the Ugly Truth About Online Anonymity

First of all, since this is a long post, I don't want to waste your time. If you're a computer expert or network engineer, etc. you will already know this stuff. If, however, you're a casual computer user who doesn't know much about the underlying principles of information systems, this will be way over your head. If you're a casual computer user who is thinking about anonymity online, this article might be useful for letting you know some more about what you don't know.

A lot of times, ignorant people refer to things they don't understand as "tinfoil." (The gatekeeper Left loves this term.) What follows, however, is so far out that it seems like tinfoil even to me. But then again, I haven't been targeted by a death squad for my activities online, like some people are in many countries around the world. So, is it tinfoil? For you, maybe. For people struggling against repressive regimes, maybe not.

When I use the term "tinfoil" below, I'm not making fun of you, I'm making fun of myself, and the roles I've had to play in corporate IT departments. You don't know tinfoil unless you've worked in a corporate IT department. Corporate IT is a technocratic pyramid built on paranoia, surveillance and fiefdoms of specialized knowledge and privileges (rights and permissions). Since all modern fascist organizations are essentially the same, I hope that my grim experiences within these organizations will help you understand more about the nature of the dire situation that we're all facing.

If you think that you're thinking outside of the box, my main purpose in writing this is to inform you that there are actually boxes within boxes, and that if you plan on engaging an opponent as powerful as the American Corporate State (or any other maniac fascist regime), it's not going to be easy. I don't know how many boxes within boxes there are. What I do know is that the U.S. Department of Defense built the underlying technologies that make the Internet possible. They built "this" world.

So, you want to be anonymous in a world that was thought up by the U.S. Department of Defense?

Most computer users don't have what it takes, in terms of technical skills, or discipline, to pull it off. I'm sorry if that sounds harsh, but it's absolutely true. I'm not claiming to be any kind of expert at all. If knowledge of computers and networks represented all the grains of sand on a beach, I'd say that I was familiar with about 5 of those grains of sand. I would like to hear from people who know more than me about any flaws in this information.

A long time ago, as a sort of theoretical challenge to myself, I tried to define a reliable protocol for remaining anonymous online. Why? Ask any nerd, "Why?" and the nerd will usually respond: "Why not?" If the nerd is unusually honest, he or she might respond, "Because I can't help it." So, somewhere between, "Why not?" and "Because I couldn't help it," I set out on this quest.

As you might already know, I studied information warfare in college and I did several years of time in corporate IT environments. I knew about the types of surveillance and control that are possible at the client, server and network levels.

I looked at the challenge as all IT people look at all IT related challenges: Assume the absolute worst.

I went even further with this. I made irrationally negative assumptions.

I assumed that everything I did online was compromised. I assumed the worst tinfoil nightmares about commercial operating systems. I assumed that my ISP was a subsidiary of the NSA, etc.

Got the idea?

Let's look at each level in a bit more detail (in no particular order):

Servers: Potential Honeypots

Many technologies that amateur anonymity fetishists are attracted to are actually designed to harvest information. Put yourself in the shoes of the NSA. If you wanted a concentrated haul of the most interesting information what would you do?

You would establish a honeypot: a service (free or paid) that purported to provide an anonymous web browsing/email capability. Who knows what people might get up to if they thought nobody was looking? That, of course, is the idea with honeypots.

If you're relying on a proxy server, how will you know that it's not simply recording your entire session for examination by acreages of the Homeland's supercomputers that are running advanced statistical Magic 8 Ball algorithms? Because the company or individual providing your proxy service says that they don't keep logs? HA

Am I saying that all proxies are run by the NSA. No. Am I saying that some number of them are. I'd bet my life on it. How many of them are run by governments? I don't know. Unless you know which governments are running which proxies, you must assume that all of them are compromised.

In reality, the NSA would probably be the least of your worries when using a proxy server or open base station.

Nerds with too much time on their hands get up to all kinds nonsense. Do they set up anonymous proxy servers and open base stations just to see what people do with them? Yes. Do criminals do it to find out personal information about you? Yes.

So even if the proxy or base station you're on isn't run by the NSA, who is running it? And why?

