

Forum:[Hack Forums](#)

Thread: [Let's Talk About Security... \[WIP\]](#)

FractumSeraph - August 31, 2016, 11:58 am

Alright, so this post is just going to be a huge spill about security practices and things like that. I plan on organizing this and making it look pretty, but right now I'm more focused on just getting all of my thoughts on paper, err, typed. If you see any information you believe is wrong, or anything you think should be added, please let me know.

There will maybe someday be a section here on why security is important. But for now, just trust me when I say that it is. Hopefully you know that.

Mobile

I'm starting off with mobile devices simply because you're probably read a million things about how to secure your computer. If you haven't, don't worry because I'll make a section for that too. I've mainly used android and iOS devices, so if you use windows phone or blackberry (or whatever else) you'll have to wait until I get more information.

First things first, your screen lock.

Vital when talking about physical access. This is probably the downfall of many users, since most people think a four-digit passcode is actually useful. It's not. It might stop your little brother from "hacking" your Facebook, but that's about it.

You need to realize that your cell phones password needs to stand up to a desktop password. Think about it. They are just as easy to hack and bruteforce, and [they contain a huge portion of your personal life](#). I'll provide a few links here showing examples, but for now I'm sure you can guess. Pictures, GPS data, times to go with your GPS location, emails, contacts, messages, etc. And what's more, your phone can be used to get whatever else someone might want. Let's use Twitter. Let's say you don't have Twitter on your phone, you're not signed in, and you haven't reused that password. Well once someone has access to your phone, they just have Twitter send them a security code to your number and they can reset your password. (https://twitter.com/account/begin_password_reset) And notice I said your number, not your phone. Even if your phone is encrypted to hell, an attacker could pop out your sim and stick it in a new one. If they have the right information, [they don't even need access to your phone to do this](#). Suddenly all your texts and calls are going there. Also don't forget, a lot of apps such as Telegram, WhatsApp and Authy use your phone number as your login, requiring nothing else to use unless you set a secondary password.

Obviously, your phone is important to secure. So how do we do that?

Like I was saying, it's vital that you have a strong password. For androids, use the highest amount of characters your device will allow. I think it's around 16 or 18. This needs to follow your standard guidelines. (Numbers, uppercase, lowercase, symbols...) If you're on iOS you're in luck. My iOS password is currently 40+ characters, and I have no idea what the max is. You may want to check out [this website](#) to test the strength of your passwords. Everything is done offline so [you don't have to worry about your password being sent anywhere](#).

Now we need to make sure this password actually does something. For androids, this means

[encrypting your device](#). If your device is encrypted, bypassing the lock screen or dumping your data to a computer won't get them anywhere, since the attacker would still have to bruteforce your password.

So at this point we have our device encrypted, and we have a hella strong password. Invincible right? No.

There are still a few more things to worry about.

I'm just guessing here, but I'd bet that most iOS users are likely to have iTunes installed on their computer. It's what you used to copy songs over and restore your device if it's broken. It's also used to make backups of your devices. If you have a 64000-character password, it will do you no good if [all your data is setting on your PC ready to be copied](#). Yes, you can encrypt your backups if you choose to, but again this can be bruteforced. If your device is being backed up to [iCloud](#) or [Google Drive](#), then it's at the mercy of whoever has access to your account. And as I mentioned before, your accounts can be taken extremely quickly if someone has access to your phone number.

Alright, no insecure backups, got it.

What's next?

Well now we need to look at a few more things. Is your device rooted or jailbroken? Are you using [developer mode/ADB](#)? This can be bad. Now keep in mind that in android's case, if you know what you're doing root can be a good thing. But it can also be bad as well. For iOS devices, I would never recommend jailbreaking if you're worried about security at all. Jailbroken devices and root provide full access to everything. [Invisible backdoors could be installed](#). Your files can be copied. Antivirus disabled, etc.

You should also learn about [Cellebrite](#). Cellebrite is a tool used to break into devices, it's has a bunch of different ways to get into your devices. I've never owned or used one, so I'm simply going off of what I've learned from reading the [manuals](#). The first mode uses your devices built in functions to basically ask for all of the information it needs. This is why it's important to disable backups and developer tools as well as keeping your device unrooted/jailbroken. The second mode just copied the files from your device. Just like if you plugged in a flash drive to your computer and copied the contents to a folder. The third mode is a full forensic bit-by-bit extraction (Meaning it can probably see your deleted files too.). The third mode will not be stopped by anything we've done above; you have to rely on the strength of your password verses the computational power of your attacker. There's a bunch of other specific functions this thing can do, but for now I'll just stop here. The other functions include a password grabber, sim cloner, and various developer tools. The most important thing about this tool is that it can bruteforce your password even if you have a self-destruct set. For example, on androids and iOS there is an option to wipe the device if an incorrect password is entered ten times. This tool can bypass that. The only [exception](#) that I am aware of is iPhones that are 5S and above. These devices have a thing called Secure Enclave, which prevents the tools from bypassing the self-destruct. However, your devices have to be fully updated and non-jailbroken. If your device is jailbreak-able, Cellebrite can jailbreak it and bypass the password.

I've been on that topic for a while now, so I'm going to move on before my brain fries. I'll go back to it later. For now, let's take a closer look at your phone settings. I no longer have my android device, so I'll start with iOS until I get ahold of one. I'll just go down the list and point out settings I deem important.

iOS settings to watch out for

Click this if you use iOS ([Click to View](#))

I plan on having an entire section dedicated to Wi-Fi, so I'll skip that for now.

