HACK THIS ZINE

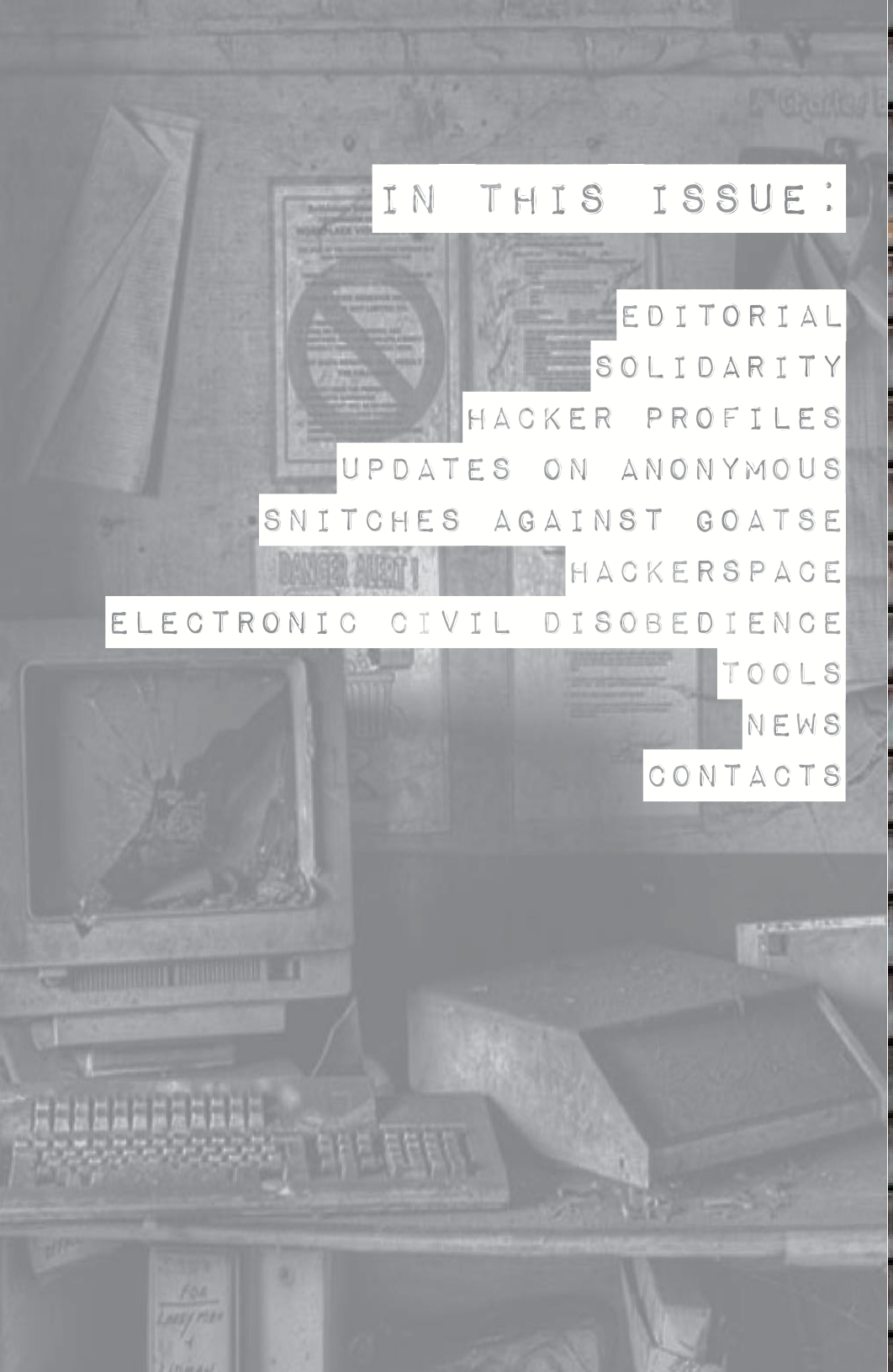
v.12 spring 2011

brought to you by hackbloc

EXPLOIT CODE NOT PEOPLE

HACK THIS ZINE

V.12 SPRING 2011



IN THIS ISSUE:

CONTACTS

2. You will receive mad props from your hacking/anarchy friends

3. You will gain instant respect from many sectors of society resulting in improved happiness and financial well-being which we all know go together.

4. You will be "leet"

5. Next time your friends make fun of you for sitting around and doing nothing all day, you can show them a copy of the zine and make them feel stupid.

6. You will be filled with that warm fuzzy feeling you get when you occasionally get off your lazy ass and do something productive.

7. You will likely be mentioned in an FBI file which is something you can show your future kids to convince them that you used to be cool.

8. You'll help introduce radical ideas to hackers around the world.

9. You'll help combat the trends of technical illiteracy and technophobia in radical circles that leads to unsafe, nonstrategic use of technology.

10. This is the secret reason which you hide from the world because of how embarrassed you are about it. We don't know what it is, but we know it's horrible and shameful so please keep it to yourself.

[CONTACTS]

To contact the HackThisZine, send an email to staff{at}hackbloc.org with HTZ in the subject line. For submissions and letters, we will assume you want them attributed to your email/name. If you prefer to have the anonymity, just let us know. Our PGP key is available on most major keyservers and linked to from hackbloc.org. We love letters and often get lonely.

Want to get involved in making the next issue of the zine? We need people to design sick graphics, do printing and distro for us, find people to submit articles, etc. Send an email to hackthiszine-subscribe@lists.hackbloc.org to subscribe to our mailing list.

We are always interested in receiving your articles, HOWTOs, theory, graphics, and reportbacks on hacking, hacktivism, anarchism, social struggle, and how they intersect. We will take submissions in most any format but prefer plain-text emails. Wonder if your article is suitable for our zine? Ask us!

Top 10 reasons to submit an article to HTZ:

1. You will receive a free subscription to the print version of the zine assuming you give us your mailing address. This subscription lasts about a year and will only be canceled when the HTZ crew has enough turnover to forget about you.

REPORTING FROM SOMEWHERE BEYOND THE ELECTRONIC FRONTIER

APRIL, 2011

The dead trees your eyes are trying to grep right now (or the PDF if you got it online) comprise issue 12 of the longest-running hacktivist zine in the world. We started publishing in 2004 so we've been doing this for almost a decade. This is no small feat given the dozens and dozens of people this project has burned through, the multiple servers and groups that have hosted us, and the literally tens of thousands of copies we have given out in real life. We've probably given out hundreds of thousands of electronic copies. This is no small feat given how few activist groups and projects last this long and it has been an uphill battle for us but we are still here. The FBI, internal disputes, political indifference, and public apathy all joined forced to stop the distribution of this material and have ultimately failed. In these times, it seems more important than ever to make sure this zine continues.

We seek to bring radical political analysis and discourse to the hacking community, to bring hacking skills to radical communities, and serve as a clearinghouse for information about hacktivist theory. We want to provide examples of real, tangible methods of hacktivism that can be easily exported anywhere and theory on how to build those methods.

In the past six months, we have seen some of the most intense and inspiring hacktivist actions that many of us have seen our entire lives. We have watched Anonymous transform from a anti-scientology griefer group to a large movement with clear analysis, political goals, articulate actions, and a bite that sinks deeper than some underground militant groups. In the past few years, we have seen governments toppled and many times it felt as if worldwide insurrection was only a domino away. We have seen Wikileaks go through its trials and fend off attacks from some of the strongest adversaries in the world. Their political vision continues to unfold for the careful observer as they hang world leaders out to dry with nothing else to do aside from beat their red faces against their freshly polished desks.

Every day the pillars holding up the institutions of power show new cracks to us and the excitement we all feel is like the first time you kissed

somebody you genuinely cared about. Maybe, just maybe, things really can be radically different on this planet. For many of us, the waiting had become unbearable and we blossomed into something beyond ourselves. All the while, those in power become more and more fearful of the coming times. Their efforts to repress and co-opt are draining them and their agendas become clearer as they lose their element of secrecy. More time is put into immediate needs instead of focusing on long-term strategies for placating the population. Some things slip their minds as they fail to keep up appearances. A missing pendant here, inconsistent press conference statements there. They continue weaving the tapestry of social control while the other end remains neglected and begins to fray. As the winds start to ruffle at the edges of their tattered clothing, they feel naked and vulnerable. Now it is our time to strike.

Hackers, this is our time. This is our time to cast aside our fears, to say "fuck what will happen to me, this needs to be done", to fight like you have never fought before and back your friends like nobody except for themselves could. No more letter writing, no more hitting the facebook like button next to Wikileaks, no more sign-holding every week. It's time to get serious and time to get strategic. What the fuck are you doing while this is all going on around you? Put this zine down right now and figure that shit out. If it makes sense to do so, pick it up afterwards and devour its contents.

We will not know until the day of the insurrection that it is happening. Let's live our lives like it's just around the corner while we build infrastructure for the long haul. Welcome to the infinite general strike, let's get to work.

--ZINE UPDATES--

Every issue we change the design of our zine and work on implementing new ideas. Last time we tried having consistent sections (tools, actions, news, and legal/solidarity) and this seems to be something people enjoy. This time we focused on not "re-posting" news articles. Some events (particularly the actions of Anonymous) have gotten significant coverage in the mainstream, alternative, and hacktivist media. You probably already know how to access this information so we won't bother you with yet another page of something you already have. We're working on reporting more on under-reported stories/struggles and focusing more on original content and analysis instead of spending all of our time tracking news stories. We also heard from multiple people that issue 11 was way too long and this was only further compounded by regurgitating stories about Wikileaks and Anonymous. We do want to report on these stories but we want original reporting (such as an article posing a feminist perspective

Thank yous:

Thanks to everyone who helps keep our bits flowing securely and to everyone who helped work on this issue of the zine: Discordia, Anonymous, The Pirate Bay, 2600, the Bay Area Anarchist Bookfair, The Portland Anarchist Bookfair, Bradley Manning, the Wikileaks Crew, alxciada, anders, flatline, evoltech, sally, sexy hexy, frenzy, AnarchistNews.org (good work with the /ban trolls), postmodern modulus III, RiseUp.net, Truecrypt, The Tor Project, March-Hare Collective and everyone else who we forgot that is working to protect and support the struggle. Thanks to all of those resisting police violence in their communities, all those facing state oppression, and those engaged in the struggle everywhere.

Thank You!

Questions? Comments? Article Submissions? Get a hold of us at: email: staff [at] hackbloc [dot] org

Get Copies Of The Zine: Electronic copies of the zine are available for free online at the hackbloc website: https://hackbloc.org/zine

There are two versions of the zine: a full color graphic PDF version which is best for printing and one which is best for reading on a computer screen. If you are printing the zine on a printer with a duplexer (one that prints double-sided) such as one which you might find at your shitty corporate job, you need to flip the zine on the "short side". You can probably find this in the "advanced", "printer properties", or other menus you have the option to visit when printing the PDF. 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) then you can order copies of this issue and all back issues online from Microcosm Publishing (microcosmpublishing.com) who are based out of Portland. If you are at the Bay Area or the NYC Anarchist Bookfairs this year in you will be able to find us tableing.

We are seeking translators to translate Hack This Zine into other languages, if you are interested send an email.

NEWS

ARE YOU READING THIS ZINE?

