sein, daß dadurch die Grundsicherung einer freien, demokratischen Gesellschaft (die Meinungsfreiheit *Zaunpfahl, winkewinke*) gefährdet würde? <Alex>*

Ein offensichtlich beliebtes Motiv: Das Cover der #90 hier im Softwaretest auf web.de

Leider ist uns beim Versenden der Einladung zur Konferenz „Datenschutz in der Informationsgesellschaft" ein Fehler unterlaufen, indem wir den Verteiler offen gehalten haben. Wir bitten Sie, dieses Versehen zu entschuldigen. *<Referat 212 Verbraucherschutz in der Informationsgesellschaft sowie in den Bereichen Verkehr und Energie Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz>*

Keine Sorge, bei uns sind die Daten in guten Händen. <Frank>

Liebe Computerprofis, eine überflüssige Frage von einem eh Paranoiden: Ist der Gedanke, daß mein LCD-Monitor mich fotografiert, total abwegig? Mir ist seit längerem ein gelegentliches, nur millisekunden dauerndes Aufblitzen des Bildschirms aufgefallen ... (Verfolgungswahn halt) aber immer werde ich das komische Gefühl nicht los, daß an einem der anderen Enden der Leitung jemand sitzt, der unbedingt wissen will, wer bei mir grad' am PC sitzt .

Mein Gedankengang hierbei: Der Lichtblitz trifft auf mein Gesicht, wird reflektiert auf die Kristalle, und löst dort eine winzige Veränderung aus, die in ein Bild umgewandelt wird ?!?!? ... aber Wahrscheinlich habe ich „zu oft" Fletschers Visionen angeschaut ...

Noch was, ganz am Rande: Die vielen silbernen Autos auf der Straße – an machen Ampeln oder Kreuzungen oder bei Schlangen = bis 5-6 auf einmal – ich glaube, das wird immer mehr: Sind wir mitten in einem PROGRAMM, in dem wir mittels Handypulsewellen oder Trinkwasser oder TV unterbewußt manipuliert werden ...? Auf manchen Parkplätzen bis zu 40% silberne? ... aber wie gesagt, Ihr dürft es nicht ganz ernst nehmen (tun meine Freunde auch schon lange nicht mehr). *<lillehavfrue>*

So wirre E-Mail drucken wir ja nur noch ab, wenn sie uns sehr belustigen. Falls das ein Fake ist: Danke für die Mühe, aber mach doch nächstes mal vor dem Versenden 'ne Rechtschreibprüfung. <erdgeist>

hallo ccc jungs

*...und Mädels *hust**

durch einen Bekannten wurde ich auf euch aufmerksam und habe nur eine kurze prägnante frage. Ist der aktuelle Prem-Code knackbar oder nicht?

Der aktuelle Premiere-Code ist derzeit nicht im Wortsinne geknackt, jedenfalls nicht öffentlich bekannt. Knackbar ist er aber ohnehin immer mit hinreichendem Aufwand.

Man kann Premiere natürlich trotzdem gucken, ohne selbst eine gültige Karte zu haben, und zwar mit Key Sharing. Das CA-System ist bereits gehackt und re-engineered worden, aber (soweit bekannt) sind Karten und Krypto noch intakt. Da gibt es entsprechende Server im Netz, wo man solche Keys pollen kann, oder aber man teilt sie mit seinen Freunden, das geht natürlich auch. Ohne daß mindestens einer eine gültige Karte hat, geht's aber nicht.

By the way, Premiere heißt jetzt Sky. <constanze>

Hack a Bike: Den Code der unter dem Bericht steht soll man den draufmachen? Oder kannst du mir erklären wie das geht *<Max>*

Da der Artikel in der Datenschleuder auf anonym zugespielten Informationen basierte (brauner Umschlag an die Redaktion), können wir leider kaum mehr Detailtiefe liefern. Allerdings ist aufgefallen, daß folgende Links ggf. hilfreich beim Verständnis der Technik sein könnten: microcontroller.net, avrfreaks.net, Google zu ida pro und avr <constanze>

Ist das dann ein Codeauszug? Wie, war einfach ein Umschlag im Briefkasten? Geht so etwas überhaupt noch?

<Blöde Antwort.> <erdgeist>

Hab mich verliebt am Donnerstag. Ich möchte wissen, auf welchem Rück-Flug Sie gebucht ist für einen Abschiedskuß. Vermutlich Air Berlin, Ablug Köln Bonn nach Palma morgen. Muß sonst 12 Stunden am Flughafen alle 3 Abflüge absitzen. *<Volker>*

Sweeeeet. <Bine>

Hi, gibt es irgendwo im Netz einen Rechner, der extra dazu da ist, ihn zu hacken????? Bitte antwortet schnell!!! *<Maximilian G.>*

Aber klar doch! Nimm 127.0.0.1, der ist extra dafür geschaffen worden. Viel Erfolg! <Bine>

Ich hätte gerne, daß mein Garmin navü 200 bei Höhenänderungen piepst. (sh variometer von Bräuninger). Schließlich kann das Ding die Höhe und Geschwindigkeit anzeigen. Wer hat Lust, mir zu helfen? *<Markus F.>*

*Ich! Ich! *piep* *pieppiep* *piep* <Bine>*

Hi liebe CCC Betreiber, beim Stöbern im Internet bin ich auch auf Eure Seite gestoßen. Es ist eine Angewohnheit von mir, immer auf das Impressum zu schauen, um die Solidität des Anbieters zu sehen. Denn ein korrektes Impressum zeigt die Ernsthaftigkeit des Betreibers (egal ob gute oder schlechte Ersthaftigkeit). Es war für mich

enttäuschend, daß auch Euer Impressum fehlerhaft ist (schade).

Nach dem MDStV §10 Absatz 3 muß eine Person benannt werden die als Verantwortlicher für die Website zeichnet und der auch direkt ansprechbar ist, also Telefon und Emailadresse. Leider ist das in Eurem Impressum nicht zu finden. Es geht nicht um Besserwisserei, denn andere bekommen keinen Hinweis von mir. Mehrheitlich sind die Impressen nicht OK, das ist mir egal – bei Euch war ich ein wenig enttäucht, denn Ihr habt immerhin einen renomierten Namen. In Freundlichkeit! *<Frank S.>*

Offensichtlich fehlt uns die entsprechende Ernsthaftigkeit. Wir versprechen, auch in diesem Punkte in Zukunft viel ernsthafter zu werden. Ernsthafte Grüße <VB>

Ich weiß, es gibt eine Hackerehtik und Hacker sind dazu da Lücken auf zu decken deshalb schreibe ich Ihnen diese Mail. Ich weiß nicht, ob sie das gemerkt haben, aber ich kann mich mit meinem FileZilla Client auf Ihrem FTP-server einlogen. Mit folgenden Daten: Benutzername: `admin` (könnte auch `anonymous` gewesen sein) Kennwort: `quasi`, Adresse: *ftp.ccc.de* Port 21.

Ich konnte mit diesen Daten Dinge up- bzw. downloaden und Dateien löschen. Ich habe natürlich keinen Schaden angerichtet, ich wollte Ihnen das bloß melden. *<Maximilian G.>*

P.S.: Die Login-Daten konnte ich aus einem youtube-Video entnehmen. Titel: *„Wir hacken den ccc FTP server"*

NEIN! Echt jetzt? Neeeee. Man kann sich auf 'nem öffentlichen Server einfach so einloggen? Wenn das Zensursula rauskriegt! Wir sind geliefert! <Bine>

In der Akte Sendung vom 28. 07. 2009 sagten Sie was von sicheren Drucker. Wie sichere ich meinen? *<Michael R.>*

Loch bohren und Fahrradschloß durchziehen? <Bine>

Mit Verwunderung habe ich festgestellt, daß die Vorkämpfer des Gemeineigentums an geistigen Erzeugnissen ihre aktuelle Veröffentlichung nicht zum Download anbieten.

Gibt es dafür Gründe neben der Absatzförderung der Printausgabe? *<Matthias>*

Statt einfach zu sagen: „Eyh, ich will Eure Zeitung runterladen und nix dafür bezahlen", deklarierst Du uns urplötzlich ganz überraschend zum „Vorkämpfer des Gemeineigentums". Und prompt müssen wir uns quasi folgerichtig rechtfertigen, warum wir Dir nicht längst unser Vereinsmagazin ins Netz gestellt haben. Kess!

Die Online-Policy ist, daß die Abonnementen die Schleuder ungefähr zwei Wochen exklusiv in den Händen haben. Wenn wir dann nicht verpeilen, gibt's das PDF online. <erdgeist>

Mobile Phone

Aachen, CCCAC, Lothringer Straße 74, 52070 Aachen, dienstags ab 20 Uhr, *https://fedev.eu/ :: info@fedev.eu*

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

Bremen, Jugendhaus Buchte, Buchtstraße 14/15, 28195 Bremen (✉ CCCHB e. V., Hauffstr. 11, 28217 Bremen), 1. und 3. Dienstag im Monat *http://www.ccchb.de/ :: mail@ccchb.de*

Chaos **Darmstadt** e. V., Trollhölle, Wilhelm-Leuschner-Straße 36, 64293 Darmstadt, dienstags ab 20 Uhr *https://www.chaos-darmstadt.de/ :: info@chaos-darmstadt.de*

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

Düsseldorf, CCCD/Chaosdorf e. V., Fürstenwall 232, 40215 Düsseldorf, dienstags ab 19 Uhr *http://duesseldorf.ccc.de/ :: mail@duesseldorf.ccc.de*

Erlangen/Nürnberg/Fürth, BitsnBugs e. V., "E-Werk", Fuchsenwiese 1, Gruppenraum 5, dienstags ab 19:30 Uhr *http://erlangen.ccc.de/ :: mail@erlangen.ccc.de*

Hamburg, Mexikoring 21, 22297 Hamburg, (✉ CCC HH e. V., Postfach 60 04 80, 22204 Hamburg), 2. bis 5. Dienstag im Monat ab etwa 20 Uhr *http://hamburg.ccc.de/ :: mail@hamburg.ccc.de*

Hannover, Leitstelle 511 e. V., c/o Bürgerschule Nordstadt, Schaufelder Str. 30, 30167 Hannover, jeden 2. Mittwoch ab 20 Uhr und jeden letzten Sonntag ab 16 Uhr *https://hannover.ccc.de/ :: kontakt@hannover.ccc.de*

Karlsruhe, Entropia e. V., Steinstr. 23 (Gewerbehof), 76133 Karlsruhe, sonntags ab 19:30 Uhr *http://www.entropia.de/ :: info@entropia.de*

Uni **Kassel**, Wilhelmshöher Allee 71-73 (Ing.-Schule), 1. Donnerstag im Monat ab 18 Uhr *http://kassel.ccc.de/*

Köln, Chaos Computer Club Cologne (C4) e. V., Vogelsanger Straße 286, 50825 Köln, letzter Donnerstag im Monat ab 19:30 Uhr *https://koeln.ccc.de :: mail@koeln.ccc.de*

Mannheim, Chaos Computer Club Mannheim e. V., Postfach 10 06 08, 68006 Mannheim

Mainz, Kreativfabrik, Murnaustraße 2, 65189 Wiesbaden, (✉ CCC Mainz e. V., Postfach 19 11, 65009 Wiesbaden), dienstags ab 19 Uhr, *http://www.cccmz.de/ :: kontakt@cccmz.de*

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

Trier, Paulinstr. 123, 54292 Trier, mittwochs ab 20 Uhr *http://ccc-trier.de/* :: *anfrage@ccc-trier.de*

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

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

Zürich, Soodring 36, CH-8134 Adliswil, mittwochs ab 19 Uhr

Aus Platzgründen können wir nicht die Details aller **Chaostreffs** hier abdrucken. Ihr findet je einen in: Aargau, Augsburg, Basel, Bonn, Bristol, Dortmund, Essen, Frankfurt am Main, Gießen/Marburg, Göttingen, Graz, Hanau, Heidelberg, Heilbronn, Ingolstadt, Itzehoe, Kaiserslautern, Kiel, Leipzig, Lübeck, Luxemburg, Münster/Osnabrück, Paderborn, Ravensburg, Regensburg, Rothenburg ob der Tauber, Stuttgart, Tübingen, Wetzlar, Wuppertal, Würzburg. Näheres unter *http://www.ccc.de/regional/*.

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

Die Datenschleuder Nr. 94

Herausgeber (Abos, Adressen, Verwaltungstechnisches, etc.)
CCC e. V., Postfach 60 04 80, 22204 Hamburg,
☎ +49.40.401801-0, Fax: +49.40.401801-41, <*office@ccc.de*>
Fingerprint: *883B 905D CFE6 A213 E301 0FA6 F219 E5FA 6C8A 25DA*

Redaktion (Artikel, Leserbriefe, Inhaltliches, etc.)
Redaktion Datenschleuder, Postfach 64 02 36, 10048 Berlin,
☎ +49.40.401801-44, Fax: +49.40.401801-54, <*ds@ccc.de*>
Fingerprint: *03C9 70E9 AE5C 8BA7 42DD C66F 1B1E 296C CA45 BA04*

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

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

Chefredaktion 46halbe und erdgeist

Layout hukl, Unicorn, erdgeist

Redaktion dieser Ausgabe

Bine, Sarah Bormann, dexter, Martin Drahanský, Petr Hanáček, Johanna Kusch, Andreas Lehner, maha, Sascha Manns, Hannes Mehnert, Filip Orság, Frank Rieger, Martin Schobert, Scytale, Stefan „Kaishakunin" Schumacher, tec, Unicorn

Return to sender, address unknown

Andreas Lehner <al@ccc.de>

Aufmerksame Leser werden die Änderung bereits auf dem Adreßaufkleber oder im Impressum wahrgenommen haben, an dieser Stelle eine ausführlichere Darstellung.

Nach zwölf Jahren im Lokstedter Weg 72 verließ der Chaos Computer Club Anfang 2010 seine bisherige Dezentrale in Hamburg-Eppendorf und zog in die City-Nord nach Hamburg-Winterhude. In der ehemaligen Filiale der Haspa – der wir ja in unserer Vereinsgeschichte bereits verbunden sind :) – am Mexikoring 27 fanden wir ein neues Zuhause. Dort ist zeitgleich auch der – nun als eigener Verein „Chaos Computer Club Hansestadt Hamburg e. V." organisierte – Erfa Hamburg sowie der Attraktor e. V. beheimatet.

Aufgrund der günstigen Lage der Postfiliale 60 am Überseering 17 haben wir dort ein neues Postfach bezogen. Unser bisheriges Fach in der Hauptpost im Hühnerposten geben wir daher auf.

Sämtliche Rufnummern bleiben dagegen unverändert, ebenso die Mailadressen der Mitglieder- und Abonnementverwaltung.

Postalisch erreicht Ihr uns demnach künftig via

Chaos Computer Club e. V.
Postfach 60 04 80
22204 Hamburg

Besuchen könnt Ihr unseren Erfa Hamburg hingegen jeden zweiten bis fünften Dienstag im Monat im

Mexikoring 21
22297 Hamburg

mit der S1 bis Rübenkamp oder mit der U1 oder S3 bis Barmbek. Bis direkt vor die Tür geht es mit dem Bus 26 bzw. 23 von der Bahn bis zur Haltestelle „Dakarweg (Sozialgerichte)". Einfach die Treppe hoch, an der Post vorbei und auf die Chaosknotenfahne am Ende des Ganges zu.

No such number, no such zone?

Andreas Lehner <al@ccc.de>

Für all jene, die nur noch Zahlensalat sehen und sich insbesondere fragen, warum das Postfach eine andere Postleitzahl als die Clubräume haben, obwohl sie nur fünfzig Meter entfernt liegen, hier ein kurzer Exkurs zur Numerierung deutscher Postfachadressen.

Im Rahmen der Zusammenführung der beiden deutschen Postleitzahlensysteme und der Entscheidung für die Einführung einer fünfstelligen Postleitzahl zum 1. Juli 1993 („Fünf ist Trümpf" mit Maskottchen „Rolf") wurde insbesondere dem Wunsch nach einer weitgehenden Automatisierung der Briefverteilung und einer Vorsortierung nach Postgroßempfängern oder Stadtteilen Rechnung getragen.

Die erste Stelle kodiert dabei die Leitzone (meist ein Gebiet mit einem Verkehrsflughafen), die ersten beiden Stellen die sogenannte Leitregion. Dort ist in den meisten Fällen ein Briefzentrum zur Weiterverteilung angesiedelt (einige Zentren bedienen mehrere Leitregionen).

Innerhalb dieses Nummernraumes gibt es dann die Leitbereiche, das sind Nummernbereiche für einzelne Orte oder Stadtteile. Die niedrigsten Nummern darin sind für Postfächer, die höchsten für Zustellbezirke vorgesehen. Dazwischen gibt es variabel viel Platz für Großempfänger, je nach Bevölkerungsdichte und Wirtschaftsleistung um 1991/92. Die überwiegende Zahl der Postleitzahlen ist als Reserve vorgehalten.

Durch dieses System können Postfachschränke nach Bedarf eröffnet werden. Leider hat der privatisierte Gilb derzeit das Gegenteil, also die Reduktion der Filialen, vor. Nach momentanem Stand der Dinge wird es wohl zum Jahresende eine Übertragung der Filialen von den Gelben auf die Blauen, also zur Postbank, geben. Zeitgleich wird versucht, durch Verkaufsschalter in Supermärkten die Grundversorgung trotz Filialabbaus zu halten. Vermutlich wird es eine Konzentration von bestehenden Schrankanlagen in Postbankfilialen geben.

Bislang jedoch ist durch die Postfachnummer eindeutig gekennzeichnet, um welches Fach es sich handelt – selbst wenn der Absender die Postleitzahl des Zustellbezirkes verwenden sollte.

Durch die Aufteilung der Postfachnummer in Zweiergruppen von rechts wird das deutlich. Das Schema hierbei ist [X]Y MM NN, wobei NN die Postfachnummer (hier: 80, Indikator für die verwendete Schrankanlage), MM die Schranknummer (hier: 4, mit führender Null geschrieben) und XY die Filialkennzahl (hier 60, Überseering 17) ist. Im Ergebnis also „60 04 80".

Für unser bisheriges Fach ist das Fach 45 im Schrank 22 in der Filiale 10, also „10 22 45".

Ich sammele im Übrigen seit vielen Jahren Photos von Schrankanlagen und freue mich – ähnlich wie die 2600 über Telefonzellenbilder – über Zusendungen. ;)

Angriffe auf sichere Hardwarelösungen

von Petr Hanáček, Martin Drahanský, Filip Orság

Was haben die eGK, der elektronische Personalausweis, Telefon-, SIM- und Geldkarten gemein? Die auffälligen Kontakte verraten es: Im Innern verbirgt sich eine Smart Card, die vertrauliche Daten vertraulich und geheime Algorithmen verborgen halten soll. Game On!

Als sichere Hardware [1], [2] wird ein gesichertes Modul bezeichnet, das normalerweise einen Mikrokontroller enthält, in dessen Speicher Daten und Algorithmen mit einer (oder auch ohne) Sicherheitseinstufung abgelegt sind.

Sichere Geräte können zu mehreren Zwecken dienen. Einerseits handelt es sich um sichere Speicherplätze für empfindliche kryptographische Daten (Schlüssel, zufällige Daten, Initialisierungsvektoren usw.), andererseits führen sie empfindliche Vorgänge durch, bei denen die Korrektheit gewährleistet werden muß (Berechnung der Kennzeichnungen der Nachrichten, Chiffrierung usw.). Selbstverständlich können beide Funktionen kombiniert werden. Sichere Geräte ermöglichen damit den direkten Zugang zu Informationssystemen und anschließend die Kommunikation zwischen den Computern. Weiterhin dienen diese Systeme als Schlüsselelement zur Erweiterung der sicheren Systeme für die digitale Unterschrift.

Eine sehr populäre Art der sicheren Geräte stellt zur Zeit die Chipkarte (smart card) dar, die für einen sicheren Speicherplatz der empfindlichen Daten gehalten wird. Die Chipkarten bieten gegenwärtig interessante Möglichkeiten in Form eines relativ leistungsfähigen Prozessors direkt in der Karte an, und das alles für einen akzeptablen Preis.

Ist es aber wirklich möglich, die Chipkarten für einen sicheren Speicherplatz für Daten zu betrachten? Der sichere Datenspeicherplatz muß eine wichtige Bedingung erfüllen: Alle innen gespeicherten Daten dürfen auf keinen Fall aus diesem Speicherplatz kopiert werden. Auf den ersten Blick sind die Chipkarten mit dem aktiven Schutz eine gute Lösung. Der Grund ist, daß zur Zeit keine direkte und einfache Möglichkeit besteht, mit der man die Daten „entwenden“ kann. Wenn wir die Möglichkeit des Abhörens der Kommunikation zwischen Lesegeräte und der Zielstation (bzw. eine Hintertür in der Software der Zielstation) vernachlässigen, dann stellt die Chipkarte eine sichere Lösung dar.

Seitenkanäle

Sichere Geräte produzieren jedoch auch unerwünschte Daten, mit denen der Entwickler nicht rechnete. Diese sicherheitsbedrohlichen Wege nennen wir Seitenkanäle (side channels). Als Angreifer sind wir fähig, diese Seitenkanäle abzuhören oder zu überwachen und damit den Zugriff zu den potentiell empfindlichen Daten zu erlangen. In den meisten Fällen ist es aber notwendig, diese Daten einer speziellen Analyse zu unterziehen. Diese ermöglicht eine Ausfilterung der Informationen, welche dann später für die Durchführung eines erfolgreichen Angriffes an den Mechanismus benutzt werden können.

Die Angriffe mittels Seitenkanälen [4], [5], [6] basieren auf der Überwachung der korrekten Aktivität des Gerätes. Allgemein kann man sagen, daß diese Angriffe aus einem einfachen Datensammeln und einer komplizierten nachfolgenden Analyse bestehen. Von diesen

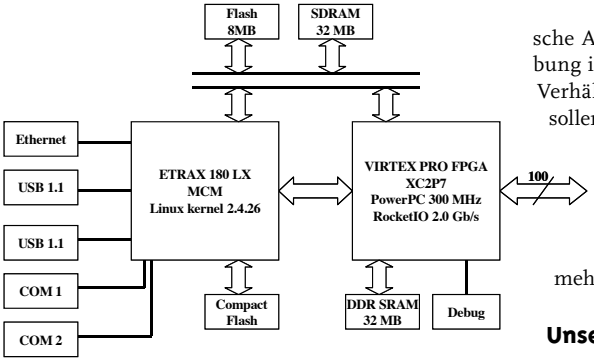


Abb. 1: Der digitale Teil des Geräts SCSAT04.

Angriffen ist vor allem die Leistungsanalyse (power analysis) äußerst interessant. Das Prinzip der Leistungsanalyse gründet sich darauf, daß verschiedene Vorgänge eine unterschiedliche Menge der Transistoren benutzen. Anhand der benutzten Vorgänge ändert sich auch der Verbrauch dieser Transistoren.

Unter Verwendung einfacher Mittel sind wir fähig, die Feinänderungen der Leistungsaufnahme des ganzen Chips zu messen. Diese Angaben können wir zu verschiedenen Zwecken verwenden. Es ist nicht möglich, die Umschaltung eines einzigen Transistors aus der direkten Beobachtung der Leistung festzustellen, trotzdem können wir durch geeignete statistische Operationen auch sehr kleine Leistungsänderungen identifizieren.

Die drei Arten der Leistungsanalyse

• Eine einfache Leistungsanalyse (SPA, simple power analysis) überwacht direkt den Verbrauch des Stroms im System. Mit diesem Verfahren ist es etwa möglich, größere Blöcke der Instruktionen zu identifizieren, die sich z. B. wiederholen. Bei einer höheren Auflösung können sogar einzelne Instruktionen erkannt werden.

• Die Differentialleistungsanalyse (DPA, differential power analysis) ist ein leistungsfähigerer Angriff als SPA, der schwieriger verhindert werden kann. SPA-Angriffe benutzen primär eine Durchsuchung der für die Identifizierung relevanten Leistungsänderungen, im Gegensatz dazu benutzen die DPA-Angriffe statistische Analysen und Techniken für Fehlerbehebung in den erhaltenen Informationen, die ein Verhältnis zu den privaten Schlüsseln haben sollen.

• Die Differentialleistungsanalyse einer höheren Ordnung (HO-DPA, high-order differential power analysis) benutzt eine Informationskorrelation einer höheren Ordnung unter mehreren kryptographischen Operationen.

