Living securely in the new age

Guy Van Sanden

“A long time ago, in a galaxy far away... The galactic empire has seized control of the planet's global communications network, called The Internet by the native species, allowing it to intercept all communications worldwide. A rebel force got it's hands on the blueprints of the empire's interception equipment through the sacrifices made by a rebel spy who, if caught, faces a lifetime in prison, probably torture and maybe death”.

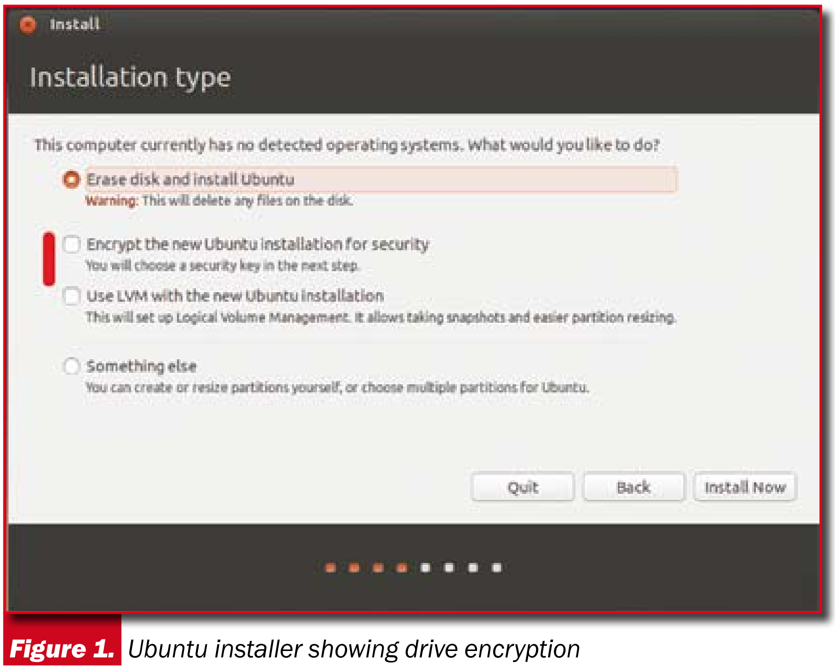
It sounds like a movie plot from Orwell meets Lucas, it could be directed by any good action flick director, but it's real life on planet earth in 2013. A “rebel” has indeed given the world the blueprints of a massive surveillance device build by the shadow government of a totalitarian regime and misused by private corporations. If you are an activist of any type, be it political or environmental, if you are a journalist or even a union leader or any citizen with an opinion, you should be concerned.

A very smart man once wrote that no political fraction should ever be granted the power you wouldn't want in the hands of the worst regime you could imagine. The solutions to this may be political by nature as the problem itself is, but this will take time (and coordinating changes over a compromised network would be insane).

But technology does hand us enough tools to secure our communications and our private lives from governments, companies and criminals, even the ones that are above the law. The answer is interestingly enough only to be found in switching to Free Software. So, if you are running a GNU/Linux system, you are already one step ahead.

The Snowden files showed us a lot of things, some more surprising than others, but the level of cooperation by closed source vendors of security technology and operating systems that they identified clearly demonstrate that none of them can be trusted and their products can be riddled with backdoors or made more vulnerable to allow wholesale surveillance unfettered access to any system.

Privacy is not dead, as it has been suggested, it is within reach for everyone willing to put an effort in to it. But as with any type of security, it will mean compromising on comfort. It requires being intentional about using technology securely and about avoiding obvious holes



Installation type

This computer currently has no detected operating systems. What would you like to do?

● Erase disk and install Ubuntu
Warning: This will delete any files on the disk.

□ Encrypt the new Ubuntu installation for security
You will choose a security key in the next step.

□ Use LVM with the new Ubuntu installation
This will set up Logical Volume Management. It allows taking snapshots and easier partition resizing.

○ Something else
You can create or resize partitions yourself, or choose multiple partitions for Ubuntu.

Figure 1. *Ubuntu installer showing drive encryption*

in ubiquitous public services. If you are serious about it, it will change the way you think about technology.

Every modern-day Linux distribution offers you the tools you need to secure your private life, but they have to be used in the proper way. This article will get you started with the basics and point out some more advanced techniques to introduce operational security in to your live, you can pick and choose to which level you implement it, if at all.

Operational security 101

Applying operational security to your everyday computing tasks may be new territory for most people. It starts out by doing a risk assessment on your data. What data do you use, what are the implications of loosing control of it, who would want to steal this information from you? From this you make a very rudimentary threat model that can be used to outline your defenses.

The important base to start from is to design your security without obvious holes and to build it in layers that still hold if one layer in the system fails. Trust is an essential part of security, but mistrust is also the greatest threat to it, so be very careful with trust and avoid trusting parties that have proven themselves untrustworthy (though it seems obvious, many people keep trusting companies with private data despite them having the worst track record imaginable).