Do you do other things in your life, like work on other radical/anarchist projects? Do those projects or others you know of need tech help to make them more effective?

Do you have some cool tech project that has implications for radicals or hackers?

Are you part of a tech collective that offers services to the wider community?

We're opening a free "classifieds" section in the next issue. Send a short description (maybe a few lines) and if it's related to the above questions, we'll put it in the zine. We'll run the ad for one issue and keep running it if you keep sending it in or we feel particularly fond of the project. Be sure to say how people can contact you and specifically what kind of help you need (if any).

VOTE FOR HACKTHISZINE!

Help budding hackers and potential hacktivists find out about our zine and stop them from getting dragged into the sketchy blackhat scene.

Vote for us at progenic:

http://www.progenic.com/vote/?id=sickreizins
http://tinyurl.com/5wlmzuc

on Wikileaks).

People have asked that we make a PDF that is more friendly towards e-readers. We don't have the time for this right now, but if somebody wants to do this they are certainly encouraged to do so. Let us know so we can link to it.

In the next issue, we will be adding a "free classifieds" section. If you are part of a radical project that needs tech help or part of a hacker project that has radical implications that needs others to get involved, submit a short description of the project to staff{at}hackbloc.org. You'd better jump on that shit though, as it's probably going to fill up real quick.

--SHAMELESS PLUG--

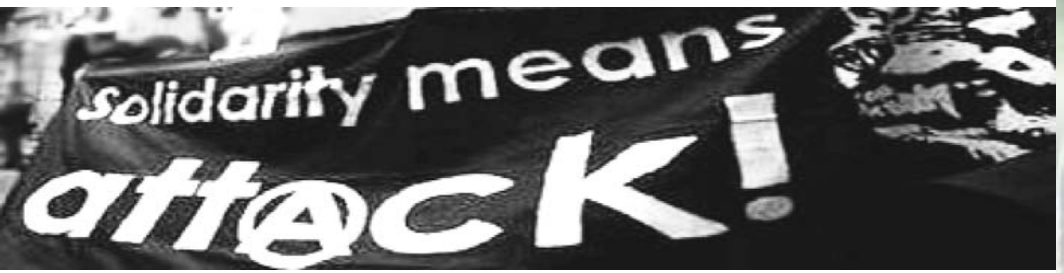
As a final note, it would be great if our readers could give us a quick vote on progenic.com. This helps us find budding hackers to read our zine and helps divert them away from all those sketchy blackhat sites that are more interested in Yahoo pwnbots and taking advantage of a hacker's desire to learn by filling up their machine with viruses.

http://www.progenic.com/vote/?id=sickreizins http://tinyurl.com/5wlmzuc

--GET IN TOUCH--

As always, feedback, articles, and letters should go to staff{at}hackbloc.org. The PGP key is available from the hackbloc.org main page. Authors/senders are not anonymous unless they request it.

This zine is provided to you for informational purposes only. If you decide to do anything illegal with the information contained in this zine, you do so at your own peril. We do not encourage such activity.



If you have been following the Bradley Manning case at all, you are probably already familiar with the sort of torture he has been receiving in military prison including being forced to strip naked for hours at a time and being put in solitary confinement. He has been charged with crimes that may very well result in his execution. Regardless of his treatment in prison, we stand with him unconditionally for his alleged leaking of information which showed gross misconduct by the US Government and governments worldwide.

Prison is a lonely and alienating place, and it can mean everything in the world to a prisoner to receive a letter from someone giving them support and love. Every letter Bradley Manning gets will help him through his darkest hour. Letters will be opened, "contraband" discarded and then mailed weekly to Bradley via someone on his approved correspondence list via Courage to Resist, a non profit organization that helps soldiers who are dissenting against the military. You can write to Bradley Manning at:

Bradley Manning
c/o Courage to Resist
484 Lake Park Ave #41
Oakland CA 94610
USA

If this is your first time writing to a prisoner, (or even if its not) please read this guide [guide] to writing to prisoners. For more information about Bradley's case, go to bradleymanning.org. Solidarity means attack!

http://www.anti-politics.net/distro/download/writing-prisonersflyer.pdf http://tinyurl.com/69jxj5z

NEWS

- Cut the wire so that it is at least one foot longer than twice the size of the rails.

- Knock the train rocks from underneath two adjacent spots on the track to feed the wire underneath the rail.
(I used a hammer and strong thin metal piece like rebar to knock the rocks out.)

- Loop the wire over the tracks and tie off the wire with itself, making a continuous loop.

- Press the wires firmly against the rails to get the most points of contact.

May resistance to capitalism and its state goons grow uncontrollable!

Solidarity with those on the streets combating state violence every day and on March 15th, the International Day Against Police Brutality.

Solidarity with the Montreal Anarchists facing repression!

NEWS

TRAIN SAFETY SYSTEM USED AGAINST ITSELF

from the communique posted on Anarchist-News.org:

Police brutality and targeted violence against poor people are standard operating procedures. Police violence is not pointless. The essential function of this violence is to protect capital. In February the Police shot dead a native man accused of stealing two lemons. Several other young men of color have died by police firing squads in Toronto in 2010.

When the police unleashed their violent campaign to siege the City of Toronto for the G20. I launched a campaign of my own. I have copper-wired 5 major train lines to simulate the presence of a train on the tracks. this obstruction can take hours to find and clear, while the major train track delays can cost millions of dollars a minute. The rail lines are an important trade route for the economy and extremely vulnerable to sabotage.

What I did

- Use a fairly thick but pliable gauge of copper-wire. (Found at hardware stores.)

HACKER PROFILES

INTERVIEW WITH ENIGMAX OF TORRENTFREAK.COM

1. Can you give a brief description of how you both got involved in pirate journalism (is that the correct term?) and TorrentFreak?

Ernesto founded TorrentFreak nearly five years ago (our birthday comes up next month) and I joined in 2007. Both of us have a keen interest in sharing technologies and believe that file-sharing will revolutionize the way we enjoy media. It is fascinating to see how, in just a few years, millions of people have constructed the largest online media library on the planet. The popularity of illegal file-sharing in particular shows that people have a need to access information whenever they want, wherever they want and it's part of our job to document this movement. We both have full-time jobs but spend as much time as we can writing for TorrentFreak.

2. What do you see the purpose of sites like TorrentFreak in the anti-copyright movement?

The whole copyright / anti-copyright debate is so polarized. There are extremists on both sides and that probably doesn't help much in reaching some sort of compromise, some middle ground where consumers are well-served and companies are happy with their return on investment. That said, we don't have much respect for companies that (ab)use ever more restrictive copyright laws to bully the little guy. Take the "pay up or else schemes" currently spreading like a virus in the UK, US and beyond, we certainly have an educational role to play there.

3. Would you describe yourself as hacktivists? Why/why not?

It's our place to report on the many elements of the file-sharing world and reporting on the work of hacktivists is very often an important part of that. Some of the most fascinating and exciting stories we've ever written on TorrentFreak have come from the work of hacktivists. Countless website defacements of the big anti-piracy organizations aside, it could be argued that companies such as MediaDefender would be free to carry on their work had they not been exposed by hacktivists.

Just recently we have seen the multiple Anonymous DDoS attacks on various pro-copyright and anti-piracy targets and of course that has given us quite a lot to keep up with. However, when those attacks lead to information leaks such as those experienced by UK law firm ACS:Law, things really step up a gear. We learned a huge amount from those email leaks, as we did from those from MediaDefender, so I guess our part in that hacktivism is to spread that knowledge to our readers.

4. How about pirates? (in reference to above question)

Pirates? Us? Of course not.

5. How would you describe pirates politically? Do you think piracy is inherently political? Anti-authoritarian?

Just recently I was having an informal chat with a rather nice guy from one of the big studios (surprise, they're not all blood-sucking vampires intent on destruction!) and he asked a similar question. There are dozens of reasons why people share files and it's my opinion, having been around this scene for more than 20 years in one form or another, that the majority don't have a political, moral or other agenda.

There are some, and you will read their opinions loud and clear in the comment section of TorrentFreak and many other online forums, that do want to destroy the entertainment companies for being 'evil', but in my opinion most just want media quickly, easily, without ridiculous DRM and if possible at a more reasonable price - it just so happens that on P2P networks that price is 'free'.

For a significant number of others, file-sharing is a sport, and a very entertaining one too.

6. What do you think is the next step or BitTorrent? DHT is a great tool but it's not perfect yet and good distributed search seems a while away. Is the next step a completely different way of distributing information?

Less dependence on centralized servers and distributed search is certainly the future, and it is already operational in clients such as Tribler. However, before people will switch over I think the current system has to fall apart, or the most used clients have to implement distributed search. I don't see this happening in the near future. In recent years, the old model of information sharing through file-hosters has become increasingly popular, this trend might continue for a few years.

NEWS

If you want me to stop then you should just kill me because i cannot live without programming, HV and Linux kernel hacking You know who am i and where i live, so come and get me !!!" [sourcel]

He is asking for funds in his legal battle against Sony. Check out his site at http://grafchokolo.com/ for donation instructions. He's currently taking PayPal at the moment.

Those who are getting involved in copwatching can take note of this story and the Wikileaks "insurance file" as a way to insure the cops don't get too excited about beating up observers.

Fuck Sony!

[kernel] http://psgroove.com/content.php?773-Graf_Chokolo-Releases-PS3-Linux-Kernel-2.6-Full-Access-to-Ram http://tinyurl.com/4b5yzen
[sourcel] http://www.ps3-hacks.com/2011/02/25/graf-gets-extorted/ http://tinyurl.com/4j99g2h
Verizon will refund between $30 and $90 million to customers for "mystery fees" charged to their wireless accounts. If you got a charge for data use on your cell phone bill that you didn't actually incur, you should have gotten a refund in Oct/Nov of this year. If you didn't get your refund, call Verizon and give them a piece of your mind.

http://www.theregister.co.uk/2010/10/04/verizon_payback/

NEWS

SONY HACKER KNOWS HOW TO DEAL WITH COPS

Graf_chokolo is an avid hacker who contributed countless tools to the PS3 console hacking scene including a Linux kernel [kernel] built for the device. He recently angered Sony by releasing the PS3 master key. With the key, anybody can effectively break Sony's copyright protection allowing them to play anything from pirated games to homebrews to backups of games they acquired legitimately. Sony sued him and got an injunction order against him which prohibited further research into the device. In response, Graf threatened to release the "hypervisor bible" which contains all the knowledge he has about the most secret functions of the PS3 if he was pushed too hard. He stayed good on his promise and released it immediately after his house was raided and he had all his equipment seized.

In an epic defying blog post, he said:
"The SONY's laywer asked me why i'm doing what i'm doing, because of my hatred for SONY ? He cannot understand why i'm doing it, because he is paid for what he does. I'm not. I don't hold a grudge against SONY even now Hatred clouds your mind, keeps you from more important things. I have a better use for my mind and knowledge

So, SONY you failed again, you took my equipment but my mind is still free and you canot control it. You failed again. They are just tools, i can get new ones and will continue my HV reversing and bringing back PS3 Linux which you took from us.

7. A lot of people don't care about anti-piracy law/enforcement. It's illegal anyways, who cares if it's more illegal? Why should pirates and anti-copyright advocates care about the law and the legislative process? Should they? If so, why and if not, why not?