Unsere Lösung SCSAT04

Unsere Hardwarelösung SCSAT04 ist ein Laborgerät, das die oben genannten Angriffe ermöglicht. Mittels dieses Gerätes können die experimentellen Daten für nachfolgende Leistungsanalyse/Modellierung erlangt werden. Weil das Prinzip der Leistungsanalyse auf der Tatsache basiert ist, daß verschiedene Firmware-Operationen des sicheren Gerätes unterschiedliche Menge der Transistoren benutzen, ist es notwendig, die Änderungen in der Leistungsaufnahme des Chips ziemlich präzise und schnell zu messen.

Nach gründlicher Überlegung aller Anforderungen wurde das SCSAT04-Gerät mit folgenden Parametern entworfen:

• Das Gerät generiert vordefinierte Impulssequenzen (data glitch generator) in zwei unabhängigen Kanälen mit einer Frequenz bis zu 50 MHz und einer Spannung bis zu 24 V.

• Es enthält acht Duplex-Datenkanäle, die mit den Spannungsniveaus +5 V/+3.3 V kompatibel sind.

• Der power glitch generator wirkt als Speiseschaltung +5 V/+3.3 V mit der maximalen Abnahme von 150 mA.

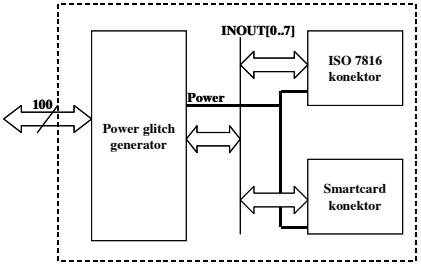
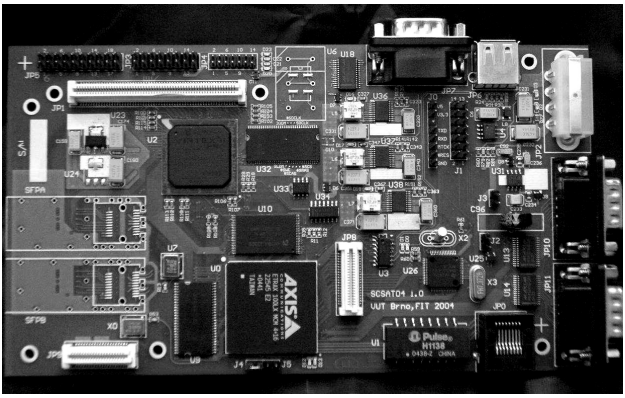


Abb. 2: Der analoge Teil des Geräts SCSAT04.

- Der Dateneingang ist durch die Datenmusterung aus dem Datenkanal mit der Geschwindigkeit 200 Msps und der Musterung des Verbrauches aus der Speiseschaltung mit der Geschwindigkeit 200 Msps mit der effektiven Auflösung 10 Bits realisiert.
- Der Speicher für gemusterte Daten hat eine Kapazität von 32 MB, wobei es sich um 400 MHz DDR-SDRAM handelt.
- Die Kommunikation mit dem System, das die gemessenen Daten bearbeitet, erfolgt durch die Schnittstelle 10/100 Mbit Ethernet, USB 1.1 und RS232.



Das Gerät SCSAT04 ist in zwei autonome Teile gegliedert. Der digitale Teil des Geräts enthält das autonome Modul ETRAX mit dem Betriebssystem Linux, das für die Verbindung mit der Außenwelt verantwortlich ist. Für die Durchführung der Messungen enthält SCSAT04 den Chip VIRTEX PRO, zu dem der Prozessor PowerPC und das Torfeld FPGA angeschlossen sind.

Der analoge Teil des Geräts enthält den power glitch generator, den data glitch generator, die Datenschnittstelle und zwei Stecker, einen für die Chipkreditkarte (ISO 7810-7816 [3]) und den anderen für einen allgemeinen sicheren Mikrokontroller.

Zusammenfassung

Die Verwendung von sicherer Hardware ist zur Zeit ein unerläßlicher Bestandteil aller Lösungen im IT-Bereich, wo mit empfindlichen Daten gearbeitet oder wo die Identitätsverifizierung der Kommunikationspartner gefordert wird. Das entwickelte Gerät SCSAT04, das die Beobachtung und Speicherung des Leistungsverbrauches eines Mikroprozessors eines sicheren Geräts ermöglicht, bietet uns die Chance, zu objektiven Informationen über die Sicherheit aller im Moment benutzten Lösungen zu kommen.

Durch die anschließende Analyse der daraus resultierenden Mängel auf der theoretischen Ebene kann man Folgerungen ableiten, die sich in der Konzeption neuer Hardware und Software für gesicherte Lösungen bemerkbar machen sollen.

[1] ISO/IEC 15408, Information technology – Security techniques – Evaluation criteria for IT security.
[2] Security Requirements for Cryptographic Modules, FIPS PUB 140-1, Federal Information Processing Standards Publication, National Institute of Standards and Technology, U. S. Department of Commerce, January 11, 1994.
[3] ISO/IEC 7816, Identification cards – Integrated circuit(s) cards with contacts, 1998, International Organization for Standardization, Switzerland.
[4] Hanáček P., Peringer P., Rábová Z.: Využití modelů při analýze bezpečnosti kryptografických modulů (Verwendung von Modellen bei Sicherheitsanalyse der kryptographischen Modulen), In: NETSS2004, Ostrava, CZ, MARQ, 2004, s. 115-120, ISBN 80-85988-92-5.
[5] Hanáček P., Peringer P., Rábová Z.: Analýza simulačních dat získaných z kryptografického modulu (Analyse der Simulationsdaten aus einem kryptographischen Modul), In: Proceedings of ASIS 2004, Ostrava, CZ, MARQ, 2004, S. 6, ISBN 80-86840-03.
[6] Hanáček P., Peringer P., Rábová Z.: Získávání vstupních dat pro modely bezpečnosti (Gewinnung der Eingangsdaten für Sicherheitsmodelle), In: Proceedings of ASIS 2005, Ostrava, CZ, MARQ, 2005, S. 68-73, ISBN 80-86840-16-6.

Plastekarten im Nacktscanner

von Björn Heller <tec@hellercom.de> und
Dexter <philipp-maier@runningserver.com>

Auch schon mal zusätzliche Sicherheit für den eigenen PayPal/Ebay-Account gewünscht? Dies ist seit geraumer Zeit mit dem „PayPal Sicherheitsschlüssel“ möglich. Uns hat interessiert, was dahinter steckt und was es mit diesem neuen Spielzeug auf sich hat.

PayPal bietet nun also einen zusätzlichen Sicherheitsmechanismus in Form eines Token an, der bisher als kleiner und kompakter Schlüsselanhänger bestellt werden konnte. Entwickelt wurde er von InCard Technologies [2] in Zusammenarbeit mit den Firmen NagraID [3], nCryptone [4], SmartDisplayer [5] und SiPix [6].

Der Kontoinhaber loggt sich zunächst ganz normal mit Benutzernamen – also seiner E-Mail-Adresse – und Paßwort ein. Im nächsten Schritt wird er gebeten, den Taster an seinem Token zu drücken. Auf diesem wird dann für dreißig Sekunden eine sechsstellige Zahl angezeigt, die er eingeben muß, um endgültig für diese Sitzung an seinen PayPal-Account zu gelangen. Der Schlüssel verfällt nach dreißig Sekunden. Mit anderen Worten: Selbst wenn jemand mit einer Phishing-Mail erfolgreich Benutzernamen und Paßwort entwendet, kommt er ohne das Token nicht an das PayPal-Konto heran, es sei denn, er leitet die Login-Session direkt ein.

Diese kleinen grauen eToken (Digipass Go 3) von VASCO[1] beinhalten eine Echtzeituhr und unterstützen DES und 3DES als Verschlüsselungsarten. Sie sollen bei normalem Gebrauch eine Batterie-Lebensdauer von ca. fünf Jahren haben. Als ich mir einen neuen bestellte, mußte ich allerdings feststellen, daß PayPal mittlerweile von dieser Art Token abgekommen scheint.

Der Token kommt in der Form einer „ISO 7816 ID1“-Karte daher und beinhaltet interessante Technologien wie z. B. ein ePaper-Display. Hält man die Karte gegen eine helle Lampe, zeichnet sich schemenhaft sein Innenleben ab: Besonders gut zu erkennen sind die Batterie, der Elektronikteil und eine halbkreisförmige Linie unten rechts. Irgendwie erinnerte uns diese Linie an eine kleine RFID-Antenne, und so ist es auch. Von PayPal unerwähnt verbirgt sich in der „Super Smart-Card“ ein „Mifare ultralight“-Tag, welcher 512 Byte Speicher beinhaltet und in 16 Bänken von je vier Byte organisiert ist. Die dritte Bank ist hierbei nur einmal programmierbar, und die ersten 2,5 Bänke sind read-only.

Nach dem Auslesen mit einem RFID-Reader wurde allerdings schnell klar, daß auf dem Tag nichts gespeichert ist, außer dessen eindeutige Seriennummer.

```
04 4a e0 26  00000100 01001010 11100000 00100110  .J.&
f9 8f 22 80  11111001 10001111 00100010 10000000  ..„.
d4 48 00 00  11010100 01001000 00000000 00000000  .H..
00 00 00 00  00000000 00000000 00000000 00000000  ....
ff ff ff ff  11111111 11111111 11111111 11111111  ....
00 00 00 00  00000000 00000000 00000000 00000000  ....
00 00 00 00  00000000 00000000 00000000 00000000  ....
00 00 00 00  00000000 00000000 00000000 00000000  ....
00 00 00 00  00000000 00000000 00000000 00000000  ....
00 00 00 00  00000000 00000000 00000000 00000000  ....
00 00 00 00  00000000 00000000 00000000 00000000  ....
00 00 00 00  00000000 00000000 00000000 00000000  ....
00 00 00 00  00000000 00000000 00000000 00000000  ....
00 00 00 00  00000000 00000000 00000000 00000000  ....
00 00 00 00  00000000 00000000 00000000 00000000  ....
```

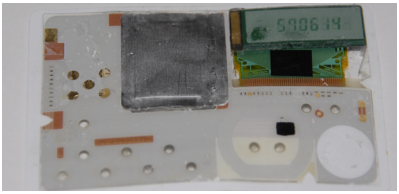
Dump der Karte

Die Frage, ob der Chip von PayPal für einen zukünftigen Gebrauch vorgesehen ist, konnte bisher noch nicht beantwortet werden. Bis zum Redaktionsschluß lag uns keine schriftliche Stellungnahme von PayPal vor. Was bleibt, ist der fade Beigeschmack, nicht darüber informiert worden zu sein.

Um nun die weiteren Innereien der Karte zu ergründen, bot es sich an, den Kunststoff der Karte aufzulösen. Hierfür eignet sich Aceton aus dem Baumarkt ganz hervorragend.

Die Karte wurde auf einen Keramikteller gelegt und mit Aceton (siehe auch den nächsten Artikel) benetzt. Man kann dann quasi verfolgen, wie sich der Kunststoff langsam an- und dann auflöst.

Man kann ein wenig mit einem Schraubendreher kratzend nachhelfen, und die Kunststoffstücke lassen sich prima abziehen. Möchte man die Karte in funktionsfähigem Zustand erhalten, sollte man vorsichtig sein, um nicht die Leiterbahnen zu durchtrennen. Ist der Kunststoff erstmal beseitigt, offenbaren sich einem die inneren Werte der Karte.

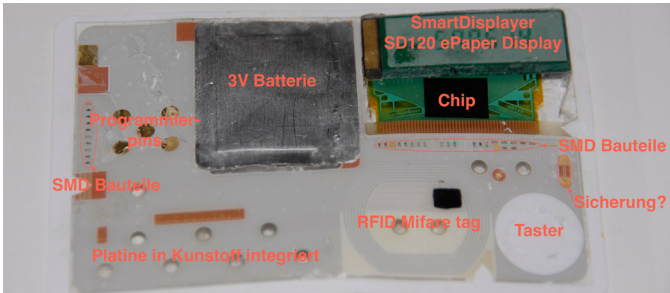


Gleich sehr gut zu erkennen ist der auf flexibler Leiterplatte aufgebrachte µController unter dem Display und die verschweißte Batterie mit einer Spannung von drei Volt. Danach fällt der Blick gleich auf den RFID-Chip samt Antenne im unteren rechten Teil der Karte. Auf der linken Seite sind fünf vergoldete Kontakte zum Programmieren der Karte zu sehen. Dies sind aber nicht die einzigen Kontakte, es finden sich noch drei weitere auf der Kartenrückseite.

Der Knopf für das Erneuern des Schlüssels auf dem Display ist als simpler Folientaster ausgeführt. Schaut man sich die Kunststoff-Leiterplatte etwas genauer an, so erkennt man einmal unter dem µController und am linken Rand kleine SMD-Bauteile der Schaltung. Unter dem ePaper-Display befindet sich auf der flexiblen Leiterplatte noch der Aufdruck „SmartDisplayer“, „SD120“ .

Abschließend bleibt zu sagen, daß wir vorhaben, uns weiter mit dieser Karte zu beschäftigen, um die Funktionsweise noch besser zu verstehen.

[1] *http://www.vasco.com/products/digipass/digipass_go_range/digipass_go3.aspx*
[2] *http://www.incard.com/products-ictkey.html*
[3] *http://www.nagraid.com/*
[4] *http://openauthentication.org/members/ncryptone*
[5] *http://smartdisplayer.com/*
[6] *http://www.sipix.com/*



All Chips Reversed

Martin Schobert <martin@weltregierung.de>

Im Dezember 2007 veröffentlichten Karsten Nohl und Henryk Plötz ihre Forschungsergebnisse über die Sicherheit des RFID-Systems Mifare Classic auf dem 24. Chaos Communication Congress [14, 15]. Sie gewannen ihre Erkenntnisse über die Funktionsweise des Algorithmus Crypto1 durch Reverse-Engineering von Protokolldaten und der Integrierten Schaltkreise (IC), die auf RFID-Transpondern vom Typ Mifare Classic eingebettet sind. Die im Vortrag dargstellten Erkenntnisse zeigen, daß für eine Analyse einfacher Schaltkreise „Küchentechnik" genügt. Crypto1 wird unter anderem für Zugangskontrollen und Bezahlsysteme verwendet.

Der Bedarf an professioneller IC-Analyse ist groß. Jeder Hersteller von Integrierten Schaltkreisen benötigt dafür entsprechende Verfahren. Die Laboratorien verfügen über Werkzeuge, z. B. um festzustellen, warum Prototypen nicht funktionieren. Auch anderen Anwendungszwecken dienen diese Analysen. Die folgenden Beispiele sollen dies zeigen.

Einige Firmen, z. B. die kanadische Firma Chipworks [7], untersuchen Halbleiterbausteine und Mikroelektronik, um Auftraggeber über Technologien der Konkurrenz in Kenntnis zu setzen. Im Falle von Patentverletzungen haben die Auftraggeber damit Material in der Hand, um gegen die Konkurrenz juristisch vorzugehen. Detaillierte Informationen über Technologien helfen, Produkte unter Einsparung eigener Forschungsmittel zu verbessern.

Im Bereich der „nationalen Sicherheit" besteht ebenfalls Bedarf an der Analyse Integrierter Schaltkreise. Militärische, nachrichtendienstliche und diplomatische Einrichtungen, die beispielsweise Chiffriertechnik oder hochtechnische Waffensysteme aus anderen Ländern einkaufen, haben ein Interesse an „hintertürfreier" Hardware. Dahingehende Modifikationen können analysiert werden, auch wenn das einen größeren Aufwand darstellt. [1,10,24]

Ein Projekt, das die US-amerikanische Defense Logistics Agency finanziert, ist das Advanced Microcircuit Emulation Program. Dabei geht es u. a. darum, Baupläne aus undokumentierten anwendungsspezifischen Schaltkreisen (ASICS) zurückzugewinnen. Anhand derer können Schaltkreise nachgebaut werden, wenn z. B. der ursprüngliche Hersteller nicht mehr existiert. [1]

Den genannten Beispielen ist gemein, daß hinter den Programmen finanzstarke Institutionen stehen. Diese können Integrierte Schaltkreise analysieren – zur Fehlersuche, um etwas über die Fähigkeiten der Konkurrenz zu erfahren, um Manipulationen festzustellen oder „auszuschließen", um Sicherheitslöcher aufzuspüren, um geheime Chiffrierschlüssel aus Speichern auszulesen und dergleichen. Je nach Fragestellung kosten kommerzielle Chipanalysen fünf- bis sechsstellige Beträge.

Auf der anderen Seite können IC-Analysen mit einfachen Mitteln durchgeführt werden. Beispielsweise war das Reverse Engineering von Crypto1 ohne ein teures Labor mit einem zusammengerechneten Zeitaufwand in weniger als zwei Mannmonaten möglich. Mit einem fiktiven Tagessatz von 500 Euro wäre der Verschlüsselungsalgorithmus für etwa 30.000 Euro Kosten extrahiert. Mit den Erfahrungen aus dem Projekt wäre ein erneutes Reverse-Engineering von Crypto1 sogar in wenigen Tagen ohne nennenswerte Kosten möglich.

Im Rahmen des Mifare-Hacks entstand der Wunsch, das Reverse-Engineering von Integrierten Schaltkreisen werkzeuggestützt zu vereinfachen. Zu diesem Zweck wurde eine Software namens *degate* entwickelt.

Dieser Text soll die Hintergründe des Reverse-Engineerings von Integrierten Schaltkreisen beleuchten und beschreiben, wie man Schaltfunktionen von Logikgattern aus IC rekonstruieren kann.

Motivation

Die Sicherheit des Verschlüsselungsverfahrens Crypto1 basiert auf dem Prinzip **security by obscurity**, d. h. auf der Geheimhaltung des Verfahrens und weniger auf der Geheimhaltung der Schlüssel. Damit verletzt es Kerckhoffs' Prinzip, welches besagt, daß die Sicherheit eines Systems nicht auf der Geheimhaltung des Verfahrens basieren darf. Üblicherweise ist die Geheimhaltung eines Verfahrens schwieriger als die von Schlüsseln zu gewährleisten. Im Falle einer Offenlegung läßt sich ein Verfahren nicht so leicht austauschen wie Chiffrierschlüssel. Das Kerckhoffs'sche Prinzip wurde bereits 1883 aufgestellt. Allerdings wird es in der Praxis oftmals ignoriert. [21]

Wären regelmäßig hardwareimplementierte Verschlüsselungsverfahren einer Low-Cost-Analyse unterzogen, müßte sich zwangsläufig das Sicherheitsniveau der Verfahren erhöhen. Kryptosysteme, deren Umgehung n Euro kosten, können keine Geheimnisse schützen, deren Umgehung n Euro Gewinn einbringt. Wenn die Umgehungskosten sinken, genügt es nicht mehr, ein potentiell knackbares Verschlüsselungsverfahren zu verwenden, dessen Sicherheit darin besteht, daß es niemand kennt.

Neben dem bei „Mifare Classic" verwendeten sind auch andere Verschlüsselungsverfahren von der Problematik **Security by obscurity** betroffen. Dazu zählen beispielsweise die proprietären RFID-Systeme „Legic prime" und „Felica" sowie das Verschlüsselungsverfahren „DECT Standard Cipher" (DSC), das Kommunikation zwischen „Schnurlostelefonen" und deren Basisstation gegen unbefugtes Abhören sichern soll. Ebenfalls ist der Eurochip-Algorithmus geheim. Dies ist ein Challenge-Response-Verfahren, mit dem Kartentelefone die Echtheit der Telefonkarten verifizieren. Der Algorithmus wurde in den 1990er Jahren eingeführt, nachdem es zu viele Betrugsfälle mit Telefonkarten-Emulatoren gab. [23]

„Legic prime" und der DSC sind seit dem 26. Chaos Communication Congress der Öffentlichkeit bekannt und gelten mittlerweile als unsicher. Die Verschlüsselungsalgorithmen wurden mittels Firmware-, Protokoll- und Chip-Reverse-Engineering ermittelt. [16, 25]

Das Enthüllen von proprietären Verschlüsselungsalgorithmen ist die hauptsächliche Motivation dafür, ein Verfahren zu entwickeln, mit der sich kostengünstig Analysen von Chips durchführen lassen. Kostengünstig bedeutet, daß für die Anschaffung aller notwendigen Geräte keine höheren Kosten als etwa 1.000 bis 10.000 Euro entstehen.

Zahlreiche IT-sicherheitsrelevante Themen sind seit den 1980er Jahren in den Fokus der zivilen Forschung gerückt, beispielsweise Betriebssysteme, Server-Software und Kryptographie. Dies hat maßgeblich zur Verbesserung von Sicherheitsstandards beigetragen. Sicherheitsstandards im Bereich Integrierter Schaltungen werden zwar ebenfalls besser, insbesondere bei smart cards, es gibt aber nach wie vor fast keine öffentliche Sicherheitsforschung im Bereich Integrierter Schaltkreise. Dies ist insbesondere daran feststellbar, daß es nur sehr wenige Aufsätze gibt, die speziell Reverse-Engineering von (Logik-)Schaltkreisen behandeln und diese de facto keine Details preisgeben.

Entwickler sicherheitsrelevanter Systeme überlegen sich zumeist, gegen welche Kategorien von Angreifern sie das System schützen wollen. Diese Kategorien orientieren sich i. d. R. an potentiellen Budgetgrößen, die den Angreifern zur Verfügung stehen. Die Bewertung von Budgetgrößen sollte jedoch kritisch betrachtet werden.

Der Arbeitsablauf im Überblick

Ausgangspunkt für die Untersuchung von Integierten Schaltkreisen sind Chips. Diese müssen zunächst entkapselt werden, um ein Plättchen aus Halbleitermaterial (engl. *die*) zu erhalten. IC bestehen aus mehreren Schichten. Diese Schichten müssen Stück für Stück entfernt werden, um darunterliegende Schichten freizulegen. Jede Schicht wird fotographiert. Dabei entstehende Teilbilder werden zusammengesetzt. Die Fotographien der einzelnen Schichten müssen in Übereinstimmung gebracht werden, so daß man später den Verlauf von Leiterbahnen über mehrere Schichten hinweg nachvollziehen kann.

Ich gehe davon aus, daß ein Chip-Layout überwiegend auf Standardzellen basiert. Diese Annahme ist statthaft, denn sie trifft auf den überwiegenden Teil von anwendungsspezifischen IC zu. Zunächst wird die Bildrepräsentation von Standardzellen ermittelt. Die verschiedenen Instanzen von Standardzellen werden identifiziert. Anschließend wird deren Verdrahtung nachvollzogen. Man muß die Schaltfunktion der Standardzelltypen analysieren. Diese ergibt sich, wenn man die Verschaltung der einzelnen Transistoren auswertet.

Wenn diese Informationen ermittelt sind, kann man sich der Analyse auf „höherer Ebene" zuwenden. Bei der eingangs genannten Motivation, proprietäre Verschlüsselungsverfahren zu extrahieren, ist nie ein vollständiges Reverse-Engineering des gesamten Chips notwendig. Es genügt, sich auf relevante Bereiche zu konzentrieren. Dieser Text geht ebenfalls darauf ein, wie man diese relevanten Bereiche identifizieren kann.

Thematische Einschränkung

Das Reverse-Engineering von Integrierten Schaltkreisen ist ein beliebig komplexes Thema und umfaßt konkrete Technologieaufklärung, etwa das Design von Flashspeichern, das optische Auslesen von Masken-ROMs, den vollständigen Nachbau von IC oder das Auslesen von Speicherinhalten mittels Microprobing. Ebenfalls gehören invasive Angriffe in das Themenfeld, bei denen Strukturen auf einem Chip gezielt modifiziert werden, z. B. um Sicherungen zu deaktivieren, die ein Auslesen von Speichern verhindern sollen.

Der Schwerpunkt dieses Textes ist die statische Analyse von CMOS-basierten (digitalen) Logik-Schaltkreisen mit der Motivation, proprietäre Verschlüsselungsverfahren zu rekonstruieren. Die Analyse soll mit geringem Budget möglich sein.

Aufwand und Kosten

Der Reverse-Engineering-Prozess läßt sich grob in drei Abschnitte unterteilen: die Entkapelsung, die Bildgewinnung und die Analyse der Schaltkreise. Jeder dieser Schritte kann bei externen Dienstleistern in Auftrag gegeben werden. Während eine Chip-Entkapselung im Labor im Wesentlichen eine Finanzierung des reinen Arbeitsaufwandes darstellt, sind darüber hinausgehende Analysen bei spezialisierten Firmen zumeist teuer. Diese Kosten können eingespart werden, wenn man die Analyse selbst durchführt.

