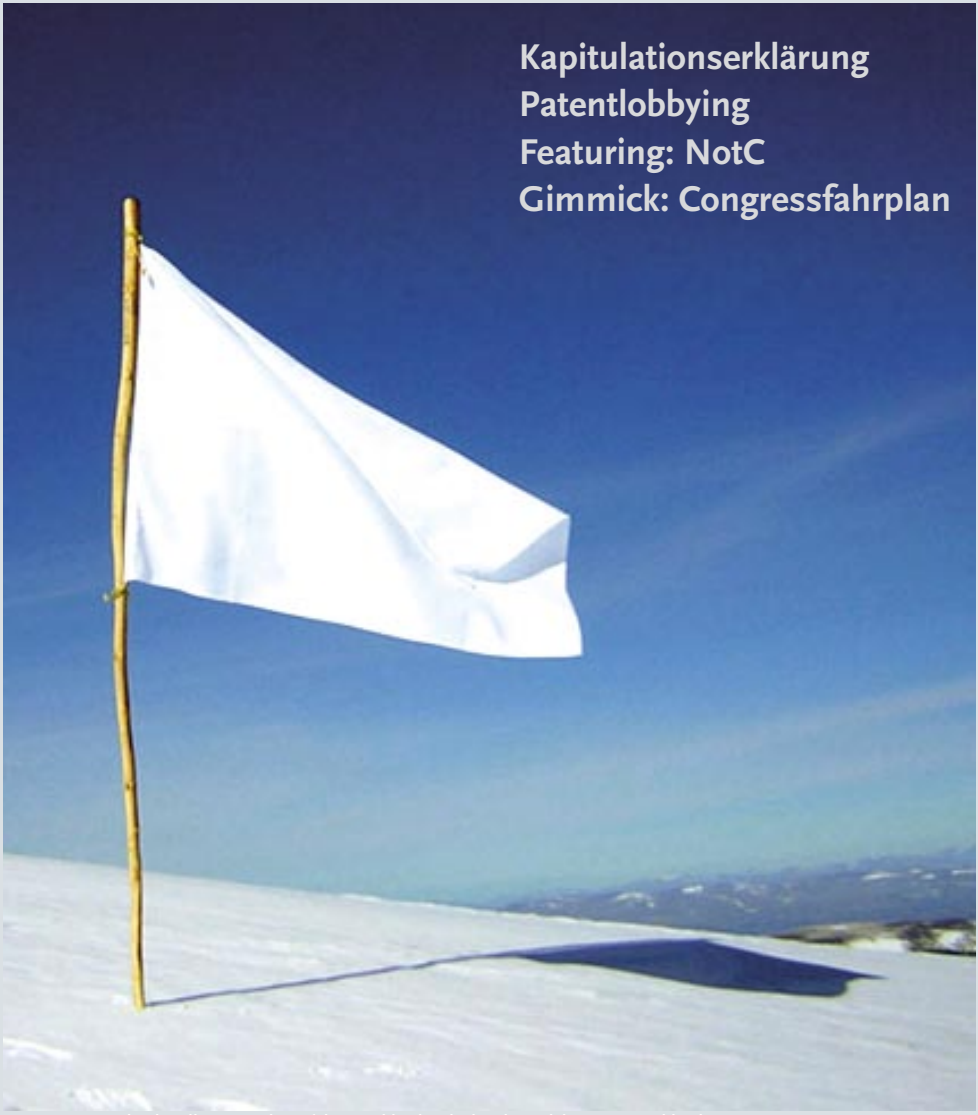
die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

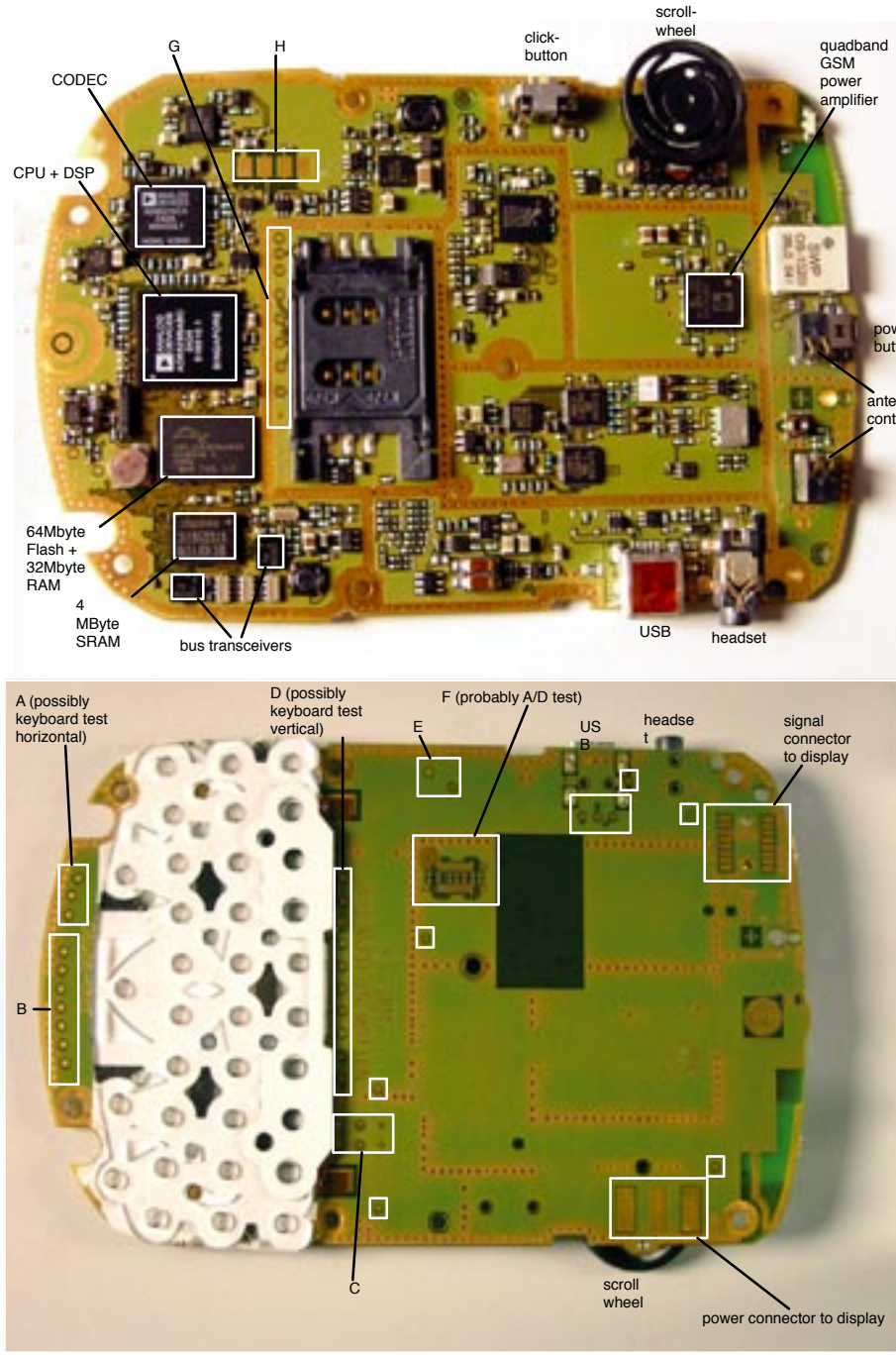


Kapitulationserklärung
Patentlobbying
Featuring: NotC
Gimmick: Congressfahrplan

Ein weiteres eindrucksvolles Beispiel sorgfältiger Bildrecherche bei der Redaktion Datenschleuder.

ISSN 0930-1054 • 2005
Sonderpreis von nur €2,50, Congressguide gibt es gratis dazu
Postvertriebsstück C11301F

#89



RIM Blackberry 7290 (nackt, Sachdienliche Hinweise zur Belegung der Testpunkte erbeten.)

Ein CCC-Kongress unter laufenden Überwachungskameras. Denkbar? "Na klar, ich hab mich doch ohnehin schon an die vielen Kameras gewöhnt – dagegen kann man sich sowieso nicht wehren!"

Seit es den Chaos Communication Congress gibt, war das Verhältnis zu jeglicher Form von Bildberichterstattung sehr angespannt. Und durchaus berechtigt. Der kreative Umgang mit Technik und die freie Reise in Datennetzen stieß nicht in der gesamten Bevölkerung auf Begeisterung.

Dazu war ein Lernprozess notwendig, der in den letzen Jahren zur deutlichen Entspannung beigetragen hat und nebenbei uns Hacker überwiegend als "die Guten" dastehen lässt.

Mittlerweile haben sich die meisten Congressteilnehmer damit abgefunden, daß mal ein Kamerateam oder ein Fotoreporter die positive Stimmung der Veranstaltung aufnimmt und an die Öffentlichkeit trägt. Und das ist gut so, wenn dabei die Persönlichkeitsrechte der Teilnehmer beachtet werden und auf Wunsch von einer Aufnahme abgesehen wird. Und letztendlich hat sowieso fast jeder Teilnehmer eine Digitalkamera oder Foto-Handy dabei und knippst damit herum wie verrückt.

Im Gegensatz dazu macht uns (der Gesellschaft) seit einigen Jahren ein neues Phänomen zu schaffen und kratzt an unseren Persönlichkeitsrechten: Die Videoüberwachung. Man kann damit Diebstähle vermeiden, Anschläge verhindern, Kriminalität eindämmen – und Versicherungsprämien senken.

Nun hat auch die Gebäudeversicherung für das frisch renovierte Berliner Congress Centrum (bcc), wo seit drei Jahren der Chaos Communication Congress stattfindet, eine Klausel in den Versicherungsbedingungen, die den Einsatz einer Videoüberwachung des Gebäudes mit Aufzeichnung vorschreibt. Die Veranstaltung würde also unter 24 Stunden täglicher Kameraüberwachung mit einer Speicherung der Aufnahmen für eine Woche leben müssen.

Ist das akzeptabel? Ein Verein, der sich den Schutz der Persönlichkeitsrechte und den Kampf gegen Überwachungstendenzen auf die Fahnen geschrieben hat, soll nun plötzlich alle Prinzipien aufgeben und sich von Kameras an der Decke rund um die Uhr filmen lassen? Was passiert mit den Daten? "Abschalten oder die Veranstaltung absagen", "einfach kaputt schlagen", "Schutzwände und Schirme vor die Kameras stellen" sind einige Forderungen, die im Clubumfeld geäußert werden.

Ein Kompromiß könnte sein: Der CCC verhandelt mit dem Veranstaltungsort, ob sich durch eine erhöhte Versicherungsprämie die Videoüberwachung vermeiden läßt. Die zusätzlichen Kosten werden auf den Eintrittspreis umgelegt. Das wäre prima! Damit bekommt die Privatsphäre einen Wert, einen Preis. Greifbar, verhandelbar – wir kaufen uns frei von der Überwachung. Das ist vergleichbar mit der Sicherheitsgebühr an Flughäfen. Der Passagier muß einen zusätzlichen Obolus leisten, damit für seine Sicherheit gesorgt wird. Diesen Preis muß er zusätzlich zum Ticket bezahlen. Wieviel wird uns die nicht-Überwachung wert sein für vier Tage? Fünf Euro? 20 Cent pro Tag? Nichts? *<frankro>*

Inhalt

We lost the war. Welcome to the world of tomorrow.

by Frank <frank@ccc.de>

Losing a war is never a pretty situation. So it is no wonder that most people do not like to acknowledge that we have lost. We had a reasonable chance to tame the wild beast of universal surveillance technology, approximately until september 10th, 2001. One day later, we had lost. All the hopes we had, to keep the big corporations and "security forces" at bay and develop interesting alternative concepts in the virtual world, evaporated with the smoke clouds of the World Trade Center.

Just right before, everything looked not too bad. We had survived Y2K with barely a scratch. The worlds outlook was mildly optimistic after all. The "New Economy" bubble gave most of us fun things to do and the fleeting hope of plenty of cash not so far down the road. We had won the Clipper-Chip battle, and crypto-regulation as we knew it was a thing of the past. The waves of technology development seemed to work in favor of freedom, most of the time. The future looked like an yellow brick road to a nirvana of endless bandwith, the rule of ideas over matter and dissolving nation states. The big corporations were at our mercy, because we knew what the future would look like and we had the technology to built it. Those were the days. Remember them for your grandchildren's bedtime stories. They will never come back again.

We are now deep inside the other kind of future, the future that we speculated about as a worst case scenario, back then. **This is the ugly future**, the one we never wanted, the one that we fought to prevent. We failed. Probably it was not even our fault. But we are forced to live in it now.

Democracy is already over

By its very nature the western democracies have become a playground for lobbyists, industry interests and conspiracies that have absolutely no interest in real democracy. The "democracy show" must go on nonetheless. Conveniently, the show consumes the energy of those that might otherwise become dangerous to the status quo. The show provides the necessary excuse when things go wrong and keeps up the illusion of participation. Also, the system provides organized and regulated battleground rules to find out which interest groups and conspiracies have the upper hand for a while. Most of the time it prevents open and violent power struggles that could destabilize everything. So it is in the best interest of most players to keep at least certain elements of the current "democracy show" alive. Even for the more evil conspiracies around, the system is useful as it is. Certainly, the features that could provide unpleasant surprises like direct popular votes on key issues are the least likely to survive in the long run.

Of course, those in power want to minimize the influence of random chaotic outbursts of popular will as much as possible. The real decisions in government are not made by ministers or the parliament. The real power of government rests with the undersecretaries and other high-level, non-elected civil servants who stay while the politicians come and go. Especially in the bureaucracies of the intelligence agencies, the ministry of interior, the military, and other key nodes of power the long-term planning and decision-making is not left to the incompetent mediocre political actors that get elected more or less

at random. Long term stability is a highly valued thing in power relations. So even if the politicians of states suddenly start to be hostile to each other, their intelligence agencies will often continue to cooperate and trade telecommunication interception results as if nothing has happened.

Let's try for a minute to look at the world from the perspective of such an 60-year-old bureaucrat that has access to the key data, the privilege to be paid to think ahead, and the task to prepare the policy for the next decades. What he would see, could look like this:

First, paid manual labor will be eaten away further by technology, even more rapidly then today. Robotics will evolve far enough to kill a sizeable chunk of the remaining low-end manual jobs. Of course, there will be new jobs, servicing the robots, biotech, designing stuff, working on the nanotech developments etc. But these will be few, compared with today, and require higher education. Globalization continues its merciless course and will also export a lot of jobs of the brain-labor type to India and China, as soon as education levels there permit it.

So the western societies will end up with a large percentage of population, at least a third, but possibly half of those in working age, having no real paid work. There are those whose talents are cheaper to be had elsewhere, those who are more inclined to manual labor. Not only the undereducated but all those who simply cannot find a decent job anymore. This part of the population needs to be pacified, either by Disney or by Dictatorship, most probably by both. The unemployment problem severely affects the ability of states to pay for social benefits. At some point it becomes cheaper to put money into repressive police forces and rule by fear than put the money into pay-outs to the unemployed population and buy the social peace. Criminal activities look more interesting when there is no decent job to be had. Violence is the unavoidable consequence of degrading social standards. Universal surveillance might dampen the consequences for those who remain with some wealth to defend.

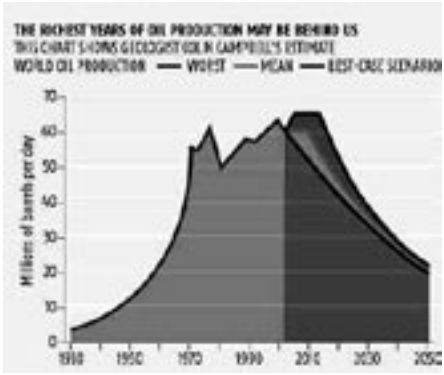
Second, climate change increases the frequency and devastation of natural disasters, creating large scale emergency situations. Depending on geography, large parts of land may become uninhabitable due to draught, flood, fires or plagues. This creates a multitude of unpleasant effects. A large number of people need to move, crop and animal production shrinks, industrial centers and cities may be damaged to the point where abandoning them is the only sensible choice left. The loss of property like non-usable (or non-insurable) real estate will be frightening. The resulting internal migratory pressures towards "safe areas" become a significant problem. Properly trained personal, equipment, and supplies to respond to environmental emergencies are needed standby all the time, eating up scarce government resources. The conscript parts of national armed forces may be formed into disaster relief units as they hang around anyway with no real job to do except securing fossil energy sources abroad and helping out the border police.

Third, immigration pressure from neighboring regions will raise in all western countries. It looks like the climate disaster will strike worst

at first in areas like Africa and Latin America and the economy there is unlikely to cope any better than the western countries with globalization and other problems ahead. So the number of people who want to leave from there to somewhere inhabitable at all costs will rise substantially.

The western countries need a certain amount of immigration to fill up their demographic holes but the number of people who want to come will be far higher. Managing a controlled immigration process according to the demographic needs is a nasty task where things can only go wrong most of the time. The nearly unavoidable reaction will be a Fortress Europe: serious border controls and fortifications, frequent and omnipresent internal identity checks, fast and merciless deportation of illegal immigrants, biometrics on every possible corner. Technology for border control can be made quite efficient once ethical hurdles have fallen.

Fourth, at some point in the next decades the energy crisis will strike with full force. Oil will cost a fortune as production capacities can no longer be extended economically to meet the rising demand. Natural gas and coal will last a bit longer, a nuclear renaissance may dampen the worst of the pains. But the core fact remains: a massive change in energy infrastructure is unavoidable. Whether the transition will be harsh, painful and society-wrecking, or just annoying and expensive depends on how soon before peak oil the investments into new energy systems start on a massive scale as oil becomes to expensive to burn. Procrastination is a sure recipe for disaster. The geo-strategic and military race for the remaining large reserves of oil has already begun and will cost vast resources.



Fifth, we are on the verge of technology developments that may require draconic restrictions and controls to prevent the total disruption of society. Genetic engineering and other biotechnology as well as nanotechnology (and potentially free energy technologies if they exist) will put immense powers into the hands of skilled and knowledgeable individuals. Given the general raise in paranoia, most people (and for sure those in power) will not continue to trust that common sense will prevent the worst. There will be a tendency of controls that keep this kind of technology in the hands of "trustworthy" corporations or state entities. These controls, of course, need to be enforced, surveillance of the usual suspects must be put in place to get advanced knowledge of potential dangers. Science may no longer be a harmless, self-regulating thing but something that needs to be tightly controlled and regulated, at least in the critical areas. The measures needed to contain a potential global pandemic from the Strange Virus of the Year are just a subset of those needed to contain a nano-tech or biotech disaster.

Now what follows from this view of the world? What changes to society are required to cope with these trends from the viewpoint of our 60-year-old power brokering bureaucrat?

Strategically it all points to massive investments into internal security. Presenting the problem to the population as a mutually exclusive choice between an uncertain dangerous freedom and an assured survival under the securing umbrella of the trustworthy state becomes more easy the further the various crises develop. The more wealthy parts of the population will certainly require protection from illegal immigrants, criminals, terrorists and implicitly also from the anger of less affluent citizens. And since the current system values rich people more then poor ones, the rich must get their protection. The security industry will certainly be of happy helpful assistance, especially where the state can no longer provide enough protection for the taste of the lucky ones.

Traditional democratic values have been eroded to the point where most people don't care anymore. So the loss of rights our ancestors fought for not so long ago is at first happily accepted by a majority that can easily be scared into submission. **"Terrorism" is the theme of the day, others will follow.** And these "themes" can and will be used to mold the western societies into something that has never been seen before: **a democratically legitimated police state**, ruled by an unaccountable elite with total surveillance, made efficient and largely unobtrusive by modern technology. With the enemy (immigrants, terrorists, climate catastrophe refugees, criminals, the poor, mad scientists, strange diseases) at the gates, the price that needs to be paid for "security" will look acceptable.