Anyone who could be subjected to a law and punished under it should be aware of where the guidelines are. The lawyers involved in anti-piracy enforcement treat the whole thing as a game, albeit a very serious one. People should take them seriously and learn the rules of the games they play. Others, with more resources and motivation, will join various groups and organizations in an attempt to get those rules changed. This is essential to counter the activities of those lobbying for even more restrictive copyright.

Having said that, pirates know only too well that the odds are stacked massively in their favor. There are millions of file-sharers in the United States alone and although it's possible to be thrown in jail or sued into oblivion there just for sharing files, that happens only to a handful of people. Legislation and punishment is not and never will be the answer to the file-sharing 'problem'.

8. Anti-copyright and piracy are both cultures of resistance. One problem we see in many cultures of resistance, especially electronic ones, is the rampant amount of snitching that goes on. This snitching destroys these communities. How should we respond to people informing on each other?

This is a very hard question to answer. No one likes a traitor but this is a knife that can cut in several directions. Speaking of torrent sites for a moment, there are always disgruntled individuals ready to rat someone out for the most trivial of reasons. Online 'friendships' and associations can easily go bad and, after all, leaking information to spite someone is just a moment of rage and a contact form or email away. At the moment we are seeing attempts by alleged scene members to damage certain torrent sites by leaking information about their owners and staff, so the pain doesn't always have to come from anti-piracy companies.

Also, and this is important, snitching is a two way street. There are plenty of 'traitors' inside Hollywood and the music industries too - where would file-sharing sites be without them? Perhaps a little more empty than they are now.....

FBI MAKES BIG MEDIA SPLASH WHILE ATTEMPTING TO PROSECUTE ANONYMOUS

News outlets are reporting [danews] that the FBI has executed 40 search warrants in an attempt to prosecute those who participated in acts of Electronic Civil Disobedience against banks, online payment processors, and other sites which (possibly illegally) colluded to deny services to Wikileaks. While we have not been able to obtain copies of all the warrants, one warrant was posted to Cryptome [cryptome]which details a raid on a dorm room at Georgia Tech. The case is still under seal.

The warrant tells FBI agents to look for a number of items including "records of denial of service attacks including, but not limited to, attacks against RIAA, MPAA, US Copyright Office, Aiplex Software, Paypal, MasterCard, Visa, and Bank of America", "records related to the Low Orbit Ion Cannon (LOIC) tool and other tools which can be used to launch a DDoS attack", "records related to internet relay chat (IRC), including software clients, applications, logged communications, channels visited, and channels managed", "records related to the group known as ANONYMOUS", "records related to software piracy and websites and groups that support or facilitate software piracy", and a number of electronics.

In particular, when searching computers, they looked for "evidence of counter-forensics programs (and associated data) that are used to eliminate data from the computer" and evidence that the computer could have been controlled by somebody aside from the owner (via a trojan or other tool), or evidence that such an infection did not exist.

In this raid in particular, they appeared to target somebody who they believed to be using the moniker INTERNETS, TICKL, or TICKLE.

This is most likely the tip of this iceberg for these raids and it's possible that prominent hackers in the community will be targeted as part of this fishing expedition. This is a good time to remind folks of the pamphlet published by the Center for Constitutional Rights entitled "If an agent knocks" [agent] that details what rights you have, under what situations agents can enter your residence, and other legal information which will come in very handy if you of your friends are targeted.

EXAMPLES

These examples are only that. The zine is not suggesting that anyone attempt such things.

- Employees organizing a strike need to know what their boss is planning to do in order to break it. They intercept his emails to upper management which details his/her plans.
- An activist group attempting to gather intelligence on corporation x puts a bug in their corporate network and sniffs hundreds of gigs of sensitive internal information. Some of it is used internally for their campaign to predict the moves of the target corporation, some of it is strategically leaked to sow distrust among the people who call shots at the corporation, and some of it is leaked to damage the PR image of the corporation.
- A revolutionary group breaks into the office of the local police precinct and gets a huge dump of their communications. They analyze it and distribute parts of it to other like-minded groups in the form of strategic intelligence bulletins. As a result, the cops lose the upper-hand in attempts to neutralize and disrupt resistance efforts in the area.
- State law enforcement in coordination with their local fusion center install a tap like this on the internet connection of the local infoshop. Because the people who use the internet at this infoshop don't follow good surveillance self-defense practices, the information gathered from this tap is used to build maps of those involved in resistance and predict the roles they will play at upcoming actions. The resistance loses the element of surprise and all get rounded up in a mass arrest.

All of these would require physical access to the target network, a device to intercept the data, and a method for transferring the data to a secure location. The device could be a netbook installed in a storage closet, above the ceiling tiles, or some other neglected area with access to electrical outlets or wires. The network sniffer dumps the network data to the disk which is then uploaded to the owners of the machine perhaps through a separate wireless network to avoid detection. With the increased sophistication of today's portable devices (iPhones, Androids, etc), this could easily be accomplished with them.

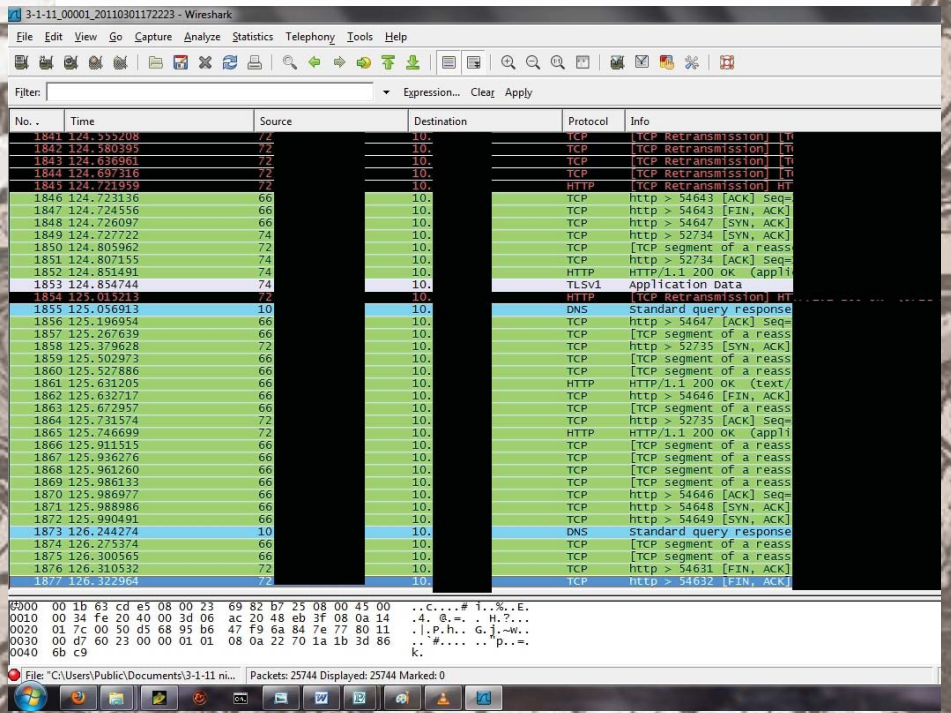
Thanks to Legotux for helping me figure this out. Check out this website for another variation on the same http://hackaday.com/2008/09/14/passive-networking-tap/

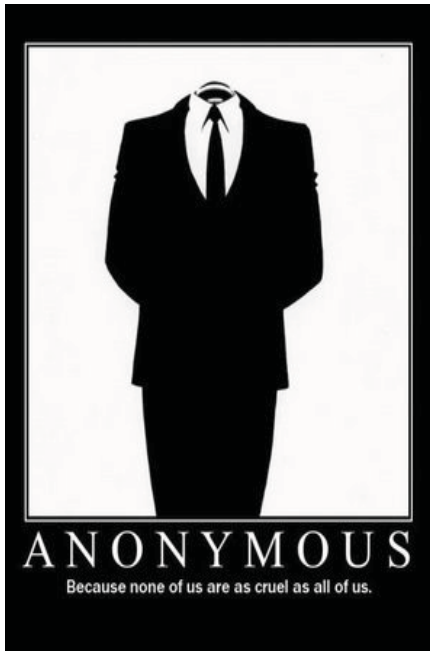
[shark] http://www.wireshark.org

The top router is the LAN router and the bottom is the WIFI router. The black CAT5 goes to the modem. The white CAT 5 goes from port 1 of the LAN router into the WAN port of the WIFI router. The TAP is connected to the laptop so that the sniffer software views transmission data.

SNIFFING WITH A TAP

I used Wireshark (free software), but there are other programs out there. I was able to view packets coming from the internal network traffic (Destination column in the picture below) and going to an external source (source column in the picture below). My interest was in seeing which ports people were opening to the outside world. With Wireshark, you can then add various filters to view specific information, such as only TCP traffic. Clicking on a specific frame can show the MAC address of the computer that is being sniffed. All sorts of fun can be had like blocking out the computer from the network, etc.





As of this time, the FBI has made no arrests in conjunction with this investigation. They are in the information gathering stage of the investigation and will likely be approaching people and asking them to provide them with evidence which they will in turn use to prosecute members of our community. Everybody hates a snitch and nobody is under any obligation to speak to them if they are approached. Here's a useful useful flyer [flyer] on why we shouldn't ever talk to the FBI.

We should be preparing prisoner support and legal support for those who are targeted in these raids and accused of participating in the heroic actions undertaken by anonymous. This means keeping track of who is getting served with what documents, where searches are happening, who is being charged with what, and what they need to fight those charges. So, hackers, who is going to take up this important task?

[agent] http://ccrjustice.org/ifanagentknocks
[danews] http://www.wired.com/threatlevel/2011/01/fbi-anonymous/
http://tinyurl.com/65u5aqu
[cryptome] http://cryptome.org/0003/fbi-search-zc.zip
http://tinyurl.com/5wymkkc
[flyer] http://www.crimethinc.com/tools/downloads/pdfs/dont_talk_to.pdf
http://tinyurl.com/66yxv4s

Related links:
They Can't Raid Us All: https://ghostofvanzetti.wordpress.com/2011/02/03/they-cant-raid-all-of-us-an-explanation-on-how-and-why-to-resist-grand-juries/
http://tinyurl.com/6abckpo

Court Documents in Case Against Goatse Hackers Reveal Unknown Snitches

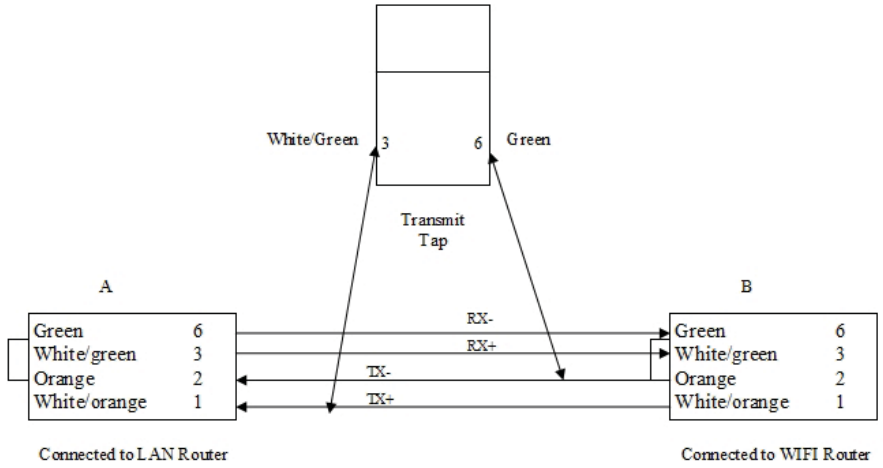
DO YOU KNOW WHO THE INFORMANT WAS?

