OPEN NETWORKING
FOUNDATION

PROJECT DELTA:
SDN SECURITY EVALUATION FRAMEWORK

Seungsoo Lee[†], Changhoon Yoon[†], Seungwon Shin[†], Sandra Scott-Hayward[§]

† KAIST, § Queen's University Belfast

October 2016

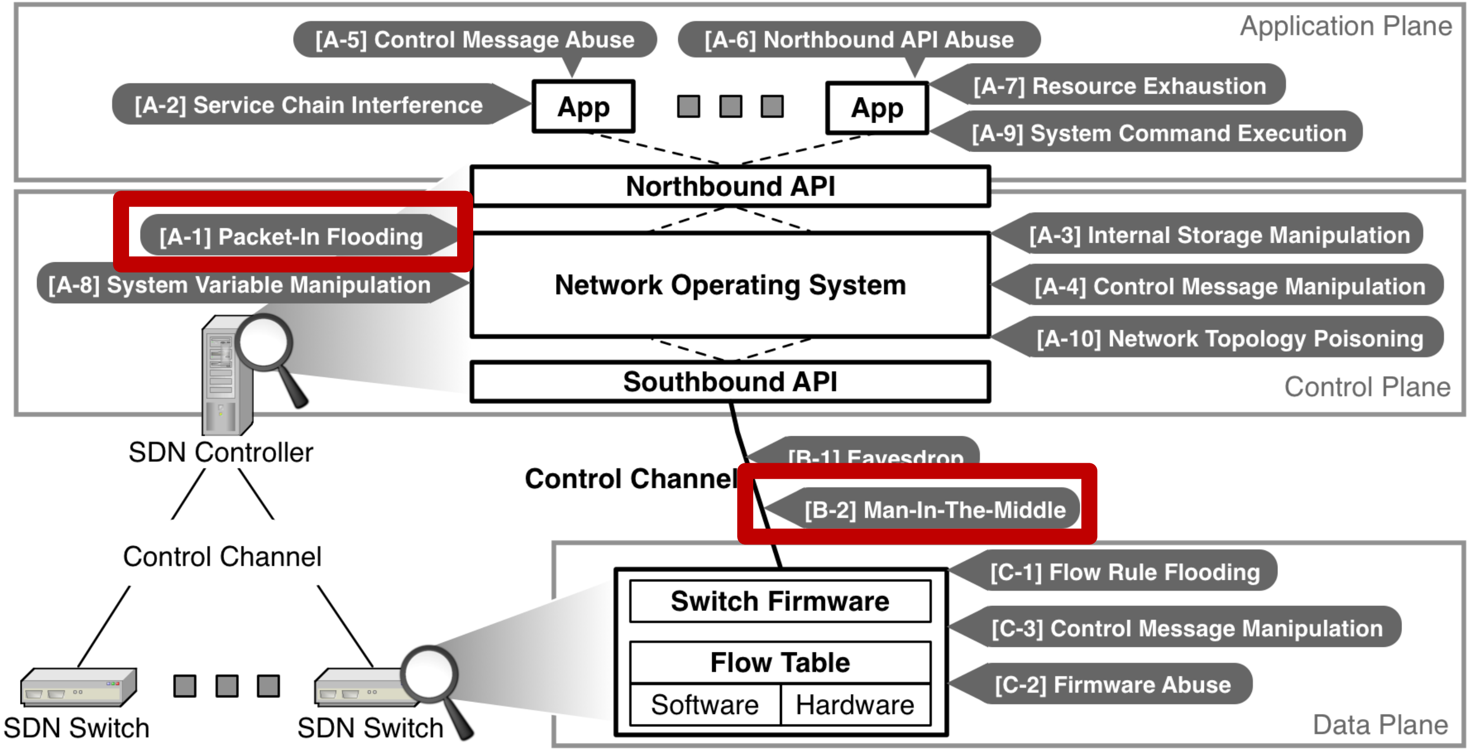
OPEN SOURCE SDN

DELTA

Outline

- SDN-related Vulnerabilities
- DELTA
- Demonstration
- Planned Actions

SDN-related Vulnerabilities


Application Plane
[A-5] Control Message Abuse
[A-6] Northbound API Abuse
[A-2] Service Chain Interference
App
App
[A-7] Resource Exhaustion
[A-9] System Command Execution
Northbound API
[A-1] Packet-In Flooding
[A-8] System Variable Manipulation
Network Operating System
[A-3] Internal Storage Manipulation
[A-4] Control Message Manipulation
[A-10] Network Topology Poisoning
Southbound API
Control Plane
SDN Controller
Control Channel
Control Channel
[B-1] Eavesdrop
[B-2] Man-In-The-Middle
SDN Switch
SDN Switch
Switch Firmware
Flow Table
Software
Hardware
[C-1] Flow Rule Flooding
[C-3] Control Message Manipulation
[C-2] Firmware Abuse
Data Plane

