Tech Talk Tuesdays #2: Privacy and Anonymity

Topics

- Privacy and Anonymity
- Encryption
- VPNs
- Tor

PRIVACY AND ANONYMITY

Why TOTAL P&A online don't exist?

When you interact online, several entities have access to different types of your data (personal info, IP, device identification, metadata, search history, etc).

These are some of those entities:

- Governments through backdoors in software
- Hardware manufacturers
- Nameservers
- Search engines
- ISPs
- Other actors
- Regular users

Proprietary hardware: a problem we have to live with, for now.

As long as we are using equipment that is not manufactured in an open way, we will never truly know if our data is being accessed despite our efforts to protect it.

Only way out: our own infrastructure.

We need to take strides to become more independent and build our own infrastructures in terms of hardware, software and means of communication in order to truly have complete privacy and anonymity.

That said...

Don't make it easy for them!!

Total P&A may not be possible at the moment, but that doesn't mean that you should make it easy for them. Make them work for it. There are always steps you can take to make it more difficult to get your data. They'll get it if they really want it, but at least you are not handing it to them.

ENCRYPTION

What is it?

"Encryption is a means of securing digital data using one or more mathematical techniques, along with a *password* or *key* used to decrypt the information. The encryption process translates information using an algorithm that makes the original information unreadable."

How does it work?

Encryption protects the contents of the message by enconding it and making it unreadable. The message can only be decoded and read using the correct key.

Keys are the key. Make sure to save them, because if you lose them you will not be able to read the messages encrypted for that key.

Why use encryption?

When you encrypt your messages, you prevent others from accessing the contents. They might still see that a message is being sent, but won't be able to read the contents. This means that, if you use an ecrypted messenger service, those who run the server will not have access to your private messages. It is important to take this into account when using services like Telegram, which does not have encryption enabled by default.

VPN

What are they?

A VPN is a closed network that is made available through a public network. For example, you can have your own self-hosted VPN to access your home network securely when connecting to the internet in a café.

VPN is not the same as a VPN service. "A virtual private network service, or VPN service, provides a proxy server to users to bypass Internet censorship such as geoblocking or users who want to protect their communications against data profiling or MitM attacks on hostile networks."

The connection with the VPN service is (usually) encrypted.

What happens?

VPN service:

- Traffic between user and VPN is encrypted.
- ISP can only see the connection to the VPN.
- VPN can see where the user connects to.
- Websites can't see who the user is.
- Websites see VPN location.

Use cases:

- Access a restricted service in your region.
- Hide traffic from ISP.
- Mask your IP from a service or website.

TOR

What is it?

"Tor, short for The Onion Router, is free and open-source software for enabling anonymous communication. It directs Internet traffic through a free, worldwide, volunteer overlay network, consisting of more than six thousand relays, for concealing a user's location and usage from anyone conducting network surveillance or traffic analysis."

How does it work?

Relays traffic over several nodes. The connection's origin and destination are unknown to single nodes.

Tor provides a degree of anonymity to the user.

Use cases:

- Host/use services without exposing IP.
- Hide traffic from ISP or VPN.
- Browse internet anonymously.