What is a phone? How does mobile communication work? [deepening activity]

image-1605640472202.png
Image not found or type unknown

The purpose of this activity is to deepen knowledge of how mobile communications works in to support participant's ability to assess and plan for risks of mobile communications. Facilitators should include this in any mobile workshop or confirm that all participants are already familiar with the information in this activity. It is the basis of assessing technical mobile risks.

This activity has 2 stages:

- Hands-on phone dissection
- Input: Mobile communication data and risk considerations

Learning objectives this activity responds to

- Understand some basic concepts of how mobile communications work in order to inform ourselves about the potential impacts of using mobile communications;

Who is this activity for?

This activity is for anyone participating in a mobile workshop.

Time required

This activity will require about **45 minutes.**

Resources needed for this activity

- some mobile phones to open up and investigate
- A whiteboard, slide, or handout with top level points

Mechanics

Mention or discuss, depending on time, that we will talk about mobile technologies – considering devices that are easily portable in a hand or pocket and have communication capabilities from voice calls and sms to web and data services. Some of this section will apply also to tablets.

Inside our phones - 5 minutes

Take this phone apart. Your phone is a tiny computer. Everyone take your out and locate:

- Parts that listen and project sound: microphones, speakers
- Parts that view and display visuals: cameras, screens
- Parts that send and receive information from other sources: GPS, Antennae, Wifi
- Parts of the computer, hardware: battery, circuitry
- Memory: SD card, other memory built-into the phone
- SIM card slot(s)

Device and SIM identity - 5 minutes

Your phone has all these pieces and it has a few identifying features, in addition to the make, model and OS, it has 2 names - a Device Identifier and a SIM Card identifier. These are important to know about because you can be identified by either one and your phone communicates this information often, especially the IMSI.

- **IMEI** is the name of your device

International Mobile Equipment Identifier (IMEI):

https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity

- **IMSI** is the name of your SIM card

International Mobile Subscriber Identity (IMSI):

https://en.wikipedia.org/wiki/International_mobile_subscriber_identity

Our phones in communication - 35 minutes

We use our phones to communicate with people: SMS, Messaging, Social Media, Apps, Calls. Our mobiles are also communicating information about our phones and ourselves - not just our messages but metadata, our location, etc, and this can be linked to other information about us like our social networks, our organizing networks, our habits and places of work.

It's good to be aware of these, mostly so that we can understand how our mobile phones use can act as a tracking device in the moment and as a historical record of our activities afterwards.

1. Your phone is chatty

Your phone is calling out to different types of networks and via different types of communication to announce it is near and to connect or check if anyone wants to connect.

Mobile carriers

Mobile carriers have towers and antennae that your phone communicates with. Each antenna can reach a specific area. Your phone checks in with whichever tower(s) you're nearest. It shares **at least your IMSI** to announce which mobile carrier you are using and your number so you can receive messages, calls, and communications to your device. Every time you are near a tower, it is like dropping a pin on a mapped timeline where you are. You mark where you are, when you are there, and what you are doing in that location in terms of using your phone.

GPS

If your GPS feature is on, your phone is communicating with GPS satellites, similarly checking in, which is like dropping pins on a mapped timeline.

Wifi

If your wifi is on, as you pass through Wifi networks, your device may both attempt to connect to those networks, leaving a pin with the wifi network, and also make a record of the network name in your phone.

Bluetooth/NFC

If these are turned on, other devices using Bluetooth and NFC may be able to communicate with your device, attempt to connect, share files. Etc.

Facilitate discussion: Which things you need to have on when? Are records of where you are a risk for you or not?

2. You are chatty

We use our phones to communicate. Different types of communication appear differently while you are communicating and once the messages have been sent.

SMS

Text messages and metadata - in communication and once stored on your device and with your carriers, are sent in cleartext. A useful analogy is that an SMS is like a post card. If someone intercepts it, they could read the entire contents as well as metadata (ex. sender, recipient, time, date).

MMS

Media messages and metadata - in communication, this may or may not be encrypted, so if someone is trying to intercept your communications, it will vary if they can see it. Once it's sent, you and your recipient's mobile providers and devices have a record of the message and so investigation into either might reveal metadata (ex. sender, recipient, time, date) and content.

Calls

Call content and metadata - similarly - calls should be encrypted as they are in progress, but your provider and your recipient's provider will store metadata about the call (ex. sender, recipient, time, date) and if your opponent has access to your providers, they may have access to listen into calls or to record them.

For more information about Apps and Messaging Apps, see:

- Discussion, input + hands-on: Choosing mobile apps

A note about state surveillance: From country to country, state surveillance varies. In some places, governments will have access to any and all data that carriers have -- so with these, you should consider all of your metadata and contents of unencrypted services accessible to governments both in real-time and after the fact if there is an investigation for these records.

Your best defense against surveillance is End-to-End Encryption.

3. A phone is a small computer

Software bug - A phone is a computer and can be infected with malware just like a desktop or a laptop. Individuals and governments alike use software to bug other people's mobile devices. This kind of software often uses parts of the phone to act as a bug or a tracking device, listening in with the microphone or sending location data.

4. The cloud is a file cabinet

Some data that my phone accessess is not on my phone at all, it's on the cloud. The "cloud" is just a term that means "the internet" -- data that is stored somewhere physically on a device that is connected to the internet. Your apps may accessing data that is in the cloud and not actually on your device.

Considerations: Is my data encrypted in transit between myself and the service? Is it encrypted when it's stored by the service? Do I know of any instances when opponents have been able to get access to this information - when, how?

Note to facilitator: As you speak, participants may ask questions about parts of phones or risks associated with communication methods you mention. Take the time to answer questions. If you can, keep a running list of issues and topics that people ask for additional information about -- a running list on a white board will do. Also keep a running list of issues and topics you will not get to this workshop so that you address it later in the workshop or suggest as follow up after the workshop.

Additional resources

- 7 Ways to find the IMEI or MEID number of your phone: http://www.wikihow.com/Find-the-IMEI-or-MEID-Number-on-a-Mobile-Phone
- International Mobile Equipment Identifier (IMEI): https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity
- International Mobile Subscriber Identity (IMSI): https://en.wikipedia.org/wiki/International_mobile_subscriber_identity

Tactical Tech's My Shadow site has a number of great training guides to facilitate learning about mobile tech.

- My Shadow downloadable materials: https://myshadow.org/materials
- My Shadow website: https://myshadow.org/

Some videos:

- How does your mobile phone work? This video at nine minutes is likely too long to show during your workshop but can be a reference for participants and for yourself to understand how cell phones work via antennas and mobile switching centers, as well as cell phone generations. https://www.youtube.com/watch?v=1JZG9x_VOwA You might like to find shorter videos that touch on some details and are more appropriate to your specific context once you are familiar with this longer video.

image-1605452256072.png
Image not found or type unknown

Revision #7
Created 16 April 2023 03:58:00 by Kira
Updated 28 July 2023 14:51:35 by Kira