Cooking up the "terrorist threat" by apparently stupid foreign policy and senseless intelligence operations provides a convenient method to get through with the establishment of a democratically legitimized police state. No one cares that car accidents alone kill many more people than terrorists do. The fear of terrorism accelerates the changes in society and provides the means to get the suppression tools required for the coming waves of trouble.

What we call today "anti-terrorism measures" is the long-term planned and conscious preparation of those in power for the kind of world described above.

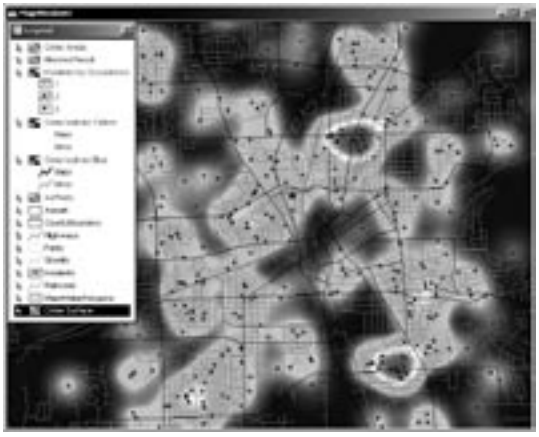
The Technologies of Oppression

We can imagine most of the surveillance and oppression technology rather well. Blanket CCTV coverage is reality in some cities already. Communication pattern analysis (who talks to whom at what times) is frighteningly effective. Movement pattern recording from cellphones, traffic monitoring systems, and GPS tracking is the next wave that is just beginning. Shopping records (online, credit and rebate cards) are another source of juicy data. The integration of all these data sources into automated behavior pattern analysis currently happens mostly on the dark side.

The key question for establishing an effective surveillance based police state is to keep it low-profile enough that "the ordinary citizen" feels rather protected than threatened, at least until all the pieces are in place to make it permanent. **First principle of 21st century police state: All those who "have nothing to hide" should not be bothered unnecessarily.** This goal becomes even more complicated as with the increased availability of information on even minor everyday infringements the "moral" pressure to prosecute will rise. Intelligence agencies have always understood that effective work with interception results requires a thorough selection between cases where it is necessary to do something and those (the majority) where it is best to just be silent and enjoy.

Police forces in general (with a few exceptions) on the other hand have the duty to act upon every crime or minor infringement they get knowledge of. Of course, they have a certain amount of discretion already. With access to all the information outlined above, we will end up with a **system of selective enforcement**.

It is impossible to live in a complex society without violating a rule here and there from time to time, often even without noticing it. If all these violations are documented and available for prosecution, the whole fabric of society changes dramatically. The old sign for totalitarian societies – arbitrary prosecution of political enemies – becomes a reality within the framework of democratic rule-of-law states. As long as the people affected can be made looking like the enemy-"theme" of the day, the system can be used to silence opposition effectively. And at some point the switch to open **automated prosecution and policing** can be made as any resistance to the system is by definition "terrorism". Development of society comes to a standstill, the rules of the law and order paradise can no longer be violated.



Now disentangling ourselves from the reality tunnel of said 60-year-old bureaucrat, where is hope for freedom, creativity and fun? To be honest, we need to assume that it will take a couple of decades before the pendulum will swing back into the freedom direction, barring a total breakdown of civilization as we know it. Only when the oppression becomes to burdensome and open, there might be a chance to get back to overall progress of mankind earlier. If the powers that be are able to manage the system smoothly and skillfully, we cannot make any prediction as to when the new dark ages will be over.

So what now?

Move to the mountains, become a gardener or carpenter, search for happiness in communities of like minded people, in isolation from the rest of the world?

The idea has lost its charm for most who ever honestly tried. It may work if you can find eternal happiness in milking cows at five o'clock in the morning. But for the rest of us, the only realistic option is to try to live in, with, and from the world as bad it has become. We need to built our own communities nonetheless, virtual or real ones.

The politics & lobby game

So where to put your energy then? Trying to play the political game, fighting against software patents, surveillance laws, and privacy invasions in parliament and the courts can be the job of a lifetime. It has the advantage that you will win a battle from time to time and can probably slow things down. You may even be able to prevent a gross atrocity here and there. But in the end, the development of technology and the panic level of the general population will chew a lot of your victories for breakfast.

This is not to discount the work and dedication of those of us who fight on this front. But you need to have a lawyers mindset and a very strong frustration tolerance to gain satisfaction from it, and that is not given to everyone. We need the lawyers nonetheless.

Talent and Ethics

Some of us sold their soul, maybe to pay the rent when the bubble bursted and the cool and morally easy jobs became scarce. They sold their head to corporations or the government to built the kind of things we knew perfectly well how to built, that we sometimes discussed as a intellectual game, never intending to make them a reality. Like surveillance infrastructure. Like software to analyze camera images in realtime for movement patterns, faces, license plates. Like data mining to combine vast amounts of information into graphs of relations and behavior. Like interception systems to record and analyze every single phone call, e-mail, click in the web. Means to track every single move of people and things.

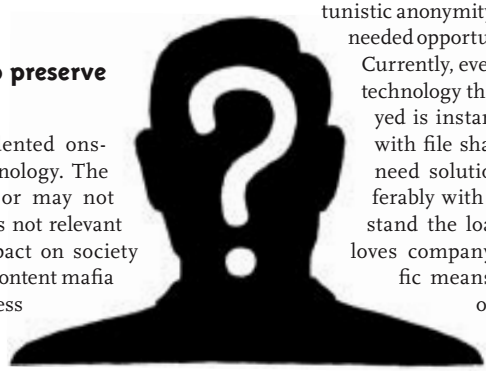
Thinking about what can be done with the results of one's work is one thing. Refusing to do the job because it could be to the worse of mankind is something completely different. Especially when there is no other good option to earn a living in a mentally stimulating way around. Most projects by itself were justifiable, of course. It was "not that bad" or "no real risk". Often the excuse was "it is not technical feasible today anyway, it's too much data to store or make sense from". Ten years later it is feasible. For sure.

While it certainly would be better when the surveillance industry would die from lack of talent, the more realistic approach is to keep talking to those of us who sold their head. We need to generate a culture that might be compared with the sale of indulgences in the last dark ages: you may be working on the wrong side of the barricade but we would be willing to trade you private moral absolution in exchange for knowledge. Tell us what is happening there, what the capabilities are, what the plans are, which gross scandals have been hidden.

To be honest, there is very little what we know about the capabilities of todays dark-side interception systems after the meanwhile slightly antiquated Echelon system had been discovered. All the new stuff that monitors the internet, the current and future use of database profiling, automated CCTV analysis, behavior pattern discovery and so on is only known in very few cases and vague outlines.

We also need to know how the intelligence agencies work today. It is of highest priority to learn how the "we rather use backdoors than waste time cracking your keys"-methods work in practice on a large scale and what backdoors have been intentionally built into or left inside our systems. Building clean systems will be rather difficult, given the multitude of options to produce a backdoor - ranging from operating system and application software to hardware and CPUs that are to complex to fully audit. Open Source does only help in theory, who has the time to really audit all the source anyway...

Of course, the risk of publishing this kind of knowledge is high, especially for those on the dark side. So we need to build structures that can lessen the risk. We need anonymous submission systems for documents, methods to clean out eventual document fingerprinting (both on paper and electronic). And, of course, we need to develop means to identify the inevitable disinformation that will also be fed through these channels to confuse us.



Building technology to preserve the options for change

We are facing a unprecedented onslaught of surveillance technology. The debate whether this may or may not reduce crime or terrorism is not relevant anymore. The de-facto impact on society can already be felt with the content mafia (aka. RIAA) demanding access to all data to preserve their dead business model. We will need to build technology to preserve the freedom of speech, the freedom of thought, the freedom of communication, there is no other long-term solution. Political barriers to total surveillance have a very limited half-life period.

The universal acceptance of electronic communication systems has been a tremendous help for political movements. It has become a bit more difficult and costly to maintain secrets for those in power. Unfortunately, the same problem applies to everybody else. So one thing that we can do to help societies progress along is to **provide tools, knowledge and training for secure communications** to every political and social movement that shares at least some of our ideals. We should not be too narrow here in choosing our friends, everyone who opposes centralistic power structures and is not geared towards totalitarism should be welcome. Maintaining the political breathing spaces becomes more important than what this space is used for.

Anonymity will become the most precious thing. Encrypting communications is nice and necessary but helps little as long as the communication partners are known. Traffic analysis is the most valuable intelligence tool around. Only by automatically looking at communications and movement patterns, the interesting individuals can be filtered out, those who justify the cost of detailed surveillance. Widespread implementation of anonymity technologies becomes seriously urgent, given the data retention laws that have been passed in the EU. We need opportunistic anonymity the same way we needed opportunistic encryption. Currently, every anonymization technology that has been deployed is instantly overwhelmed with file sharing content. We need solutions for that, preferably with systems that can stand the load, as anonymity loves company and more traffic means less probability of de-anonymization by all kinds of attack.

Closed user groups have already gained momentum in communities that have a heightened awareness and demand for privacy. The darker parts of the hacker community and a lot of the warez trading circles have gone "black" already. Others will follow. The technology to build real-world working closed user groups is not yet there. We have only improvised setups that work under very specific circumstances. Generic, easy to use technology to create fully encrypted closed user groups for all kinds of content with comfortable degrees of anonymity is desperately needed.

Decentralized infrastructure is the needed. The peer-to-peer networks are a good example to see what works and what not. As long as there are centralized elements they can be taken

down under one pretext or another. Only true peer-to-peer systems that need as little centralized elements as possible can survive. Interestingly, tactical military networks have the same requirements. We need to borrow from them, the same way they borrow from commercial and open source technology.

Design stuff with surveillance abuse in mind is the next logical step. A lot of us are involved into designing and implementing systems that can be abused for surveillance purposes. Be it webshop systems, databases, RFID systems, communication systems, or ordinary Blog servers, we need to design things as safe as possible against later abuse of collected data or interception. Often there is considerable freedom to design within the limits of our day jobs. We need to use this freedom to build systems in a way that they collect as little data as possible, use encryption and provide anonymity as much as possible. We need to create a culture around that. A system design needs to be viewed by our peers only as "good" if it adheres to these criteria. Of course, it may be hard to sacrifice the personal power that comes with access to juicy data. But keep in mind, you will not have this job forever and whoever takes over the system is most likely not as privacy-minded as you are. Limiting the amount of data gathered on people doing everyday transactions and communication is an absolute must if you are a serious hacker. There are many good things that can be done with RFID. For instance making recycling of goods easier and more effective by storing the material composition and hints about the manufacturing process in tags attached to electronic gadgets. But to be able to harness the good potential of technologies like this, the system needs to limit or prevent the downside as much as possible, by design, not as an afterthought.

Do not compromise your friends with stupidity or ignorance will be even more essential. We are all used to the minor fuckups of encrypted mail being forwarded unencrypted, being careless about other peoples data traces or bragging with knowledge obtained in confidence. This is no longer possible. We are facing an enemy that is euphemistically called "Global Observer" in research papers. This is meant literally. You can no longer rely on information or communication being "overlooked" or "hidden in the noise". **Everything is on file. Forever.** And it can and will be used against you. And your "innocent" slip-up five years back might compromise someone you like.

Keep silent and enjoy or publish immediately may become the new mantra for security researchers. Submitting security problems to the manufacturers provides the intelligence agencies with a long period in which they can and will use the problem to attack systems and implant backdoors. It is well known that backdoors are the way around encryption and that all big manufacturers have an agreement with the respective intelligence agencies of their countries to hand over valuable "0 day" exploit data as soon as they get them. During the months or even years it takes them to issue a fix, the agencies can use the 0 day and do not risk exposure. If an intrusion gets detected by accident, no one will suspect foul play, as the problem will be fixed later by the manufacturer. So if you discover problems, publish at least enough information to enable people to detect an intrusion before submitting to the manufacturer.

Most important: have fun! The eavesdropping people must be laughed at as their job is silly, boring, and ethically the worst thing to earn money with, sort of blackmail and robbing grandmas on the street. We need to develop a "lets have fun confusing their systems"-culture that plays with the inherent imperfections, loopholes, systematic problems, and interpretation errors that are inevitable with large scale surveillance. Artists are the right company for this kind of approach. We need a subculture of "In your face, peeping tom". Exposing surveillance in the most humiliating and degrading manner, giving people something to laugh about must be the goal. Also, this prevents us from becoming frustrated and tired. If there is no fun in beating the system, we will get tired of it and they will win. So let's be flexible, creative and funny, not angry, ideologic and stiff-necked.

Update fürs Herkunftswörterbuch

von Corinna Habets <ds@geekin.de> und Gerd Eist <erdgeist@erdgeist.org>

Die Herkunft bestimmer Computer-Wörter ist in Hacker-Kreisen bekannt. Daß z.B. das Wort "Hacker" in den Sechzigern im Tech Model Railroad Club des MIT als Bezeichnung für eine originelle, wenn auch wenig elegante Lösung erfunden wurde. Auch die vermeintliche Herkunft von "Bug" kennen viele. Die Legende besagt, daß die Grand Dame der Computergeschichte, Grace Hopper herself, eigenhändig eine Motte aus einem Relais des Mark II klaubte, dieses als Bug im Logbuch verzeichnete und so den Begriff prägte. Der Wikipedia zufolge [1] wurde "Bug" jedoch schon im 19. Jahrhundert zur Bezeichnung kleiner technischer Fehler verwendet.

Zur weiteren Mehrung der etymologischen Kenntnisse wenden wir uns nun ein paar Begriffen zu, deren Herkunft weniger bekannt ist. Als erstes dem Begriff

Skriptsprache

Skriptsprachen sind Programmiersprachen, die eine Teilmenge der folgenden Eigenschaften haben:

- hohe Abstraktion: wenig Code, viel Wirkung
- interpretiert, nicht kompiliert: die Programme werden als Plain-Text vom jeweiligen Interpreter eingelesen und ausgeführt
- schwache oder keine Typisierung von Variablen
- spezialisiert: Skriptsprachen sind oft auf eine bestimmte Umgebung oder einen bestimmten Zweck zugeschnitten

Prominente Vertreter sind Python, Perl, JavaScript, Ruby, PHP, Lua, ShellScript, u.v.m.

Die Grenzen zwischen Skript- und anderen Programmiersprachen sind schwammig, weil es viele Ausnahmen gibt. Perl beispielsweise ist eine Skriptsprache, obwohl die Programme kompiliert werden.

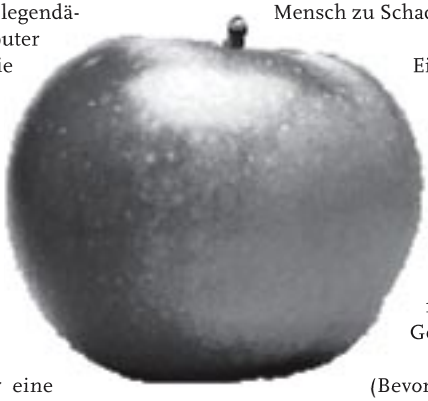
Der Oberbegriff für diese bunte Mischung Sprachen wurde für die erste ihrer Art geprägt: Zusammen mit UNIX erschien die Shell als Schnittstelle zwischen Betriebssystem und Benutzer auf der Bildfläche. Die Shell interpretiert eine interaktive Skriptsprache. Außerdem gibt es die Möglichkeit mehrere Befehle zusammen in einem Text-Dokument zu hinterlegen und auszuführen. Diese Befehlslisten liefen dann wie "nach Drehbuch" ab. Von "script", dem englischen Wort für "Drehbuch", haben Skriptsprachen ihren Namen.

Bootstrappen

Der Baron von Münchhausen stand bei diesem Ausdruck Pate: Es gibt eine Geschichte von/über Münchhausen, in der er sich am Riemen ("strap") seiner eigenen Schuhe ("boots") aus einem Sumpf zieht. Wenn das keine nette Analogie ist ...

Apple & Macintosh

Mitte der siebziger Jahre waren Steve Wozniak und Steve Jobs im legendären Homebrew Computer Club bekannt als "die zwei Steves". Wozniak war der Erfinder des "Apple"-Computers. Jobs promotete das Produkt. Er verlieh dem Computer auch seinen Namen – Jobs hatte mal auf einer Obstplantage gearbeitet. [2]



"Macintosh" war nur eine konsequente Fortführung dieser Benamungsstrategie, denn "McIntosh" ist eine Apfelsorte. Wie gut, dass in der Obstplantage nicht Braeburn-Äpfel angebaut wurden. Ob sich für einen "iBrae" wohl Käufer gefunden hätten?

Font

Diese Wortherkunft ist straight-forward: Lateinisch "fundere", französisch "fonte" bedeutet "gießen" oder "schmelzen". Das Wort geht also auf das Gießen der Bleilettern zurück, die früher zum Drucken verwendet wurden.

Roboter

Dieses Wort ist slawischen Ursprungs. Im Russischen heisst "Robota" Arbeit. Im Tschechischen und Östereichischen ist es speziell "Fronarbeit", also unbezahlte Arbeit für einen Grundherren. Die letztere Bedeutung hatte der Tscheche Karel Capek im Kopf, als er 1921 das Theaterstück "R.U.R." schrieb. Darin bezeichnete er für die Fronarbeit gezüchtete Menschen als "Roboter". Der Verbreitung des Begriffs halfen vermutlich auch die berühmten drei Robotergesetze, die Isaac Asimov in einem seiner Romane aufstellte:

Ein Roboter darf niemals einen Menschen verletzen oder durch Untätigkeit zulassen, daß ein Mensch zu Schaden kommt.

Ein Roboter muß den Befehlen der Menschen gehorchen, es sei denn, solche Befehle stehen im Widerspruch zum ersten Gesetz.

Ein Roboter muß seine eigene Existenz schützen, solange dieser Schutz nicht mit dem ersten oder zweiten Gesetz in Konflikt gerät.

(Bevor Capek das Wort "Roboter" erfand, nannte man Roboter in der Literatur "(Halb)Automaten".)

Nerd

Die Autoren sehen in der Herkunft dieses Wortes ihre Beobachtung, daß Nerds eher Kiffer als (Bier-)Trinker sind, historisch bestätigt. Ursprünglich wurde es nämlich "knurd" geschrieben, von "drunk" (rückwärts geschrieben) und meinte all jene, die sich nie betranken.

Slashdot

Die Webseite hat sich zu einer der effizientesten Zeitvernichtungswerkzeuge für Nerds, die etwas auf sich halten, entwickelt. Daß der Name jedoch vom deutschen "schlag tot" abgeleitet ist, auf eine Story so lange einzuschlagen, bis sie tot ist, wissen jedoch die Wenigsten.

Firewall

Wenn man "Firewall" hört und nicht weiß, wie eine Software zum Schutz eines Rechners vor Viren, Würmern und Trojanern zu diesem Namen kam, könnte man eine Marketing-Entscheidung vermuten.

Ungefähr so: Schlipsträger.oO('Wie nennen wir das nun... Mmmh, irgendwas mit "Wall" ist gut. Unser Produkt ist eine Mauer, eine Bastion gegen alles Übel im Netz. Da geht nix durch! [3] Aber was noch... "WormWall" klingt scheiße. Ah, ich weiss, wir nehmen Feuer, da weiß jeder sofort, daß es was Schlechtes ist.')

