SETTING UP DELTA IN A HETEROGENEOUS TELCO SDN ENVIRONMENT

Sebastian Dittrich, Telekom Security
AGENDA

01 Introduction

02 Network Transformation @ DT

03 Setting up DELTA
   Used hard- and software
   DELTA architecture
   Issues encountered during installation
   Demonstration

04 Future plans / next steps
Sebastian Dittrich

- Security Consultant @ T-Systems International GmbH, Telekom Security
  - Network and Infrastructure Security, Security of Access and Optical Networks
- Project Security Manager for CORD-driven project Access 4.0 @ Deutsche Telekom
- Bachelor of Engineering in Computer Science and Telecommunications @ University of Applied Sciences Leipzig
- Certified Cyber Security Professional (Cologne Chamber of Commerce and Industry)

Let’s connect: LinkedIn XING
02 NETWORK TRANSFORMATION @ DT
SDN/NFV-ENABLED PROJECTS AT DEUTSCHE TELEKOM

Pan IP programme
- DT's Pan-European telco network for a centralised production of services
- Enabled by (Open)Contrail

Next Generation Enterprise Network Alliance
- A new global business network that enables Industry 4.0
- Enabled by SDN technologies from Cisco

Access 4.0: Innovation project @ DT
- Reduce complexity in DT's access networks (fixed, mobile and hybrid)
- Following CORD-approach
- Enabled by ONOS

ACCESS 4.0
DELTA is a penetration testing framework that regenerates known attack scenarios for diverse test cases. This framework also provides the capability of discovering unknown security problems in SDN by employing a fuzzing technique.

PROJECT’S GITHUB
03 SETTING UP DELTA
USED HARD- AND SOFTWARE

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP ProLiant DL360 G6 (single machine)</td>
<td>Mostly according to documentation on GitHub</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>OS</td>
</tr>
<tr>
<td>2x Intel Xeon-Prozessor X5560 @ 2.8 GHz</td>
<td>Ubuntu 16.04.4 LTS (Kernel 4.4.0-116)</td>
</tr>
<tr>
<td>RAM</td>
<td>Agent manager</td>
</tr>
<tr>
<td>6x 8 GB DDR3-1333</td>
<td>Vagrant (2.0.2) + VirtualBox (5.0.40)</td>
</tr>
</tbody>
</table>
03 SETTING UP DELTA
DELTA ARCHITECTURE*

* As documented on GitHub
** Ubuntu 16.04
03 SETTING UP DELTA
ISSUES ENCOUNTERED DURING INSTALLATION

1. jdk-7 packages are not available anymore
   installation of components seems to work fine, however

2. Manual installation of VirtualBox is needed,
   dependencies cannot be resolved (libvdx, ...)
   Switch to KVM?

3. Configuration is best done via GUI, given X server is running (which in my case was not 😞)
   For headless server: providing vboxmanage command?

4. setup scripts assume $DELTA_HOME directory in ~
   Setups fail, manual adaptation necessary

11.04.2018
Sec&Perf Brigade Workshop
Telekom Security // Security of Access and Transport Networks // Sebastian Dittrich
03 Setting up DELTA Demonstration
04 FUTURE PLANS / NEXT STEPS
OBJECTIVES FOR FURTHER EVALUATION

- Get SDN controller up and running
  - Provided auto-deployment scripts fail
  - What about other controllers?
- Test DELTA behaviour
  - Available test cases
  - Coverage of DT’s requirements
  - Reporting
- Install DELTA on real hardware & availability for security teams

But why?!

Currently, Deutsche Telekom tests every single network component manually
  - Heavy on resources for testers, testing equipment, testing period, ...

Centralised testing frameworks leverage productivity
  - Software bits can be tested almost automatically in real-time (little to no preparation required), sophisticated security tests can be done on the things that cannot be done automatically

Currently, there are no best practices for scope, test cases (specific to SDN), tools etc.

DELTA has the potential to become the de facto standard at DT for pen-testing multiple SDN controllers
CONTACT
SEBASTIAN DITTRICH
S.DITTRICH@TELEKOM.DE