Chip (analysierter Teil)	Anzahl Zelltypen	Anzahl Zellen	Verbindungen
NXP Mifare Classic	40-70	600	1500
Legic prime	25	600	2100
DSC im SC14421CVF	26	300	1000

Komplexität des Reverse-Engineerings

Diese Tabelle gibt einen Überblick über die Komplexität des Reverse-Engineerings ausgewählter Integrierter Schaltkreise, bei der jeweils das Verschlüsselungsverfahren extrahiert wurde. Der Zeitaufwand für das Ermitteln der Zelltypen und jeweils deren Funktion beträgt etwa drei Tage und ist überwiegend von der Übung des Analysten abhängig. 300 bis 600 Plazierungen von Standardzellen kann man in maximal einer Woche halbautomatisiert ausfindig machen. Das manuelle Nachvollziehen von Leiterbahnen ist der aufwendigste Teil und dauert ein bis zwei Wochen. Die letzten beiden zeitintensiven Schritte können schneller umgesetzt werden, wenn deren Automati-

sierungsgrad höher ist. Eine weitere Verkürzung der Gesamtdauer ist durch kollaboratives Reverse-Engineering zu erreichen.

Die in der Einleitung veranschlagten 1.000 bis 10.000 Euro entfallen im Wesentlichen auf die Posten Mikroskop und Poliermaschine. Dabei handelt es sich um Einmalkosten, die eventuell vermeidbar sind. Poliermaschinen findet man z. B. in Geologie- oder Optik-Instituten, Mikroskope mit Digitalkameras in nahezu jeder materialwissenschaftlichen Einrichtung. Ein Labor mit Rauchabzug ist für die chemische Entkapselung mit konzentrierten Säuren notwendig. Wenn man ein Auftragslabor für die Entkapselung zur Hand hat, benötigt man dies nicht.

Entkapselung

Integrierte Schaltkreise werden je nach Anwendungsfall in verschiedenen Gehäusematerialien verpackt. Meistens handelt es sich um Epoxidverbindungen, Keramik oder Metall. Die hier beschriebene Methode bezieht sich auf die Entfernung von Epoxidverbindungen.

Epoxidverbindungen gehören zu den Duroplasten und zeichnen sich durch hohe chemische und mechanische Beständigkeit aus. Epoxide lassen sich nicht aufquellen und hauptsächlich nur durch aggressive Säuren oxidativ zersetzen. Der Anteil an Epoxiden in diesen Kunststoffgehäusen beträgt aber lediglich 20 bis 25 Prozent. Mit zwei Dritteln bilden Quarzmehl und Glasfasern den überwiegenden Anteil. [8]

In der Literatur werden zwei Fälle unterschieden: Mitunter wird nicht das gesamte Gehäuse entfernt, sondern lediglich das Gehäusematerial, welches über dem Siliziumplättchen ist, wenn die Funktionalität des Chips erhalten werden soll, insbesondere um den IC noch in einer Schaltung zu betreiben. Der andere Fall ist die Komplettentfernung des Gehäusematerials. Dieser Weg wird hier eingeschlagen. Durch das Herunterpolieren der einzelnen Schichten wird der Chip zerstört. Der Nachteil besteht darin, daß man die Bedeutung der *bond pads*, d. h. der Flächen auf dem Halbleiterplättchen, an denen die Leiterbahnen von den Pins des Chips befestigt sind, ggf. manuell ermitteln werden muß.

Bei einer chemischen Entkapselung sollten mit jedem Durchgang mehrere Chips des gleichen Typs behandelt werden, damit bei mißlungenem Politurvorgang noch Ersatzchips übrig sind.

Eine nahezu vollständige Beschreibung verschiedener Entkapselungsverfahren gibt Friedrich Beck. [3]

Aufquellen von Thermoplasten

Vergleichsweise ungefährlich ist das Aufquellen von Thermoplasten. Hersteller von Chipkarten (Telefonkarten, Mensa-Karten, Zugangskarten, usw.) benutzen Thermoplaste, um den Chip einzubetten. Thermoplaste lassen sich mit Aceton aus dem Baumarkt aufquellen. Der Prozeß dauert etwa zehn bis zwanzig Minuten. Das Material verliert dabei an Stabilität. Der Chip fällt dann heraus.

In Thermoplaste eingebettete Chips sind meist in einer weiteren Ummantelung aus Epoxid verpackt. In diesem Fall ist eine Behandlung mit Säuren unumgänglich.

Entfernen von Thermoplasten mittels Aceton

Chip-Entkapselung in der Industrie

Für die Entfernung von Epoxiden kann rauchende Salpetersäure [11, 22] oder konzentrierte Schwefelsäure [6] verwendet werden. In eini-

gen Anwendungsfällen wird eine Mischung aus konzentrierter Salpetersäure und konzentrierter Schwefelsäure benutzt. Das soll für einige Verpackungsmaterialien die Reaktion beschleunigen und das Silber in den *bond pads* schonen.

Nick Chernyy beschreibt seine Methode in [6] wie folgt. Die Chips werden in ein Becherglas (40 ml) gelegt. Konzentrierte Schwefelsäure wird dazugegeben bis die Chips vollständig bedeckt sind. Erste Lösungserscheinungen sind sofort bemerkbar. Das Becherglas wird unter einem Rauchabzug erhitzt, um die Aktivität der Säure zu erhöhen. Die Temperatur ist unkritisch, etwa 60°C bis 90°C genügen. Die Siliziumscheibchen im Chip vertragen viel höhere Temperaturen und sind mit der Säuremethode praktisch nicht zerstörbar. Nach etwa zwanzig Minuten sollte der Kunststoffanteil zersetzt sein. Er bleibt als mehr oder weniger schwarze Flüssigkeit bzw. als Schaum im Becherglas zurück.

In ein zweites Becherglas (500 ml) werden 400 ml Wasser gegeben. Der Inhalt des ersten Becherglases wird vorsichtig in das zweite Becherglas gefüllt. Das Mischen von Wasser und Säuren ist bekanntlich exotherm und führt bei Fehlanwendung zu Unfällen!

In ein drittes Becherglas (1000 ml) werden 400 ml Wasser gegeben. Der Inhalt des 500-ml-Becherglases wird vorsichtig in das Literglas gegossen, so daß die Siliziumplättchen mit anhaftenden Metallteilen im 500-ml-Becherglas verbleiben. Die Siliziumplättchen werden mit Wasser gereinigt, so daß keine Säure und kein Schmutz mehr anhaftet.

In einigen Fällen kann es passieren, daß die Kunststoffummantelung nicht vollständig entfernt ist. Dann ist eine erneute Behandlung mit Säure notwendig. Saubere Ergebnisse ergeben sich, wenn statt Schwefelsäure konzentrierte Salpetersäure verwendet wird. Die Rückstände sind dann nicht so trübe, daß die Chips im Becherglas nicht mehr sichtbar sind. Mit auf 90°C erhitzter Salpetersäure dauert die Entkapselung nur etwa fünf Minuten.

Das Experiment wurde mit rauchender Salpetersäure (mehr als 99,5%-ige Konzentration) in einem Labor in Auftrag gegeben, um in Epoxidmasse eingeschlossene Chips aus einem RFID-Transponder zu entkapseln. Das Labor berichtete, daß die Reaktion bei Raumtemperatur sofort einsetzte und binnen kürzester Zeit abgeschlossen war.

Wenn das Gehäuse entfernt ist, ist noch eine Behandlung im Ultraschallbad notwendig, um eventuelle Anhaftungen zu entfernen. Dazu stellt man ein mit Aceton gefülltes Becherglas inklusive Chips in einen Ultraschallreiniger. Werden mehrere Chips gleichzeitig gereinigt, sollte die Reinigung nicht länger als eine halbe Minute andauern. Die Chips könnten aneinander reiben und gegenseitig die Oberflächen zerkratzen. Bei Einzelbehandlung dauert die Ultraschallreinigung drei bis fünf Minuten.

Ist keine geeignete Arbeitsumgebung vorhanden, unterläßt man die Entkapselung. Der Umgang mit konzentrierten Säuren ist gefährlich. Der Bedarf an einer geeigneten Arbeitsumgebung ist nicht aus Sicht der Bequemlichkeit zu verstehen. Wenn die Arbeitsumgebung nicht geeignet ist, entstehen zusätzliche Gefahren. Die genannten Säuren sind Standardchemikalien im Labor. Laboratorien verfügen über geeignete Arbeitsumgebungen. Eine Entkapselung im Auftragslabor ist preiswert verglichen damit, daß die Säure sonst selbst beschafft, transportiert, angewendet, gelagert und entsorgt werden müßte. Für weniger als hundert Euro kann man Laboratorien mit der Chip-Entkapselung beauftragen.

Im Ergebnis erhält man den Chip als Plättchen (engl. *die*), an dem meistens noch die Verbindungsdrähte zur Außenwelt hängen. Kleine Chips haben eine Abmessung von etwa einem Quadratmillimeter und eine Stärke von wenigen zehntel Millimetern.

Chip-Entkapselung mittels Kolophonium

Kolophonium nennt man den Rückstand des Baumharzes von Kiefern, bei dem Wasser und

Terpentinöl abdestilliert wurden. Der Aggregatszustand von Kolophonium ist fest. Kolophonium selbst ist ungiftig, wenngleich dessen Dämpfe Allergien auslösen können. Kolophonium wird z. B. als Flußmittel beim Löten, von Musikern zum Behandeln von Geigenbögen oder Gitarrensaiten und von Bergsteigern zur Erhöhung der Haftreibung verwendet. Kolophonium ist billig, leicht zu beschaffen, zu lagern, zu entsorgen und anzuwenden. Es ist ideal, um Chip-Entkapselungen durchzuführen, die keinen Laborstandards genügen.

Friedrich Beck beschreibt eine Möglichkeit zum Enkapseln mittels Kolophonium:

Zum Öffnen wird das Bauteil im Drahtkörbchen in das auf 320 - 360 °C erwärmte Kolophonium getaucht, bis der Chip völlig freiliegt (5 - 10 Minuten); anschließend läßt sich mit trockenem Aceton das anhaftende Kolophonium entfernen. [3]

IC-Entkapselung durch Kochen in Kolophonium

Beck schreibt ferner, daß die Kolophoniumdämpfe Rückstände im Abzug bilden, diesen verunreinigen und schwer zu entfernen sind. Dies sei der Grund, warum das Verfahren selten angewandt wird. Tatsächlich wird dieses Verfahren in aktuellen Quellen nicht mehr beschrieben. Die Zeitangabe von Herrn Beck konnte im Experiment nicht bestätigt werden. Tatsächlich sind die Kochzeiten sehr viel höher. Experimentell konnte jedoch bestäigt werden, daß das Verfahren prinzipiell funktioniert. [20]

Zum Entkapseln nimmt man ein breites, langes und temperaturbeständiges Regagenzglas, fülle es mit Kolophonium und den Chips. Der Inhalt wird – abhängig von der Chipgröße – 30 bis 150 Minuten gekocht. Da das Halbleiterplättchen hohe Temperaturen verträgt, ist die Kochzeit unkritisch.

Reinigung der Halbleiterplättchen im Ultraschallreiniger

Den Inhalt des Reagenzglases läßt man anschließend auf Zimmertemperatur abkühlen, so daß das Kolophonium erstarrt. Man gibt dann etwa 10 ml Aceton oder Isopropanol (technische Reinheit genügt) in das Reagenzglas. Diese Chemikalien lösen das Kolophonium. Dieser Vorgang läßt sich durch Ultraschalleinwirkung erheblich beschleunigen.

Den gelösten Reagenzglasinhalt filtriert man. Das Halbleiterplättchen bleibt fast immer im Reagenzglas haften. Mittels mehrfachem Nachspülen mit Aceton oder mit einem Holzstäbchen kann man das Plättchen vorsichtig aus dem Reagenzglas befördern.

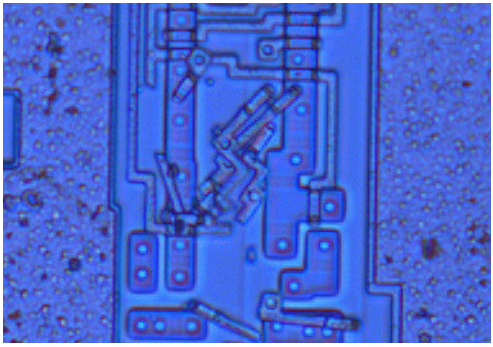
Anschließend sollte das Plättchen in einem oder mehreren Reinigungsgängen von anhaftenden Kolophonium- und Expoxidresten mittels Ultraschall befreit werden.

Bei dieser Form der Chip-Entkapselung entfallen die Probleme, wie sie sich im Umgang mit konzentrierten Säuren ergeben. Dennoch ist davon auszugehen, daß der Entkapselungsprozeß gesundheitsgefährdend ist. Die Verwendung von Schutzbrillen ist hier unumgänglich, denn Kolophonium neigt zum Spritzen.

Mit etwa vierzig Prozent ist Abietinsäure der wirksame Hauptbestandteil von Kolophonium. Abietinsäure hat ähnliche Konsistenzeigenschaften wie Kolophonium. Sie kann bei ausgewählten Chemikalienhändlern in Reinform erworben werden. Damit ließe sich der Entkapselungsprozeß beschleunigen, was mangels an Privatpersonen liefernden Händlern experimentell bisher nicht bestätigt werden konnte.

Abtragung einzelner Schichten

Integrierte Schaltkreise sind mehrschichtig aufgebaut. Von jeder einzelnen Schicht werden Fotos aufgenommen. Dazu muß jede einzelne Schicht des Chips entfernt werden. Der Integrierte Schaltkreis besteht hauptsächlich aus Siliziumdioxid. Einzelne Schichten lassen sich chemisch oder mechanisch entfernen.

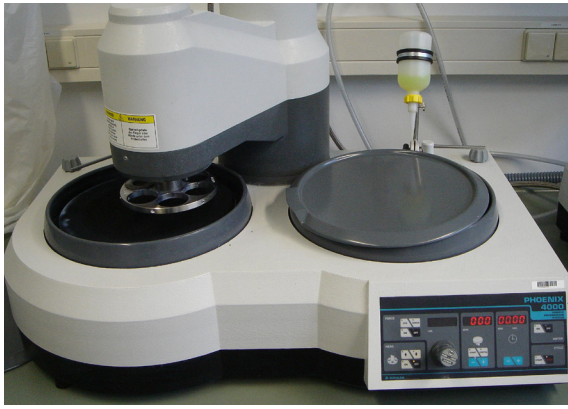


Unterätzung (Foto: starbug)

Die einzige Säure, die Siliziumdioxid angreift, ist die Flußsäure (Fluorwasserstoffsäure, HF). Flußsäure ist geeignet, um die Transistorschicht freizulegen. Der Nachteil besteht darin, daß Flußsäure auf den höheren Schichten zum Unterätzen neigt (siehe Abbildung). Da Flußsäure schwierig zu handhaben ist, wird hier die mechanische Entfernung von Chip-Ebenen bevorzugt.

Für das Polieren von Oberflächen gibt es spezielle Poliermaschinen, beispielsweise das Modell Phoenix 4000 der Firma Buehler GmbH. [5] Mit mehreren tausend Euro ist das Gerät entsprechend teuer. Vergleichbare Geräte findet man an Universitäten in Geologie-Instituten.

Für den Poliervorgang benötigt man etwa 20 ml Poliersuspension mit einer Korngröße von 0,1 µm.



Poliermaschine Phoenix 4000 der Firma Buehler (Foto: starbug)

Der Chip wird mit seiner Grundfläche auf eine Art Stempel geklebt. Dabei muß darauf geachtet werden, daß die Chipoberfläche parallel zur Polieroberfläche verläuft. Anderenfalls ist der Materialabtrag beim Polieren unterschiedlich stark.

Es ist möglich, den Vorgang komplett manuell durchzuführen. Für das Polieren von Glasfaserkabelenden bietet der Fachhandel feinstes Polierpapier. Das ist zwar kostengünstig, der Nachteil besteht jedoch darin, daß sich Verschmierungen auf dem Chip bilden können.

Der Fortschritt des Poliervorgangs muß regelmäßig unter einem Mikroskop kontrolliert werden. Wenn der Materialabtrag unterschiedlich stark ist, gibt es zwei Möglichkeiten. Entweder wird das Bildmaterial durch manuelle Nachbearbeitung korrigiert oder der Poliervorgang mit einem weiteren Chip erneut gestartet.

Bildgewinnung: Mikroskopierung

Für die Aufnahme der Bilddaten benötigt man ein Mikroskop mit einem Kameramodul. Derartige Geräte kann man zwar für wenig Geld erwerben, jedoch ist nicht jedes Gerät geeignet. Für die Aufnahme der Bilddaten des Chiptyps

Mifare Classic wurde ein Labormikroskop vom Typ Olympus BX61 verwendet. [17]

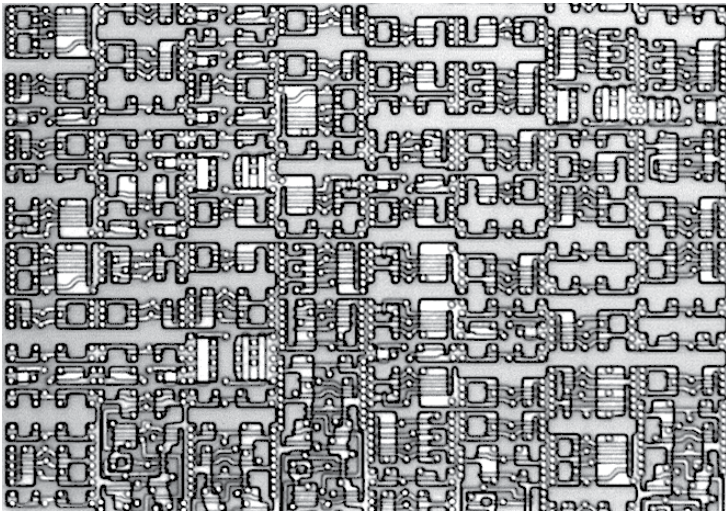
Mikroskop (Foto: starbug)

Das Mikroskop sollte eine 500- bis 2000-fache optische Vergrößerung erreichen. Das trifft in der Regel selbst auf die günstigsten Lichtmikroskope zu, jedoch muß das Objektiv geeignet sein. Umso stärker die Objektivvergrößerung ist, desto kleiner ist der Arbeitsabstand zwischen Objektiv und Objekt.

Die Bilder werden mittels Auflichtmikroskopie gewonnen. Eine externe Lichtquelle beleuchtet die Chipoberfläche. Die Lichtstrahlen reflektieren in das Objektiv. Das Objektiv darf nicht zu nahe am Objekt sein, anderenfalls reflektiert nicht genug Licht. Für die Auflichtmikroskopie werden deshalb spezielle Objektive verkauft, die mit Beleuchtungsmöglichkeiten ausgestattet sind.

Das Mikroskop sollte mit einem XY-Tisch ausgestattet sein. Damit läßt sich die Probe einspannen und verfahren, ohne daß sie sich versehentlich verdreht. Wenn die Bilder mit verschiedenen Drehwinkeln aufgenommen werden, muß dies vor dem Zusammensetzen der Bilddaten (manuell) korrigiert werden. Der Fachhandel bietet Mikroskope mit motorgetriebenen XY-Tischen an. Diese sind im Gesamtpaket mit mehreren tausend Euro jedoch teuer. Die besseren XY-Tische lassen sich drehen. Dadurch kann man die Probe bereits so auf dem Tisch orientieren, daß das Raster auf dem Chip parallel bzw. senkrecht zu den Bildrändern verläuft.

Ein Kameramodul mit zwei oder mehr Megapixeln ist erforderlich. Wenn man keine Mikroskopkamera hat, kann man diese ab etwa zweihundert Euro erwerben. In diesem Zusammenhang ist wichtig, daß sich die optische Gesamtvergrößerung multiplikativ aus der Objektivvergrößerung und der optischen Vergrößerung durch die Kamera ergibt. Für günstige Mikroskopkameras ist oftmals keine optische Vergrößerung angegeben.



Bildausschnitt des Transistor-Layers eines Schaltkreises vom Typ Mifare Classic

Als Strukturgröße in der Halbleitertechnik bezeichnet man die Abmessung der kleinsten anzutreffenden Bauteile. In der CMOS-Technik ist das die kleinste Gate-Länge eines CMOS-Transistors. Für die Analyse der Schaltkreise ist es hier nicht wesentlich, alle Details der Transistoren zu erkennen. Die Abbildung links zeigt Transistoren eines Schaltkreises vom Typ „Mifare Classic“ unter dem Mikroskop bei 500-facher Vergrößerung. „Mifare Classic“ wurde in einer Strukturgröße von etwa 500 nm gefertigt. Die einzelnen CMOS-Transistoren kann man gut erkennen.

Die Grenze der optischen Auflösung bei konventioneller Lichtmikroskopie hängt von der Wellenlänge der Beleuchtung und der Numerischen Apertur des Objektivs ab. Die Grenze liegt etwa bei 350 nm-Halbleiterprozessen. CPUs basierend auf dieser Strukturgröße wurden ab 1995 hergestellt. Zum Vergleich: führende Halbleiterhersteller arbeiten derzeit an der Einführung von 22 nm-Prozessen.

Um jenseits der Auflösungsgrenze operieren zu können, bedarf es anderer Mikroskopiekonzepte. Beispielsweise lassen sich mittels Konfokalmikroskopie oder Rasterelektronenmikroskopie höhere Auflösungen erzielen.

Zusammenfügen und Nachbearbeitung der Bilddaten

Die zu untersuchenden Schaltkreise sind größer als der Bildausschnitt im Mikroskop, Einzelbilder müssen zusammengefügt werden. Manuell kann man dazu Graphikbearbeitungsprogramme verwenden, beispielsweise das GNU Image Manipulation Program (gimp). Für das semiautomatische Zusammensetzen sind sogenannte Stitching-Programme geeignet. Man verwendet diese hauptsächlich zum Zusammensetzen von Fotos zu einer Panoramaaufnahme.

Als gerade so brauchbare freie Software hat sich das Programm „hugin“ erwiesen. Hugin ist die graphische Oberfläche zu den PanoTools. [18] Das kommerzielle Stitching-Programm „PanaVue ImageAssembler 3“ soll ebenfalls gute Ergebnisse beim Zusammensetzen von fotographierten Chipoberflächen liefern. Der „PanaVue ImageAssembler“ ist in Professional- und Enterprise-Edition für Bilddaten bis 100.000 x 100.000 Bildpunkte ausgelegt. Ferner ermöglicht die Software ein automatisiertes Zusammensetzen der Bilddaten, wenn genug Überlappung der Einzelbilder vorhanden ist. [19]

Für das manuelle Zusammensetzen von Chip-Bildern anhand von Referenzpunkten hat Sven Kaden ein Programm geschrieben, das ohne weiteres Parameter-Tuning benutzt werden kann. [9]

Wenn die Bilddaten zusammengesetzt sind, kann es für eine spätere automatisierte Bildanalyse sinnvoll sein, das Bildmaterial zu entrauschen. Dafür ist das quelloffene Werkzeug GREYCstoration geeignet. [26] Es entrauscht Bilddaten, versucht aber, wesentliche Merkmale des Bildes beizubehalten. Insbesondere bleiben dadurch Kanteninformationen erhalten.

Analyse von Integrierten Schaltkreisen anhand von Bilddaten

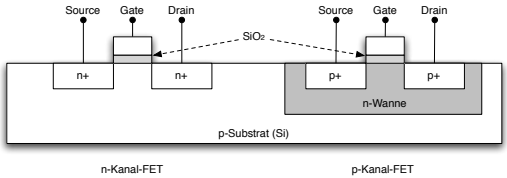
Dieses Kapitel soll sich der Fragestellung widmen, was anhand der Bilddaten zu erkennen ist. Es soll dargestellt werden, wie man bei vergleichsweise einfachen Schaltkreisen, etwa Chips vom Typ „Mifare Classic“, in Hardware umgesetzte Algorithmen findet.

Für eine detaillierte Einführung in die CMOS-Technik seien die einleitenden Kapitel aus dem Buch **CMOS VLSI Design** [27] empfohlen. Das Buch erklärt anschaulich, wie CMOS-Technologie funktioniert und wie Designs erstellt und in Hardware umgesetzt werden. Die Darstellung hier faßt die wesentlichen Punkte aus der Sicht des Reverse-Engineerings zusammen.

Feldeffekt-Transistoren

Feldeffekt-Transistoren (FET) sind Halbleiterbausteine, die in Logikschaltkreisen als elektronische Schalter dienen. Die Abbildung zeigt den Aufbau beider Typen auf einem gemeinsamen Substrat.

