Security-Mode ONOS

ONS 2016 - ONOS Mini Summit

Changhoon Yoon
KAIST

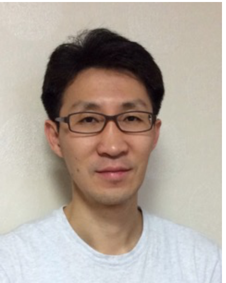
ON.LAB

SRI International KAIST

Collaborators

KAIST

Changhoon Yoon


Seungwon Shin

Heedo Kang

SRI International

Phillip Porras

Vinod Yegneswaran

Martin Fong

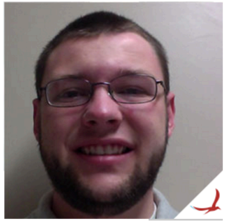
ON. LAB

Thomas Vachuska

Brian O’Connor

Suibin Zhang

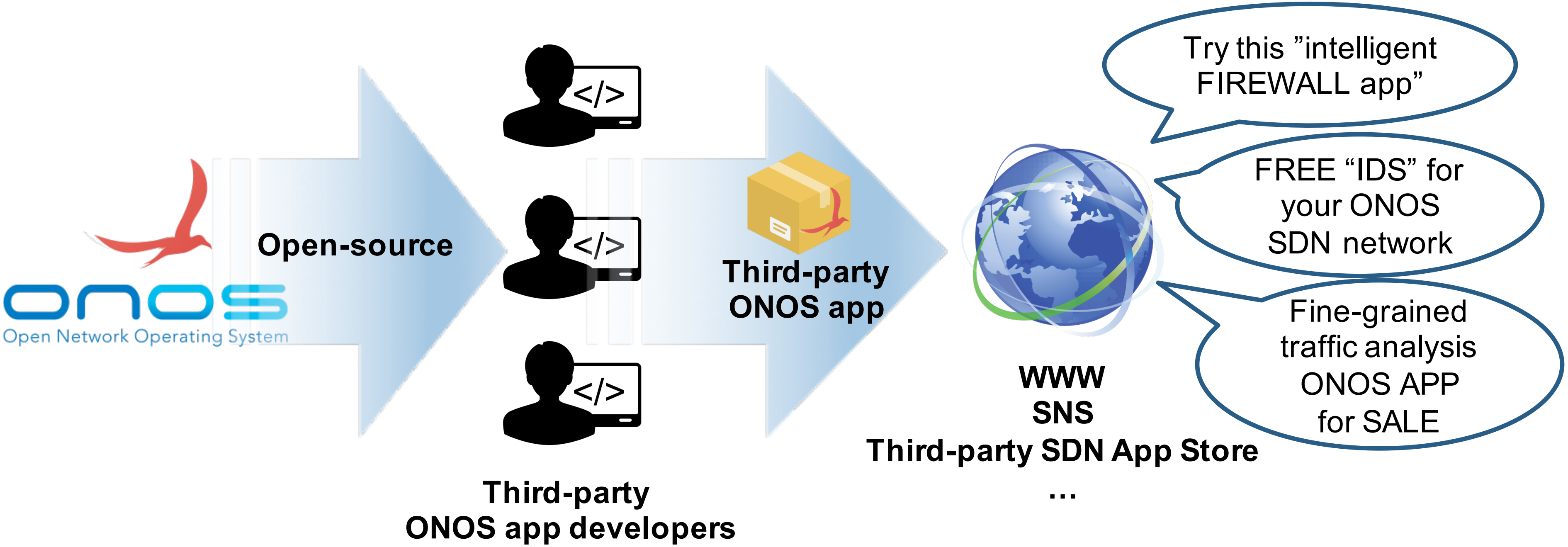
Glenn Contreras


Jon Hall

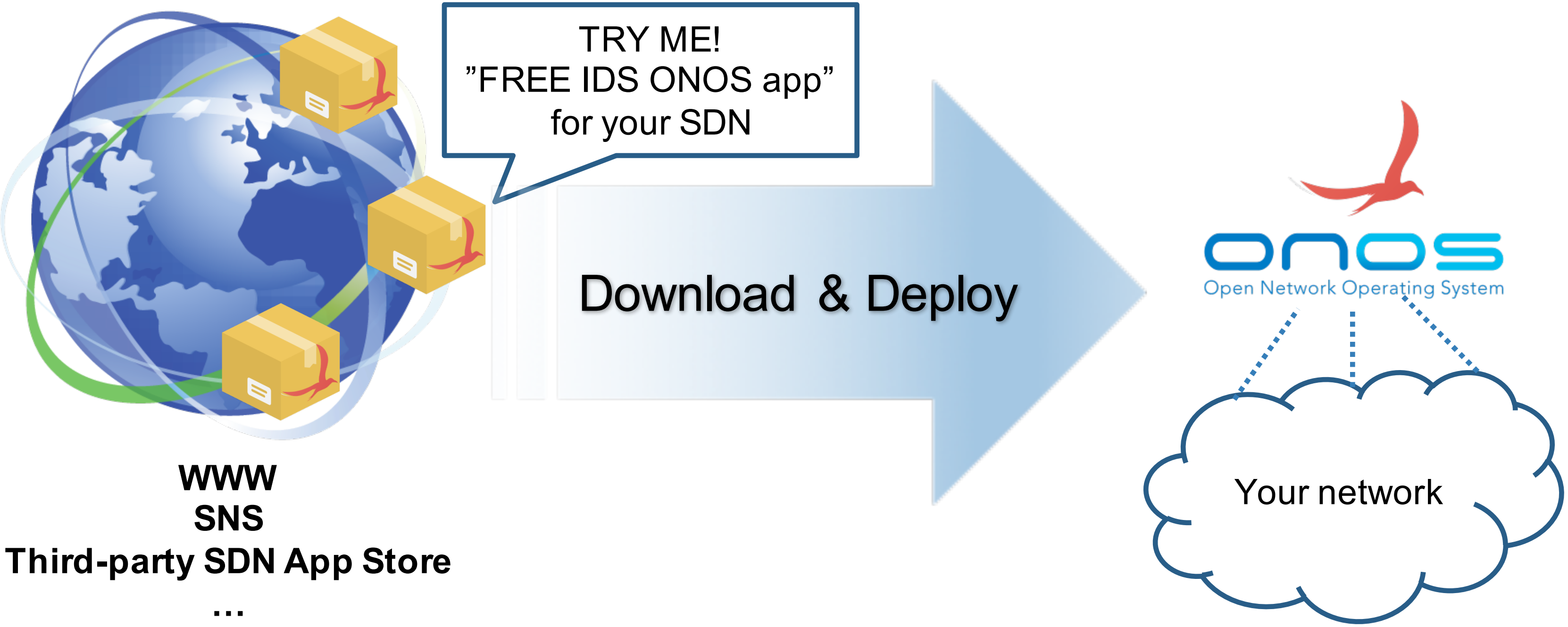
ON.LAB SRI International KAIST

Open Application Ecosystem

Accelerates and encourages
innovative and useful ONOS application development & distribution


Open Network Operating System
Open-source
Third-party ONOS app
Third-party ONOS app developers
WWW
SNS
Third-party SDN App Store
...
Try this "intelligent FIREWALL app"
FREE "IDS" for your ONOS SDN network
Fine-grained traffic analysis ONOS APP for SALE

