Feature proposal

ONOS Security:

Conservative-mode

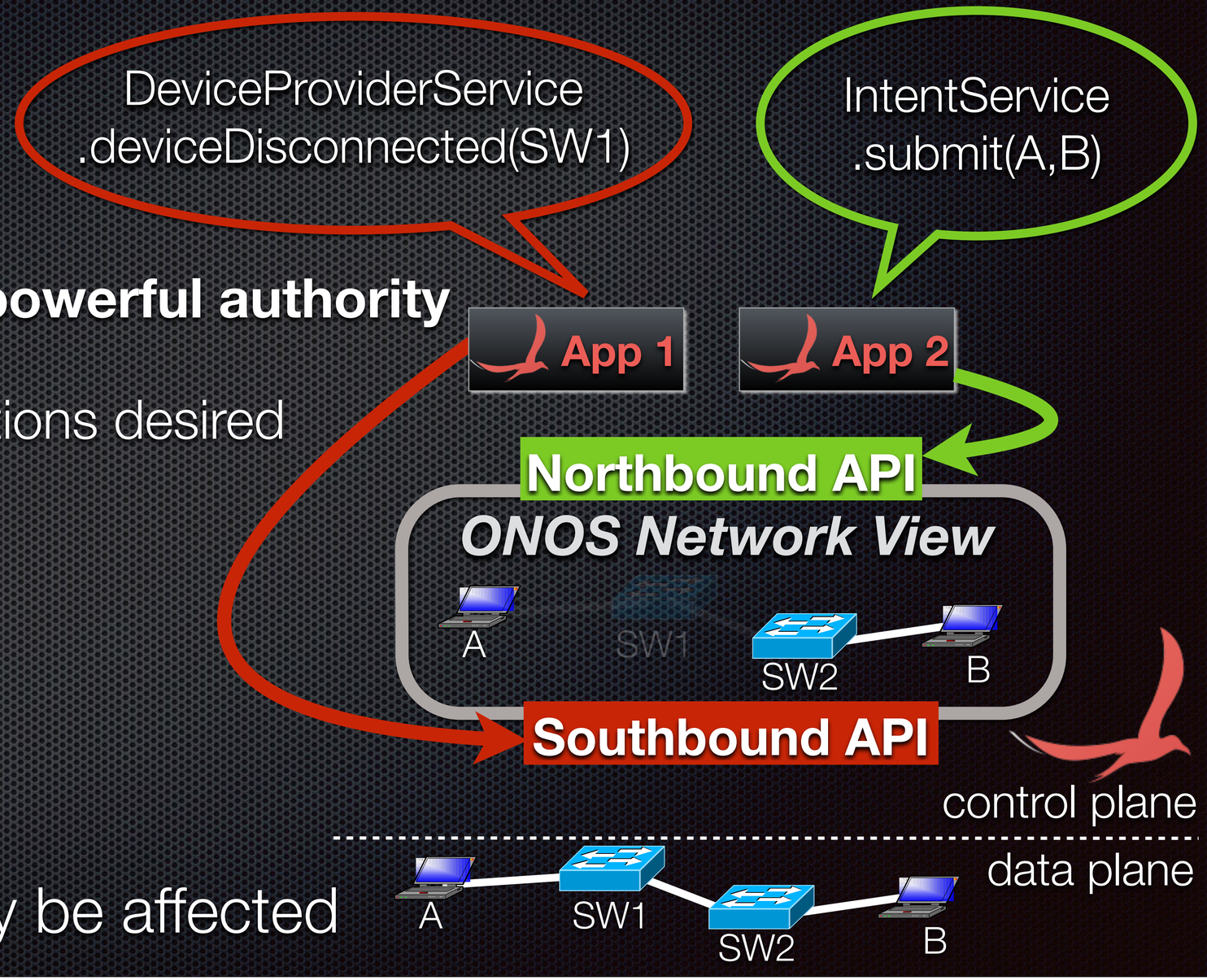
ONOS
Open Network Operating System

SRI International
Phillip Porras (porras@csl.sri.com)
Martin Fong (mwfong@csl.sri.com)

KAIST
Seungwon Shin (claude@kaist.ac.kr)
Changhoon Yoon (chyoon87@kaist.ac.kr)

Motivation

- ONOS applications are granted a **powerful authority**
  - Can perform any network operations desired
    - **Install flow rules!**
    - **Read flow statistics!**
    - **…**
    - **Modify network topology!?**



Mission-critical applications may be affected

Conservative-mode ONOS: The Objectives

- Offer a new option for granting the true minimum required capability to ONOS applications (*Least-privileged*)
- Let the network operators know what each ONOS application is capable of

Conservative-mode ONOS: Permission model

(1) Bundle-level Role-based Access Control

ONOS applications must **ONLY** access the **NB APIs** and other necessary utilities

(2) Application-level Role-based Access Control

Non-administrative ONOS applications must **NOT** access the **Administrative NB APIs** (Admin Services)