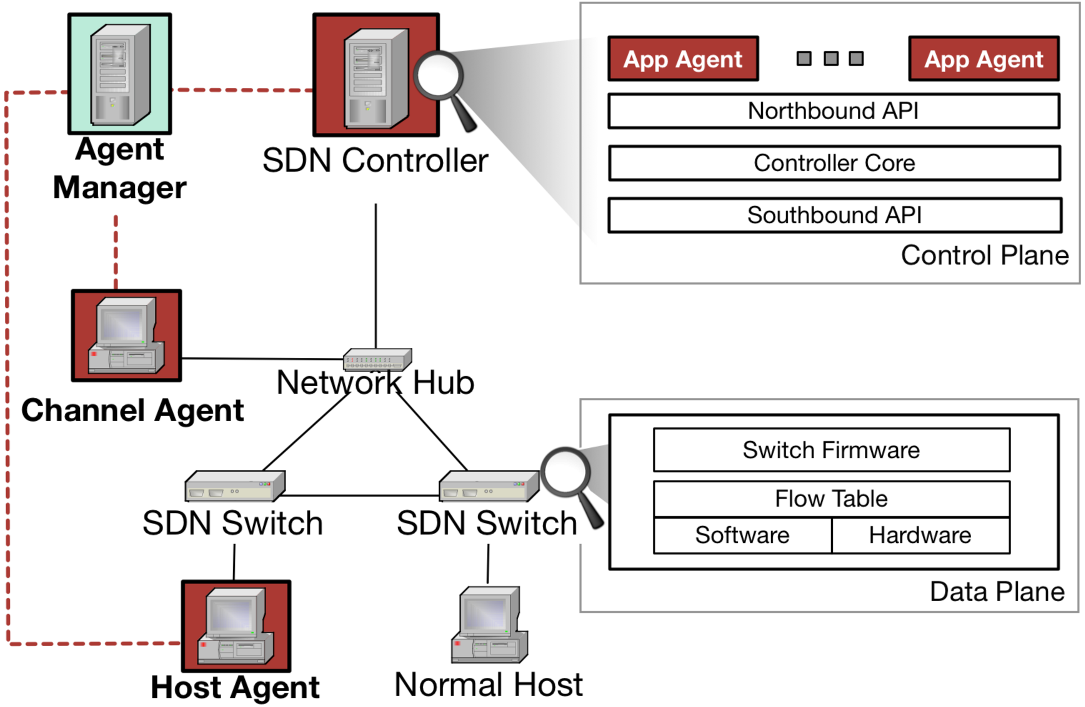
PROJECT DELTA: SDN SECURITY EVALUATION FRAMEWORK

- **Motivation**
  - SDN security threats are real
  - Security assessment is essential
  - Performing security tests against SDNs is difficult

