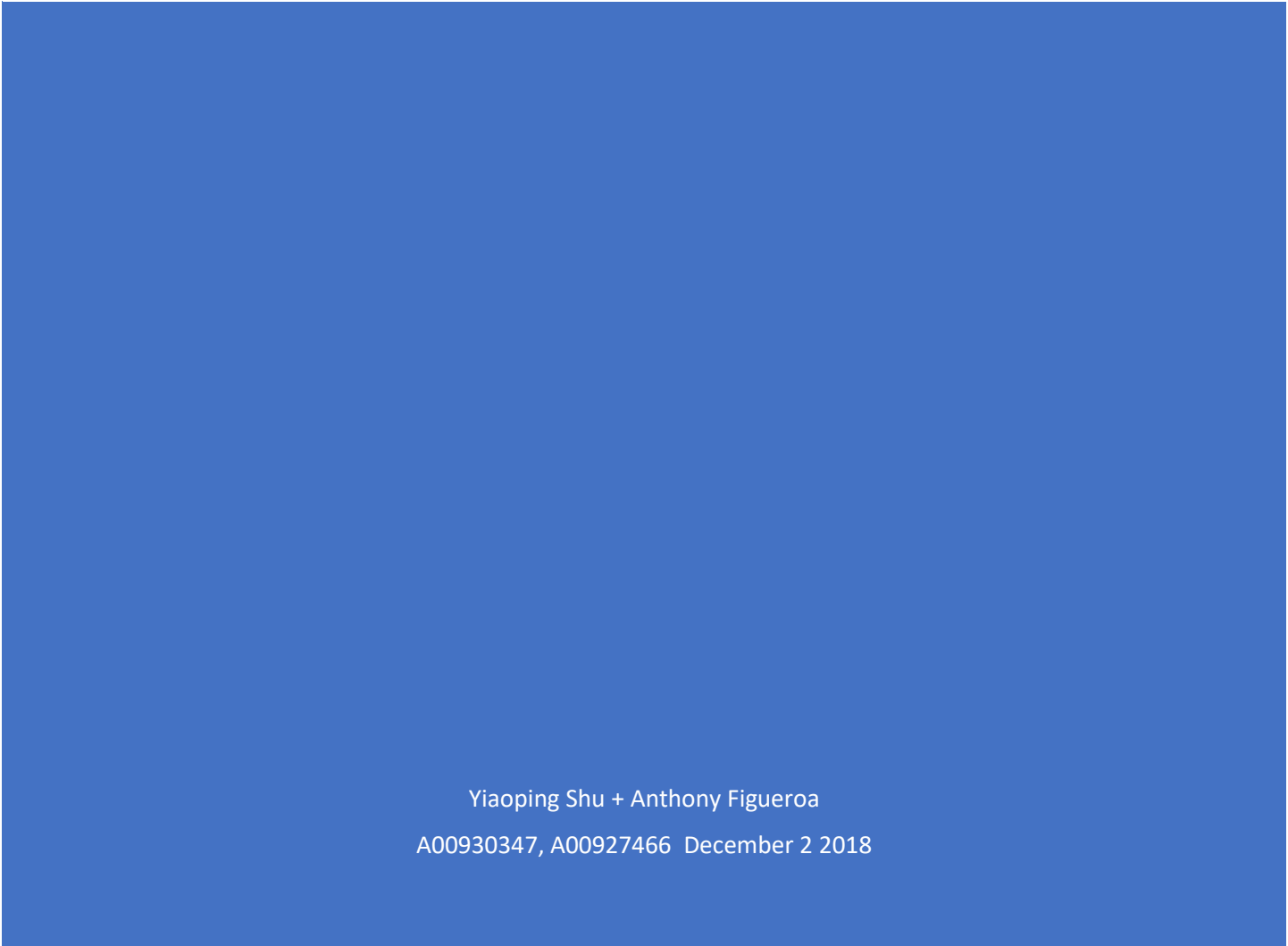




# COMP 8505 FINAL ASSIGNMENT DESIGN DOCUMENT



Viaoping Shu + Anthony Figueroa  
A00930347, A00927466 December 2 2018

## Contents

Covert Backdoor Client State Diagram .....	2
Covert Backdoor Client Pseudocode.....	4
Covert Backdoor Server State Diagram .....	5
Covert Backdoor Server Pseudocode.....	6

## Technical Report

The protocol that was used for this covert backdoor application is done in TCP. The client connects to the server backdoor that's located on the victim machine and sends shell commands to the target to be processed and have the results returned. The client can also send commands such as file watching, which watches a specific directory for changes such as modification, deletion, and creation of file. Another feature of our backdoor application is that it can record keystrokes and logs it to a file. We can then ex-filtrate this, or any other file, downloading the contents of the file to our client. The data (commands, file names, etc) is being sent by means of covert channel through the IP headers. Our processes are all also being masked. A way that the covert activity could be detected is that the user will be able to see transfer of data between our machine and their machine. They can see that the information is coming back to the IP of our machine. Our data is encrypted, but it isn't strongly encrypted. What we could improve on is the encryption and possible use a much harder encryption such as AES encryption. Another way to improve our covert backdoor is to spoof our IP, or have the commands bounce from machine to machine, hiding the origin of the attack. Although we mask the process, the user, if familiar with the process names on his machine, will notice the malicious processes being ran. If possible, like Meterpreter, to improve our backdoor application we can migrate our process to an existing process. A feature that we can add in addition to our program is to take screenshots of the victim machine. Our covert backdoor application is special in that it can change out of the current directory, navigating between different directories and downloading any file it wants. A way to ensure backdoor aren't installed on their computers is to ensure all firewalls are turned on along with anti viruses. Do not be away from the computer without having it shut down or at the minimum, logged off.

