Performance and Security Influence of Augmenting IDS using SDN and NFV

SSP 2017

Lukas Iffländer & Jonathan Stoll

2017/11/9

http://se.informatik.uni-wuerzburg.de/
Content

- Motivation
- Background
- Approach
- Evaluation
- Conclusion
MOTIVATION
Motivation

• Attack detection requires DPI
• In inline mode IDS presend an active and potentially limiting component.

Signatur:
alert tcp $EXTERNAL_NET any -> $HOME_NET 12345:12346
(msg:"MALWARE-BACKDOOR netbus getinfo"; flow:to_server, established;
content:"GetInfo[OD]"; metadata:ruleset community;
clastype:trojan-activity; sid:110; rev:10;
Problem
- Active in-line IDS are a bottleneck
- IDS detect false-positives in overload scenarios

(Expected) Benefit
- Load removal from the IDS
  - Improves network performance
  - Improves attack detection
- Allows global reaction to attacks in the network

Idea
- Route only relevant traffic over the IDS

Action
- Develop SDN based algorithms to route only relevant traffic over the IDS
BACKGROUND
IDS Categories

Intrusion Detection Systems

- Monitored platform
  - Host-based
  - Network-based
- Attack detection method
  - Misuse-based
  - Anomaly-based
- Monitoring method
  - Real-time
  - Polling
- Deployment architecture
  - Non-distributed
  - Distributed
Performance and Security Influence of Augmenting IDS using SDN and NFV

Lukas Iffländer & Jonathan Stoll
Related Work


APPROACH
Assumptions

- Attacks only from the outside
  - only incoming traffic to be monitored
  - outgoing traffic is benign

- Only applications the IDS has signatures for are relevant

- Only the first packets of a connection contain attacks (e.g. HTTP-Requests)
Routing Concepts

Development of three SDN-based algorithms for routing traffic via the IDS

- **Adaptive Blacklisting**
  - Permanent blacklists for some services
  - Temporal blacklists for selected connections

- **Adaptive Whitelisting**
  - Permanent whitelists for some services
  - Temporal whitelists for selected connections

- **Selective Filtering**
  - Permanent routing of selected services over the IDS
New Connection

Blacklisted Traffic?
- Yes: temporal routing via the IDS
- No: Direct routing to server

Incoming Connection

Attack detected?
- Yes: permanent routing via the IDS
- No: Direct routing to the server

Whitelisted Traffic?
- Yes: Direct routing to server
- No: temporal routing via the IDS

Incoming Connection

Blacklisting
- Time (t)

Whitelisting
Blacklisting

Non-blacklisted traffic:

- Direct routing between Q and S

Blacklisted traffic:

1. New connection
2. Route via IDS for X seconds
3. No attack detected: Direct routing after X seconds for Y seconds
   - Attack detected: Permanent routing via IDS
Whitelisting

Normal traffic:

1. New connection
2. Route via IDS
3. Require information whether attack occurred within X packets
   If not permanent routing from Q to S

Whitelisted traffic:

Direct routing between Q and S
Selective Filtering

**Normal traffic:**
- Direct routing between Q and S

**Selected traffic:**
- Routing of incoming traffic via the IDS
- Direct routing of outgoing traffic
Used technologies

- SDN: OpenFlow + Ryu Controller
- IDS Snort with barnyard2
- Application: Apache Webserver
- Virtual Switch: Open vSwitch
- SDN Controll: L7sdntest
Reference Scenarios

1a (optimum reference)

Switch

1b (minimum reference)

IDS

2 (Switch VNF + IDS)

Open vSwitch + IDS
Intelligent Routing Scenarios

3
IDS + SDN Switch

SDN-Controller

Hardware-Switch

IDS

S ... S

4
IDS + SDN Switch VNF

SDN-Controller

Open vSwitch (SDN-Mode)

Q

IDS

S ... S
Metrics and Workloads

- Throughput [Mbit/s]
- Delay [ms]
- Alarm-Rate
  - False positives
  - False negatives
- HTTP Requests

Workload 1: Constant Load
\[ a = \frac{\lambda}{\mu} = 1 \]

Workload 2: Overload
\[ a = \frac{\lambda}{\mu} > 1 \]
Workload 1: Throughput [Mbit/s]
Performance and Security Influence of Augmenting IDS using SDN and NFV

Lukas Iffländer & Jonathan Stoll
Workload 1: Alerts

Performance and Security Influence of Augmenting IDS using SDN and NFV

Lukas Iffländer & Jonathan Stoll
Workload 2: Throughput [Mbit/s]

Performance and Security Influence of Augmenting IDS using SDN and NFV

Lukas Iffländer & Jonathan Stoll
Workload 2: Delay [ms]

Performance and Security Influence of Augmenting IDS using SDN and NFV

Lukas Iffländer & Jonathan Stoll
Workload 2: Alerts

Performance and Security Influence of Augmenting IDS using SDN and NFV

Lukas Iffländer & Jonathan Stoll
Workload 2: Packets via IDS per Second

Performance and Security Influence of Augmenting IDS using SDN and NFV

Lukas Iffländer & Jonathan Stoll
Summary

- Throughput was increased
- Delay was decreased
- Improved attack detection
  [further work needed for more precise statements]
- Large differences between native and virtual switches
- Packet throughput at IDS indicator for system performance
Future Work

- Evaluation with other Hardware Switches
- Extension by load balancing solutions for IDS
- Evaluation of other IDSe (Bro, Suricata, Snort2, …)
- More detailed inspection of attack detection results
- Application of learned knowledge for function chaining of security VNFs
Thank you for your attention!

lukas.ifflaender@uni-wuerzburg.de

https://twitter.com/bladewing678