

1 Introduction

I have noticed an increased trend in the use of full disk encryption recently, especially among Linux users. However, this growing trend is not entirely a good one, many users are treating full disk encryption as a panacea, thinking it invulnerable and wholly trusting the security of their data to it. I have taken the time writing this paper to address this dangerous line of thinking, and to suggest ways to fix the most common flaws with full disk encryption.

Unfortunately, I do not have the time at the moment to write detailed guides to enact my solutions, so I will leave this as an exercise to the reader and the community in general. It's important to note before continuing that this paper is discussing the flaws common to full disk encryption, if you do not use full disk encryption than your data is already vulnerable, and it would be wise to take the steps necessary to protect it.

2 Why your data may already be compromised

I will kindly ask you to examine the following list, and see if one or more of these items fits your computer's usage and environment.

- My kernel is stored unencrypted on an internal drive
- My system has a firewire port
- I leave my system alone (even occasionally) without shutting it down
- I leave my system alone after shutting it down without a second thought

Now, if any of the above items apply to you, your use of full disk encryption is nothing more than a false sense of security, anyone who really wants access to your data has multiple ways to access your encryption keys, and in some cases your data directly!

3 The World Ends With Your Kernel

What is the most important piece of software on your entire machine? Your kernel, of course, followed by your bootloader, which is responsible for loading the kernel in the first place. Your kernel is God on your machine, it handles disk and network I/O, access to memory, multitasking, everything that allows your software to do its job. Having such power comes with great responsibility: the kernel can do whatever it wants, including sending your encryption keys, passwords and passphrase's to some unsavory party.

But you don't have to worry, right? You use full disk encryption after all, don't you? Well, here's the common misconception, your disk isn't actually fully encrypted, your kernel has to be stored somewhere unencrypted for the bootloader to access it. Yes, that God-like piece of software that controls every bit of information passing through your machine is sitting there, unprotected. It's no difficult task for someone to install a modified kernel that sends your encryption keys to them, and then your efforts to secure your system were in vain.

So why can't we just encrypt the kernel? Simple, then the bootloader would have to decrypt it, which means security falls onto the bootloader, and that could just as easily (if not easier) be modified and replaced as your kernel. Above the bootloader, what is there, your hardware? You can't very well trust your hardware to encrypt your bootloader, since that would essentially prevent installing anything but the bootloader that came with your machine, tying you into whatever OS it came with. Yeowch, we don't want that.

So if we can't leave security up to our machines, is there no way to have a truly secure system? Are we doomed to using full disk encryption in vain for the rest of time? Fortunately, no, and it goes back to an old computer security adage: "there's no security without physical security."

To keep our data safe our kernel must be physically guarded, along with our bootloader. To keep your kernel and bootloader physically secure, without needing to watch your PC 24/7, we need a way to carry them with us. Fortunately, most (if not all) PC's today allow booting from USB flash drives or external USB hard drives. This means we can store our kernel and bootloader on a cheap flash drive that we carry with us. If this God-like piece of software is on you at all times, no one will be able to secretly slip a modified version into your system. How about that?

If you lose your flash drive, or it is stolen, you can simply reinstall the bootloader and kernel on a new one and continue on with life, since it's likely that your old one has been compromised if it shows up again.

4 Firewire Needs a Firewall

It's quite unfortunate, Firewire was designed to be a high-speed data bus for connecting digital video/audio equipment and external storage devices, but today it is almost nothing more than a gaping security hole to your system. Firewire allows host and guest devices to access each others memory directly using DMA or Direct Memory Access, this means a Firewire device plugged into your system can access your system memory and create a dump of it, likely snagging your encryption keys for your disks in the process. Even worse, they could modify your kernel in-memory or on-disk if the person trying to access your data is clever enough.

This makes Firewire a very easy vector for attackers to access your data, and if you do not make use of the technology I suggest you disable it in your systems BIOS or blacklist the kernel module.

5 RAM Remembers When

Another vulnerability most people don't know about is less obvious than the gaping hole in the Firewire specification. Did you know that DRAM does not reach a full discharge immediately after it loses power? Also of note, when DRAM is frozen it will retain its charge for a prolonged period of time. Put simply, this means two things: an attacker can freeze your memory to keep data such as encryption keys 'live' long enough that he can plug it into a new power source and make a dump of it; but they can also do it shortly after your

machine has shut down since data will remain in RAM for about a minute at the least before it starts discharging.

Thankfully, the Linux disk encryption provided by dm-crypt bit-flips the keys it uses in memory constantly, preventing your system RAM from building up a large enough charge to store the key for more than a minute or so. But you still have to worry about other data that may be in memory, like your unlocked SSH keys, or a top-secret document. If you must leave your machine alone, you should shut it down and keep an eye on it for at least a minute to make sure no one attempts to freeze your RAM when it is most vulnerable.

6 Conclusion (Perfect Security Doesn't Exist)

Unfortunately, it's a fact of life that nothing is perfect, and perfect security doesn't exist either. In fact, security is only as strong as we are, and it's extremely easy to overlook little holes that may give someone unauthorized access to your data. This is why it is important to be vigilant and read up on any security measure you use, and make sure you use a combination of them (but don't go overboard, you'll just make it harder for yourself to access your data, which is not the goal of security).

I hope this paper has informed you of some risks of using full disk encryption alone as a security measure, because while it does help, it is not a security panacea and should not be treated as one. Always ensure your kernel is protected or you might as well not have any security at all.