Nette Vorstellung, aber natürlich war alles ganz anders: Der Begriff "Firewall" ist ziemlich alt. Schon im Mittelalter gab es in manchen Städten Backsteinmauern zwischen Vierteln, damit im Falle eines Feuers nur ein Viertel und nicht die ganze Stadt abbrannte.

Das nächste Mal taucht der Begriff bei den ersten Eisenbahnen auf: Beim Schaufeln der Kohle in den Heizkessel entstand jede Menge leicht entzündlicher Kohlestaub in der Luft. So nah am Feuer ließ dieser Staub denn auch öfters mal den Heizraum und angrenzende Waggons in Flammen aufgehen. Weil verkohlte Passagiere extrem schlechte Publicity sind, wurde eine Eisenwand zwischen dem Heizraum und den Passagierwaggons installiert, um zu verhindern, daß solche Feuer sich auf die Passagierwaggons ausbreiteten – eine Firewall. Der aufmerksame Leser fragt sich jetzt vielleicht, was im Fall des Falles mit dem Heizer passierte. Er verbrannte. Offenbar generierte ein verkohlter Heizer nicht so viel schlechte Publicity...

So weit die historischen Wurzeln. Wie kommt es aber nun, daß ein Begriff der dafür steht, eine Katastrophe auf kleinen Raum zu begrenzen, um etwas Größeres zu schützen, zu einer Bezeichnung wurde für den Schutz eines kleines Bereichs vor dem großen "bösen" Internet?

In den ersten wackligen Netzwerken wurden um die besonders wackligen Bereiche Firewalls gebaut, damit im Falle eines Absturz des Teilbereichs nicht das gesamte Netz crashte. Die ersten Firewalls im Computerbereich waren also tatsächlich noch Schadensbegrenzer der ersten Art, analog zu Mauern und Eisenwänden. Erst später änderte sich die Funktion zu dem, was wir heute kennen. Der Name blieb. [4]

Die letzte Geschichte kann man vielleicht mal bei einem gemütlichen Hacker-Lagerfeuer zum Besten geben. Aber nur wenn keine Eisenwand drumrum ist :)

[1] *http://de.wikipedia.org/wiki/Programmfehler#Das_Wort_.E2.80.9EBug.E2.80.9C*
[2] Stammt aus dem sehr empfehlenswerten Buch "Hackers" von Stephen Levy
[3] Stimmt nicht. Siehe DS #86
[4] Die Eisenbahn-Anekdote stammt aus dem ebenfalls sehr guten Buch "Secrets & Lies" von Bruce Schneier

Warum Softwarepatente Sinn machen

von Keywan Najafi Tonekaboni <keywan@prometoys.net>

Die Debatte um Softwarepatente als Analysemittel für unsere Gesellschaft. Welche Machtinteressen verstecken sich hinter dieser Forderung. Wie werden diese vertuscht und gerechtfertigt. Und warum ist das nur typisch.

Softwarepatente sind erstmal sehr nützlich, zumindest für mich. Ich kann diese als Symbol oder Stellvertreter verwenden um einige Missstände, die ich meine erkannt zu haben, zu analysieren.

Bei den Leuten, die ich mit diesem Text erreichen möchte, sind die Fronten zu diesem Thema klar. Softwarepatente sind böse. Es gibt eine Lobby mit handfesten Interessen, welche mit fadenscheinigen Argumenten versucht, noch mehr Geld und Macht in ihre Hände zu bekommen. Diese klaren Fronten - eine sehr praktische Schwarz/Weiß-Welt - macht es mir wesentlich einfacher, mein Anliegen zu erläutern und rüberzubringen. Wenigstens hoffe ich das ...

Was die Softwarepatent-GegnerInnen glücklicherweise erkannt haben ist, dass es nicht darum geht, durch die Einführung dieser Patente die Welt besser zu machen, Innovation zu fördern, die Wirtschaft zu stärken oder zu mehr Erfindungen im IT-Sektor zu ermutigen. Ihre Kritik basiert hauptsächlich auf dem Argument, dass diese Argumente schlicht falsch sind und das eigentliche Anliegen vertuschen sollen. Um dieses zu verstehen ist ein kleiner Exkurs zur Idee und Realität des Patentsystems unvermeidlich.

Das Patentsystem in der Idee...

Angeblich wurde das Patentsystem eingeführt, um Erfinder (Innen wäre an dieser Stelle lächerlich, weil zu der Zeit Frauen in der Küche bleiben sollten) zu ermutigen, diese Errungenschaften und das damit verbundene Wissen zu veröffentlichen. Dieser große und noble Schritt wurde mit einem zeitlich begrenzten Monopolrecht auf die Verwertung belohnt. Damit sollten Investitionen refinanziert werden können und ein Schutz vor parasitären Abstaubern gegeben sein. Hört sich doch erstmal toll an, wo ist also das Problem?

... und der Realität

Die Probleme ergeben sich daraus, dass heute (vielleicht auch schon früher) Patente eine Quasi-Währung und ein Instrument zur Machtausübung sind. Das Problem der Technizität, also ab welcher Komplexität eine Erfindung “patent-würdig” ist, halte ich für eine irrelevante Detailfrage.

Wie schon Robert Barr, seines Zeichens Patentanwalt bei Cisco, gegen über der Federal Trade Commission (US-amerikanische Bundeshandelskommission) äußerte (DOC), führen Patente nicht zu Innovation. Sie dienen dazu, gewisse Häppchen vom Markt zu sichern und diese in Verhandlungen als Portfolio und Verhandlungsgrundlage anzubieten. Zudem können bei Patentverletzungen die eigenen Patente als Tauschmittel angeboten werden. Viele vermeintlich stark konkurrierende Firmen wie etwa AMD und Intel betreiben ein solches “Cross Licensing”, also eine gegenseitige Erlaubnis, die Patente des jeweils anderen zu nutzen. Dadurch werden in solchen Verhandlungen jene benachteiligt, die kaum oder gar nicht über Patente verfügen. Nach Barr’s Aussage war Cisco’s Motiva-

tion, Patente zu erhalten, ein solches Arsenal an Verhandlungshilfe und Gegenwaffen zu haben und nicht um eine einzige technische Entwicklung zu schützen.

Des weiteren werden Patente auch gerne verwendet, um unliebsame Konkurrenten zu verdrängen, wenn nicht gar auszuschalten. Adobe konnte mit Erfolg ihr Patent auf schwebende Paletten gegenüber Hauptfeind Macromedia geltend machen. Seitdem haben die Macromedia-Programme eine etwas unpraktischere Oberfläche. An dem freien Grafik-Programm Gimp wird meistens kritisiert, dass es keine Unterstützung für den CMYK-Farbmodus bietet. Dieses liegt aber nicht an der programmiertechnischen Unfähigkeit der Gimp-ProgrammiererInnen, sondern den rechtlichen Problemen aufgrund patentierter CMYK-Methoden. Somit kann und wird das Patentsystem darauf verwendet, Konkurrenten oder Gruppen aus einer erlauchten Runde auszuschließen.

Aus dem Vorangegangenen wird hoffentlich offensichtlich, dass es bei Patenten nicht darum geht, irgendjemanden vor irgendetwas zu schützen, sondern ein Machtinstrument in der Hand zu haben, mit denen Beziehungen gestaltet und kontrolliert werden können.

Die Rolle der Patentämter

Ein weiteres problematisches Konstrukt sind die Patentämter. Diese erhalten Geld, um Patentanträge zu prüfen und neue Patente zu erteilen. Der klassische Punkt der wirtschaftlichen Abhängigkeit ist schon mal vorhanden. Des weiteren ist es für eine/einen MitarbeiterIn im Patentamt wesentlich komfortabler, ein Patent zu erteilen, statt dieses begründet und anfechtbar abzulehnen. Daher kann schon strukturell kein Interesse bei den Patentämtern bestehen, die vermeintlich gutgemeinten Qualitätskriterien ansatzweise durchzuziehen. Selbst wenn Sie dieses versuchen würden, wären Patente als Druck- und Machtmittel weiterhin vorhanden. Sie wären lediglich nicht ganz so einfach zu ergattern, aber die Kreativität beim Lücken finden sollte nicht unterschätzt werden.

Warum die Kritik weitergehen muss

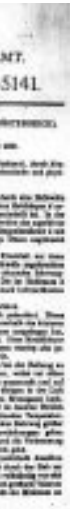
Soweit nichts Neues. Ich unterscheide nun aber nicht zwischen Patenten, Softwarepatenten und so genannten Trivialpatenten (Wenn mensch in einen Hundehaufen tritt interessiert es auch nicht ernsthaft wie groß dieser war, es ist nun mal Scheiße). Die Unterscheidung zwischen diesen wird gerne - besonders von den Befürworten - genutzt, um zu suggerieren, dass es ein faires System, einen fairen Markt gibt. Dem ist aber nicht so. Es geht darum, Macht, Kapital und Profitabschöpfung zu konzentrieren und zu maximieren. Bevor ich als paranoid und Anti-Kapitalist (Danke) abgetan werde, sollten die Finanzgesetze, Globalisierung, Marktmechanismen und die alltägliche Realität reflektiert werden. Sprüche wie “Softwarepatente schaden dem deutschen Mittelstand” bringen uns nicht weiter. Diese Missstände sind keine Krankheit, ein Irrweg des Systems, sondern Teil des Planes. Natürlich muss jemand vor dem anderen geschützt werden, aber nicht der große Fisch vor dem kleinen, sondern umgekehrt.


ÖSTERREICHISCHES PATENTA
PATENTSCHRIFT Nº 14

Die Frage muss daher lauten: warum ist ein solcher Schutz notwendig? Was ist die Ursache und wie kann diese beseitigt werden? Warum muss jemand sich darum Gedanken machen, wie Investitionen zurück fließen können oder wovon sich die Person ernährt? Vielleicht liegt der Fehler nicht darin, dass jemand Plagiate erstellen könnte, sondern dass beim Prinzip der Gewinnmaximierung Leute auf der Stecke bleiben können (sprich im wahrsten Sinne des Wortes “verrecken”). Wenn ich mir nicht Sorgen machen muss, wie ich morgen was zu Essen auftreiben kann, ist es mir vielleicht auch egal, wer meine Erfindung ausnutzt oder ich nehme dieses dann gar nicht mehr als solches wahr, sondern betrachte es als teilen.

Ich bin mir über die utopische Komponente meiner Gedankengänge im klaren, aber Utopie ist relativ und kein logischer Fehler. Ich finde es auch gut, kurzfristig gegen neue Gesetze, welche die fürchterliche Lage noch schlimmer machen, zu mobilisieren um diese zu verhindern. Aber meiner Meinung nach ist es wichtig diese Gedanken und Aspekte nicht aus dem Blickfeld zu verlieren, weder während der Proteste, noch wenn das kurzfristige Ziel erreicht oder gescheitert ist.

Willkommen in der Demokratie



Nun engagieren sich die GegnerInnen seit mehreren Jahren und konnten mehrfach erfolgreich gegen Softwarepatente vorgehen. Trotzdem sehen sie sich einer scheinbar übermächtigen Lobby gegenüber, die mit miesen Tricks und guten Beziehungen trotzdem ihre Pläne durchzudrücken scheint. Naiv und verwundert werden T-Shirts gedruckt mit "Power to the parliament". Dabei darf nicht vergessen werden, dass Parlamente in ihrer ursprünglichen Idee dafür gedacht waren, die Meinungsverschiedenheiten der gutbetuchten aufstrebenden bürgerlichen Schicht zu klären und dieser Mitspracherecht gegenüber Adel und König zu gewähren. (Ein Ausgleich zwischen den Interessen der Unterschicht und der Mittel- wie Oberschicht war nicht vorgesehen und jegliche Versuche in diese Richtung sind in den letzten 100 Jahren auf kurz oder lang gescheitert). So heftig ist es heutzutage nicht mehr, jede Person darf unabhängig von Einkommen und Geschlecht wählen (vorausgesetzt sie ist ein guter Deutscher/EU-Bürger). Aber in der Demokratie haben seit jeher Interessengruppen geherrscht und nicht "das Volk". Ob nun alte Macht-Cliquen oder neue. Der Chef von Siemens (VW, Microsoft, ...) hat nicht nur eine Stimme alle vier Jahre, sondern kann auch mit allerhand drohen, vorzugsweise entziehen von Arbeitsplätzen und steuerpflichtigem Einkommen. Ich hatte noch keine Audienz beim Kanzler und vermutlich hat dieser eher eine bei Herrn Heinrich von Pierer. Demokratie bedeutete seit jeher, den Massen eine scheinbare Macht zu geben, weil es billiger, effektiver und einfacher ist, als sie zu unterwerfen und im gleichen Atemzug zu manipulieren und ihren Einfluss zu beschränken. Je nach Zeit, Möglichkeiten und Notwendigkeit wahlweise durch Kirche, RTL, Wahlgesetze oder -fälschungen.

Es ist daher kein Skandal, wenn sich die Kommission (selbst aus Demokraten-Sicht sollte die Hierarchie der EU sehr fragwürdig erscheinen) und die Regierungschefs einfach über den Willen des Parlaments oder gar des Auftraggebers namens "Volk" hinwegsetzen. Es ist ebensowenig verwunderlich, dass Patentämter "ohne rechtliche Grundlage" seit Jahren Softwarepatente erteilen, um vollendete Tatsachen zu schaffen. Das ist nun mal deren Aufgabe und die Regeln sind ihre. Diese werden gebogen und umgedeutet, wann immer es nötig ist und irgendein Ministeriumsmitarbeiter findet schon eine kreative Ausrede ("A Punkte wurden schon immer durchgewunken"). Zweck von Verfahrens- und Formfehlern ist nicht die vernünftige Entscheidung, sondern ein Teil des Brechen- und Biegenprogramms. Schließlich muss ein Krieg durchgesetzt oder die Wirtschaftsordnung aufrecht erhalten bzw. "verbessert" werden. Daher ist meine Forderung nicht "Power to the parliament", sondern "Power to the coders, to the street, to the people". Hört sich hippieesque an? Mag sein, aber dem Großteil der ParlamentarierInnen würde ich nicht mal das Klo meiner Katzen anvertrauen. Warum sollte ich denen also anvertrauen, wie ich zu leben habe und warum sollte das jemand mir anvertrauen, wenn ich in irgendeiner Machtposition bin. Wenn, dann können wir nur uns das nur selbst anvertrauen und gegenseitig, auf gleicher Augenhöhe aushandeln. Ist kompliziert und anstrengend, aber Effektivität ist nicht das Maß aller (irgendwelcher) Dinge.

Wir könnten nun davon ausgehen, dass sich die Softwarepatente nur einreihen in eine Reihe von Entwicklungen der letzten Zeit, welche die Situation zu Gunsten der derzeit Stärkeren verschärfen. Softwarepatente haben aber eine besondere Tragweite, die sie gegenüber Reformen der Sozialkassen, Hartz, Anforderungen an ArbeitnehmerInnen, neuer Gnadenlosigkeit gegenüber wirtschaftlich schwächeren Ländern und "neuer Weltordnung" heraus sticht.

Patente und freie Software

In einem anderen Artikel erwähnte ich die Notwendigkeit von kreativen Gegenentwürfen. Es macht keinen Sinn, das alles zu kritisieren, ohne sich aktiv auf eine Alternative zuzubewegen. In den letzten 30 Jahren hat sich im Computerbereich ein Gegenentwurf herausgebildet, der in den letzten Jahren sehr populär geworden ist. Freie Software ist für mich digitale Anarchie (im eigentlichen Sinne, nicht dem umgangssprachlichen). In den beiden Hauptströmungen mit Selbstschutz (GPL) und ohne (BSD) bietet sie die Möglichkeit zur freien und gleichberechtigten Kooperation. Gefällt mir etwas nicht innerhalb eines Projekte, so kann ich ohne größere Nachteile mein eigenes Ding drehen. Solche Trennungen haben sich immer wieder als sehr positiv herausgestellt, wie z.B. Inkscape (Sodipodi-Fork) zeigte. Die Quellen sind verfügbar und ich habe das Recht zu ändern, zu lernen und weiterzuverbreiten wie ich mag. Somit ist weder Zugang zu Ressourcen, Wissen noch "dem Markt" verwehrt. Dieses Prinzip freier und diskriminierungsloser Kooperation hat dazu geführt, das sich binnen kürzester Zeit (nachdem eine gewisse Hemmschwelle vor 10 Jahren überschritten wurde) rasant, flexibel und vielfältig weiterentwickelt hat. Und die kapitalistischen Trittbrettfahrer wie SUN, IBM oder Apple stören nicht wirklich, denn sie können mich nicht einschränken. Und in einem Teil der Fälle lässt sich schon in diesem kruden Wirtschaftssytem der Magen zufrieden stellen.

Meiner Meinung nach ist dieses Prinzip der Kooperation im Digitalen nahezu unaufhaltsam und "exponentiell" (im metaphorischen, nicht im mathematischen Sinn). So lässt Wikipedia den Duden-Verlag bereits nach vier Jahren schlottern und kaum ein System hat sich so schnell und weit verbreitet in den letzten Jahren wie GNU/Linux. Apple weiß das, IBM weiß das, SUN weiß das und vor allem weiß das Microsoft. Wenn proprietäre Software in naher Zukunft noch Bestand haben will, dann müssen sich diese was einfallen lassen, denn technisch, gesellschaftlich und psychologisch spricht alles für freie Software. Das größte Gift für ein Unternehmen, einen Herrscher oder anderen, die aus Abhängigkeitsverhältnissen ihre Vorteile ziehen, ist Autonomie. Wenn Behörden, Firmen, Einrichtungen und Privatpersonen nicht mehr von der Vorgabe einer zentralen Stelle, einem Monopol oder einer Oligarchie abhängig sind, dann ist es schwer, diese auszubeuten. Wenn sich aber weder technisch, noch mit Marketing (Propaganda) oder gar mit Kapital (weder GNU, ASF noch BSD lassen sich aufkaufen), also mit Mitteln des "freien Marktes" diese revolutionäre Bewegung aufhalten lässt, dann müssen die Spielregeln geändert werden. Und ab diesem Punkt werden Softwarepatente sehr interessant. Ob mittels trojanischer Pferde, was C#/Mono vorgeworfen wird, oder Trivialpatenten, das Patent- und Urheberrecht ist der Schlüssel um freie Software niederzuschlagen.

Fazit

Wenn wir uns also langfristig vor einer bedrohlichen Einflussnahme schützen wollen, reicht es nicht aus, vor Parlamenten zu demonstrieren und hier und dort die GPL von Gerichten bestätigen zu lassen. Das sind notwendige kosmetische Korrekturen. Das dahinter liegende System muss erkannt, bekämpft und vielleicht sogar beseitigt werden, damit so etwas "gefährliches" wie Freie Software auf Dauer Bestand hat. Die digitale Komponente macht vieles leichter, vor allem das Teilen, aber wenn die Idee, die Denkstrukturen, die Freiheiten und Arbeitsweise in den analogen, sprich die physische Welt umschlagen, wird es für die herrschenden Verhältnisse gefährlich. Deshalb geht es bei Softwarepatenten sowohl für "die", als auch "uns" um mehr, als nur ein paar geschützte Algorithmen.

Literatur

Kühnl, Reinhard: "Formen bürgerlicher Herrschaft. Liberalismus - Faschismus." Reinbek 1971

Spehr, Christoph: "Die Aliens sind unter uns! Herrschaft und Befreiung im demokratischen Zeitalter." München 1999

Kahin, Brian: "Auf dem Holzweg" in c't 1/2003 Seite 74ff.