Deren Funktionsweise besteht – vereinfacht dargestellt – darin, daß durch Anlegen einer Steuerspannung am *Gate* die Region unter dem *Gate* an Ladungsträgern verarmt oder mit Ladungsträgern angereichert wird. Wenn genug Ladungsträger unter dem *Gate*-Anschluß vorhanden sind, entsteht ein elektrisch leitender Kanal zwischen den Anschlüssen *Source* und *Drain*. Zwei Typen von Feldeffekt-Transistoren unterscheidet man nach Art der Ladungsträger.

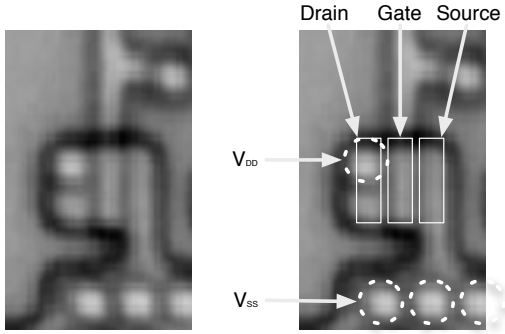


n-Kanal- und p-Kanal-FET auf einem gemeinsamen Substrat

Feldeffekt-Transistoren des n-Kanal-Typs bestehen aus stark n-dotierten Bereichen[1] für Quelle und Abfluß und einem p-dotierten Substrat. Das Siliziumdioxid unter dem *Gate*-Kontakt stellt einen Isolator dar. Bei positiver *Gate*-Spannung bildet sich zwischen *Gate* und Substrat ein elektrisches Feld, so daß sich Elektronen unter dem *Gate* sammeln. Dadurch wird ein Stromfluß zwischen *Source* und *Drain* möglich.

Beim p-Kanaltyp dienen positiv geladene Defektelektronen modellhaft als Ladungsträger. Um einen leitenden Defektelektronen-Kanal zu erzeugen, muß die *Gate*-Spannung null sein. Dadurch sammeln sich Defektelektronen unter dem *Gate*. *Source* und *Drain* eines p-Kanal-FET sind stark p-dotiert und dessen Substrat ist n-dotiert, d. h. genau anders herum als beim n-Kanal-Typ. Um beide Transistortypen auf einem gemeinsamen Substrat betreiben zu können, werden bei der Chip-Herstellung sogenannte Wannen erzeugt.

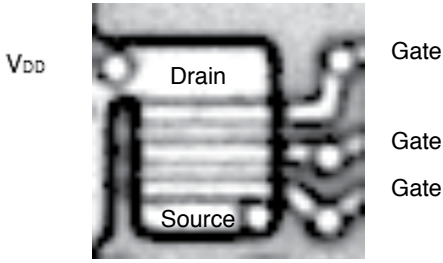
1 In Abbildungen wird die starke Dotierung mit einem Pluszeichen symbolisiert. Starke Dotierung bedeutet ein Verhältnis von 10^4 Siliziumatomen zu einem Donator bzw. Akzeptor. Bei mittleren Dotierungen ist das Verhältnis 10^6 Siliziumatome zu einem Akzeptor (p-Dotierung) bzw. 10^7 Siliziumatome zu einem Donator (n-Dotierung).



n-Kanal-FET unter dem Mikroskop (Chip: Mifare Classic)

Die Abbildung zeigt ein Foto eines Feldeffekt-Transistors unter dem Mikroskop. *Source*, *Gate* und *Drain* sind durch zwei schmale vertikale Striche im Bild links abgegrenzt.

Wenn sich benachbarte Transistoren einen Anschluß teilen, kann es schwierig sein, zu erkennen, welche Bereiche *Source*, *Drain* und *Gate* sind. Da der *Gate*-Anschluß immer als Signal-Eingang eines Transistors dient, ist dieser leichter zu identifizieren. Folgende Abbildung zeigt drei in Reihe geschaltete p-Kanal-FET. Zwischen den *Gates* befindet sich jeweils das gemeinsam genutzte *Source* und *Drain*.

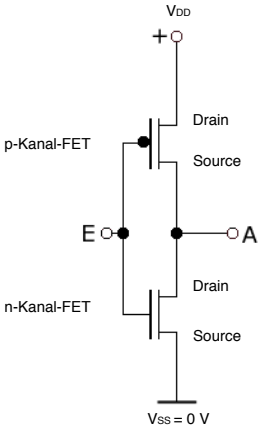


Drei p-Kanal-FETs in Reihenschaltung (Chip: Mifare Classic).

Feldeffekt-Transistoren sind symmetrisch aufgebaut. *Source* und *Drain* könnten also vertauscht werden. Zumindest ist das bei den einfachen FET der Fall und bei den Chips, von denen hier Bildmaterial gezeigt wird. Die Symmetrieeigenschaft läßt es zu, daß man bei der Analyse nicht *Source* und *Drain* explizit im Bild benennen muß. Es reicht die Vorstellung eines Schalters,

mit dem man *Source* und *Drain* elektrisch verbinden kann.

In den Schaltkreisen wird Information als Spannungspotential gespeichert – LOW oder HIGH. Es ist deshalb nicht notwendig, sich zu überlegen, in welche Richtung der technische oder physikalische Strom fließt. Strom fließt im Gegensatz zu Bipolartransistoren hauptsächlich nur beim Umschaltvorgang.



CMOS-Inverter

Das Modell lautet also: Wenn das **passende** Signal am *Gate* anliegt, sind *Source* und *Drain* elektrisch verbunden, und der Transistor schaltet durch. Anderenfalls sperrt der Transistor.

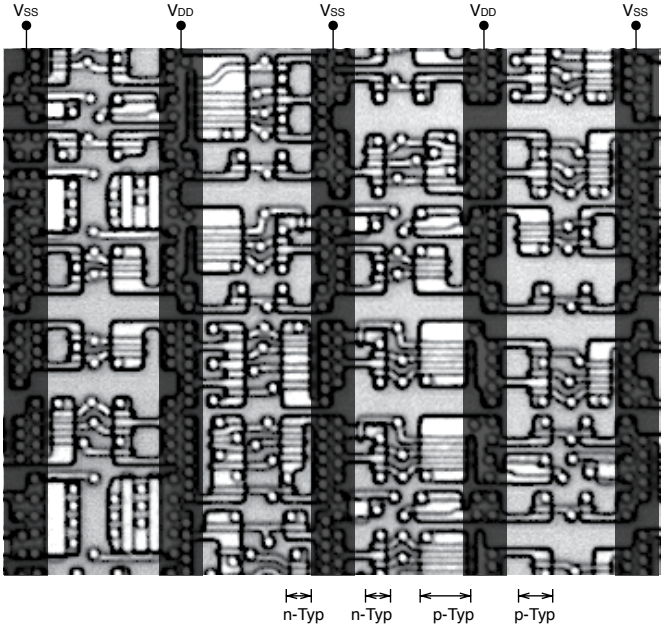
Komplementäre Verwendung von FETs

CMOS ist das Akronym für Complementary Metal Oxide Semiconductor. Feldeffekt-Transistoren werden in CMOS-Gattern nicht einzeln eingesetzt, sondern immer komplementär geschaltet. In Schaltungen wird jedem p-Kanal-FET ein n-Kanal-FET gegenübergestellt. Der p-Kanal-FET ist Teil des Pull-up-Netzes, der n-Kanal-Typ ist Teil des Pull-down-Netzes. Je nach Steuerung hat ein Ausgang eines Gatters das Spannungspotential des Pull-up-Netzes oder das Potential des Pull-down-Netzes.

Beide Netze eines (Teil-)Gatters sind immer komplementär geschaltet. Wenn das eine Netz gesperrt ist, ist das andere geöffnet und umgekehrt. Das sei am Beispiel des CMOS-Inverters aus obiger Abbildung, der die logische Funktion NOT umsetzt, dargestellt.

Ist das Eingangssignal HIGH (positives Potential), entsteht ein leitender n-Kanal zwischen *Source* und *Drain* im Pull-down-Netz. Der Ausgang wird quasi geerdet. Gleichzeitig ist der p-Kanal-FET im Pull-up-Netz gesperrt, so daß keine leitende Verbindung zwischen dessen *Source* und *Drain* besteht. Ist das Eingangssignal LOW (0 V), ist der n-Kanal-FET gesperrt und der p-Kanal-FET offen. Der Ausgang hat dann das Potential V_{DD}.

In der Umsetzung im Chip durchziehen parallele spannungsführende Leiterbahnen wie Schienen den Bereich, in dem die Logik-Gatter plaziert sind. In der Abbildung unten sind das die dunkel markierten Streifen. Die Schienen für das Potential V_{DD} und V_{SS} wechseln sich dabei ab. Die Pull-up- und Pull-down-Netze sind zwischen den Leiterbahnen angeordnet.



Typenweise Anordnung von p- und n-Kanal-Transistoren zwischen den Potentialschienen (Chip: Mifare Classic)

Die hellen Punkte in der Abbildung sind Durchkontaktierungen zu höheren Schichten im Schaltkreis. Die *Gate*-Anschlüsse verlaufen zwischen den Transistortypen und sind jeweils mit einer Durchkontaktierung versehen.

Die z. T. haken- und ösenförmigen Transistoren weisen unterschiedliche *Gate*-Längen auf. P-Kanal-FET haben meist eine größere *Gate*-Länge gegenüber n-Kanal-Typen. Das liegt daran, daß die Beweglichkeit der Löcher geringer ist als die der Elektronen. Um so größer der Kanalquerschnitt zwischen *Source* und *Drain* ist, desto mehr Defektelektronen können in der gleichen Zeit durch den Kanal driften.

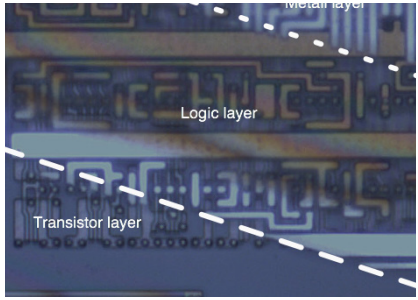
Anhand der Zuordnung, auf welcher Seite jeweils die p-Kanal-Typen und auf welcher die n-Kanaltypen verlaufen, kann man den Leiterbahnen Spannungspotentiale zuordnen. Am *Drain* des p-Kanal-FET ist die Spannung V_{DD} angelegt, am *Source* des n-Kanal-FET das Potential V_{SS}.

Tatsächlich ist es möglich, p- und n-Kanal-Typen vertauscht anzuwenden. N-Kanal-FET können besser LOW-Signale weiterleiten. Dagegen leiten p-Kanal-FET besser HIGH-Signale weiter. Beim Vertauschen der Typen sind die Spannungspotentiale am Ausgang des Transistors etwas größer als V_{SS} bzw. etwas kleiner als V_{DD}. Man spricht dann von degradierten oder schwachen Signalen. Dies möchte man beim Design von CMOS-Schaltkreisen vermeiden. [27]

Aufbau von Logik-Gattern

In den letzten zwei Abschnitten ist beschrieben, wie man Transistoren als Schalter benutzt und wie Transistoren auf dem Substrat angeordnet sind. Herstellungsbedingt ist die Anordnung der Transistoren auf mehreren Schichten (*front-end-of-line*, FEOL) verteilt. Diese sollen hier zur Vereinfachung als Transistor-Layer bezeichnet werden. Um elementare Logik-Gatter aufzubauen, müssen mehrere Transistoren zusammengeschaltet werden. Auf dem Transistor-Layer sind bereits einzelne Leiterbahnen plaziert. Die Leiterbahnen müssen kreuzungsfrei verlegt werden. Dazu sind zusätzliche Ebenen im Chip notwendig (*back-end-of-line*, BEOL).

Eine besondere Bedeutung kommt der ersten Verdrahtungsebene über dem Transistor-Layer zu. Sie bildet das Verbindungsgerüst, um aus den darunterliegenden Transistoren die logischen Grundfunktionen zu formen, beispielsweise NAND und NOR. Diese Schicht wird *Metal 1* oder kurz *M1* genannt. Die Transitoren eines Gatters sind immer beieinander angeordnet.

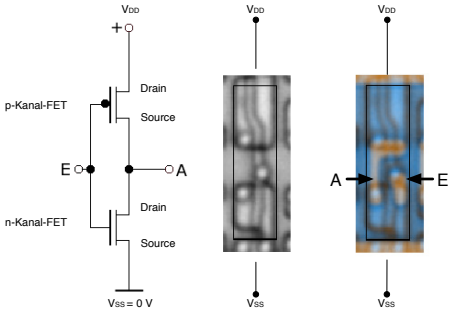


Der Materialabtrag beim Polieren der Chipoberfläche war nicht gleichmäßig. Dadurch ergibt sich eine Blick auf drei verschiedene Ebenen. (Mifare Classic)

Für die Anfertigung der Masken für den Herstellungsprozess können Chip-Designer grundlegende Funktionsblöcke aus vorgefertigten Bibliotheken verwenden. Bei Mifare Classic sind etwa siebzig verschiedene Grundbausteine zu finden, u. a. etwas komplexere Typen wie Flipflops und Volladdierer. Darunter sind aber einige Formen enthalten, die gleiche logische Funktion umsetzen, nur daß leicht verschiedenen Masken zur Anwendung kommen. Im *„Silicon Zoo“* zeigt Karsten Nohl die bei Mifare Classic verwendeten Grundbausteine. [13]

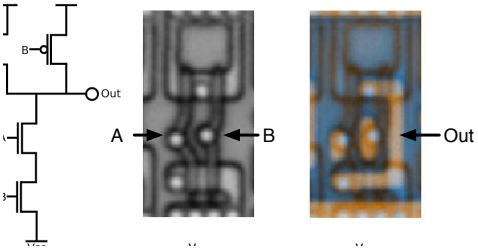
Obige Abbildung stellt den schichtweisen Aufbau von Logik-Schaltkreisen dar. In der Schicht *M1* sind die fingerförmig angeordneten Leiterbahnen für V_{SS} und V_{DD} untergebracht. Über dem M1 sind weitere Schichten, die Leiterbahnen für die Verschaltung von Grundgattern beinhalten.

Wie kann man nun anhand von Bilddaten die Schaltfunktion eines Gatters ermitteln?



CMOS-Inverter (Mifare Classic)

Die beiden Abbildungen zeigen beispielhaft zwei Grundgatter in CMOS-Technologie nebst Schaltbild. Die Funktionsweise des CMOS-Inverters wurde bereits beschrieben. In der oberen Abbildung sieht man die beiden Transistoren, die Durchkontaktierungen und die Verbindungen mit V_{SS} und V_{DD}. Der Eingang E ist auf das *Gate* beider Transitoren geschaltet. Im Ausgang A sind *Source* des p-FET und *Drain* des n-CMOS vereint.



CMOS-NAND (Mifare Classic)

In der zweiten Abbildung ist ein NAND aus insgesamt vier Transistoren dargestellt. Man beachte, daß die *Gate*-Längen im Pull-up-Netzwerk in der Abbildung nicht größer sind als im Pull-down-Netz, weil die beiden n-Kanal-FET aus dem Pull-down-Netz seriell geschaltet sind und sich damit deren Widerstand verdoppelt. Die Driftgeschwindigkeiten der jeweiligen Majoritätsladungsträger sind damit in beiden Netzen etwa gleich.

Für das Reverse-Engineering einfacher Gatter ist es sinnvoll, die wenigen Transistoren und Leiterbahnen übersichtlich geordnet auf ein Blatt Papier zu skizzieren. Oft ist der Gattertyp sofort zu erkennen. Es kann sein, daß man aufgrund vorheriger Analyse anderer Gatter eine Grundstruktur wiedererkennt. Beispielsweise sieht ein 3-NAND, d. h. ein NAND für drei Eingänge[2], nicht wesentlich anders aus als ein 2-NAND. Im Pull-up-Netz sind drei statt zwei Transistoren parallel geschaltet und im Pull-down-Netz sind drei FETs seriell verbunden (vgl. Abbildung CMOS-NAND).

Mitunter kann es hilfreich sein, eine Wahrheitstabelle aufzustellen, indem man für alle möglichen Belegungen der Eingänge den Wert am Ausgang ermittelt. Anhand der Wahrheitstabelle kann man eine Boolesche Funktion aufstellen. Die Tabelle zeigt das beispielhaft für ein 3-NAND-Gatter. Für alle $2^3 = 8$ möglichen Belegungen der Eingänge A, B, und C ist das Ergebnis der Booleschen Funktion in der letzten Spalte angegeben.

Eingang A	Eingang B	Eingang C	Ausgang NAND(A, B, C)
T	T	T	F
T	T	F	T
T	F	T	T
T	F	F	T
F	T	T	T
F	T	F	T
F	F	T	T
F	F	F	T

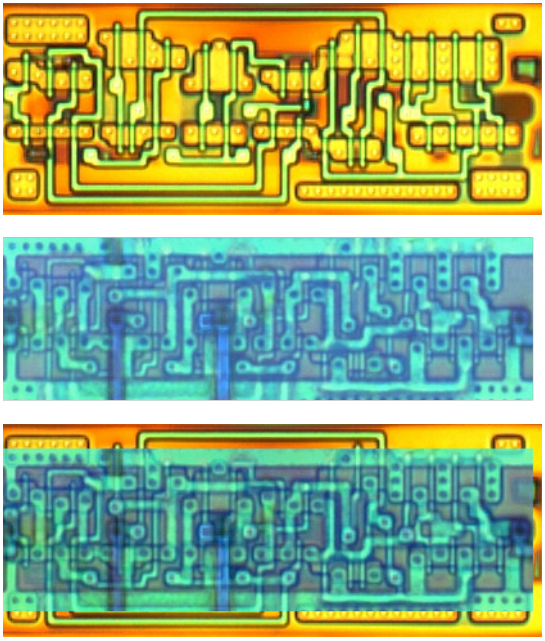
Wahrheitstabelle für einen 3-NAND

Aus der Tabelle kann man ablesen, daß die Schaltfunktion sich als $\overline{A} \wedge B \wedge \overline{C}$ darstellt. Das geht hier deshalb einfach, weil es nur eine Belegung gibt, wo der Ausgang den Wert falsch annimmt. I. d. R. stellt man die Kanonische Alternative Normalform auf. Diese ist etwas sperrig und lautet $\Phi(A, B, C) = (A \vee B \vee \overline{C}) \wedge (A \vee \overline{B} \vee C) \wedge (A \vee \overline{B} \vee \overline{C}) \wedge (\overline{A} \vee B \vee C) \wedge (\overline{A} \vee B \vee \overline{C}) \wedge (\overline{A} \vee \overline{B} \vee C) \wedge (\overline{A} \vee \overline{B} \vee \overline{C})$. Diesen Ausdruck versucht man dann soweit zu vereinfachen, so daß möglichst wenige logische Operatoren auftreten.

Bei der Rekonstruktion einer Gatterfunktion mittels einer Wahrheitstabelle verliert diese an

2 $\text{3-NAND}(A, B, C) = \overline{\text{AND}(A, B, C)}$

Anschaulichkeit. Insbesondere für den Fall, daß sich bei der Rekonstruktion Fehler einschleichen, sind diese schwierig festzustellen.



zu identifiziereder CMOS-Schaltkreis

Die Abbildung zeigt einen komplizierteren CMOS-Schaltkreis. Die Transistorschicht ist in der Abbildung oben dargestellt, darunter die Metallverbindungen, die dann die Transistoren zu einem Gatter verbinden. Die untere Darstellung zeigt beide Layer zu einem Bild vereint. Im Transistor-Layer sind 34 Transistoren zu erkennen: 17 p-Kanal-Transistoren oben und 17 n-Kanal-FET unten. Der dargestellte Schaltkreis soll beispielhaft für eine Analyse herhalten.

Anhand der Transistorgrößen – genauer der *Gate*-Längen – ermittelt man, welche Seiten zum Pull-up-Netz gehören und welche zum Pull-down-Netz. P-Kanal-FET müssen nicht zwangsläufig größer sein als n-Kanal-Typen. Oben sieht man, daß die p-Kanal-Transistoren an der oberen Seite angeordnet sind. Das mittlere Bild zeigt am oberen und unteren Rand die Leiterbahnen für die Versorgungsspannung und Masse. V_{DD} ist hierbei oben, V_{SS} unten.

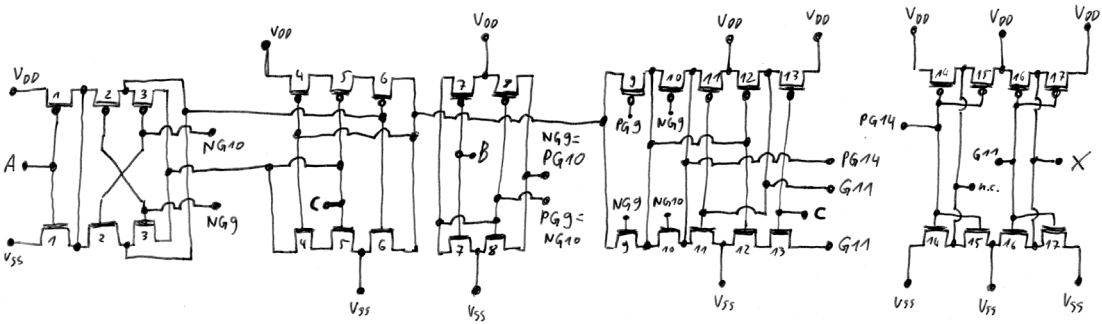
Die Transistoren findet man wieder anhand der *Gates*. Die Transistoren eines Gatters werden durchnummeriert. Z. B. von links nach rechts P1...P17 und N1...N17. Dazu ist es hilfreich, das Bild in einem Graphikbearbeitungsprogramm zu öffnen und beispielsweise jedes fünfte *Gate* mit einer Beschriftung zu versehen.

Die Transistoren überträgt man auf ein Blatt Papier. Für jeden Transistor sind die Leiterbahnen zu verfolgen und in die Zeichnung zu übertragen. Für das Abzeichnen ist es empfehlenswert, die Transistoren wie im physischen Gatter anzuordnen und die *Gates* zur Mitte hin zu zeichnen. Anderenfalls hat man schnell zahlreiche unübersichtlich gekreuzte Leiterbahnen. Die Abbildung auf der rechten Seite zeigt den zugehörigen Schaltplan.

Beim Übertragen der Leiterbahnen aufs Papier werden sich durchaus Fehler einschleichen. Dann hilft es, nach offenen Transistoranschlüssen zu suchen. Durchkontaktierungen kann man anhand ihres punktförmigen Aussehens erkennen. Wenn man vermutet, daß zwei übereinanderliegende Leiterbahnen elektrisch verbunden sind, dann muß es eine Durchkontaktierung geben. Weitere Fehler findet man eventuell bei der späteren Analyse. Wenn die Verschaltung mehrerer Transistorpaare keinen Sinn ergibt oder zu viele Transistoren effektiv nicht benutzt werden, lohnt sich ein erneuter Blick in das Ausgangsbild. Es ist möglich, daß nicht alle Transistoren eines Gatters verwendet werden. So werden beispielsweise die Transistoren P14, P15, N14 und N15 hier im Gatter nicht verwendet.

Die Ein- und Ausgänge des Gatters sind einfach zu finden. In der Mitte der Abbildung sind das die beiden senkrechten Striche, die von außen kommen und etwa bis zu Bildmitte verlaufen (blaue Färbung in der PDF-Version).[3] Im allge-

3 Das Bild links wurde mit einem Konfokalmikroskop aufgenommen, das verschiedenen Tiefen im Untersuchungsobjekt verschiedene Farben zuordnet.

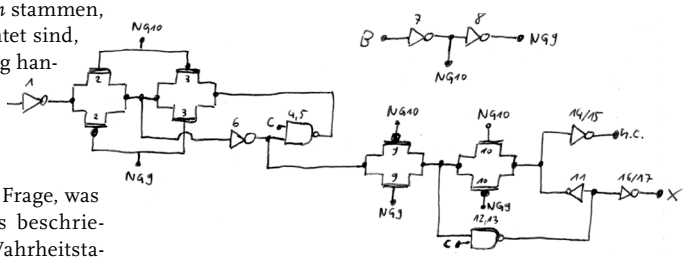


Rekonstruiertes Schaltbild des zu identifizierenden CMOS-Gatters

meinen Fall findet man auf der Schicht *M1* entsprechende Durchkontaktierungen und auf den darüberliegenden Verbindungslayern Leiterbahnen, die auf diese Kontakte geschaltet sind. Wenn eine Verbindung von außerhalb mit einem Gate verbunden ist, muß es sich um einen Eingang handeln. Wenn Verbindungen, die von einem *Source* oder *Drain* stammen, in die Außenwelt des Gatters gerichtet sind, muß es sich um einen Gatterausgang handeln. Folglich sind die Anschlüsse A, B und C im Schema Eingänge und X der Ausgang.

