

Misuse/Attack Possibilities and Defense in Open Source Software-Defined Networking

Seungsoo Lee
NSS LAB

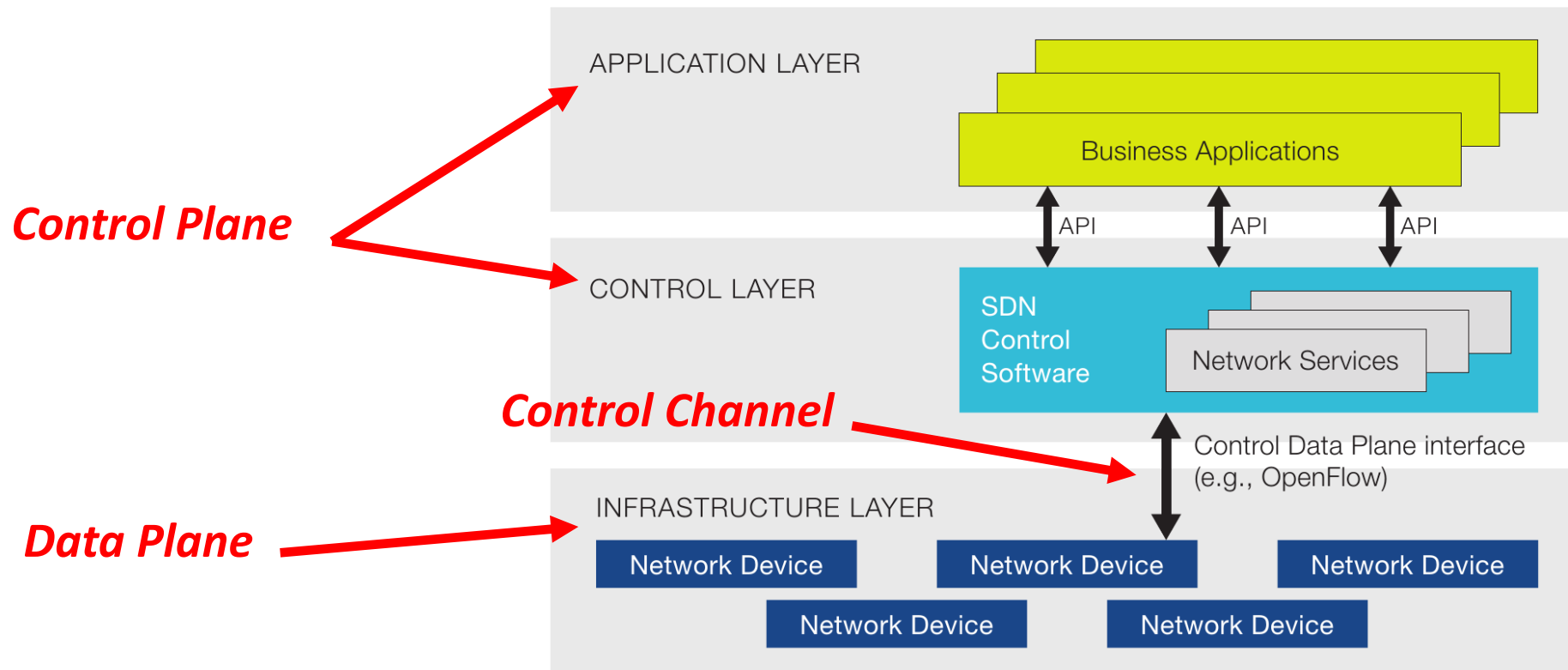
4/8/2016 (Fri.)

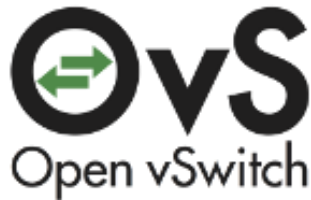
Open Networking Korea 2016 Spring

Contents

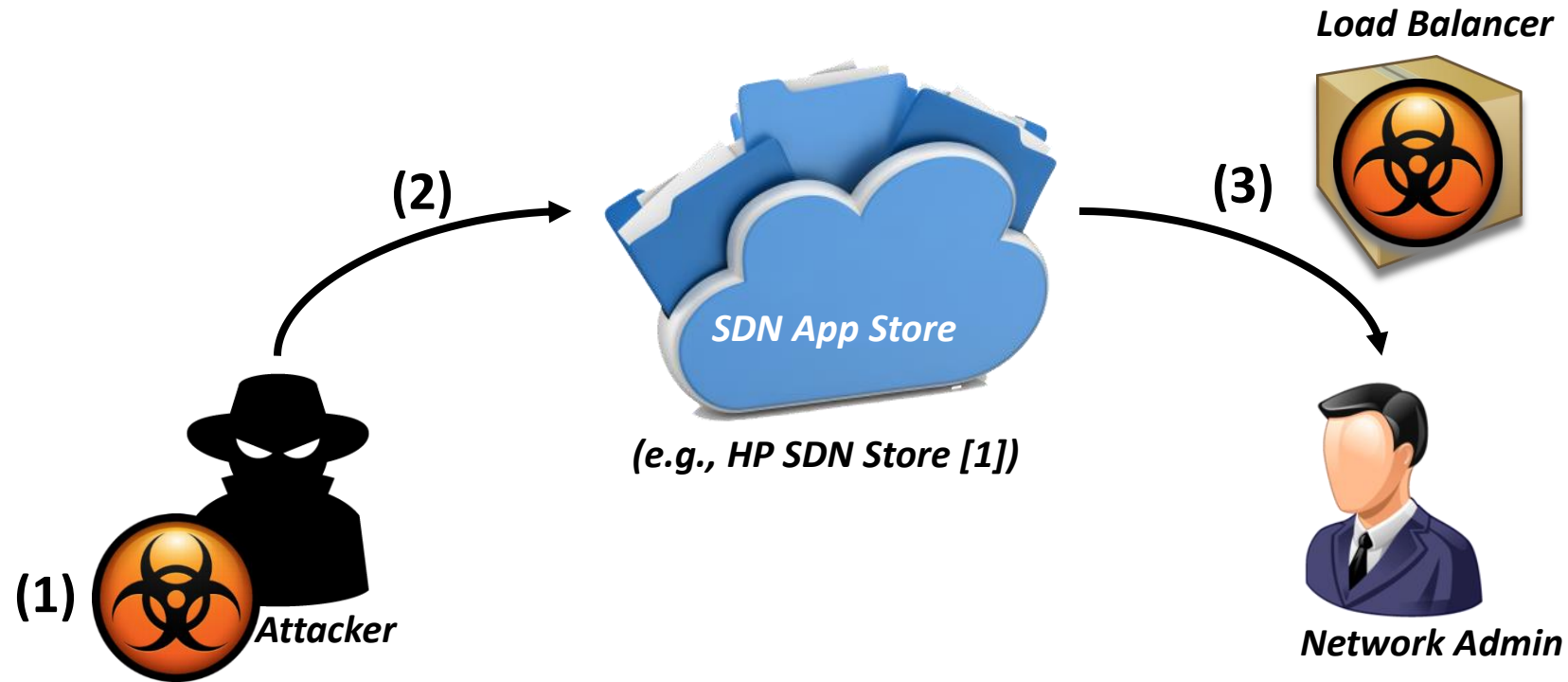
1. Introduction
2. Background
3. Attack Overview
4. Control Plane Attack
5. Control Channel Attack
6. Data Plane Attack
7. Possible Defense Mechanism

- SDN only leaves ***simple data plane functions*** (at which hardware is good) to a network device and moves complex and dynamic control plane functions into software applications at a separate box, a controller.