WSIS Review – Hacking a Dictatorship

von Markus Beckedahl <markus@nnm-ev.de>

Vom 16.- 18. November 2005 fand in Tunis / Tunesien der zweite World Summit on the Information Society (WSIS) statt. Der WSIS-Prozess wurde von den Vereinten Nationen gestartet, um eine globale Vision einer Informationsgesellschaft zu debattieren und Lösungen für die Verringerung der Digitalen Spaltung weltweit zu finden.

Der erste WSIS fand im Dezember 2003 in Genf statt. Damals entstanden eine Gipfel-Erklärung und ein Aktionsprogramm. Da wurde, kurz zusammengefasst, in blumigen und diplomatischen Worten eine Informationsgesellschaft für alle gefordert und mit dem Aktionsplan wollte man alle nötigen Schritte einleiten, um bis zum Jahre 2015 das Internet bis "ins letzte Dorf in Afrika" zu legen. Aufgrund der Entscheidungsstrukturen der Vereinten Nationen kam damals natürlich nur ein Minimalkonsens ohne jegliche Vision heraus. Beinahe hätte sogar ein offizieller Bezug auf die UN Menschenrechtserklärung von 1948 den Einzug in das Gipfeldokument verpasst.

Zwei Fragen wurden damals ausdiskutiert, aber nicht gelöst: Die Frage der Internet Governance und der Finanzierungswege, um die digitale Spaltung zurück zu drängen. Wie immer in solchen Situationen gründete man zwei Arbeitsgruppen, die, dem UN-Generalsekretär Kofi Annan unterstellt, im zweiten Gipfelprozess Empfehlungen und Lösungsvorschläge ausarbeiten sollten. Beide „Working Groups" waren nach dem Multistakeholder-Ansatz besetzt, das heißt paritätisch durch Vertreter der einzelnen Stakeholder „Regierungen", „Wirtschaft" und „Zivilgesellschaft" besetzt. Auf dem Gipfel oder besser der letzten Vorbereitungskonferenz drei Tage davor sollte es also zum Showdown kommen.

Internet Governance – Wer kontrolliert noch mal das Netz?

Die letzten drei Jahre dominierte im WSIS-Prozess ein Thema, das eigentlich nicht viel mit den ursprünglichen Zielen zu tun hatte:

Internet Governance. Viele Länder wollten den Zustand ändern, dass das Domain Name System (DNS) von ICANN und damit letztendlich vom US-amerikanischen Handelsministerium kontrolliert wird. Statt einer Regierung sollten viele Regierung eine „Weltregierung" bilden, am besten unter der Kontrolle der International Telecommunication Union (ITU). Die ITU ist eine UN-Organisation für

den Post- und Telekommunikationsbereich und war federführend verantwortlich für den WSIS-Gipfelprozess. Bis wenige Monate vor dem zweiten Gipfel standen sich Staaten wie China, Brasilien und Pakistan den Industrieländern streitend gegenüber, was das favorisierte Modell betraf. „ITU oder ICANN " wurde fast zur einzigen Frage des Gipfels. Auf der vorletzten Vorbereitungskonferenz zum Tunis-Gipfel brachte die EU unerwartet ein Kompromisspapier in die Debatte ein, um eine gemeinsame Lösung zu finden und den Gipfel diesbezüglich nicht scheitern zu lassen. Die USA waren alles andere als amüsiert, dass ihre Bündnispartner ihnen in den Rücken gefallen waren und starteten eine internationale Medien- und Diplomatiekampagne. Diese spielte das Vorurteil aus, dass die Regierungen das Internet übernehmen wollten. Der UN-Generalsekretär Kofi Annan veröffentlichte zwar noch kurz vor Tunis in der Washington Post einen Beitrag um darauf hinzuweisen, dass die UN nicht das Internet übernehmen wollen würde – da war der Zug aber schon abgefahren.

In der Nacht vor dem Gipfelbeginn einigten sich die Regierungen auf ein gemeinsames Papier, was den Status Quo bei ICANN erstmal erhält - inklusive der Kontrolle der US-Regierung über ICANN und damit das DNS. Allerdings konnten sich die Europäer durchsetzen, ein "Global Forum on Internet Governance" auf internationaler Ebene zu installieren, das diese Fragen weiter entwickeln soll – und das in einem Multistakeholder-Verfahren durch Einbeziehung von Privatwirtschaft und Zivilgesellschaft. Das erste „Global Forum" soll nächstes Jahr im Sommer in Athen stattfinden, weil ein griechischer Diplomat als erstes den Finger gehoben hatte. Bei der Ausgestaltung der Global Forums wird sich zeigen, was dieser Gipfel gebracht hat. Leider finden sich im Gipfel-Dokument mehr „soll"- als „muss"-Formulierungen. Allerdings gehen die Interpretationen schon so weit, dass man aus dem Forum vielleicht tatsächlich was brauchbares machen könnte: Beispielsweise mal ein „Global Forum" mit dem Schwerpunkt auf Freie Software.

Digitale Spaltung?

Ach ja, es gab noch ein zweites strittiges Thema, nämlich Finanzierungswege zur Verringerung der digitalen Spaltung – Kabel legen sich ja nicht selbst. Hier fand man keine wirkliche Lösung, da die Industriestaaten zu sehr an ihrem Paradigma festhielten, dass Investitionen erst nach Marktöffnung getätigt werden sollten. Mit anderen Worten, wenn ein armes afrikanisches Land seine Märkte öffnet, kommt eventuell gerne Siemens vorbei und errichtet Internet- und Mobilfunk-Netze. Der so genannte „Digital Solidarity Fund", eine zentrale Forderung aus der ersten WSIS-Phase, wurde letztendlich zu einem freiwilligen zahnlosen Tiger nach Vorbild eines Gütesiegels. Ganze sieben Millionen Euro wurden schon eingezahlt, davon fast die Hälfte aus afrikanischen Staaten. Die Überwindung der digitalen Spaltung, vor allem in den ärmsten Ländern ist somit nur noch eine Frage der Zeit... Aber dafür gibt`s ja jetzt den 100$ Notebook.

Tunesischer Sicherheitsapparat

Tunesien gibt sich nach außen hin als Musterbeispiel einer arabisch liberalen und offenen Demokratie und ist für viele ein günstiger und attraktiver Ferienort. Weniger bekannt ist, dass Tunesien seit 1987 eine Schein-Demokratie hat mit einem auf Lebenszeit „gewählten Präsidenten" Ben Ali. Dieser hat sich seine Entscheidung, auf Lebenszeit Präsident zu sein, vor zwei Jahren in einer „demokratischen Volksabstimmung" noch mal vom Volk mit 99,8 % bestätigen lassen. Die Opposition wurde aber schon 1987 entweder gleichgeschaltet, des Landes verwiesen oder verfolgt. Eine freie Opposition ist kaum vorhanden, fundamentale Menschenrechte wie Presse-, Meinungs- und Versammlungsfreiheit wurden praktisch abgeschafft – natürlich nur für den Kampf gegen den Terror. Oppositionelle Gruppen haben praktisch kaum Möglichkeiten, Kritik zu üben, eine freie Presse ist nicht vorhanden. Schon nach der Entscheidung der UN, Tunesien als Gastgeberland des zweiten WSIS zu ernennen, hagelte es massive Kritik. Immerhin sollte der WSIS auch ein Gipfel der Informationsfreiheit sein. Die Kritik wurde allerdings von den meisten Staaten nicht ernst genommen. Auf der ersten Vorbereitungskonferenz der zweiten Gipfelphase in Hamamed / Tunesien gab es massive Einschüchterungsversuche der „tunesischen Zivilgesellschaft" gegenüber Menschenrechtsaktivisten der Zivilgesellschaft.

Weitere Vorbereitungskonferenzen wurden deshalb danach auf „sicherem Boden", nämlich der Schweiz abgehalten. Was wir dort erlebten war gleichsam bizarr. Grosse Gruppen tunesischer „Gongos" (von uns so genannt, steht für „Governmental NGOs") reisten an, um sämtliche zivilgesellschaftlichen Vernetzungstreffen zu stören und um alles zu protokollieren. Dies führte zu leicht bizarren europäischen Vernetzungsmeetings, wo immer in der letzten Reihe tunesische Vertreter saßen und alles auf Papier aufzeichneten. Die Arbeit der Zivilgesellschaft wurde so massiv gestört. Selbst auf einem Vernetzungstreffen nach der „Wizards of OS Konferenz 3" in Berlin gab es Besuch von der tunesischen Regierung.

Organisation des Citizen Summit

Nach vielen ungehörten Protesten starteten die Diskussionen über einen Boykott des WSIS2. Allerdings gingen die Diskussionen ziemlich schnell in die Richtung, dass ein Boykott und ein "Alternativgipfel" außerhalb Tunesiens zum selben Zeitpunkt wenig bringen würde und dass die Kritik an der tunesischen Regierung in ihrem eigenen Land besser aufgehoben sein würde. Die Planungen für den "Citizen Summit" starteten im Spätsommer diesen Jahres. Ziel war ein Alternativgipfel in Tunis parallel zum WSIS, wo vernachlässigte Themen wie Menschenrechte, Privacy und Zugang zu Wissen in der Wissensgesellschaft von einem gro-

ßen Bündnis aus Menschenrechtsorganisationen thematisiert werden sollten.

Viele Versuche wurden gestartet, in Tunis Hotels anzumieten. Das klappte erstmal immer, nach und nach wurden aber selbst von weltweit agierenden Hotelketten die Buchungen mit fadenscheinigen Argumenten gecancelt. Mal waren es Sicherheitsgründe, dann wurden kurzfristig unvorhergesehene Bauarbeiten genannt. Für ein Hotel wartet eine Organisation immer noch auf die Rückerstattung einer Anzahlung in vierstelliger Höhe. Der Citizen Summit konnte leider letztendlich nicht stattfinden, aber die Organisation und das „geschickte Händchen" der tunesischen Krisenmanager hatte genug mediale Aufmerksamkeit geschaffen, dass die Arbeit alles andere als nutzlos war.

Übergriffe tunesischer Sicherheitsbehörden

Am Montag vor dem Gipfel gab es wegen der Raumproblematik ein anberaumtes Vorbereitungstreffen im deutschen Goethe-Institut in Tunis. Nur Wenige wußten von dem Treffen, an dem neben zivilgesellschaftlichen Organisatoren und wenigen tunesischen Oppositionellen auch der deutsche Botschafter teilnehmen wollte. Als die Teilnehmer des Treffens um 14 Uhr vor dem Goethe-Institut auftauchten, war das Gelände weiträumig von der Geheimpolizei abgeriegelt. Die tunesischen Oppositionellen sollten in Autos gezerrt und verschleppt werden, selbst dem deutschen Botschafter wurde der Zutritt zum Goethe-Institut in Begleitung zweier Oppositioneller verwehrt – was dieser natürlich nicht amüsant fand. Wenige Stunden später ergab sich das gleiche Bild bei einem von der Heinrich Böll Stiftung anberaumten Vernetzungstreffen von deutschen und arabischen Mitgliedern der jeweiligen Zivilgesellschaften.

Auch hierfür wurden alle Räumlichkeiten kurzfristig abgesagt. Allerdings bot eine unabhängige tunesische Frauenrechtsorganisation ihr Büro als Treffpunkt an. Nicht verwunderlich war, dass das Telefon und das Internet der Organisation ab dem Zeitpunkt der genaueren Planungen aus „technischen Gründen" nicht mehr funktionierten. Wenige Teilnehmer kamen vor dem verabredeten Zeitpunkt in das Gebäude, alle anderen wurden an den etwas später errichteten Absperrungen der Geheimpolizei abgewiesen, die die Veranstaltung als „illegal" bezeichneten. In den Tagen vo dem Gipfel wurden noch ein Journalist der französischen Zeitung „Le Liberation" und ein Fernsehteam des belgischen Senders RTBF in Tunis von Beamten in Zivil zusammengeschlagen, als diese über Menschenrechtsverletzungen recherchieren wollten: Hautnahe Recherche quasi. Der Generalsekretär von „Reporter ohne Grenzen" wurde bei seiner Ankunft auf dem Flughafen in Tunis direkt im Flugzeug wieder nach Hause geschickt, weil seine Organisation in der Vergangenheit Tunesien wegen Menschenrechtsverletzungen kritisiert hatte.

Sicherheit auch in den Hotels

In allen Hotels lungerten die üblichen Gruppen von Männern mit Knopf im Ohr und schlecht sitzenden Anzügen herum und sorgten für „Sicherheit" – bei uns eher für ein Gefühl der Unsicherheit. Glücklicherweise ließ deren Technikkompetenz zu wünschen übrig und wir konnten in unserem Hotel für fast eine ganze Woche einen WLAN-Router ans Hotel-Netz anschließen, bis er erst am letzten Abend leider „entfernt" wurde. Druckereien waren übrigens in der Woche des WSIS überall in Tunis von der Regierung geschlossen worden. Damit niemand auf den Gedanken kam, regierungskritisches Material drucken zu lassen.

Fotografieren verboten?

Ich musste verwundert feststellen, dass das Fotografieren von Polizeieinrichtungen oder Straßensperren in Tunesien anscheinend strengstens verboten ist. Einige hatten schon beim Check-In auf dem Gipfel von Problemen berichtet, die ich aber nicht nachvollziehen konnte, weil ich ständig meine Digikam auf alles draufhielt. Am letzten Tag in Tunis spazierte ich aber noch mal durch die Strassen und fand ein lustiges Schild, wo "Police Technique" drauf geschrieben stand. Als ich einen Schnappschuss von dem Schild machte, war ich

plötzlich von drei Polizisten, wie immer in Zivil, umringt, die mich festnehmen wollten.

Nach zehnminütiger Diskussion, von beiden Seiten in gebrochenem Französisch, konnte ich glücklicherweise darauf hinweisen, dass ich kein Terrorist bin, sondern dass mich mein WSIS-Badge als Vertreter der deutschen Regierungsdelegation auszeichnete. Glücklicherweise hatte ich das Badge noch in der Tasche. Auf die Idee, dass man auf Digikams auch Fotos löschen könnte, kam zum Glück niemand von den dreien. Später stellte ich fest, dass ich die technische Abteilung des Informationsministeriums abgelichtet hatte.

Sicherheit und RFID

Das Gelände des WSIS war weiträumig abgesperrt und von mehreren Sicherheitsringen umzäunt. Auf das Areal selbst kam man nur mit Shuttlebussen und einem WSIS-Badge. In diesem waren RFID-Chips eingebaut, die man am Eingang an ein Lesegerät halten musste, um das darauf befindliche Bild mit dem Gesicht des davor Stehenden zu verifizieren. Manchmal funktionierte die Technik aber nicht und man kam auch so rein. Eine Privacy-Police wurde nicht veröffentlicht. Bis heute ist unklar, wer im Besitz der Personen bezogenen Daten ist, ob nur die ITU und damit die UN einen Zugriff darauf hat oder auch die tunesische Regierung die gesamten Datensätze behalten dürfte. Richard Stallman rannte bei seinem Besuch auf dem Gipfel mit einen mit Alufolie umwickelten Badge herum und wurde dafür beinahe von tunesischen Polizisten in Zivil abgeführt. Das sei ja unhöflich und so... Nach mehrmaligem Durchschreiten der Sicherheitsschleusen mit viel Technik in den Taschen hatten wir auch das Gefühl, dass es kein Problem gewesen wäre, Bomben in Einzelteilen aufs Gelände zu schleppen und dort zusammenzusetzen.

Expression without Repression

Das Gipfelgelände selbst war in zwei Teile unterteilt: Eine große Messe mit dem Schwerpunkt "ICT4Development" befand sich auf tunesisch kontrolliertem Territorium, inklusive eines zensierten Internets. Der direkt daran anschließende WSIS-Gipfel mit den meisten Veranstaltungsräumen wurde wiederum von der UN kontrolliert, inklusive eines weit gehend

unzensierten Internets. Bei einer Veranstaltung mit dem Titel „Expression without Repression" auf dem tunesischen Gelände wurde der Unterschied offensichtlich. Der zweitägige Workshop thematisierte, wie man in repressiven Regimen von seinem Menschenrecht auf freie Meinungsäußerung durch technische Hilfe wie Blogs und Anonymizer Gebrauch machen kann. Nach einer Diskussion über „Blogs und Meinungsfreiheit" stand ein Bericht der OpenNet Initiative zur Filterinfrastruktur in Tunesien auf dem Programm. Gegen Ende der Diskussion füllte sich der Raum immer weiter mit den üblichen tunesischen Beamten in Zivil und es wurde offensichtlich, dass diese die Veranstaltung „sprengen" wollten. Die geplante Pause wurde abgesagt, die Diskussion ging weiter und wir mobilisierten viele weitere Teilnehmer per SMS, um genug Aufmerksamkeit auf die Repression zu lenken. Das klappte auch irgendwann und die Tunesier verschwanden wieder, weil der Raum und der davor liegende Flur überfüllt waren. Dafür gab`s kein Internet mehr im Raum.

Tunesische Zensur im Netz

Während einer Woche Aufenthalt in Tunesien konnten wir uns auch ausführlich mit der tunesischen Internet-Zensur auseinandersetzen. Sehr viele Seiten sind gesperrt, darunter die komplette tunesische Opposition im Netz, viele vor allem französische Nachrichtenseiten und natürlich die meisten Menschenrechtsorganisationen. Amnesty International wiederum nicht, was uns etwas wunderte. Auch waren beispielsweise die deutschen Seiten von „Reporter ohne Grenzen" erreichbar, die internationalen jedoch nicht. Beim Googlen wurden Suchbegriffe wie "Anonymizer" mit einer französischen Fehlermeldung beantwortet. Der Filterbericht der OpenNet Initiative konnte noch ganze sechs Stunden nach Veröffentlichung herunter geladen werden, dann funktionierte die Zensur auch hier.

Problemlos nutzbar waren aber Anonymizer wie TOR oder aber SSH Tunneling aus Tunesien heraus. Nur der Vertreter von Siemens kam nicht in sein Siemens-VPN und fand dies nicht lustig. Allerdings dürften Tools wie TOR für tunesische Bürger auch keine große Lösung bedeuten, da man dort selbst für das Ansurfen „verbotener Seiten" schnell mal für ein paar Wochen einfach so verschwinden kann. Als nette Lösung dafür wurde auf dem „Expression without Repression"-Workshop eine TOR-USB-Lösung vorgestellt, um in jedem Internetcafe einfach unkompliziert und anonymisiert surfen zu können.

Dann gab`s ja auch noch einen Gipfel

Auf dem WSIS-Gelände gab es eine Vielzahl an Veranstaltungen, insgesamt wohl über 400 innerhalb von fünf Tagen. Aber nur wenige davon fand ich interessant. Dafür freute ich mich über eine HighSpeed-Connection und einigermaßen Ruhe in den Civil Society Offices, um meine vielen Podcast-Interviews schnell und unkompliziert uploaden zu können, die ich dort machte. Die Politiker veranstalteten in der „Plenary Hall" einen Redemarathon, der aber gewohnt eintönig blieb. Bei einer sehr knappen Redezeit von teilweise nur drei Minuten war neben den Dankesfloskeln an die ITU, Tune-

sien und manchmal noch anderen nur wenig Zeit, um die üblichen Floskeln wie „bridging the digital gap" unterzubringen und das jeweilige vertretende Land in den höchsten Tönen zu loben. In die Eröffnungszeremonie kam ich leider nicht mehr rein, weil ich eine dreiviertel Stunde draußen vor der Sicherheitsschleuse warten musste. Zu viele „Jubel-Tunesier" warteten auch auf Einlass, um ihrem Diktator bei seiner Eröffnungsrede zujubeln zu können. Als ich die „Plenary Hall" kurz vor Beginn endlich erreichte, wurden die Türen vor uns geschlossen und es kam beinahe zu Tumulten. Unvergessen war ein Mensch aus der Ukraine, welcher sich gegenüber den UN-Polizisten vor der Tür als Minister der Ukraine zu erkennen gab und beinahe handgreiflich wurde. Wie auch viele andere Jubel-Tunesier. Bei der „Opening Ceremony" selbst kam es dann zu einem kleinen Eklat: Direkt nach dem tunesischen Diktator dürfte der schweizer Bundespräsident sprechen, da die Schweiz den ersten WSIS ausgerichtet hatte. Als dieser in seiner Rede auf Menschenrechtsverletzungen in Tunesien zu sprechen kam, wurde die Live-Berichterstatung vom WSIS im tunesischen Fernsehen abgeschaltet und die arabische Übersetzung in der „Plenary Hall" gleich mit – vermutlich, damit die Jubel-Tunesier keinen seelischen Schaden nehmen mussten.