Contact Hackbloc Staff at staff@hackbloc.org

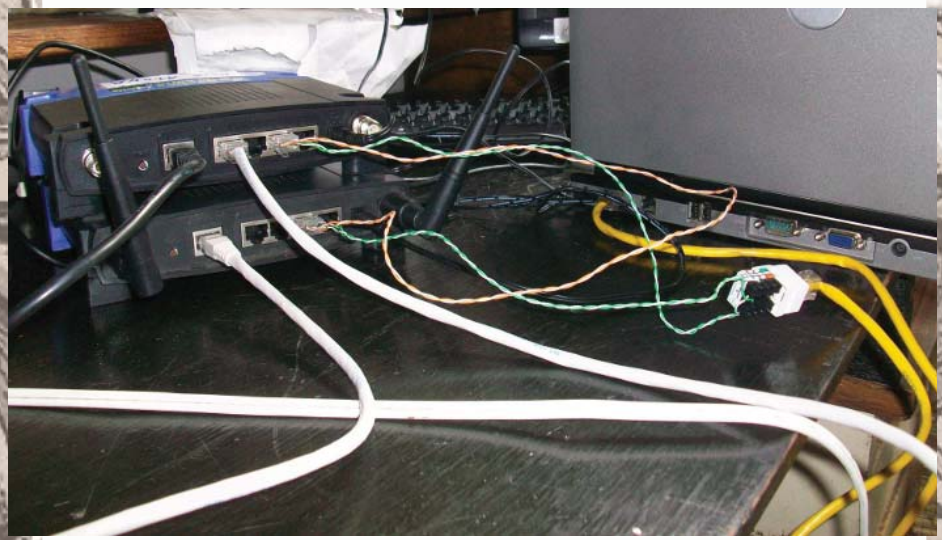
For those who haven't been following the story, Daniel Spitler and Andrew Auernheimer, alleged members of the computer security group Goatse[goatse] have been charged with Conspiracy to Access a Computer Without Authorization and Fraud in Connection with Personal Information for their alleged role in exposing a major flaw[majorflaw] in the way AT&T was storing the personal information of iPad users. The email addresses of many in rich and powerful circles was open to exposure including members of the White House Staff.

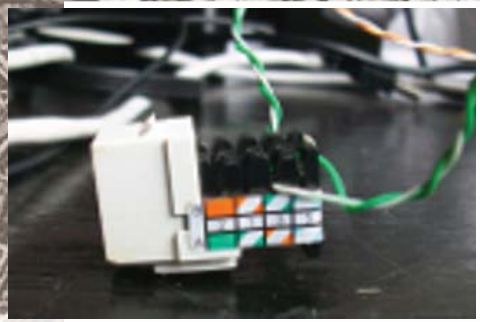
While the Department of Justice claims these two "hacked into" AT&T databases, the reality is that they simply queried them a number of times. On a public-facing web page, you could ask the database who was associated with which hardware ID and it would tell you.

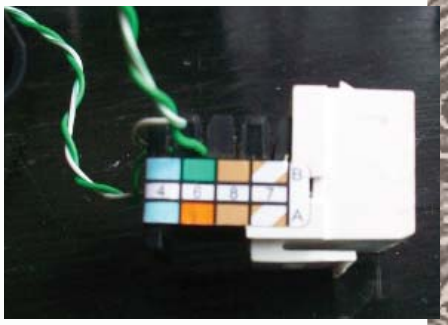
In a court document posted on Cryptome [cryptome], it's revealed that a confidential informant provided IRC chat logs to the FBI. According to the affidavit, "Approximately one month after the search of defendant Auernheimer's home, a confi-



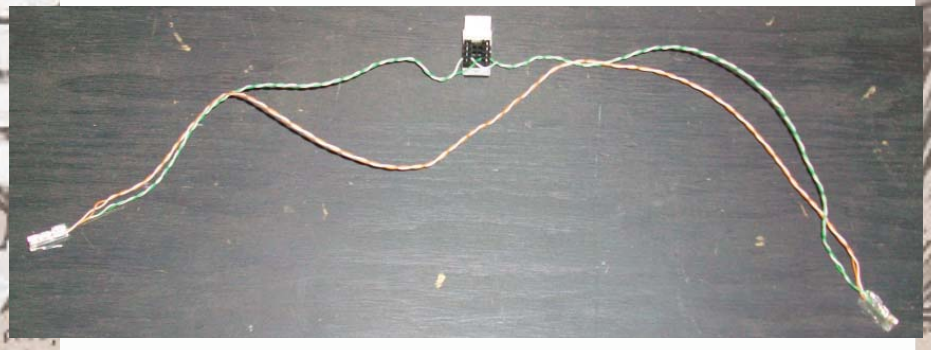
I plugged one end of another CAT5 cable into the NIC on a laptop and the other end into the tap as shown here:







The final result should look like this:



INSTALLATION OF TAP

As I said above, I choose to put the tap between my 2 routers, although they can go between a switch and a router too. The one labeled A (see below) was put in my LAN router and the one labeled B was put in the WIFI router. The WIFI traffic transmitted packets to the LAN router via the orange pair. The WIFI router received packets from the LAN router via the green pair. This particular tap is just for viewing transmission packets. I would need another NIC for a receiving tap.

dential source (the "CS") contacted federal law enforcement officers and stated, among other things, that the CS routinely monitored "#dominion," one of the IRC channels used by Goatse Security members to communicate with one another. The CS also provided law enforcement officers with chat logs from the "#dominion" channel from on or about June 2, 2010 through on or about June 11, 201 O. Extending over 150 pages, those chat logs conclusively demonstrate that defendants Spitler and Auernheimer were responsible for the data breach and conducted the breach to simultaneously damage AT&T and promote themselves and Goatse Security. Excerpts from the chat logs are provided below."

While there was a snitch within IRC channel, it appears [weak] that Goatse members have also offered to work with the Department of Justice "hand in hand for a stronger country" which is all somebody would need to not trust the goatse folks. Future informants against other "malicious hackers"? The idea unfortunately isn't that far-fetched.

It shouldn't be hard to figure out who this snitch was in this case given that they were idling in an IRC room for extensive periods of time. We must protect our communities against snitches who will sell their friends down the river in exchange for legal immunity, status, nationalism, or anything else. Snitching only weakens our community, divides it, and sows distrust into our relationships. Find snitches, publicly out them, and excommunicate them from our community!

A statement was posted [statement]on the goatse site which is copied below:

"On the heels of the arrest of two of Goatse Security's researchers, I felt compelled to write a statement reiterating a few points regarding last year's AT&T breach which I believe are important:

1. The only data gathered was a list of e-mail addresses. No real names, mailing addresses, or any associated data was breached.

2. The data gathered was PUBLICLY AVAILABLE on AT&T's web server. Any person could say "What is the e-mail address associated with ID XXXXXXXX" and the server would happily reply "johndoe@yahoo.com" or "invalid ID". The process of doing so was simply automated using random IDs. There was no "real" hacking involved.

3. Through intermediary channels, Goatse Security notified AT&T of the hole in their system and waited until it had been patched before we made our disclosure.

4. Under no circumstances was the data EVER made public. It was only given to Gawker Media under the condition that it would be redacted, just as proof that the data *HAD* been leaked and this was not a fictitious claim.

5. AT&T has pressured the USDoJ and the FBI into building and prosecuting a baseless case because they care more about their own share price than their customers. Stated another way: the American government works at the behest of private corporations.

AT&T, the FBI, and the prosecution have labelled this as a "malicious" attack, directly against AT&T's interests and their customers. This could not be farther from the truth. The flaw was quite literally stumbled upon; AT&T was never targeted, and upon gathering the data, it was not sold, distributed, or used otherwise (although it certainly had the potential to be used quite maliciously) – it was only disseminated to a single media outlet because we believed it was important enough to share. Were the hole discovered by a malicious party, the data could have been easily sold to the RBN at a very high price, could have been used to target iPad owners with AT&T phishing e-mails, the e-mails could have been sent iPad trojans, or otherwise. The private discussions we had to determine the extent of the flaw will undoubtedly be twisted and redacted by the prosecution to create an appearance of malice, as these were

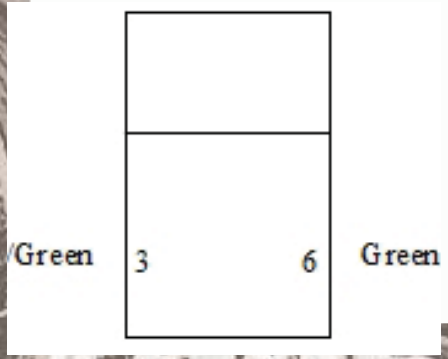
HOW TO MAKE TAP

Take a CAT 5 cable and cut it the length you will need to extend the cable between the network devices. In my case, I put the cable between the LAN router and the WIFI router. Open up the cables revealing the wires. Separate the orange and green pairs from the other wires.
Take 2 RJ11 plugs and on each plug, but the green in slot 6, the white/green slot 3, the orange in slot 2 and the white/orange in slot 1 as shown below:

Green	6
White/green	3
Orange	2
White/orange	1

White/orange	1
Orange	2
White/green	3
Green	6

Take the keystone and use a punch down tool to punch down the white/green in the 3 slot and the green in the 6 slot of the keystone as shown here:



HOW TO MAKE A NETWORK TAP

by sally

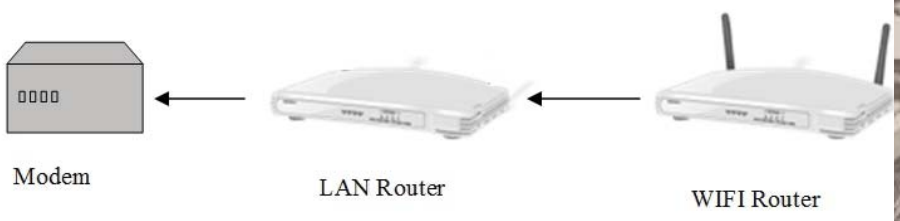
Recently, I needed the ability to "sniff" a network that I run to detect unwanted traffic. I work for a non-profit that can't afford costly boxes that can check for "network intrusion." I told a friend about my dilemma and he taught me how to make one for cheap!
This guide explains how to create a cheap and easy network tap.

WHAT YOU NEED

- 2 RJ 11 plugs
- CAT 5 cable
- CAT 5 RJ 45 keystone module insert
- A network sniffer such as Wireshark[shark]
- Scissors
- Plyers
- Punch down tool

ROUTER SETUP

I'll be using what I did as an example, but there are a variety of ways of setting this up. My set up is as follows:



The DSL modem is plugged into the wall and connected to an ISP. A Linksys WRT54GLis connected to the modem strictly as a LAN router. Then another Linksys WRT54GL is connected to the LAN router.

all topics touched upon. This can be damning even though the discussion itself is not a crime.

The case is based entirely upon IRC logs, anonymously submitted, which could be completely fabricated with no method of verification. The transcripts of these logs are solely being used to create an image of malicious intent.
The fact of the matter is quite simple: AT&T put their own customers at risk through negligence, their share price dropped when this fact was exposed, and they have now co-opted the USDoJ and the FBI to attempt to shift the blame from themselves to individuals who were looking out for the public good.

