Digital Security

Protecting your organization and the communities you serve

Carlos Guerra - 2025

About the speaker and the format

CARLOS GUERRA

- Venezuelan
- Direct experience in most countries in Latin America
- For the last four years, I have worked in a global project covering 39 countries, including some sensitive ones
- Interests/Experience
  - Security in high-risk contexts
  - Technical surveillance
  - Technical censorship
  - Malware analysis
  - Computer forensics

THIS ACTIVITY

- A bit over one hour, and then time for questions
- We will share some resources; they will be linked at the end
- These slides are designed to be shared
- Please feel free to interrupt, use the chat, raise hands (if available), etc.
- It is OK to ask things outside of the current content (as long as they are related to digital security ;)
- Slides are numbered, if that is helpful for questions or reference

Some disclaimers

INFORMATION SECURITY IS VAST

There are a lot of topics to cover. Usually, these trainings last multiple days.

WE HAVE A VERY DIVERSE AUDIENCE

Not all backgrounds have the same needs.

UNITED STATED VS. OUTSIDE

Guidance might look very different depending on the use case, and historically, the US had a different context.

SOME THINGS MIGHT BE TRIGGERING

It is important to focus on this group as a safe space to discuss bad scenarios before they happen (if they occur).

General map

Threat Modeling
Understanding our risks

Communications
How we talk with others

Accounts
Our presence on internet

Devices
The tech we interact with

Tracking/Surveillance
What is actually possible and what should be worrying us

Threat modeling

Transforming uncertainty/ fear/ anxiety/ unawareness into action by understanding our risks and responding to them

There is a lot of security guidance out there designed for many different scenarios, so…

Do those scenarios apply to our context?

Where do we start?

Threat modeling

There are many ways to start this exercise, so don’t worry if you don’t like one in particular.
(links to others in the references)

One good starting question could be:

What information might represent a problem if accessed by the wrong actor?

Some recurrent examples of sensitive information include

- **Our funders**
- **The topics we cover**
- **Confidential sources**
- **Victim/survivor identities**
- **Etc..**

And all of these usually require **different approaches!**

Pit stop!

Think about your own digital security. What type of sensitive information do you handle most often?

(A) Work-related confidential data,

(B) Personal identifying information,

(C) Communications with vulnerable individuals,

(D) Other.

Share in the chat!

Threat modeling

Once you have clear what information can be problematic if disclosed, we can move to understand who can be a problematic actor more specifically:

- ❑ **Who might be interested in getting the sensitive information?**
- ❑ **What are their capabilities and intent?**

Here, we can have a better sense of the actual risks and start narrowing down a sea of possibilities into a more manageable set of scenarios that seem more realistic and actionable.

Once we have a good idea of the information to protect and adversaries, the next two questions are

- ❑ **What is the impact if any of the scenarios occur?**
- ❑ **What can we do to avoid these scenarios and reduce the probability and/or the impact of them occurring?**

Threat modeling

The previous exercise was focused on the unintended disclosure of information (**confidentiality**), which is the most recurrent fear of organizations in civil society. However, other aspects of information security are also frequently overlooked and require some thinking: **availability** and **integrity** of the information. Other relevant questions covering those could be:

- ❑ **How impactful would it be if our operations were disrupted? How probable is this?**
- ❑ **How impactful would it be if our information was lost or contaminated? How probable is this?**

These questions should start many conversations that would be impossible to predict without knowing the organization's specific context so that every group will have its own flow. It is key to close those conversations with the last two questions of the previous slide so we understand the impact of bad things happening and what we are willing to do to avoid or mitigate those scenarios.