Fazit: Was hat`s gebracht?

Dass der WSIS-Prozess seinen Ansatz, „eine gemeinsame globale Vision für die Informationsgesellschaft" nicht halten können würde, war uns schon in der ersten Gipfel-Phase bewusst. Entscheidende Fragen einer sich entwickelnden Informationsgesellschaft, wie beispielsweise der Zugang zu Wissen geregelt werden kann, wurden von den Regierungen abgeblockt und zur WIPO verwiesen. Das Hauptinteresse vieler zivilgesellschaftlichen Vertreter war, zu verhindern, dass die Regierungen nicht zuviel schlechte Sachen beschließen und damit Schaden anrichten – und natürlich die Vernetzung. Letztere hat prima geklappt, denn durch den WSIS-Prozess entwickelten sich Netzwerke über Kontinente hinaus, die sicherlich noch länger Bestand haben werden. In Tunis selbst waren mehr als 25 000 Menschen. Wenn man von den Diplomaten, Lobbyisten, Journalisten, Jubel-Tunesiern und Informationsgesellschafts-Urlaubern absieht, konnte man immer noch genug interessante Menschen kennen lernen oder wieder treffen. Am besten dazu waren die Abende geeignet, wo man sich außerhalb des Messe- und WSIS-Troubles vernetzen konnte. Gleichsam hat das Ziel geklappt, dass die tunesische Regierung den WSIS nicht dazu nutzen konnte, ihre Scheindemokratie im besten Licht erscheinen zu lassen. Die mediale Aufmerksamkeit auf Menschenrechtsverletzungen in Tunesien und die Bedeutung von Menschenrechten in der Informationsgesellschaft war vor allem in den westlichen Medien viel höher als erhofft und erwartet.

Auch brachte alleine die Woche in Tunis eine Menge an Erfahrungen, wie es sich in repressiven Ländern lebt. Der ganze WSIS-Prozess brachte viel Einblick in internationale Politik und politische Prozesse. Die funktionieren dort eigentlich wie auf jeder politischen Ebene – mehr ein Jahrmarkt der Eitelkeiten als an Lösungen interessiert. Vor allem ist es eigentlich erschreckend, wie wenig technisches Verständnis Diplomaten und Regierungsvertreter zu haben brauchen, um ihr jeweiliges Land in Fragen der Informationsgesellschaft vertreten zu können. Beim ersten Gipfel vor zwei Jahren formulierten wir noch eine Pressemitteilung mit dem Titel "WSIS - Die UNO sucht die Informationsgesellschaft". Gefunden wurde sie bisher immer noch nicht.

Links:

Ausführliche Berichte und Audio-Interviews rund um den WSIS finden sich bei netzpolitik.org: *http://www.netzpolitik.org/category/wsis/*

Den Gipfelprozess begleitete die WorldSummit2005-Webseite der Heinrich Böll Stiftung: *http://www.worldsummit2005.de*

Mehr Informationen rund um die Internet-Zensur in Tunesien bietet der Filter-Bericht der OpenNet Initiative: *http://www.opennetinitiative.net/studies/tunisia/index.htm*

Erfa-Kreise / Chaostreffs

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

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

Friends & Family

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

Die Datenschleuder Nr. 89

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

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

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

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

Layout
Dirk Engling, Florian Holzhauer, fukami

Chefredaktion
Dirk Engling <erdgeist> und Tom Lazar <tomster>

Redaktion dieser Ausgabe
Frank, Hannes Mehnert, Andreas Bogk, stesie, Keywan Najafi Tonekaboni, Corinna Habets, fukami, Markus Beckedahl, Frank Rosengart

Besonderer Dank
für den BlackBerry: Maxim
für das hintere Umschlagfoto: Sven Hiersemann
http://www.hiesve.de/Staatsrat/crw_0051.htm

01	Saal 1	Saal 2	Saal 3	Saal 4
11				
12	**Software Patenting** Adequate means of protection for software. *André Rebentisch*	**Collateral Damage** Consequences of Spam and Virus Filtering for the E-Mail System *Peter Eisentraut*	**VoIP 2005 - Regulierte Revolution** Ansätze für die Regulierung von VoIP und NGN im vergangenen Jahr *Jörg Müller-Kindt*	**A way to fuzzy democracy** How modern communication can be used to transform the way we think about democracy and make our political decisions. *Christiane Ruetten, Svenja Schröder*
13	**Informationsfreiheitsgesetz** *Jörg Tauss*	**3G Investigations** Scanning your GPRS/UMTS IP network for fun and profit *Achim „ahcf" Friedland, Daniel „btk" Kirstenpfad*	**Seaside: Agile Web Application Development with Squeak** *Marcus Denker*	**10 Thesis on Informational-Cognitive Capitalism** *George N. Dafermos*
14	**Das Geheimnis - Reloaded** *Peter Glaser*	**Military intelligence for terrorists(tm)** A lamer's introduction to retrieving'sensitive 'intelligence information' *Andreas Krennmair*	**AJAX Based Web Applications** *mesch*	**Hashing Trusted Computing** Der aktuelle Stand *Rüdiger Weis*
16	**Black Ops Of TCP/IP 2005.5** New Explorations: Large Graphs, Larger Threats *Dan Kaminsky*	**Was ist technisches Wissen?** Philosophische Grundlagen technischer Wissenschaften *Sandro Gaycken*	**Robots for fun and research** *Verena*	**Lightning Talks Day 2** Nine five minutes talks by various speakers
17	**Personal experiences bringing technology and new media to disaster areas** Experiences from Iraq and post Katrina New Orleans *Jacob Appelbaum*	**Lawful Interception in VoIP networks** Old Laws and New Technology the German Way *Hendrik Scholz*	**PyPy - the new Python implementation on the block** Language/VM R&D, whole program type inference, translation to low level backends, fun *Armin Rigo, Carl Friedrich Bolz, Holger Krekel*	**Sony BMGs digitaler Hausfriedensbruch** Über die Durchsetzung industrieller Interessen um jeden Preis *fukami, Markus Beckedahl*
18	**Search Engines - Oracles of the Information Society** The Saga continues: Search Engines, Technology, Politics, Prostitution, Corruption, Privacy and Espionage. *Frédéric Philipp Thiele, Hendrik Speck, Wolfgang Sander-Beuermann*	**Vulnerability markets** What is the economic value of a zero-day exploit? *Rainer Böhme*	**Privaterra – Report from the field** IT Security and Human Rights organizations – The needs, the challenges and recommandations *Robert Guerra*	**Anonymous Data Broadcasting by Misuse of Satellite ISPs** An open-source project to develop a tool for broadband satellite broadcasts *Sven Löschner*
19	**Mehr Medienvielfalt durch Blogs** *Johnny Haeusler, Markus Beckedahl*	**Old Skewl Hacking - InfraRed updated** MMIrDA - Major Malfunction's InfraRed Discovery Application *Major Malfunction*	**Anonymität im Internet** Rechtliche und technische Aspekte *Andreas Lehner, Peter Franck*	**Alter Wein in einer neuen Flasche: Rootkits unter dem 2.6 Kernel** Kernel Module unter dem 2.6er Kernel für gut und böse? *k-mode, newroot*
21	**Technological art off the trodden tracks** Artists (mis)using technology *Jussi Ängeslevä, Régine Débatty*	**Secure Code** Why developing Secure Software is like playing Marble Madness *Paul Böhm*	**Digital Identity and the Ghost in the Machine** Once I Was Lost But Now I've Been Found *Max Kilger*	**The Cell Processor** Computing of Tomorrow or Yesterday *Torsten Hoefler*
22	**Corp vs. Corp** Profiling Modern Espionage *Fabio Ghioni, Roberto Preatoni*	**Learning cryptography through handcyphers** Shaping a digital future with ancient wisdom *Brenno de Winter*	**Autodafé: An Act of Software Torture** Presentation of an innovative buffer overflow uncovering technique called 'Fuzzing by weighting attacks with markers' *Martin Vuagnoux*	**Lyrical I** Abschluss des CCC-Poesie-Wettbewerbs *Henriette Fiebig, Jens Ohlig, Martin Haase*
23	**Literarisches Code-Quartett** The good, the bad, and the ugly *Andreas Bogk, Felix von Leitner, FX of Phenoelit, Lisa Thalheim*	**Geometrie ohne Punkte, Geraden & Ebenen** Buckminster Fullers Theorie und Praxis einer Wissenschaft zum Selberbauen *Oona Leganovic*	**Community mesh networking** Ubiquitous wireless mesh clouds with olsrd from olsr.org *Elektra Wagenrad*	**Capture The Flag und "Das Hacker Sportstudio"** *Jens Ohlig, Lexi Pimendis, Maximillian Dornseif, mc.fly*

Saal 1	Saal 2	Saal 3	Saal 4	10
	Transparenz der Verantwortung in Behörden *Philipp Sonntag*	**COMPLETE Hard Disk Encryption with FreeBSD** Learn how to effectively protect not only your data but also your applications *Marc Schiesser*		11
	Data Mining für den Weltfrieden *Jule Riede-Buechele*	**Academic tools and real-life bug finding in Win32** *Rafa Wojtczuk*	**The Right Track** A new approach to copyright in the digital world *Nicholas Bentley*	12
Private investigations in searching How to find any book (and many other roadkills) on the Information Super-Highway *Fravia*	**e-Voting: The silent decline of public control** Why German voting machines do not meet the requirements of democratic elections. *Ulrich Wiesner*	**The Web according to W3C** How to turn your idea into a standard *Bert Bos*	**Attacking the IPv6 Protocol Suite** *van Hauser*	13
I See Airplanes! How to build your own radar system *Eric Blossom*	**Internet Voting in Estonia** First-ever pan-national official occasion. *Tarvi Martens*	**Open Source, EU funding and Agile Methods** Sprint methodology in funded OSS projects *Beatrice Düring, Holger Krekel*	**Logical Language Lojban** A Hackers' /Spoken/ Language?! *Sven Moritz Hallberg*	14
Changing Realities Innovation, user-creation, activism and entrepreneurship in Second Life *Cory Ondrejka*	**Fuzzing** Breaking software in an automated fashion *Ilja*	**EvoCell - free software for evolving cellular automata** Exploring the huge space of possible cellular automata by evolution *Philipp Tiefenbacher*	**Lightning Talks Day 3** Nine five minutes talks by various speakers *fukami*	16
Towards the first Free Software GSM Phone Reverse Engineering the Motorola EZX (A768,A780,E680) series of Linux-based GSM phones *Harald Welte*		**Learning JavaScript with the Google Maps API** *mesch*	**Esperanto, die internationale Sprache** Eine gut strukturierte Sprache für Geeks und die EU *pallas*	17
„Xbox"and"Xbox 360"Hacking 17 Mistakes Microsoft Made in the Xbox Security System&Xbox 360 Hacking *Franz Lehner, Michael Steil*	**Disassembler Internals II: Automated Data Structure Recognition** *Richard Johnson*	**Atmel AVR für Dummies** Was ist denn nun eigentlich so ein ‚Interrupt'? *fdo*	**Random Windows Stuff** An introduction to exploitation *Ollie Whitehouse*	18
	How to construct Utopia The relationship between the publication of Moore's death certificate and hacker culture *Lena Elisa Nalbach*	**WarTracking** Satellite Tracking, harvesting and security *M. Elias, Thomas B. Rücker - dm8tbr*	**Hosting a Hacking Challenge - CTF-style** Background information on CIPHER, an international Capture-The-Flag contest *Lexi Pimendis*	19
The truth about Nanotechnology A concise introduction to what NT is, what it can't do yet and what we should be aware of *Niels Boeing*	**Intrusion Detection Systems** Elevated to the Next Level *Alien8, Matthias Petermann*	**Free Software and Anarchism** does the compute? *Sandro Gaycken*	**Memory allocator security** *Yves Younan*	21
Fnord Jahresrückblick Was wirklich geschah *Felix von Leitner, Frank Rieger*	**Zauberhafte Naturwissenschaften** *Wolfgang Hahn*	**Honeymonkeys** Chasing hackers with a bunch of monkeys *Krisztian Piller, Sebastian Wolfgarten*	**Unix sanity layer** A class oriented interface to Unix system management *Sascha Krissler*	22
Hacker Jeopardy The one and only hacker quizshow *Ray, Stefan „Sec" Zehl*	**Entschwörungstheorie** Verschwörungstheoretiker sind hinter mir her! *Daniel Kulla*	**Hexenbesen und heiliger Gral** Vorläufige und subjektive Gedanken zur inhaltlichen Qualität von Wikipedia-Artikeln *Henriette Fiebig*	**Breaking Down the Web of Trust** *Seth Hardy*	23

Saal 1

12 **WSIS - The Review**
Hacking a Dictatorship
Markus Beckedahl, Robert Guerra

13 **Quantum Entanglement**
An introduction
Stephanie Wehner

14 **Covert Communication in a Dark Network**
A major new version of freenet
Ian Clarke, Oskar Sandberg

16 **Bluetooth Hacking - The State of The Art**
A roundup and live demonstrations of all currently known Bluetooth vulnerabilities.
Adam Laurie, Marcel Holtmann, Martin Herfurt

17

18 **Blackberry: call to arms, some provided**
Teach yourself upper management in 22 days
FX of Phenoelit

19 **Security Nightmares 2006**
Oder: worüber wir nächstes Jahr lachen werden
Frank Rieger, Ron

20 **22C3 Closing Event**
Tim Pritlove

Saal 2

Urheberrecht
Fakten, Mythen, Geschichte(n) und mögliche Zukünfte
Jenny-Louise Becker, Julian „hds“ Finn

Fair Code
Free/Open Source Software and the Digital Divide
Meike Ric, hter

Access to Knowledge
Copyright, Patents and Politics at the World Intellectual Property Organisation
Karsten Gerloff

WiFi Long Shots
Wireless connections of 20km and more
Elektra Wagenrad

GNU/Linux für Blinde und Sehbehinderte
Erfahrungen aus der Praxis
Lars Stetten, Sebastian Andres

Advanced Buffer Overflow Methods [or] Smack the Stack
Cracking the VA-Patch
Izik

Saal 3

A discussion about modern disk encryption systems
Jacob Appelbaum

Paper-Prototyping Workshop
Eine Usability-Methode
Antenne Springborn, Ellen Reitmayr

Terminator Genes and GURT - Biological Restrictions Management
Five Years after the announcement of a quasi moratorium
Julian „hds“ Finn, Oliver Moldenhauer

PocketTCP
A Userspace TCP/IP Stack
Paul Böhm

The Realtime thing
What the heck is realtime – and what to do with it
Erwin Erkinger

22C3 Network Review
Sebastian Werner, Stefan Wahl

Saal 4

The Future of Virtualization
The ‘anyOS‘ paradigm and its implications through virtualization
Felix Erkinger

Kochen für Nerds
Christian Jeitler, Hans Knöll

Lightning Talks Day 4
Nine five minutes talks by various speakers
prometoys

The very early Computer Game History
How the games have become the first digital mass product
Andreas Lange

Wargames - Hacker Spielen
Männliche Identitätskonstruktion und spielerische Herangehensweisen an Computer
Francis Hunger

CHAOS COMPUTER CLUB E. V.

- ○ Ja, ich möchte Mitglied im CCC e.V. werden (Aufnahmegebühr 10€ , Datenschleuder inkl.) und habe die Satzung[1] gelesen
  - ○ Normal für 72 € p.a.
  - ○ Reduziert[2] für 36 € p.a.
- ○ Ich möchte ein Abonnement der Datenschleuder, 8 Ausgaben (ca. 2 Jahre, für Mitglieder inkl.)
  - ○ Normal für 32 €
  - ○ Reduziert für 16 €
  - ○ Gewerblich gegen Rechnung für 50 €
- ○ Ich möchte meinen ausstehenden Mitgliedsbeitrag bezahlen
- ○ Ich möchte meine Mitgliedsdaten ändern

Bitte in Druckbuchstaben ausfüllen!

Name, Vorname _____

Straße und Hausnummer _____

PLZ _____ Ort _____

Land _____

Bankverbindung _____

Ich bezahle. . .

- ○ in bar (Betrag in €)
- ○ mit beiliegendem Verrechnungsscheck
- ○ per Überweisung auf das CCC-Konto[3]

Datum _____ Unterschrift, bei Minderjährigen die gesetzlichen Vertreter

Bemerkungen _____

Anlage(n) _____

[1] https://www.ccc.de/club/statutes
[2] Ermäßigungen nur für Studenten, Schüler, Arbeitslose, Unsoldaten, Rentner – geeigneter Nachweis erforderlich!
[3] Bei Mitgliedschaft Verwendungszweck erstmalig "NEU" , später die Chaos-Nr.

Adresse:
Chaos Computer Club e. V.
Lokstedter Weg 72
D-20251 Hamburg

Telefon:
Tel: +49-40-401 801-0
Fax: +49-40-401 801-41

Internet:
https://www.ccc.de/
E-Mail: office@ccc.de

Bankverbindung:
Bank: Postbank Hamburg
BLZ: 200 100 20
Kto: 2340 2046 01
BIC: PBNKDEFF200
IBAN: DE41 2001 0020 0340 2046 01

Dylan Hackers @ ICFP 2005

von Andreas Bogk <andreas@ccc.de> und
Hannes Mehnert <hannes@berlin.ccc.de>

This year saw the 8th annual ICFP programming competition. The contest traditionally runs over 72 hours and is open to all contestants. Entries may be submitted using any programming language. [1]. This is a writeup from the Dylan Hackers team, which won both 2nd Prize and the Judges' Prize.

The Task

"In the far-flung future of the year 2000, functional programming has taken over the world and so humans live in an almost unimaginable luxury. Since it's so easy, humans have used robots to automate everything, even law enforcement and bank robbery – the only job left to humans is to write their robots' control programs."

This year's ICFP competition differed from previous years in having a twofold task. The two halves of the task were roughly two weeks apart. The first half was announced on Friday June 24th, and its task was to write two programs, a Cop-Bot and a Robber-Bot. The Robber-Bot was to rob banks and avoid being caught by the Cop-Bots. The Cop-Bot needed to be able to work together with other Cop-Bots to catch the Robber-Bot. The initial entries had to be submitted on Monday June 27th. The full task description is here [2].

The second half of the task was announced about 2 weeks later on Saturday July 9th, and required the programs to be modified. Robber-Bots could now bribe Cop-Bots, and Cop-Bots would be able to accuse other Cop-Bots of being bribed. Reuse of code would be very important here. The full description of this second task is here. The final entries were due on Sunday, July 10th.

About Dylan

Dylan is an advanced object-oriented programming language. It combines the advantages of expressive "scripting" languages such as Python or Ruby with performance comparable to C.

