Security in Softwarized Networks: Prospects and Challenges

Nicholas Gray, Thomas Zinner, Phuoc Tran-Gia

comnet.informatik.uni-wuerzburg.de

sardine-project.org
Motivation

- Average cost of data breach $3.62 million (IBM)
- Cloud infrastructure is the next frontier for cyber crime (Symantec)
- Nation-state cyber attacks change the security game (Microsoft)

→ Both sides of the scale need to be addressed
Agenda

- Overview of the SDN Attack Surface
- Fuzzing as Quality Assurance Technique
- Omni-present SDN Firewall
OVERVIEW OF THE SDN ATTACK SURFACE
SDN Attack Surface

One compromised component is enough to take down the whole system.
FUZZING AS QUALITY ASSURANCE TECHNIQUE
Fuzzing as Proactive Security Testing Technique

- Automated proactive software testing technique
- Proven method for uncovering unknown security vulnerabilities (Heartbleed, Crazy bad, Shellshock …)
- Feedback Loop is vital for efficient input generation
FlowFuzz – Core Features

- Protocol Aware
- Python Based
- Supports OF v1.0/1.3

Corpus of Valid Inputs
Directed and Random Input Generation
Various Sources as Feedback Loop

- Full featured fuzzing framework
- Specialized for OpenFlow-enabled software/hardware switches
FlowFuzz - Architecture

- Modular design allows for fast and custom adaptations
- Selection of modules is configurable to best fit the use case
FlowFuzz - Feedback Sources

- Use case specific selection of feedback sources
- Adjustable weights of sources during the evaluation stage
- All sources are combined to fingerprints to reflect the test paths
Feedback Sources – Evaluation of Response Times

- Response times reflect execution of different code segments
- Baseline measurement is required per device and firmware
OMNI-PRESENT SDN FIREWALL
Can we enhance network security with SDN?
Can we enhance network security with SDN?
Security in Softwarized Networks: Prospects and Challenges

Nicholas Gray
Demo Setup

https://www.youtube.com/watch?v=e_CmcGPXJGY
Fine-granular Access Control
NFV Monitoring

Virtual Network Functions
Security in Softwarized Networks: Prospects and Challenges

Nicholas Gray
Offloading of Trusted Flows

Firewall VNF Offloading
Conclusion

- SDN provides new opportunities but also introduces new risks

- In our opinion the benefits will outweigh the challenges
  - Tight integration of quality assurance in the deployment stage
  - Adaptation of software testing methods to the networking domain

- Related Talks and Publications
  - SDN/NFV-enabled Security Architecture for Fine-grained Policy Enforcement and Threat Mitigation for Enterprise Networks, SIGCOMM 2017