The most important thing about threat modeling is **transforming uncertainty/fear/anxiety/unawareness into action**

Secure communications

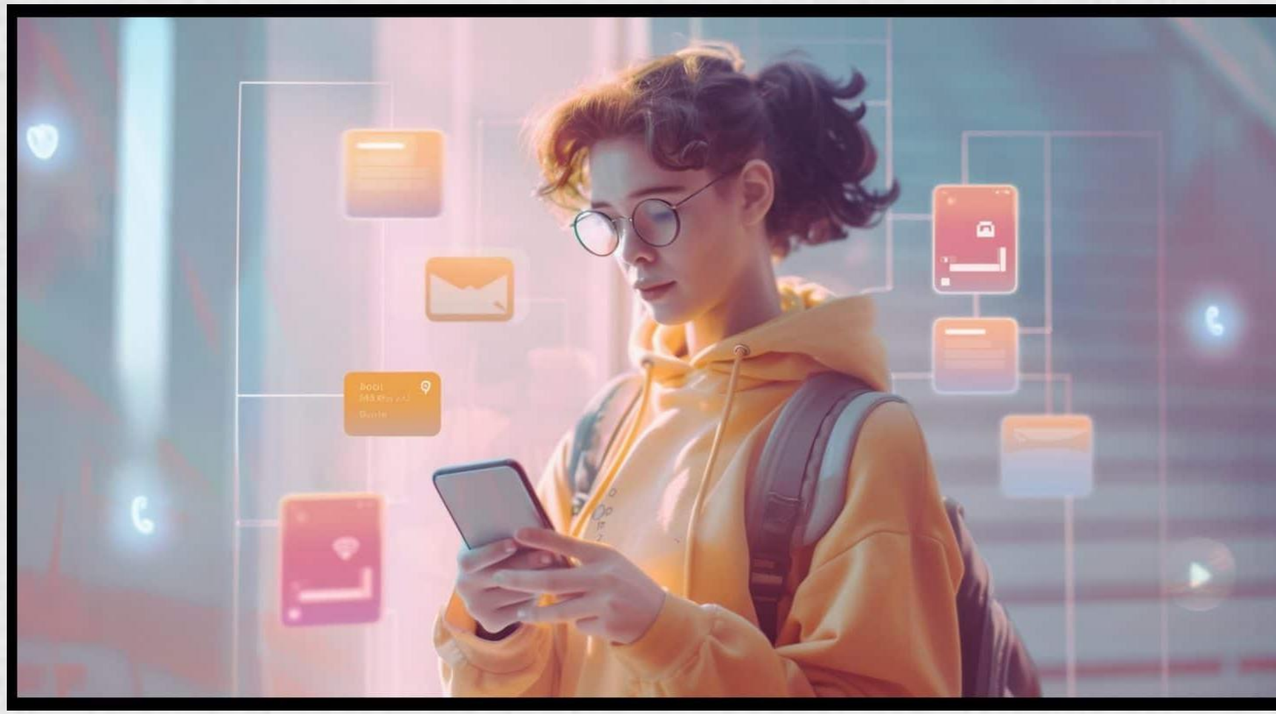
- If you feel that depending on where you are, the interception of communications is a possibility and can represent a security problem for the organizational information:
- First, think about what information you are communicating over which channels, and from there, we can better tailor any specific guidance. Some general tips might be:
  - Avoid cellphone/landline calls to discuss sensitive information in favor of internet-based alternatives. This also applies to SMS
  - A more widely adopted solution in the community is using Signal; WhatsApp might be another option, but keep in mind that Signal has many more options to ensure the security of the communication.

Secure communications

- Some general tips might be:
  - If it is relevant to you, consider deleting old chats or files from your devices tied to actors that might be at risk if the chat or its content is leaked. Also, look at your tools for self-destructing messages
  - Careful with cloud-based back-ups; there might be a lot more information than intended, especially for WhatsApp
  - Some messengers have some form of multi-factor authentication, mostly in the form of a short numeric security code anyone needs to provide if they want to use your number on a new phone, try to use this feature. In some contexts, this is a standard attack and setting up the security code is an easy and effective way to prevent it.