Public vs private

If anything, the revelations by Snowden have confirmed what any decent security professional already knew, *there is no such concept as privacy once information moves outside your control*. That means that you should never trust privacy controls implemented by third parties to protect your data. The only way to make this manageable to yourselves is to think about privacy levels in simple terms like public and private. If something can not be made public to the entire world, it should not go beyond the people that actually need to have it. This concept has implications to how we deal with information online as you should only share things on sites like Facebook or Google that you wouldn't mind to end up in your local newspaper, regardless of the privacy switches they put in you profile.

This applies to status or location updates, but also to files you put on cloud services. Anything that leaves your control is potentially public. If your are a journalist or political activist, this goes even more so for you, treat all public services as compromised as they most likely are. If you must store files in any of them, encrypt them first.

The basics

To start building any security, you need to make sure that so-called endpoints are secure. This means making sure that it's hard to get to data on your devices. Today, it's quite easy to do that as most systems have the capability to fully encrypt storage devices. If you use Ubuntu (as well as most other Linux distributions), you can select whole drive encryption during the installation. Again, if you are protecting against a more capable adversary, you need to shun any closed source encryption products, including encryption functions built in to many modern hard disks. But the technology built in to Linux is safe.

Make sure you choose a strong key to encrypt your drive in addition to a strong password to log in. Oh, and for heaven's sake, lock your systems when you walk away from them, make it a habbit.

Without encrypted storage, securing data transfers will often be futile. And of course, physically traveling with unencrypted data is never smart and one of the most common mistakes.

With your data sitting securely on an encrypted drive, it's time to start dealing with online communications, which is much harder to do securely. Again, freely giving out access to private information on social media for example defeats any purpose of securing it. The best thing would be not to use any of these networks, but if you do, think about how you use them.

Going online

E-mail

A lot of people online communications happen via E-mail. E-mail is a fossilized communications protocol with no hint of security in place. It's often compared to sending a letter, but in reality, it's worse. E-mail offers the same level of security as a letter sent without an envelope. Both the content and the metadata (sender, recipient, timestamp) are visible to anyone that can access the path it travels. Don't be fooled by the https icon your webmail shows you, this only encrypts the path from your browser to the server of your mail provider, nothing beyond that and even https cannot be fully trusted any more (as both certificate signers as big mailproviders provide backdoors).

When it comes to E-mail, the only part you can actually secure is the content, metadata like from, to and subject will always leak unless you are both within the same and secured mailserver. Securing metadata as well as content will require a different technology (or a shared, secure, dedicated server between sender and recipient).

To secure your E-mail communications, (Open)PGP is your best option as it does not rely on trusting intermediary parties. OpenPGP is offered by default on Ubuntu through GPG and can be used to sign and/or encrypt both mails and files. Ubuntu installs seahorse by default, which is a nice graphical utility to manage keys and sign or encrypt content.

OpenPGP employs a technique that breaks a key in to two parts, one part public that can be used to encrypt data or verify signatures but carries no value beyond that. The other part is private and can be used to sign data or to decrypt secure files. If you generate such keys, do so on a secure machine and set the key size to an increased value (4096 bits is a good start).

The weakness in using E-mail encryption is that most receivers are not set up to use it, which is a big hurdle to cross. Encrypting every mail you send would be ideal (and would significantly raise the cost of wholesale surveillance), but it's hard to do and some recipients will refuse to bother with it.

But if your threat model identified data that is important enough not to send it in the clear, you could make the effort to get the other side set up or just choose to send the data in another way, which will involve encryption anyway.

Surfing

Browsing the Internet leaves a lot of traces, if you truly want to be anonymous, you'll need to use TOR (which we will get in to a bit later in this article). But even your average browsing sessions can be made more secure.

To avoid centralized tracking, you need to set some options in your browser. "Do not track" is a start but it is ignored by a lot of trackers. Disabling third party cookies makes sense as well as making flash only run on whitelisted sites (FireFox 24 in Ubuntu handles this very well). Flash cookies can be used to track you when normal cookies don't do the trick and there's no good way to avoid that beyond avoiding flash itself.

Secondly, if you are logged in to networks like Facebook or Google, they can track any other sites you visit, so only use those services in another browser (or a clean profile) and keep them separate from your normal browser profile.

If you have to log in to services or submit any private data, do it only on https sites, which is better than sending it unencrypted even with certificate authorities compromised.

TOR

The Onion Router or TOR is a system that routes data randomly through virtual tunnels over several nodes that are connected through encrypted connections. The goal is to prevent the endpoint form being able to identify the source of the data.

On the TOR website, you can easily download a bundle consisting of both the TOR program, hooking you up to the network, as a Firefox browser preconfigured to make full use of it.