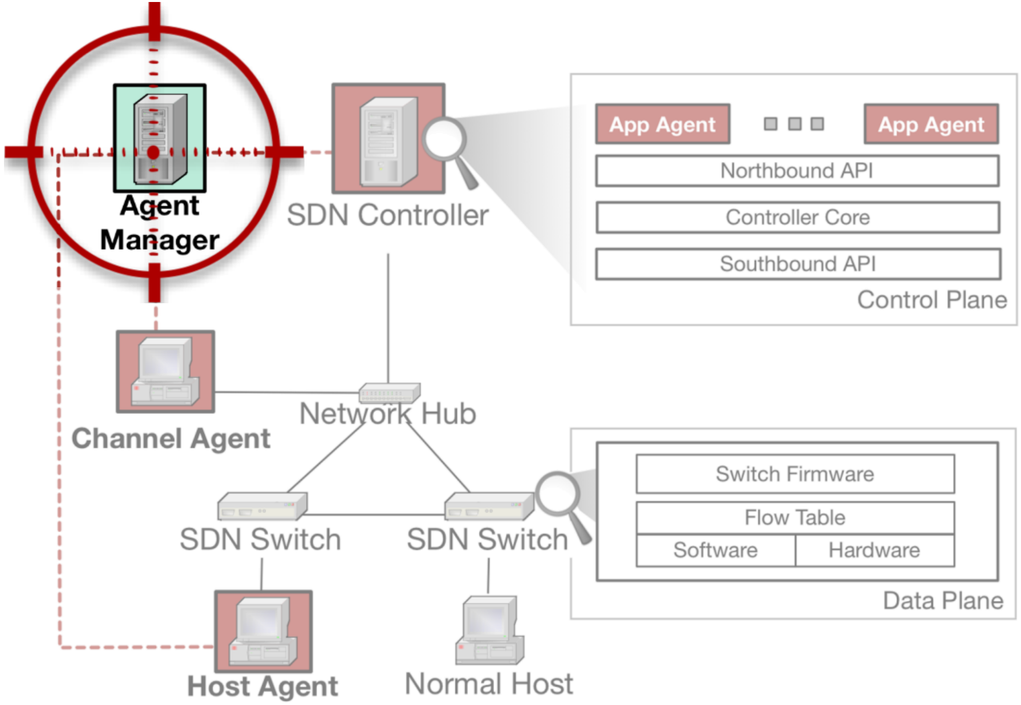
- **Our goal**
  - A feasible and usable SDN security evaluation framework
    - Automatically construct test environments and perform security tests

