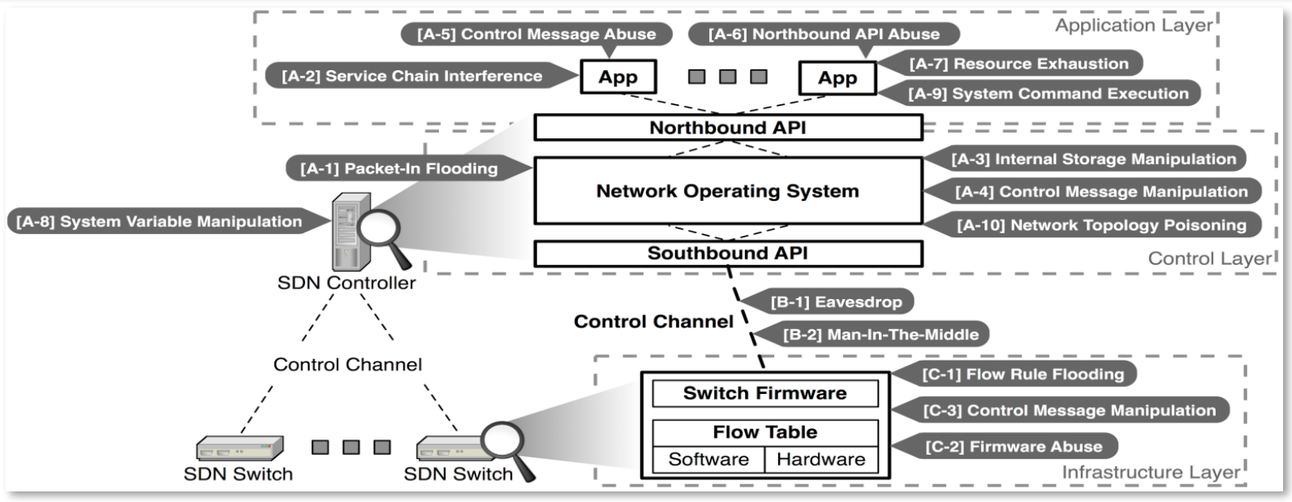
Security-Mode ONOS

Heedo Kang, Jinwoo Kim, Seunghyeon Lee, Seungwon Shin
KAIST

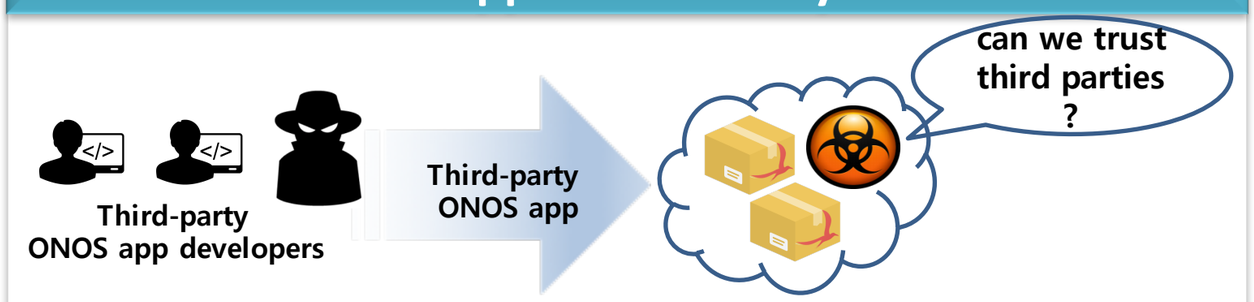
Motivation

- **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



From SDN vulnerability genome project – SDNSecurity.org

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)"