Secure accounts

- Online accounts like email and social media are one of the easiest targets for someone who wants to access your information. A big percentage of compromises in our communities are consequence of less secure configurations in accounts:
- About passwords: there are many different approaches to secure passwords, so you might find even contradictory guidance; that said, also check if the reasons behind certain tips apply to you
- Avoid using easy-to-guess information like pet names, favorite band/food, etc. It must be easy to remember/get for you and hard to guess for others.
- Always prefer long and easy-to-remember passwords over short and hard-to-remember ones with caps, numbers, symbols, etc.

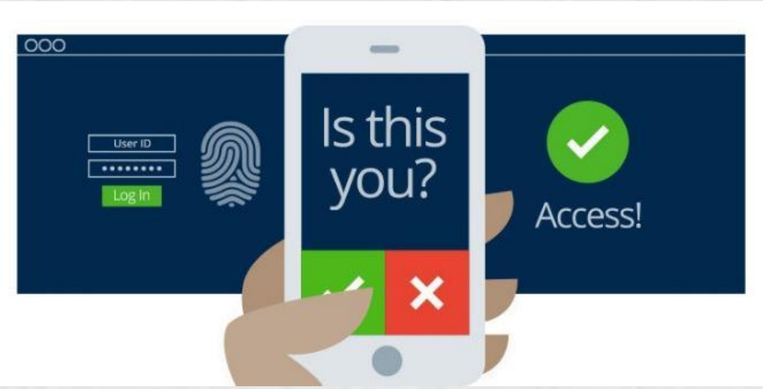


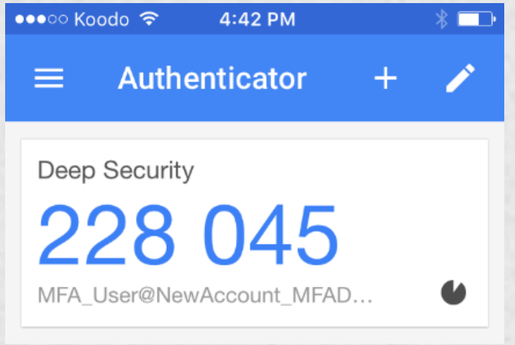
Secure accounts

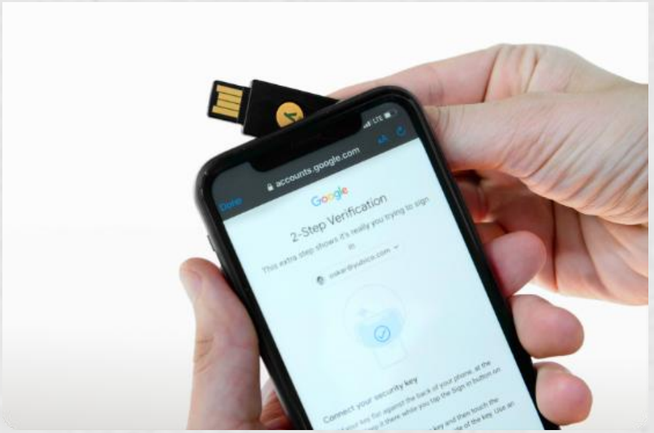
- About passwords:
  - Also, you can use **password managers** that will create very complicated passwords and remember them for you, so you have to remember only one password (for your password manager), and the tool will take care of the rest.
- If your provider uses security questions, please make the answers not obvious; otherwise, some people can research a bit about you on social media, hit “I forgot my password”, and answer correctly, taking your account from you.
- Please log off after using an account on a shared device (in public devices, it is not advisable to log in)

Secure accounts

- The most impactful change you can make on your accounts in terms of security is enabling Multi-factor authentication (or two-step, MFA, 2FA, etc.)
  - This way, even if an attacker has your password, there is an extra step they need to complete that is extra easy for you and extra hard for them.
    - Authenticator apps
    - USB security keys (most advisable)
    - Application notification
    - Others (avoid SMS codes when possible)
- **Keep an eye on Passkeys**. They offer very good security vs more traditional logins, but their usability and adoption are still evolving







Secure devices

- ❑ Update everything!
  - ❑ Many recent attacks leverage vulnerabilities in operating systems and applications that are usually fixed by companies but are only available through updates.
- ❑ Careful with organization-issued devices
  - ❑ Inform yourself about the level of access your organization has through your devices.
- ❑ Protect the physical aspect of devices
  - ❑ Good screen lock mechanisms
  - ❑ Screen patterns?
  - ❑ Biometrics?

