Network Security Demonstration
- Snort based IDS Integration -

Hyuk Lim (hlim@gist.ac.kr)
with TJ Ha, CW Jeong, J Narantuya, JW Kim

Wireless Communications and Networking Lab
School of Information and Communications
Gwangju Institute of Science and Technology (GIST)

http://wits.gist.ac.kr
Contents

- Introduction
- Network security with SDN, Snort, and sFlow
- Scalable network security
- Experiments
Network Attacks

- Denial of Service (DoS) attack
  - An attempt to make a resource unavailable to legitimate users
  - A malicious user floods excessive traffic to make network servers incapable of servicing legitimate users
  - Distributed denial of service (DDoS) attack launched by leveraging a large number of machines

- Malicious data propagation
  - Any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system
  - Attack scripts, viruses, worms, Trojan horses, malicious active content
Intrusion Detection with SDN

- Network traffic has increased explosively, and the detection of malicious traffic is getting much harder.

- Traditional IDS
  - Placed at several choke points in the network
  - Monitor as many packets as possible

- Scalable IDS with SDN
  - Exploit the topology and flow information of the network
  - Decide where to monitor and adjust the inspection level for traffic monitoring
  - Efficiently utilize the distributed resources for network security such as firewall, IDS/IPS and so on.
SDN for Network Security

- The flow paradigm is ideal for security processing because it offers an end-to-end, service-oriented connectivity model.
- Logically centralized control for effective performance and threat monitoring across the entire network.
- Granular policy management can be based on application, service, organization, and geographical criteria rather than physical configuration.
- Resource-based security policies enable consolidated management of diverse devices with various threat risks, from highly secure firewalls and security appliances to access devices.
- Dynamic and flexible adjustment of security policy is provided under programmatic control.
- Flexible path management achieves rapid containment and isolation of intrusions without impacting other network users.”

Mike McBride et al., “SDN Security Considerations in the Data Center,” ONF Solution Brief, October 8, 2013
Network Security Architecture
SDN Controller

- OpenFlow: a communications protocol that gives access to the forwarding plane of a network switch or router over the network.

- SDN Controller: a platform for network programmability to enable software-defined networking with OpenFlow.
  - Floodlight (BigSwitch): the world’s leading open source SDN controller
  - OpenDaylight (Cisco, IBM): the SDN controller under The Linux Foundation
sFlow

- sFlow protocol samples traffic flows and forwards to sFlow collector.
- sFlow can summarize the information of traffic flows.
- sFlow agent can be installed in PC’s, switches, routers, etc.
Snort

- Snort is an open source network-based intrusion detection system (NIDS)
  - It has the ability to perform real-time traffic analysis and packet logging on Internet protocol (IP) networks
  - It performs protocol analysis, content searching, and content matching
- Snort can be configured in three main modes:
  - Sniffer mode
  - Packet logger mode
  - Network intrusion detection system (NIDS)
sFlow + Snort

- **sFlowToolkit**
  - Installed in the sFlow Collector machine
  - Listens sFlow packets from sFlow agent
  - Converts standard sFlow data to snort-readable format
  - Send them to the Snort for detailed packet tracing and analysis
Barnyard vs. Prelude

- **Barnyard** is an add-on tool for Snort (unified log reader)
  - Snort creates a special binary output format
  - Barnyard reads this file, and then sends the data to a database
  - Allowing Snort to write to disk in an efficient manner

- **Prelude** is a distributed hybrid IDS framework
  - Collects and aggregates event reports from available security systems (IDS-snor)
  - Analyses them on a central system
Security Loop

Observe
Sample Traffic

Detect
Analyze Traffic

React
Update Strategy

Defense
Control Traffic

Flow & topology information
Router/Flow Grouping

- Since DDoS attack uses a large number of flows, it can be detected more easily by grouping closely related flows and forwarding to the same IDS.
Sampling Strategy

- Sampling strategy affects the false negative performance of IDS.

How much sampling?
Be Smarter

- How to exploit the flow and topology information from SDN and prior observation of attack traffic.
EXPERIMENTS
Experiment Environment

- SDN based experiment environment with virtualization tools
  - VMs on KVM hypervisor, virtual network with Open vSwitches
- Provide more realistic network compared with network simulators
  - Open vSwitch supports core SDN and superior functionalities
  - KVM (Kernel-based Virtual Machine) generates VMs highly similar to real machine
### Topology Manager

- **Topology manager**
  - Parses topology output file generated by Brite topology generator
  - Saves the created topologies in the topology DB
  - Provides web based GUI showing network topologies using D3 (data virtualization library)
OVS-based SDN Network Topologies

10 routers

20 routers

50 routers

5 AS (5*10 routers)

4 AS (4*20 routers)

10 AS (10*10 routers)
Traffic Manager

- Creates traffic attack using Hping3 with various configurations such as malicious traffic ratio, traffic bandwidth, attack type
- Controls attack node to generate large scale network attack
**Attack Traffic Generation**

- **Hping3: Traffic generator**
  - One of the de-facto tools for security auditing and testing networks
  - Customized ICMP/UDP/TCP packets can be used
  - Fully scriptable using the TCL language

- **Example) DDOS attack generated by Hping3**

![Example DDOS attack](image-url)
sFlow Manager

- **sFlow Manager**: Centralized sFlow agent control
  - Remotely configures the sampling rate, sampling period, header byte, collector IP
sFlow Control Examples

No sFlow

Static configuration 1

Static configuration 2

Random sampling
Scenario

- 3 attack VM nodes generate DDoS attack
  - DDoS control with the traffic manager (malicious traffic ratio 0~100%)

- 3 Snort IDS nodes detect security attack

- sFlow control with sFlow manager
  - 50 OVS switches
  - Static sampling rate

- VM resources
  - IDS (CPU 1 core, RAM 1024)
  - Attack node (CPU 1 core, RAM 512)
  - Victim node (CPU 1 core, RAM 512)