Bei diesem Schaltplan stellt sich die Frage, was die Schaltung bewirkt. Wie bereits beschrieben, wäre es möglich, dazu eine Wahrheitstabelle aufzustellen, beispielsweise unter Zuhilfenahme von Simulationspaketen wie etwa SPICE. Man kann allerdings versuchen, im Schaltbild intuitiv Funktionsblöcke auszumachen.[4] Als Hinweis auf die Abgrenzung der Funktionsblöcke können die Zuführungen der Spannungspotentiale V_{DD} und V_{SS} dienen. In Abbildung links kann man im Transistor-Layer erkennen, daß seriell geschaltete Transitoren in Blöcken gruppiert sind. Diese Gruppierung spiegelt im Wesentlichen die Funktionsblöcke wider.

Meistens hilft es, für jeden dieser Funktionsblöcke eine alternative **gewohnte** graphische Darstellung zu finden. So sieht man beispielsweise, daß das Transistorpaar 4 und 5 ein NAND bildet und das Transistorpaar 6 einen Inverter darstellt. In vereinfachter Form gezeichnet entsteht ein Schaltplan wie in dieser Abbildung:



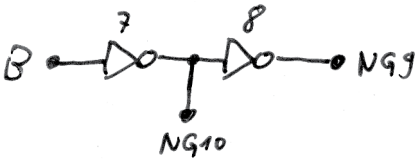
Schaltung eines Flipflops. Die angegebenen Zahlen geben an, welche Transistoren bzw. Transistorenpaare zum Teilgatter beitragen.

Der abgebildete Schaltkreis stellt einen taktflankengesteuerten Master/Slave-Flipflop dar. Das **Eingangsbit** liegt an Eingang A an und das Taktsignal an Eingang B. Mit einem Signal auf Eingang C kann man den Informationsspeicher zurückstellen. Am Ausgang X liegt das gespeicherte Signal an. Das Gatter beinhaltet einen invertierten Ausgang. Der wird allerdings nicht genutzt.

Diese Abbildung eines vereinfachten Schemas zeigt zwei weitere Konstruktionsmechanismen, wie man sie desöfteren findet. Deshalb sollen sie hier kurz beschrieben werden.

4 Für die Verifikation von Schaltkreisen existieren Werkzeuge, um auf dem Substrat angeordnete Gatter anhand von Netzlisten darauf zu prüfen, ob sie die intendierte Funktion erfüllen. In [4] wird beschrieben, wie man mittels eines Prolog-Programmes Schaltungen analysieren kann. Für das Reverse-Engineering wäre das ebenfalls praktisch.

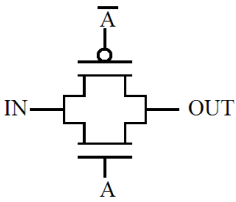
Man sieht, daß die beiden Transistorenpaare 7 und 8 das Taktsignal B zweifach invertieren.



Doppelter Inverter zur Signalauffrischung.

Das Transistorpaar P8 und N8 erscheint überflüssig, da die doppelte Negation des Signals wieder das normale Taktsignal ist. Diese Konstruktion stellt einen Puffer dar. Wie bereits erwähnt, leiten p- und n-Kanal-FET Signale unterschiedlich gut weiter. Insbesondere bei Serienschaltung mehrerer Transistoren führt das intern zu Spannungsabfällen, so daß die Signalpegel nicht mehr ideal sind. Durch die genutzte Konstruktion wird das Taktsignal *aufgefrischt* und hat wieder die idealen Spannungspegel V_{DD} oder V_{SS}. Der Nachteil besteht darin, daß diese zusätzlichen Gatter das Signal verzögern. Das Signal auf der Leiterbahn NG9 ist gegenüber dem Signal B phasenverschoben.

Als weiteres Konstruktionselement findet man im vereinfachten Schema mehrere sogenannte Transmission-Gates. Ein Transmission-Gate besteht aus einem n- und einem p-Kanal-Transistor, die wie hier zu sehen zusammengeschaltet sind. Ein n-FET schaltet bei positiver *Gate*-Spannung durch, und ein p-FET sperrt bei positiver *Gate*-Spannung. Wenn das Signal am p-FET invertiert ist, dann schalten beide Transistoren bei HIGH durch und sperren beim LOW-Signal. Dadurch ergibt sich im Flipflop die taktflankengesteuerte Übernahme des Eingangssignals.



Transmission-Gate
(Bildquelle: Wikipedia)

Wiederverwendung von Logik-Gattern

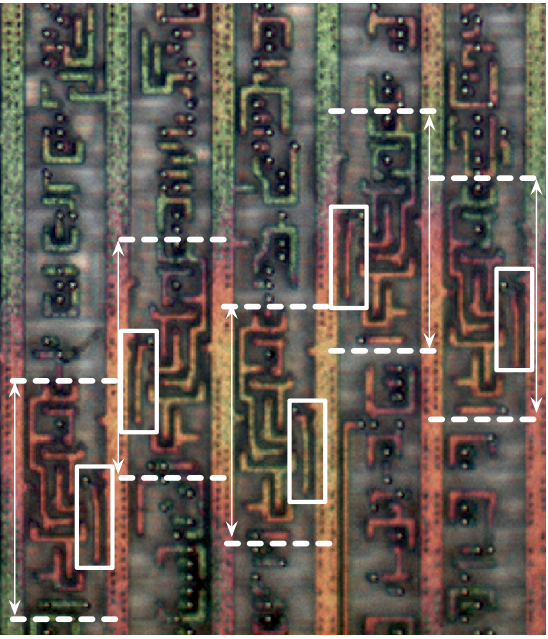
Wenn Ingenieure Schaltungen in Hardware umsetzen, erstellen sie nicht für jeden Chip-Typen ein vollständig neues Layout aller Transistoren, sondern nutzen vorgefertigte Grundgatter. Für diese Grundgatter existieren vorgefertigte Masken für den lithographischen Herstellungsprozeß. Die sind weitgehend optimiert und wurden bereits auf Praxistauglichkeit hin untersucht.

Was man für Gattertypen auf einem Chip findet, hängt von den verwendeten Maskenbibliotheken ab. Es kann beispielsweise sein, daß man einen Halbaddierer als AND- und OR-Gatter getrennt realisiert findet. Es kann aber sein, daß die Maskenbibliothek bereits einen Halbaddierer in Gänze beinhaltet und sich das auf dem Chip als eigenständiges Gatter widerspiegelt. Ferner ist es möglich, daß diese Maskenbibliotheken ganze Allzweck-CPU oder speziell für die Signalverarbeitung geeignete Rechenwerke beinhalten. Das ist jedoch eher ein Sonderfall.

Die Wiederverwendung von Grundbausteinen ermöglicht beim Reverse-Engineering folgende Vereinfachung. Wenn man ein Gatter aus der Bibliothek bereits erkannt hat, ist es einfacher, diesen Gattertyp auf dem Chip wiederzufinden, als die Bedeutung aller Transistoren einzeln zu ermitteln.

Die dafür geeigneten Muster sind auf der Schicht *M1* und auf dem Transistor-Layer. Meist ist *M1* einfacher auszuwerten. Man sucht nach Mustern im Verdrahtungsgeflecht, die man an anderen Stellen auf dem Chip findet. Wenn man ein wiederkehrendes Muster identifiziert hat, beispielsweise die in folgender Abbildung mit Rechtecken hervorgehobene Haken, vergleicht man die verschiedenen Instanzen, um einen maximal konstanten Bildbereich zu finden. Die plazierten Gatter gehen nahtlos ineinander über, ohne daß eine definierte Abgrenzung vorhanden ist. Vergleicht man die Instanzen, sieht man, welche Teile des Verdrahtungsgeflechts noch zum Gatter gehören. Idealerweise sucht man zuerst nach größeren Gattern.

Mittels normalisierter Kreuzkorrelation, einem Verfahren aus der Signalverarbeitung, ist es möglich, Bildmaterial an anderen Stellen wie-



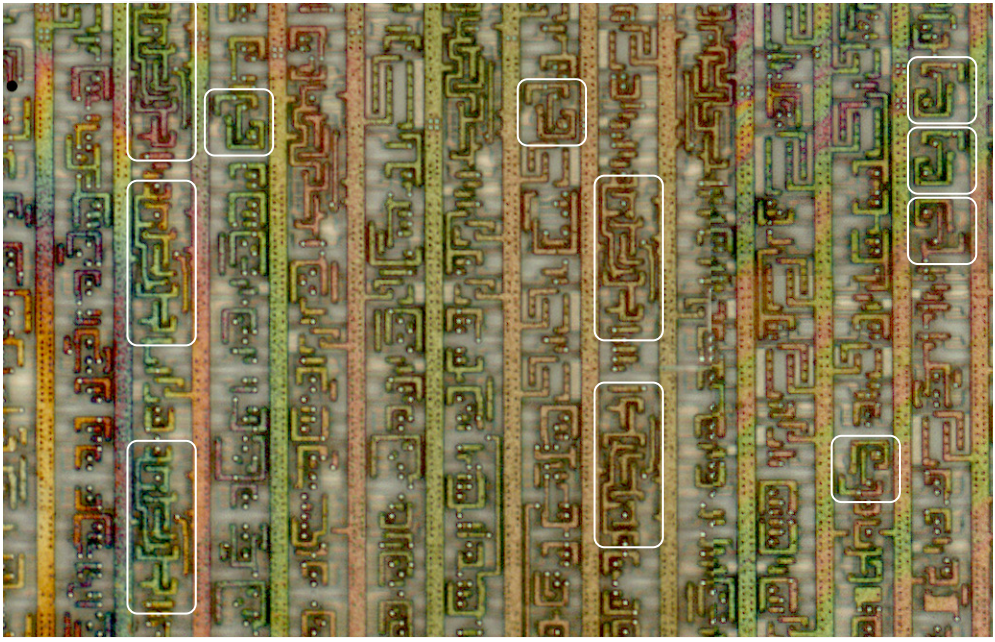
Wiederfinden markanter Muster (Chip: Mifare Classic)

derzufinden, an denen ein Muster ebenfalls auftritt. Die Schritte wendet man iterativ an, bis man alle Gattertypen ermittelt hat.

Gezielte Suche

Das komplette Reverse-Engineering eines Chips ist zu aufwendig und nicht notwendig. Dies ist mit dem Reverse-Engineering von Software mittels Disassemblern vergleichbar. In der Regel sind vorab konkrete Fragestellungen gegeben, z. B. wie ein Verschlüsselungsverfahren implementiert ist. Deshalb muß kein Chip komplett analysiert werden.

Beispielsweise werden Stromchiffrierer mittels Schieberegister (Flipflops) konstruiert. Da funktional zusammenhängende Bereiche auf dem Chip benachbart plaziert sind, muß man lediglich nach Bereichen suchen, in denen viele Flipflops zu sehen sind. Flipflops sind leicht zu erkennen, da sie innerhalb typischer Standardzellenbibliotheken die größten Elemente bilden. So beschreiben die markierten Bereiche im ersten Bild Flipflops. Andere Gatter, die eben-



Manuelles Ermitteln der Gattergrenzen anhand von Verdrahtungsmasken (Chip: Mifare Classic)

falls in der Abbildung zu sehen sind, z. T. sogar paarweise, sind vergleichsweise klein.

Daß die markierten Bereiche zu einem Standardzellentyp gehören, ist ebenfalls am Grad der „Verzahnung“ der Leiterbahnen auf der Schicht *M1* zu erkennen. Wenn man ein Gefühl dafür entwickelt, wieviele Flipflops unter der Metall-Maske Platz finden, kann man die Maskengröße als Indiz dafür werten, daß es sich um einen Flipflop handelt. Diese Aussage ist jedoch nicht allgemeingültig. Es gibt Fälle, in denen auf der Schicht *M1* Unterschiede in den Verdrahtungsmasken zu finden sind, obwohl es sich um den gleichen Typ Standardzelle handelt.

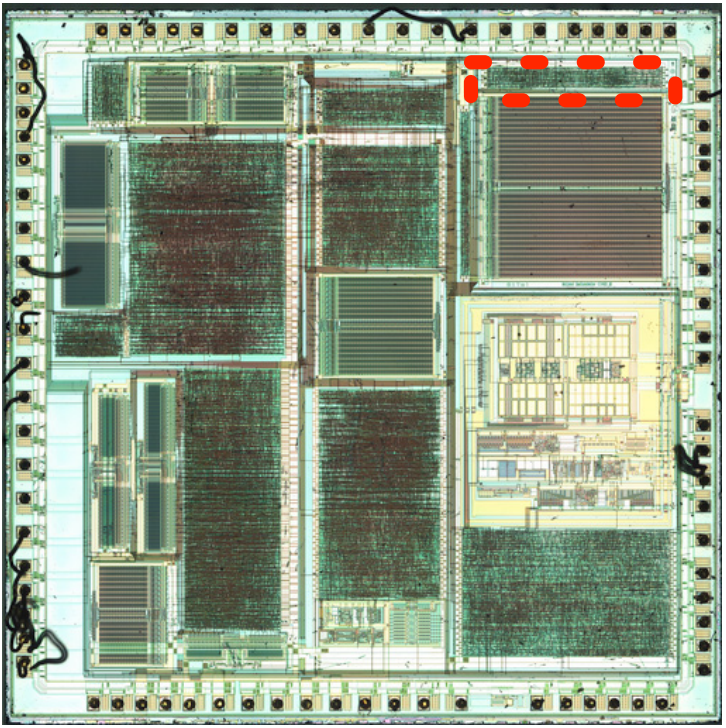
Kenntnisse von Schlüsselgrößen kryptographischer Routinen helfen ebenfalls. Wird der gesamte Schlüssel in der Hardware gespeichert, müssen sich mindestens entsprechend viele Flipflops finden lassen.

Es ist möglich, daß die Schaltkreise in einem separaten Bereich plaziert sind. Dies ist beispielsweise bei der Realisierung des DECT Standard Ciphers im SC14421CVF der Fall (Bild unten). Insbesondere sind in derartigen Bereichen hohe Flipflop-Konzentrationen leicht feststellbar.

Darüber hinaus können Masken einzelner Bereiche in Nachfolgern eines Chipdesigns übernommen werden, selbst wenn ein Technologiewechsel im Halbleiterprozeß stattfindet. Dies ist nützlich, da man sich bei der Analyse auf Chips älteren Typs konzentrieren kann.

Fazit

Das Reverse-Engineering von Logikschaltungen in Integrierten Schaltkreisen ist mit einfachen finanziellen und technischen Mitteln möglich. Die Kosten für die Ausstattung hängen hauptsächlich davon ab, auf welche Geräte man Zugriff hat und welche Geräte man gegebenfalls selbst bauen kann. Die Einstiegshürden sind deshalb vergleichsweise gering. Folglich ist die Annahme, daß in Integrierten Schaltungen verborgene Algorithmen gegen Angreifer mit geringem Budget geschützt sind, nicht haltbar.



Übersicht des DECT-Chips SC14421CVF. Der DECT Standard Cipher ist innerhalb der Markierung im oberen rechten Bildbereich plaziert.

Das für das Reverse-Engineering von Logik in IC notwendige Wissen kann innerhalb kurzer Zeit erlernt werden. Spezielle Vorkenntnisse sind dafür nicht notwendig.

Der Aufklärung von proprietären Verschlüsselungsverfahren sind im Rahmen des veranschlagten Budgets Grenzen gesetzt. Dieses Budget wird hier mit 1.000 bis 10.000 Euro bemes-

sen. Die technischen Grenzen sind durch die optische Auflösung des Mikroskops festgelegt. Würde man ein größeres Budget veranschlagen, könnte diese Hürde überwunden werden. Für 20.000 bis 30.000 US-Dollar kann man gebrauchte Rasterelektronenmikroskope erwerben, die zur Analyse aktueller Halbleiterprozesse geeignet sind. Es ist ferner davon auszugehen, daß die Preise für Gebrauchtgeräte weiter fallen und geeignete Geräte in wenigen Jahren für unter 10.000 Euro gehandelt werden.

Für das Reverse-Engineering von Logikschaltkreisen gibt es kaum Software. Die wenigen Firmen, die in diesem Marktsegment tätig sind, machen ihre Softwarewerkzeuge nicht publik, da Programme Teil des Geschäftskonzeptes sind. Mangelnde Dokumentation der Prozesse und unzugängliche Software sind höchstwahrscheinlich Ursache dessen, daß dem Reverse-Engineering von ICs bisher kaum Beachtung zuteil wurde.

Das Reverse-Engineering von Logikschaltkreisen ist in vielen Teilen ein kreativer Prozeß, der sich jedoch durch Computerunterstützung wesentlich beschleunigen läßt. Es ist daher unumgänglich, Software zu entwickeln, die zur Automatisierung beiträgt.

Literatur und Quellen

[1] Sally Adee. *„The hunt for the kill switch"*. In: IEEE Spectrum (Mai 2008). URL: *http://www.spectrum.ieee.org/print/6171*

[2] L. R. Avery u. a. *Reverse Engineering Complex Application-Specific Integrated Circuits (ASICs)*. 2002. URL: *http://www.gemes.com/ company_info/reverse_engineering_complex_ASICS.pdf*

[3] Friedrich Beck. *Präparationstechniken für die Fehleranalyse an integrierten Halbleiterschaltungen*. VCH Verlagsgesellschaft mbH, 1998. ISBN: 3- 527-26879-9.

[4] Inderpreet Bhasin und Joseph G. Tront. *„Block-Level Logic Extraction from CMOS VLSI Layouts"*. In: VLSI Design 1 (3 1994), S. 243–259. DOI: 10.1155/1994/67035. URL: *http://www.hindawi.com/getarticle. aspx?doi=10.1155/1994/67035*

[5] Buehler GmbH. *Phoenix Grinder-Polishers*. 2008. URL: *http://www.buehler-met.de/produkte/schleifenpolieren.html*

[6] Nick Chernyy. *HOW TO: write an IC Friday post*. 2008. URL: *http: //microblog.routed.net/2008/07/15/how-to-write-an-ic-friday-post/*

[7] Chipworks. *Webseiten der Firma Chipworks*. URL: *http://www.chipworks.com/*

[8] Prof. Dr. rer. nat. H. Kück. Vorlesung: *Aufbau- und Verbindungstechnik von Silizium-Mikrosystemen*. 2002. URL: *http://www.uni-stuttgart. de/izfm/lehre/AVT_Geh.pdf*

[9] Sven Kaden. *Image stitching*. 2009. URL: *http://degate.zfch.de/ HAR2009/*

[10] Samuel T. King u. a. *Designing and implementing malicious hardware. 2008*. URL: *http://www.usenix.org/event/leet08/tech/full_ papers/king/king.pdf*

[11] Oliver Kömmerling und Markus G. Kuhn. *Design Principles for Tamper- Resistant Smartcard Processors*. 1999. URL: *http://www.cl.cam.ac. uk/~mgk25/sc99-tamper.pdf*

[12] Karsten Nohl. *Reverse-Engineering Custom Logic (Part 1)*. Sep. 2008. URL: *http://www.flylogic.net/blog/?p=32*

[13] Karsten Nohl. *The Silicon Zoo*. 2008. URL: *http://www.siliconzoo.org/*

[14] Karsten Nohl und Henryk Plötz. *24C3 Video Recordings: Mifare – Little Security, Despite Obscurity*. Dez. 2007. URL: *http://chaosradio.ccc. de/24c3_m4v_2378.html*

[15] Karsten Nohl und Henryk Plötz. *24th Chaos Communication Congress: Mifare – Little Security, Despite Obscurity*. Dez. 2007. URL: *http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html*

[16] Karsten Nohl und Henryk Plötz. *26th Chaos Communication Congress: Legic Prime – Obscurity in Depth*. Dez. 2009. URL: *http://events.ccc.de/congress/2009/Fahrplan/events/3709.en.html*

[17] Olympus Europa Holding GmbH. *Olympus – Motorisiertes Forschungsmikroskop BX61*. 2008. URL: *http://www.olympus.de/microscopy/22_ BX61.htm*

[18] Panorama Tools Portal. 2008. URL: *http://www.panotools.org*

[19] PanaVue. *PanaVue ImageAssembler 3*. 2008. URL: *http://www.panavue.com/en/products/index.htm*

[20] Martin Schobert. Experiment: *IC-Entkapselung mit Kolophonium*. 2010. URL: *https://berlin.ccc.de/mediawiki/index.php?title= Experiment:_IC-Entkapselung_mit_Kolophonium&oldid=7463*

[21] Bruce Schneier. *Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C*. 1. Auflage 1996 / 1., korrigierter Nachdruck 1997. Addison-Wesley, 1997. ISBN: 3-89319-854-7.

[22] Sergei P. Skorobogatov. *Semi-invasive attacks. A new approach to hardware security analysis. Techn. Ber.* UCAM-CL-TR-630. University of Cambridge, Computer Laboratory, 2005. URL: *http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-630.pdf*

[23] Der Spiegel. *"Tip von Urmel"*. In: Der SPIEGEL, 38/1995 (Sep. 1995). URL: *http://www.spiegel.de/spiegel/print/d-9221784.html*

[24] Res Strehle. Verschlüsselt – *Der Fall Hans Bühler*. Werd Verlag, Zürich, 1994. ISBN: 978-3859321410.

[25] Erik Tews. *26th Chaos Communication Congress: DECT (part II). What has changed in DECT security after one year*. Dez. 2009. URL: *http:// events.ccc.de/congress/2009/Fahrplan/events/3648.en.html*

[26] David Tschumperlé. *GREYCstoration. Open source algorithms for image denoising and interpolation*. 2008. URL: *http://cimg.sourceforge. net/greycstoration/*

[27] Neil H. E. Weste und David Harris. *CMOS VLSI Design. A Circuits and Systems Perspective* / International Edition. 3. Aufl. Pearson Education, 2005. ISBN: 0-321-26977-2.

Selbstversuch Datenbrief

von Sascha Manns <saigkill@opensuse.org>

Inspiriert durch einen Vortrag auf dem Chaos Communication Congress habe ich mich mit dem Datenbrief auseinandergesetzt.

Die Forderungen waren im Rahmen des Rechtes auf digitale Intimsphäre folgende:

- jährlicher Datenbrief,
- Infos zu Geschäftsforfällen wie Inkasso und Schufa,
- Auflistung sämtlicher Kontaktdaten,
- Auflistung der Firmen, an die meine Kontaktdaten weitergeleitet wurden.

Testweise habe ich drei sehr verschiedene Firmen kontaktiert, um deren Auskunftsfreudigkeit zu überprüfen. Das waren Reichelt Elektronik, GMX und der Weltbild-Verlag.

Als Basis nutzte ich folgenden Formbrief, den ich erstellte:

Änderung meiner geschäftlichen Bedingungen

Sehr geehrte Geschäftspartner,

am 15. Dezember 1983 wurde ein Urteil des Bundesverfassungsgerichtes rechtskräftig, das erstmals ein Grundrecht auf informationelle Selbstbestimmung garantierte.

Auszugsweise heißt es dort: „Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig."

Bezugnehmend auf dieses Urteil möchte ich gerne einen Überblick aller meiner personenbezogenen Daten der letzten zwei Jahre in Ihrer Firma erhalten. Dazu zählen Kontaktdaten, Geschäftsvorfälle, Eintragungen bei der SCHUFA und Namen und Kontaktdaten der Firmen, an die Sie eventuell die Daten weiterverkauft oder anderweitig weitergegeben haben. Dies betrifft sowohl die Papier- als auch die digitalen Medien.

Desweiteren möchte ich gerne einen jährlichen Datenbrief erhalten, in dem obige Aufzählungen für das jeweils letzte Jahr enthalten sind. Praktischerweise könnte dies zum Jahreswechsel geschehen. Der Datenbrief kann per E-Mail oder per Brief versandt werden.

Für künftige Datenerhebungen oder Datenweitergaben möchte ich gerne ein „Double Opt-In", ein Verfahren, das zweimal nachfragt, ob die Daten verarbeitet werden dürfen. Sollten Sie mit diesen neuen Geschäftsbedingungen nicht einverstanden sein, so betrachten Sie unsere Geschäftsbeziehungen als beendet.

Dennoch sind sie auskunftsverpflichtet und somit zumindest für die Angaben der letzten zwei Jahre verpflichtet. Sollten Sie unsere Geschäftsbeziehung beenden wollen, verfüge ich hiermit, sämtliche personenbezogenen digitalen Daten zu löschen. Die Papiervariante darf gelagert werden, jedoch nur bis zum Ende der kaufmännischen Pflicht.

Das Dokument habe ich erstmal als ODT-Datei an alle drei Kandidaten geschickt. GMX und Reichelt konnten damit nichts anfangen und baten um ein anderes Format. Nachdem ich RTF verwendete, gaben beide erstmal Ruhe.