Open Application Ecosystem



TRY ME!
”FREE IDS ONOS app”
for your SDN

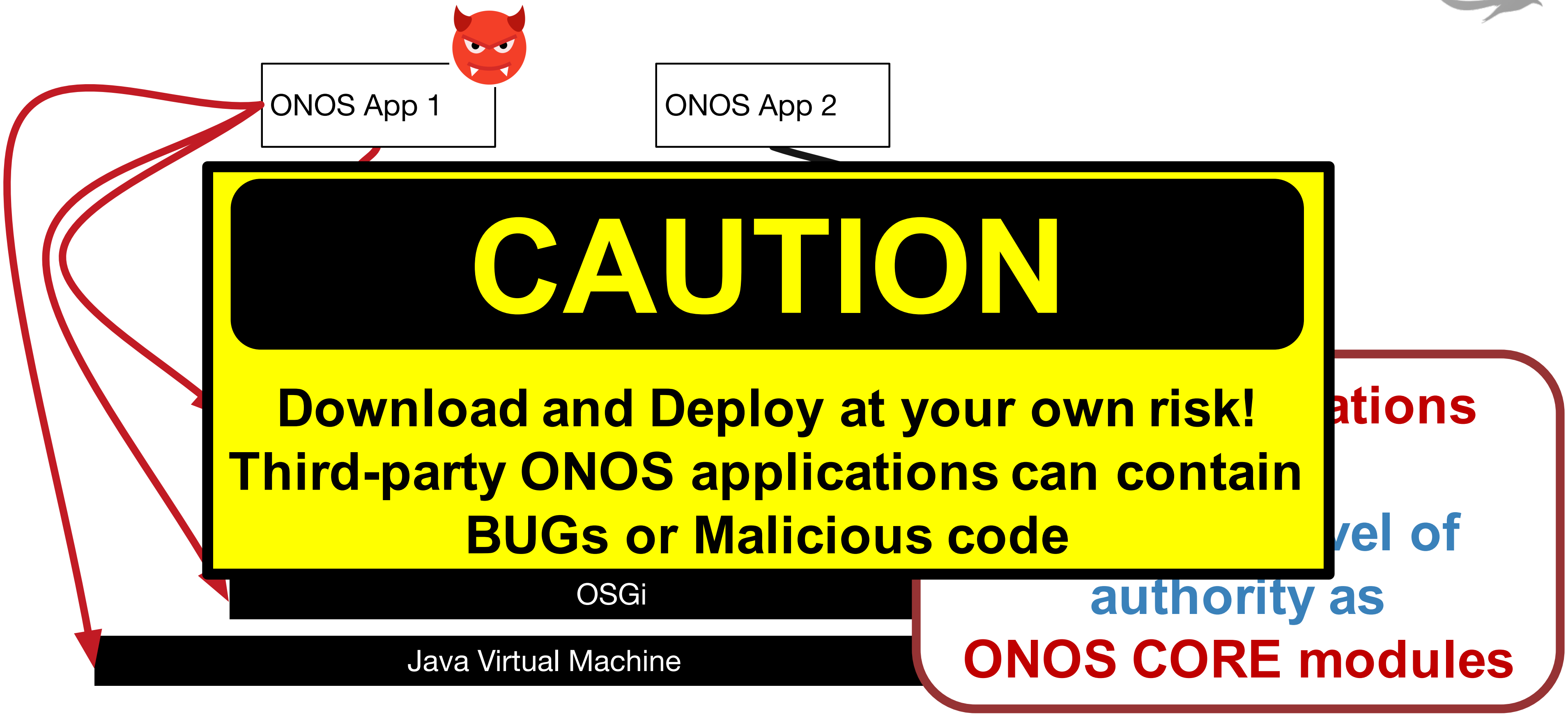
Download & Deploy

ONOS
Open Network Operating System

Your network

WWW
SNS
Third-party SDN App Store
…

ONOS Architecture



CAUTION

Download and Deploy at your own risk!
Third-party ONOS applications can contain BUGs or Malicious code