Framework Design

Out-of-band, dedicated DELTA control network

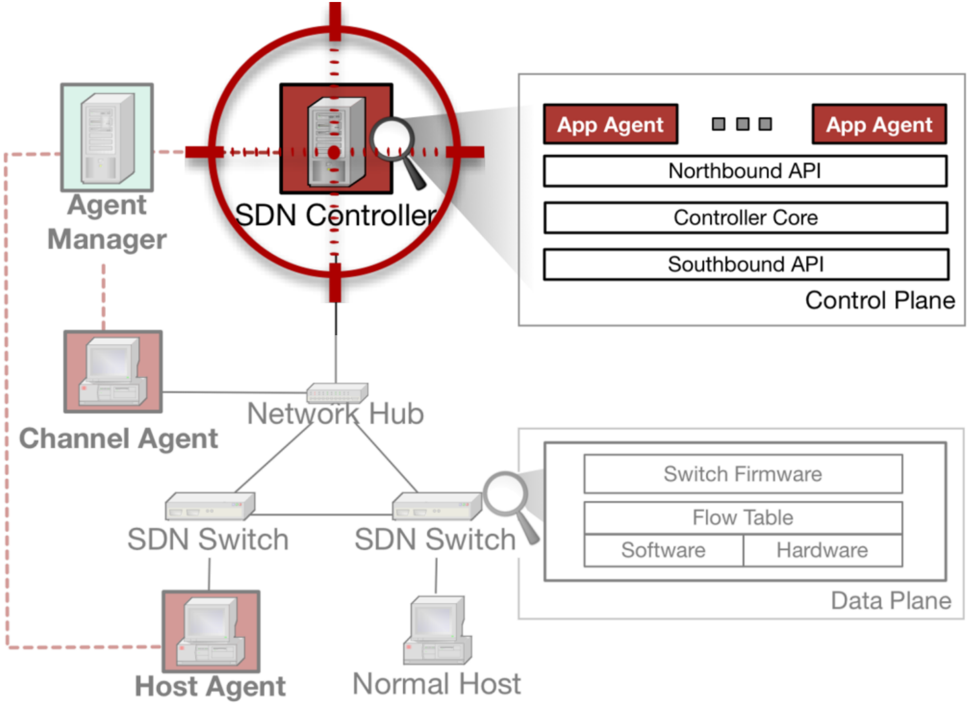


Agent Manager



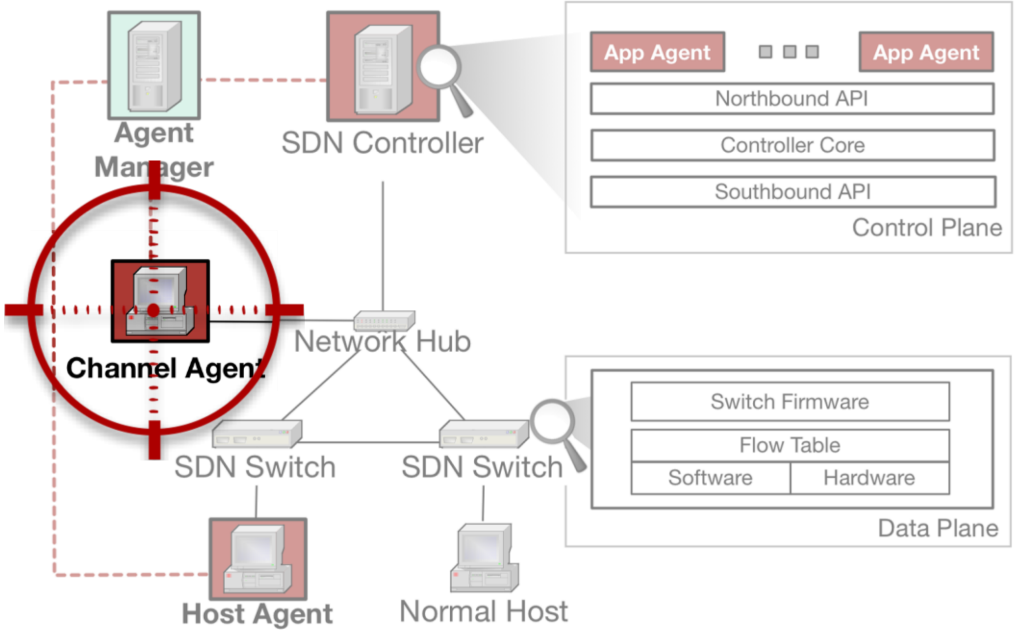
- **The "Control tower"**
- Remotely controls the agents deployed in the target network
- Leverages different agents to perform various security test cases
- Analyzes the test results collected from the agents
- Implements CLI & Web-based UI

Application Agent



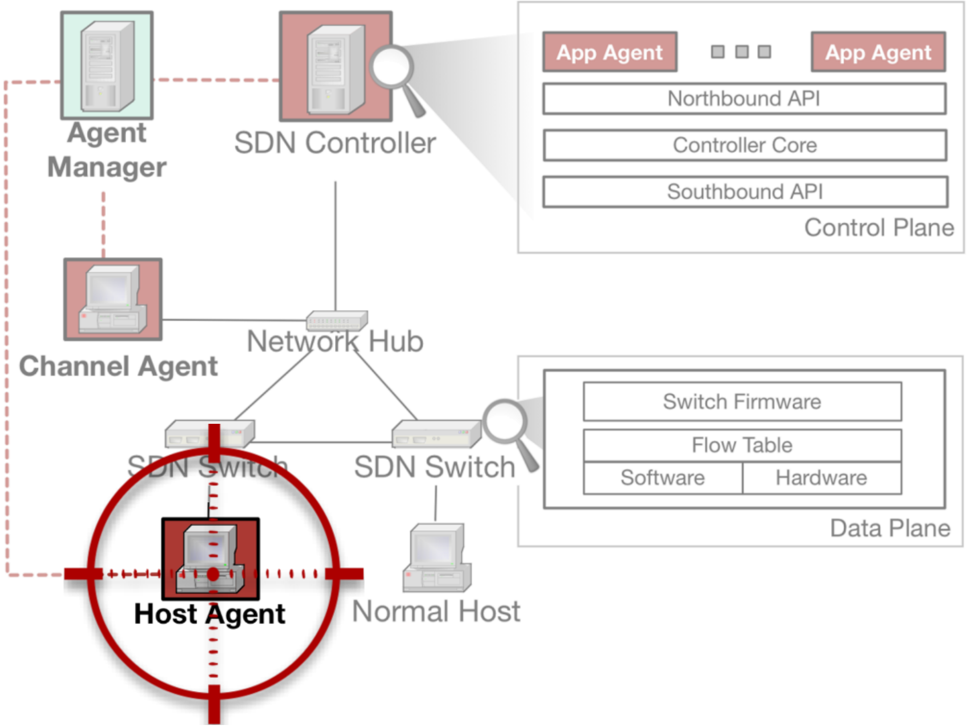
- **Conducts attack procedures as instructed by the manager**
- Implements the known malicious functions as an application agent library

Channel Agent



- Is located between the control plane and the data plane
- **Sniffs** and **modifies** the **unencrypted** control messages

Host Agent



- **A legitimate network host** participating in the target SDNs
- Generates network traffic as instructed by the agent manager
  - e.g. DDoS, LLDP injection, etc.