## Covert Backdoor Client State Diagram



## Covert Backdoor Client Pseudocode

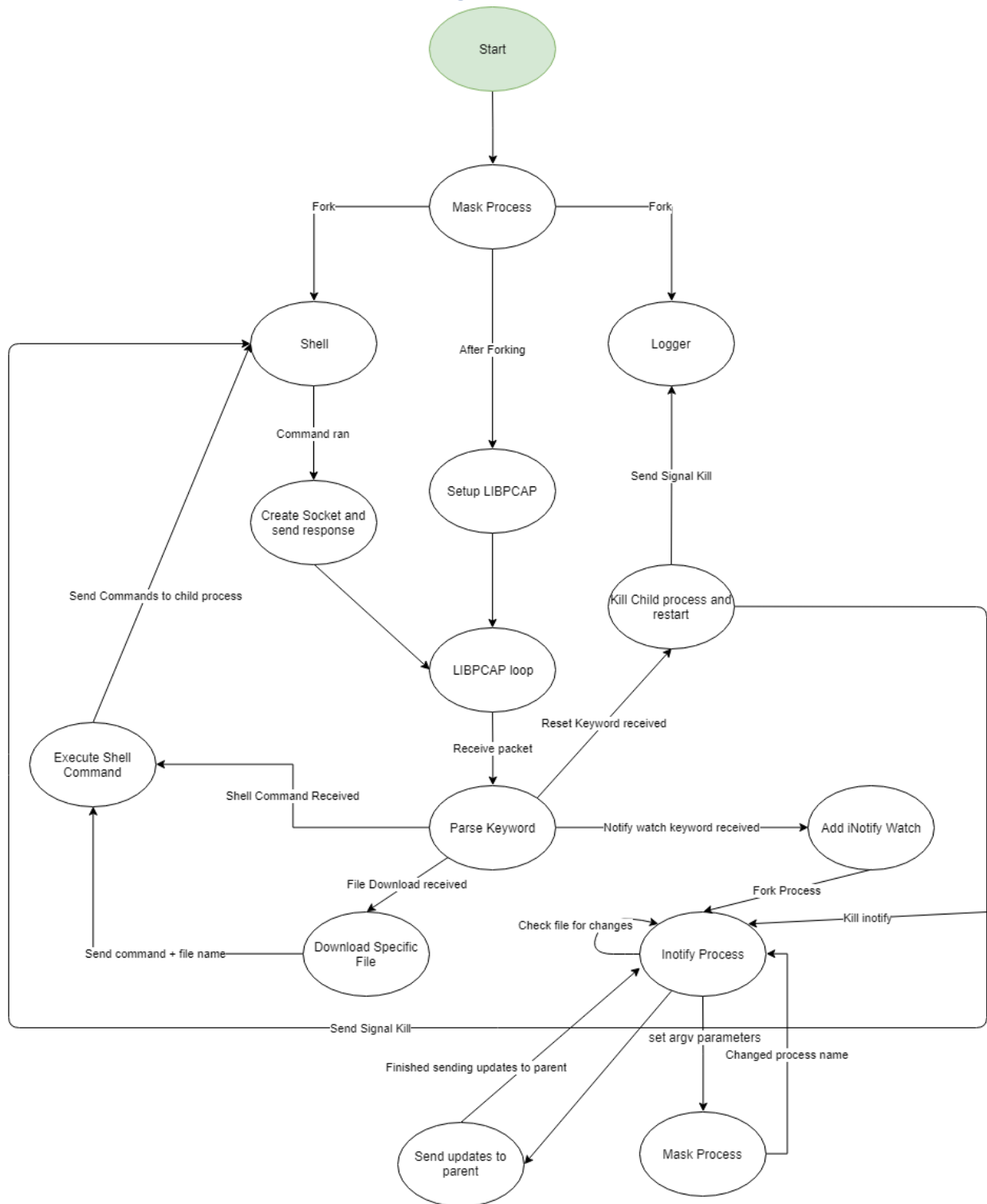
Client started

- Create a socket to read from
- Ask the user for the target Ip
- If the target IP is valid
  - Ask user for source IP
- Connect to target using IPs given
- If connection is successful
  - Display usage to user
- Wait for the user input
- If user received a watch keyword, go to encryption (watch)
- If user received a get keyword, go to encryption (get)
- If user received a reset keyword, go to encryption (reset)
- If user received a command string keyword, go to encryption (string)
- Else if user received exit keyword, exit program
- Wait for response from the server
  - If response from socket, call Encryption(msg)
    - print the decrypted message to user
    - Go back to reading from user input
  - Else if timeout occurs, go back to reading from user input

Encryption(msg)

- Encrypt message
- For each letter in message, xor it with the keyword
- Return the encrypted msg

## Covert Backdoor Server State Diagram



## Covert Backdoor Server Pseudocode

Server started

- Mask the process

- Fork Shell

  - Shell command ran

  - Create the socket and send the response back to client

- Fork Logger

- Setup the Libpcap

- Keep reading for incoming packets

- If packet is received

  - Parse the keyword

- If keyword is shell command

  - Execute the shell command

  - Sent the commands to the forked shell process

- If keyword is File Download

  - Send the command and file name to shell to be processed

- If keyword is notify\_watch

  - Fork inotify\_watch

    - Mask the inotify\_watch process

  - Check for file changes

    - If there's a file change, update the parent

- If keyword is Reset

  - Kill the child process and restart

  - Send Sigkill to logger

  - Send Sigkill to Shell

  - Kill inotify