Homerwork 1: Privacy as a Human Right

José Antonio Álvarez Ocete

Main concepts presented

The first concept we learned in this class, and maybe also the most important one, was the **threat model**. This is the first thing we have to tackle when thinking about security -- and not only computer security. It consists of two points:

- Who is your attacker, what is their motivation and what capabilities do they have?
- What assumptions do you make and why?

This for me was quite eye-opening. I'll discuss it thoroughly in the next section.

In the second lecture we focussed on phone privacy, starting with **where data is stored in our phones and who can access it**. To provide some background we looked at some OSs and how they handle these issues:

- Solaris: Private within users, everything shared within the same user. Can share with other users explicitly. Problem: having only one user (basically all our computers since 2000) and malware can access potentially everything.
- Android and iOS: One "user" per app, with individual permissions and accesses.

We also talked about **covert channels** and **side channels**. I like to think about these concepts with an easy analogy. Let's see you to get inside Sam's office to obtain some information. A covert channel is finding someone with a key to the room, such as cleaning staff, and ask them to get it for you. A side channel is finding a way inside avoiding the "security measures" (aka the door), like finding the window open.

Finally, the third lecture was a little more technical and we went over some basic computer security concepts related to the paper we studied:

- **Metadata**: Is the context data, or the data that describes the actual user data. It's underestimated by users and the most important thing for corporations.
- **Symmetric encryption**: A way of encrytion used in communication that uses a single key to cipher and decipher the messages. It requires that both members of the communication know the key beforehand to be secure.
- **Public and private key encryption**: A way of encrytion used in communication where each user has a public (known by all) and a private key (known by only the user). If *A* wants to send a message to *B*, *A* uses *B*'s public key to encrypt the message and *B* uses their private key to decipher it.
- **Mixing networks**: A protocol using multiple servers to encrypt metadata. It requires at least one of the servers to be safe for the whole system to be safe.
- **Onion routing**: A protocol that uses public and private key encryption to break the view of end-to-end communication. The messages are sent through a chain of servers using several layers of encrytion Again, the protocol is safe as long as one of the servers is safe.

Future Work

Lecture Ideas

First of all, I would like to discuss some ideas I came upon while attending to these lectures. The first one is **how the threat model works** and how upon securing a system you want to prevent specific kinds of attacks, not every single attack. By doing these you can focus on the attacks that would really have an impact and minimize them.

The second idea is the **trade-off between security and privacy** exposed at the end of the second lecture. The question, in particular, arose from letting Uber block your account upon detecting a weird kind of access. I have always looked at these kinds of *privacy intrusions* from a "sure, they want to make things easier for me but, in reality, all they want is my data" point of view. I

had never considered how security affects this issue and that my data could also be used in that sense. There is a thin line between being too intrusive and not too secure, I guess.

Finally, **how *Vuvuzela*'s ideas could be scale to the whole internet**. As explained in the video, using *Vuvuzela* is already kind of suspicious. But, what if the whole internet was built using *Vuvuzela*'s ideas? It's not something that can be done nowadays as if would require changing protocols used by every single device connected to the internet, but it is interesting to think of how IP, DNS and others protocols would change in this case and if real privacy could be achieved online by these methods.

Future work research related ideas

Tackling the first video, there are millions of things that could be done following this line of work. What other information is accessed by apps that are denied permissions? Is the IMEI the only thing sent? What can be learnt from someone by just knowing their IMEI? What other side channels are used to obtain the IMEI or any other information? Which apps have the code to use this side channel and don't use it, and why?

On the other hand, ***Alpenhorn*** is the natural extension for *Vuvuzela*. It provides a secure way to add friends and establish new connections by just knowing someone else's username (email address) without leaking any metadata. You can read more about it here.