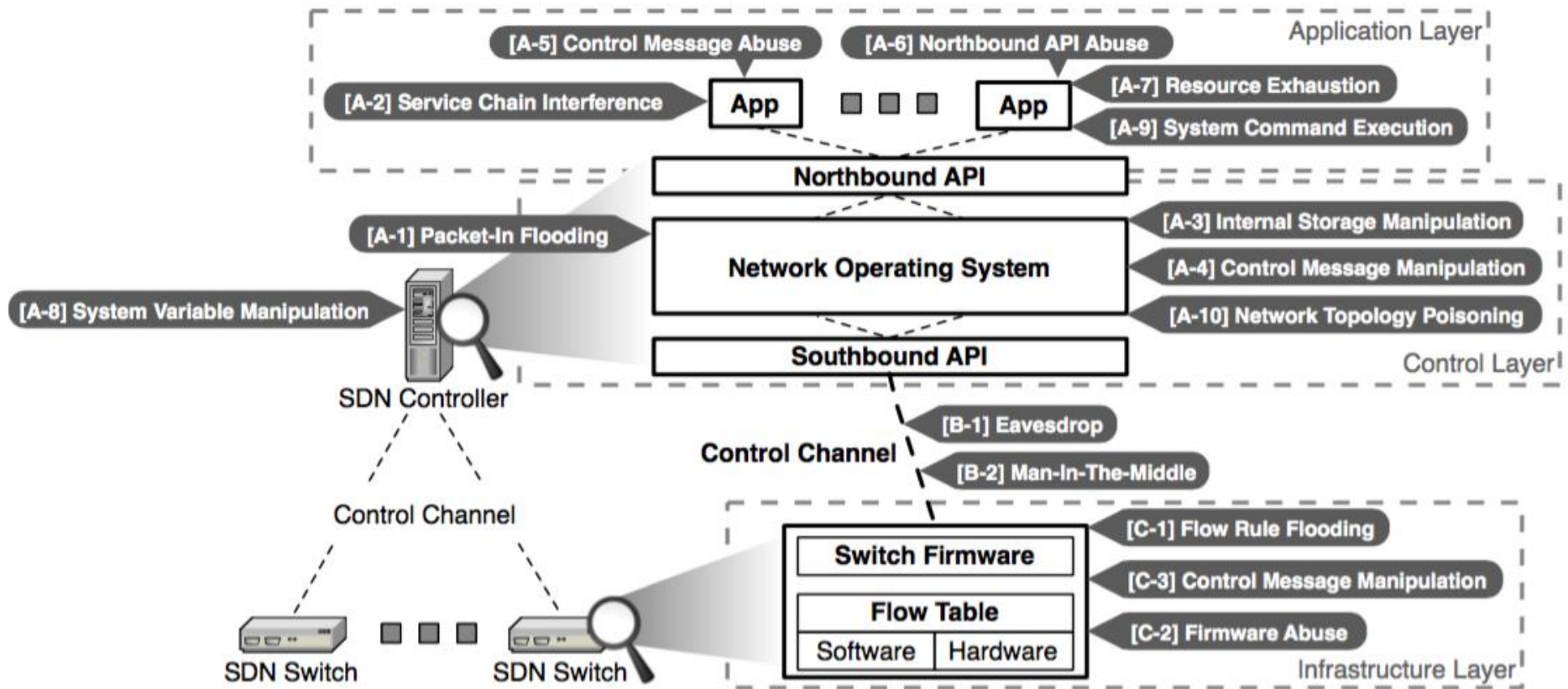




- Controller (Network operating system) manages the entire SDN environment as the ***control plane***
- Popular ***open-source*** controllers (e.g., ONOS and OpenDaylight)



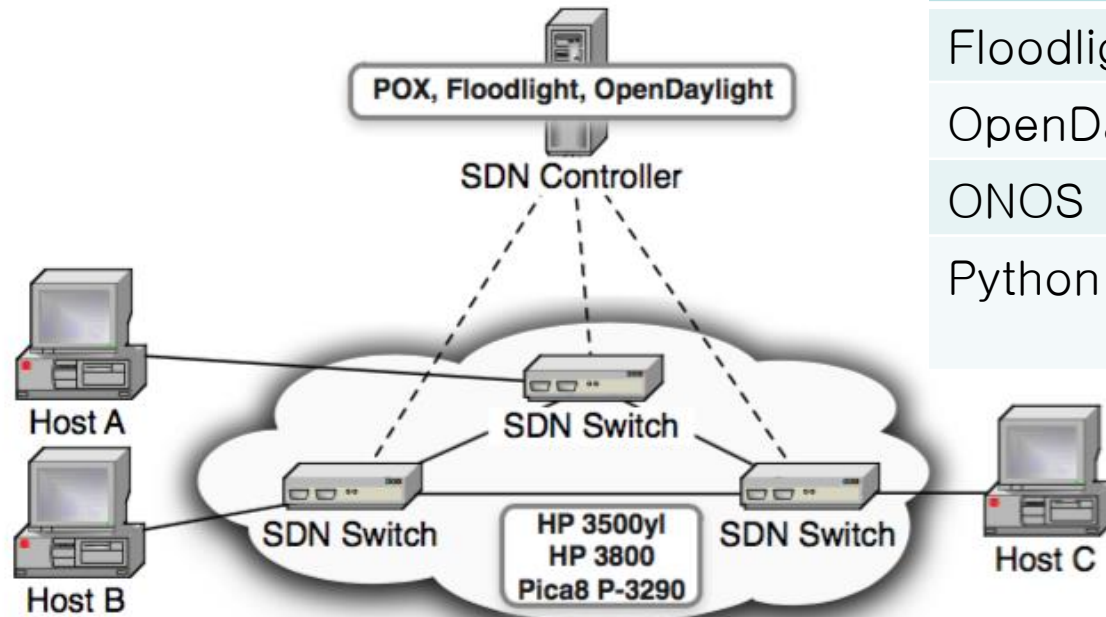
- i) Controller plays a role as the traditional operating systems
→ There are also **security holes** !
- ii) Anyone can easily develop and distribute SDN applications



- **Control Plane** : Application Layer + Control Layer (A-1 ~ A-10)
- **Control Channel** : Channel between Controller and Switch (B-1 ~ B-2)
- **Data Plane** : Infrastructure Layer (C-1 ~ C-3)

