UNSW
SYDNEY

COMP6441

My Something Awesome - Project Report

Frank Su
z5264786

April 9, 2022

Contents

1 Project summary

This project report will detail the process I took to create a keylogger for the "My Something Awesome" project for the COMP6441 course I took during 2022T1. A keylogger is defined as a piece of software that records the keystrokes made on the computer for which the software installed. Within these keystrokes can contain the users credentials allowing unauthorised access to various accounts related to the user.

The keylogger I created fulfils this basic premise of a keylogger but I also implemented other features allowing the attacker to extract other pieces of information about the users device including:

- Exact timing of the keystroke
- Internal/external IPs of the device
- MAC address of the device
- Screen capture of the device upon certain keystrokes

2 Project timeline

For the first couple of weeks I was looking into the idea of another project being if it was possible to create a program that could record from my webcam without triggering the indicator light. However, after some research the knowledge I would need for such a project was far beyond the scope of what I currently know and also not something learn-able over the course of the trimester. Specifically, in order to do this project I would need to learn how to edit my webcams firmware.

Afterwards I decided to pivot into making a keylogger as such a project seemed interesting but also within the bounds of what would be possible throughout this trimester.

The first couple weeks of starting this project involved installation and configuration of the various Python modules that I was going to use to create the keylogger. This process was quite tedious as many of the modules referenced in online guides on how to create a keylogger were deprecated leading

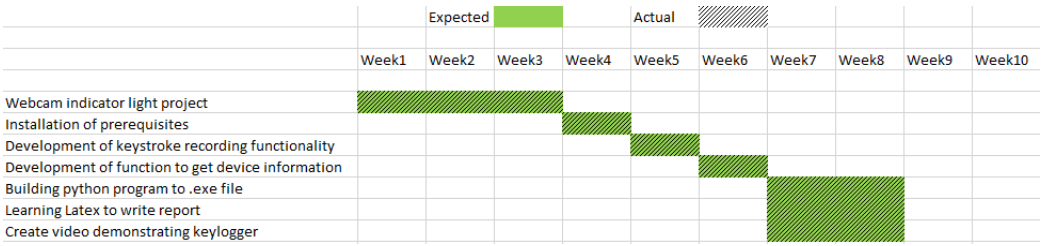
me through a process of trial and error before finding the functionalities I needed that were also still supported. In the end, the keystroke recording functionality was developed using a Python module intended for error-logging purposes.

After finishing the keystroke recording functionality of my keylogger, there was still more time for me to work on this project and so I thought about what other information would be useful to an attacker that I could also write code to easily obtain. This is how I had the idea to implement a feature that would extract the internal/external IPs and the MAC address of the device that the keylogger was installed on. This information could then be used by the attacker for various attacks.

The final screen capture feature came from a consideration of my own computer usage habits. For the sites I frequently visit I have bookmarks set up so that I do not have to type the address each time into the URL bar. In such a situation no keystrokes are recorded and so I implemented a feature where the keylogger will take a screen capture of the device its installed on whenever a "@" keystroke is recorded. This is done as for many websites the login is an email where by combining the recorded keystrokes and information available in the screen capture, attackers will be able to gain access to the accounts depicted in the screen capture.

The major limitation of my keylogger at this stage was that it would only work on computers where Python and all the prerequisites are installed. For the final feature I intended to build my Python program into an executable that could be run on any windows computer. There were are large amount of resources available to achieve this however there was one major flaw with the compiled executable being a command-prompt terminal that briefly flashes for each recorded keystroke. I had some idea on why this was happening but to fix it would involve rewriting my entire keylogger which I unfortunately did not have sufficient time for.

A rough gannt chart of my project progression of over the trimester can be viewed below.



3 Code repo

The repository can be found at `https://github.com/HeadYak/MySomethingAwesome` and to build the program the terminal command is

```
$ pyinstaller keylogger.pyw
```

After building there will be an executable in the dist folder that can be run.

Alternatively to run the python program without building it into an exe the command is

```
$ python3 keylogger.pyw
```

Note that you may need to install prerequisites.

Any keystrokes made while the program is running are found in a file keylog.txt and screenshots are also saved as .png files in the same directory as where the program is.

4 Reflection

I found the process of developing a keystroke very interesting but I honestly imagined it would be harder than it actually was. I suppose this is due to keyloggers not being a new concept. Throughout my readings on keyloggers the FBI already had a piece of keylogging software known as "Magic Lantern" who existence was only made public in 2001 following a freedom of information request.

Similarly, I was surprised how easy it was to write the code for my program to take a screen capture. I figured such a feature would have required administrative privileges much like how the keystroke recording functionality needed it but no such configuration was needed. Perhaps this is due to my Windows user account already having administrator privileges. Additionally, the programs behavior on if the storage was full was not tested, i.e what happens if the program tries to take a screen capture but there is no more storage space. These are the behaviours of my program that I would have tested next if I had more time.

The biggest challenges I faced throughout this project was in general just getting the code to work. Some of the error messages were not very self-explanatory and so much of the effort was spent on trial and error in the debugging process

The terminal error message from below is displayed when you attempt to take a screen capture from inside a virtual machine. In my case I was initially using WSL but had to finish the development of the keylogger within Windows due to this error.

```
user@DESKTOP-PFGGRHO:~/MySomethingAwesome$ python3 keylogger.py
Traceback (most recent call last):
  File "keylogger.py", line 1, in <module>
    from pynput import keyboard
  File "/usr/local/lib/python3.7/dist-packages/pynput/__init__.py", line 40, in <module>
    from . import keyboard
  File "/usr/local/lib/python3.7/dist-packages/pynput/keyboard/__init__.py", line 31, in <module>
    backend = backend(__name__)
  File "/usr/local/lib/python3.7/dist-packages/pynput/_util/__init__.py", line 82, in backend
    if resolutions else '')
ImportError: this platform is not supported: ('failed to acquire X connection: Bad display name ""', DisplayNameError(''))

Try one of the following resolutions:

 * Please make sure that you have an X server running, and that the DISPLAY environment variable is set correctly
user@DESKTOP-PFGGRHO:~/MySomethingAwesome$
```

While creating the keylogger it also occurred to me that hardware keyloggers are also currently used by attackers in committing credit card fraud. Credit card skimmers being the biggest example of this.


AIB
BANKLINK