One important thing to do is to make sure that the control center is not accessible from the lock screen. This is useful to prevent an attacker from putting your device in airplane mode. If your device is in airplane mode, then remote wipe functions become a lot less useful. Just make sure to take care of your notifications if you do this.

On the flip side, if your device is in airplane mode then your device will be unable to receive calls that might give away details such as your contacts. You will also not get any notifications that may contain personal information. It's up to you to decide which option is best for your situation.

Turning off Siri will help stop your phone from collecting a ton of information about you. And also prevent it from being used in the lock screen.

Turning off HandOff will help stop attackers from gaining information if they have access to your iCloud account.

Touch ID can be very useful if you have an extremely long password such as mine, but keep in mind you can be physically forced to unlock the device if someone is physically with you. If typing a long password is a bother, consider setting the auto lock time fifteen minutes or an hour. If you manage to get an early warning, you can turn off your device in about five seconds which will require a password on boot. Yes, this is a security risk, but I understand most of you won't use a long password without touch ID any other way.

Be careful about using share my location for obvious reasons. While your phone could be tracked with it off, it would be much easier for someone to track you using a friend or family members phone. iCloud needs to be off. End of story.

On phone settings, make sure to set a SIM pin. This will help prevent your sim card from being used by an attacker. You will most likely have to call your provider to get your PKU, but afterwards you can change it.

iMessage uses end-to-end encryption. More on that later, but basically you don't have to worry about leaving it on, however you might want to disable read notifications for plausible deniability.

For your safari settings there isn't all that much you can do. Set your search engine to DuckDuckGo, don't save passwords or autofill, set do not track, disable cookies and JavaScript if you can afford to.

Apps

Don't use [Facebook](#), Twitter, or any other social media. I recently did the "Download your data" thing on Facebook. I eventually got a link to a .zip file containing all the data Facebook had from my profile. [The contents](#) were so creepy I immediately [deleted my Facebook](#). I won't go in to details since I'd prefer you to see for yourself on your own account.

Now that that's out of the way, let's talk about some apps you should be aware of. This list will include apps for both Android (A) and iOS (I).

Authy ([Click to View](#)) (A) (I):

This is a manager for 2FA. The main benefit you gain is that you can set a password for your account. This way if an attacker gains access to your phone/sim/number, you still have a layer of

defense. Besides, if you're not using 2FA on your accounts, you need to start. Just make sure to write down the codes given as backups. Keeps them somewhere safe. Dig a hole or something.

BoxCryptor ([Click to View](#)) (A) (I):

This is used to secure cloud storage. I was given about 200Gbs of storage on Microsoft OneDrive. Great right? Not really, considering Microsoft would have full access to whatever I stored there. This is where Boxcryptor comes in. It basically encrypts everything on your devices before it is uploaded to the cloud. You might also want to check out SpiderOak if you don't mind spending some money.

ChatSecure ([Click to View](#)) (A) (I):

This app makes use of XMPP and OTR to provide secure chats. The app itself is password protected, which is important in case an attacker is able to get past your phone lock.

OpenKeychain ([Click to View](#)) (A):

A PGP manager for android. If you don't know what PGP is, you should definitely [do some research](#). I'll make a section over it, but don't wait on me.

ProtonMail ([Click to View](#)) (A) (I):

If you're using Gmail or some other mainstream email provider you need to stop. Use a more privacy focused provider such as ProtonMail. ProtonMail automatically handles PGP encryption, our emails stay encrypted on the servers, and the app itself is encrypted. Another alternative is RiseUp.net. While RiseUp doesn't have as many security features, they are still privacy aware. [Unseen.is](#) was recommended by another user below and appears to be much like RiseUp.

Signal ([Click to View](#)) (A) (I):

This is a really great app because it allows non-technical users to use encrypted chat. It's an SMS client, and on Android it can be a full on replacement for your texting app. Using this app, messages to other Signal users are automatically encrypted without requiring any sort of setup. Optionally, you can add a password to protect your messages if the lock screen is bypassed. As an added bonus, the app supports encrypted voice calls.

Telegram ([Click to View](#)) (A) (I):

This app is a bit more like a traditional instant messaging app. In pretty much every way really, it has everything you might expect. Friends, Group chats, Reachable by number or Username. It's basically Kik. It also has an optional Secret Chat mode. This mode adds end-to-end encryption and other security features such as self-destructing messages. This app uses the Signal Protocol from the creators of Signal. Again, don't forget to set a password.

VPN Apps ([Click to View](#))

I won't list them here, since there are way too many, but make sure to use a VPN. 99% of all VPNs keep logs, even if they claim they don't. But even so, this is another layer of defense, and will help prevent mitm attacks on your network.

Wickr Me ([Click to View](#)) (A) (I):

I don't see this app used as much, but it has a few of the features telegram offers. It's password protected, encrypted, and has self-destruct timers. The main reason I have this app installed is for the Secure Erase feature. If you're on android you can do this with a billion other apps, but the iOS market doesn't have any alternatives. Use this feature to help prevent forensics from recovering deleted files.

Another user has also suggested this [\\$40 eraser for iOS](#).

I'm sure I've forgotten some apps, but that's why this is a work in progress. Stay tuned.

For now, I'm going to work on the PC section a bit. And since this post is too long:

[Click here for part two!](#)

~ **Left HF For Good** ~ - August 31, 2016, 1:40 pm

Just skimmed through here, and phew is there a ton of information in here.

I am posting to come back to this later. Amazing tutorial OP, keep it up!

Lucent - August 31, 2016, 2:20 pm

A lot more people need to see this, you'd be surprised how many people don't know about these simple tips.

Very informative, good job OP!