LIST OF TESTED SDN CONTROLLERS

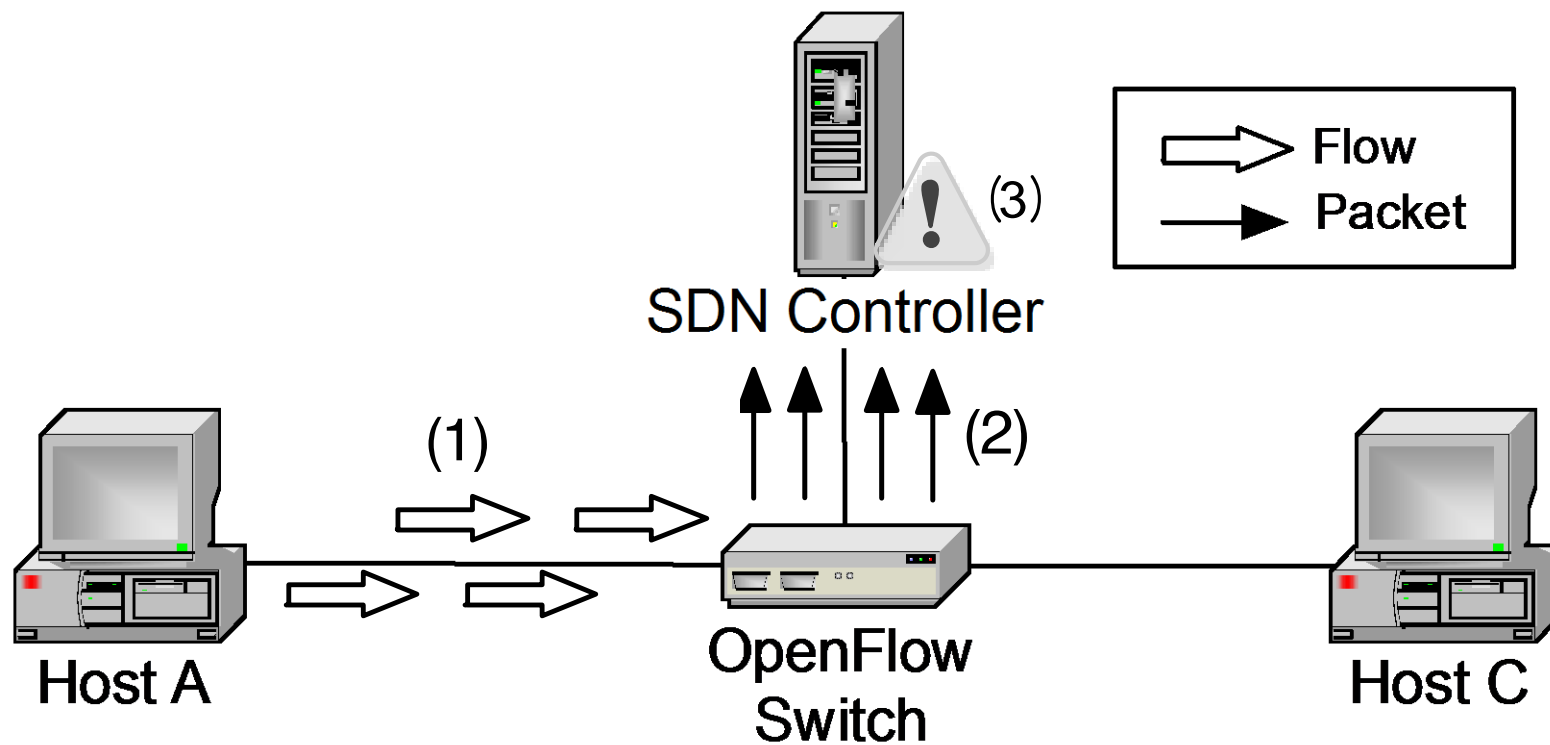
<i>Name</i>	<i>Language</i>	<i>Version</i>
Floodlight	JAVA	v0.91
OpenDaylight	JAVA	helium-sr3
ONOS	JAVA	v1.1
Python	Python	Active: dart-2 01 4-summer



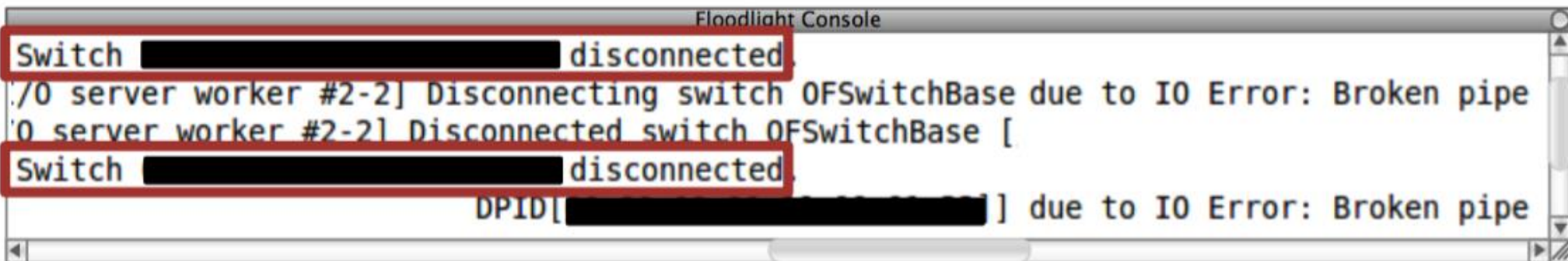
LIST OF TESTED SDN SWITCHES

<i>Vendor</i>	<i>Switch Model</i>	<i>Firmware Version</i>
HP	3500yl	K.15.12.0010
HP	3800	KA.15.13.0005
Pica8	P-3290	PicOS 2.3

