Guidance on communications security and encryption
Author:
Adison Verlice
Publisher:
Blindsoft enterprises.

Key terms

- PSTN: refers to the public switched telephone network (PSTN).
- Public infrastructure: this refers to encrypted infrastructure that is made available to the **public. As an example, signal, whatsapp, etc.**
- Private infrastructure: refers to encryption/security infrastructure that you own and control.
- Managed infrastructure: refers to encryption infrastructure owned by an organization. This could be a corporation, a business, government, or any other organization which hosts their own encryption.
- Encryption refers to data security using encryption.
- End to end encryption, refers to encryption from end to end, meaning only the parties involved in an end to end encrypted session can view the contents.

introduction

This document contains guidance on how to implement proper communication security.

Note:

While this mainly talks about communications security, miscellaneous topics like file security and even password manager. Only a small part of this document has miscellaneous information.

Why would you need communications security?

Any organization from small business to large corporations get hacked every day.
Communications security (ComSec) would help to mitigate this risk.
No method is hack proof, but this document will try to give you a better understanding.

The problem with regular phone calls

Phone calls are very convenient. You can make them from anywhere in the world basically.

AT&T, Verizon, T-mobile, take your pick.
It's usually as simple as turning your cellphone/telephone on, dialing a phone number,, and boom. You're good and gravy.
Here are some security failures of the public switched telephone network (PSTN).

1. Ability to intercept calls at will.

From the electronic privacy information center
"The Wiretap Act prohibits any person from intentionally intercepting or attempting to intercept a wire, oral or electronic communication by using any electronic, mechanical or other device."
However, we now know from some examples that they do not always get warrants nore have cause to wiretap.
Here is an example
warrantless surveillance from the national security agency
To give you a brief summary, this allowed the national security agency to record phone calls of civilians to foreign countries.
While without a warrant, they couldn't tap the call contents, what they could tap was the location of the call, the phone number/caller ID, the carrier, and other forms of metadata

2. Hacking of the telecommunications grid to spy on americans.

Here is an example

https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications
Publisher:
Cybersecurity And Infrastructure Security Agency (CISA)
Date: 11-13-2024
From the text : "The U.S. government's continued investigation into the People's Republic of China (PRC) targeting of commercial telecommunications infrastructure has revealed a broad and significant cyber espionage campaign.

Specifically, we have identified that PRC-affiliated actors have compromised networks at multiple telecommunications companies to enable the theft of customer call records data, the compromise of private communications of a limited number of individuals who are primarily involved in government or political activity, and the copying of certain information that was subject to U.S.

law enforcement requests pursuant to court orders. We expect our understanding of these compromises to grow as the investigation continues.“

So how did they get in?

https://abc7ny.com/post/china-hack-chinese-hackers-gain-access-millions-american-cellphone-records/15622337/#:~:text=The%20investigation%20has%20revealed%20that,Technologies%20and%20other%20telecommunications%20companies.
Pierre Thomas, Luke Barr, and Katherine Faulders
Publish date: 12-4-2024
Publisher: ABC News

“The investigation has revealed that China's campaign exploited U.S. computer routers serving telecom corporations, giving them the gateway to the phone numbers of significant numbers of customers of Verizon, AT&T, Lumen Technologies and other telecommunications companies.”

Note:

This does not just apply to phone calls.

This can apply to emails, text messages (SMS) internet traffic, files in cloud storage, and, if bad enough, even your phone itself.

What can you do to protect yourself

https://www.npr.org/2024/12/17/nx-s1-5223490/text-messaging-security-fbi-chinese-hackers-security-encryption#:~:text=Life%20Kit-,How%20to%20keep%20text%20messages%20secure%20as%20FBI%20warns%20of,to%20keep%20their%20info%20safe.

Title: **FBI warns Americans to keep their text messages secure: What to know**

Publish date
12-17-2024
Author: Bill Chappell

“The FBI and other agencies are encouraging people to use end-to-end encryption, citing what they say is a sustained hacking operation linked to China. In this 2021 photo, a smartphone's screen shows messaging apps including WhatsApp, Signal and Telegram.”