Northlam - August 31, 2016, 4:51 pm

Another email I would suggest is unseen.is. ! they have alot of anonymous features and secure voice and chat as well, similar to signal but a web application. But great read! Glad I found out about authy :)

FractumSeraph - August 31, 2016, 5:40 pm

PC

The majority of the people reading this are probably windows users so I'm going to focus this guide there. Windows 10 specifically.

If you're wondering why not windows 7 since you don't have to worry about the spying

News Flash: [The spying stuff in Windows 10 has been back ported into Windows 7](#). Might as well just upgrade.

BIOS

We're going to start off with booting your machine. Ideally, whenever you're attacked, your machine will be offline. Please remember that if your machine is running and unlocked when it's compromised, neither BIOS settings or full disk encryption will help you.

Whenever your PC first turns on, it will go through BIOS. Since it's the first thing that happens, it's the first thing we will secure. There are many different BIOS options, and not every device has the same one. So You're going to have to use some common sense if yours is different.

Also, the majority of BIOSes can easily be flashed to default settings, so it's important to not rely on this by itself.

The first thing we want to do is add a boot password. (Sometimes called a user or system password) and an admin password. A user password will prevent people from accessing your device, and an admin password will prevent changes to the BIOS settings. The main goal of this is so people can't change the boot order and allow booting from USB/CD drives.

On that note, you're going to want to change your boot order/priority to make your laptop hard drive boot first, and disable booting from anything else. It's important to completely disable the rest, since an attacker could remove your hard drive to force the machine to boot from another device, then simply reconnect the hard drive after booting.

You'll want to disable options such as recovery and ones that store the BIOS on your hard drive. If your computer has it, you'll want to enable hard drive locking. This password protects your hard drive. One other thing to note about this is that a lot of Dell laptops (and maybe more) have a special built-in password that securely erases the hard drive if the password is entered. Much like a cryptonuke that I'll talk about later. I have this "delete everything" password written down on a

piece of paper and "Half-hidden". If someone looks at my desk they will see the sticky note labeled "HDD0-SE". And since the password prompt says HDD0, they will assume this is the password. They will try it, and then all my data is deleted.

Next, be sure that features such as secure boot and anything else mentioning security are turned on. The only exception to this are tools such as LowJack and CompuTrace, which need to be disabled.

FDE

After BIOS, your computer would normally load your operating system. But we want to encrypt that in order to keep our data safe if your device or hard drive is stolen.

Depending on what operating system you're using the process will be different.

For Windows, you'll want to use [VeraCrypt](#) to encrypt your system partition. Make sure to use a PIM to make your password two-dimensional. If you're feeling adventurous, try using a hidden operating system. You'll have to disable secure boot to use VeraCrypt, but this won't be a problem since you've looked the boot order and encrypted your hard drive.

Windows does support Bitlocker, but this is closed source, and is also [vulnerable to lots of attacks](#). And depending on how you set it up, there is a strong chance that Microsoft will have a copy of your recovery keys. Not to mentioned you need a TPM module or USB alongside your password.

For Linux, you'll want to set up LUKS encryption. And make sure to [add nukes](#).

Looks hard, but I promise it isn't. [\(Click to View\)](#)

After your device is encrypted with luks, use this command to add "delete everything" passwords: `cryptsetup luksAddNuke /dev/sda5`

What are nukes? Just like before with the secure erase password, these are special passwords that will wipe your encryption headers when typed in. My Kali install is using all 8 keyslots. I have one really long and complicated password that will unlock my device. I have seven more passwords that will delete everything.

Make sure to put the letter "A" as a nuke, and "AAAAAAAA", as this will help ensure that bruteforce attempts destroy your data. For the five remaining keyslots, I use passwords that I have previously used, that way an attacker who has been following me is likely to try it to see if I have re-used the password.

I'm not sure what options are available for a Mac, as I don't use them.

Hardening Windows

So now we focus on the actual windows installation itself. Here we try to make it harder to break into.

The very first thing you need to do is reinstall your OS. I get it, that probably sounds pretty cumbersome, but I do it multiple times a month and it's not nearly as bad as it seems. Besides, if you're already compromised before we begin then this won't do you much good...

So now you have a fresh installation, and you made sure to turn off all spying stuff when you were installing it. Once you have Windows fully loaded and running, we're going to want to get rid of stuff. (Like why TF does the Candy Crush and Sports apps come with it? I have zero (0) interest in either of those...)

To do this, we will use tool called [Decrap My Computer](#). This will go through and get rid of all the software that's been added on top of windows.

Then of course you're going to want to use some of the [many programs](#) to help stop the spying telemetry.

There is a really nice [website](#) that has a walk through showing you how you should have your windows installation set up. I'm not going to lie, it's long and tedious, but if you're serious about this you should give it a shot. Maybe at some point somebody can automate it. The trick is balancing security with usability.

This mainly comes down to things like disabling services, setting very strict firewall rules (whitelist mode, not blacklist), and running everything in sandboxes.

It does mention a few programs you should check out, but really the ones I would recommend are [MBAE](#), [Sandboxie](#), and a good antivirus. Also, if your antivirus doesn't have a built in firewall, you'll definitely want to [get one](#).

[Part Three!](#)

3azraiell - August 31, 2016, 5:45 pm

good job bro i have learned things but already know thank you anyway ;)

~ Left HF For Good ~ - August 31, 2016, 6:06 pm

Just seen you added more, keep it up man. ?

FractumSeraph - August 31, 2016, 8:06 pm

I might get off for the night. If anyone has any suggestions for the next section, let me know.

I plan on making this really really huge, so I'll be covering as much as I possibly can.

thematador - August 31, 2016, 10:12 pm

Very informative, lots of useful stuff in this. Thanks for posting.