- Scenario



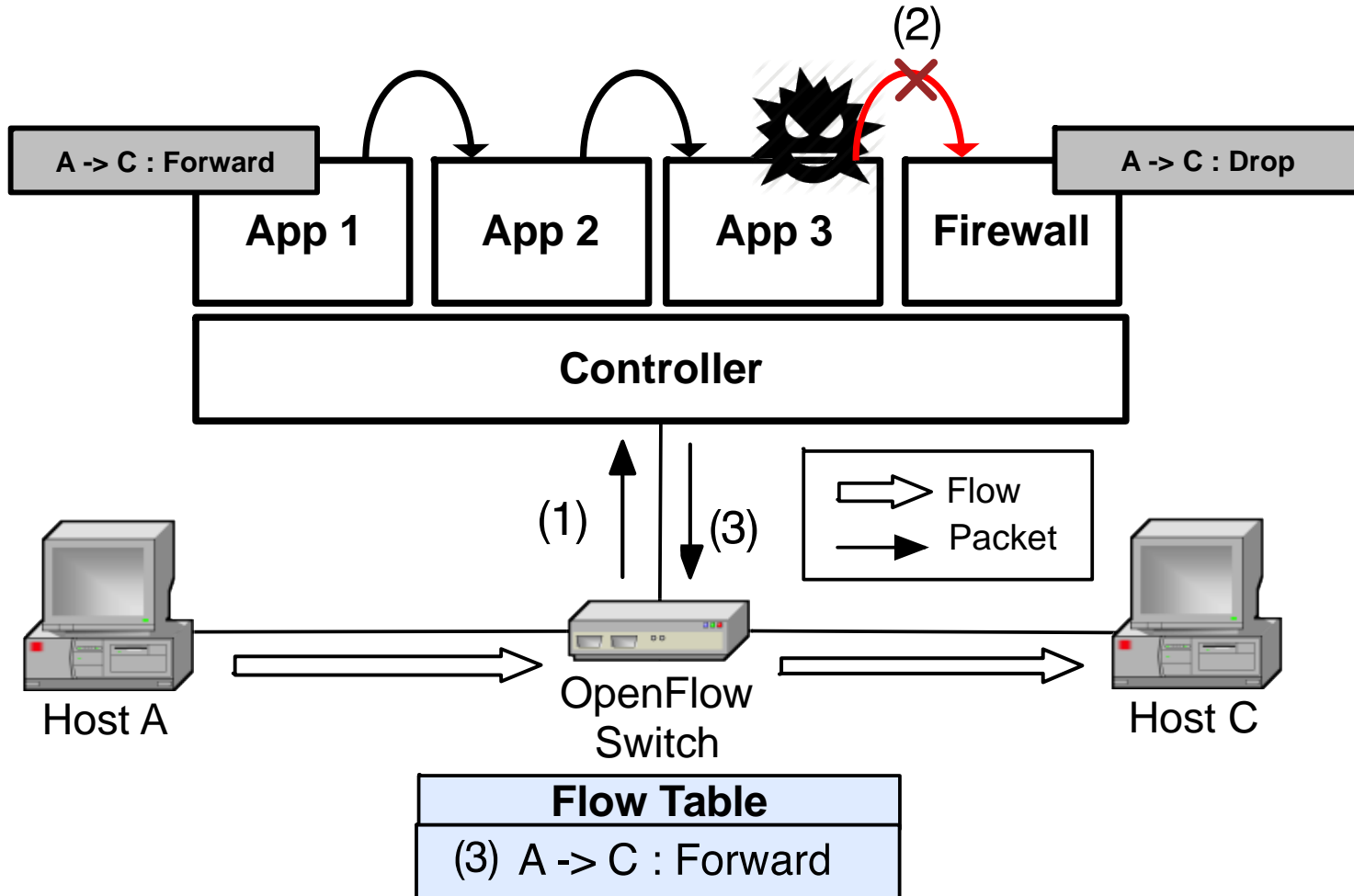
- Switch disconnection



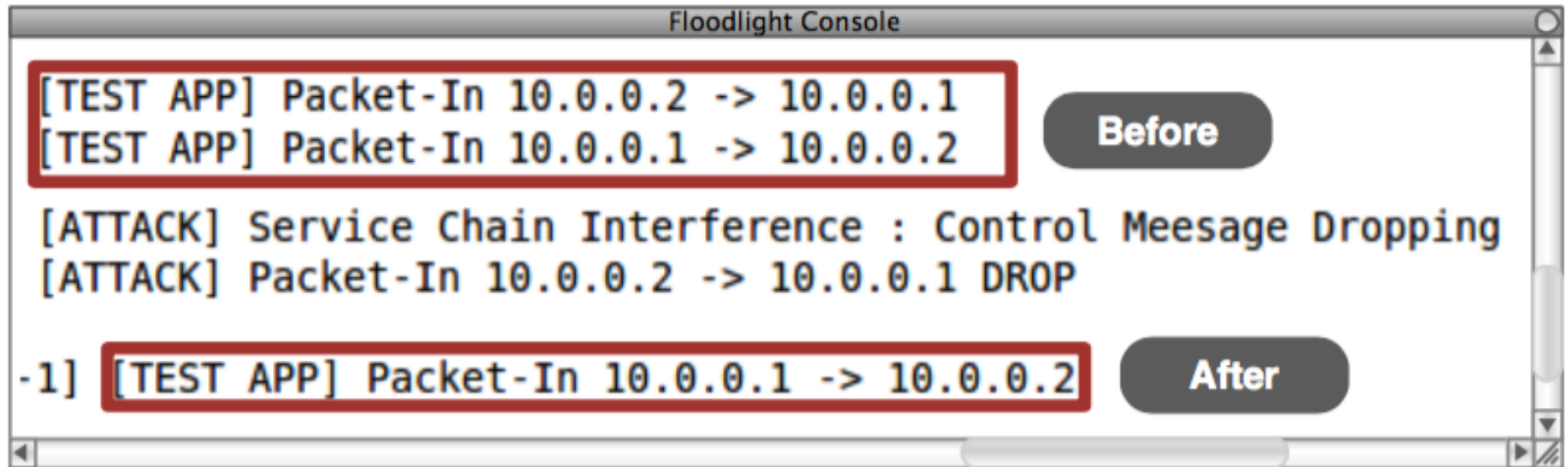
The screenshot shows a terminal window titled "Floodlight Console". It contains several lines of log output. Two lines are highlighted with red rectangular boxes: "Switch [REDACTED] disconnected." and "Switch [REDACTED] disconnected.". The other visible log lines include: ". /0 server worker #2-2] Disconnecting switch OFSwitchBase due to IO Error: Broken pipe", ". /0 server worker #2-2] Disconnected switch OFSwitchBase [", and "DPID[[REDACTED]] due to IO Error: Broken pipe".

```
Floodlight Console
Switch [REDACTED] disconnected.
./0 server worker #2-2] Disconnecting switch OFSwitchBase due to IO Error: Broken pipe
./0 server worker #2-2] Disconnected switch OFSwitchBase [
Switch [REDACTED] disconnected.
DPID[ [REDACTED] ] due to IO Error: Broken pipe
```


- Scenario



- Packet-In cut-off



The screenshot shows a window titled "Floodlight Console" with a log of network events. The logs are divided into two sections: "Before" and "After".

Before:

- [TEST APP] Packet-In 10.0.0.2 -> 10.0.0.1
- [TEST APP] Packet-In 10.0.0.1 -> 10.0.0.2

Attack Event:

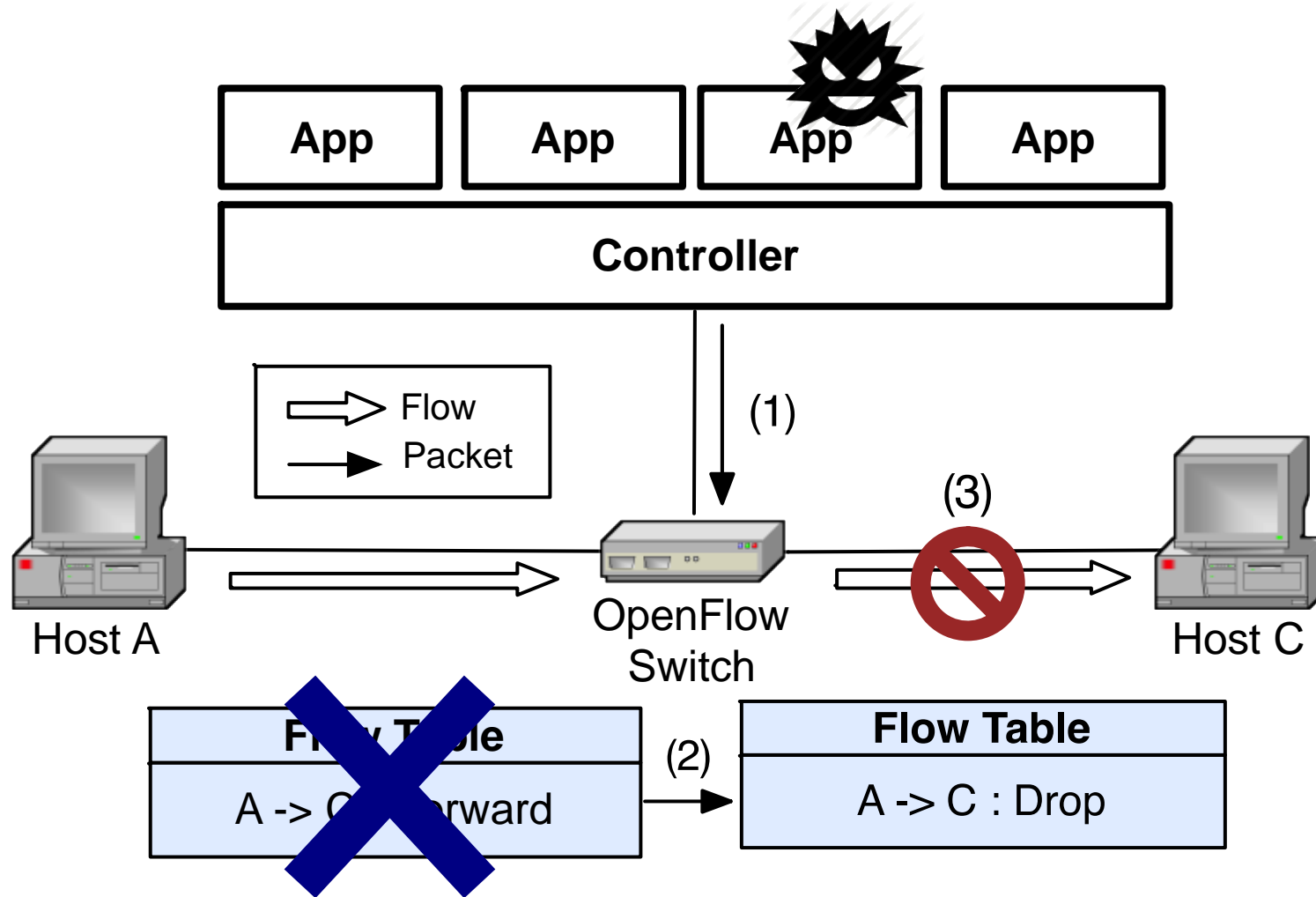
- [ATTACK] Service Chain Interference : Control Meesage Dropping
- [ATTACK] Packet-In 10.0.0.2 -> 10.0.0.1 DROP

