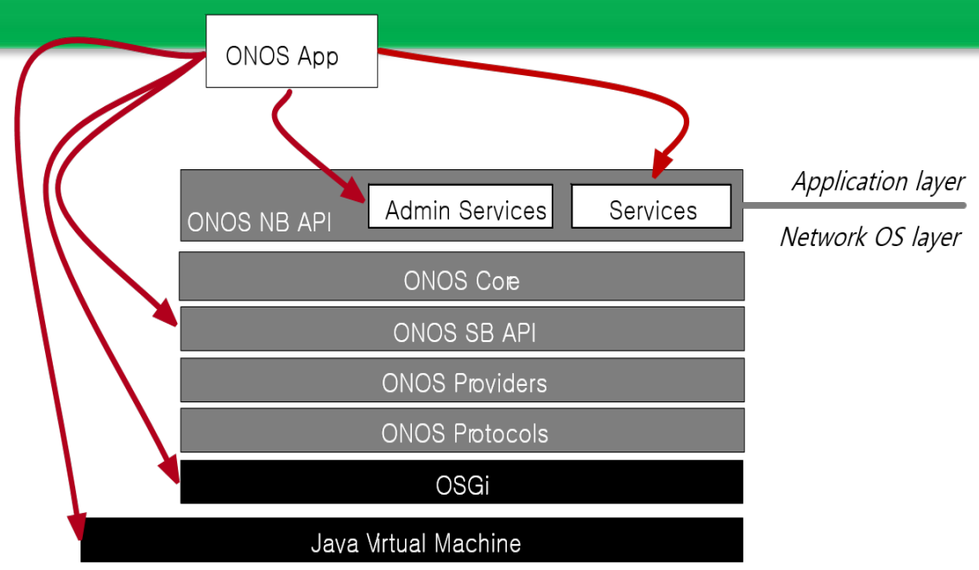
Multi-layered Security-Mode ONOS

Suyeol Lee, Heedo Kang, Haney Kang, Seungwon Shin KAIST

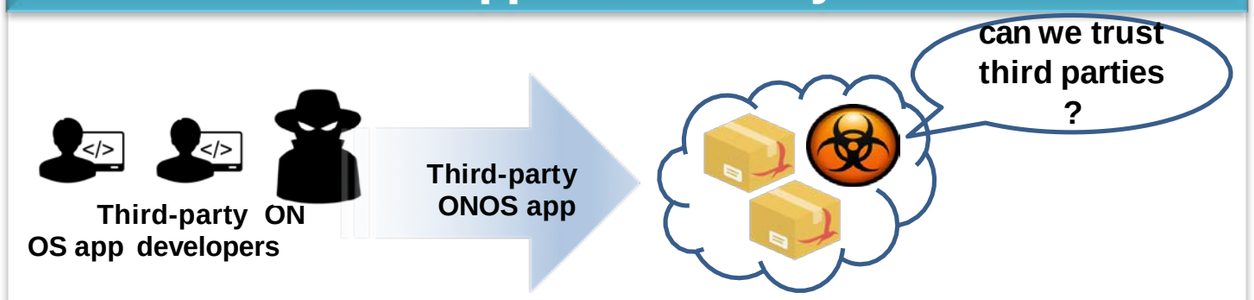
Motivation

- **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 controller architecture

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

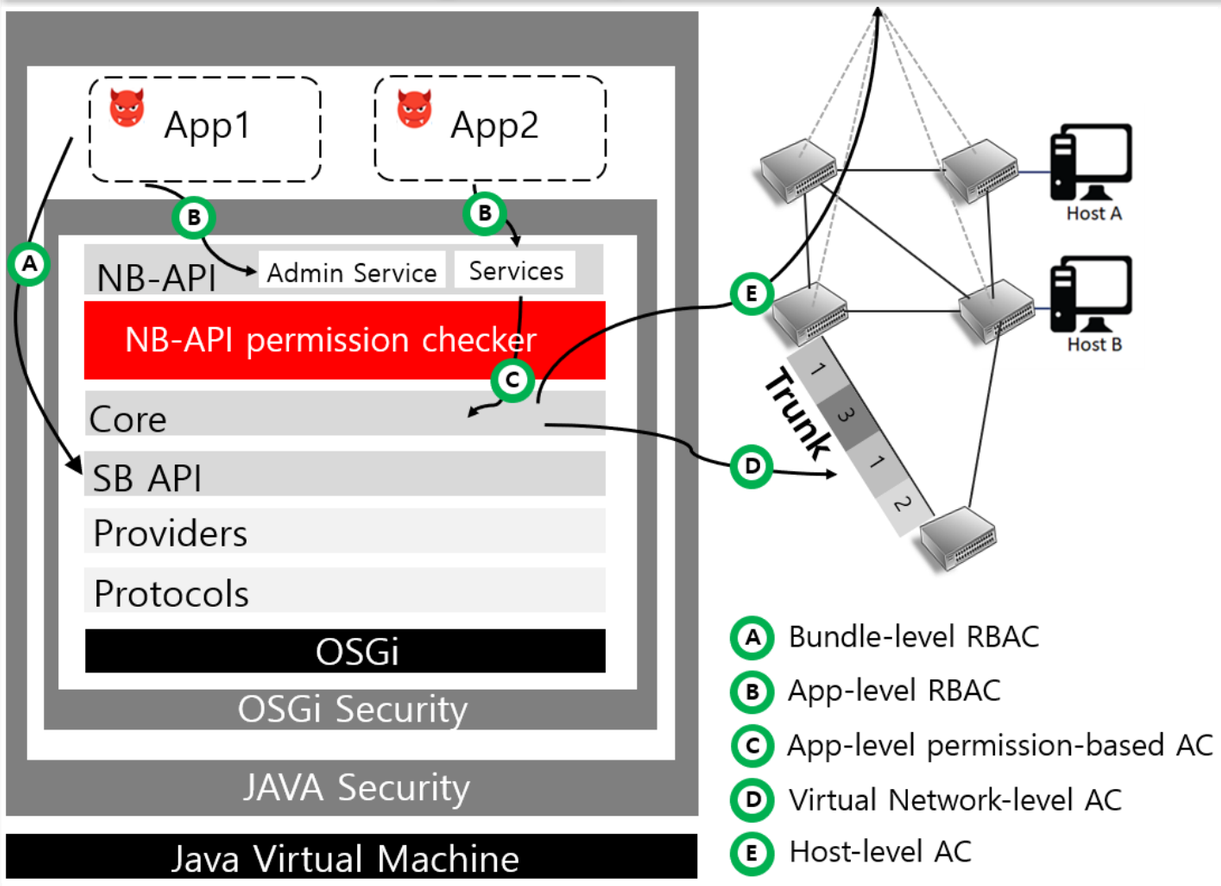
- **Permission model**
  - » Bundle-level Role-based Access Control
  - » Application-level Access Control
  - » Virtual Network-level Access Control
  - » Host-level Access Control
- **SM ONOS policy file**

```
<security>
    <role>USER</role>

    <VNs>
        <VN>
            <VNID>5</VNID>
            <VN-perm>VN_READ</VN-perm>
        </VN>
        <VN>
            <VNID>2</VNID>
            <VN-perm>VN_READ</VN-perm>
            <VN-perm>VN_EVENT</VN-perm>
            <VN-perm>VN_WRITE</VN-perm>
        </VN>
    </VNs>

    <permissions>
        <app-perm>VN_CREATE</app-perm>
        <app-perm>VN_REMOVE</app-perm>
        <app-perm>DEVICE_READ</app-perm>
        <app-perm>PACKET_WRITE</app-perm>
        <app-perm>HOST_READ</app-perm>
        <java-perm>
            <classname>org.osgi.framework.AdminPermission</classname>
            <name>*</name>
            <actions>metadata></actions>
        </java-perm>
        <java-perm>
            <classname>org.lang.RuntimePermission</classname>
            <name>modifyThread</name>
        </java-perm>
    </permissions>
</security>
```