Gamer Fusion - August 31, 2016, 10:22 pm

More people need to actually read this haha. Thanks OP.

shashwat97 - August 31, 2016, 11:07 pm

Never knew about Facebook's "Download your data" thing. Would be interesting to see what shows up for me.

FractumSeraph - September 3, 2016, 4:09 pm

PGP

Personal message and file encryption.

For this you're going to need [Gpg4win](#).

When it first opens you'll be asked to generate a key, this is important, so it will be the first thing we do.

It will ask for some information. First your name. Keep in mind all of the information you use will be public, so if you don't want people knowing your real name, use your screen name.

Next your email. Again this will be public, but it's important that you use a real email address, so people can more easily get in contact with you.

Now you will be asked to make a backup copy of your secret key. I'll explain what it is shortly, but for now just treat it as a password. Don't share it. But you do want to make a backup.

Now we wait a few moments for the key to be created. During the creation, you'll be asked to create a password. As always, use a mix of numbers, letters and symbols. The longer the better.

It will ask where to save your backup. Store a backup on an encrypted USB drive or something, it's to be treated as a password, so don't just leave it lying around on your desktop.

Okay, so now you've created a PGP key and you're ready to start using PGP.

The main uses of PGP come down to Encryption/Decryption and Signing/Verifying. Allow me to explain a bit. Or just skip this part since it's somewhat complex, and hard to explain simply.

Spoiler ([Click to View](#))

I have a public PGP key. We will call it KeyFallenPublic. You have a Public PGP key, which we will call KeyReaderPublic. Lets say you wanted to send me a message that says "Hey Fallen, how's it going?" but you don't want anyone else in the world to be able to read it. What you would do is download my Public PGP key, type the message, and then encrypt it using my public key. (Don't worry, the software handles this for you, I'm just explaining a bit.)

Since you encrypted it using my key, only I can read it. Even if you were to post it to your wall on facebook, I'd still be the only person able to read it. Everyone else would just see a jumble of random letters and stuff.

Every PGP user has a public key and a secret key. The public key is available to anyone, this is what you use to encrypt things in a way that only they can read it. The secret key is used to open messages sent to the corresponding public key. This makes PGP more secure as it uses both a password, as well as a key. Even if someone knew my password, they still couldn't open the message sent to me, since they don't have my secret key. On the other hand, if they had my secret key, they would still need my password.

So now that we've set our name and email, then generated they keys, there is just one more thing before we're ready to start using it. We need to get our public key and put it online. People need your public key in order to send messages and stuff to you.

To get your public key, right click on the key in the programs windows. In the menu the appears, click Export Key. Simply save it somewhere like your desktop. It will be a file ending in .asc

Send this to anyone you plan on communicating with. Usually it's just easiest to upload this file to the internet, so anyone can download it if they need it. I'll cover that later.

Okay, PGP is set up and you want to send me an encrypted message. How do you do it?

Sending/Receiving an encrypted message.

First you need my public key. You can either search for it online with a keyserver, or you can just download my key directly at the section below for trying it out.

Now that you have my key, you need to add it to your program. Just click the big Import button on the top, then select my key.

Next, open the Clipboard in the top right.

Type whatever you want to send me in this notepad type thing. When you're done, click the button on top that says Encrypt. A window will appear showing you all of they keys you have. Click on mine to select it.

Just below the box with all of they keys, there is a checkbox that says "Sign". Tick the box, I'll explain it later.

Once you click Okay it will ask you for your password, then it will encrypt the message.

When it's done, you'll see a bunch of random text. This is the encrypted version of the message. Send this to me however you'd like. Email, PM, Post, whatever. As long as I have your public key and you choose my public key from the list, I'll be able to read it.

Now you need to know how to read messages that were sent to you. (Trust me, it's easy.)

Do the same steps as above to send a message, but this time send it to yourself instead of me. Once you get the random text, save it in a text file or something.

Optionally, you can close everything so it's more like you were sent a real message instead of you making it yourself.

Once you get your message, open up the program again. Then open the clipboard again. Now copy and paste the entire encrypted message into the clipboard, then press Decrypt. If everything worked, it will ask you for your password, then once it's entered the message will be decrypted and readable.

Practice this a few times, just in case. Remember you can also encrypt files too, I might cover that later. Pretty much the same.

So now that you know how to read and send messages, you can upload your public key to a server that way people can start using it. Before doing this, make sure your name and email is correct. It's a real pain to have to revoke keys and reupload them and stuff like that. It's much easier to just get everything right the first time.

To upload your key, you'll want to go to a keyserver. This is extremely simple. First, go to the key you want to share, the right click it. On the menu, click Send Key. This will upload it to a server. Anyone who wants your public key can search for it on that server.

Now you'll probably want to upload it to more than one server, that way it's easier for people to find it. I'd recommend going to these websites and adding them there as well.

<https://pgp.mit.edu/>

<http://keyserver.pgp.com/vkd/GetUploadKeyScreen.event>

<https://sks-keyservers.net/i/#submit>

<https://pgp.key-server.io/>

Signing and Verifying

As promised, now I'll explain signing a bit.

Signing is basically a way of saying "Hey, I approve of this message/file."

If I send you a program that instantly levels you up to level 50 on Pokemon Go, I could sign it. Then, using my public key, you could verify that the file is from me.

If someone hacks my account and replaces the file with a fake one, possibly with a pokemon go account stealing virus, when you go to verify the file, it won't be correct. This way you can tell that someone has replaced the file or modified it in some way.

The easiest way of dealing with files is by using the shell extension that got installed when you installed the program. This means you can just right click on a file and use all the functions from there.