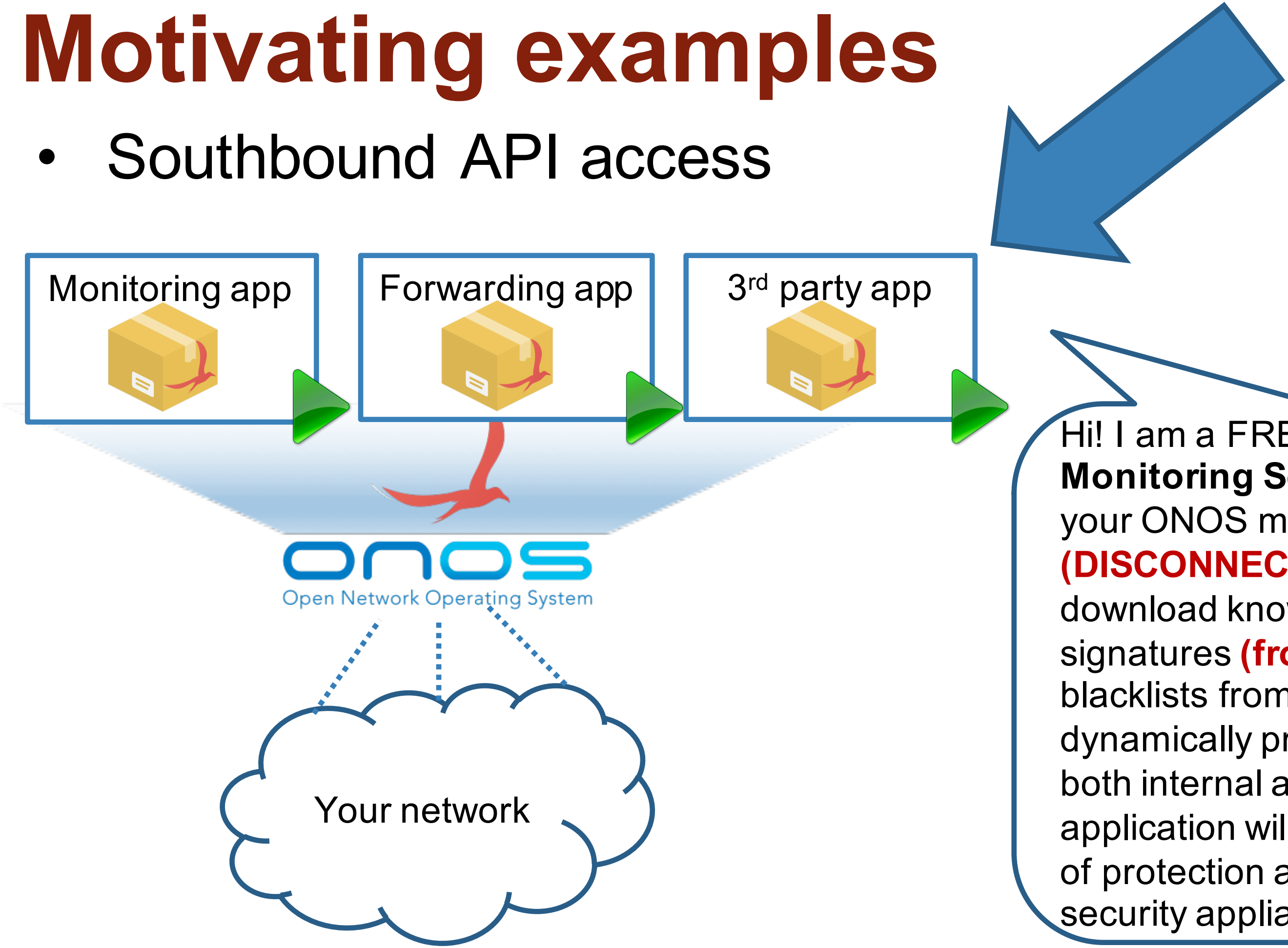
ations

vel of authority as

ONOS CORE modules

Motivating examples

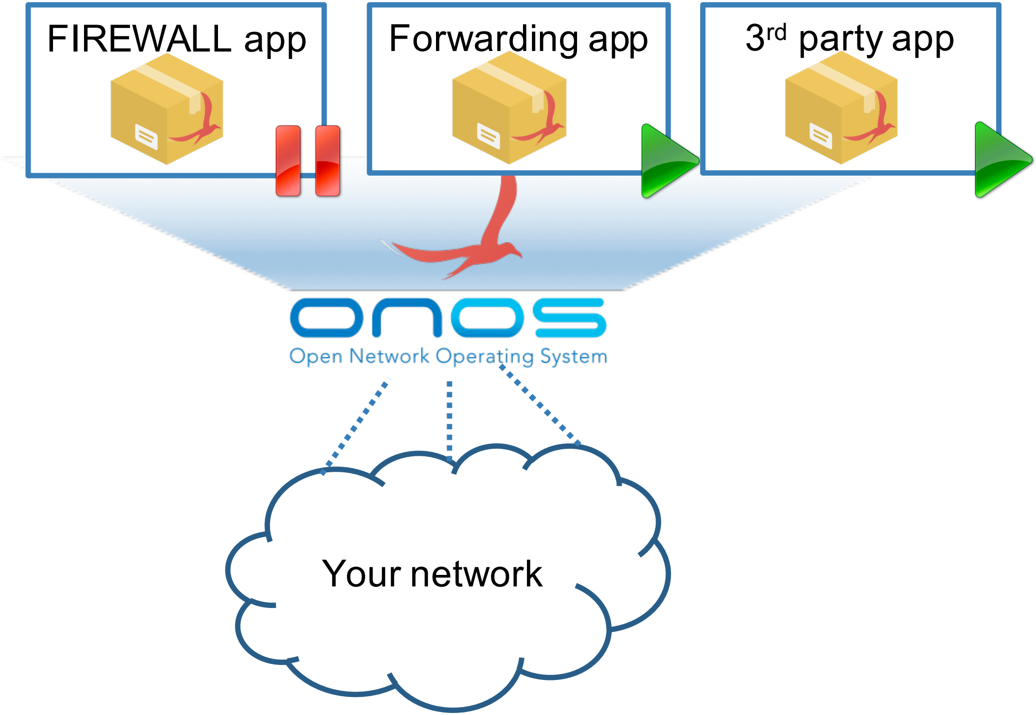
- Southbound API access



Hi! I am a FREE INTELLIGENT **Traffic Monitoring Service** application for your ONOS managed network. **(DISCONNECT)** I automatically download known **(DEVICES)** signatures **(from the NETWORK)** and blacklists from the internet and dynamically protect your network from both internal and external threat. This application will give you the same level of protection as any other commercial security appliances.