Gwydion Dylan refers to a specific compiler, d2c, that was originally developed by the Gwydion group at Carnegie Mellon University. It is now maintained as an open source project by the Gwydion Dylan hackers [3]. As the name indicates, the compiler translates Dylan code into C code and then compiles it. It's stable, and produces very efficient code. It's also extremely portable.

The Dylan hackers have entered ICFP since 2000, recieving the Judges' Prize in 2003 [4] and a Second placing in 2001 [5]).

The team

Keith Bauer, Andreas Bogk, Bruce Hoult, Hannes Mehnert, Alex Potanin. Some contributions were also made by Jes Hall, setting up the team's subversion repository and web-based subversion front end to use for the competition.

The first task

Keith Bauer

I began by writing a simple cop and robber in Ruby, to get a head start on thinking about strategies whilst the Dylan libraries came up to speed. Once the Dylan libraries were usable, I converted the Ruby robber over to Dylan, and worked on improving its cop-avoidance techniques and bank-robbing abilities. I don't think much of what I did ended up in the final robber, but it provided a benchmark to test our cop

against during the competition. I didn't participate in the second part of the competition.

Bruce Hoult
At the start of the contest I downloaded the task specification, discussed it briefly with other team members and then went to bed to sleep on it. By the time I woke up Andreas and Hannes had a working framework in Dylan that could correctly parse and respond to all messages from the server, for both the cop and the (much simpler) robber.

Unfortunately, they forgot to check in one file that contained the Dylan equivilent of all the #include directives. This meant that Alex and Keith and I could not compile the program until I'd taken all the "foo not declared" error messages and tracked down what library they came from -- not especially difficult, but tedious and time consuming. While I'm working on this Keith completes the framework necessary for a robber in Ruby and starts working on algorithms for a robber. Alex starts working on the strategy code for a cop even though he can't compile it yet.

The rest of the first day, and all of the second day, I work on improving the usability and features of the framework and build system, helping others with problems, profiling cops- and robbers-in-progress and optimizing hot spots. And thinking about what the ideal robber would do.

The third day I spent entirely on implementing my ideas for a robber. By then Andreas and Hannes had a cop well in hand. It seemed to be better than Alex's cop and was performing well against Keith's robber.

Search Strategy

Ideally, you'd like to choose your move using a minimax algorithm [6] so that you make the best move you have available, given the assumption that your opponent makes the best response that he has available, given the assumption that you make the best reply to his response, and so on to preferably a large number of layers of second-guessing. This approach works fairly well (with alpha-beta pruning) for Chess on modern computers. In the midddle part of a Chess game each player has typically 30 to 40 possible moves each turn. Minimax made computers unbeatable on games with fewer choices each move -- such as Checkers/Draughts or Othello/Reversi -- even on the computers available in the 1960's.

Unfortunately, in our cops and robbers game the five cops have, in combination, more than 1.4 million possibilities for their first move. It's not so bad later in the game, when cops mostly don't have the choice of travelling either by car or on foot at each move, but there are still around a thousand possible cop moves each time. This suggests that even looking ahead two robber moves and two cop moves will be very very hard to acheive within the required five second response time. My sincere congratulations to any team that acheived this, but I don't think such a small amount of look-ahead is useful for the robber anyway in this game where if the robber is touched by a cop even once then he is dead and gets zero points. It's like a game of Chess where you lose if you lose even one pawn.

Because touching a cop is so deadly, I have the robber, each time it is his move, simply start from the current position of each cop and figure out the set of all possible positions that one or more cops could get to on the next move, with no attempt to figure out what a smart cop would actually do. From that set of positions I can then calculate all the places that cops could possibly be after two moves, then after three moves, and so on.

I then have the robber look for the shortest path to a bank such that there is the minimum (preferably zero) possibility of meeting a cop on each

move. I do that using a new A* [7] search each time it is the robber's turn to move, with path costs freshly updated from the new positions of the cops, and with the cost of traversing each intersection dependent on whether it is possible to find a cop there at the time the robber will actually get there.

Refinements

The limitation of this technique is that the world is small and connected enough that cops can usually get to anywhere within about ten moves. This is especially so if some cops are in cars, so there is no point in trying to look further ahead than that. In fact, trial and error showed that it seemed to be best to project out only the next six cop moves and then use that same set for any planning out beyond six moves.

Sometimes, when you start to get surrounded by cops there isn't any way out of the trap that has zero probability of meeting a cop. But if they're surrounding you it's probably because they think they know where you are so it's much better to make a break for it than to stay put, even if your present position looks like the safest place to be for the next five or six moves. Therefore when I calculate where the cops might be I assign probabilities to each location rather than just possible or impossible. After you've made your first move towards a gap between cops and the cops have moved, the chances are good -- if the cops aren't close enough to actually smell you -- that the gap has stayed the same size, or even grown larger, and you might now have a clear run through it to safety.

I didn't worry too much about smell. Smell tells a cop approximately where you are: he knows that you're within one or two moves of his current position. This may give the cops a much better idea of where you are than they had before, and so of course they will start to converge on that position. But if you already know that you have a way to get to the next bank you want to rob with no possibility of a cop touching you on the way then it's not at all a bad thing if the cops all converge somewhere that you aren't any more. In fact, in my testing it seemed that an ideal situation that my robber was often able to exploit was to have all the cops just one or two moves behind as my robber dashed in a circuit around and around the four centrally-located banks!

Conclusion

I was pretty happy with my robber. Even against five of our cops cooperating with each other the robber was able to get 85% - 90% of the money about half the time. The other half of the time the robber was caught by our cops. I think they're both pretty good, with the robber being perhaps just a little too much on the risk-taking side. Certainly I expect we'll soundly beat the cop and robber written by the contest organisers and therefore get through to the main round. In the main round I expect to see very little meaningful cooperation between cops written by different teams and daring robbers may well have a field day.

Andreas Bogk & Hannes Mehnert
After start of the competition, we started working on implementing the protocol. We mostly made use of the regular expression matching facility to to the parsing, and wrote one class for each message type used in the protocol. After this was satisfactorily working, we went to bed.

After getting up on the next morning, we discovered that we had forgotten to add the library imports file to our source repository, meaning that the New Zealand team wasted quite some time reproducing that. Oops.

We kept working on the code building classes from protocol messages, replacing string references to objects like locations and players by actual references to the representing object itself. We also wrote a driver loop to drive dif-

ferent kinds of agents while running the protocol. The interface consisted of a number of generic functions called on some subclass of agent, which the agent implementor had to provide. We also provided simple default methods for all messages. If the called generic function threw an exception, we still sent valid messages (we didn't want to get disqualified by an illegal instruction). So the agent implementors code wasn't part of the trusted code base.

We fixed a bug in our regular expression library, it has a cache of regular expressions, and used \== (identity) for comparison whether the expression was already in the cache. We generated the regular expressions dynamically, so they were equal (\=), but not the same object. Our demo cop used >512MB memory, after the change from \== to \= in the regular expression library, it used <10MB memory.

We proceeded by writing code that generated a set of possible moves for an agent, taking care to properly represent the differnt properties of cops moving by either car or foot. Next was code to advance the state of the world, giving a set of moves for all players in the world. At this point, we were able to do random walks, and telling the McGruffs to do random walks too.

We then started to work on something a little more intelligent for the cops. The basic idea we followed was to keep a map of probabilities for each node, representing the likelihood to find the robber at a given node. For this, we collected all the information we could get, such as setting the probability to zero for all fields where the robber should have been smelled, but wasn't, for banks which have been robbed or not robbed, and integrating information coming in from other cops. Probabilities were kept normalized. For every turn, the cop would predict probabilities for the robber's location next turn, based on the known probabilities from all sorts of sources, and assuming that each of the possible robber moves was equally likely.

It was very interesting to see that this simple approach, based solely on accumulation of probabilities and predicting the next turn only, was powerful enough to win big against a lot of simple robbers we threw against it. We could observe behaviour emerging from those simple rules that looked like serious strategic planning, although we never explicitly coded any such behaviour. If the location of the robber was known, such as the start of the game, or after robbing a bank, all cops would head towards the suspected location. After arriving, they started to spread out and scan the area for traces of the robber. If one of the cops came within smelling distance, the cops started chasing him, spreading out when losing the track, coming together again once he was found again, and eventually cornering the robber on the edge of the map.

We decided not to sleep on the second night at this point, and kept debugging and improving the cop, watching lots of trial runs. Bruce eventually started working on a serious robber, and the last few hours were spent on gradually improving both sides.

Somewhere on the way we implemented voting on plans, which by many participants in the contests was regarded as a problem too hard to solve. In fact, we had a pretty easy metric to deal for that. We have probabilities for the robber locations, so we can give scores to all cop moves which bring that cop closer to one of the suspected robber locations. We would order plans by this score.

Now if our plan wasn't the winning plan, we decided to just follow the winning plan, and not attempt any tricks. The reasoning was that catching the robber was hard enough when you had cooperating cops, and becomes impossible when you don't. So if we wouldn't cooperate, chances are that the team contolling the robber would score points, and we wouldn't. Of course, we would check that the moves suggested by other players were actually valid.

The second task

Andreas Bogk & Hannes Mehnert

We spent the first eight hours implementing the new game protocol. We thought about strategies for deciding whether and when to bribe and take

bribes. After a lengthy discussion with Bruce we decided to play it straight. We considered the robber to be good enough so splitting the loot with other teams wouldn't be worth the trouble. We also decided to use a straight cop, mainly because we couldn't come up with a good strategy to tell when being bribed would increase chances of winning.

What we did work on was detection of rogue cops, though. We used scoring points for behaviour we considered bad, and started to blame a cop once a certain score was reached. Not following the winning plan was considered a minor offense, but repeatedly doing so made a cop suspicious. We figured that somebody not following orders is either stupid (not cooperating, and chances of winning are slim anyway) or a rogue cop. Also, we blamed cops not passing knowledge about evidence, or submitting informs about the robber location that were impossible based on our knowledge of the world.

Of course, we also implemented bad cops and a bribing robber, for the purpose of testing our code. Especially taking over other cops and controlling them had to be tested.

So we spent the rest of the 24 hours testing, fine-tuning and watching battles.

Overall, it was a fun contest. It was a lot like real-world projects: the deadlines are tight, the rules are unforgiving, and the competition is unknown. Some people complained it were too much work for such a short period of time, but we think we've shown that using a sufficiently powerful programming language allows to be done with the mechanics part in time, leaving plenty of opportunity to care about the challenge itself.

Bruce Hoult

Once again I looked at the task specification when it came out, discussed it briefly with other team members, and then went to bed. By the time I woke up Andreas and Hannes had updated the framework to correctly parse the new messages and create default null responses so our old cop and robber code was automatically a valid entry for the second round. So I was able to spend the entire day improving the robber code itself.

Strategy

Nothing in the changed rules made life any easier for cops, so I decided that if our basic robber was good enough in the first phase of the contest then it was still good enough. In particular I didn't see any reason that we'd ever want to try to bribe the cops. It just means giving up a lot of money if you survive, and there is no way to be sure that a bribed cop will do anything useful to you anyway becuase if it does then it is very vulnerable to being accused by other cops. I also didn't implement "shoving".

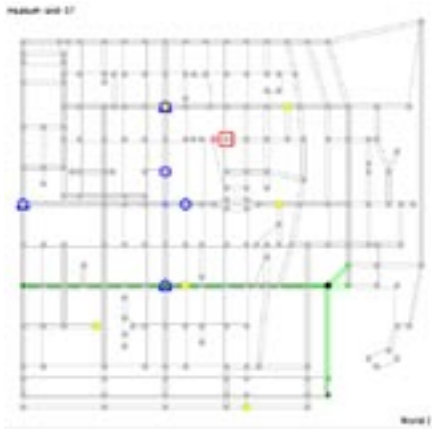
Refinements

What I spent the day doing was making my robber a better bank robber. Everything I did would have been equally useful in the first phase if I'd thought of it then, or had time to implement it.

There was a certain amount of tweaking of various "fudge factors" in the evaluation function for the A* algorithm, but the main change was in how far ahead the robber planned.

In the first submission the robber planned only how to get to a bank safely but gave no thought to how to safely get away from the bank afterwards! This is bad. When the robber got the cops into the pattern of all the cops following it around this was fine as all the cops would be on the same side of the bank and the robber could just carry on out the other side of the bank and away. But ocassionally there would be cops close to the bank on several sides and once they saw it was robbed they could get there quickly and trap the robber.

So the change was that instead of only trying to find a safe path to a bank the robber looked for a safe path of length at least eight moves that included a bank. Once the robber got within less than eight moves from a bank it would automatically start planning the escape, and the closer it got the more certain the escape had to be.



This made the robber quite a bit more cautious, and lowered the average score a bit on the times that the robber survived. It would often approach to within two or three moves of a target bank and then loiter for several moves until the cops happened to randomly move away far enough (or just into the right configuration) for a safe getaway to be certain.

Conclusion

At the end I was much happier with the robber than I had been after the first submission. It seemed significantly more likely to survive even against well-organized cops. I just wish that I'd been able to get it as good in time for the first submission.

The real wild-card in this round of the contest is I think in how often robbers offer bribes and how often cops accept them and how often other cops are able to detect bribed cops, accuse them, and take them over. That gives a real opportunity for not only much better cooperation between cops if several are controlled by one team, but also for that team to double or triple the score their cop earns from a game. Our robber never offers bribes so it will never come up against such better-cooperating cops. Our cop on the other hand does try to detect bribed cops and may sometimes find itself with an opportunity for a windfall.

I'm very glad that we were using Dylan for this contest. Because Dylan is nearly as fast to program in as the "scripting" languages, we had valid entries ready within eight hours of each task announcement, leaving the rest of the time for working on strategy. But because Dylan is a fast compiled language we were never under any performance pressure. The cop, in particular, had a very large amount of communications to parse and respond to and I suspect that many entries will have used a large fraction of the available five second response time just dealing with that. Both our cop and our robber always respond to the server within a small fraction of a second so we didn't even bother to write checks for getting near the end of the allowed time.

Aftermath

In summary, it seems this approach worked fairly well. The Dylan Hackers find ICFP a fun, challenging opportunity to gain more exposure for the Dylan programming language and submit some interesting sample code into the repository for the curious to examine. [8]

The Dylan hackers believe that using Dylan gave them an edge. Dylan being very expressive and lending itself to fast development allowed them to have a valid entry very early on that they could then refine. Its speed as a compiled language let them concentrate on improving their program without worrying about whether it would be fast enough to avoid being disqualified.

Special thanks go to Jes Hall for setting up the subversion server and repository the team used, setting up WebSVN so we could browse the changes, and for putting together this web page.

[1] *http://icfpc.plt-scheme.org/*
[2] *http://icfpc.plt-scheme.org/twist.html*
[3] *http://www.gwydiondylan.org/*
[4] *http://www.hoult.org/~bruce/icfp2003/*
[5] *http://www.gwydiondylan.org/icfp/icfp2001.phtml*
[6] *http://en.wikipedia.org/wiki/Minimax*
[7] *http://en.wikipedia.org/wiki/A%2A*
[8] *http://www.gwydiondylan.org/cgi-bin/viewcvs.cgi/trunk/examples/ICFP2005/trunk/src/*

Elster, Coala, Wiesel ... und das noch mit Unterschrift

von stesie <stesie@brokenpipe.de>

Ab dem 1. Januar des kommenden Jahres gibt's die Elster auch mit Signatur. Gemeint ist natürlich das inzwischen berühmt-berüchtigte Elster-Verfahren, zur Abgabe von Steueranmeldungen und -erklärungen auf elektronischem Wege.

Wie vermutlich größtenteils bekannt sein dürfte, sind Umsatzsteuervoranmeldungen sowie Lohnsteueranmeldungen bereits seit Beginn des Jahres 2005 auf elektronischem Wege an die Finanzverwaltung zu übermitteln. Die bis dato gewohnte Abgabe auf totem Baum war – zumindest abgesehen von Ausnahmegenehmigungen, wenn man keinen Computer besitzt – plötzlich nicht mehr zulässig.

Der Ruf des Verfahrens wurde auch dadurch nicht besser, daß die Übermittlung ohne jede Authentifizierung stattfand, bzw. nach wie vor so stattfindet. Ganz im Gegenteil, etliche Datenschutzbeauftragte und weitere Anhänger dieses Zirkels liefen dagegen Sturm – zuerst ohne große Resonanz.

Nach einer Weile kippte jedoch auch die Meinung der Steuerverwalter um, man bemühte sich plötzlich, eine Lösung zu finden: Die Authentifizierung sollte eingeführt werden, ElsterOnline war geboren [1] – zuerst im Rahmen einer Pilotphase seit etwa Ende September 2005. Ab dem Jahreswechsel 05/06 soll dann der Produktivbetrieb folgen.

Bis dahin räumen einige Oberfinanzdirektionen auch ein, daß man wieder das gewohnte Papierformular abgeben dürfe, wenn einem die Onlineübermittlung so gar nicht zusagt. Vorreiter war hier das Land Nordrhein-Westfalen.

[1] *https://www.elster.de/eportal/*
[2] *http://www.taxbird.de/*

Coala mit Unterschrift

Der Pilotbetreib erstreckte sich erst über die Länder Bayern, Berlin, Hessen, Nordrhein-Westfalen und Sachsen - gut so, dann durfte ich als Franke wenigstens von Anfang an dabei sein...

Um mitmischen zu können, mußte man sich erstmal anmelden, das heißt: Steuernummer, Geburtsdatum und E-Mail-Adresse hinterlassen. Daraufhin bekommt man einen Aktivierungs-Code (per Snail-Mail) und eine Aktivierungs-ID (per E-Mail).

Weiter müssen wir uns zwischen drei Möglichkeiten entscheiden, wie unser privater Schlüssel gesichert werden soll. ElsterOnline bietet uns

- Signaturkarte (... und Kartenleser; "ELSTER-Plus")
- ELSTER-Stick (das ist ein USB-Dongle mit integriertem Kryptochip; "ELSTER-Spezial")
- Software-Zertifikat (ELSTER-Basis)

Ich hab mich für die kostengünstigste Möglichkeit entscheiden – das Softwarezertifikat. Natürlich mit dem Nachteil, daß es auch am unsichersten ist – aber ich will ja eh nur testen ...

Sobald man Aktivierungs-Code und Aktivierungs-ID in Händen hält, kann's weitergehen. Erster Login. Certificate Request. Fertig.

Wir haben jetzt einen mittels PIN geschützten PKCS#12-Container, der zwei private Schlüssel und die dazugehörigen X.509-Zertifikate enthält. Jeweils ein Paar zum Verschlüsseln,

eines zum Signieren – wobei wir nur das Letztere wirklich brauchen. Verschlüsselt wird mit dem Public-Key der Clearingstelle und ansonsten symmetrisch.

Wie das Datenübermittlungsverfahren selbst funktioniert, darauf möchte ich hier nicht mehr näher eingehen. Stattdessen sei auf neko's Artikel in der DS #086 verwiesen.

Wie lautet die logische Fortsetzung aus XML, GZIP, 3DES, PKCS#7, Base64 und HTTP? Genau, es kommt PKCS#1, XML-DSig, SHA1 und RSA zum Einsatz. Naja, hätte schlimmer kommen können – es handelt sich ja um lauter zugängliche Sachen. openssl und die libxmlsec1 kümmern sich um die Details.

Soviel zur Theorie.

