EE379K Enterprise Network Security Lab 1 Report

Student: Brian Cheung bc32427
Professor: Mohit Tiwari
TA: Antonio Espinoza
Department of Electrical & Computer Engineering
The University of Texas at Austin

September 9, 2019

1 Part 1

part 1 paragraph

1.1 Step 1 - Echo Server

1.1.1 Build server and client

In a terminal window, start at root directory of project and run the following commands:

```
$ cd Part\ 1
$ make
```

1.1.2 Run server and client

Run the following commands to start the server:

```
$ cd Part\ 1
$ ./server
```

Open a new terminal window and run the following commands to start the client:

```
$ cd Part\ 1
$ ./client
```

1.2 Step 2 - DOS Attack

The DOS attack was performed using a program called ***hping3***. The attacker flooded the server with SYN packets while using a spoofed IP address to hide the source IP address. Without the correct IP, the server was unable to send SYN and ACK packets back to the attacker, which prevented the three-way handshake from being completed. By flooding the server with SYN packets and preventing the three-way handshake from being completed, the server cannot process other clients' requests because it is too busy trying to complete the attacker's requests, so clients that want to connect to the server are left waiting.
The following command was used to perform the DOS attack:

```
$ sudo hping3 -S -w 64 -p 12000 --flood --rand-source 127.0.0.2
```

hping3 command flags and options:
-S: flood with SYN packets
-p: 12000: port 12000
–**flood**: send packets as fast as possible
–**rand-source**: generates a spoofed IP address to hide the source IP
127.0.0.2: IP address of server

2 Part 2

part 2 paragraph
Example Figure 1 shows X. Example reference to paper [1].

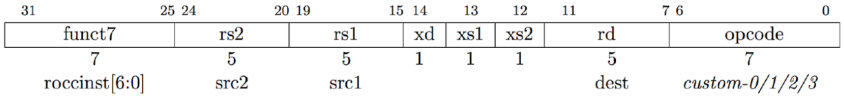

Figure 1: The RoCC Accelerator Instruction Encoding

3 Part 3

part 3 paragraph

```
int main() {
  printf("Hello World");
```

```
    return 0;
}
```

4 Part 4

5 Conclusion

Please provide feedback so we can improve the labs for the course. How many hours did the lab take you? Was this lab boring? Did you learn anything? Is there anything you would change? Feel free to put anything here, but leaving it blank will result in the loss of points.

References

[1] F. Brasser, U. Müller, A. Dmitrienko, K. Kostiainen, S. Capkun, and A.-R. Sadeghi, "Software grand exposure: SGX cache attacks are practical," in *11th USENIX Workshop on Offensive Technologies (WOOT 17)*, (Vancouver, BC), USENIX Association, 2017.