Currently Supported Controllers and Switches

- **SDN controllers**
  - ONOS: v1.1 / v1.6
  - Floodlight: v0.91 / v1.2
  - OpenDaylight: Helium-SR3

- **Switches**
  - Any OpenFlow-enabled switches
    - Including software switches (e.g. OVS)

Security Test Cases

- **Test set 1: Data plane security**
  - OpenFlow messages from a controller to a switch
  - Number of test cases implemented/proposed: 17/23

- **Test set 2: Control plane security**
  - OpenFlow messages from a switch to a controller
  - Number of test cases implemented/proposed: 7/15

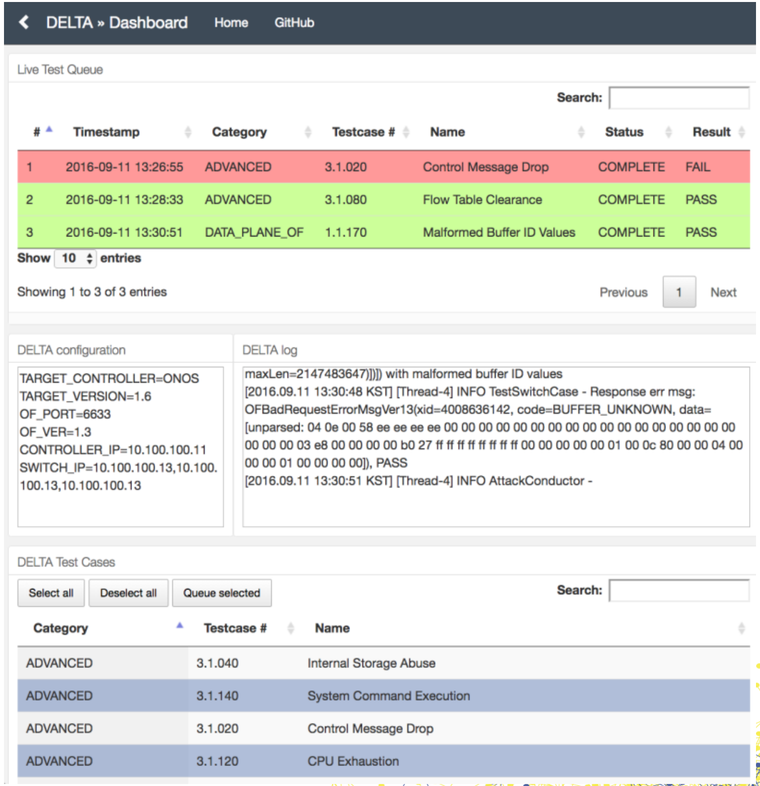
- **Test set 3: Advanced security**
  - Sophisticated security tests exploiting a variety of vulnerabilities
    - e.g. SDN applications exploiting SDN controllers' architectural vulnerabilities
  - Number of test cases implemented/proposed: 18/20

DELTA Web UI

Live test queue:

Configuration and log pane:

Test case inventory:



Live Test Queue

Search:

#	Timestamp	Category	Testcase #	Name	Status	Result
1	2016-09-11 13:26:55	ADVANCED	3.1.020	Control Message Drop	COMPLETE	FAIL
2	2016-09-11 13:28:33	ADVANCED	3.1.080	Flow Table Clearance	COMPLETE	PASS
3	2016-09-11 13:30:51	DATA_PLANE_OF	1.1.170	Malformed Buffer ID Values	COMPLETE	PASS

Show 10 entries

Showing 1 to 3 of 3 entries

DELTA configuration

```
TARGET_CONTROLLER=ONOS
TARGET_VERSION=1.6
OF_PORT=6633
OF_VER=1.3
CONTROLLER_IP=10.100.100.11
SWITCH_IP=10.100.100.13,10.100.
100.13,10.100.100.13
```