In the end, regardless of how the chat logs are made to appear, the facts do not change: GoatSec researchers found a hole, made sure it was closed, and responsibly disclosed its existence."

[goatse] http://security.goatse.fr/
[majorflaw] http://www.huffingtonpost.com/2010/06/09/ipad-security-breach-expo_n_606700.html http://tinyurl.com/3yqj5pl
[cryptome] http://cryptome.org/0003/spitler/spitler-001.pdf http://tinyurl.com/4vfhf4a
[weak] http://security.goatse.fr/open-letter-lee-vartan

HACKERSPACE

You know what we like? Lockpicking. Why? Because it's useful. It'll get you out of a bind, it'll show you how the world around you works. If you can crack a lock, you can probably figure a few other interesting things too. Maybe you'll start thinking about other places these skills would be useful, and maybe you'll join up with other curious, ambitious and knowledgeable people. We could learn something together. With more access to resources – time, tools and especially creative input – we could do something that no one person could have done alone.

We are Skullspace, a hackerspace born of the frozen prairie hellscape that is Winnipeg. We're not the first, but we're the first in our city. We're not alone either – the global hackerspace community gave us the ideas and knowledge we needed to start, and neighbouring spaces are popping up across the country. We do programming, graphics, electronics and hardware. Sometimes we bake cupcakes and send them halfway across the globe. Most of the time we get together and figure out how things work. Things like microcontrollers and locks.

There's another reason we're so hung up on picking locks: because it's knowledge. Simple. If you can teach someone how to pick a lock then you've passed on knowledge. You've taught something. Knowledge is free. What they teach you in schools, that's free but that's not knowledge. It's packaged consumer goods: reading, writing, adding, dividing. It'll let you figure out if the price of wonderbread has gone up or down since last week. It'll show you which detergent offers how much more percent of whatever the fuck planet-killing toxins they decided to pump into it. Yeah, that's not knowledge and that's not what we're after. No, knowledge shouldn't be proselytized at

Cryptbin has a unique feature called "insurance mode" where you can provide a password and once it is entered, the data is permanently decrypted and available to everybody who visits the page. This is probably inspired by the Wikileaks insurance file, which was released in encrypted form to prevent harm or assination of Julian Assange or the Wikileaks projects. The site owners are nice enough to publish their source code at https://cryptbin.net/release under an open source license but unfortunately it doesn't allow people to make derivative works. The site was produced by the hacker project anapnea.net.

URL: https://spaste.com
Host-Proof: Partial (they only store a hash of your password)
Encryption Password: Yes. AES of unknown strength
Logs IPs: Yes
Country: USA
SSL: Yes
Emails your recipient for you: No
Javascript: Yes
Self-destruct: Yes, if you set it
Retention Control: Yes
Spaste allows you to control your data with elevating levels of security and takes care to explain each level of security. For instance, pastes are deleted after 30 days by default but you can specify the note to be deleted on a specific date or after a certain number of views. They have also released their source code on their site and licensed it under the New BSD License, making it free software.

Self-destruct: No
Retention Control: No
This service is for creating encrypted lists, not messages. As a result, pasting in a message that spans multiple lines will put it all on one line. This can easily be overcome by creating multiple numbers for the list or using it to exclusively send short messages such as passwords. They have a very well-explained privacy policy and terms of service. This particular site uses the mouse to generate entropy for the encryption. The other sites didn't seem to have this, so it's unknown whether they do it in the background or at all. Strong encryption relies on entropy to ensure the the large prime numbers used to encrypt data are "random enough". If "random enough" numbers cannot be generated for encryption, the encryption becomes severely weakened.

* Https certificate appears broken temporarily but worked a few weeks ago

URL: https://privnote.com
Host-Proof: Yes
Encryption Password: Yes, strength and algorithm unknown
Logs IPs: No
Country: USA
SSL: Yes
Emails your recipient for you: No
Javascript: Yes
Self-destruct: Yes
Retention Control: No, but messages auto-delete in 30 days
Unlike other sites, this sites has a policy of not logging IP addresses. It also contains a neat feature which can email you when your note is read.

URL: https://cryptbin.net
Host-Proof: No
Encryption Password: Yes. Twofish of unknown strength
Logs IPs: Yes
Country: UK
SSL: Yes
Emails your recipient for you: No
Javascript: No
Self-destruct: No
Retention Control: Yes

you and made to be regurgitated verbatim. It should be passed from person to person, free of charge. We want to pass on the knowledge of digital systems, of the nets we're part of, the communication that surrounds us. We want to be better informed to navigate the world we live in. We want to know more than the average person knows. When something fucks up, we want to know how to fix it.

We're not alone. We've reached out, to our equals, to people we've never met. To people who understand, who want to share their knowledge. What we've built – what we're building – is not built on a totalitarian ideology or on some ultimately binding ideal. It's built on a globe-spanning database of human knowledge. We've seen that people are willing to help when they're being treated as equals, when they're working towards a common goal. We don't want the profits, the patents and all the other things that commoditize our experience. We don't want to focus on the bottom line. We want to build a community, to build a culture. We want to make a positive, long-lasting change to society by encouraging free pursuit of knowledge.

We don't want to be like the wage slave. The wage-slave is reluctant to give up his knowledge, knowing that every minute is worth a finite amount. If the balance doesn't weigh out in his favor, if his knowledge tips the scale, he'll share nothing, give nothing. He plays a zero-sum game. If you want to do something, inspire someone, help build something bigger than yourself – you'll give your knowledge up for free. Hackerspaces know this, they give away information worth thousands in seminars, discussions, and in face to face or online conversations.

Knowledge is free, groups are power.
Go join your local hackerspace today.

Electronic Civil Disobedience in Solidarity with Hunger Strikers in Greece

On March 2, an ECD was called in solidarity with hunger strikers in Greece. Below are a few excerpts from the call-out:

"INSTRUCTIONS
1. Download the program (html file) from any of the links at the bottom of this page.
2. At 11.00 (greek time, GMT+2), on Tuesday 2/3, double-click to open.
3. Keep the window open as long as you can
4. This works by loading images from Greek State web-pages , overloading their servers and making them unfunctional and useless for sometime. If we see some pictures not being able to load then our goal is fullfilled
5. Solidarity is our weapon!"

"Thanks for participating in this Elecronic Civil Disobedience against the Greek state. This action was chosen to demonstrate the solidarity with the 300 labourers-migrants hunger-strikers who decided to fightback with their own body and life against a system of explotation and opression that capitalism sets up for migrants .

PLEASE KEEP THE WINDOW OPEN AS LONG AS POSSIBLE
This works by loading images by Greek State web-pages , overloading their servers and making them unfunctional and useless for sometime. If you see some pictures not being able to load then our goal is fullfilled.
IN ORDER TO PARTICIPATE,SIMPLY DOWNLOAD THE FILE AND OPEN IT. SOLIDARITY IS OUR WEAPON"

URL: https://thismessagewillselfdestruct.com
Host-Proof: Partially (the decryption password is stored on the server as a hashed salt)
Encryption Password: Yes
Logs IPs: Yes
Country: USA
SSL: Yes
Emails your recipient for you: No
Javascript: No
Self-destruct: Yes
Retention Control: No
This site has a long name but also has a URL shortener at www.tmwsd.ws.

URL: http://safemess.com
Host-Proof: Yes
Encryption Password: Yes, 128-bit XXTEA.
Logs IPs: Yes
Country: Sweden
SSL: No
Emails your recipient for you: No
Javascript: Yes
Self-destruct: No
Retention Control: Yes
The encryption algorithm used on this site has some known weaknesses but the author does not know enough about them to say whether they apply in this case. Unlike the rest of the sites surveyed here, this one is not located in the US which could provide additional privacy for some users.

URL: https://cryp.sr*
Host-Proof: Yes
Encryption Password: Yes, AES of unknown strength
Logs IPs: Yes
Country: USA
SSL: Yes (had some certificate issues at time of press)
Emails your recipient for you: No
Javascript: Yes

Javascript: Yes
Self-destruct: No
Retention Control: Yes
Once you have created your note at this site, it will show up on the left column and you'll have to copy the link from there.

URL: https://pastee.org
Host-Proof: Partially (the passphrase is stored as a SHA-256 hash)
Encryption Password: Yes AES 256-bit encryption
Logs IPs: Yes
Country: USA
SSL: Yes
Emails your recipient for you: No
Javascript: No
Self-destruct: No
Retention Control: Yes
This site has a nice simple interface and features very strong encryption.

URL: https://onetimemessage.com
Host-Proof: Partially (the encryption password is not stored on the server, but is submitted during retreival)
Encryption Password: Yes 1024-bit RSA
Logs IPs: Yes
Country: USA
SSL: Yes
Emails your recipient for you: Yes
Javascript: No
Self-destruct: Yes
Retention Control: Yes
This site's SSL certificate was expired when it was tested, resulting in a scary browser pop-up. This will probably be fixed soon. If not, as long as the certificate is for the correct site with the exception of the expiration date it should still be safe to use. It requires an email address for the sender and the recipient. The recipient must be a real address or else they won't get your message. The sender email address can be faked. If you want to generate links to send to people manually, you have to register which you can do with a one-time email address such as those available at mailinator.com.

Of particular interest is that the call-out and instructions were translated into five different languages in order to get as many participants as possible. The ECD tool was also hosted on a number of temporary file hosts, some of which were still online as of press time. A number of websites of the Greek Government were knocked offline during this ECD.

The tool used during this ECD looks to be a modified version of the one used in another Greek ECD during 2008 in solidarity with the ongoing insurrection. Approximately a week after the ECD, the hunger strike was ended in victory as the government conceded to some demands of the strikers.

NOTE:
A new guide published on zinelibary.info shows how one can plan and execute an act of civil disobedience. It covers the various tools which are available for launching an ECD, examples of past ECDs, how to anonymously participate in ECDs, and much more.

http://zinelibrary.info/how-plan-and-execute-act-electronic-civil-disobedience-ecd-v2

Get your copy at http://zinelibrary.info/how-plan-and-execute-act-electronic-civil-disobedience-ecd-v2 http://tinyurl.com/6bx3pzd

We do not encourage anybody to use this information towards any illegal ends. This is provided for informational and educational purposes only.

(A) Quick and Dirty Guide To a Fairly Secure Twitter Gateway by trem

Here I'll show you how to send tweets over the command line over SSH using perl script called TTYtter (http://www.floodgap.com/software/ttytter/) in Ubuntu.

This is specifically geared towards those living in countries where access to twitter is either monitored or forbidden. Ideally, this server would be hosted in a jurisdiction with friendlier laws regarding free speech and the media.