After:

- 1] [TEST APP] Packet-In 10.0.0.1 -> 10.0.0.2

The "After" section shows that only the packet from 10.0.0.1 to 10.0.0.2 is received, while the packet from 10.0.0.2 to 10.0.0.1 is dropped.

- Scenario



- Modification Result

The image displays two screenshots of the Floodlight web interface, illustrating a flow rule modification. The top screenshot, labeled 'Before', shows a table of flow rules. The bottom screenshot, labeled 'After', shows the same table with the action field removed for the second rule.

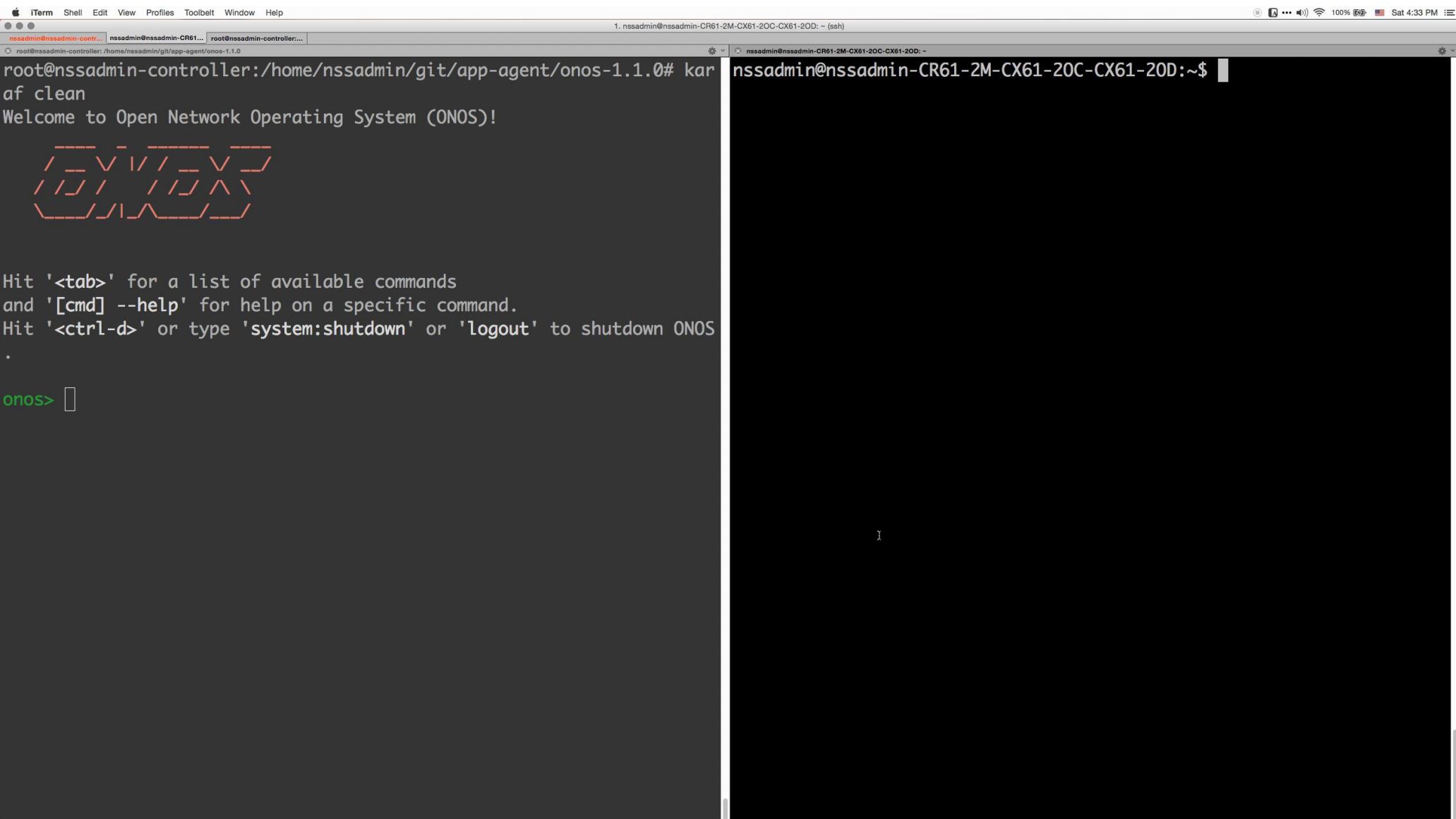
Before State:

Cookie	Priority	Match	Action
9007199254740992	0	port=17, VLAN=-1, prio=0, src=50:b7:c3:7d:2e:8a, dest=f0:bf:97:e9:49:84	output 19
9007199254740992	0	port=19, VLAN=-1, prio=0, src=f0:bf:97:e9:49:84, dest=50:b7:c3:7d:2e:8a	output 17