DELTA log

```
maxLen=2147483647)])]) with malformed buffer ID values
[2016.09.11 13:30:48 KST] [Thread-4] INFO TestSwitchCase - Response err msg:
OFBadRequestErrorMsgVer13(xid=4008636142, code=BUFFER_UNKNOWN, data=
[unparsed: 04 0e 00 58 ee ee ee ee 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 03 e8 00 00 00 00 b0 27 ff ff ff ff ff ff ff 00 00 00 00 00 01 00 0c 80 00 00 04 00
00 00 01 00 00 00 00]), PASS
[2016.09.11 13:30:51 KST] [Thread-4] INFO AttackConductor -
```

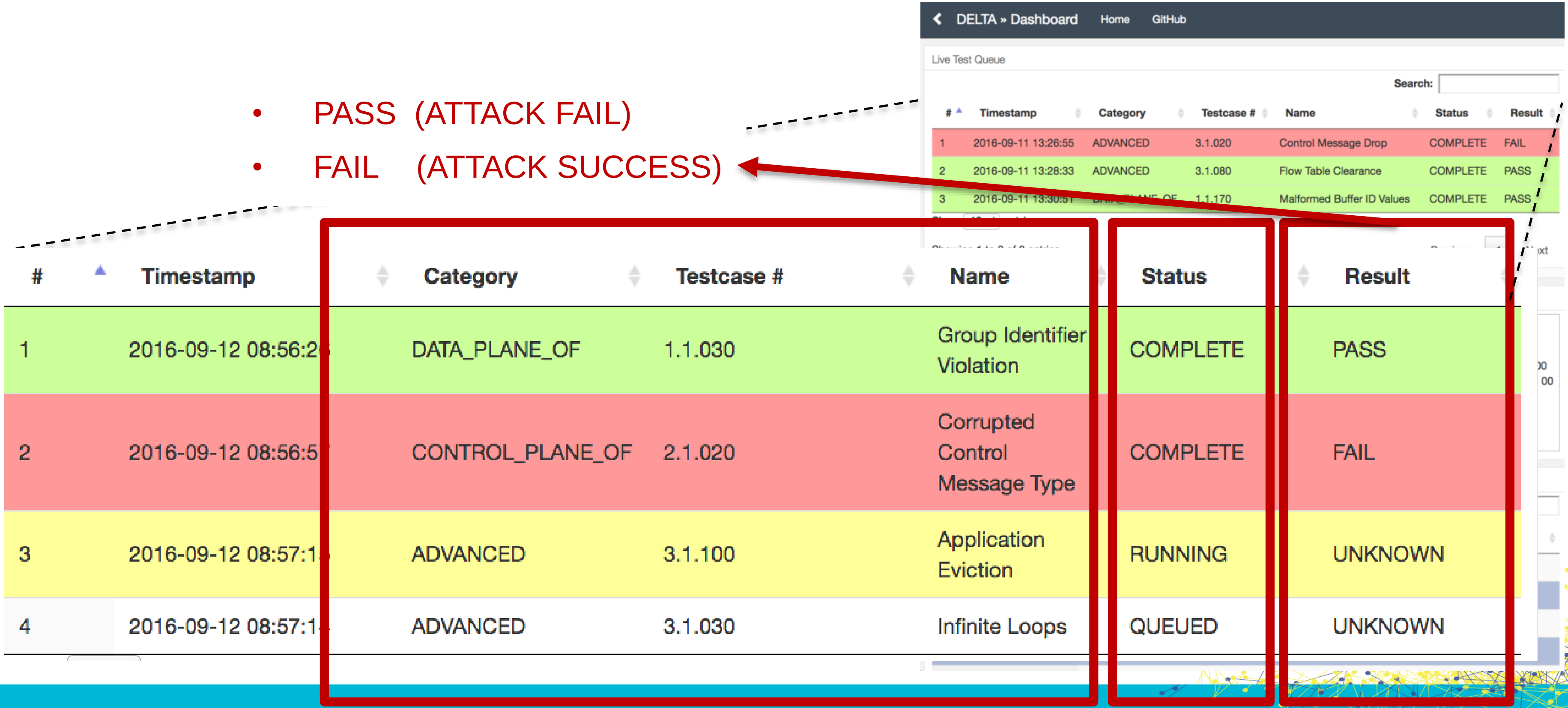
DELTA Test Cases

Search:

Category	Testcase #	Name
ADVANCED	3.1.040	Internal Storage Abuse
ADVANCED	3.1.140	System Command Execution
ADVANCED	3.1.020	Control Message Drop
ADVANCED	3.1.120	CPU Exhaustion

DELTA Web UI

- PASS (ATTACK FAIL)
- FAIL (ATTACK SUCCESS)