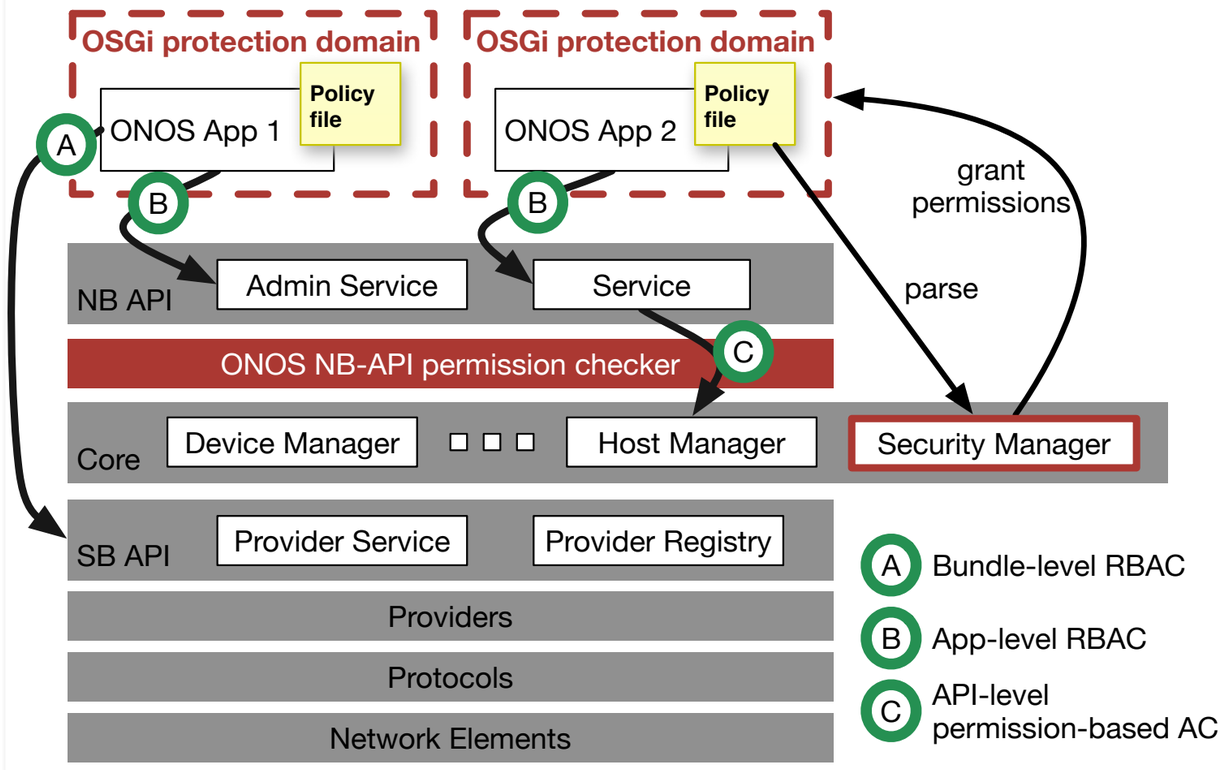
Security-Mode ONOS

- **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

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

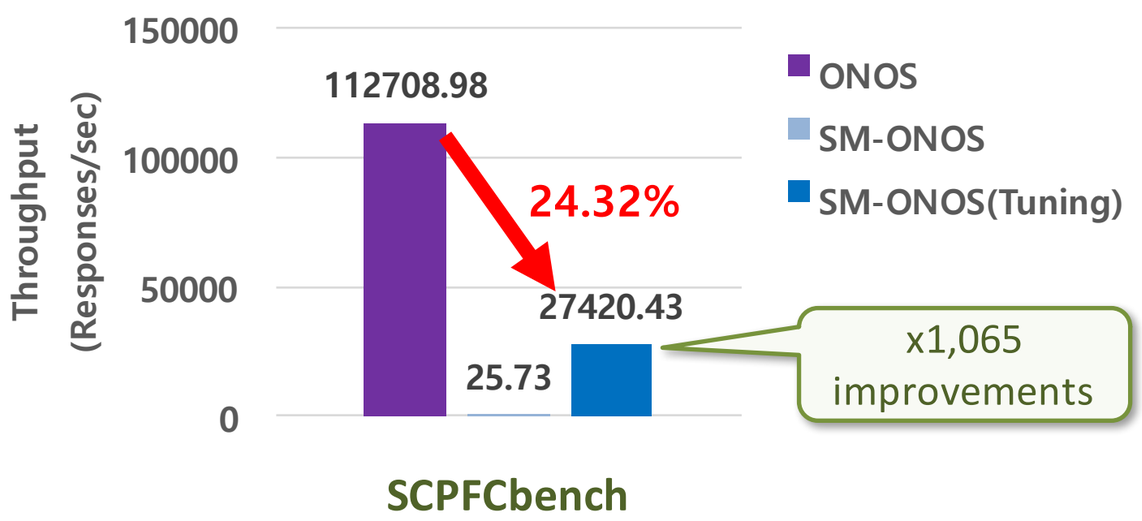
SM ONOS policy file

Design & Implementation



Performance evaluation

- **Experimental environment**
  - » Intel(R) Xeon(R) CPU E5-2650 v2 @ 2.60GHz / 8GB RAM



SCPFCbench

Roadmap

- **Now, we are working on …**
  - » Automatic policy extraction tool (**Hedoo Kang**)
  - » Virtual network permission (**Seunghyeon Lee**)
  - » Security policy enforcement on boot (**Jinwoo Kim**)
- **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