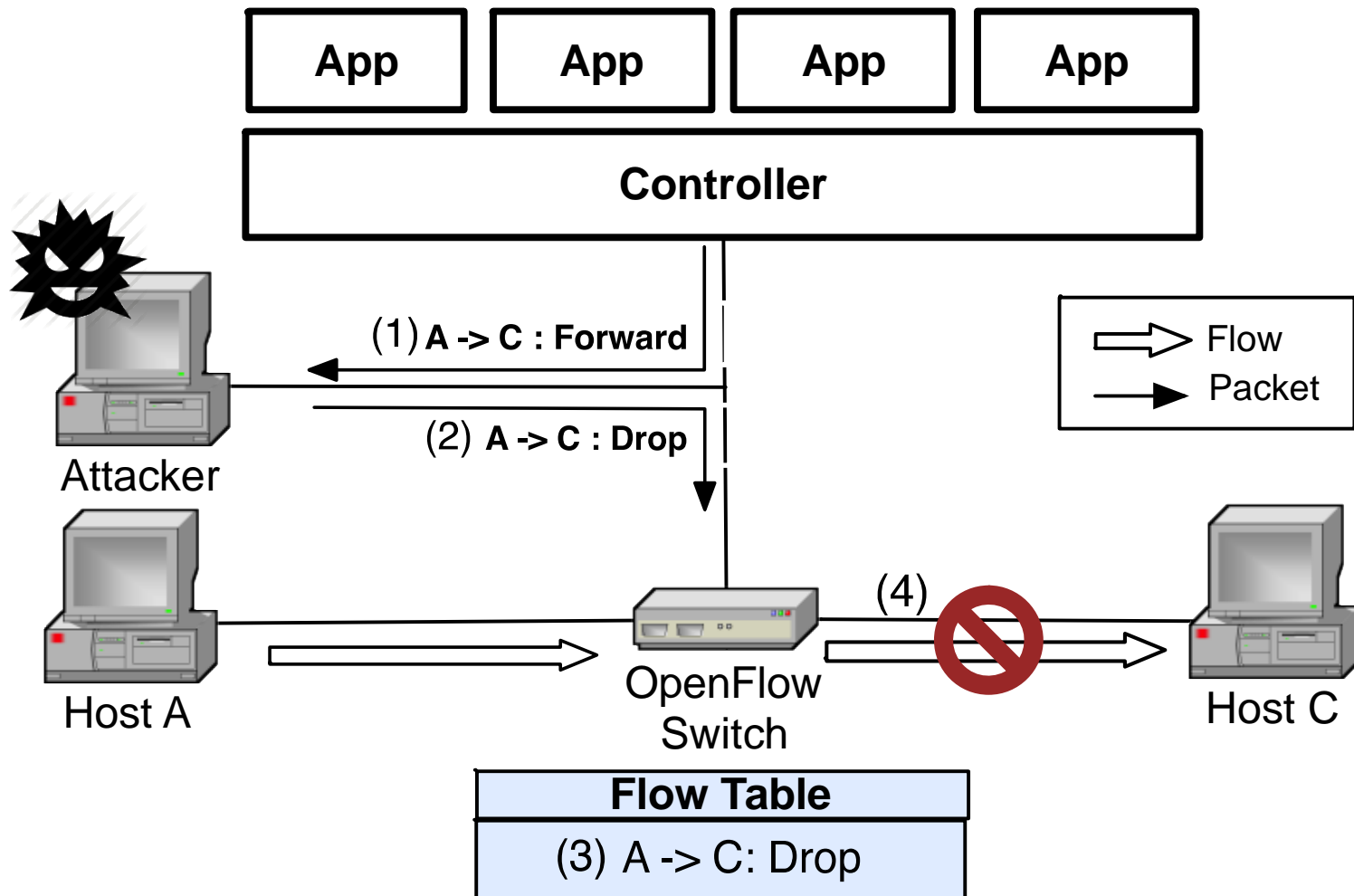
After State:

Match	Action
port=17, VLAN=-1, prio=0, src=50:b7:c3:7d:2e:8a, dest=f0:bf:97:e9:49:84	output 19
port=19, VLAN=-1, prio=0, src=f0:bf:97:e9:49:84, dest=50:b7:c3:7d:2e:8a	

Action field removed



- Scenario



The image shows a Floodlight GUI window titled "Flows (2)" and a Wireshark 1.8.2 window titled "Capturing from Pseudo-device that captures on all interfaces: any".

Wireshark Filter: `of.pktout && icmp`

No.	Time	Source	Destination	Protocol	Length	Info
2033	146.797185000	10.0.0.3	10.0.0.1	OFP+ICMP	270	Packet Out (OFP+ICMP)
2037	146.805351000	10.0.0.1	10.0.0.3	OFP+ICMP	270	Packet Out (OFP+ICMP)

Output Action(s)

- ▼ Action
 - Type: Output to switch port (0)
 - Len: 8
 - Output port: 15**
 - Max Bytes to Send: 65535
 - # of Actions: 1

The actual flow rule issued

Flow Rule Table:

Cookie	Priority	Match	Action
9007199254740992	0	port=15, VLAN=-1, prio=0, src=e8:11:32:4c:42:03, dest=50:b7:c3:7d:2e:8a	output 17
9007199254740992	0	port=17, VLAN=-1, prio=0, src=50:b7:c3:7d:2e:8a, dest=e8:11:32:4c:42:03	

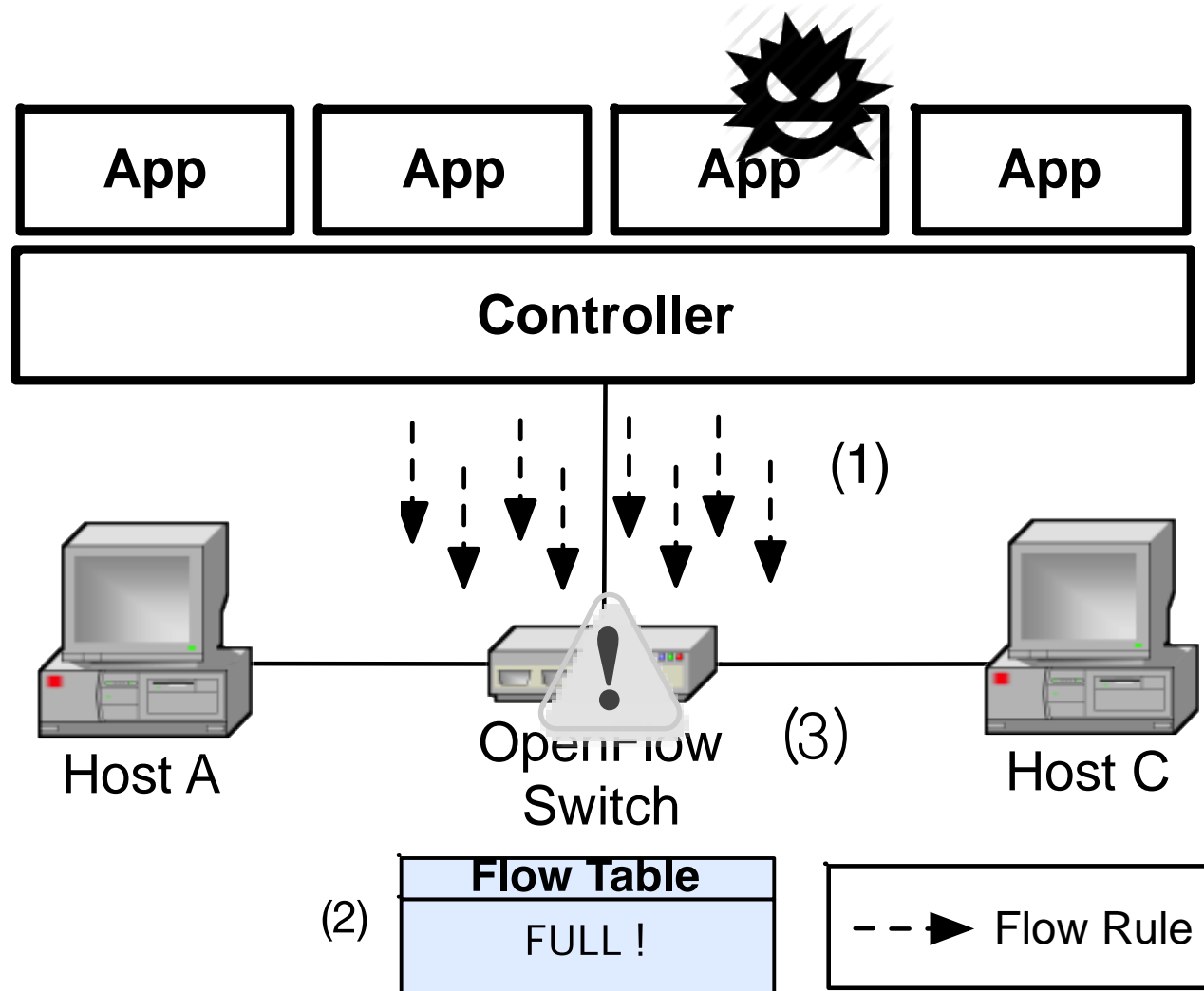
Different flow rule installed

[B-2] MITM attack

5. Control Channel Attack

[illegible]

