Trumpet Messenger

TU Wien - 188.982 - Privacy Enhancing Technologies

> "Look at those fingerprints, are they small fingerprints?"
> "'If they're small, something else must be small.' I guarantee you, there's no problem. I guarantee."
>
> Mr. Paranoid recently launched his newest project: **The TRUMPET Messenger** ("Make secure messaging great again!").
> This messenger is mainly based on the Signal Protocol, with a simple difference: As Mr. Paranoid thinks, complete fingerprint comparison is only necessary for the elite, the fingerprints of the TRUMPET Messanger are only the last 5 integer values of a typical Signal fingerprint.
>
> We already de-anonymized Mr. Paranoid. But we found out he had an accomplice: Mr. Cipher!
> We also know that Mr. Paranoid was only communicating with him using *The TRUMPET Messenger*.
> **You have to find a way to stop Mr. Cipher too!**

Installing the dependencies

This script uses Python 3, so make sure you are using the correct version.

- Clone `trumpet-axolotl` from GitHub and install it:

  ```
  cd ..
  git clone https://github.com/PETS-TUWien/trumpet-axolotl.git
  cd trumpet-axolotl
  python3 setup.py install
  ```

- Install the requirements for this project:

  ```
  pip3 install -r requirements.txt
  ```

- `trumpet-axolotl` is an intentionally vulnerable library. You should remove it after doing this assignment:

```
pip3 uninstall trumpet-axolotl
```

- If you do not want to install `trumpet-axolotl` directly to your packages, you can also use virtualenv.

Running the script

- Run the script with `python3 trumpet-spoofing.py`
- Make sure there are no import errors anymore!
- The script is `armed`, which means it does not send requests to Mr. Cipher by default.

  It has to be explicitly activated (using the argument `-a`).

  Mr. Cipher will get suspicious if you contact him too often, especially with a fingerprint he doesn't know.

  In other words the backend has a pretty hard rate limit activated! Make sure you implement your solution offline and arm the script then.

Hints

- There is a `TODO` in the code describing what to do.
- Try to understand how the fingerprint check is working by analyzing the `trumpet-axolotl` source.
- Mr. Paranoid's protocol is a bit stripped, he is always directly communicating with Mr. Cipher. You do not have to care about any server middleware, Pre-Keys and so on.
- Mr. Paranoid's implementation is based on `python-axolotl` and he didn't modify the API at all. Therefore please go to python-axolotl for installation instructions, API documentations and examples.