

# Open Networking Korea 2018 Fall

K-ONE KAIST 우승원, 이승현, 강희도

## Extended Security Mode ONOS

### Motivation

#### Security problems in Network Operating System (NOS)

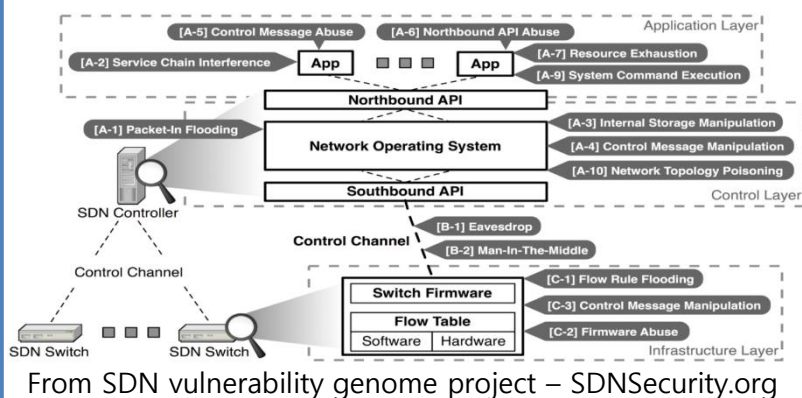
- » Critical infrastructure management
- » Security issues (SDN vulnerability genome project)

#### ONOS controller

- » Useful Northbound abstractions and APIs

#### Security problems in ONOS controller

- » Potential misuse opportunities
- » Software failures



### ONOS Application ecosystem



### Objectives

#### Mandatory application auditing prior to deployment

- » Provide explicit insight for application behaviors
- » Control over the ONOS core Services and APIs

#### Sandboxing application

- » Provide a network application permission-enforce model

#### Key Insight

"Granting the true minimum required capability to ONOS applications (Least-privileged)"

### Security-Mode ONOS

#### Permission model

- » Bundle-level Role-based Access Control
- » Application-level Role-based Access Control
- » API-level Permission-based Access Control

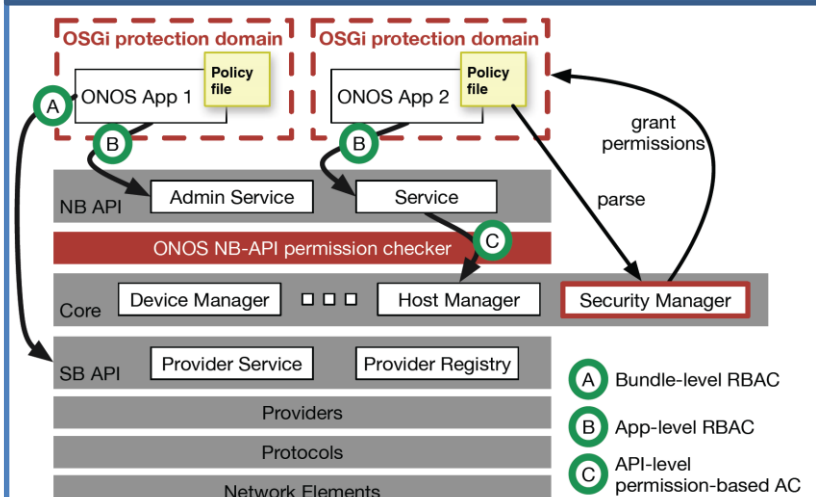
#### Permission negotiation

- » Centralized policy enforcement and permission negotiation

```
1. <security>
2.   <role>USER</role> ONOS Application role
3.   <permissions>
4.     <app-perm>DEVICE_READ</app-perm> ONOS Application permissions
5.     <app-perm>TOPOLOGY_READ</app-perm>
6.     <app-perm>FLOWRULE_WRITE</app-perm>
7.   </permissions>
8.   <osgi-perm>
9.     <classname>ServicePermission</classname>
10.    <name>org.onosproject.demo.DemoAPI</name> OSGi permissions
11.    <actions>get,register</actions>
12.  </osgi-perm>
13.  <java-perm>
14.    <classname>RuntimePermission</classname> Java native permissions
15.    <name>modifyThread</name>
16.  </java-perm>
17. </security>
```

SM ONOS policy file

### Design & Implementation



### Roadmap

#### Additional Service

- » Network Level Access Control (Virtual Network)
- » Service Level Access Control

#### Future works

- » Integrated Multi-layered Security-Mode ONOS