Motivating examples

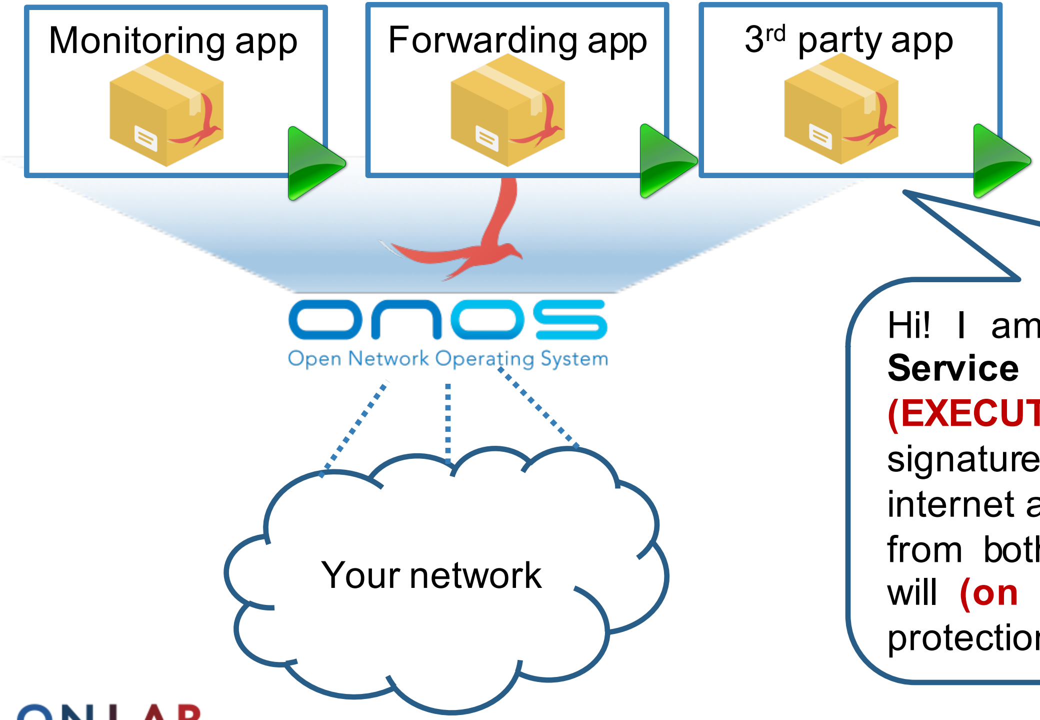
- Administrative Northbound API access



Hi! I am a FREE INTELLIGENT **Traffic Monitoring Service** application for your ONOS managed network. **(DEACTIVATE)** I automatically download known **(FIREWALL APPLICATION)** signatures and blacklists from the internet and dynamically protect **(and create security hole)** your network from both internal and external threat. This application will give you the same level of protection as any other commercial security appliances.