Installing SSH

From the command line, type the following

`SUDO APT-GET UPDATE`

```
trem@junky:~/.nothing/scripts/twitter$ sudo apt-get update
Get:1 http://security.ubuntu.com lucid-security Release.gpg [198B]
Ign http://security.ubuntu.com/ubuntu/ lucid-security/main Translation-en_CA
Ign http://security.ubuntu.com/ubuntu/ lucid-security/restricted Translation-en_CA
Hit http://archive.canonical.com lucid Release.gpg
Ign http://archive.canonical.com/ lucid/partner Translation-en_CA
Hit http://deb.torproject.org lucid Release.gpg
Hit http://ca.archive.ubuntu.com lucid Release.gpg
```

Next, we'll install the SSH daemon using the command

`SUDO APT-GET INSTALL OPENSSH-SERVER`

```
trem@junky:~/.nothing/scripts/twitter$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  rssh molly-guard openssh-blacklist openssh-blacklist-extra
The following NEW packages will be installed:
  openssh-server
0 upgraded, 1 newly installed, 0 to remove and 46 not upgraded.
Need to get 0B/304kB of archives.
After this operation, 815kB of additional disk space will be used.
WARNING: The following packages cannot be authenticated!
  openssh-server
Install these packages without verification [y/N]? y
Preconfiguring packages ...
Selecting previously deselected package openssh-server.
(Reading database ... 192986 files and directories currently installed.)
Unpacking openssh-server (from .../openssh-server_1%3a5.3p1-3ubuntu5_amd64.deb) ...
Processing triggers for ureadahead ...
Processing triggers for ufw ...
```

REVIEW OF SERVICES

TERMS:

Host-Proof: Is the website hosting your secret message unable to read it?
Encryption Password: Are you provided a password to decrypt your message? How strong is the encryption on your message?
Javascript: Is javascript required to use this service? Some users browsing the web anonymously may not want a javascript-based service while others may prefer it as truly host-proof systems require it.
Self Destruct: Will the message self-destruct upon being read?
Retention Control: Can you change when the message is deleted (aside from self-destruction)?

For the survey of these sites, many did not say whether they logged IP addresses or how long they retained data. In such cases, it's assumed that they log IPs and retain data forever.

URL: https://privatepaste.com
Host-Proof: No
Encryption Password: Yes
Logs IPs: Yes
Country: USA
SSL: Yes
Emails your recipient for you: No
Javascript: Yes
Self-destruct: No
Retention Control: Yes
This service puts the encryption password in the URL and also offers a file upload service with the same features. It features a nice minimalist design.

URL: http://securepastebin.com
Host-Proof: Yes
Encryption Password: Yes. 56-bit encryption for short passes, 3DES for longer ones but unknown bit strength
Logs IPs: Yes
Country: USA
SSL: No
Emails your recipient for you: No

should certainly be using email encryption.

If you're concerned about your privacy and anonymity, you'll want a service that doesn't log IP addresses. The claim that they don't log your personal information is nearly impossible to verify. Nevertheless, it makes sense to support providers that don't log IP addresses. With secret message services, you're often relying on the word of the website you're using to protect your information. A good policy is to use sites interchangeably, minimizing the damage that can be caused by a compromise at one of the site due to their own malice or a simple coding mistake.

As a final note, the laws that govern access to the data stored on these secure message services are quite different than those for email. Certain thresholds are required to be passed in the US (The Electronic Communications Privacy Act among others) if the government wants access to your email. Services which simply store data, such as secure messages services and twitter are governed by different laws and court rulings. To see a concrete example of this, see DoJ v Jacob Appelbaum et al [cryptome].

Editor's Note: This article only overviews a few services out there that the author could find, there are certainly many more. If you have one to recommend to others, please let the us know at: staff{{{{at}}}}}hackbloc.org. We'll hopefully have more to add in the next issue!

[1] http://iamnotarapperispit.com/2010/12/08/eff-warns-of-untrustworthy-ssl-undetectable-surveillance/ http://tinyurl.com/5rvdvyx
[2] http://news.infoshop.org/article.php?story=20080804081217280 http://tinyurl.com/6d3tofz
[tor] https://torproject.org
[cain] http://www.oxid.it/cain.html
[dsniff] http://monkey.org/~dugsong/dsniff/
[wireshark] http://wireshark.org
[fire] http://codebutler.com/firesheep
[cryptome] http://cryptome.org/0003/appelbaum/usa-v-appelbaum.htm http://tinyurl.com/5rql6f8

Then, we'll start SSHD by typing the following:

```
SUDO /USR/SBIN/SSHD
```

Installing cURL/Lynx

We're going to need to install cURL or Lynx in order to use TTYtter. (for this tutorial, we'll install cURL) type the following command:

```
SUDO APT-GET INSTALL CURL
```

```
trem@junky:~$ sudo apt-get install curl
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  curl
0 upgraded, 1 newly installed, 0 to remove and 46 not upgraded.
Need to get 0B/210kB of archives.
After this operation, 336kB of additional disk space will be used.
WARNING: The following packages cannot be authenticated!
  curl
Install these packages without verification [y/N]? y
```

Installing TTYtter

Then, we'll need to download the TTYtter script using wget, then rename it. We'll do this by typing the following:

```
WGET HTTP://WWW.FLOODGAP.COM/SOFTWARE/
TTYTTER/DIST1/1.1.10.TXT
```

```
trem@junky:~/.nothing/scripts/twitter$ wget http://www.floodgap.com/software/ttytter/dist1/1.1.10.txt
--2011-02-19 02:35:11--  http://www.floodgap.com/software/ttytter/dist1/1.1.10.txt
Resolving www.floodgap.com... 66.159.214.137
Connecting to www.floodgap.com|66.159.214.137|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 150600 (147K) [text/plain]
Saving to: `1.1.10.txt'

100%[======================================================================================================>]

2011-02-19 02:35:17 (24.3 KB/s) - `1.1.10.txt' saved [150600/150600]

trem@junky:~/.nothing/scripts/twitter$
```

Let's rename the script something a little easier to remember. Type the following command.

```
MV 1.1.10.TXT TWITTER.PL
```

```
trying to find cURL ... /usr/bin/curl
-- no version check performed (use /vcheck, or -vcheck to check on startup)

++------------------------------------------------------------------++
||  WELCOME TO TTYtter: let's get you set up with an OAuth keyfile!  ||
++------------------------------------------------------------------++
Twitter now requires all applications authenticating to it use OAuth, a
more complex authentication system that uses tokens and keys instead of
screen names and passwords. To use TTYtter with this Twitter account,
you will need your own app key and access token. This requires a browser.

The app key/secret and user access token/secret go into a keyfile and
act as your credentials; instead of using -user, you use -keyf. THIS
KEYFILE NEVER EXPIRES. YOU ONLY NEED TO DO THIS ONCE FOR EACH ACCOUNT.

If you DON'T want to use OAuth with TTYtter, PRESS CTRL-C now. Restart
TTYtter with -authtype=basic to use a username and password. THIS IS
WHAT YOU WANT FOR STATUSNET, BUT WILL NOT WORK WITH TWITTER!
If you need help with this, talk to @ttytter or E-mail ckaiser@floodgap.com.

Otherwise, this wizard will create a keyfile /home/trem/.ttytterkey
for you. Press ENTER/RETURN to begin the process.
```

Then, we'll run the script by typing the following:

```
PERL TWITTER.PL
```

Press Enter or Return, and start Firefox and log into your twitter account. Copy and paste the URL into Firefox.

```
Start your browser.
1. Log in to https://twitter.com/ with your desired account.
2. Go to this URL (all one line). You must be logged into Twitter FIRST!

http://dev.twitter.com/apps/key_exchange?oauth_consumer_key=XtbRXaQpPdfssFwdUmeYw

3. Twitter will confirm. Click Authorize, and accept the terms of service.
4. Copy the entire string you get back.
-- Paste it into this terminal, then hit ENTER and CTRL-D to write it ---------
```

against a sophisticated adversary. For most people in most situations, host-proof services are a great way to beef up their email security.

While host-proof service providers are nice, they all require some type of active scripting such as Javascript to be run in your browser. While Javascript is great for this application, it can be a barrier when trying to anonymously send notes. If you're using a proxy, Javascript can break out of your proxy and directly connect to any website, revealing your true IP address and location. (Using Tor[tor] with TorButton blocks this malicious behavior.) If you need the anonymity, this poses a risk and you may not want to use host-proof services. The next best option is to use online services which encrypt the data and pledge not to decrypt it.

Even if your site stored your data in an encrypted fashion, if you're worried about it becoming compromised you want to make sure that encryption is strong enough to protect it. These days, anything which is 128-bit or higher is probably sufficient. Cracking 128-bit encryption has been compared to finding a grain of sand in the Sahara Desert. Anything less than 128-bit is no longer recommended for storing sensitive information. Additionally, using a long password will take advantage of the full strength of 128-bit encryption.

Another common example: let's say you send somebody a link for your secret message and the password for it. This is nice security theater, but if somebody intercepts that email with the link in it then they'll be able to view your secret message. A nice way around this is to send messages which self-destruct. If your intended recipient gets to the secret message first, they'll be the only one to get it. Otherwise, they will be able to tell that the message was compromised. I have used this self-destructing feature with great results. In one situation, it provided conclusive proof that somebody was intercepting my messages.

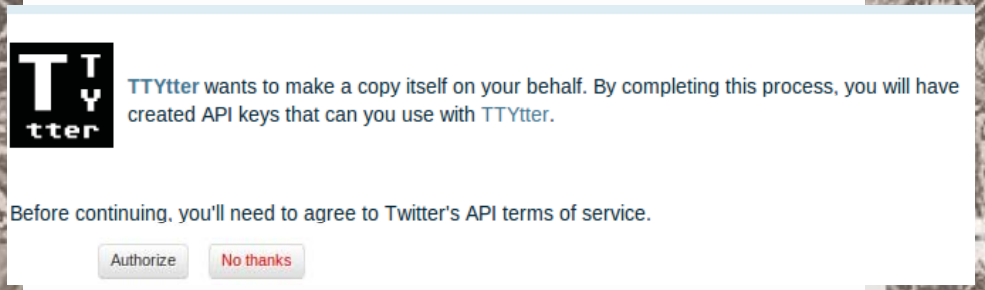
Another point of consideration is the country your secret message will be hosted in. If you're a whistleblower in Nigeria and the site you're transmitting your secret messages on (or the owner of the site) is located there as well, you can bet your ass they'll roll over for your government. In this case, you'll want to pick a server that isn't located in your country. If they are outside of your national borders, it's much more difficult to obtain or enforce a court order. Taking account of legal geography is how sites like WikiLeaks and The Pirate Bay can continue to operate despite so much legal pressure. If you're worried about this then you

nection is encrypted but unfortunately your data is stored in plain-text on the server end. Some providers encrypt data on their hard drive but also store the private keys necessary to decrypt the data in the same place.