Maybe you're eLitE and use several proxies. You can probably assume that the proxies aren't colluding directly, but what about the networks? Which leads us to the next level…

Networks: If You Feel Like You're Being Watched, It's Because You Are

The network providers are keeping end to end records of every session. The question is: Are the network providers colluding with the U.S. Government? Since you can't assume that they're not, you must assume that they are. I would assume that the U.S. Government has end to end coverage of every IP session that starts and ends on U.S. networks. With corporate collusion and off the shelf hardware and software, this isn't a stretch at all. For non U.S. networks, the NSA gets in with multi billion dollar tools like the U.S.S. Jimmy Carter, and who knows what else…

There are dozens of off the shelf products that you would swear were designed for use by intelligence agencies, but they're routinely peddled to—and used by—corporations. If corporations have and use these surveillance capabilities, what are the intelligence agencies running on the service providers' networks? I'll be buggered if I know, but I know it's not good. That recent ATT/NSA thing is just a tiny/trivial tip of the iceberg.

Clients: NSA Side Projects?

Microsoft and Apple sought assistance from the U.S. National Security Agency.

Evil Corporations Working with the NSA + Closed Source Binaries = Not Good.

What is that thing actually doing? I don't know. Thank you. That's all I need to know.

Countermeasures

Access the Internet Using an Open Wireless Network, Preferably from Great Distance

In terms of a threat assessment, for our purposes, I see the networks as posing the biggest problem.

People write to me all the time raving about the dreaded Google cookie. HA. "We must use scroogle!" for freedom and safety, etc.

When I mention that their ISP is, most likely, keeping every URL that they visit in a database, at a minimum, and that NSA boxes are probably analyzing every FORM tagged submission, well, that's a hard lesson for people. Go ahead, use scroogle. Maybe the people running it aren't evil. So what. Scroogle might make you feel good, but it has nothing to do with security or anonymity, not when you consider the capabilities of the enemy on the network.

Give any 14 year old hacker access to the right network switch and, unless you know what you're doing, he or she will use a packet sniffer to find out what you had for breakfast. Now, the difference between most 14 year old hackers and the NSA is that the pimply faced kids don't have physical access to the network that would allow them to conduct man in the middle surveillance on you. The NSA does. Again, that NSA/ATT thing is fly fart level. That's nothing. That's just the piece of the program that got outed.

You need a false flag connection to the Internet. In other words, access the Internet via someone else's open wireless router, preferably from great distance. Lots of organizations, businesses and individuals provide free, wireless Internet access; on purpose, believe it or not. Ideally, you would use a cantenna or a high performance parabolic antenna to authoritatively distance yourself from any surveillance cameras that are likely saturating your local coffee shop or other business that provides free Internet access. Hitting the base station from hundreds of meters away would be nice.

If you were to carry the paranoia to an extreme level, you would assume that They would show up at your access point and use direction finding equipment to spot your physical location. "Tinfoil!" you say? Keychain WiFi access point finders have had crude DF capabilities for years. Then you have civilian grade WiFi network engineering stuff like the Yellow Jacket. Direction finding is as old as the hills and trivial to do. If you do happen to attract the wrong kind of attention on an anonymous base station, pinpointing your location would be a simple matter.

Solution? If you are playing this game as if your life is on the line, don't use the same open base station twice. Hey, this post is going out to those of you who send me the paranoid emails. You wanted to know, I'm telling you! I mean, it would suck to look toward your friendly anonymous WiFi provider with a pair of binoculars and see a guy in a suit looking back at you. Hint: if you see a van with several antennas arranged in some geometric pattern on the roof, that would not be a positive development. But that was 1980s era technology, the last time I dabbled with DF gear with a buddy of mine. Here's a nice little integrated soup to nuts solution that is probably more like what They would be using.

Surf Away: Just Don't Do Anything That You Normally Do Online

All of the stuff that you do with your "normal" online persona, you know, online banking, checking email, discussion groups, etc: You can't do any of that. The second you associate a user profile on a server with your behavior, you're back to square one. The Matrix has you. You would have to create what the intelligence business calls a "legend" for your new anonymous online life. You may only access this persona using these extreme communications security protocols. Obviously, you can't create an agent X persona via your anonymous connection and then log into some site using that profile on your home cable modem connection. To borrow another bit of jargon from the people who do this for real, full time, you must practice "compartmentalization."

If you actually attract the wrong kind of attention on a server, OR a network, with your agent X persona, if you haven't f@#$%& up in some way, all roads will lead back to the open base station.

"After connecting through the open WiFi network, should I also use an anonymous proxy?"

