COMP 8505 Final Project Design Doc

Alex Zielinski – A00803488

03/12/2018

Table of Contents

Finite State Machines 3

Backdoor Software..........3

Command and Control (CnC) Software 4

Pseudo Code 5

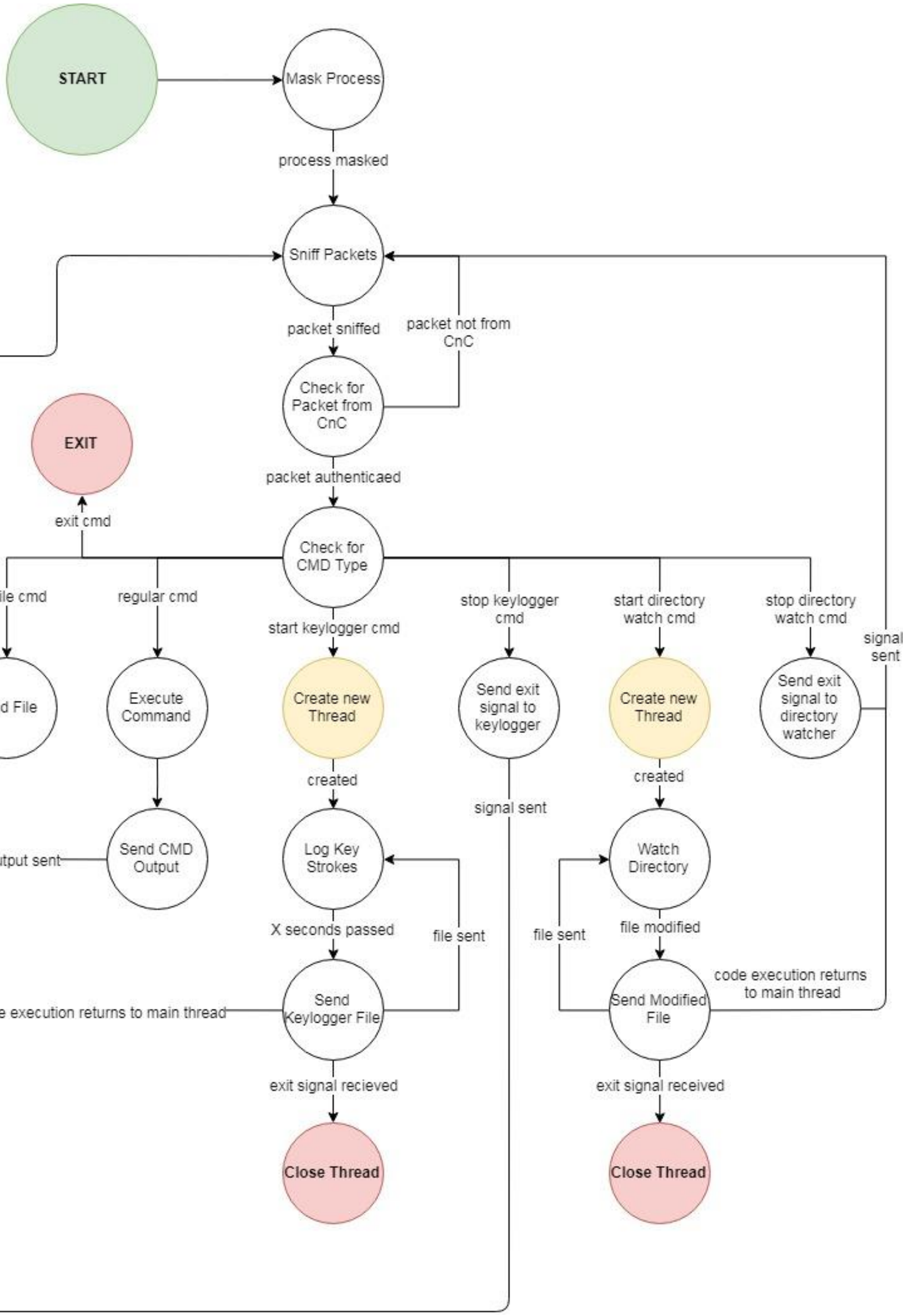
Backdoor Software..........5

Command and Control (CnC) Software 7

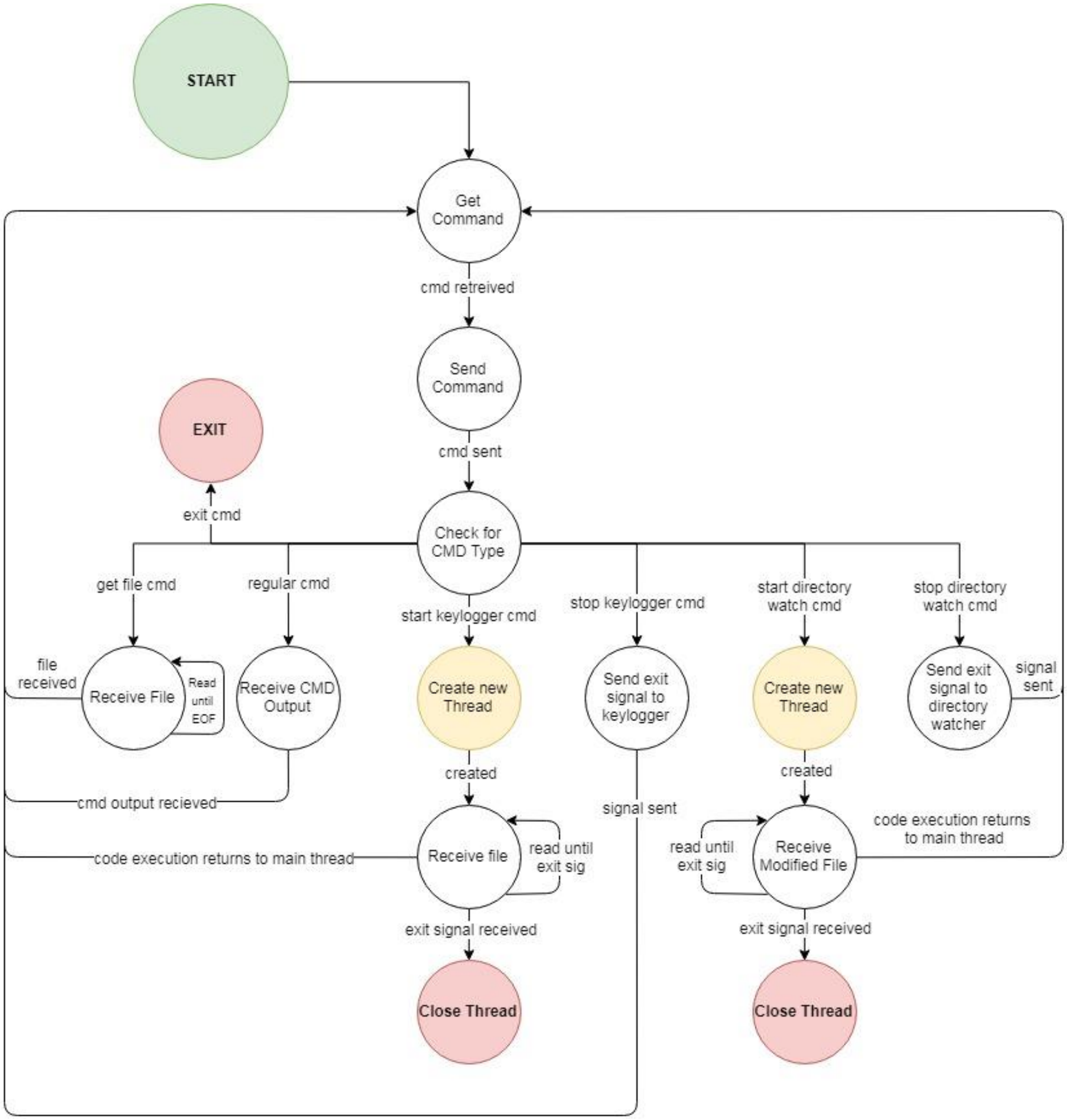
Timeline 9

Finite State Machines

Backdoor Software



Control & Center (CnC) Software



Pseudo Code

Backdoor Software

Mask Process

```
Modify process ID via CMD ARG as to change process name in process table
Go to Sniff Packets
```

Sniff Packets

```
Using libpcap read incoming packet
Go to Check for Packet from CnC
```

Check for Packet from CnC

```
Decrypt payload
If payload contains authentication password, go to Check for CMD Type
Otherwise go back to Sniff Packet
```

Check for CMD Type

```
If command is 'get file' then go to Get File CMD
If command is regular command, then go to Execute CMD
If command is 'start keylogger' then go to Keylogger CMD
If command is 'stop keylogger' then go to Stop Keylogger CMD
If command is 'start directory watch' then go to Directory Watch CMD
If command is 'stop directory watch then go to Stop Directory Watch CMD
Otherwise go back to Sniff Packets
```

Get File CMD

```
Go to Send File and pass file specified via command as parameter
Go back to Sniff Packets
```