Als erstes kam eine Reaktion von GMX. Sie nahmen die Gelegenheit wahr, eine E-Mail zu schreiben. Und es kam alles sauber rüber. Sie gaben die Kontaktdaten preis, und welche Geschäftsvorfälle gespeichert waren. Auch das

beauftragte Inkassobüro wurde aufgeschrieben. Somit bin ich da erstmal zufrieden.

Als nächstest kam eine E-Mail der Rechnungsstelle von Reichelt, die sich informieren wollten, was ich überhaupt will? Sie haben den Brief nicht verstanden. Also habe ich es möglichst einfach nochmal erklärt. Dann kam eine E-Mail, die verlangte, daß ich das Ganze per Brief beantragen soll.

Zuletzt kam ein Brief vom Weltbild-Verlag, dafür aber gleich zwei Seiten, wo vor und Rückseite bedruckt ist. Und die Abteilung im Weltbild-Verlag heißt „Datenschutz“. War mir sehr angenehm. Zuerst kam die Kontaktadresse und die Kundennummer. Dann haben sie zwei Firmen hingeschrieben, an die Sie die Daten weitergegeben haben, mit Adresse und Ansprechpartner. Dann kommen Screenshots von der Kundendatenbank: Kundendatenbank, Auftragsübersicht und die Debitorenübersicht. Zuletzt haben Sie empfohlen, mich auf die Robinsonliste zu setzen.

Es ist relativ klar, daß die letzte Antwort die beste Lösung für meine Anfrage darstellt und es bleibt zu hoffen, daß in Zukunft auch andere Firmen dem Beispiel folgen.

Alles in allem kann ich jedem nur empfehlen, es ebenfalls auszuprobieren. Vielleicht kommen ja in Zukunft weitere Beiträge von anderen, und vielleicht können wir unsere Erfahrungen etwas austauschen.

WIKIPEDIA
DELETING YOUR KNOWLEDGE
SINCE 2001.

Tschunk nach Art des Hauses

1. Limonen waschen, achteln und in ein stoßfestes Glas (35 cl) geben,
2. einen Teelöffel braunen Zucker darüber streuen,
3. Limonen und Zucker mit einem Holzstößel zerdrücken,
4. Glas bis zur Hälfte mit *crushed ice* auffüllen,
5. 6 cl Havanna Club (3Y) hinzugeben,
6. mit Club-Mate auffüllen,
7. liebevoll mit Strohhalm und Deko verzieren.

Tschunk für junge Hacker

1. Limonen waschen, achteln und in ein stoßfestes Glas (35 cl) geben,
2. einen Teelöffel braunen Zucker darüber streuen,
3. Limonen und Zucker mit einem Holzstößel zerdrücken,
4. Glas bis zur Hälfte mit *crushed ice* auffüllen,
5. – entfällt –
6. mit Club-Mate auffüllen,
7. liebevoll mit Strohhalm und Deko verzieren.

Zweites Leben für C-Netz-Telefone

von Philipp Fabian Benedikt Maier

<philipp.maier@runningserver.com >

Vor dem GSM-Netz gab es das C-Netz. Manch einer wird sich erinnern, es war das letzte Mobilfunknetz, bei dem die Sprache noch analog übertragen wurde. Als Abhörschutz verwendete man eine Sprachverschleierung, die das Audiospektrum invertierte und die Sprache so unverständlich machte. Das C-Netz gibt es nicht mehr. Die Telefone allerdings schon, und es gibt Hoffnung.

Es ist nämlich so, daß ganz in der Nähe des C-Netzes (450 Mhz), etwas weiter unterhalb bei 440 Mhz, das 70 cm Amateurfunkband beginnt. Wenn man es schaffen könnte, den Transceiver eines C-Netz-Telefones so zu verbiegen, daß er im 70cm-Amateurfunkband arbeitet und zusätzlich eine neue Telefonsoftware schreibt, könnte man sein C-Netz-„Handy“ als Funkgerät wiederbenutzen.

Ein Informatiker [1] aus Hessen hat genau das für gleich mehrere C-Netz-Telefone gemacht. Je nach Telefon müssen ein paar mehr oder weniger einfache Modifikationen am HF- und Digitalteil des Telefons durchgeführt werden. Eine neue Firmware erledigt den Rest.

Für den Umbau geeignet sind Siemens C3, C4, C5 und das Philips Porty. Beim C5 ist der Umbau und die neue Software bisher am weitesten entwickelt. Selbst der Kartenleser funktioniert, und die alte C-Netz-Karte kann als Frequenzenspeicher wiederverwendet werden. Ideal, wenn man den Standort wechselt, denn dann kann man die ortsspezifischen Relais auf einer dedizierten Karte speichern. Auch in Zukunft wird es um das C5 noch einmal spannend werden, eine digitale D-Star-Karte ist zur Zeit in Entwicklung.

Um damit dann auch telefonieren bzw. funken zu können, braucht man noch eine Amateurfunklizenz. Diese bekommt man von der Bundesnetzagentur, nachdem man die Amateurfunkprüfung (ein Ankreuztest wie beim Führerschein) bestanden hat.

[1] *http://www.digisolutions.de/*

PS: Auch der Skyper lebt im Amateurfunkband weiter – aber das ist eine andere Geschichte.

The dark side of cyberspace

Keine Ausbeutung mit Steuergeldern – für den fairen öffentlichen Einkauf von PCs

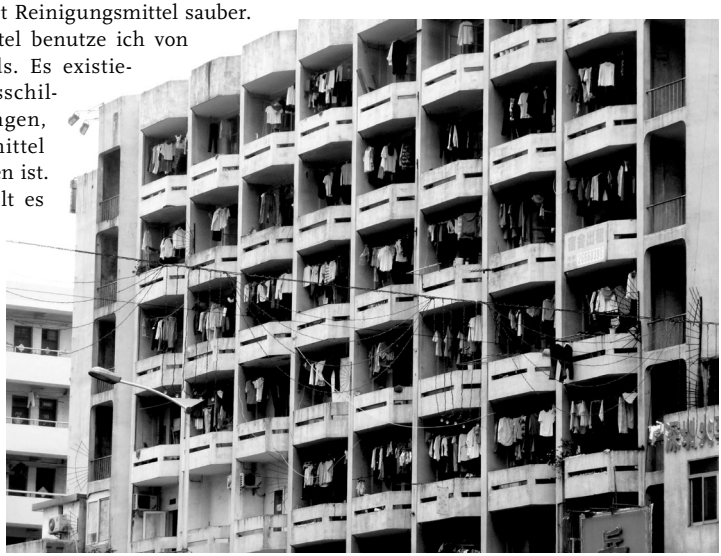
von Sarah Bormann und Johanna Kusch

Markenkonzerne wie Fujitsu-Siemens-Computers (FSC) pflegen ihr grünes Image und zunehmend gewinnt die Energieeffizienz der Geräte an Bedeutung. Aber auf die Forderung, grundlegende Arbeitsrechte in der Produktion einzuhalten, fällt den Unternehmen bislang nichts Schlaues ein. Statt gewerkschaftlicher Organisierung setzen sie auf einen nichtssagenden Verhaltenskodex – den Electronic Industry Code of Conduct (EICC). Der Weg zum „fairen" PC ist noch lang. Es eröffnen sich allerdings neue Perspektiven, wenn sich die öffentliche Hand mobilisieren läßt.

Grün ist nicht genug. Auf der CeBIT 2008 wurde erstmals „Green IT" zum Thema gemacht. Das ist begrüßenswert, allerdings decken Umweltbelastung und Elektroschrott nur die eine Seite der Medaille ab. Die ökologischen Kosten der Produktion und Verschrottung von PCs sind weltweit ungleich verteilt, und unter der Verwendung giftiger Stoffe leiden als erstes die Arbeiterinnen in den Fabriken. Die zweite Seite der Medaille sind folglich die sozialen Probleme. "Jeden Tag mache ich Leiterplatten mit einer Art Reinigungsmittel sauber. Dieses Lösungsmittel benutze ich von morgens bis abends. Es existieren keine Hinweisschilder oder Erklärungen, wie das Lösungsmittel richtig zu handhaben ist. Unser Aufseher hält es nicht für notwendig, irgendwelche Schutzmaßnahmen zu treffen, ihm ist es völlig egal", berichtet eine junge Arbeiterin aus China in einem Interview mit SACOM, die bei Excelsior Electronics Leiterplatten reinigt. Das Zulieferunternehmen produziert u. a. für FSC, Apple, Sony, Intel und AMD. SACOM ist eine Hongkonger Organisation, die sich aktiv für die Einhaltung von Arbeitsrechten einsetzt und öffentlich das Fehlverhalten von Unternehmen kritisiert.

Die Einkaufsmacht der öffentlichen Hand

Noch gibt es ihn nicht, den „fairen" Computer, der unter Einhaltung fundamentaler Arbeits-



Die wahren Hardware-Spezialisten

rechte und minimaler Umweltbelastung produziert wird. Individuelle Verbraucherinnen unterliegen hier ausnahmsweise mal nicht der Qual der Wahl. Ob das Notebook den Markennamen von Hewlett Packard, Dell, Lenovo oder Fujitsu-Siemens-Computers trägt, in der Regel sind es eine begrenzte Anzahl von Kontraktfertigern, die auf dem chinesischen Festland die Notebooks unter zweifelhaften Bedingungen produzieren. Anders ist die Situation für öffentliche Einrichtungen. Sie haben die Möglichkeit, in ihren Ausschreibungen zum Einkauf von Produkten und Dienstleistungen die Einhaltung von ökologischen und auch von sozialen Standards von den Bietern zu fordern. In der Europäischen Union beschafft die öffentliche Hand jährlich ca. 600.000 Desktop-PC (*http://www.beschaffung-info.de/*). Damit verfügt sie über eine enorme Einkaufsmacht, mittels derer sie Handlungsdruck auf Unternehmen erzeugen kann.

Faire Beschaffung ist im Kommen

Schon jetzt nehmen immer mehr Gemeinden soziale Kriterien in ihre Ausschreibungen auf: Fair produzierte Kleider für das Feuerwehrpersonal, Pflastersteine ohne Kinderarbeit oder fair gehandelte Nahrungsmittel in den Kantinen sind einige Beispiele. In punkto Computer geht die Schweiz mit gutem Beispiel voran. Dort verfügen bereits viele Städte über eine sozial und ökologisch ausgerichtete Beschaffungsstrategie von IT-Geräten, oder aber sie haben das Postulat „für eine nachhaltige öffentliche Beschaffung von Computern“ angenommen bzw. zur Abstimmung in den Gemeinde- bzw. Kantonsrat eingereicht. Auch der aktuelle Gesetzesentwurf der Schweiz setzt auf einen sozialen Einkauf. So müssen alle vom Bund gekauften Güter, also auch Computer, unter Einhaltung der Kernarbeitsnormen der Internationalen Arbeitsorganisation produziert werden.

Schlußlicht Deutschland

In Deutschland wurde die Reform des Vergaberechts aufgrund der Vereinheitlichung der Vergaberegelung in der Europäischen Union notwendig. Mit drei Jahren Verspätung hat die Bundesregierung Anfang 2009 das neue Vergabegesetz verabschiedet. Den Trend hin zu einer sozialen und ökologischen Beschaffung hat sie allerdings verschlafen. Es bleibt bei einer Kann-Regelung, wonach es der öffentlichen Einrichtung lediglich möglich ist, soziale Kriterien zu berücksichtigen. Eine Empfehlung hierzu oder gar eine Verpflichtung zur Anwendung sozialer und ökologischer Kriterien besteht nicht. Trotz dieser Schwäche herrscht nun mehr Klarheit über die praktischen Möglichkeiten der Beschaffungsstellen. Noch im August 2007 argumentierte ein Gutachten im Auftrag des Bundesministeriums für Wirtschaft [1], daß soziale Kriterien bei der öffentlichen Auftragsvergabe vergabefremd und damit obsolet seien. Dieses Gutachten kann nun getrost im Mülleimer landen.

Der Bedarf nach fortschrittlichen Präzedenzfälle ist da. Geiz ist bekanntlich geil – aber geht es auch anders? Die im neuen Gesetz erwähnte Variante sieht die Nennung der sozialen Kriterien in den sogenannten Auftragsausführungsbestimmungen vor. Diese sind nur für den Bieter bestimmend, der die Ausschreibung gewonnen hat. Die Umsetzung erfolgt meist in Form einer standardisierten Bietererklärung, in der der öffentliche Einkäufer definiert, welche Anforderungen vom Bieter erfüllt und nachgewiesen werden müssen. Auf die Wertung aller eingegangenen Angebote haben sie allerdings keinen Einfluß. Um in sozialer Hinsicht progressive Bieter zu bevorzugen, wäre jedoch genau dies wünschenswert. So könnte beispielsweise neben dem günstigsten Preis und der Erfüllung der technischen Anforderung auch die Einhaltung von bestimmten sozialen Kriterien in die Gesamtbewertung jedes einzelnen Angebots einfließen.

Es spricht also viel dafür, in Ausschreibungen auch progressivere Varianten zu erproben, die entsprechend größere Wirkung zeigen. Die Auslegung des Vergaberechts ist derzeit noch umstritten und wird sich im Wechselspiel mit der Vergabepraxis entwickeln. Auch die Anwendung ökologischer Kriterien war vor wenigen Jahren noch nicht rechtssicher umzusetzen. Mittlerweile ist grüne Beschaffung europaweit fest etabliert. Durch ambitionierte Ausschreibungen wurden hier Präzedenzfälle geschaffen.

Öffentlichen Druck erzeugen

Die Möglichkeit ist vorhanden, ökologische und soziale Kriterien beim öffentlichen Einkauf von Computern zu berücksichtigen. Die Hürde stellt nun die praktische Umsetzung dar. Die zuständigen Beschaffungsstellen müssen für das Problem sensibilisiert und mobilisiert werden. Es bedarf der Unterstützung politischer Entscheidungsträgerinnen, vor allem aber auch einer wachsenden Aufmerksamkeit der kritischen Öffentlichkeit. Die globalisierungskritische Organisation WEED (Weltwirtschaft, Ökologie und Entwicklung) setzt sich seit 2005 mit ihrem Projekt PC Global für Arbeitsrechte und Umweltgerechtigkeit in der Produktion und Verschrottung von Computern ein. Im Jahr 2008 initiierte sie die europäische Kampagne procureITfair. [2] WEED unterstützt Einzelpersonen, die sich an ihrem Arbeitsplatz, ihrer Uni, in ihrer Gemeinde für eine soziale und ökologische Beschaffung von Computern einsetzen wollen. Darüber hinaus berät WEED auch Beschaffungsstellen bei ihren Ausschreibungen.

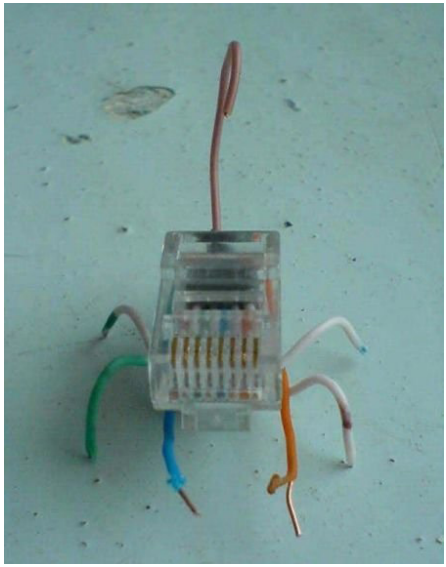
Weitere Informationen

Digitale Handarbeit – Chinas Weltmarktfabrik für Computer, DVD, 28 Minuten, 2008, (dt., engl., frz.)

Leitfaden für die soziale und ökologische Beschaffung von Computern. Bestellung bei WEED: *http://www.weed-online.org/*, E-Mail: *weed@weed-online.org*

[1] Stellungnahme des wissenschaftlichen Beirats beim Bundesministerium für Wirtschaft und Technologie: „Öffentliches Beschaffungswesen", Mai 2007

[2] *http://www.pcglobal.org/* und *http://www.procureitfair.org/*



Die Welt von morgen: FAQ Familieninternet 2017

von maha <maha@ccc.de>

Oft gestellte Fragen zum Familieninternet, aus einer Broschüre des Bundesministeriums für Familie, Wahres, Gutes, Jugend und Sport (Stand: 1. Juni 2017)

Ist es unbedenklich, im Familieninternet zu surfen?

Ja, geeignete Internet-Filter sorgen dafür, daß Inhalte, die in der Lage sind, potentiell gefährlich zu sein, von vornherein für alle Nutzer des Familieninternets unzugänglich gemacht werden.

Welche Inhalte gelten als bedenklich?

Die Bundesregierung möchte auch den jüngsten Surferinnen Zugang zum Familieninternet ermöglichen. Daher werden alle Inhalte als bedenklich eingestuft, die das psychische Gleichgewicht und die Entwicklung von Kindern ab einem Alter von zwei Jahren gefährden könnten, denn die Bundesregierung geht davon aus, daß Kinder ab diesem Alter selbständig surfen sollen. Zudem sind alle Inhalte als gefährlich anzusehen, die geeignet sind, das Wahlverhalten oder die Wertvorstellungen der Bürgerinnen zu beeinflussen.

Werden überall die gleichen Inhalte gefiltert?

Die europäische Filterbehörde kennzeichnet alle Inhalte danach, in welcher Region sie gefiltert werden. Das ist besonders für ein föderales Land wie Deutschland wichtig, da hier in den einzelnen Bundesländern unterschiedliche Vorstellungen über das Gefährdungspotential von Inhalten bestehen.

Sie profitieren vom Familieninternet: Kinderreiche Familie in Deutschland.

Ist es möglich, die Filtermechanismen zu umgehen?

In Ausnahmefällen kann es sogenannten Hackern – also Schwerstkriminellen – gelingen, durch illegale Anonymisierung Filter zu umgehen. Schon das Ansinnen steht allerdings unter Strafe.

Was geschieht, wenn ein Nutzer absichtlich oder unabsichtlich eine gesperrte Seite ansurft?

Gelegentlich wird ein Stop-Schild angezeigt. In den meisten Fällen wird jedoch gar nichts angezeigt, oder es erfolgt eine Umleitung auf eine harmlose Seite. In jedem Fall werden alle verfügbaren Informationen über diesen Nutzer in die zentrale Gefährderdatei aufgenommen.

Wie kann ich verhindern, daß meine Inhalte gefiltert werden?

Als Anbieter von Inhalten sollten Sie nur Unbedenkliches im Netz publizieren (s. o.). In Zweifelsfällen berät sie gern eine der von der Bundesregierung eingerichteten Wahrheitsagenturen.

Wie bin ich vor Falschinformationen aus dem Internet geschützt?

Die Bundesregierung bemüht sich, Webseiten auszufiltern, die aus ihrer Sicht Falschinformationen enthalten. Sie arbeitet im Übrigen mit der Wikitrust-Foundation zusammen, die für die spurlose Löschung von Informationen aus der Wikipedia verantwortlich ist. Gelöscht werden Informationen, die von der US-Regierung für falsch oder irreführend gehalten werden könnten, und solche, die wichtige Rechte bestimmter Persönlichkeiten beeinträchtigen könnten. Für die Bundesregierung ist das ein sinnvoller Beitrag zum Datenschutz – auch über die Wikipedia hinaus! Sollten Sie dennoch Falschinformationen auf Webseiten finden, zeigen Sie diese bitte zur einstweiligen Sperrung an.

Warum gibt es nicht auch für Rundfunk und Fernsehen solche effizienten Filtermaßnahmen?

Rundfunk und Fernsehen sind in Deutschland privat oder öffentlich-rechtlich. Die Bundesregierung hat hier also nicht die gleichen Steuerungsmöglichkeiten. Allerdings gibt es inzwischen immer mehr Filtermöglichkeiten, dadurch daß das Internet bevorzugter Übertragungsweg für Rundfunk und Fernsehen wird. Auch der Telefonverkehr (VoIP) unterliegt den Filtermaßnahmen.

Handelt es sich bei diesen Maßnahmen um Zensur?

Nein, eine Zensur findet nicht statt.

CENSILIA 2.0

Anmerkung des Autors

Ich schrieb diese Dystopie Anfang 2009. Inzwischen hat sich vieles in der deutschen Politik verändert: Dystopien treten schneller ein, als man sie schreiben kann. Da ich davon ausgehe, daß es noch in dieser Legislaturperiode zu weitreichenden Einschränkungen der Grundrechte kommen wird, möchte ich die Jahreszahl 2017 durch 2012 ersetzen. *<maha>*

Die Volkszählung 2011 – SELECT * FROM BUERGER

von Scytale <scytale@oqlt.de> und

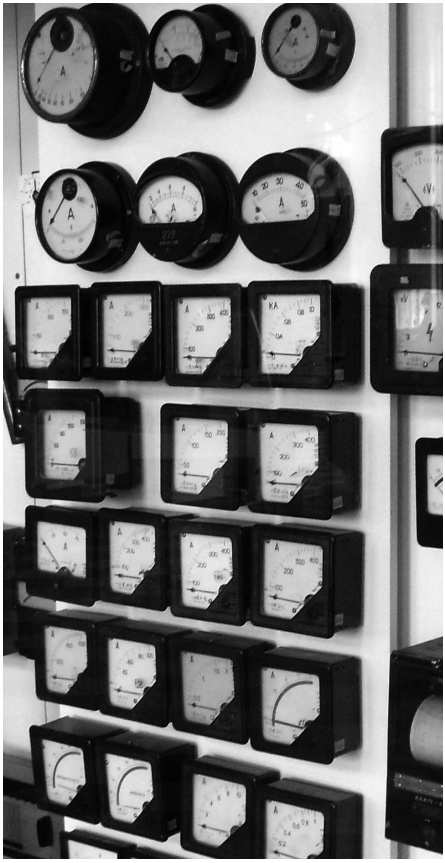
Unicorn <mail@oliverknapp.de>

Name, Anschrift(en), Geburtsdatum, Geschlecht, Familienstand, Ehepartner, Kinder, Heiratsdatum, Scheidungsdatum, Teilnahme an einem Zeugenschutzprogramm, Religionszugehörigkeit, Arbeitgebe, Ausbildung, Beruf und Arbeitslosenstatus. Das alles bekommen die Landesämter für Statistik. Für jeden einzelnen Bürger. Und leiten es an das Bundesamt für Statistik weiter, das all diese Daten in eine riesige Datenbank wirft. Verknüpft unter einer gemeinsamen Ordnungsnummer.

Klingt wie ein schlechter Scherz? Ist es nicht. Die Vorbereitungen laufen auf Hochtouren. Stichtag ist der 9. Mai 2011. An diesem Tag wird das alles stattfinden, die nächste Volkszählung (neudeutsch: Zensus). Beschlossen schon vor fast einem Jahr im am 16. Juli 2009 verkündeten „Gesetz über den registergestützten Zensus im Jahre 2011“ (ZensG 2011). Umgesetzt wird, wie so oft, eine EU-Richtlinie (763/2008). Natürlich schießen wir mal wieder vorbildlich über das Ziel hinaus: Von der Abfrage der Religionszugehörigkeit beispielsweise ist in der Richtlinie keine Rede.

Nach dem massiven Widerstand in der Bevölkerung, der 1983 die geplante Volkszählung vor das Bundesverfassungsgericht gebracht hat und in einem wegweisenden Urteil (dem wir das Recht auf informationelle Selbstbestimmung verdanken) mündete, mußte der Zensus damals um vier Jahre verschoben, umstrukturiert und anonymisiert vorgenommen werden. Diesmal läuft es anders: Die Vorbereitungen laufen unter dem Radar, kaum jemand in der Bevölkerung weiß überhaupt, daß es 2011 eine Volkszählung geben soll. Google News findet zum Thema nur ca. dreihundert Artikel — je einhundert in den Jahren 2008, 2009 und 2010.

Ein weiterer Unterschied zu den Achtzigern ist, daß damals noch mit Papier und Stift jeder einzelne Deutsche befragt wurde. Da solch ein Ansatz aber (so zumindest die offizielle Begründung) als zu teuer eingeschätzt wird, soll 2011 ein „registergestützter Zensus“ durchgeführt werden. Das bedeutet im Grunde nichts anderes, als daß die Datenbanken der Meldebehörden und Arbeitsagenturen als Datengrundlage herangezogen werden. „Herangezogen“ heißt hier: Sie werden ohne Anonymisierung an die Statistikämter weitergeleitet. Konkrete Vorgaben zu Verschlüsselung oder anderen techni-



schen Vorkehrungen bezüglich der Speicherung macht das Gesetz nicht. Aber hey, keine Sorge, das sogenannte Statistikgeheimnis schützt uns alle vor Mißbrauch.