Secure devices

- Careful with the apps you install
  - The easiest way to get infected is when we install the malware ourselves. Many pirated apps and application clones have some form of malicious code.
- Careful with alarming news
  - Most of the recent attacks covered leverage very sophisticated and/or expensive solutions; never forget about your threat model.
- Pro-tip:
  - Recently, phones have a more secure architecture compared to computers.
- Pro-tip 2:
  - Apple lockdown mode (iOS)

Some notes about tracking/surveillance

- Careful with the administrator's dilemma
  - Who is running the services we are using?
  - What can the admins see?
  - What can the admins share? (especially important)
- Careful with timing (things are changing very rapidly!)
  - Do we have sensitive information today that wasn't sensitive yesterday? What to do with it?
  - Is there an actor that wasn't dangerous yesterday but that is dangerous now?

Pit stop

The majority of organizations use Google/Microsoft services. Judging by recent developments and the work you do, do you think they represent a security risk?

(A) They shouldn’t represent a problem

(B) They are not a problem, but they might give information to more problematic actors

(C) They are a direct threat to our work

(D) Other

Share in the chat!

Some notes about tracking/surveillance

- Do we need to adjust our threat model?
  - If you are asking this to yourself, the answer probably is yes
  - Be especially careful when people are in danger because of changes in the context
- Regarding information at rest (it can also be susceptible to surveillance)
  - Where do we host the digital copies?
  - Where do we host the physical copies?
  - For how long do we keep sensitive data?
  - How can we process and delete sensitive data?

A pit stop on operational security

Communications
Who knows which information we made public
How are we communicating
What can be heard

Attitude
Respect
Cautiousness
Do no harm
Humility

Computer
Encryption
Integrity
Password
Sensitive data
Screen lock
Somebody can see from behind

Where are you going
with whom do you let yourself be seen
Who are you
Papers, notes, cameras
Physical environment

Encryption
Password
Which data is stored
Screen lock
Integrity
Chats and other comms
Mobile devices

From Internews' SAFETAG team

A pit stop on operational security

General map

Threat Modeling
Understanding our risks

Communications
How we talk with others

Accounts
Our presence on internet

Devices
The tech we interact with

Tracking/Surveillance
What is actually possible and what should be worrying us

Digital Security

Very useful references

- ❑ EFF Surveillance Self-Defense - https://ssd.eff.org/
- ❑ SAFETAG risk matrix activity - https://safetag.org/activities/risk_matrix/
- ❑ Electronic Frontier Foundation - https://www.eff.org/
- ❑ AccessNow Digital Security Helpline - https://www.accessnow.org/help/
- ❑ Internews SaferJourno - https://saferjourno.org/
- ❑ CiviCERT Digital First Aid Kit - https://digitalfirstaid.org/
- ❑ Ford Foundation’s Cybersecurity Assessment Tool - https://cybercat.tools/
- ❑ SOAP, security policies generator - https://usesoap.app/
- ❑ Do you know another? Please share in the chat!

The tip of the iceberg

- ❑ Secure communications (in more detail)
- ❑ Extra measures for at-risk communities
  - ❑ Investigative journalists
  - ❑ Human Rights Defenders
- ❑ Malware
- ❑ Secure browsing
  - ❑ VPNs
  - ❑ Tor
- ❑ Internet of Things (IoT)
- ❑ Internet disruptions
- ❑ ...

Questions?

These slides and a list of references can be found at
https://guerracarlos.com/lpc
cguerrave@gmail.com
https://bsky.app/profile/cguerra.bsky.social

Thank you!!