Permissions per VN

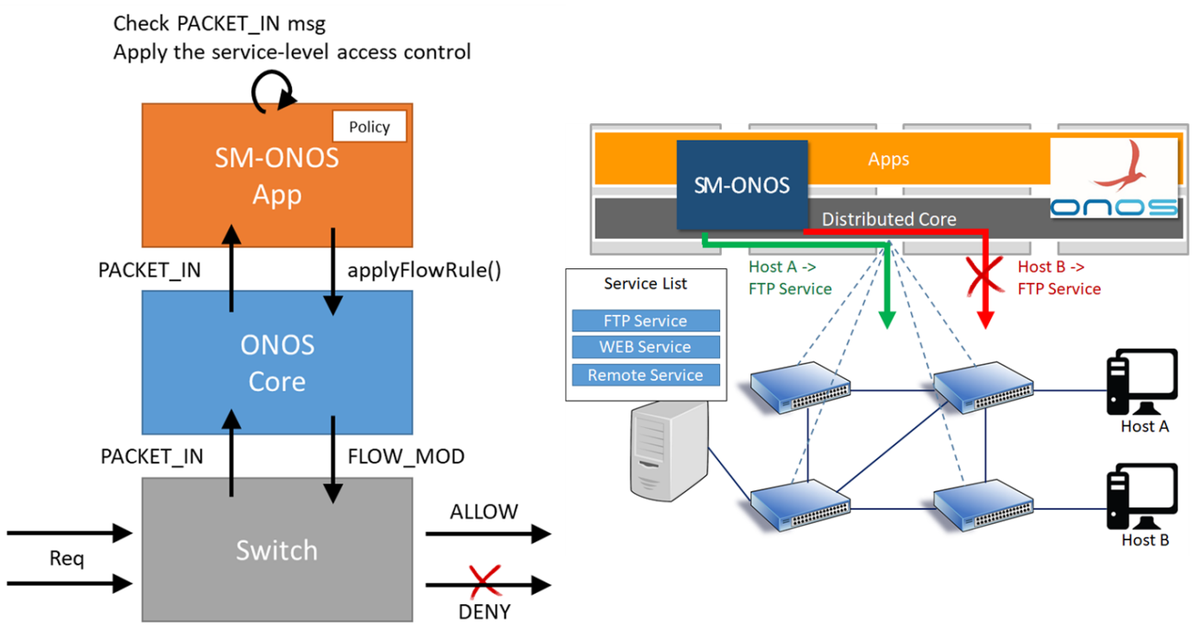
SM ONOS permissions

Design & Implementation



Host-level Access Control

- Basic Mechanism & Example



Roadmap

- **Now, we are working on …**
  - » Unified Multi-layer access control (**Suyeol Lee**)
  - » Automatic policy extraction tool (**Hedoo Kang**)
  - » Security vulnerability on ONOS (**Haney Kang**)
- **Future works**
  - » ONOS Application security-instrumentation
  - » Static + dynamic analysis for ONOS application
- **References**
  - » Security-Mode ONOS Feature Proposal (KAIST, SRI International)
  - - https://wiki.onosproject.org/display/ONOS/Security-Mode+ONOS

K-ONE KAIST

IITP 정보통신기술진흥센터 Institute for Information & communications Technology Promotion

ONK OpenNetworkingKorea