Geplant wird diese umfangreiche Datensammlung bereits seit Anfang 2000 (siehe auch Datenschleuder #75), seitdem arbeiten Statistiker bundesweit an der Optimierung ihrer Algorithmen. Das Problem ist die nur begrenzt genaue Datensammlung in den Meldebehörden, welche zudem noch nicht mal unbedingt einheitliche Datensätze vorhalten. Aus diesem Grund sollen etwaige Fehlmeldedaten mit Hilfe der anderen Datenbanken ausgeglichen werden. Es ist in den Statistikämtern also nicht nur möglich, sondern konkret angedacht, die einzelnen Datenbanken personengenau miteinander zu verknüpfen. Daß dabei die umfassendste Bevölkerungskartei der Geschichte Deutschlands entsteht, ist nicht Bug, sondern Feature.

Als zusätzliches Bonbon für eine hoffentlich stattfindende verfassungsrechtliche Klärung des Zensus 2011 werden diese Daten dann auch noch über eine eindeutige Personenkennziffer verknüpft und zugänglich gemacht. In seinem Volkszählungsurteil hat das Bundesverfassungsgericht zum Thema Personenkennziffer ausgeführt, daß *„eine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebensdaten und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger […] auch in der Anonymität statistischer Erhebungen unzulässig [ist].“* (BVerfG 65, 1 Abs. 177)

Leider ist wohl aufgrund der geringen medialen Präsenz des Themas unseres Wissens nach noch kein Bürger auf dem Weg nach Karlsruhe.

Warum wird überhaupt gezählt?

Auf Grundlage der Bevölkerungsverteilung werden in Deutschland viele zum Teil wichtige Entscheidungen getroffen. Ein gerne angeführtes Beispiel ist das Stimmengewicht eines Bundeslandes in Bundesrat. Augenscheinlich findet hier eine Stimmgewichtung nach Einwohnerzahl der Bundesländer statt. Gerade beim Bundesrat handelt es sich um ein System, welches auf der Basis geschichtlicher Entwicklung und machtpolitischer Spiele während der Gründung der Bundesrepublik entstanden ist. Es geht beim Bundesrat weniger um ein gleiches Stimmgewicht für alle Bundesländer (basierend auf der Bevölkerungszahl), als vielmehr um eine stark vereinfachte Verteilung mit wenigen Rahmenbedingungen (Stichwort Sperrminorität). Dieses System führt dazu, daß jeweils rund 220.000 Bremer durch einen Sitz im Bundesrat vertreten werden, allerdings in Nordrhein-Westfalen ein Sitz fast drei Millionen Bürger repräsentiert. (Im Durchschnitt entsprechen übrigens 1,2 Millionen Einwohner einem Sitz im Bundesrat.)

Auf Gemeindeebene wird gern die leistungsgerechte Bezahlung der Bürgermeister angeführt. Da solch eine Regelung nur schwer zu finden ist, wird versucht, anhand der Einwohnerzahl das Gehalt zu begründen. Aber nicht nur das Gehalt des Stadtvorsitzenden hängt an der genauen Zahl der Beherrschten, sondern auch die fürs Ego enorm wichtige Frage, ob er denn nur Bürgermeister oder etwa doch Oberbürgermeister genannt wird.

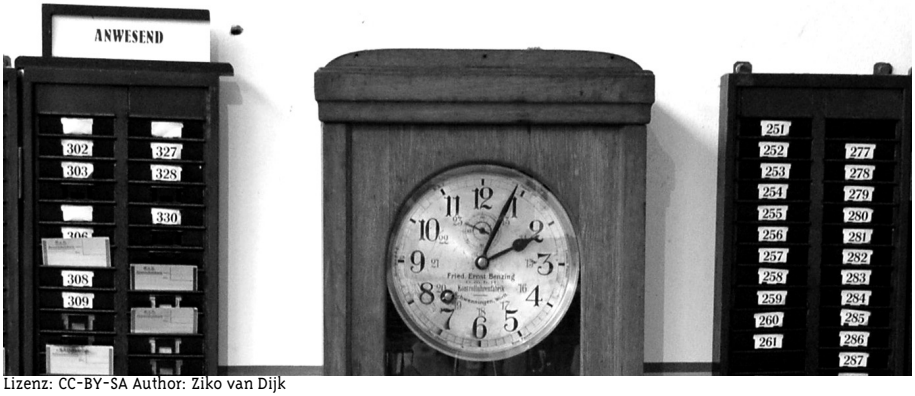
Darüberhinaus hat der Zensus allerdings auch sehr viel großflächigere (und wohl für einige Bundesländer schmerzhafte) Auswirkungen. Neben der bereits angesprochenen Stimmenanzahl im Bundesrat wird die Tatsache, daß der sogenannte Länderfinanzausgleich (der dazu dient, die Finanzkraft der Bundesländer sukzessive anzugleichen) zu einem Großteil auf der Einwohnerzahl basiert, und die zu erwartenden Korrekturen der Einwohnerzahlen sicherlich zu heftigen politischen Diskussionen führen. Denn eigentlich drückt sich die Politik seit Jahren um die Veränderungen, die hier auf sie zukommen werden. Womöglich war einigen Abgeordneten damals beim Handheben nicht klar, welche Konsequenzen ein neuer Zensus haben wird.

Gibt es eine Alternative?

Wenn man sich das ZensG 2011 durchliest, stellt man recht schnell fest, daß es während der Ausarbeitung keinerlei störende Einflüsse von Datenschützern gegeben hat. Die Alibi-Beteiligung der Datenschutzbeauftragten der Länder und des Bundes haben offensichtlich nicht dazu geführt, daß das Gesetz dem Grundsatz der Datensparsamkeit gehorcht.

Anstatt einer Auswahl wirklich nötiger Datenbankfelder wird einfach eine Komplettsammlung aller Meldedaten festgeschrieben. Das führt zu einer anschriftengenauen Speicherung, die dann noch mit Hilfe der Daten von Beamten und der Bundesagentur für Arbeit optimiert wird. Während 1987 noch eine sogenannte „blockweise Anonymisierung“ (im Sinne von „Häuserblock“) durchgeführt wurde, soll es diesmal also personengenau zugehen. Auf lästige Hindernisse wie die eigentliche existierende Zweckbindung der Meldedaten sowie die informationelle Selbstbestimmung eines jeden Deutschen wird bewußt verzichtet.

Eine Alternative für das Problem der Feststellung der genauen Einwohnerzahl wäre daher eine dem Subsidaritätsprinzip gehorchende Summenerfassung. Anstatt also alle Einzeldaten in einer zentralen Datenbank zu speichern, könnte man eine reine Summenübermittlung (blockweise oder straßenweise) mit anschließender Löschung der Einzeldaten durchführen. Natürlich steigt hier der Erhebungsaufwand, allerdings ist dies im Hinblick auf die Einschränkung der Grundrechte wohl eine der wenigen gangbaren Möglichkeiten zur datenschutzkonformen Zensusdurchführung.



Demogrundregeln für Nerds

Noch keine Terroristen <ds@ccc.de>

In den vergangenen Jahren wurden Nerds vermehrt mit Ansammlungen von Gleichgesinnten zur Bekundung ähnlicher Absichten in der realen Welt konfrontiert. Dieses Konzept ist für die meisten Bürger nicht neu und unter dem Namen „Demonstration" bekannt. Primäres Ziel ist es dabei, andere Menschen über die eigene Absicht und das meist politische Bestreben aufzuklären.

Hierzu dienen kleine Papierfetzen (Flyer) und große Layer-Ads, zuweilen auch Fahnen. Anders als im Internet gelten im echten Leben teils überraschende Spielregeln – für Anfänger bietet sich vielleicht zunächst ein Realitätsabgleich im Supermarkt, für Hardcore-Zocker auch der Besuch in einer Großraumdisco nach Wahl an.

Jede Demonstration bekommt verschiedene „Auflagen", das sind die erweiterten ACL, wo auch die Route konfiguriert ist. Meistens ist die Route nicht nach Effizienz- oder Geschwindigkeitskriterien optimiert, sondern soll im Gegenteil die Öffentlichkeits-Exposure jedes Pakets maximieren. Dies sollte sich auch bei der Bewältigung dieser Route bemerkbar machen: Anders als auf einer Platte ist eine Fragmentierung also durchaus der Stackbildung vorzuziehen. Auch die Anwendung von optimierenden Routenfindungsalgorithmen reduziert unnötig die *exposure time*. Zur Erinnerung: Zweck des Auf-die-Straße-Gehens ist das öffentlichkeitswirksame Präsentieren der eigenen Präferenz – ganz wie die ‚powered by emacs/vim/pico'-Badges auf Deiner Homepage – als feste

Überzeugung, Sendungsbewußtsein, deutlich sichtbar für alle.

Hier als *quick reference* die wichtigsten Spielregeln vorab: Waffen (Messer, Bathlets, Lockpick-Sets), auch passive, sind verboten – hierzu zählen meist auch Stahlkappenschuhe sowie Schutzbewaffnung wie „Storm Trooper"-Helme, stählerne Notebook-Schutzhüllen und Thermoskannen. Und auch wenn es den durchschnittlichen Nerd überrascht: Ein Leatherman wird aufgrund der an ihm befestigten Klinge vordergründig als Waffe und nicht als Werkzeug wahrgenommen. Und da trainiertes Personal auch mit harmlosen „Club Mate"-Flaschen Critical-Damage-Attacks landen können, sind sie als „gefährliche Gegenstände" von einigen Demonstrationen banned. Diskussionen mit dem Admin erübrigen sich hier. Der Süchtige sollte durch Umfüllen vorsorgen. Neuerdings sind sogar Fahrräder ungern gesehen, denn sie sind als Blockadewerkzeug verschrien. Nicht verboten sind hingegen Geräte zur visuellen Dokumentation.

Es ist nur auf den ersten Blick erstaunlich, daß es bei diesem Spiel die *player stats* nicht randomisiert, sondern zugunsten Team Grün oder Schwarz und neuerdings auch Blau biased sind. Während die Demonstranten einzig mit Hand und Fuß unterwegs sind, haben diese Teams Knüppel, Feuerlöscher, Reizgas, Pistolen und zuweilen Quarzhandschuhe dabei. So eine geschlossene Einheit muß man sich als Horde Orks mit Quad Damage und GM-Hotline vorstellen. Dies alles ist im Gewaltmonopol des Staates begründet, im Klartext: Im *real life* ist der Staatsdiener *root*. Ein Einreihen in den eigenen Zug muß dabei – wie das Capturen der eigenen Flagge – verhindert werden.

Und als ob die *man pages* nicht schon jetzt verwirrend genug würden, gibt es neben Waffen noch eine weitere mögliche Problemquelle: das Vermummungsverbot, der eingebaute Wall-Hack der Polizei. Im Prinzip ist Vermummen wie das Surfen über Proxy, jedoch wird es in der echten Welt als verbotenes Cheating verstanden, wenn das Gesicht soweit verdeckt ist, daß eine Identifikation nicht mehr möglich ist. Dieses Gesetz gibt es seit der Proteste gegen die Startbahn West und existiert fast ausschließlich in Deutschland. In anderen Staaten ist es vollkommen legitim, vermummt zu demonstrieren, in Deutschland bleiben einzig Voll-, Schnauz- und Zickenbärte, Fußballfarben im Gesicht sowie Make-up in beliebig dickem Auftrag. Perücken und Hornbrillen sind wegen der Silversurfer auch erlaubt. Da eine Guy-Fawkes-Maske oder ein ins Gesicht gezogenes Halstuch die Identifikation verhindert, könnte sie einige unangenehme Folgen haben. Dazu später mehr.

Im Gegensatz zur bijektiven Abbildung der freiwilligen Demonstrationsteilnehmer hat das Programm beim *reverse lookup* für die im Dienst befindlichen Teilnehmer einen Bug: Er funktioniert nur so mäßig. Rein optisch ist nur das Class-C-Netz leicht zuordenbar, der für

die individuelle Hostidentifikation notwendige Scan nach dem Dienstnummernport wird häufig wahlweise mit einem NXDOMAIN oder mit einem DDoS der gesamten Teams beantwortet. An einem Fix wird aber gearbeitet.

Meistens wollen die grünen Männchen als Action-Replay übrigens die schönsten Szenen der Demonstration nochmal anschauen. Daher machen einige dieser sogenannten Polizisten ein vollständiges *screen recording* während der Zeit der Demonstration und darüberhinaus. Eigentlich dürfen sie das nur bei Straftaten, also nicht grundlos. In der Praxis wird das Dauerfilmen irgendwie begründet, zum Beispiel dadurch, daß es dem Filmenden oder seinen Vorgesetzten stets so scheint, als würde eine Straftat unmittelbar bevorstehen. Wir kennen diese Argumentation alle zur Genüge und verzichten daher auf eine nähere Erläuterung.

Die Eigenfilmung – für das Familienalbum oder den „Beweis“, dabei gewesen zu sein – ist vielleicht eine schöne persönliche Erinnerung. Leider gibt es ein unschönes *real life back orifice*, manchmal bekommt die Rennleitung Zugriff auf die aufgenommenen Eindrücke. Und da es nicht immer möglich ist, keine Straftaten zu filmen, sollte versucht werden, die Daten nicht zu verlieren. Auch der Upload nach der Demo sollte gut überlegt sein; wenn da Menschen drauf zu erkennen sind, haben auch diese Persönlichkeitsrechte. Daher lieber mit einer Bildbearbeitungssoftware drübergehen und die Gesichter pink ausmalen. Für reine Erinnerungsbilder ist HD-Qualität nicht erforderlich. Einfach schön pixelig lassen, spart ja auch Bandbreite.

Es werden auch einige NPCs unter Euch sein. Ein paar davon sind leicht zu erkennen, andere schwerer. Es ist immer wichtig, diese Spezies zu isolieren. Die leicht zu erkennenden NPCs haben einen Knopf im Ohr. Andere sind durch wiederkehrende Verhaltensweisen erkennbar: Sie sind meist gepflegter und besser riechend und frisiert als Ihr, tragen Lederslipper aus der Kleiderkammer und manchmal Schnauzbärtchen; sie kiffen nicht und artikulieren keine Sprechchöre mit Euch. Eine mehr oder minder diskrete Markierung einmal erkannter NPCs gibt Karmabonuspunkte. Mehr Anhaltspunkte: Sie laufen auch nicht in Ketten von mehr als zwei Personen.

Pro-Tip: Das Vorwärtsschreiten in Ketten oder ähnlichen Formationen von mindestens fünf Personen zeigt Geschlossenheit. Typische Capture-the-Flag-Formationen sind hier durchaus praktisch. Falls es kalt ist, helfen Ketten auch durch gegenseitiges Wärmen bis hin zur Fraternisierung, nebenbei dienen sie der generellen Motivation.

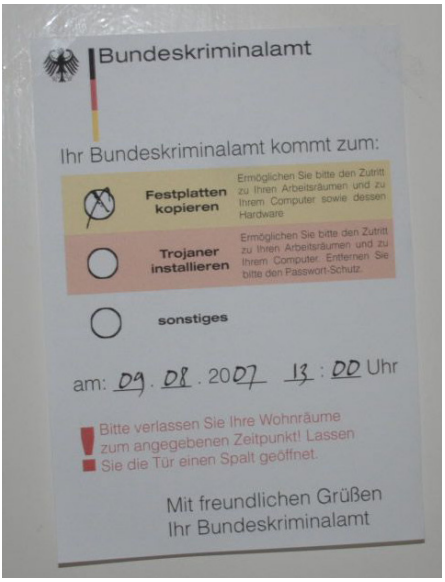
Polizisten auf Demonstrationen sind – anders als der Abschnittsbevollmächtigte/Kontaktbereichsbeamte bei Dir auf dem Dorf – kein Experimentierfeld für bürgernahe Kommunikation von Beamten. Versuche nicht, Bemerkungen und Phrasen, wie Du sie vom Chat kennst, beim Demonstrationen zu erproben. Vermeide auch mißverständliche Abkürzungen und Akrony-

me. Rechtsphilosophische Betrachtungen langweilen die meisten Polizisten eher.

Die Faustregel ist daher: Offen gezeigter Heiseforum-Umgangston wird dabei mit einem *forceful ban* bestraft: Zeigen des Mittelfingers in die Kamera, „Kameramann, Arschloch"-Sprechchöre, auch das sogenannte Mooning, welches üblicherweise durch das Herunterlassen der Hose durchgeführt wird, beendet das Abenteuer. Ein Neustart kann nicht sofort durchgeführt werden, denn diese und weitere Vorgehensweisen gelten als Beleidigung, im Falle des Moonings allerdings nur durch männliche Demonstrationsteilnehmer. Mangels körperlicher Masse oder meßbarer Kraft im Oberkörper wirst Du wahrscheinlich auch bei Anwendungen einfacher körperlicher Gewalt gegen andere Demonstrationsteilnehmer als Kollateralschaden weggewischt.

Falls Du im Eifer des Gefechts nach Einwirkung einer wasserähnlichen Substanz ein mittelschweres Reizen in Augen, Mund und andere Schleimhäute bemerkst, hast Du vermutlich das CS-Gas- oder Pfefferspray-Quest unlocked, seltener droppen die NPC radioaktive Substanzen aus russischen Beständen. Man vermeidet den vermehrten Kontakt mit diesen Substanzen, indem man ein *watch point* auf Männlein mit auf dem Rücken geschnallten Flüssigkeitsfläschchen setzt. Doch Vorsicht: Zuweilen erscheinen sie aus dem Nichts, und der Immu-Hack C_2H_5OH gegen CS-Gas hilft nicht bei Pfefferspray. Erfahrene Demonstrierer können auch neuartige Mentaltechniken einsetzen, und ein gewisser Prozentsatz der Bevölkerung ist ohnehin immun gegen Pfefferspray. Ob Du dazugehörst, kannst Du nur durch einen mutigen Selbsttest herausfinden.

Überwindest Du den *specific annoyance threshold* eines der Spielleiter, hast Du eventuell sogar die Gelegenheit, eine sogenannte Wache zu besuchen. Diese Wache mußt Du Dir als Respawn-Point für Polizei-NPCs vorstellen. Dafür ist es dringlich zu empfehlen, zur Authentifizierung Client Certificates in gedruckter Form dabeizuhaben (Ausweispapiere). Gelegentlich werden einem dann kostenfreie Fahrdienstleistungen



nach Hause angeboten, zu anderen Gelegenheiten wurde von überraschendem Einlaßbegehren im festgestellten *home* mittels einer der Root-CA signierten Login-Urkunde (aka Durchsuchungsbeschluß) berichtet.

Einmal hereingelassen startet der Besuch ein `grep -R evil *`. Daher zuhause aufräumen. Zufallsfunde (kopierte mp3s, nicht bezahlte Software, usw.) sind unschön und meist nicht Seiteneffektfrei. Einige Vertreter der Horch&Guck-Gruppe nehmen gar alles mit, was komplex genug aussieht, um der Wache einen modernen Look zu verleihen. Hierzu gehören leider in letzter Zeit immer wieder Computer. Um seinem demokratischen Recht auf obig erwähnte Überzeugungsbekundung unbeschadet nachgehen zu können, lohnt es, die Ratschläge zu verinnerlichen und vor allem möglichst oft live und auf der Straße anzuwenden.

Weitere informationen:

Udo Vetter: Sie haben das Recht zu schweigen
http://events.ccc.de/congress/2006/Fahrplan/events/1346.en.html

Psychologische Grundlagen des Social Engineering

Stefan Schumacher <stefan@net-tex.de>

Social Engineering ist eine Angriffsstrategie, die nicht die Technik als Opfer auserkoren hat. Stattdessen wird hier lieber – und vor allem effizienter – der Mensch bzw. sein Verhalten angegriffen. Ein Angreifer verwendet verschiedene Strategien und Taktiken, um aus Benutzern der Systeme Informationen wie Paßwörter oder IP-Adressen herauszuholen. Mit Hilfe dieser Informationen kann er erfolgreiche Angriffe gegen Zielsysteme fahren.

Die Motivation für einen Angriff kann unterschiedlich sein, neben professionellen Gründen wie Industriespionage oder Identitätsdiebstahl kommen auch soziale Gründe wie Rache oder Spaß und Machtgefühl in Frage. Das „richtige" Social Engineering, Human Based Social Engineering genannt, setzt zum Großteil auf soziale Beziehungen als Angriffsvektor.

Zuerst benötigt der Angreifer möglichst viele Informationen über die anzugreifende Organisation. Diese kann er aus freien Informationen, wie beispielsweise der Webseite oder Werbebroschüren, zusammensammeln und sich so ein Bild machen. Man kann auch den Müll durchwühlen und so an relevante Daten kommen. Außerdem können gewieftere Angreifer über E-Mail oder Telefon Kontakte zu Mitarbeitern herstellen und sich als jemand anderes ausgeben: als ein Kunde oder Vorgesetzter beispielsweise, der dringend Informationen benötigt. Mit diesen kann er dann andere Opfer beeindrucken oder einwickeln. So kann er anderen Mitarbeitern am Telefon beispielsweise intime Kenntnisse des Betriebs vorgaukeln oder schneller Kontakte knüpfen.

Dieses Sympathie-Aufbauen läßt sich auf verschiedenen Wegen durchführen, beispielsweise durch Verbrüderung mit Opfern, indem man einen gemeinsamen Gegner vorgibt. Andere Maschen sind Vorspiegelung von Autorität, was insbesondere in strengen Hierarchien wie Polizei, Armee oder Feuerwehr gut funktioniert. Selbst jemand, der nur Grundwehrdienst geleistet hat, kann mit etwas Geschick und Witz als Offizier auftreten und eine Dienststelle auseinandernehmen. Wer das nicht glaubt, sollte einmal die Abenteuer des Gefreiten Asch in Hans Helmut Kirst (1954) nachlesen oder den Hauptmann von Köpenick anschauen.

Aber auch in normalen Unternehmen gibt es Hierarchien, die sich ausnutzen lassen: So kann sich der Angreifer als wichtiger Kunde oder hoher Verantwortlicher einer anderen Filiale ausgeben. Unter Aufbau einer passenden Drohkulisse kann man hier Mitarbeiter zur Herausgabe von Daten bewegen. Gerade bei Telefonaten muß der Angreifer über rhetorisches Geschick und Intelligenz verfügen.

Psychologische Grundlagen der Manipulation

Ein Social Engineer (auch Trickbetrüger oder Hochstapler) verwendet als Angriffstechnik verschiedene Beeinflussungsmethoden. Dabei helfen ihm Faustregeln und Stereotype des menschlichen Verhaltens. Dies sind feste Handlungsmuster, die praktisch jedesmal gleich ablaufen. Sie verkürzen und vereinfachen anhand von Urteilsheuristiken gedankliche Prozesse der Entscheidungsfindung. Hervorgerufen werden sie durch ein oder mehrere Auslösemerkmale. Man bezeichnet eine derartig mechanische Reaktion auf bestimmte Informationen als automatisches Verhalten.

Analysiert man solche psychologischen Reaktionen und Verhaltensweisen, kann man automatische Reaktionen besser verstehen, aber auch herbeiführen. Dazu ist es lediglich notwendig, die Auslösemerkmale für automatische Handlungsmuster zu kennen und geschickt einzusetzen.

Reziprozität

Die Regel der Reziprozität (Wechselseitigkeit) besagt, daß wir uns für erhaltene Gefälligkeiten, Geschenke und dergleichen revanchieren. Da diese Regel enormes Potential für eine Gesellschaft birgt, setzt sie alles daran, ihre Mitglieder entsprechend zu sozialisieren. So werden Menschen, die nur nehmen anstatt zu geben, schnell ausgegrenzt. Die Erwartung der Gegenleistung gilt nur dann nicht, wenn der Beschenkte nicht in der Lage ist, sich entsprechend zu revanchieren – schließlich würde niemand ein Gegengeschenk erwarten, wenn er seiner zweijährigen Nichte einen Teddybären schenkt.

Die Durchschlagskraft dieser Regel ist beeindruckend, sie wurde in Experimenten etwa von Denis Regan untersucht: Zwei Versuchspersonen sollten einige Bilder bewerten. Einer der Teilnehmer, der in Wirklichkeit ein Assistent war, verschwand nach einer Weile und brachte zwei Cola mit zurück. Eine gab er dem anderen – echten – Teilnehmer, die zweite trank er selbst. Im Anschluß an die gestellte Bildbewertung erzählte der Assistent, daß er Losverkäufer sei und noch ein paar Lose verkaufen müsse. Es verwundert nicht, daß der Verkäufer in der Gruppe, der er eine Cola spendierte, mehr Umsatz generierte als in der Kontrollgruppe ohne Cola.

