Homework 5

COM402 - Information Security and Privacy 2019

- The homework is due **Tuesday, May 21, 2019 at 23h55 on Moodle**. Submission instructions are on Moodle. Submissions sent after the deadline **WILL NOT** be graded.
- In the event that you find vulnerabilities, you are welcome to disclose them to us (can even have a bonus !)
- Do not forget to submit your source files to Moodle along with your tokens.

(30p) Exercise 1: Listen Carefully

Steganography is the art of hiding data within data. Data can be in the form of files (images, video, audio etc.) or messages. The goal of this exercise is to help you explore a simple steganographic technique and understand how pieces of information can be concealed in files without attracting undue attention.

You are given an audio clip in the WAV file format. You have to find the token in this file. The token is of the form: COM402{**<token>**}. When you submit the token, only submit the portion within the curly brackets, i.e., remove the COM402{} part.

You can find your file in the folder at:
https://drive.google.com/drive/folders/190X0pJ3KxRwKloWf1MThOIMbV3WLGUJ2?usp=sharing
Your file name will be of the form <your_email_address>.wav.
To solve this exercise, you need to look at commonly used steganographic techniques and figure out which technique has been used to hide the token.

Note: While the exercise can be completed without any packages, the wave Python module can be useful when dealing with WAV files. Link: https://docs.python.org/3/library/wave.html **.** Another useful tool in Steganography analysis is ExifTool - it can give you basic information about different file types.

(30p) Exercise 2: Just In Time

In this exercise, you're being asked to guess credentials on the website.

To login, you must send a POST request with a JSON body looking like:

```
{ "email": <youremail>,  "token": <yourguessedtoken> }
```

to

`http://com402.epfl.ch/hw5/ex3`

Don’t try to brute force the token. There are much faster ways to guess the correct token.

For example, the developer here used a modified function to compare strings which express some very specific timing behavior for each valid character in the submitted token…

The response code is `500` when the token is invalid and `200` when the token is valid. Look at the body of the response, you can get some useful information too. The “real” token that you can submit to moodle will be in the response body.

This exercise will require some patience and trial-and-error, as time in networks is never 100% accurate. In order to be precise, you should calibrate your measurements first, before trying to do any guessing on the token.

(40p) Exercise 3: Is it a bird, is it a plane?

This is an exercise on machine learning that we’ll release soon. We’ll post an announcement on Moodle when we update the handouts with the description of the exercise.

Don’t forget to have fun and good luck !