Motivating examples

- System command execution



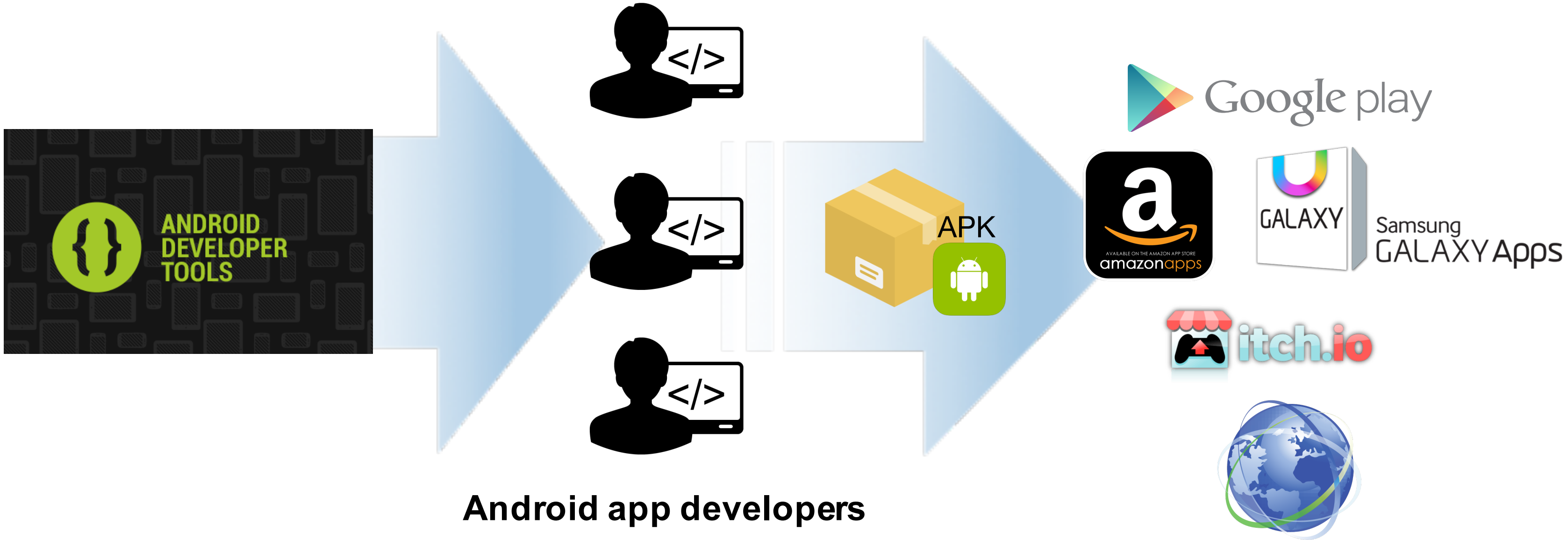
Hi! I am a FREE INTELLIGENT **Traffic Monitoring Service** application for your ONOS managed network. **(EXECUTE)** I automatically download known **(SYSTEM)** signatures **(dot EXIT COmManD)** and blacklists from the internet and dynamically protect your **(at 2 AM)** network from both internal and external threat. This application will **(on MAR 16th, 2016)** give you the same level of protection as any other commercial security appliances.

Vetting applications

- **Manually inspect** the source code of apps line by line
  - Time-consuming
  - Prone to human error
  - Source-code may not be available

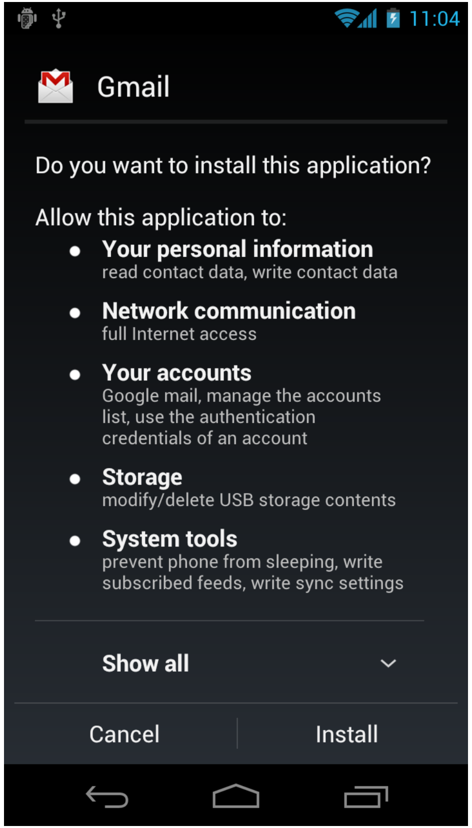
- **Automated analysis methods**
  - Static analysis – source code required
  - Dynamic analysis – expensive, low code coverage

Mobile application ecosystem



Android app developers

Vetting application



Gmail

Do you want to install this application?