(3) API-level Permission-based Access Control

ONOS application must be granted a **permission** to make each API call

Conservative-mode ONOS: Policy file (example)

```
<bundle name="onos-example-app" description="ONOS App policy example">

  (1) <type> ONOS Application </type>

  (2) <role> non-admin </role>

  (3)   <uses-permission onos:name="onos.permission.INTENT_WRITE"/>
        <uses-permission onos:name="onos.permission.DEVICE_READ"/>
        <uses-permission onos:name="onos.permission.TOPOLOGY_EVENT"/>
        <uses-permission onos:name="onos.permission.PACKET_EVENT"/>

</bundle>
```

(1) Bundle-level Role-based Access Control

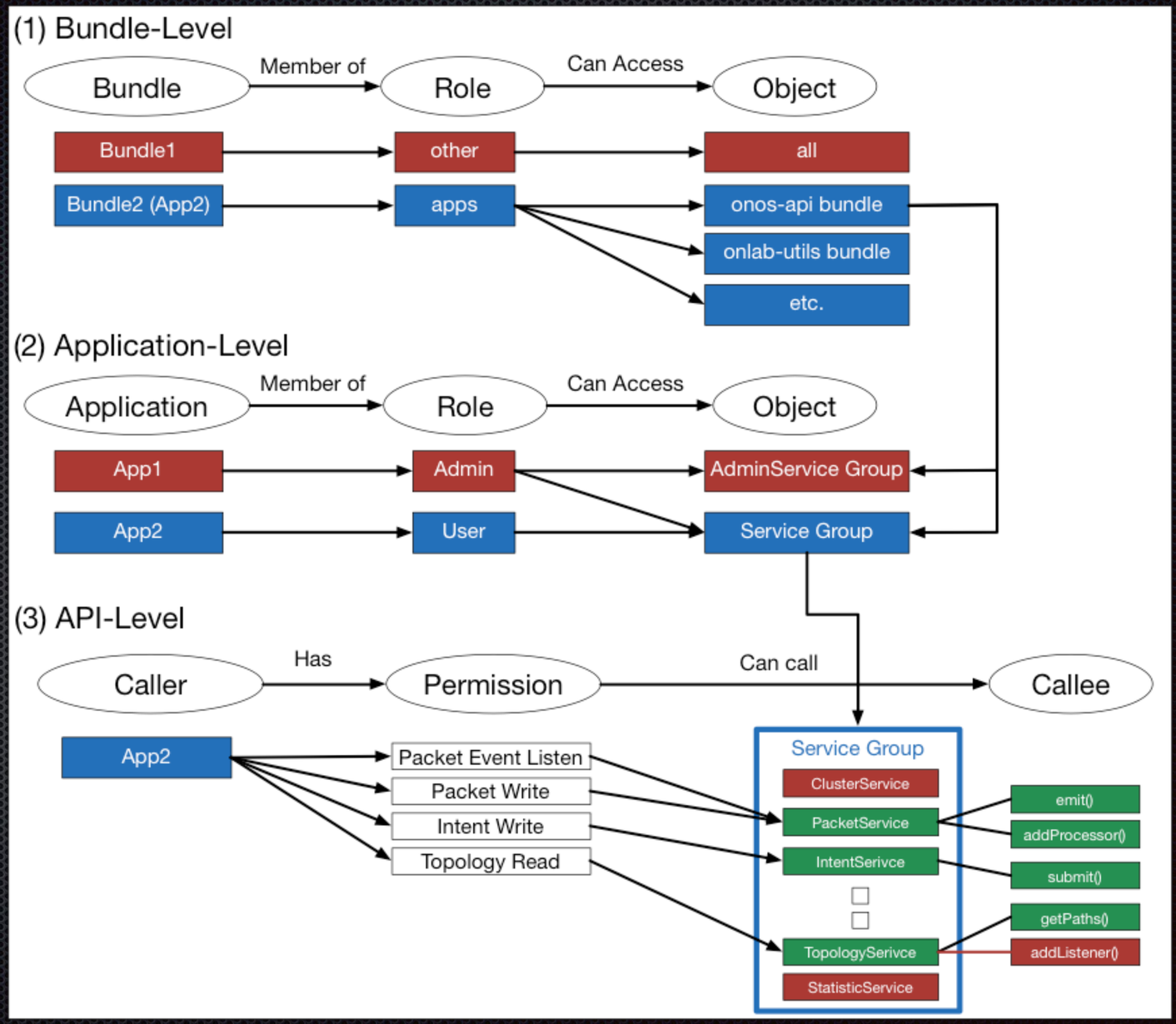
(2) Application-level Role-based Access Control

(3) API-level Permission-based Access Control

- **<type>** : a **bundle** is an **ONOS application or NOT**
- **<role>** : an **ONOS application** is **administrative** app or **NOT**
- **<uses-permission>** : a list of **permissions** to be granted to an ONOS app bundle

Thank you!

Backup


(1) Bundle-Level
Bundle
Member of
Role
Can Access
Object
Bundle1
other
all
Bundle2 (App2)
apps
onos-api bundle
onlab-utils bundle
etc.
(2) Application-Level
Application
Member of
Role
Can Access
Object
App1
Admin
AdminService Group
App2
User
Service Group
(3) API-Level
Caller
Has
Permission
Can call
Callee
App2
Packet Event Listen
Packet Write
Intent Write
Topology Read
Service Group
ClusterService
PacketService
IntentSerivce
TopologySerivce
StatisticService
emit()
addProcessor()
submit()
getPaths()
addListener()