Weit interessanter als diese Erkenntnis ist aber, daß der Losverkäufer den Beschenkten nicht wesentlich sympathischer erschien. Für gewöhnlich entscheidet die Sympathie darüber, ob wir einem Unbekannten einen Gefallen tun oder nicht – bei den mit der Cola Beschenkten spielte dies keine Rolle mehr. Die Reziprozitätsregel ist so mächtig, daß unbeliebte Personen damit ihre Erfolgschancen wesentlich erhöhen können.

Nun kann man natürlich die Frage stellen, ob eine derartige Masche das „Opfer" nicht doch verärgern könnte und es eine gegebene Zusage nicht einhält. Miller et al. (1976) untersuchten dies in einem Experiment, indem sie Studenten um Blutspenden baten. Zuerst baten sie sie darum, drei Jahre lang alle sechs Wochen zu spenden – was prompt abgelehnt wurde. Danach wurde um eine einfache Blutspende gebeten. Es ist nun nicht überraschend, daß aus dieser Gruppe wesentlich mehr Studenten wirklich zur Spende erschienen, als aus der Gruppe, die nicht um eine regelmäßige Spende gebeten wurden.

Wer A sagt ...

Den Menschen wohnt ein geradezu zwanghaftes Verhalten inne, in Konsistenz mit ihren früheren Handlungen zu erscheinen, also konsequent zu sein. Wurde eine Entscheidung getroffen, treten intra- und interpsyschische Vorgänge in Kraft, die uns dazu drängen, konsistent zu bleiben. In einer Studie haben Knox und Inkster (1968) Menschen, die gern auf Pferde wetten, untersucht. Nachdem die Wetter einen Wetteinsatz auf ein bestimmtes Pferd gesetzt haben, steigt ihre Zuversicht, daß das Pferd gewinnt.

Dieses Verhalten läßt sich auch in den beliebten »Heiligen Kriegen« beobachten. Die wenigsten Benutzer eines Systems oder Texteditors wollen ihre einmal getroffene Entscheidung rückgän-


http://www.anchor.com.au/blog/2010/01/vi-gangstas/

gig machen bzw. ihr widersprechen. Daher verbeißen sich die Gegner ineinander und »diskutieren« sich tot.

Die Konsistenz ist so stark, daß Menschen gegen ihre eigenen Interessen verstoßen, nur um nach außen hin als konsistent zu gelten. Moriarty (1975) führte dazu ein Experiment durch: An einem Strand breitete neben einer zufällig ausgewählten Versuchsperson ein Assistent ein Strandtuch aus und baute ein Radio auf. Nach ein paar Minuten schlenderte der Assistent von dannen und ließ das Radio zurück. Ein weiterer Assistent gab den Taschendieb, griff sich das Radio und rannte damit weg. In zwanzig Durchläufen hat nur eine einzige der Versuchspersonen eingegriffen und versucht, den Dieb zu stellen. Modifizierte er das Experiment, stieg die Erfolgsrate dramatisch. Der erste Assistent bat einfach seine Nachbarn, auf das Radio achtzugeben. Nun verfolgten 19 von 20 Versuchspersonen den »Dieb« und stellten ihn teils unter Einsatz körperlicher Gewalt zur Rede.

Ein wunderbares Beispiel für den kommerziellen Einsatz der Konsistenz führt Cialdini im dritten Kapitel seines Buches auf: die Spielzeugbranche unter saisonalen Schwankungen. In der Vorweihnachtszeit explodiert der Umsatz, dafür bricht er nach Weihnachten um so dramatischer ein. Daher etablierten einige Unternehmen eine interessante Absatzstrategie. Zu Beginn der Vorweihnachtszeit wurde ein neues interessantes Spielzeug eingeführt und massiv und aggressiv beworben. Solch ein Beispiel ist Furby. Das Produkt wurde zwar aggressiv beworben, aber in viel zu geringer Stückzahl auf den Markt gebracht. Dies führte dazu, daß viele Eltern zwar einen Furby zu Weihnachten versprachen, aber keinen kaufen konnten. Also kauften sie ein anderes Geschenk. Nach den Weihnachtsfeiertagen setzte die Furby-Werbung erneut ein – was die Kinder wieder an ihren alten Weihnachtswunsch erinnerte. Also marschierten sie schnurtracks zu ihren Eltern und verlangten einen Furby. Da diese es ihrem Nachwuchs meist schon vor Weihnachten versprochen hatten, waren sie in der Konsistenzfalle gefangen.

Commitment

Was ist nun das Auslösemerkmal für eine solche Konsistenzreaktion? Die Sozialpsychologie geht davon aus, daß es eine Bindung an oder eine Festlegung auf etwas ein sogenanntes Commitment ist. Jede darauf aufbauende Überzeugungsstrategie arbeitet damit, uns zu einem Commitment zu bringen. Spenden-

sammler von Wohltätigkeitsprganisationen (oder Drückerkolonnen) beginnen ein Telefonat oft mit einer Frage nach dem Befinden. Antwortet der Angerufene, daß es ihm gut geht, gibt er schon ein Commitment ab. Im weiteren Verkaufsgespräch wird darauf zurückgegriffen und versucht, die Spendenbereitschaft zu erhöhen, indem von der mißlichen Lage der Spendenbegünstigten berichtet wird.

Viele Vertreter oder Verkäufer beginnen eine »Spirale der Willfährigkeit« in Gang zu setzen. Dazu drängen Sie den Kunden dazu, eine Reihe kleinerer Commitments abzugeben. Drückerkolonnen, die Zeitschriftenabos verticken, fangen beispielsweise immer mit der Frage »Sehen Sie sich gerne gute Filme an?«, um das Opfer einzuwickeln. Auch einige Tierschutzorganisationen (die meist mehr an Geld als an Tierschutz interessiert sind) beginnen häufig mit der Frage, ob man Tiere möge.[1]

Die Taktik, mit einer kleinen Bitte zu beginnen, um sich dann zur großen vorzuarbeiten, wird in der Sozialpsychologie und im Marketing »Fuß-in-der-Tür-Taktik« genannt. Hat man das Selbstbild einer Person erst einmal in eine neue Rolle manipuliert, tut die Person nahezu alles, um mit dem neuen Selbstbild konsistent zu bleiben.

Allerdings wirken nicht alle Commitments gleich: Es muß aktiv, öffentlich, mit Anstrengung verbunden und freiwillig sein. Ein aktives Commitment ist das Versprechen, etwas zu tun. In der umgekehrten Form – nicht versprechen, etwas nicht zu tun – zeigte es keinen großen Einfluß. Ein öffentliches Commitment zeigt mehr Wirkung, als ein nicht-öffentliches, schließlich wird dieses ja nicht bekannt und kann so das Bild einer Person ändern. Am effizientesten ist eine schriftliche Verpflichtung. Dies ist ein unumstreitbarer materieller Beweis für eine Festlegung. Deshalb empfehlen auch viele Diät- oder Anti-Rauch-Ratgeber, die gefaßten Vorsätze schriftlich niederzulegen.

Wichtiger noch ist, daß es kein »Belohnungs-Hintertürchen« geben darf. Jemand, der ein Commitment nur wegen einer hohen Belohnung abgegeben hat, wird nicht so stark daran gebunden, wie jemand der keine oder nur eine niedrige Belohnung bekommt. Es geht nicht darum, jemandem irgendein Commitment abzuringen, sondern er muß die volle Verantwortung dafür übernehmen.

Ein Versuch beweist diese These: Man verbot mehreren sieben- bis neunjährigen Jungen, mit einem besonders interessanten Spielzeug zu spielen. Und wer Jungs kennt – insbesondere in dieser Altersgruppe – weiß, daß Verbote etwas nur wesentlich interessanter machen. Eine Gruppe wurde mit einer Drohung dazu gebracht, die andere mit einer Begründung. In beiden Gruppen, jeweils 22 Jungen stark, spielte nur ein Einziger verbotenerweise mit dem Spielzeug.

Sechs Wochen nach dem Test wurden die selben Gruppen wieder in Kontakt mit dem Spielzeug gebracht. Diesmal wurde kein Verbot ausgesprochen, so daß 17 Jungen aus der »Drohungsgruppe« sofort zum verbotenen Spielzeug griffen. Da sie nun nicht mehr mit der Bestrafung rechnen mußten, wurde das sechs Wochen vorher ausgesprochene Verbot quasi wirkungslos. In der zweiten Gruppe, die mit einer Begründung vom Spielzeug abgehalten worden waren, griffen nur sieben Jungen zum verbotenen Spielzeug.

Die erste Gruppe hatte also sehr schnell erkannt, daß der Testleiter nicht mehr da war, um seine Drohung wahrzumachen. Nur wenn die Jungen befürchteten, ertappt und bestraft zu werden, hielten sie sich an das Verbot. Die zweite Gruppe hingegen wurde nicht mit einer Strafandrohung vom Spielzeug ferngehalten, sondern mit einer Begründung. Das erste Testergebnis entsprach dem der ersten Gruppe – nur jeweils ein Junge spielte mit dem verbotenen Spielzeug. Das Entscheidende spielte sich im Inneren der Jungen ab – in der zweiten Testgruppe gelangten sie zu dem Entschluß, nicht mit dem Spielzeug spielen zu **wollen**.

1 Meine Standardantwort »Ja, am liebsten als Chicken McNuggets!« läßt das Verkaufsgespräch sehr schnell beenden.

Ein im Marketing bzw. im Verkauf eingesetzter Trick des Commitments ist die sogenannte »throwing a low ball«-Taktik. Hierbei wird ein PKW unter dem üblichen Marktwert angeboten. Natürlich erhöht dieses Schnäppchen den Absatz, es werden mehr Kunden angelockt. Wenn diese dann den Vertrag unter Dach und Fach bringen wollen, bemerkt der Verkäufer oder die Finanzierungsbank, daß der Betrag aufgrund eines Fehlers zu niedrig ist und man den Preis auf das marktübliche Niveau erhöhen muß. Normalerweise würde man davon ausgehen, daß verärgerte Kunden diese Autohäuser scharenweise verlassen und nie wieder betreten. Das Gegenteil ist aber der Fall: Sehr viele Kunden kaufen den Wagen trotzdem – da sie eben schon einige Commitments gemacht haben, als sie den »Papierkram« ausfüllten.

Abwehrstrategien

Konsistentes Verhalten ist – wie auch alle anderen automatischen Reaktionen – von großem Nutzen für uns und die Gesellschaft. Es ermöglicht uns, Situationen schnell und meist effizient einzuschätzen und uns angemessen zu verhalten. Die Gesellschaft hingegen kann das Verhalten einzelner Personen besser beurteilen und voraussagen, wenn sich diese konsequent verhalten.

Daher fällt es schwer, auf konsistentes Verhalten zu verzichten und jede Entscheidung erneut abzuwägen. Es gibt allerdings Signale, auf die man achten sollte. Zum einen ist es das Bauchgefühl, zum anderen der »Grund des Herzens«. Meist merken Menschen im Magen oder im Herzen, ob sie betrogen oder ausgenutzt werden sollen. Es gibt einige Studien, die belegen, daß wir Gefühle Sekundenbruchteile vor unserer verstandesgemäßen Antwort wahrnehmen.

Wenn Sie also Zweifel an der Ehrlichkeit einer Person haben, stellen Sie sich folgende Frage: »Bei dem, was ich jetzt weiß, wie würde ich mich entscheiden?«. Achten Sie dabei auf ihre erste Gefühlsregung oder Intuition, wenn Sie das so nennen wollen. Spätestens wenn sich hier Zweifel einstellen, sollten Sie alle jetzt bekannten Fakten neu überdenken und auf Basis dieser Informationen die Entscheidung treffen.

Sympathie

Nicht wirklich überraschend ist, daß uns sympathische Menschen eher zu etwas verleiten können. Jeder vernünftige Verkäufer versucht, dem Kunden gegenüber besonders sympathisch zu erscheinen. Sympathie verstärkt alle anderen eingesetzten Überzeugungstricks.

Da die Sympathie eine sehr große Rolle spielt, wird sie oft als Waffe eingesetzt – aber auch sehr gut erforscht. Daher gibt es Anhaltspunk-

te dafür, was uns jemanden als sympathisch erscheinen läßt.

Besonders stark lassen wir uns von besonders attraktiven Menschen beeinflussen. Hier führt der sogenannte Halo-Effekt dazu, daß die herausstechende Eigenschaft Attraktivität alle anderen Eigenschaften überstrahlt. Testpersonen schrieben einer besonders attraktiven Person automatisch besonders positive Eigenschaften zu.

Ein weiterer, leichter anzupassender Faktor ist Ähnlichkeit. Sympathie und Hilfsbereitschaft steigen gegenüber Menschen, die uns ähnlich gekleidet sind, neben der äußeren Erscheinung können auch die Herkunft oder ähnliche Interessen Sympathie erzeugen.

So versuchen beispielsweise Autohändler, aus dem Auto des Kunden Rückschlüsse auf seine Hobbies zu ziehen und diese dann als eigene Hobbies auszugeben. Mehrere Untersuchungen zeigten, daß selbst belanglos erscheinende Ähnlichkeiten ihre Wirkung nicht verfehlten, so zeigte Evans () anhand von Verkaufsunterlagen von Versicherungen, daß Kunden eher geneigt waren, eine Versicherung abzuschließen, wenn zum Vertreter Ähnlichkeit hinsichtlich Alter, Religion, politischer Einstellung und Rauchen bestand.

Schmeicheleien, Sympathiebekundungen oder Flirts sind Möglichkeiten, jemanden für ein Anliegen zugänglich zu machen. Selbst wenn die Schmeicheleien offensichtlich der Manipulation dienen, zeigen sie noch Wirkung. Die Komplimente müssen gar nicht unbedingt zutreffend sein, um zu wirken. Positive Kommentare brachten dem Schmeichler stets gleich viel Sympathie ein, ob sie nun stimmten oder nicht.

Abwehrstrategien

Es gibt auch hier wieder kein Abwehrrezept, sondern nur verschiedene Punkte, die alarmieren sollten. Finde ich das Gegenüber attraktiver/sympathischer/ähnlicher als es sein sollte? Würde ich das Produkt auch kaufen, wenn es mir ein anderer Verkäufer präsentieren würde? Würde ich die Information herausgeben bzw. den Gefallen tun, wenn es sich um jemanden anderes handeln würde? Wurde die Sympathie zu schnell aufgebaut?

Autorität

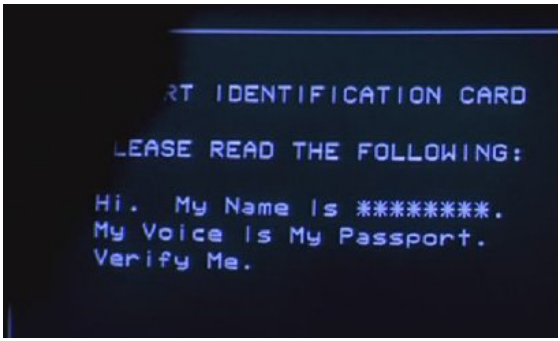
Besonders interessant ist, daß wir nicht unbedingt auf »echte« Autorität reagieren, sondern auch auf vermeintlich zur Schau gestellte. In den USA lief mehrere Jahre ein Werbespot für entkoffeinierten Kaffee. Der Werbeträger war Robert Young – in seiner Fernsehrolle als Dr. med. Markus Welby. Obwohl alle Zuschauer wußten, daß Young kein Arzt ist, verhalf er dem Produkt zum Durchbruch.

Verschiedene Untersuchungen identifizierten drei Autoritätssymbole: Titel, Uniformen und Luxus.

Schon 1966 wurde ein interessantes Experiment über Fehlmedikamentierungen in Krankenhäusern durchgeführt. Einer der Forscher rief in 22 Krankenhausabteilungen an, gab sich als dortiger Arzt aus und trug dem Pflegepersonal auf, einem bestimmten Patienten 20 mg Astrogen zu verabreichen.

Aus vier guten Gründen hätte die Schwester oder der Pfleger auf diese Anweisung mit Mißtrauen reagieren müssen:

(1) Die Anordnung wurde per Telefon gegeben, was eine Verletzung der Grundsätze des Krankenhauses bedeutete.
(2) Das Medikament durfte gar nicht verordnet werden. Astrogen war weder zum Gebrauch freigegeben noch befand es sich regulär auf der Bestandsliste der Station.
(3) Die verschrieben Dosis war eindeutig zu hoch. Auf der Packung stand unmißverständlich, daß die Tageshöchstdosis bei zehn Milligramm lag, die Hälfte der verschriebenen Menge.
(4) Die Anordnung kam von jemandem, den die Pflegekraft nie zuvor persönlich kennengelernt oder wenigstens telefonisch gesprochen hatte.



Dennoch ging der Pfleger bzw. die Krankenschwester in 95% der Fälle unverzüglich zum Medizinschrank der Station, entnahm die verschriebene Dosis Astrogen und machte sich auf den Weg zum Zimmer des Patienten, um sie ihm zu verabreichen. An diesem Punkt griff ein heimlicher Beobachter ein und klärte die Pflegekraft darüber auf, daß es sich um ein Experiment handelt.

Einer weiteren Studie nach reagieren Autofahrer respektvoller auf große Luxuswagen. Ein alter Kleinwagen und ein neuer Oberklassewagen warteten an einer Ampel und fuhren nicht sofort bei Grün los. Der Kleinwagen wurde fast immer angehupt und zweimal sogar angerempelt, der Oberklassewagen aber nur in ca. 50% der Fälle. Später befragten die Versuchsleiter Studenten, wie sie sich in der Situation verhalten hätten: Fast alle gaben an, den Oberklassewagen anhupen zu wollen, und zwar nach recht kurzer Wartezeit.

Ein weiteres Autoritätssymbol ist die Kleidung. Verschiedene Studien zum Gehorsam zeigten, daß lediglich 42% der Bitte eines Mannes in Straßenkleidung nachkamen, aber 92%, wenn der Mann eine Wachdienstuniform trug.

Abwehrstrategien

Ein wichtiger Punkt ist die Ausschaltung des Überraschungsmoments. In der Regel wird Autorität nicht bewußt wahrgenommen, aber trotzdem beachtet. Daher ist es sinnvoll und hilfreich, generell mehr Aufmerksamkeit auf die eigenen Entscheidungen zu legen.

Ebenfalls wichtig ist es, festzustellen ob die Autorität echt oder vorgetäuscht ist. Bei Polizisten o. ä. Autoritätspersonen sollte man den Dienstausweis überprüfen. Ebenso sollte man in Organisationen die Einführung von Dienstausweisen überprüfen.

Außerdem ist es wichtig, auch den Autoritätspersonen klarzumachen, daß sie ihre Autorität nicht mißbrauchen dürfen. Gilt im Rahmen der Sicherheitsrichtlinie eine Ausweispflicht, dürfen Abteilungsleiter, Manager usw. diese nicht ignorieren. Setzen sie sich darüber hinweg, unterminieren sie die gesamte Sicherheitskultur. Halten sie sich daran, helfen sie alleine durch ihre Autorität.

Bei Titeln, wie einem Doktor oder Professor, sollte man nachforschen, woher der Titel stammt und ob die Institutionen vertrauenswürdig sind. Außerdem sollte man darauf achten, wessen Interessen die Autorität vertritt. Handelt sie in meinem Sinne oder gegen mich?

Fazit

Es gibt keinen »Abwehrzauber« gegen Social Engineering, denn dabei handelt es sich um Verhalten, das in der Regel sozial erwünscht ist. Technische Maßnahmen sind nicht in der Lage, derartige Vorfälle zu verhindern, da es sich um ein soziales Problem handelt.

Es reicht daher nicht, einfach Daten zu verschlüsseln, zu sichern, zu löschen, oder die Systemcalls zu überwachen. Zur Abwehr wird die Fähigkeit benötigt, soziale Beziehungen und Kontexte zu deuten. Daß dies von Computern nicht geleistet werden kann, zeigen schon einfache automatische Übersetzungsversuche. Vielmehr ist es notwendig, in Organisationen ein Sicherheitsbewußtsein zu schaffen.

Dabei ist darauf zu achten, daß es zu Einstellungs- und Verhaltensänderungen kommt, sowie Lerntransfere sichergestellt werden. Daher ist es notwendig, eine Didaktik der

Sicherheit bzw. des sicherheitsbewußten Verhaltens zu entwickeln. Die vorgestellten Grundlagen des Social Engineerings lassen sich weder verhindern noch ausschalten, denn sie stellen auch die Grundlagen unseres sozialen Zusammenlebens als »Zoon Politikon« dar.

Erfolgreiches Social Engineering setzt oft bei der mangelnden Authentifizierung des Angreifers an. Daher ist es notwendig, sinnvolle Authentifizierungsmechanismen (z. B. Dienstausweise, Anruf-Parolen o. ä.) zu etablieren. Dabei gilt es aber, derartige technische Lösungen sozial akzeptabel zu machen.

Eine sinnvolle Maßnahme kann es sein, Schulungen zum Thema Social Engineering im Rahmen einer Security-Awareness-Kampagne durchzuführen. Dabei ist es aber notwendig, Sicherheit als Teil der Firmenkultur zu begreifen und nicht als mechanistisches Element, das beliebig manipuliert werden kann.

Literatur

Hans Helmut Kirst: 08/15 in der Kaserne, 08/15 im Krieg, 08/15 bis zum Ende. Verlag Kurt Desch, 1954.

Miller, R. et al.: Perceptual contrast versus reciprocal concession as mediators of induced compliance. In: Canadian Journal of Behavioural Science 8, S. 401-409, 1976.

Knox, R. E., Inkster, J. A.: „Postdecision dissonance a post time". In: Journal of Personality and Social Psychology 8.4, Part 1, 1968, S. 319–323, *http://www.sciencedirect.com/science/article/B6X01-4NPKJ71-1/2/63bf229ea9ee2a8c8e0cd86005ffe926* vom 27. Juli 2009.

Cialdini, R. B.: Die Psychologie des Überzeugens. Verlag Hans Huber, 2007.

Evans, F. B. (1963). „Selling as a Dyadic Relationship: A New Approach." In: American Behavioral Scientist 6, Seiten 76 – 79.

VS NfD
BfV, Am Reichstag 3, 10512 Hauptstadt

Bundesamt für Verfassungsschutz, falsche Verdächtigungen und Gedankenkontrolle

Sehr geehrte(r) Frau/Herr/Gefährder _____

Ihnen wird vorgeworfen, Mitglied der terroristischen Vereinigung

- ❑ Autonome Rhein-Main-Koordination (ARMK)
- ❑ Militante Gruppe (mg)
- ❑ Christliche Djihad-Union (CDU)

zu sein. Aus den Gesprächsprotokollen unseres V-Mannes

- ❑ Codename 123, bürgerlicher Name [redacted]
- ❑ Codename 007, bürgerlicher Name [redacted]
- ❑ Codename 023, bürgerlicher Name IM Erika

geht hervor, dass nach Ihren Angaben ausweislich der Email von Ihnen an die Verdachtsperson [redacted] Ihr Traumberuf angeblich

- ❑ Berufsrevolutionär
- ❑ Raubmordkopierbildertauscher
- ❑ Innenminister eines STASI-Lands (Sachsen, Brandenburg, Thüringen)

sei. Gemäß §129a erfüllen Sie damit den Straftatbestand der

- ❑ Mittäterschaft in einer kriminellen Vereinigung
- ❑ Gedankenverbrechen am deutschen Politikervolk
- ❑ freien Meinungsäußerung.

Wir machen Sie darauf aufmerksam, dass Sie [redacted] auch [redacted] sowie viel[redacted] mehr, aber in jedem Falle [redacted].
Wir fordern Sie hiermit auf, dem Strafbefehl Folge zu leisten und dem Verfassungsschutz zwecks

- ❑ verfassungswidriger Überwachung Ihres Email-Zugangs
- ❑ unbegründeter Abhörmaßnahmen Ihres Mobiltelefons
- ❑ rechtswidrigem Lauschangriff auf Ihre Wohnräume

Ihre

❑ Paßwörter ❑ Mobilrufnummer ❑ Haustürschlüssel

auszuhändigen.

Wir weisen Sie darauf hin, dass im Fall einer Nichtbefolgung dieser Anweisung

- ❑ die Trachtengruppe des nächstgelegenen Polizeireviers
- ❑ die Geheime Schutzgruppe 9 (GSG9)
- ❑ die Bundeswehr im Inneren

angewiesen wurde, alle Beweismittel an Ihrem Wohnsitz inklusive aller Nebengelasse im Internet zu

- ❑ deponieren
- ❑ fälschen
- ❑ beschlagnahmen.

Dieses Schreiben wurde rechtswidrig angefertigt
und trägt daher keine Unterschrift.