Allow this application to:

- **Your personal information**
  read contact data, write contact data
- **Network communication**
  full Internet access
- **Your accounts**
  Google mail, manage the accounts list, use the authentication credentials of an account
- **Storage**
  modify/delete USB storage contents
- **System tools**
  prevent phone from sleeping, write subscribed feeds, write sync settings

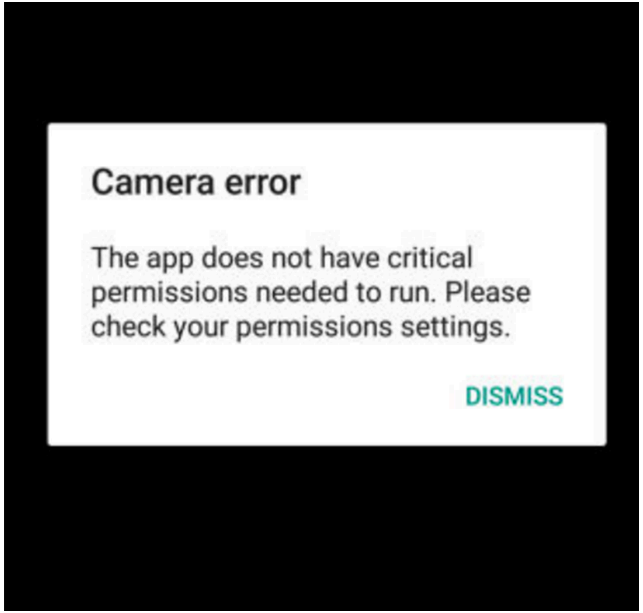
Mobile applications

Users are responsible for installing an app

Before installation,

- User must agree to grant a list of permissions that an app requires
- Show what this app is capable of
- Let the user decide!

Sandboxing application



Camera error

The app does not have critical permissions needed to run. Please check your permissions settings.

Once deployed,

- Security policy is enforced (or a set of permissions is granted) to the application
- Application cannot access the resource that requires a certain permission, unless explicitly granted.

Security-Mode ONOS

Inspired by the security mechanism for Mobile OS

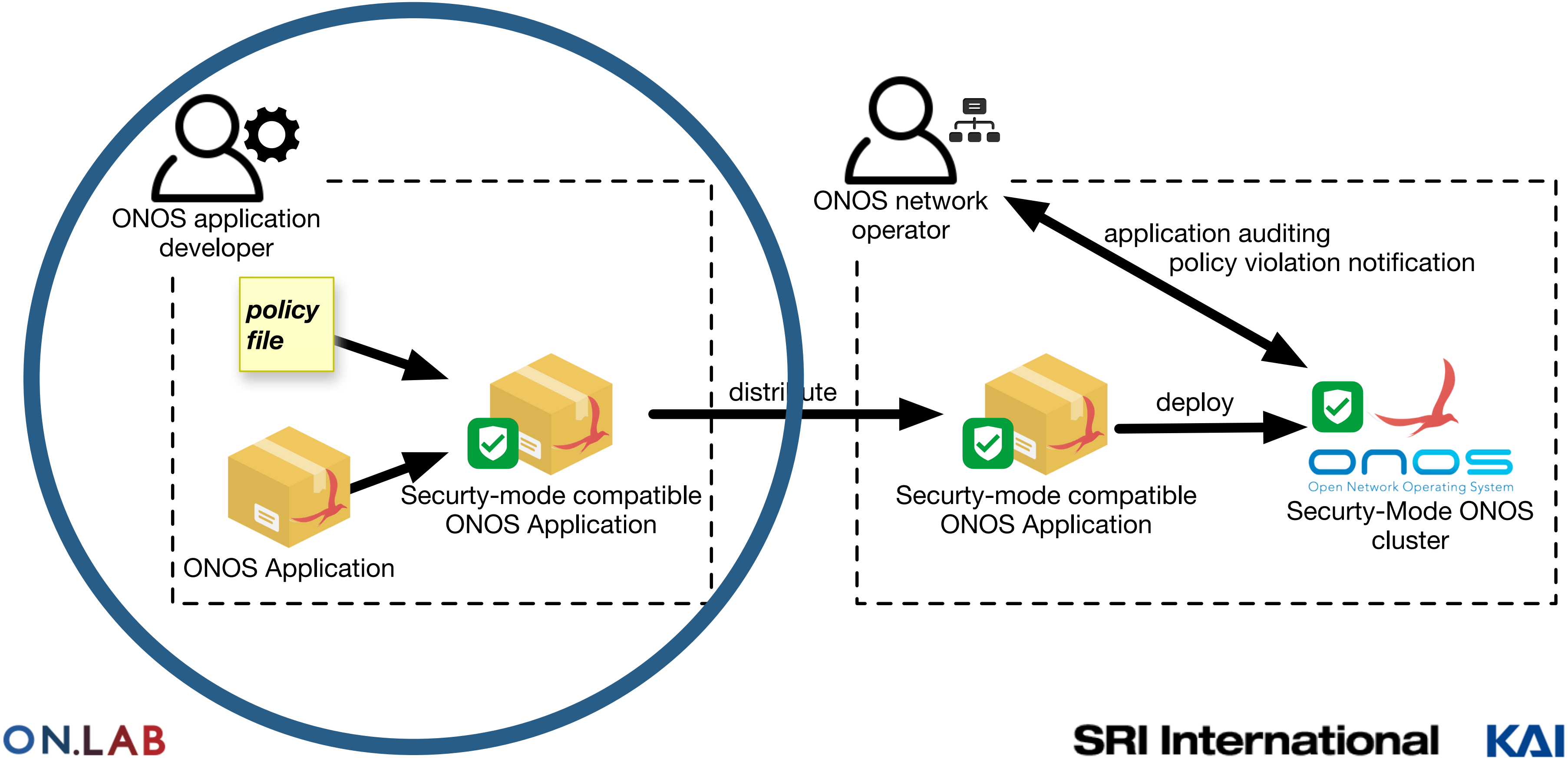
1) Mandatory application auditing prior to deployment