Yes, the FBI is now recommending you use end to end encryption.

Non technical overview.

Imagine you were whispering a super secret message to one of your friends in a super secret way.
Maybe you were whispering very quietly so friends around you can't hear it.
Maybe you…put it in a safe, and only you and your friend have the code to unlock that safe.
That is basically end to end encryption.
Only you and your friend have access to that super secret safe.

Technical overview

With end to end encryption, the information you are transferring is encrypted at your (the senders) level.
Then, it is transmitted to the receiving ends device, where it can be decrypted after a secure login to the application/client (signal, whatsapp, matrix, etc)

Here is an example.
PGP (pretty good privacy) is one of those encryption algorithms that can do end to end encryption.
It can also encrypt files, too.
Here is an example
Imagine you have sensitive data that you want to store in the cloud. This is not a nextcloud instance isolated from the internet, we'll get to that later.
This is google drive, microsoft outlook, or maybe even some business clouds like cloudflare r2.
Data is encrypted in transit, and encrypted on the server side.
There is a small problem, however.
This means anyone working at said company can gain access to that data.
This means if you upload, say, mysocialsecuritynumber.pdf, even though it is uploaded encrypted at rest, it's only protected at the server level.
Malicious employees, subpoenas, a lot of bad can happen.
We can solve this by implementing client side encryption, or end to end encryption.
For pgp, this means that rather than uploading the normal copy, socialsecuritynumber.pdf, you would upload a dot PGP file. So it would be, my social security number.pgp, or if you wanted to obscure the metadata, you could use a random filename, EG, my favorite cats.pgp.
Rather than showing the actual file contents, it will simply just show scrambled data.
As an example, we will view a txt file, and compare that with a pgp file.
Here is a simple text file with a fake social security number on it.
This will be the target file to decrypt.
https://blindsoft.net/mysocialsecuritynumber.txt
Now imagine we just encrypted that with a pgp file.
I obscured the purpose of the file so i retitiled it, my favorite cats.pgp.

Here is what it would look like in this instance.
https://blindsoft.net/myfavoritecats.pgp
You can see that it's just nonsense, you cannot make sense of the file unless you have the decryption key, or in pgp, known as the private key.
Now you can transfer this to your public cloud, and your cloud service provider, google, amazon, cloudflare, outlook, etc, cannot see the real file, they just see scrambled data.
You can also refer to this as client side encryption. Along with the server side encryption already provided in mentioned cloud services, I'm also encrypting the data at the client side.
This means that not even a third party would have to have my pgp private key to decrypt the data. And as long as I don't accidentally expose that by acting stupid, I should be good.
This encryption can also be applied to emails.
Email encryption can use pgp. For example, thunderbird, an open source email client encrypts emails using PGP.
It can also encrypt the email subject.
As for message end to end encryption, normally, with apps like signal, whatsapp, (etc) they will usually have end to end encryption using a number of algorithms.
In the signal case, it's curve25519, advanced encryption standard (AES) 256, and HMAC-SHA256.
If you would like to read more on the signal protocol, rea here

Private infrastructure/managed infrastructure.

Thus far, we've only been talking about public infrastructure.
Private infrastructure is closed off at a private level. For example, private/business owned (managed) infrastructure will typically require you to be on a specific network.
This network could be a VPN network.
This VPN could be air gapped and you have to be at that site to access it.
These networks typically do not use whatsapp, signal, or any of these other public platforms.
Instead, they use their own dedicated servers which they can control themselves.
These servers can be located in the cloud (EG, amazon web services, google cloud platform, etc) or they can be located on prem, like in an office building in a dedicated server room somewhere with both physical and digital security layers.
If you're a selfhoster, you could be hosting your on-prem server in your closet somewhere in home terms.

Should you use public or private infrastructure?

Depends on your needs.
Signal is the gold standard for secure messaging.
It is open source, and, as mentioned in above statements within this document, uses end to end encryption.
visit signal.org

The problem with applications like whatsapp and telegram.

