Outline

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

[A-1] Packet-In Flooding

[A-2] Service Chain Interference

[A-3] Internal Storage Manipulation

[A-4] Control Message Manipulation

[A-5] Control Message Abuse

[A-6] Northbound API Abuse

[A-7] Resource Exhaustion

[A-8] System Variable Manipulation

[A-9] System Command Execution

[A-10] Network Topology Poisoning

[B-1] Eavesdropping

[B-2] Man-In-The-Middle

[C-1] Flow Rule Flooding

[C-2] Firmware Abuse

[C-3] Control Message Manipulation

Switch Firmware

Flow Table

Software

Hardware
• **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
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
Applications 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:
DELTA Web UI

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