Let's say you're working on a new program and you want me to try it out. However, you don't want anyone else to steal it since it's still in development.

Simply right click the file, click Sign and Encrypt.

A box will come up with more options, just choose Sign and Encrypt, then click next.

Now choose the key you want to send it to, click add, then next.

It will ask for your password and then it will be created.

Now that you've sent me the program, I would just have to right click it and press Decrypt and Verify.

Wanna try it out?

If you want to test this whole PGP thing, feel free to message me at any time. A link to my keybase account is in my signature, or you can [download my public key here](#).

If you want to try verifying a file, [download this zipped folder here containing a few examples](#).

More on PGP later, for now, food...

XMPP

Instant Messaging service.

Windows Clie

This guide will show you how to set up an XMPP account and use it. I'll be using a windows program, but it's basically the same no matter what you use. I'll also cover OTR (Off The Record), which is used to encrypt your messages. I'm not going to go into the details of how XMPP works. Besides, there are many other tutorials out there for this that are exactly the same, so I'm just going to make this brief. You send a message, it goes to a server, the server sends it to the recipient. Simple. Much like email.

To start off we are going to need the xmpp client, Pidgin. And we need to download the OTR plugin for it as well.

For pidgin, you need to go to [this address here](#), and choose the newest version. (The top folder) Then download the file that ends with offline.exe. There is an [online installer](#) as well, but it seems to have a bunch of problems, so it's best to avoid it.

Next we need to download the otr plugin, you can find this download at the bottom of the [main website](#).

If you use PGP (you should) then you can verify both of these files. On each download there is a corresponding signature file (.asc) that can be used to make sure your download hasn't been intercepted or infected.

Now that you have them downloaded we can begin. Just double click the Pidgin setup. You can leave everything to defaults if you want, or you can add different localisations for other languages if you need them. You can change the install folder if you need to, but if you do you'll have to change it in otr as well.

Once you have pidgin installed, it should run automatically. If not, go to your start menu and open it.

Once Pidgin opens it will ask you to add an account. We don't have one yet, so this is where we will create one. First change the protocol from AIM to XMPP. Now you'll see the rest of the options we need. For the username, choose whatever you wish. If it's already taken it will let you know when you try to register.

For domain, this is the server you are creating your account on. (Like gmail or yahoo on email.) There are tons of jabber (XMPP) servers online, so just google them until you find one you like. A few I'd recommend are swissjabber.ch, jabber.calyxinstitute.org, and creep.im. You want one that doesn't keep logs, and isn't a closed system. A closed system is one that can't communicate with other ones. If gmail was a closed system, you would only be able to message other gmail users. Not aol or yahoo. hackforums.im is an example of a closed system.

For resource, this is a way of saying which of your devices you are using. It's not required, but can be helpful to other members dealing with fingerprints.

Next of course is your password, just follow strong password settings and you should be good here.

The rest of the options are either not required, or are already on the values they should be at. The only exception is if you use a proxy. If so, add this to the tab at the top labeled Proxy.

Now you just need to tick the checkbox near the bottom saying to create the new account, then click add. A few servers will require you to make an account on their website instead of using the checkbox. But the majority of them will work this way.

Now you have an account and can message people. You can add buddies to your friends list and start chat in the top left. You can add a buddy icon in the bottom right. Change your mood/status in the bottom left. And change your settings/preferences at the top.

The net thing we need to do is add otr so that your chat's can be encrypted.

OTR

Okay, so now we need to install the otr plugin you downloaded earlier. Just double click it and let it install. You can keep everything default unless you've changed your Pidgin location.

Once it's installed, open pidgin and go to your plugins. (Tools->Plugins)

Scroll down to the off-the-record messaging plugin and tick the box to enable it. Now select it and press configure plugin.

The next step is to generate your key.

Select your account from the drop down list, then click generate. (Easy, right?)

If you want, you can also tick the box to require encryption. If you have this ticked, you won't be able to message someone without using encryption.

You're not done just yet though. Whenever you start a chat with someone, you have to turn on OTR, it doesn't just automatically protect everything you type.

Once you're in a chat, there will be a box in the top right.

Either click the box or the menu that says OTR. In the dropdownbox, click the button to start the private chat.

Next you'll have to wait for the other person to join the private mode as well. Once it is done, you'll be asked to verify.

Verifying is a way to make sure the person you are talking to isn't an impostor. Anyone can make an account with the name Obama@whatever.com. To make sure you're talking to the right person, always send a verification code using something else. Like a private message or email. For HF users, you can use the [verify secret](#) function for this. (Yeah, most people download know about all the [Extras](#).)

That's about all for now. This was a bit rushed, so sorry if anything is confusing. I'll go back and edit this soon.

sucet pop - September 8, 2016, 2:47 am

I was going to leave this in a pm but i don't have 25 posts yet.