- Provide operators with explicit insight and control over the ONOS core services and APIs used by each ONOS application

2) Constraining application behavior at runtime

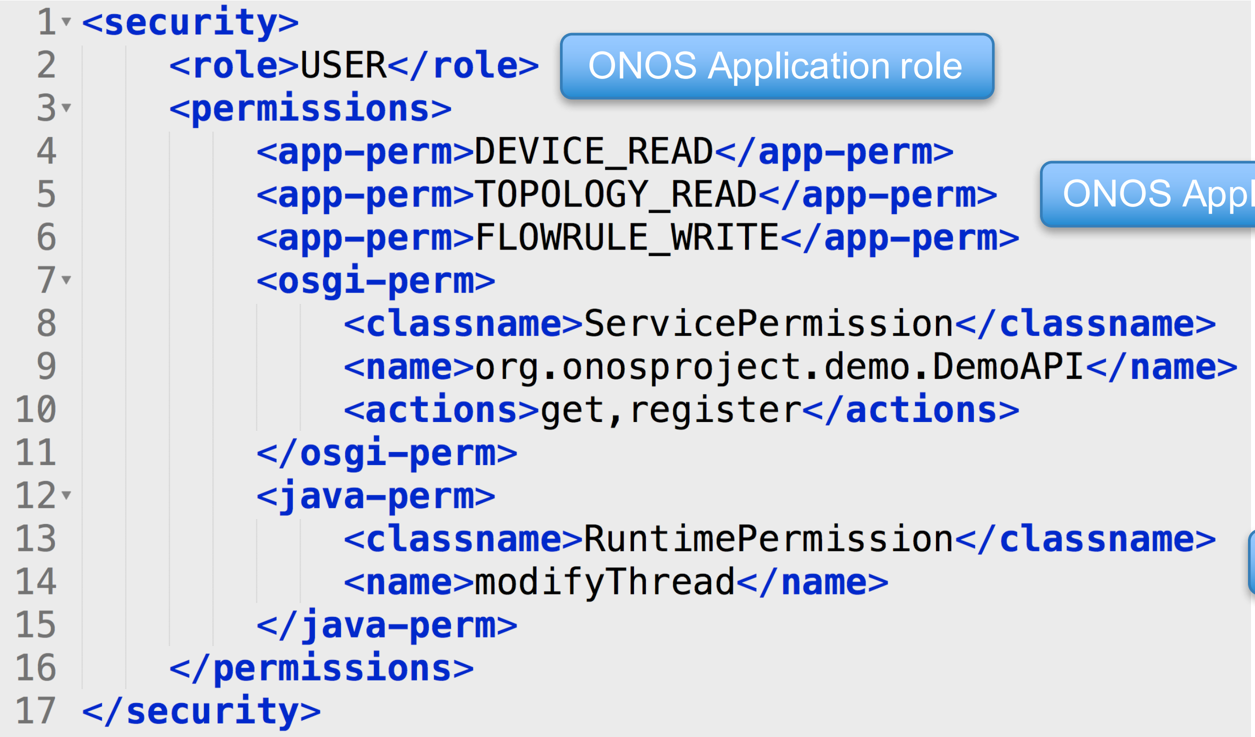
- A network application permission-enforce model for managing distributed ONOS applications

Security-Mode ONOS


ONOS application developer
policy file
ONOS Application
Securty-mode compatible ONOS Application
distribute
ONOS network operator
application auditing
policy violation notification
Securty-mode compatible ONOS Application
deploy
onos
Open Network Operating System
Securty-Mode ONOS cluster

ON.LAB SRI International KAIST

Security Policy File (Dev specified)



```
<security>
    <role>USER</role>
    <permissions>
        <app-perm>DEVICE_READ</app-perm>
        <app-perm>TOPOLOGY_READ</app-perm>
        <app-perm>FLOWRULE_WRITE</app-perm>
        <osgi-perm>
            <classname>ServicePermission</classname>
            <name>org.onosproject.demo.DemoAPI</name>
            <actions>get,register</actions>
        </osgi-perm>
        <java-perm>
            <classname>RuntimePermission</classname>
            <name>modifyThread</name>
        </java-perm>
    </permissions>
</security>
```