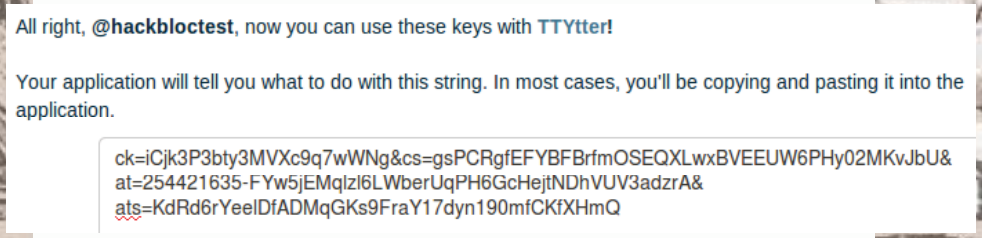
If you're worried that your provider might roll over upon receiving a legal threat or a visit from some characters in suits, you're going to need a little more security. Even if you don't, we should support providers that put the control of your data back into your hands. In host-proof encryption, the data is stored on the server encrypted and all the encryption/decryption takes place in the browser via Javascript. Because the encryption is done in the browser, when you submit your secret message to secretmessagestorage.com, it is stored encrypted and they have no way to decrypt it short of trying every possible password. When your recipient requests your secret message, they receive the data in encrypted form and use the password to decrypt it in their browser. Some services are partially host proof -- they will store encrypted data along with your password in the form of a hash. A hash is a cryptographic function that's applied to data which is easy to do one way but impossible to reverse. For instance, the MD5 hash (or sum) of "fuck the police" is 19801a5032467c91b4ee34d17efb50af. In order to find out what that long set of letters and numbers was before it was hashed, one would have to try hashing every possible combination of text until they got a match. This may sound difficult, but with the aid of a computer this is fairly trivial. There are numerous sites online which will break hashes for free. A salted hash uses a salt (a series of bits usually derived from the password an account) in conjunction with a regular hash to make hashes which are stronger and more resistant to attacks through lists of pre-computed hashes called Rainbow Tables.

Keep in mind that in host-proof systems anybody who requests your message will receive it assuming it isn't self-destructing. The message will be encrypted, but if you use a short password it will be easy to break. Likewise, unless you're connecting via HTTPS, your weak-password-protected information is being sent across without additional protection. Keep in mind that if you emailed the recipient the password or sent it over other insecure channels, the data could be captured by your adversary and decrypted when combined with that password. Also, the website you are using can always deliver you custom code which sends your information back to them in plaintext. There's a good article which overviews how this works here. [2] Ultimately, if the website you use will roll over for a court order, know your IP address, and know you'll be storing messages there at a future date, you're fucked. That's assuming they know a lot of things and that you're up

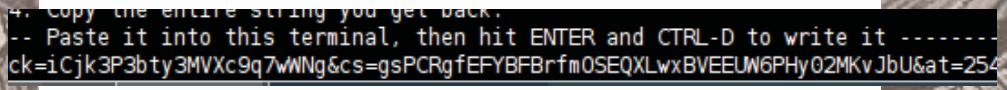
Click the 'Authorize' button



Now click the 'I Accept' button. On the next page, you will receive your key.



Copy and paste your key into TTYtter.



Hit enter then type CTRL-D

```
-- EOF ----------------------------------------------------------------
Written new key file /home/trem/.ttytterkey
Now, restart TTYtter to use this keyfile -- it will use this one by default.
(For multiple key files with multiple accounts, manually write them to other
 filenames, and tell TTYtter where the key is using -keyf=... . You can just
 use a text editor for that.)
```

This should be what you see if it was successfully installed.

Tweeting

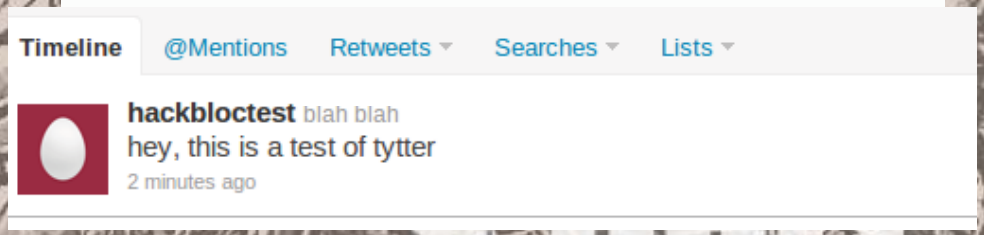
Finally let's run the script and send a test tweet. Type the following

`PERL TWITTER.PL`

```
##################################################        +oo=========oo+
        TTYtter 1.1.10 (c)2011 cameron kaiser             @             @
                all rights reserved.                       +oo=    =====oo+
      http://www.floodgap.com/software/ttytter/          a==:  ooo
                                                         .++o++. ..o**O
  freeware under the floodgap free software license.     +++   :O:::::
       http://www.floodgap.com/software/ffsl/            +**O++ #   :ooa
                                                                  #+$$AB=.
         tweet me: http://twitter.com/ttytter                     #;;ooo;;
            tell me: ckaiser@floodgap.com                         #+a;+++;O
##################################################               ,$B.*o*** O$,
#                                                              a=o$*O*O*$o=a
# when ready, hit RETURN/ENTER for a prompt.                      @$$$$$@
# type /help for commands or /quit to quit.                       @o@o@o@
# starting background monitoring process.                         @=@ @=@
#
TTYtter> -- notification: API rate limit is currently 350 req/hr
-- no version check performed (use /vcheck, or -vcheck to check on startup)
-- you are logged in as hackbloctest

TTYtter> hey, this is a test of tytter
TTYtter>
```

From the TTYtter> prompt, here we can send our message to twitter.



When the internet was designed, not a whole lot of thought was put into information security. It was assumed that if you wanted to send information securely, you'd be the one to figure out how to do so. As a result, encryption and privacy in general wasn't built-in to many of the protocols we use to send information across the net today. SSH and SSL/HTTPS are the two most well known methods for securely transmitting information online.

HTTPS is a technology supported by every major web browser that allows you to encrypt your connection to the website you're viewing. Sites that do not support HTTPS send their data (web pages) across in plain-text which allows anybody on your wireless/local network, your internet service provider, and the government to see what it is. For most people, this means that their emails, social networking information, Facebook password, site login information, and a host of other nice things are visible to anybody who would like them. If you want to see what you're sending out in plain-text, check out Cain and Abel (Windows)[cain], dsniff (Linux)[dsniff], Firesheep (Windows, OS X)[fire], and Wireshark (all, made for more advanced users)[wireshark].

Sites that support HTTPS will display it in the address bar. For instance, an address like http://www.sketchywebsite.com doesn't have HTTPS enabled whereas https://www.sketchywebsite.com does. Notice the extra "s"? It stands for secure. It verifies that the connection between you and the site is encrypted. The encryption is strong enough that you don't have to worry if somebody intercepts your data as they won't have the resources to crack it. If they did, they could just get the unencrypted logs and other data on the site you're connecting to or your computer anyways (as HTTPS only protects your data in transit). If you want to see what this looks like, just log on to riseup.net, hackbloc.org, or your favorite online bank.

As a note, HTTPS relies on a network of "certificate authorities" to authenticate the site you're connecting to. This system is largely broken due to a number of factors. If somebody with a court order or leet hacking skills were to approach these certificate authorities, they could spoof a false certificate and decrypt your data[1]. This would obviously require a significant amount of work, so for the sake of this article we'll assume this won't happen. When browsing a site that supports HTTPS, your con-

Using Secure Pastebin Services to Beef Up Your Email Security

by withoutsubmission

Email security has come a long way since we first started sending each other messages across the world wide web, but the adoption of email security practices by many has been slow. An extremely small minority of people support email encryption. Hackers, computer security experts, government agencies, and HIPPA-mandated institutions such as hospitals tend to use it the most. There is a small subset of computer savvy activists which use email encryption, such as the animal liberation/rights community in the UK that have learned through house raid after house raid that they must use encryption to protect their information. This may be a rough estimates based off of personal experiences, but the basic fact that most people don't use encryption still holds true. Even among hackers who know more about data security than most, encryption adoption still isn't as widespread as one might expect.

On the provider side, most webmail providers don't encrypt your emails when you view them online (allowing anybody on your wireless network to read them). Few email providers support technologies such as StartTLS which encrypt emails in transit between email servers, and even fewer email providers encrypt your emails when they are stored on their servers. Riseup.net and other "activist" tech collectives are the few exceptions to this.

A common problem scenario is wanting to send an encrypted email to somebody without encryption support. For instance, how do you securely send a password to somebody across the world without requiring that they install any specialized software? The obvious solution is for the recipient to use an email client with encryption but a quick fix is to securely host the message on a website which specializes in fixing just this type of problem. While any of the services listed here will increase the security of sending your messages, they all offer different benefits for different situations. All of the services in this article are more secure than sending somebody a message in plain-text using email. Let's go into what factors might go into analyzing which service is the best for you. No service is 100% secure (not even email encryption) so you'll be making a call as to which security configuration makes the most sense in your situation.

Success!

How to use this server

This tutorial has showed you how to install SSHD and a command line twitter program. Utilizing these tools, users can send twitter messages over an encrypted connection. Shell hosting in the EU is fairly inexpensive.

example:

```
SSH <SERVERIPADDRESS>
```

then:

```
CD /PATH/TO/TTYTTERDIR

PERL TTYTTER.PL
```

Further reading:

https://hackbloc.org/content/how-plan-and-execute-act-electronic-civil-disobedience
https://hackbloc.org/sites/hackbloc.org/files/browservm.pdf
https://ssd.eff.org/
http://www.torproject.org/docs/tor-hidden-service.html.en
http://www.ubuntugeek.com/securing-ssh.html
http://www.howtoforge.com/truecrypt_data_encryption

ANONYMIZING LOGS WITH LOGROTATE

BY CALL TO RUPTURE

Many service providers for social movements such as Indymedia make the choice to not keep logs that contain personally identifying information (PII). This is great, but this can create immense headaches for the many people behind these service providers. Imagine you run (or maybe you already do) a mail server for activists in the area. Somebody contacts you complaining that they are having problems receiving mail through their mail client. You have to parse through your logs but there isn't an obvious error message. You now have to find the logs of this particular person's connection but can't because you deleted all the personally-identifiable information before it even hit the disk.

For many system administrators, writing logs to an encrypted disk for a set period of time and then scrubbing them may be a more practical solution than never allowing PII into the logs. Unfortunately, this means that you have to figure out a way to scrub the logs on a schedule. Instead of looking for another piece of software to install on your server, you can use pre-existing utilities to do the job.

Most servers come with sed and logrotate installed. With these two utilities, we can scrub our logs on a schedule. Logrotate is a utility on Linux servers which manages log retention. According to the manpage, "logrotate is designed to ease administration of systems that generate large numbers of log files. It allows automatic rotation, compression, removal, and mailing of log files. Each log file may be handled daily, weekly, monthly, or when it grows too large. Normally, logrotate is run as a daily cron job." For example,

/var/log/messages turns into /var/log/messages.1.gz then /var/log/messages.2.gz.

At some point, it gets deleted. Logrotate is convenient because it's already managing your logfiles and it's a safe way to modify logs. Some programs are extremely picky about their logs and will malfunction or shutdown if they see that a log has been modified without their knowledge.

The first thing we'll need to do is find our logrotate config file. In the case of our system, it was in /etc/logrotate.conf. We can add our customizations

2. You want a fun way to find new music and movies. File sharing is cool, but what do people in your area watch and listen to? This is a way to find out.

3. Document X, which reveals wrongdoing by the government, a corporation, or somebody else with power is censored and needs to get out to people quickly.

4. You want to anonymously leak information to the public about a local political issue. If these drop boxes get high usage, this could be a way to do it. For instance, you can publish an electronic zine on the local police which gives people names, pictures, and analysis of their current activities. In the past, literature like this has been distributed through radical bookstores, cafes, etc. Could this be a new model for doing the same?

If you want to set up a dead drop, here are a few quick tips to get you started:

1. Find a place you want to put it. This could be a naturally or artificially created hole in a brick wall, a hole in a tree, or pretty much anywhere else.
2. Get your flash drive and remove the case if necessary. Wrap it in plumbers tape to keep it dry and put it in its new home.
3. Make sure people don't have to turn their laptop upside down to access it.
4. Use quick-drying cement/patching cement to fill the area surrounding the drive. For some surfaces, epoxy may work better.