-----BEGIN PGP MESSAGE-----

```
hQEMA/YPwtymdfczAQf/WA2rFVW3cC5r4jcS3b16CLzda0j19hE9/uxsxNvZWNe/  
zVTRLG8THstEjS9j5HdHpvo10SIlc/xaovSb+cqE3h9Bo/D8X0NTiFXo8uPjnj  
WYfjWAdHSZ4BQi+i1LPaownxxYOVKXLURg4Q3iaQscbYeBhmJGEa6MoWVBWKhx6  
keRhSopYVvm5Lo/10knMfwsr7YA3sgil05LiwEwyg24rxnfpz9WxqAz7Z8hsOKo/  
3q2j1/H9NeHxDyxPwwLOAOEKGzBTj+wBa36BsBdBZRGW2/XzLpbAP4mlZpeoDdAi  
8TaWzCtHVSQD26CnR9uJ1/SG4I3onu4w/Ax6TkVnsNLL7QH88xaP9QV3hPmK+6d2  
N0Ve7YqLRppe6g6NIZG1P2kDsEFIUzGAfZya1bt1e/mszYL3aF2XbGHo3wulWdo1  
mBpoR3UAvj9A14SFCuz3mVzp3ZmsjAP8U5P/X/PPmAikdb8BVtSiRVI3jb9rvAVC  
LqRICMptffGIKCEPzXie8cakqna0O3izaISlPH5belccdcDq06mqvN7oJW532P9d  
tzPUrxfb9xGGT6/PZwGTnGcV9JAVQXU5THxouHB4OxyDE/z8T5sqMFXJEG0o6mmv
```

AgSSEr0rH83weTVRKLZHXQ9zoC58rQF/yNgQvgH5IIOPt5Pnr47azC7yQV/qewLT
Y65VuBAuhCg21hzpIWl8eT0HGSMPlxApKc1hD+9zJCT1Mn5Qv3Mx7YdYlqGI9C5N
MJlHEkzsyvfJM7WgTIs/93Ed6yxllyOc3W9zK307rNV6htVr/tZABn8QNKnv7Ni
reK6oEVMMEgcHAqzLAzxNWFiT476PaRyojkt+s6xfs0+mxt90XkuaaQa/PqtamU
IQ8Wy8EuzWs9c8xQZZpL9fP5/e7ft+3sd8ueUuzGLcZEILccda6wq1MULeiVB/7c
AAz9ic+jyvcqN9/QvOL7uL/5rtFjODW3+w8hfMCCm9vc1m0oI9LgS2J5gB9HC0c+
5iBf0e0W7VFcAjTgzbmux73Q9LY8gEILwfpa+QBA7brB45BSD9nbz4mRiLo1CDb
0BbAZPCaJKdthwrCakhwn2SMt+2ijGQ1crgM6FosrU6osVe2GEorOMegjF65+ fwd
2ZszW8DWOQcoM3Jinhu9DJqvJGHNSMSgu3PQRHr1S27WGI4UIUpFjbNxxNE2EuuE
JHV1hpxFAJjfNI7VjgKPNNGoP150IQP1Wpe8fRabE+fkIurhbEZNMIa/WaY/DzdP
c3+E4Wb4S+EbhRFVZEGMxCMRU29sCmVc91KcSAhZuxWxxomlc6yGqqx75/UXVCpZ
uLR39LjrsAwH2kYDuSHOQAdOB0mbMrT9du2hS4gxLWldrfh0Odw3iuMjhZYFqaua
vgeYcYKUpPbCmYCCJJpRaWfYbR5kfvEpfiRJOXYdrrtfgLZwBWD0Z5PLNcjoGUGPP
+ANoUSDR2uCPqXUjMaFFskx0G6un1oS4yM+268t5CcB29k8wNdzxglRVOFYalfIN
4xWgYn/5ZXxyS6uP/2bLYKQts0YKZ4Wgdn6dJof+Vrb7kgCRwVdLIYjhFjclCa2g
A5gkzy3szaWpm+ZFIqn6bohM69trQa2WJ/dlUv2Hw/g/OXUwY8ywRd7uonPxxyv6Q
ozlhqYliUauaFC5jd7zujJzAcB9G9QAYkjyxWys7xx+HsHbmjM/q1EdhKzCh1LkQU
bJY1bFTPVP6Rf5qYdKZGXhFR3GfESpxflmCmTtxopam8pohDqGVR9NK19dMIQ/k9
LtyMGfsXIVCEBnrB0/IR3GW0qgW+L/NKVnyd4y5q2AkQmo7PJzQ0gYJ+7xasWa2H
ZN/IJ+enx/qmH1Vxq36ucuU1xkl1n9Md6aSXRnFMI2qOCkBpiWjft1gctewGv/73
M4OVaPtVtsJyLTP/m+D9Uj5RBsEn+Z70oqrSMIHBar0AdrGrDIqjY/0jyEgjE9xE
XB446maN3S9k5TXyk3umHrCizhQXUKGbzjvQNLcfunvK0G2apkFQqlgM32rTucGi
v2W40d+sQLGGA8W9AH+LM+jDxSOMAgokTsc61MAOW6tvWvxjRPHq7fktwmOYKSnC
+4UKi/nlMqwnLZNctyAi6dCA1g9t1znMXp7o2nEXUIPnMRPhNCuj6Pj/WwLMeHhX
QEF9ckonRpGtOmm+0FbID0dGpoXMfjxbvhg4deCCvz3CJZy0eP9b0OsD9/mGtinn
ILO+TrvkFzixsuhSbvw6j8LULI+GfqMHiE0wyb/LkPZmdH5NI7jdTU4HHixryRdU
y18uUXYA9rZ1FkTN9bIprzHonUXVwfjMCSJH8rdbT/HZJxklgGTzD35dLp6iweI2
tdKO1ZrUIEDjwIDOXNILbnz44WOJISTANvG6v9/gL8tD5q/y4W0FJtvp6Of6a6RI
1wN42bFQdOftS30dwfeCyDjAgBi/A3E6DM4J9ANGeB404rMZrNMznsvOqsw2ToDa
6Sx30elfZXks7mgDvmWJujzuMYMZEXG0GfDBpe6o5RY0+vMN831iS5oDCw0KAhLe
EfK0fuS1P+EsKF6FBTCz8OzG1gUGdg2F7tpUhCZ9Dmo87U1cG7hNCBZI2OGcEI9Y
+EZKN3TUxdmPT1eIIWPQmPVRYXjK2xIL6ncZIZECzpNN6N3PLiNYTqqEA+tQQcPo
TboRDE4DjSW+y/ytpwLVuDpoU85KyqplCcxZRMhpuK+wFphPyiA23MTg5DWMh0Rfl
+leuwbk/SmatnJdlZQ1B8l/x+5VfxikCIKJkzCzcjGGURdIEF+u0+T8dYhfytJsC
os2zs5BZNK4qlfjyoeABZyPSHilD7MXnMjlrqLdKSh1CE1AeM3leLw4KUB5VHTI
vdljUgjG6riRQ26FFZFky3FwVz8ywSFTER7TDcwStRmip2JU4d4X14jfbSrAKWAn
jGcou0Ejo0dG3IOIPvk5gYPpXAo5qXfSbT6qVFGaeFg7oLQ2uKuZyRWxtHcTM3uF
4/DfMZXLu7I8nIfEd+lqxW+1zrz0dBabRJ0fYKcrQM8hO+fgeVTLp7g43U7+6L5i
GA7zU455wNINITLUvqQgwWdApeKzB0SPFYJ49hmnfG886ESBUILOf6Wg8LHK/+Ae
mHQFifVFCZQV8f7H1Kv+1oNprnrfZL7McalRYDH+EeRh2DM7WAXqhXpBjN5uvWGM
X08A4dcyvmMswmtTB/uyMZxG540Zb0URHTMwIHRjcO1KMbR5hOnE5l/6/6+Fwmxr
ykJbG63Bv8SzQOjXNNIN8Aeu/RBLc2u/wrOtIqZYP2g1JBAL67nKAiYnPmf+l6BI
FyHSd+c65WPbdipw/OtbZTnWlxdH117gqmMRHIT/vz0SUVYU5KK+5x7FiMRWTxne
c48UhcOHWPUnJNTQko6f7caQozvWTP+6DxPxbgpxCksk4pJ3adQx8OOWIYKdTYeV
FUInsGNHil71Xd5yA9ZIJb9PoEfhlddtIEqplmYyxcvgPhvtfyS2GXvk9BUU9nXq
fCkplchcS8h50Dp08kReB8XtoQjy7KMk+r+OTDYAzkt51F7pwk/bKy1hNj9gGAoW
x/JOx/nze/76fXcpDrdVnroKivEBcP8EhMJzZ9A48Ttw7Sv4VQeum5wtiAqF2T66
PuXvXUaFmX6/2CSqjsaC66kxIBDL6QOFZPiX/WpDYwuJoa3nUttzmELzP3eCf5Es
vsryVA5tednhJXsyn4OJ+KYtkivnE5ntFnI8SbOuR7NmiP/IBLrGJ+uoNAcsww7p
EHj8ZE7LCukzImdYaV5iVG8/hT66bSL2K01xqcEqGQoCBsTMWaldRtDBp6SyaRqd
0/ceMs/kQl2KFEF+DCiBMgAhjWGPs6RPGek1QU3fPSJHw0luHaY4HnM07wg5ZAm8
WKIkDwCWS0fw9q4HTa+AKMhUwUz1zcS+Fz3p9q+uxgzJMd1Mi6vcWsHNamap0VvP
vPEt1V7X+K/zGCYQyxSZts9XVUnfkHOjUsyt6N/yDzyxtBC+w1ds4fss36KqOeOz