Execute CMD

```
Execute command and write output to file
Go to Send File and pass output file as parameter
Go back to Sniff Packets
```

Keylogger CMD

```
Start new thread
Thread
    Loop
        Write keystrokes to file
        If X amount of time passed, then go to Send File and pass key strokes file as parameter
        If exit signal is caught, then exit thread
    Loop
Thread
Main thread execution goes to Sniff Packets
```

Stop Keylogger CMD

```
Send exit signal to keylogger thread
Go back to Sniff Packets
```

Directory Watch CMD

```
Start new thread
Thread
    Loop
        Watch directory for any changes
        If anything changed, then go to Send File and pass file that was modified as parameter
        If exit signal is caught, then exit thread
    Loop
Thread
Main thread execution goes to Sniff Packets
```

Stop Directory Watch CMD

```
Send exit signal to keylogger thread
Go back to Sniff Packets
```

Send File

```
Open file specified by function parameter
Loop
    Read file to buffer
    Encrypt and Encode data into packet
    Send packet
    If more data to read from file, then loop
    Otherwise break out of loop
Loop
Close file
Code execution returns to function that called this ‘Send File’ function
```

Command and Control (CnC) Software

Get Command

```
Get user command
Go to Send Command
```

Send Command

```
Read command into buffer
Encrypt and Encode command into packet
Encrypt and Encode authentication password into password
Send packet
Go to Check for CMD Type
```

Check for CMD Type

```
If command is ‘get file’ then go to Get File CMD
If command is regular command, then go to Execute CMD
If command is ‘start keylogger’ then go to Keylogger CMD
If command is ‘stop keylogger’ then go to Stop Keylogger CMD
If command is ‘start directory watch’ then go to Directory Watch CMD
If command is ‘stop directory watch then go to Stop Directory Watch CMD
Otherwise go back to Get Command
```

Get File CMD

```
Go to Receive File and pass file specified via command as parameter
Go back to Get Command
```

Execute CMD

```
Go to Receive CMD Output
Go back to Get Command
```

Keylogger CMD

```
Start new thread
Thread
    Loop
        Go to Receive File and pass key strokes file as parameter
        If exit signal is caught, then exit thread
    Loop
Thread
Main thread execution goes to Get Command
```

Stop Keylogger CMD

```
Send exit signal to keylogger thread
Go back to Get Command
```

Directory Watch CMD

```
Start new thread
Thread
  Loop
    Go to Receive Modified File
    If exit signal is caught, then exit thread
  Loop
Thread
Main thread execution goes to Get Command
```

Stop Directory Watch CMD

```
Send exit signal to keylogger thread
Go back to Get Command
```

Receive File

```
Open file specified by function parameter
Check for knock
Loop
  Read in a packet
  Decrypt and Decode data into packet
  Write data to file
  If more data to read from file, then loop
  Otherwise if EOF sent then break out of loop
Loop
Close file
Code execution returns to function that called this 'Receive File' function
```

Receive Modified File

```
  Check for knock
  Read in a packet
  Decrypt and Decode data from packet
  Open file specified by data from packet
Loop
  Read in a packet
  Decrypt and Decode data from packet
  Write data to file
  If more data to read from file, then loop
  Otherwise if EOF sent then break out of loop
Loop
Close file
Code execution returns to function that called this 'Receive Modified File' function
```

Timeline

Backdoor Portion	Deadline	CnC Portion	Deadline
-	-	Port Knocking	Thursday Nov 8, 2018
Process Masking	Thursday Nov 8, 2018	-	-
Authenticate Packets	Thursday Nov 8, 2018	Authenticate Packets	Thursday Nov 8, 2018
Exit CMD Functionality	Saturday Nov 10, 2018	Exit CMD Functionality	Saturday Nov 10, 2018
Regular CMD Functionality	Saturday Nov 10, 2018	Regular CMD Functionality	Saturday Nov 10, 2018
Get File Functionality	Monday Nov 12, 2018	Get File Functionality	Monday Nov 12, 2018
Start Keylogger Functionality	Sunday Nov 18, 2018	Start Keylogger Functionality	Sunday Nov 18, 2018
Stop Keylogger Functionality	Wednesday Nov 21, 2018	Stop Keylogger Functionality	Wednesday Nov 21, 2018
Start Directory Watch Functionality	Sunday Nov 25, 2018	Start Directory Watch Functionality	Sunday Nov 25, 2018
Testing	Sunday Dec 3, 2018	Testing	Sunday Dec 3, 2018
Documentation	Sunday Dec 3, 2018	Documentation	Sunday Dec 3, 2018