Die Implementierung war dann doch zum Teil non-trivialer Natur, es gab kaum Leute, die sich sonst noch mit dem Thema beschäftigen. In Kombination mit Open Source dann eigentlich keinen mehr. Schade eigentlich. Beispiele, wie das Ergebnis aussehen soll? Fehlanzeige. Fehlermeldungen? Nichts sagend. Hätte wohldokumentierter sein können – zugegeben, war ja noch der Anfang der Pilotphase, von daher will ich mal nicht weiter meckern.

Side Effect: Ich könnte jetzt digital signierte Umsatzsteuervoranmeldungen abgeben (wenn ich ein Unternehmen hätte). Jedem, der eines hat, sei geraten, das möglichst schnell zu tun. Wer nämlich einmal eine Voranmeldung mit Signatur eingereicht hat, wird bei dessen Steuernummer ein Marker gesetzt, daß keine unsignierten Anmeldungen mehr ohne Nachfrage verarbeitet werden.

Soll heißen: bis auf weiteres wird man nämlich nicht zur Signatur verpflichtet, wer also immer ohne Signatur einreicht, erfährt keinen Vorteil.

ElsterOnline will mehr werden

Jaja, ElsterOnline will noch groß und stark werden. Mehr als ein Internet-Portal zur Vergabe von PKCS#12 Containern. Gegenwärtig gibt's bereits die Möglichkeit, die Umsatzsteuervoranmeldung sowie die Lohnsteueranmeldung in ein Java-Applet zu erfassen und zu übermitteln. Hessen bietet seine Steuerkontenabfrage.

Kommen sollen noch die Lohnsteuerbescheinigungen, die sogenannte Zusammenfassende Meldung (zwecks innergemeinschaftlichem Warenverkehr), signierte Kommunikation, etc.

Der Begriff "persönliches elektronisches Finanzamt" machte schon die Runde – mal sehen, was uns noch so erwartet.

Fazit

Alles in allem ist die Umsetzung der digitalen Signatur ganz gut gelungen. Es ist zwar grundsätzlich nach wie vor möglich, Anmeldungen mit fremder Steuernummer abzugeben, nachdem das dafür vorgesehene Feld nicht mit der Steuernummer übereinstimmen muss, für die das Zertifikat ausgestellt wurde. In diesem Fall ist jedoch zumindest nachvollziehbar, wer Urheber der Transaktion war, da bekannt ist, an wen das Zertifikat ausgestellt worden ist.

Die Abgabe dahingehend zu beschränken, daß nurmehr für die eigene Steuernummer abgegeben werden kann, ist nicht zielführend – ansonsten kann der Steuerberater nichts mehr übermitteln (oder er muß Zertifikate und PIN-Codes sammeln).

Die Dokumentation ist nicht unbedingt prickelnd, aber es gibt wichtigere Baustellen.

Bei der Konzipierung wurde auf offene Verfahren gesetzt – keine proprietären Verfahren, eigene Dateiformate, etc.pp

Wer von euch also regelmäßig eine Steueranmeldung abzugeben hat, sollte sich möglichst umgehend beim ElsterOnline-Portal anmelden und zukünftig mit Signatur übermitteln.

PS: Wer das Ganze einfach selbst mal ausprobieren will, dem sei ein Blick auf die libgeier [2] empfohlen.

Leserbriefe / Farewell

An dieser Stelle übernimmt der Chaos Communication Congress die Datenschleuder. Die Redaktion entläßt euch aber nicht, ohne ein Schmankerl aus unserem Leserbriefearchiv hervorzukramen, der 21C3 bekommt Fanpost der besonderen Art. Wir freuen uns auf euch zwischen den Jahren im bcc.

Hallo, Ihr lieben Hacker!

Jetzt ist wieder Dezember, und da erinnert man sich gerne an eine nette Überraschung, die ich vor einem Jahr erlebt habe. Ich komme nach Hause, setze mich an meinen PC, schau auf meiner Website vorbei und sehe da eine häßliche Bluescreen mit dummen Parolen und eurem Vereinskürzel drauf. Außerdem ist mein Forum geplättet. Daraufhin rufe ich die Polizei an (die mir erklärt, daß sie machtlos gegen euch ist), danach überlege ich Möglichkeiten, mir den Hacker persönlich vorzuknöpfen, und zum Schluß stoße ich auf eurer Website auf einen Hinweis, daß ihr eine "Chaos-Telefonhotline" eingerichtet habt. Daraufhin ruf ich da an, und der Typ am Telefon erklärt mir, daß der Hacker, der mich besucht hat, eindeutig auf eurem Treffen sitzt (ergibt schnell ein IP-Vergleich), aber ihr erstens keine technischen Möglichkeiten habt ihn zu finden, und zweitens eh ganz liebe Jungs seid, die keine Verantwortung für die "paar Idioten, die Mist bauen wollen" (Zitat) tragt.

Daraufhin aber (und das fand ich echt nett) habt ihr dafür gesorgt, daß man von eurem Treffen aus auf meine Website (XXX.com) nicht mehr zugreifen konnte. Danach war Ruhe.

Um uns allen dieses Jahr viel Ärger zu ersparen und mir außerdem zu zeigen, daß ihr doch keine Nihilisten seid, die am liebsten alles zerstören würdet, sondern eigentlich doch ganz nett, bitte ich euch hiermit um Folgendes: Bitte sperrt dieses Jahr von eurem Treffen aus von vorneherein meine URL. Ich hab zwischen den Jahren ne Menge zu tun, muß meine Diplomarbeit fertigschreiben, und daher keine Zeit für eure Späßchen. (bzw. die von den Leuten, die auf eure Treffen kommen, aber die ihr angeblich nicht kennt und nicht orten könnt.)

Ich bitte um eine positive Rückmeldung. Nach letztem Silvester hatte ich ein halbes Jahr lang kein Forum mehr und habe gerade eben erst nem Nachwuchsinformatiker einen dreistelligen Betrag dafür gezahlt, daß er mir ein neues, hoffentlich hacksicheres bastelt. Für eine nichtkommerzielle Website, die kostenlos ist etc. und sich durch Werbung über Wasser hält, ist das ein dicker Brocken.

Gruß Markus H., Webmaster XXX.com

Haecksen

This year the Haecksen found a new home base at the congress. Their gathering place is in the Haecksen Area at the back of the Hackcenter (A08). As usual there will be a sofa, some tea and nice lights making the Haecksen Area one of the cosier places at the congress, so if you are interested in meeting other women who are into this computer stuff like you are, this is the place to be. Don't be shy if you are the owner of a y-chromosome, you are most welcome too, of course.

The Haecksen Area is more than a nice hang-out for the female hackers, however. The annual Haecksen get-together and breakfast will take place there, as well as other events, such as the networking meeting with the webgrls. So have a look at their website and look out for their signs and flyers to stay informed.

Hackcenter

9fans

Developed by the people who devised UNIX, i.e. Bell Labs, Plan 9 takes OS development back into the realm of research. While UNIX can be said to be a research tool, the OS principles remain largely the same throughout all developments. Plan 9 (the name is taken from the title of the Worst Film Ever Made, Ed Wood's Plan 9 From Outer Space) is an attempt to work on the concept of operating system from the ground up, reworking the whole idea using modern concepts and technology.

At 22C3 we will try to build a small Plan9 network to show the power of Plan9. We also try to create a meeting point for 9fans and spread the word of Plan9.

CoreWars Project

We will have some corewar experience and some tournaments in the Hackcenter of the great 22C3. Everybody is invited to join us and have some fun with CoreWars! If you don`t know what Corewar is all about check out this wikipeadia article (http://en.wikipedia.org/wiki/Corewar) or come to the Day 1 Lightning Talks where we will announce our corewars project to take place in the Hackcenter. At the Day 4 Lightning Talks we will honour the CoreWars_Project winners 2005 on 22C3.

Dance Dance Revolution

Last year there was quite a crowd at the Dance Dance Revolution (http://en.wikipedia.org/wiki/Dance_Dance_Revolution) pads which were set up spontaneously. Because it was a lot of fun and some motion between hacking and lectures surely won't do any harm, we thought: Let's do this again this year. We can be found right next to the entrance of the Hackcenter on the left.

Questions/Suggestions? Simply talk to Poldi (tristan@helmichs.de or 4553 DECT).

All these solutions share the disadvantage, that one actually has to write normal source code - most kids (and other non-programming persons) are left out. Therefore, we always have one or two windoze systems...

As far as we know there is no graphical interface running on Linux offering the possibility to just click 'n' build one's programs. So we plan to develop a Lego-Clicki-Bunti-Programming-Software (similiar to the original lego mindstorms) running on Linux.

Features:

- graphical interface to click-n-build a program using ready-made, customizable program bricks
- save program
- convert to C program for BrickOs (or similiar language)
- transmit to RCX (using infrared)

OrangeBot II

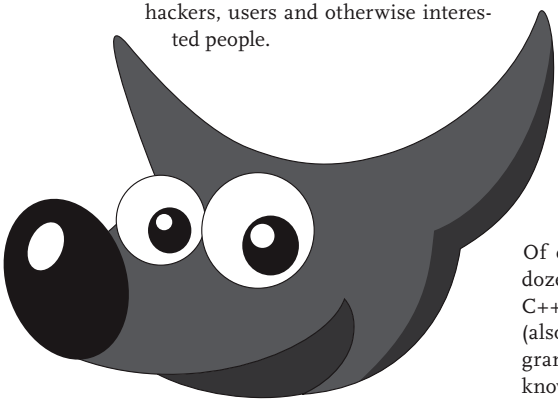
Herr Schmidt presents his newest robotic project and looks for comrade-in-arms.

Go Lounge

There will be a Go Lounge again. You will have the opportunity to sit and enjoy a nice game or two, learn the game or simply watch others play. If you don't know what Go is, you might want to read a wikipedia article first: http://en.wikipedia.org/wiki/Go_%28board_game%29. If you want to participate or have any questions, please contact Tomyum (al@koeln.ccc.de or 2101 DECT)

GIMP

The GIMP Area will be located in Art & Beauty this year. As usual, there will be some GIMP hackers, users and otherwise interested people.



We will hack GIMP, talk about it and be the contact point for all people interested in GIMP.

Come asking questions, giving suggestions or complaining :) or just hang around with us, doing GIMP things.

Lego and Mechatronics

There will be some robots to look and play with.

Lego Duplo + railway

Big bricks for small ones. A big cover (12 square meters) with lots of duplo and the duplo railway. Also perfectly suitable for big kids and - since we control the railway switches and barriers by lego-technic - even for hackers.

Homeomorphic Final Assembly

Build lego stuff without opening the plastic wrapping - a fiddly challenge for big kids with sleight of hand. One competition on each of the first three days at a given time.

Lego-CD-Burning-System

The well known and loved Lego CD burning system goes for the next round. This time we'd like to make a blueprint so others can build one, too.

Linux-Lego-Clicki-Bunti

Lego offers an operating system for the RCX (the programmable lego brick) and a windoze software to write (i.e click together) programs with a graphical interface. Suitable for kids, powerful, sufficient for most stuff and nice (also with some quirks, but hey - it's software ;)

Of course one can also program the RCX in dozens of "real" programming languages - C/C++, Java, Perl, NQC, ... , even VisualBasic (also some would doubt wether VB is a real programming language). With BrickOS (formerly known as LegOS) there is also a alternative (and of course better) operating system (which most of alternative languages use).

Projects @ 22C3

Art & Beauty

You can create art & beauty on a computer.

Art & Beauty is the central area at the ground floor of 22C3. It houses a list of interesting projects devoted to doing creative things with technology. It is also the central relaxation point at the congress. You will also find the catering facilities here along with good music day in and day out. Furthermore, you can buy congress shirts, sweaters, jackets, posters and such.

BlinkenArea

The BlinkenArea is a group of people that devote themselves to the development and operation of blinking objects. The BlinkenArea was founded at the 2nd Chaos Communication Camp, where hackers with Arcade- and Blinkenlights-reproductions teamed up. But the sphere of activity does not only include building miniature editions of the original installations. The crew is growing steadily and in the meantime more than 40 hard- and software projects have been developed.

At 22C3 there will be new projects in BlinkenArea again. The possibilities of interaction will increase with BlinkenBluetooth. BlinkenBluetooth is a project that combines Bluetooth and blinking objects. It is a joint project of Chaostal, the local CCC group in Wuppertal, and BlinkenArea. If an active bluetooth device enters the Blinkenarea, an animated Bluetooth symbol will be shown on some of the blinking objects. Additionally we are working on a feature, that will allow you to send vCards to the blinking objects via Obex Push. This text will be displayed as a ticker. It will be possible to trigger precast animations with special keywords or Bluetooth devices.

We'll provide some services this year as well. With your phone, you can play Pong, Tetris, Snake, TickTackToe or Pacman. Of course, movies may be started on demand.

The BlinkenArea streams can be requested dynamically with BlinkenSim, BlinkenSimVb, aablinkensim, UdpPlayer, ArcadeListener or BlinkenPlayerExxtreme. If you are at the congress and do not have a phone, you can come and play on one of the four phones we will set up in the BlinkenArea for public use.

Because the BlinkenArea is very service-oriented, we will provide telephone support during the congress and answer all your blinking questions around the clock. The BlinkenArea Hotline is 2023. Before and after the congress, you can use our BlinkenArea-FAQ, our mailing list and our forum. You can also email us at any time.

Like last year, the BlinkenArea is offering kits for you to build your own blinking device. AntiKippenLights-Mini, BlinkenLEDs Pro red and green and Fnordlicht are being offered this time.

If you have any questions, please contact ST st@blinkenarea.org or 2078 DECT.

http://www.blinkenarea.org/

Rings

Wireless Community Corner

The Wireless Community Corner is an international gathering space for wireless community networking at the 22C3. We are located in area C02 around the stairs.

Wau Holland Stiftung

Wau Holland Foundation takes part at the congress with a place to stand. It asks for donations exspecially for their next big project, the "Hackerarchiv", where they will concentrate the archive material of the CCC and the effects of Wau Holland as first pieces to work on them professionally and condition it for public. For the first two years they estimate about 80,000 Euro. 10,000 Euro they have for that. Thanks to the donators.

They sponsor the Congress by acceptance of the speaker's expenses and thank their generous donators for that.

And in fact they remember their friend and data philosopher Wau Holland, who founded with others the Chaos Computer Club and is the initiator of this traditional event 22C3.

Wikipedia

Like last year the Wikipedia project will be present at 22C3. This year the project plans to have a photo exhibition. This exhibition shows a collection of 24 images, which have been elected to be excellent by the Users of the German Wikipedia. The objective of this exhibition is to prove the diversity and quality of Wikipedia multimedia content. Please vote for one image of your choice. It is possible to vote anonymously, but if you disclose your name, you get the chance to win a copy of your favourite image at the Wikipedia stand.

Semapedia

Semapedia is a community-driven project that invites you to create connections between physical places and their respective virtuaö information. They create this connection by merging the physical annotation technology of Datamatrix with content from the free online encyclopedia Wikipedia.

FoeBuD

The FoeBuD is based in Bielefeld. It is an association which formed in 1987 for the Promotion of "Mobile and Immobile Public Data Traffic", as one possible translation of the name goes. FoeBuD became known for being an active member in early citizens' networks such as Zerberus, running its own BIONIC bbs, the ZaMir peace network, the German manual for the Pretty Good Privacy (PGP) encryption software and its monthly talks/events series PUBLIC DOMAIN (PD) covering topics between future and technology, science and politics, arts and culture. FoeBuD is also the organizer of the German BigBrother-Awards.

We all have to accept that there is something profoundly romantic about the hacker that fell asleep behind his/her keyboard that just isn't as romantic when applied to ever-growing groups of non-showered people in sleeping bags on air-matresses surrounded by bags and garbage on every imaginable bit of floor space at every time of the day or night. We've reached the point where it simply makes the place feel dirty, full and overused. Adding to this are some rather obvious issues with the BCC's own staff as well as with fire-inspectors.

Given the fact that the congress adds an extra day this year, chances of making it through the whole thing with only minute amounts of sleep have significantly decreased. On a more personal note, the organizers of the congress have come to realize that a healthy (or near-healthy) amount of sleep is vastly underrated in our community. Also, we would like to point out that apart from making you feel refreshed, regular showers have been known to benefit the people around you.

Bottom line: We're sorry, but everyone will need to find a place to crash in Berlin that isn't inside the BCC. Please check the wiki for affordable accomodations near the congress.

Videotaping & Taking Photographs

Filming and taking photographs is generally allowed. Visual recordings of lectures are permitted, if explicit approval has been granted by the lecturer in question. In any case, no visual recordings of the audience are permitted.

The participants of the Chaos Communication Congress insist on their right to their own images. Therefore even when events are recorded no pictures of participants may be taken unless explicit permission is granted.

Furthermore, it is considered polite to ask first if you are filming or photographing people up close. If you have a webcam or other camera that records faces in close-up or an open microphone that would record recognizable speech, then please make a sign if it is something people might otherwise miss.

Congress Etiquette

General Rules

- Be conservative in what you send and liberal in what you receive.
- Create rough consensus and running code.
- Please do not smoke inside the BCC.
- Do not, under any circumstances, operate a wireless access point.
- Even the 22C3 power system can be overloaded. Please do not connect any home appliances (like electric heaters or coffee-machines) or soldering irons in the Hackcenter unless you have spoken to the power people.
- Do not destroy anything at the BCC, we have to pay every damage.
- Do not use any sticky tape to put something on a wall. You can get some adhesive tape for your signs at the Infodesk.
- There will be no hardware labelling, nevertheless the security angels will check bags that are larger than a 15" notebook when exiting the BCC.
- The BCC insurance policy requires four active outdoor cameras (one for every door) up and running or there will be no reimbursement. The records will be automatically deleted after one week, which we will verify.

Garbarge/Waste Managment

A crowd like ours literally produces tons of waste. Garbage bags are available for free at the Infotresen. There are bigger garbage bags to be found at various places in the building, so please use them. If one is full, try the next one, or call the Infodesk at 1111 and tell them your area needs garbage collection.

Catering & Foods

The catering facilities are located in the Art & Beauty area. The food is prepared and served by ProGast. You can bring your own food to 22C3, but the rule of thumb is: Feel free to bring the cookies your grandma baked - but never order pizza (or things like that) into the BCC.

- One reason is that ProGast holds the exclusive right to sell food inside the BCC, this is standard inside locations like the BCC and this is not open for discussion - no ProGast no congress inside the BCC. While we're on the subject: please be polite to ProGast employees and interact respectfully with them; if you have complaints which cannot be resolved with them directly, please speak with Kathe (Angels will know where to find her or call 2013).
- The other reason is that last year the amount of waste from pizza boxes and other food containers was so tremendous that it made quite a mess at the congress. So this year we would like to prevent as much waste as possible. Please eat your pizza in the pizzeria!

Alcohol and other Drugs

For all drugs (incl. alcohol, Coke and Club Mate), we assume you are an adult, know your limits and that you will not bother anyone. We've never had to, but we will not hesitate to kick people out for drug-related misbehaviour, whether the drug was legal or not. We've never had any problems with this, but... In the unlikely event that you use the wrong or simply too many drugs, and the even more unlikely event that this would cause you to need first aid, our first aid volunteers would find it very helpful if you or someone else knew what and how much you actually took, and when you took it. We would like to point out that an event like the Chaos Communication Congress is probably not a good place to try any mind-altering drug for the first time.

Sleep

As many of you have noticed, the number of people sleeping at the congress has been growing exponentially over the past years. This paragraph is intended for those of you that are planning to use a staircase, hallway, an area of the hackcenter floor or any other spot inside the BCC as their hotel. We are afraid we have some bad news for you: there is to be no sleeping at the BCC this year.