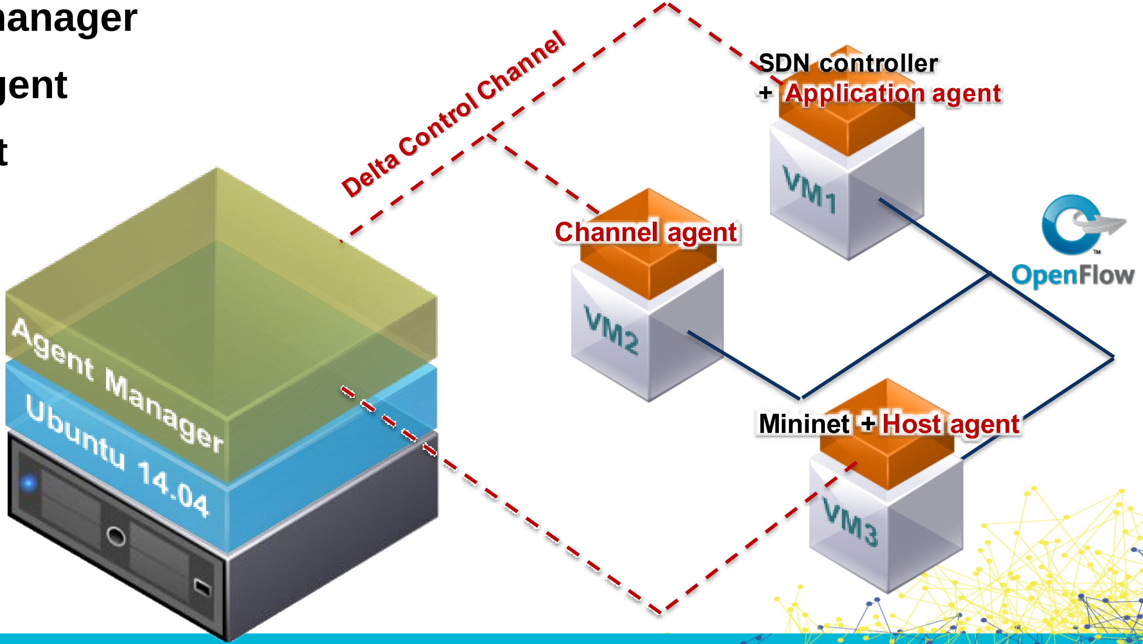


#	Timestamp	Category	Testcase #	Name	Status	Result
1	2016-09-11 13:26:55	ADVANCED	3.1.020	Control Message Drop	COMPLETE	FAIL
2	2016-09-11 13:28:33	ADVANCED	3.1.080	Flow Table Clearance	COMPLETE	PASS
3	2016-09-11 13:30:51	DATA_PLANE_OF	1.1.170	Malformed Buffer ID Values	COMPLETE	PASS

#	Timestamp	Category	Testcase #	Name	Status	Result
1	2016-09-12 08:56:2	DATA_PLANE_OF	1.1.030	Group Identifier Violation	COMPLETE	PASS
2	2016-09-12 08:56:5	CONTROL_PLANE_OF	2.1.020	Corrupted Control Message Type	COMPLETE	FAIL
3	2016-09-12 08:57:1	ADVANCED	3.1.100	Application Eviction	RUNNING	UNKNOWN
4	2016-09-12 08:57:1	ADVANCED	3.1.030	Infinite Loops	QUEUED	UNKNOWN

Demo: Environment

- One server machine (Ubuntu 14.04)
  - Hosts 3 virtual machines to construct a target SDN (Ubuntu 14.04)
- Server machine: **Agent manager**
  - VM1: **Application agent**
  - VM2: **Channel agent**
  - VM3: **Host agent**



Demo: Test Scenarios and Security Issues

1.1.070: Unsupported Version Number (bad version)

- ***Scenario:*** Dummy controller sends a connection setup request with OF_HELLO message containing an unsupported version number and then verifies that an OF_ERROR message is returned
- ***Security Issue:*** The possibility of manipulating network functions by use of mismatched network commands

3.1.020: Control Message Drop

- ***Scenario:*** An application agent participates in a service chain and drops control messages before the other applications receive them
- ***Security Issue:*** The possibility of a malicious application interfering with neighboring applications and the network functionality

Demo: Video

Q&A