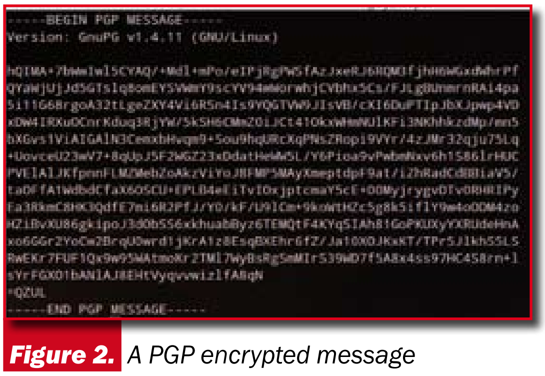
Even though there have been successful targeted attacks against TOR users, mainly exploiting browser vulnerabilities, TOR itself remains unbroken. In fact, Snowden's files show an NSA slide stating that they cannot break TOR and they have to jump through significant hoops (and rely on user mistakes) to get info on a single target.

But keep in mind that TOR does not alter or anonymize your data itself, if you send an unencrypted mail over a TOR connection, it will still be readable on the mailservers it passes through.

Being a target

If you suspect that you are being targeted by any government surveillance (most competent investigative journalist should consider themselves in this category), you should of course apply all guidelines above. But it will not suffice as you are defending against an enemy with resources the size of a planet. So, in addition to applying all the rules, you will need techniques and self discipline that would make some paranoid movie-plot computer geek think you are crazy.

If you fall in to this category, most of the technological wonders that assist you every day become your worst enemy. Cell phones leak your location, possibly even when turned off and can be used to record conversations. So leave them home when doing sensitive work. Buy an unlocked device for which there are open source firmware options available and install them (for example CyanogenMod for Android).



```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

hQIMA+7bWw1w15CYAQ/+Wdl+mPo/eIPjRgPW5fAzJxeRJ6RQMIfjhH6WGxdWhrPf
QYaWjUjJd5GTs1q8omEYSVWmY9scYV94wWorwhjCVbhx5Cs/FJLgBUnmrnRAi4pa
5i11G68rgoA32tLgeZXY4Vi6R5n4Is9YQGTVW9JIsVB/cXI6DuPTIpJbXJpwp4VD
xDW4IRXuOCnrKduq3RjYW/5kSH6CMmZ0iJCt41OkxWHmNUlKFi3NKhhkzdMp/mn5
bXGvs1ViAIGAlN3CemxbHwqm9+5ou9hqURcXqPNsZRopi9VYr/4zJMr32qju75Lq
+UovceU23wV7+8qUpJ5F2WGZ23xDdatHeWW5L/Y6Pioa9vPwbmNxv6h1S86lrHUC
PVEIAlJKfpnnFLMZWebZoAkzViYoJ8FMP5MAyXmeptdpF9at/i2hRadCd8BiaV5/
taOFfA1WdbdCfaX6OSCU+EPLB4eEiTvIOxjptcmaY5cE+OOMyjrygvDTvORHRIPy
Fa3RkmC8HK3QdfE7mi6R2PfJ/YO/kF/U9lCm+9kowtHZc5g8k5ifIY9w4oODM4zo
HZiBvXU86gkipoJ3d0b5S6xkhuabByz6TEMQtF4KYqSIAh8iGoPKUXyYXRUdeHnA
xo6GGr2YoCm2BrqUOwrd1jKrA1z8EsqBXEhr6fZ/Ja1OXOJKxKT/TPr5J1khS5LS
RwEKr7FUF1Qx9w95WAtmoKr2TMi7WyBsRgSmMIrS39WD7f5A8x4ss97HC458rn+1
sYrFGXO1bANIAJ8EHtVyqvvwizlfA8qN
=QZUL
-----END PGP MESSAGE-----
```

Figure 2. *A PGP encrypted message*

Generate and use encryption keys on a computer that has not been physically connected to the Internet (called an air-gap). Transfer encrypted files to and from it from your Internet connected computer using USB sticks. Set up the Internet computer you use for your sensitive work with TOR and use another computer to do your normal online tasks. Ideally, run your TOR browser bundle from a Live CD to prevent it from being infected with malware.

If you carry devices like a phone, USB stick or laptop when traveling, make sure they are encrypted but also encrypt the data files on them separately with another technology. Only carry data you actually need and, if possible, make sure you don't have the decryption key on you (or you don't know the passphrase) to prevent from being forced to decrypt drives.

Should your device be taken from you for even two minutes at any point, dispose of it afterwards (yes, this is expensive. If it's something like a laptop, physically trash the drive and sell the device). Making even the smallest mistake will defeat any of the measures you took so far.

Conclusion

For the average user, staying mostly private online is not that hard. The techniques outlined above may seem a lot of work, but once you have the basics in place, it won't be much harder to use computers than before. Actually, some things become easier as loss of a device with data on it will no longer require costly recovery options like canceling credit cards and rotating passwords.

Now, if you think you are a target and you want to defend against a government targeting you, it does get hard.

But as wholesale surveillance has put unprecedented power in the hands of the attacker, encryption technology has put unprecedented defenses in to your hands. The fact that people like Snowden can use computers to coordinate with journalists in other countries, the fact that they can transport USB drives across borders means that these technologies work. ■