Whatsapp is closed source.
This means it is very hard to trust meta.
In fact, there are more articles to suggest not trusting meta than *to* trust meta.
For example, according to the european data protection board (EDPB)
From the text:
“ On 13 April 2023, Meta Platforms Ireland Limited (Meta IE) was issued a 1.2 billion euro fine following an inquiry into its Facebook service, by the Irish Data Protection Authority (IE DPA). This fine, which is the largest GDPR fine ever, was imposed for Meta’s transfers of personal data to the U.S. on the basis of standard contractual clauses (SCCs) from 16 July 2020. Furthermore, Meta has been ordered to bring its data transfers into compliance with the GDPR.
Andrea Jelinek, EDPB Chair, said: “The EDPB found that Meta IE’s infringement is very serious since it concerns transfers that are systematic, repetitive and continuous. Facebook has millions of users in Europe, so the volume of personal data transferred is massive. The unprecedented fine is a strong signal to organisations that serious infringements have far-reaching consequences.””

Also, here's a theory.

Note that because facebook is proprietary, this theory is not confirmed.

Back in 2021, the FBI revealed an operation called anom

One of the ways the FBI would gather data is not by implanting the phone's anom sent out with malware, o no. it sent a blind carbon copy (BCC) to another user controlled by the FBI. so in reality it was end to end to end encrypted, on 3 different ends.

There’s a good possibility that whatsapp could be doing this to appease the intelligence overlords.

Whether that’s actually happening is yet to be discovered.

As for telegram, only the client was open source.

For a truly secure app, you’d want both the client and the server to be open source.

Open source applications recommended in this document

- signal private messenger
- session private messenger good for routing communications over onion routing.
- Matrix

Public encrypted by default cloud storage

- Nordlocker
- mega.nz
- sync.com

Miscellaneous

Best public facing password manager

- Bitwarden

Best public facing VPN for privacy/security

- mullvad VPN
- protonvpn

Private infrastructure.

If you need regulatory compliance, or you feel you need to store your messages outside of the public facing servers, you may want to consider private infrastructure.
1 of the things i recommended for the public facing side is matrix.
Welp, I got news.
Matrix is not just public infrastructure.
Matrix is decentralized, therefor has something called matrix homeserver
This means, you can run your own, yes, your very own, matrix server on your own network and send end to end encrypted messages.
Yes, this can apply to managed/business infrastructure as well.

As it is your infrastructure, you get to control everything in it, from how it is accessed, to who gets to join, everything.
Also, if you do things correctly, no calls will be sent out to the public internet. They will stay on your local network.

An example for deploying an ultra secure environment to managed infrastructure

Note:
If you are not interested in this part, skip to the last heading
Back around 2013, there was a project called, project fishbowl, run by the national security agency.
It is still alive, though the name is commercial solutions for classified (CSFC)
here are the specifications
What if we could make an open source version of that, less expensive than the NSAs $2000 system
For the phones, I would use a nitrokey nitrophone4 with grapheneOS, with the camera and mic out of the phone.
I would also use NitroMDM for mobile device management.
For the network side, I would make sure there is a proper firewall. For example, PFSense, OPNSense are some good open source firewalls.
If we're going to use a VPN, let's pretend we're the NSA and use the IP Security (IPSec) protocol.
We can use something such as NSA GoSecure
Note:
The VPN you use really does not matter, as long as it is secure.
If we're going to air gap the network, let's inshore we can at least get the software installed first, because air gapping it/isolating it from the internet means that it will not be able to connect to the internet and that someone will have to be on site to access it.
We can have the phone then, at the OS level, connect to our VPN with the user's credentials.
Finally, the user logs onto the matrix application, and boom. They can now start sending and receiving end to end encrypted calls.

Best private infrastructure for calls, messages, files, etc.

For calls and messages

- Matrix

private/managed infrastructure for files

- Nextcloud

Password manager

- bitwarden (managed infrastructure)
- bitwarden (private infrastructure)

Conclusion

The conclusion is simple: secure your data.
Stop using unencrypted applications for your messaging.