In Case of Connectivity Need

NOC - Network Operation Center

The Network Operation Center, responsible for basically everything in our infrastructure that listens to a MAC Address - and that is quite a lot, including 16 GBit/s upstream and a huge amount of really expensive networking hardware. If you have any questions, feel free to ask the NOC Helpdesk in C02 or by phone (DECT: 1212).

The basic rules are simple, but nevertheless very important: Do not operate any own Wireless Lan Access Points, DHCP servers or similar applications. Never. Fair use is the basic principle. If you see anyone operation an access point, please ask him friendly to shut it off - rogue access points are causing serious problems within our network.

802.11b Wlan will be distributed on channels 1,6 and 11, 802.11a will be available, too - please try to use 802.11a if your hardware is capable to do so. We try our best to get Wlan everywhere up and running, and we have new and quite cool hardware from Aruba this year, but the bcc is not the best location for wireless stuff, so dont be too disappointed if something doesnt work.

POC - Phone Operation Center

The Phone Operation Center (POC) is the telephone exchange of the congress. Sascha Ludwig and Martin Assenmacher are responsible for the POC. The POC will provide the telephone system (Alcatel OmniPCX 4400) and some DECT handsets as well. Additionally they will bring cable bounded phones, which will be connected via the CAT5 cable system of the BCC. Everybody can bring his or her own DECT/GAP compatible phone, which will be integrated into the system. You will receive your own direct extension number.

There is a list of phones which are known to be incompatible with the POC-Network in the Eventphone-Wiki as well as phones which are known to work. Better check in advance if you have to get another phone. Please register your

DECT, analog and ISDN extensions in advance by using the GenericUserRegistrationUtility (Guru). This will speed up the registration process at the congress. All registered extensions will automatically show up in the phonebook.

The POC Help Desk can be found in C02 right next to the NOC-Helpdesk.

In Case of News

Press service

Members of the press with questions, requests for interviews or a guided tour around the congress must first inquire at Press Service. You can call Press Service at 1221.

- Location: Chaos Care Center
- Phone: 1221
- Team Leader: Maik Musall

Infodesk

If you have questions about the congress, the conference program, anything about Berlin, or about anything else to do with the congress, which is not yet covered by this booklet, come to the Infodesk near the entrance. Going there is always better, but if they have a spare moment, they will answer the phone at 1111.

- Location: Chaos Care Center
- Phone: 1111
- Team Leader: Sokrates

Editorial Office

At 22C3 we provide current information in the Weblog and Public Wiki. But we still need your help in gathering this information. If you hear something about activities at 22C3, if you want to present a project you are working at or if you want to write a review about a lecture, give the editorial office a call at 1311 or just drop by at the desk in B01.02.

- Location: Chaos Care Center
- Phone: 1311
- Team Leader: Wetterfrosch

CongressRadio

What is the "CongressRadio"? Since 19C3, the 19. Chaos Communication Congress, members of an action group called "radiokampagne.de" have been organizing a temporary radio station for the annual conventions of the Chaos Computer Club between Christmas and New Year's Eve in Berlin. From the 10th of December 2003 until the 11th of January 2004, the airwaves of Berlin rattled as young radio enthusiasts united to broadcast a new kind of radio station - "radioriff" and "radioriff away on travel". Every evening, the latter went away from the studio to another place like a bar, a club, a cinema, a workspace, an event location - and it went, of course, to the 20C3 at the Berlin Congress Center when it was the first time that the Chaos Communication Congress took place there. At 21C3 our four radio shows were broadcasted from 8-9 PM on TwenFM 104,1 MHz. We presented news, interviews with lecturers and visitors from the 21C3 and nice music.

Naturally the CongressRadio will be present at the 22C3 again - but this year we will not be broadcasting at a local radio station in Berlin, instead we will be podcasting in German and English. Thus, there will be some contributions or even complete radio shows at community radio stations in other German, Austrian and Swiss cities and of course the national news show of community radios in Germany called "ZIP-FM".

For more information have a look at our weblog, where the first podcasts already can be found. If you want to participate or have any questions, please call us at the 22C3 at our POC phone number: "1234" or contact us via our weblog contact form.

- Location: C81
- Phone: 1234
- Team Leader: Oliver

Security & Survival

In Case of Emergency

CERT

If you need the police, fire department or an ambulance, call 112 on any DECT telephone to be connected to the 22C3 emergency operator.

Photographer: Frank Stausberg

You may want to put this number in your mobile phonebook. Thanks to the Chaos Emergency Response Team (CERT) and various other volunteers, we have very competent and well-trained fire-responders and first-aid people on the field. The 22C3 emergency operator will also take care of notifying the normal German emergency services as well.

If you or anyone else calls the outside emergency operator directly, make very sure the organization knows about it (have someone run to the CERT or the office!), so we know we have incoming emergency services and we know where they need to go.

For situations that aren't true emergencies, visit the Chaos Emergency Response Team (CERT) in room B04 or call them on the internal extension 112. They are quite likely to be able to help you themselves and if not, they can help you get to a doctor, hospital emergency room, mental health crisis center, optician, veterinarian, dentist or pharmacy.

Network Abuse Phone

The network abuse hotline can be reached at 1114. This number is staffed 24 hours a day and is primarily for outside entities complaining about incidents originating from our IP-range. Please call this number only when you think some situation warrants attention from the network security crew. For other needs of the network crew, you can call the NOC helpdesk at 1212.

Chaos Care Center

The Chaos Care Center will be found at the larger information desk known from previous years. Inside the cubicle not far away from the entrance, you'll find a competent team with answers to your questions about the congress, Berlin and quite everything else.

This year we've merged several previously independent groups into the Chaos Care Center. These are the Infodesk, which you will notice at first, the back office, which is our investigational counterpart for the Infodesk as well as the secretaries for coffee, the editorial office for producing news on the Weblog and Wiki, the so-called Vereinstisch for becoming a CCC member or correcting the CCC office's database entries and last but not least, press service where the press can ask questions or receive a guided tour of the congress.

Smoking Policy

One of the biggest complaints about the last congress was the unacceptable air quality due to smoke within the building. There are good reasons to completely forbid smoking inside the BCC, but since the congress takes place during winter, it would be really mean to force all smokers to smoke outside the building. This is why we decided to start a "social experiment": We kindly ask everyone not to smoke in the building. If you really have to smoke, do so, but please keep in mind that if we cannot keep the smoke to a level where the ventilators will be able to deal with it, we will be forced to forbid smoking completely next year. Smoking in the hackcenter and A&B is forbidden, like last year.

Lockpicking

The German lockpicking championship will no longer take place at the congress, but there will still be some workshops.

Hackcenter

This year the back part (A08) of the Hackcenter will be the area for the Haecksen, Phenoelit, the BSD-Community and the Workshop Area. About half of the front part of the Hackcenter is a lounge, the other part is reserved in advance, as usual - please try to be fair and don't occupy those seats.

Software goodies

There will be a backchannel system this year to accompany the lectures, and the lecture reminder is up and running again, and supports notification via mail this time as well.

Changelog

Conference

Last years congress yielded many complaints, too many interesting things were going on simultaneously, too many talks were missed due to people oversleeping and too many people were squeezed into small, overcrowded lecture halls. So this year we something different, for a change.

The most obvious change is a fourth day, allowing even more interesting talks to be held. There you go: listen to more of them without the need of time travel or astral projections.

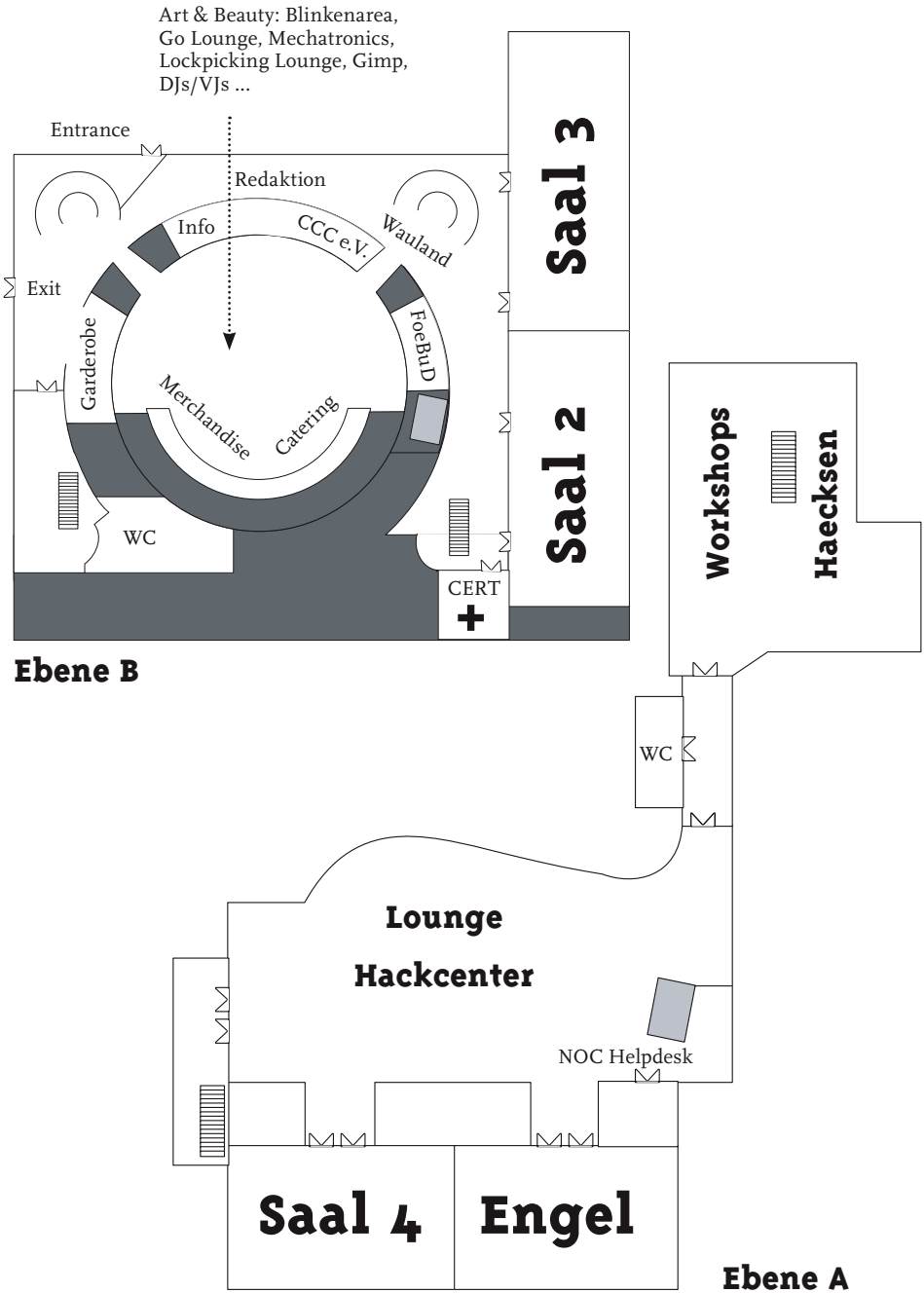
We reconsidered our schedule, as well: conference program starts at noon and ends at midnight, thus leaving one more hour to sleep, so **everyone** can be brighter than ever. An additional break in the conference program (making it two) allows catching some fresh air, eating something outside the conference venue. You might even find yourself chatting with someone or finishing your hacking project without anxiety of missing anything interesting during the conference.

We also decided to restucture most of our conference rooms, only Saal 1 remains the same as it was last year. The three lecture rooms on entrance level have been merged into two bigger conference rooms, now known as Saal 2 and Saal 3. Saal 4 will be in the basement, in the areas known last year as the Workshop rooms and the Haecksen rooms. Only four of the six rooms will remain, but most of them significantly larger than last year. We hope this will solve most of the problems related to overcrowded lecture halls, such as lack of oxygen, large clusters of people in front of doors and as a result, an unhappy Chaos Emergency Response Team.

Workshops

Unlike the previous years there will not be a workshop room with a pre-planned lecture program. Instead, we offer a table under the skylight of room A08 at the end of the Hackcenter. At this table, about 23 people will be able to sit down and there will be no digital projector. You can reserve some time for your workshop to be held at the Workshop Area in the Public Wiki.

Photographer: Thomas Gutzmer


Art & Beauty: Blinkenarea,
Go Lounge, Mechatronics,
Lockpicking Lounge, Gimp,
DJs/VJs ...
Entrance
Redaktion
Info
CCC e.V.
Wauland
Exit
FoeBuD
Garderobe
Merchandise
Catering
WC
CERT
Saal 3
Saal 2
Workshops
Haecksen
Ebene B
WC
Lounge
Hackcenter
NOC Helpdesk
Saal 4
Engel
Ebene A

Welcome to 22C3

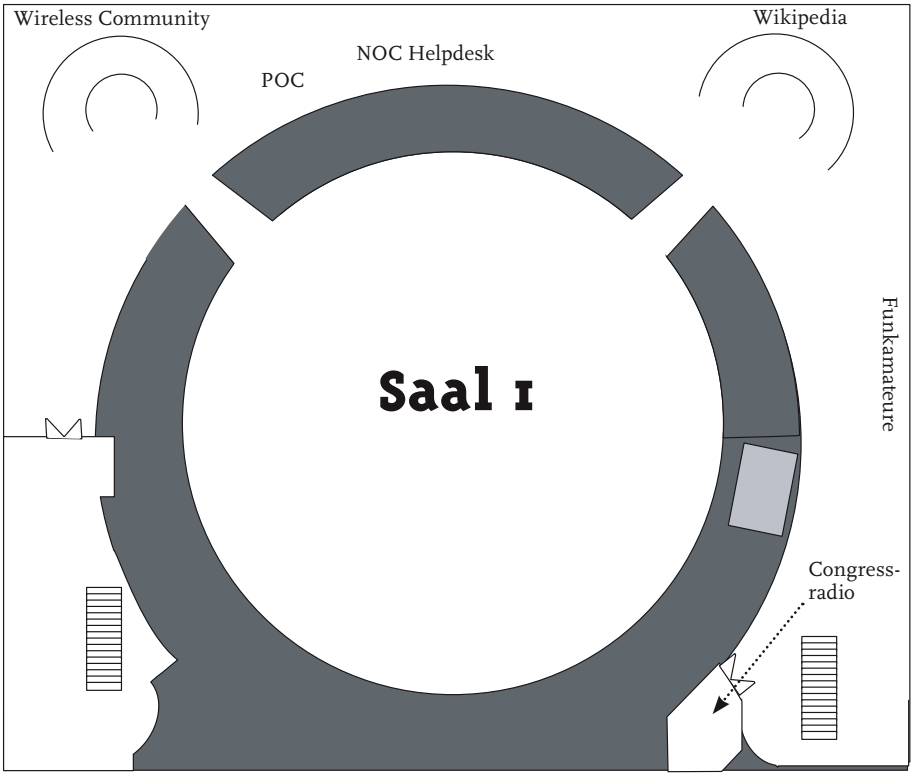
Welcome! Wow! We're glad you made it here! We hope you make yourself at home and that we'll all have an event to remember. This guide contains some information about the 22C3. Please read it even if some things are familiar because you've already read the weblog or kept yourself up-to-date using the website and wiki.

Important web pages:

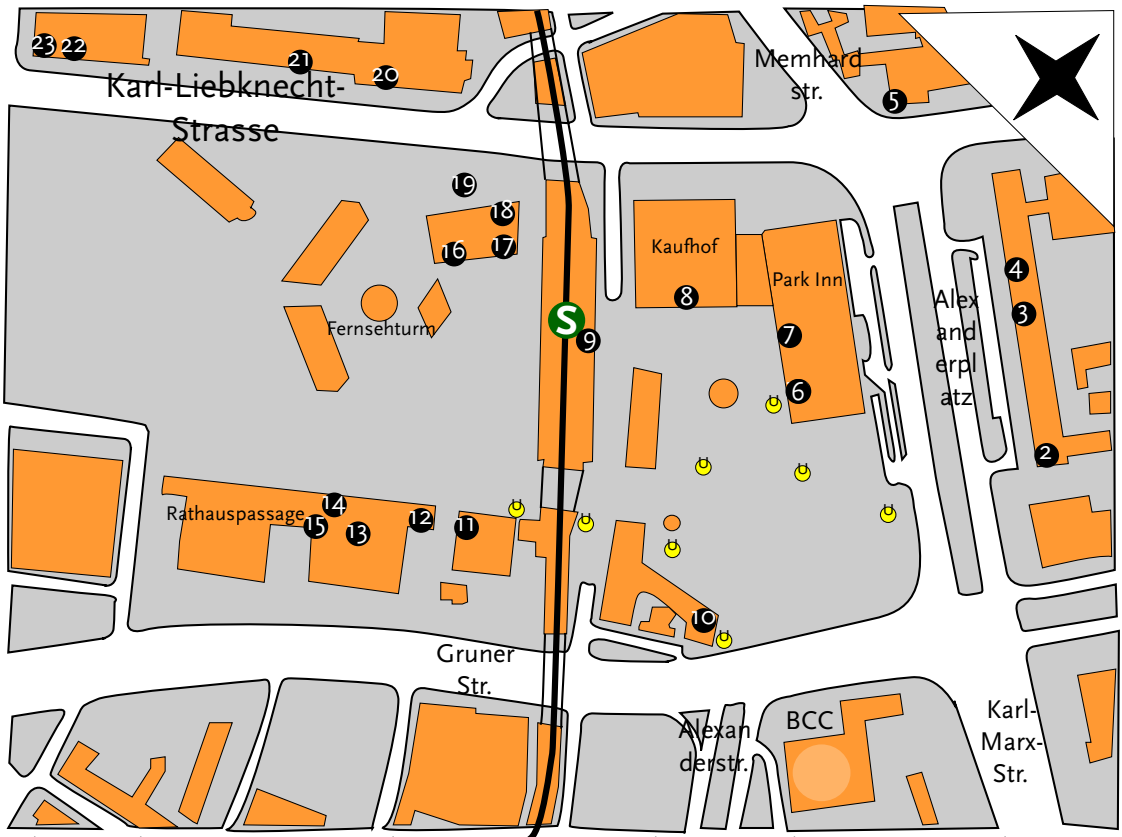
Weblog http://events.ccc.de/
Website http://events.ccc.de/congress/2005/
Wiki https://events.ccc.de/congress/2005/wiki/
Lecture Reminder http://22c3.fholzhauer.de/

Phone numbers:

Chaos Emergency Response Team (CERT) 112, 911
Info Point
Speakers Info Point
Network Operation Center (NOC) Help Desk 1212
Phone Operation Center (POC) 2000
Angel of Death - "He solves problems." 113
Kathe - "She solves problems with ProGast." 2013
Congressradio.de 1234



Ebene C



1) bcc 2) Deutsche Bank 3) K&M Elektronik 4) Pizza 5) Grill House 6) Saturn
7) Burger King 8) Kaufhof 9) Bahnhof Alexanderplatz (several shops + restaurants)
10) Sparkasse 11) Dubinsky 12) Dunkin Donuts 13) Postbank 14) Apotheke / Pharmacy
15) China Imbiss 16) Subway 17) Commerzbank 18) Apotheke / Pharmacy
19) Döner,Pizza,Pasta 20) McDonalds 21) Döner Imbiss 22) Steakhouse 23) Nordsee

der congressguide

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

Der definitive Guide zum 22c3
Kongressfahrplan
Raum- und Umgebungskarten
Gimmick: Die Datenschleuder

Foto von Sven Hiersemann, hiesve at web dot de

ISSN 0930-1054 • 2005
Sonderpreis von nur €2,50, Datenschleuder gibt es gratis dazu
Postvertriebsstück C11301F

#89