- Scenario



Before

```
nss@nss-VPCSA35GK:~$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_req=1 ttl=128 time=5.31 ms
64 bytes from 10.0.0.1: icmp_req=2 ttl=128 time=1.18 ms
64 bytes from 10.0.0.1: icmp_req=3 ttl=128 time=1.21 ms
64 bytes from 10.0.0.1: icmp_req=4 ttl=128 time=1.19 ms
```

Flows (32768) ← Number of Flow Rules Installed

Cookie	Priority	Match
32766	32766	port= src=1
32765	32765	port= src=1
32764	32764	port= src=1

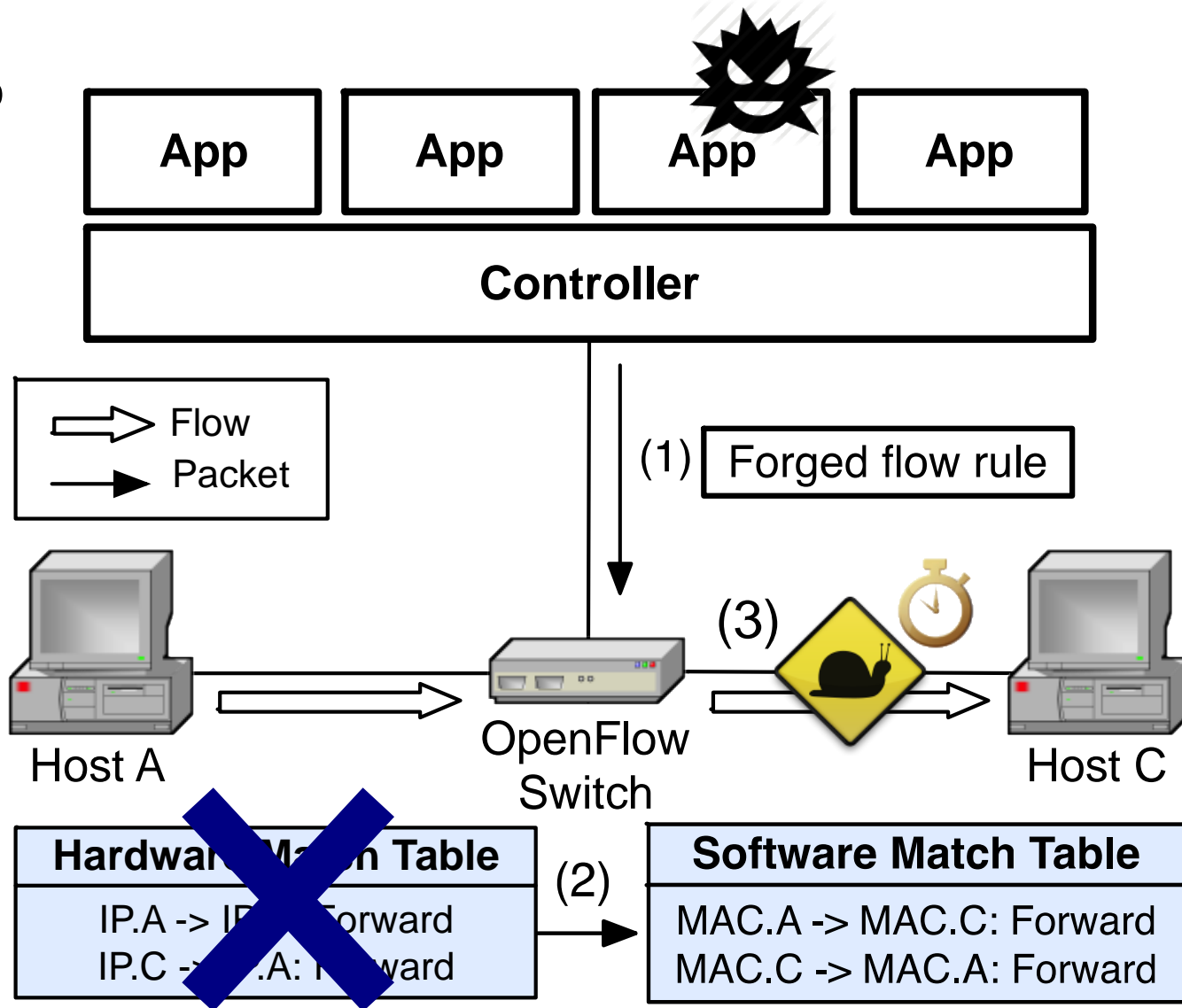
After

```
nss@nss-VPCSA35GK:~$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_req=1 ttl=128 time=787 ms
64 bytes from 10.0.0.1: icmp_req=2 ttl=128 time=1.14 ms
64 bytes from 10.0.0.1: icmp_req=3 ttl=128 time=1.04 ms
```

150x < performance degradation

```
onos>
```

- Scenario



- Degrading network performance

The image displays two terminal windows. The top window, titled 'Floodlight Console', shows a message: 'ver worker #2-1] [ATTACK] Control Message Abuse : Flow Rule Clearance' followed by two lines of text: 'Clearing all flows on switch OFSwitchBase [/10.0.0.252:51248 DPID[00:' and 'Clearing all flows on switch OFSwitchBase [/10.0.0.252:51248 DPID[00:'. A red box highlights these two lines, and a red arrow points from this box to the 'After' console window. Below the Floodlight Console window, the 'Host Console' window is shown. It is divided into two sections: 'Before' and 'After'. The 'Before' section shows a 'ping 10.0.0.1' command and its output: 'ping 10.0.0.1' followed by '1: icmp_req=1 ttl=128 time=5.31 ms', '1: icmp_req=2 ttl=128 time=1.18 ms', '1: icmp_req=3 ttl=128 time=1.21 ms', and '1: icmp_req=4 ttl=128 time=1.19 ms'. A red box highlights the four low-latency results. The 'After' section shows the same 'ping 10.0.0.1' command, but the output is partially obscured by a large red box. A red arrow points from the 'Before' box to the 'After' box, with a label '~ 500x Latency increase'. The 'After' box contains the text '64 bytes from 10.0.0.1: icmp_req=1 ttl=128 time=5.26 ms', '64 bytes from 10.0.0.1: icmp_req=2 ttl=128 time=5.25 ms', and '64 bytes from 10.0.0.1: icmp_req=3 ttl=128 time=5.67 ms'. A red box highlights these three high-latency results.