UWhCGLIK6X2ug0lXYUK9yatuWQxjrBtGmyoWlIGRi0G1AZIG3DZm5xbOT7j5Hg3A
8DsdccjJUvLufKFxmEyT/5Tu3Gr1ANSvKpHjYBKTGo0ltTIGqUSzUtc3yFvUvMgs
NHLJrFZ1zyNq/8dSN2gEnbK2GoF/6FFh4Z0PBz2lr02DLt0i7VIDsAbPys0bkZY
TmiwEliH0DPCPGzT2l4PjemMdZLhBSQBsQGQRqtmYyj7cAC3zeICucb9Pba5iNJH
mji1e3tQsH0QUc7zvnzBJkUbHYBIE77RHZ+LsypExxnRp+X9GLMRx4Gk+4D3D1fz
IVAbOunuMkLSYovLYgx7FTYL0TJn3tZzU6uuvDa2ougVM7bG8au28BQgL9g38HwF
0VXuFy83KHM74B8Ua+PPM++1WoZc+Bl9lznFypgMXE+IgXBw6C5iR+edV7ruYvOJ
HYPntgo/4q/4lwbAHVSTYRgfrbpnpkP0auYjAvMmpKfY/HMBJg7hzfDubdaX4NKa
7RIQJgvyM+ZBugq9W42roXPkEhhNRteZXCNRrUsQeQLbBsQDmr7gHYvIM21tk9y7
ICJ6e2JYSOaZKZnCicX8TgQjbp8vqke4jEjjePr/3poN4X1QRh2KORN3IXe/UWXs
YMle8hEaHLj1hDowry1U
=budZ
-----END PGP MESSAGE-----

FractumSeraph - September 8, 2016, 11:50 am

(Sep 8, 2016 02:47 AM)sucet pop Wrote: [\[CITE\]](#) I was going to leave this in a pm but i don't have 25 posts yet.

-----BEGIN PGP MESSAGE-----
-snip-
-----END PGP MESSAGE-----

Awesome! Worked just fine.
I'll PM you a response in case you want to try it.

Mi2414 - September 8, 2016, 11:53 am

Posting to read over later, Thanks for the great information OP!

Xernive - September 8, 2016, 11:56 am

Saving this so I can come back later and read all of this. Thank you for the time and work putting into this thread. Very much appreciated.