I would assume that even if the proxy is clean, and there is no way to know that it is, They will have that thing covered on the network, end to end. Physical disassociation from the access point is the best proxy.

Client Side

Never write anything to disk. Oh, you weren't planning on using your Windows or MacOS laptop with all of those closed source binaries whirring away, were you? Man, I don't know where you got your tinfoil hat, but that thing is obviously defective.

You will have to learn about Live CD distributions of Linux.

You boot that thing. Do your business. Turn off the computer. Nothing is written to the hard disk.

"But I need to save my work?"

If you want to save your work, the easiest way of routinely handling encrypted workflow is to use an encrypted volume and a tool that only decrypts your data on the fly, in RAM. The best tool I know of for handling encrypted volumes is TrueCrypt. Hint: Use cascading encryption algorithms. Do They have some technology, in an underground hanger at Area 51, that's capable of breaking one of those cascading crypto schemes? I don't know. I doubt it, but anything is possible when infinite budgets are involved.

Hey, man, you wanted to save your work, right? That's the score when you've got half a role of Reynolds WrapÂ® Aluminum Foil around your head.

"But I need to send email."

For our purposes here, I wouldn't. Email is locked down and heavily surveilled, partially because of the plague of spam, but read on…

I don't believe in web based email solutions that purport to provide strong encryption and/or anonymity. Who knows what their applets and servers are doing? Not me. And if they rely on SSL, well, that's ok for buying a book online, but no tinfoiler in his right mind would bet his life on SSL. The Thunderbird/Enigmail/GPG solution is the best way to send and receive VERY secure email that I know of. But will your agent x persona be able to deliver email via SMTP? I wouldn't count on it. And from which domain? Unless you are very naughty, you shouldn't be allowed anonymous access to a SMPT server anyway.

You might have to go with a throw-away web based email account and then cut and paste your encrypted messages into that. As a rule, however, never compose a message that you plan on encrypting in a web based form. Some of them use technologies that transmit what you're typing over the web AS YOU TYPE. This is so you don't lose what you typed if the session cuts out, but guess what? That's right, you just blew it.

Use open source tools that are running locally on your system to encrypt and decrypt messages.

An effective way of communicating with someone, outside of email, would be via newsgroup or bulletin board that allows anonymous posting. (Note: If you try it here, I’ll just delete it.) You are, in effect, using the board as a numbers station. You’re not trying to hide the signal. You assume that it will be intercepted. You encrypt your message to the recipient, using his/her public key, and post the ciphertext to the board. The recipient goes on there, copies the message and decrypts it. I first encountered this in the mid 1990s on usenet. Of course, the person on the other end needs to have the same level of discipline and paranoia as you for this to work properly.

Last but not least: Make sure that you spoof your MAC address EVERY time you go online. Funny story: I worked at a place that was locked down to the point that every MAC address was screened at the network level. Say, for example, that someone brought in a personal laptop from home, even though there was no chance of being able to use the network for much (domain sign on was required) the switch would alert a sys admin indicating that an alien device was plugged into the network, along with the jack/cube/desk number.

MAC addresses are unique, and perfect for surveillance purposes. Always spoof your MAC address when you’re running in agent x mode.

Well, that’s pretty much it. (Actually, I’m tired of typing.) I didn’t say it was going to be easy, and you should watch out for people and products that make those claims.

Of course, evil people could use the above techniques to do evil things, and that is the argument that the government will use to convince you to submit to total surveillance of everything you do.

In case you’re curious about how I get online: I use Windows XP on a five year old laptop, from home. While I’m running two firewalls, there’s no onion routing, proxies, live CD operating systems and I don’t bother with spoofing my MAC address. If you use a bank that knows where you live, They know where you live. Since I’m forced to use such a bank, I don’t bother with the rest. The Matrix has me.

If you think being anonymous online is hard, try living without a bank account…. Sorry, being homeless in a city park doesn’t count.

Oh yeah, what about Tor…

HAHA. Imagine my shock.

Via: tin0.de:

A group of 9 Tor routers also functioning overtly or indirectly as Tor exit nodes have been observed colluding on the public Tor network.Due to the sheer amount of traffic apparently passing through this collusion network, consolidation and analysis of exit node traffic is only one of several forms of anonymity attacks made more feasible. Hence these 9 routers appear to pose a significant anonymity threat to users of the public Tor network.