Floodlight Console

```
ver worker #2-1] [ATTACK] Control Message Abuse : Flow Rule Clearance
Clearing all flows on switch OFSwitchBase [/10.0.0.252:51248 DPID[00:
Clearing all flows on switch OFSwitchBase [/10.0.0.252:51248 DPID[00:
```

Persistent flow table clearance

Host Console

Before

```
ping 10.0.0.1
1: icmp_req=1 ttl=128 time=5.31 ms
1: icmp_req=2 ttl=128 time=1.18 ms
1: icmp_req=3 ttl=128 time=1.21 ms
1: icmp_req=4 ttl=128 time=1.19 ms
```

~ 500x Latency increase

After

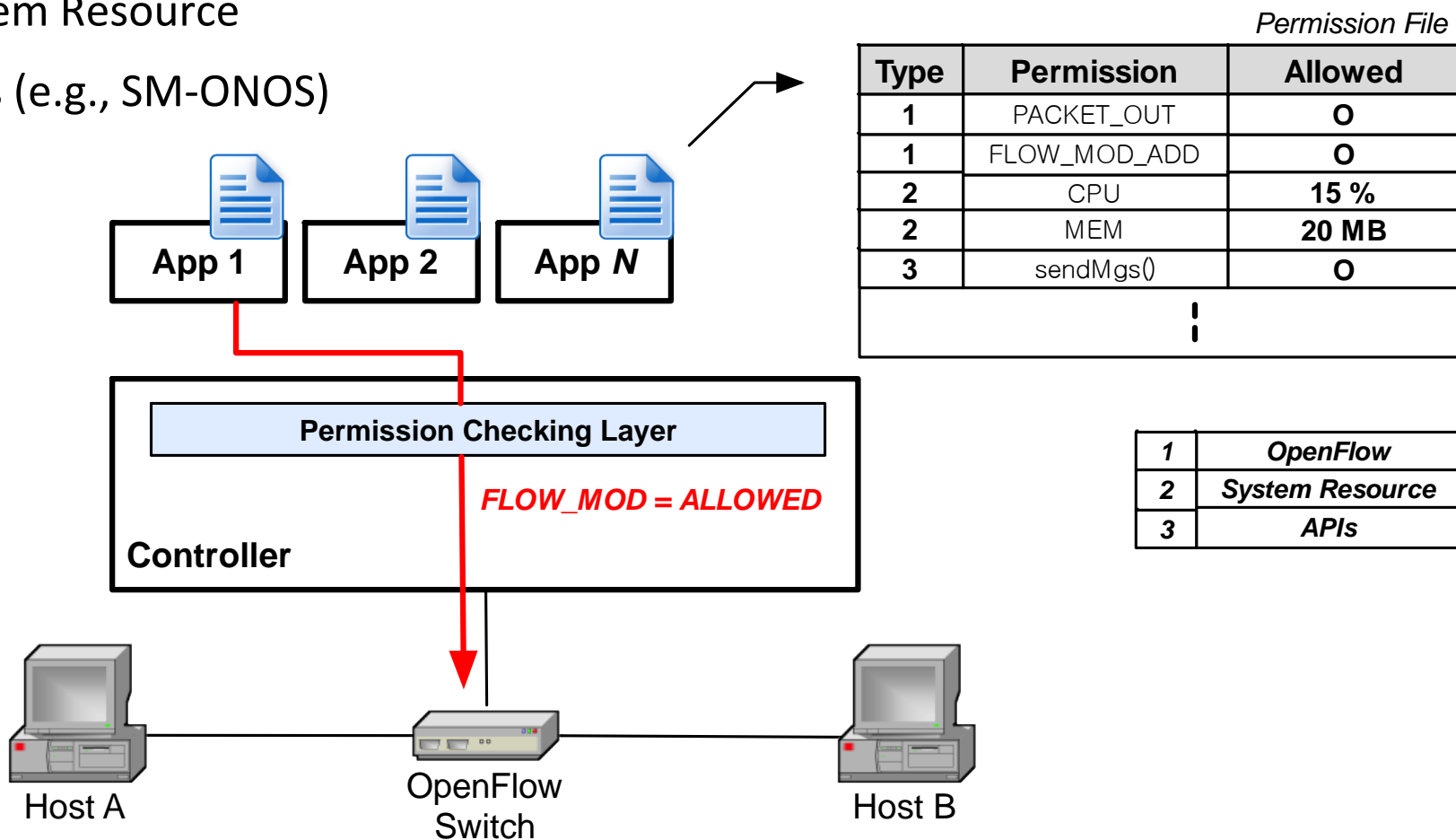
```
64 bytes from 10.0.0.1: icmp_req=1 ttl=128 time=5.26 ms
64 bytes from 10.0.0.1: icmp_req=2 ttl=128 time=5.25 ms
64 bytes from 10.0.0.1: icmp_req=3 ttl=128 time=5.67 ms
```



```
iTerm Shell Edit View Profiles Toolbelt Window Help
1. nssadmin@nssadmin-CR61-2M-CX61-20C: ~ (ssh)
root@nssadmin-controller: /home/nssadmin/workspace/s3/floodlight
nssadmin@nssadmin-CR61-2M-CX61-20C-CX61-20D: ~$
tchImpl, writeThrottle=false, description Switch Desc - Vendor: HP Ne
tworking Model: BTTF Make: None Version: VER 1.0 S/N: None
06:36:28.480 INFO [n.f.c.OFSwitchBase:New I/O server worker #2-1] Cle
aring all flows on switch OFSwitchBase [/10.0.0.253:51514 DPID[00:0a:
f0:92:1c:21:5d:80]]
06:36:28.482 WARN [n.f.c.i.C.s.notification:main] Switch 00:0a:f0:92:
1c:21:5d:80 connected.
06:36:28.919 INFO [n.f.c.i.OFChannelHandler:New I/O server worker #2-
2] New switch connection from /10.0.0.252:57245
06:36:28.922 INFO [n.f.c.i.OFChannelHandler:New I/O server worker #2-
2] Switch OFSwitchBase [/10.0.0.252:57245 DPID[00:0a:f0:92:1c:21:3d:c
0]] bound to class class net.floodlightcontroller.core.internal.OFSwi
tchImpl, writeThrottle=false, description Switch Desc - Vendor: HP Ne
tworking Model: BTTF Make: None Version: VER 1.0 S/N: None
06:36:28.923 INFO [n.f.c.OFSwitchBase:New I/O server worker #2-2] Cle
aring all flows on switch OFSwitchBase [/10.0.0.252:57245 DPID[00:0a:
f0:92:1c:21:3d:c0]]
06:36:28.923 WARN [n.f.c.i.C.s.notification:main] Switch 00:0a:f0:92:
1c:21:3d:c0 connected.
06:36:28.928 INFO [n.f.l.i.LinkDiscoveryManager:New I/O server worker
#2-1] Inter-switch link detected: Link [src=00:0a:f0:92:1c:21:3d:c0
outPort=15, dst=00:0a:f0:92:1c:21:5d:80, inPort=15]
06:36:28.928 WARN [n.f.l.i.L.s.notification:New I/O server worker #2-
1] Link added: Link [src=00:0a:f0:92:1c:21:3d:c0 outPort=15, dst=00:0
a:f0:92:1c:21:5d:80, inPort=15]
06:36:28.930 INFO [n.f.l.i.LinkDiscoveryManager:New I/O server worker
#2-2] Inter-switch link detected: Link [src=00:0a:f0:92:1c:21:5d:80
outPort=15, dst=00:0a:f0:92:1c:21:3d:c0, inPort=15]
06:36:28.930 WARN [n.f.l.i.L.s.notification:New I/O server worker #2-
2] Link added: Link [src=00:0a:f0:92:1c:21:5d:80 outPort=15, dst=00:0
a:f0:92:1c:21:3d:c0, inPort=15]
```

• Checking List

- i) OpenFlow Message
- ii) System Resource
- iii) APIs (e.g., SM-ONOS)



- **Static/Dynamic Analysis of SDN applications**

- **Static manner:**

- Control Flow Graph and API call list

- **Dynamic manner:**

- Sufficient test inputs (e.g., control messages such as PACKET_IN)

- Make a decision whether the target application is malicious or not.

- Need a definition of malicious behavior for each controller