Northlam - September 8, 2016, 9:27 pm

hell yea fallen angel, very well written. I'm familiar of most of these methods however I'm a big fan of how you contextualize your info. Definately learning alot from you guys in this forum. Cheers

FractumSeraph - September 12, 2016, 4:32 pm

A few people have asked if I was done with this.

No, I'm still working on it. It's just that [Mr. Robot](#) made a [thread](#) that got me watching the show. In between episode I'm still typing up stuff I assure you, next on the list is anti forensics. I have it split in to two parts. The first is stopping information from being saved to your hard-drive in the first place, and the second part is how to deal with the stuff that has to be saved.

And I mean securely for the second part. Sure you can have your browser delete your history when you close it, but anyone with a copy of [Recuva](#) can recover that...

sucet pop - September 13, 2016, 4:09 pm

(Sep 8, 2016 11:50 AM)Fallen Archangel Wrote: [\[CITE\]](#) Awesome! Worked just fine.
I'll PM you a response in case you want to try it.
It def worked! Very cool.

FractumSeraph - September 15, 2016, 2:12 pm

Anti-Forensics

Okay, so you have your computer fairly secure from theft, but we still have other problems to worry

about.

Most of the security practices we've covered so far will not protect you if your computer is fully unlocked and running at the time of attack. So the next thing we need to cover is anti-forensics.

Even if the majority of your files are protected in some way, an attacker with access to your computer can still gather a lot of information about you. By looking at file creation, modification, and read times, they can get a good idea of how long it's been running the current OS, and a list of times where you've been on the computer.

Logs from things like antivirus will reveal names of files and directories, even if you've since moved them.

Firewall logs can list websites you've visited or interacted with.

Uninstalled programs may still leave behind files and configuration on your computer, especially in places such as %appdata%.

The list goes on and on. Locations you've been to, devices you've plugged in, all sorts of information. My point is, you need to take care of this. The sooner the better.

So let's get right to work. There are two things ways to do this. Preferably, we need to stop our system from recording things in the first place. If it's never saved then there is nothing to recover. Unfortunately, sometimes that isn't an option. Sure you can have your web browser delete everything when you close it, but even then it does touch your hard-drive. Therefore, the second option is securely erasing whatever files do manage to be saved.

These aren't really in any particular order, just follow as many as you can.

You need to disable hibernation. If someone gets a hold of the hibernation file, they can see all of the running processes inside.

The easiest way to disable this is to open command prompt (as admin) and run this command. `Code Powercfg/h off` If you are on a laptop or have a wi-fi adapter, make sure to "Forget" known networks, as they can be used to build a profile of places you've visited. An attacker does not need physical access to your device to see this information either. More on that in the WiFi article. The command for this is:

`Code netsh wlan show profiles`

`netsh wlan delete profile name=* i=*`

Next you will definitely want a tool called [CCleaner](#). It's a windows equivalent of [Bleachbit](#).

In the settings, make sure you have it set to secure deletion, then check as many of the items you feel comfortable with. This will take care of a lot of items. Things left over from your browser history and cache, windows error reports, recently opened files, etc. This tool is definitely on the must-have list. You can set it to run automatically at boot, or set it to run automatically with the paid version. It also has a tool to wipe the free space of a hard drive.

If you find yourself using the secure erase feature often, you should also look at [Eraser](#). It provides a shell extension to make things easier.

The next thing to consider is your time-stamps. Right click a file and view its properties. If you look towards the bottom you will see its MACE values. These are the time-stamps of when the file was last Modified, Accessed, Changed, and Entered into the file table. Using this information it could be proven that you had knowledge of something, or were using something at a certain time.

To remove these values, you can use a tool such as Timestamp. or [SetMACE](#).

I'm going to stop this post here while I attempt some restructuring. I'll go ahead and post this since it's been a while, but keep in mind that I will be coming back to this soon. There is much more to cover.

However, I'm probably just going to continue this on [my blog](#) rather than cross posting. It's easier on me and plus it brings more traffic. #SelfPromoting

SSA_RedTeam - January 3, 2017, 9:05 pm

Actually thanks for giving me -ve just because i made another account after messaging to administrator.

semendaemon - January 3, 2017, 11:55 pm

Shame there's no linux hardening section

Quote:The very first thing you need to do is reinstall your OS. I get it, that probably sounds pretty cumbersome, but I do it multiple times a month and it's not nearly as bad as it seems. Besides, if you're already compromised before we begin then this won't do you much good...

You'll be shortcoming the death of your hard-drives faster this way. Don't actually format every week, that's completey unnecessary.

Legionhoster - January 4, 2017, 6:31 pm

Nice and helpful guide for beginners.

n31ght0 - February 13, 2019, 7:17 pm

looking for signal vs xmpp and found this thread. how to bookmark/save this useful thread on my profile?

spacepants - February 14, 2019, 6:13 am

This thread is awesome. It covers a lot of ground regarding basic hardening and encrypted messaging. I'd love to see a section on hardening a linux based OS. I'd love to contribute if you need/want someone to help keep the project running. Just dont want to steal your thunder here.

FractumSeraph - September 17, 2019, 12:09 pm

(Feb 14, 2019 07:13 AM)spacepants Wrote: [\[CITE\]](#) This thread is awesome. It covers a lot of ground regarding basic hardening and encrypted messaging. I'd love to see a section on hardening a linux based OS. I'd love to contribute if you need/want someone to help keep the project running. Just dont want to steal your thunder here.

I've been MIA for about a year and a half now, but I'm back and better than ever. I'll be updating this soon and adding LOTS of material.