Remember that locations which are shielded from the rain will probably last longer than others. Be creative, lots of structures could be turned into public data access areas. Many handheld devices and phones now have the ability to connect to USB devices. So.. get to it!

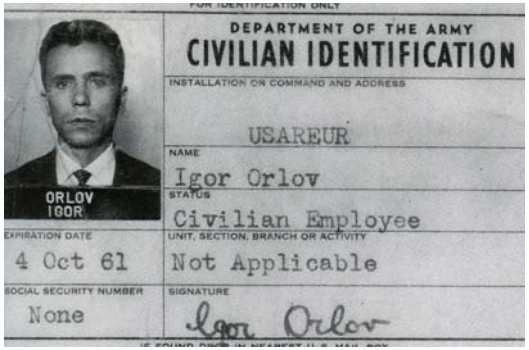
For more info and a database of dead drops, see http://deaddrops.com/. A nice instructable is available at http://www.instructables.com/id/USB-Dead-Drops/ http://tinyurl.com/2wfpa3m

[analysis] https://secure.wikimedia.org/wikipedia/en/wiki/Social_network#Social_network_analysis http://tinyurl.com/4lgo8el

How to Use Electronic Dead Drops and Feel Like a KGB Agent

Remember the thrill of reading spy novels as a kid? Want to feel like a KGB agent while helping setup public infrastructure?

Luckily for you, there's a new cool project that enables you to do just this. Electronic dead drops can refer to a lot of things but for the purposes of this article, we're talking about electronic storage devices that are embedded into the cityscape and are publicly accessible. For example, a flash drive cemented into a hole in a brick wall or an external hard drive embedded in a (hopefully dead) tree.



These dead drops are:

*Anonymous
*Decentralized
*Peer-to-peer
*Publicly accessible
*Resistant to surveillance
*Somewhat subversive

Ok, so that's cool, but what practical application do these have? Let's look at a few use case scenarios.

1. You and a few of your friends are involved in a copwatch program. You need a way to securely transfer data between each other. You could send each other encrypted emails, but you want your method of transmission to be resistant to network analysis[analysis], interception, and disruption. You and your friends drop intelligence into these public drop boxes and the intended recipients can pick them up at their leisure. If they are encrypted, the cops don't know what the file is about, who the sender is, or who the intended recipient is. Better yet, they probably don't even know to look in the drop boxes in the first place or who is putting the data there. You could even assign codenames to the drop boxes. For instance, when talking on the phone, you could say "I left some documents for you with Tina".

there or we can create specific configs in /etc/logrotate.d. Regardless of which method you choose, you'll need to add customizations for each file we want to pull PII out of. For instance, here's what our config for our apache logs looks like. Comments added by the author are followed by // but don't try importing those into logrotate.

```
/var/log/apache2/*.log /var/log/apache2/ssl_error_log /var/log/apache2/
ssl_request_log { //Defines which logs we will be working on
        daily //rotate logs daily
        missingok //If the log file is missing, go on to the next one without
issuing an error message.
        rotate 5 //Logs are only rotated five times after which they are de-
leted, mailed out, etc
        compress //Compress logs when rotating them
        create 640 root adm //Create a new log with the following permis-
sions
        sharedscripts //Only run postrotate once when rotation is done as
opposed to during each rotation prerotate //Before rotating we run these
commands to remove PII. This section is critical. For each log this for state-
ment finds, we run the sed statement to pull out IPs and replace them with
0.0.0.0. Note that this will also sanatize kernel version numbers so it's not
perfect.
            for i in /var/log/apache2/*.log /var/log/apache2/ssl_error_log /var/
log/apache2/ssl_request_log
            do
              sed -i -e 's/[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\
{1,3\}/0.0.0.0/g' $i
            done
        endscript //our scripting is done, this is an important line
        postrotate //do this after rotation
              if [ -f "`. /etc/apache2/envvars ; echo ${APACHE_PID_FILE:-/
var/run/apache2.pid}`" ]; then
                    /etc/init.d/apache2 reload > /dev/null
              fi
        endscript
}
```

Logrotate is a complicated beast with a lot of moving parts. It's easy to break and some problems are incredibly hard to diagnose. It took us around six hours to even figure out how to put that sed line in there. For this reason, only add/modify what is absolutely necessary and then do all your fun hacks later. The

basic format used in the PII-remover script should be clear, so let's look at some other sed statements we have been using in our mail.log. These statements use regular expressions, which are hard to use at first but will significantly improve your sex life with sustained use.

Remove IPs
```
sed -i -e 's/[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}/0.0.0.0/g' $i
```
Remove IPs of our users
```
sed -i -e 's/connect from [^ ]\+/connect from <anonymized_host>[0.0.0.0]/g' $i
```
Remove FROM addresses
```
sed -i -e 's/from=<[^>]\+>/from=<anonymized_email_addr>/g' $i
```
Another FROM format
```
sed -i -e 's/to=<[^>]\+>/from=<anonymized_email_addr>/g' $i
```
Remove usernames
```
sed -i -e 's/user=[^,]\+,/user=anonymized_username,/g' $i
```

Thanks for reading and giving a damn about the privacy of your users.

Related Links:
Indymedia Wiki with Tips for System Admins https://docs.indymedia.org/Sysadmin/
Using Regular Expressions with sed http://www.tutorialspoint.com/unix/unix-regular-expressions.htm http://tinyurl.com/69hj988

Editor's note: There are certainly many other useful statements for removing PII in other logfiles. If you have some, send them in to staff{at}hackbloc.org for inclusion in the next issue.

The Hidden Tracker Returns

The Hidden Tracker returned to normal operation this December. It seems like every day we hear about operators of BitTorrent trackers being harassed, arrested, and sued simply for providing the infrastructure people need to share files using the BitTorrent protocol. As a solution to this problem, a number of people have hosted trackers in countries with laws friendly to trackers only to have those countries (such as Sweden) bow to political pressure.

Decentralized tracking of torrents through DHT is slowly pushing trackers into obsolescence but the BitTorrent ecosphere does still rely to some extent on trackers. The Hidden Tracker is a project to run a publicly accessible tracker that doesn't have to worry about being shut down. The project utilizes the "hidden services" feature of Tor to anonymously host the website. This means that it's nearly impossible to find out where this site is hosted or shut it down. Note that this doesn't add any anonymity for downloaders/uploaders, just for the tracker itself.

If you are making a torrent, particularly one that is likely to be subject to censorship you might want to include this tracker. Just add these trackers to your torrent and voila! your torrent can't get shut down. One of the links uses the Tor2Web service which acts as a gateway to Tor which is accessible through the regular internet.

http://z6gw6skubmo2pj43.onion:8080/announce
https://kg6zclbtm7kwqide.tor2web.org/announce

Related links:
The Tor Project/Software: torproject.org
The Hidden Tracker Website: http://z6gw6skubmo2pj43.onion http://tinyurl.com/nvr5j4
via Tor2Web https://z6gw6skubmo2pj43.tor2web.org/ http://tinyurl.com/68fwros

```
# Check to make sure the phone home connection is running.
# Instructions for setting up ssh to a tor hidden service are here:
# http://ubuntu-unleashed.com/2008/03/howto-setup-anonymous-ssh-via-tor-hidden-services.html
FORK:
syslog(LOG_INFO, "Phone Home. $ssh_command");
system($ssh_command);
my $exit = $?;
syslog(LOG_ERR, "ssh command exited with $exit. error: $!. $ssh_command");
sleep(5);
goto FORK;

sub usage {
print <<END;
$0 [options]
  --user <user>      The username on the remote server we should be connecting with.
  --server <server> The onion server name. ie. wmnw4fdnbdvzfcrg.onion
  --verbose          Increase the verbosity of this tool.
END
}
```

PHONE HOME

Have you ever been in a situation where you got a box out in the "field" and you need to ssh into it, but chances are good it is going to be in a hostile environment? The people getting the computer start looking around the room for a kitten when you tell them to cat a file, the mention of the word firewall conjures up images of Bruce Willis in Die Hard 3 in the minds of your contacts on the receiving end, and you suspect the fucking pigs are gunna be subpoenaing all hosts and ips connected to from where your computer will be installed.

Have no fear, you now have the phone_home script to make that zombie
call home with reverse ssh to another host running ssh on a tor hidden service.

```
# This is the startup script that will get the box callinghome on startup
# and restarting the connection if it is lost
#! /bin/sh

### BEGIN INIT INFO
# Provides:                phone_home
# Required-Start:  $remote_fs $syslog
# Required-Stop:   $remote_fs $syslog
# Default-Start:   2 3 4 5
# Default-Stop:            1
# Short-Description:       OpenBSD Secure Shell server
### END INIT INFO

set -e

# /etc/init.d/ssh: start and stop the HB Phone Home daemon

test -x /root/bin/phone_home.pl || exit 0

. /lib/lsb/init-functions

# Are we running from init?
run_by_init() {
```

```
    ([ "$previous" ] && [ "$runlevel" ]) || [ "$runlevel" = S ]
}

export PATH="${PATH:+$PATH:}/root/bin"

case "$1" in
  start)
        log_daemon_msg "Starting HB Phone Home Daemon" "phone_
home.pl"
        if start-stop-daemon --start --quiet --oknodo --pidfile /var/run/
phone_home.pid --exec /root/bin/phone_home.pl ; then
            log_end_msg 0
        else
            log_end_msg 1
        fi
        ;;

  *)
        log_action_msg "Usage: /etc/init.d/phone_home {start}"
        exit 1
esac

exit 0

##### END of script

# And here is the actual phone home daemon
#!/usr/bin/perl
use strict;
use warnings;
use Getopt::Long;
use Sys::Syslog qw(:standard :macros);
openlog('phone_home daemon', 'nofatal', LOG_DAEMON);

# Instructions for a reverse ssh session are here:
# http://oogies.org/2009/07/08/reverse-ssh-tunneling/
# using tor has a tendency to forget about the host key:
# http://linuxcommando.blogspot.com/2008/10/how-to-disable-ssh-host-
key-checking.html
# Don't forget to set up public key authentication:
# http://sial.org/howto/openssh/publickey-auth/#s2
# parse command line options
my $username;
my $server;
GetOptions (
  'verbose+' => \$verbose,
  'user=s' => \$username,
  'server=s' => \$server,
);

if (!defined($username)) {
  print "Expecting a username.\n";
  usage();
  exit 0;
}

if (!defined($server)) {
  print "Expecting an onion server name to connect to.\n";
  usage();
  exit 0;
}

my $hidden_server = $username .'@'. $server;
my $ssh_command = '/usr/bin/ssh -R 9000:localhost:22 '.
  '-o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no '.

use POSIX qw(setsid sys_wait_h);

chdir '/'                 or die "Can't chdir to /: $!";
umask 0;
open STDIN, '/dev/null'   or die "Can't read /dev/null: $!";
open STDOUT, '>/dev/null' or die "Can't write to /dev/null: $!";
open STDERR, '>/dev/null' or die "Can't write to /dev/null: $!";
defined(my $pid = fork)   or die "Can't fork: $!";
exit if $pid;
setsid                    or die "Can't start a new session: $!";
```