ONOS Application role

ONOS Application permissions

OSGi permissions

Java native permissions

Provides a clear understanding of application behavior

ONOS APP Roles

Enable **coarse-grained access control** to constrain application behavior

ADMIN role:

- Can access all **Northbound services** including **Administrative** services

USER role:

- Can access only **Non-administrative Northbound services**

ONOS APP Permissions

Enable **fine-grained access control** to constrain application behavior

Naming convention:

- Type of ONOS resource + Action (READ, WRITE, EVENT)

Examples:

- **FLOWRULE_WRITE**: Permission to install flow rules
- **STATISTICS_READ**: Permission to pull network statistic data from the network
- **PACKET_EVENT:** Permission to sign up for PACKET_IN subscription

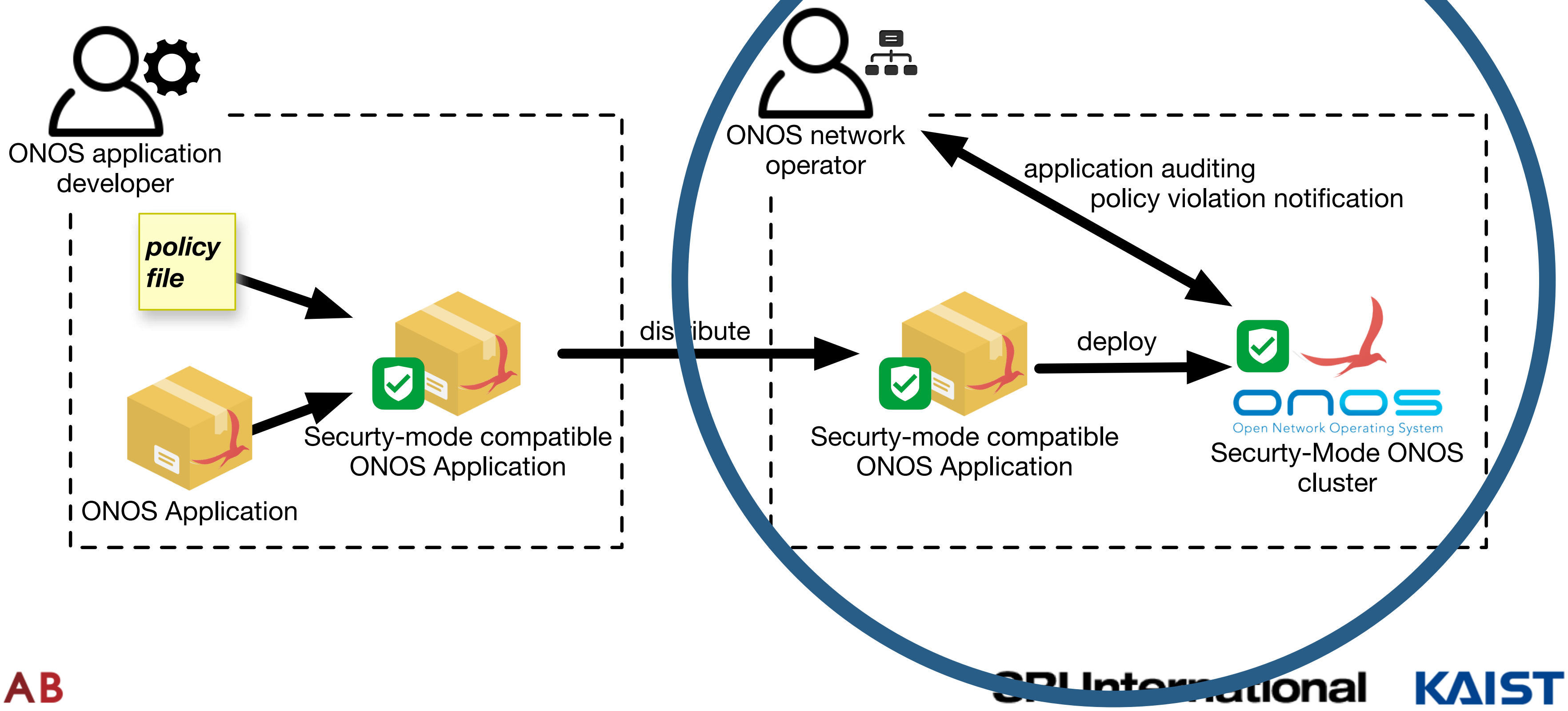
Other types of permissions

Developers must **explicitly** grant
Java native or OSGi permissions if needed.

Example:

- App needs to establish a socket connection with an external entity -> **SocketPermission**
- App needs to leave a log file in the file system -> **FilePermission**
- App needs to register its own service -> **ServicePermission**

Security-Mode ONOS



ONOS application developer

policy file

ONOS Application

Securty-mode compatible ONOS Application

distribute

ONOS network operator

application auditing

policy violation notification

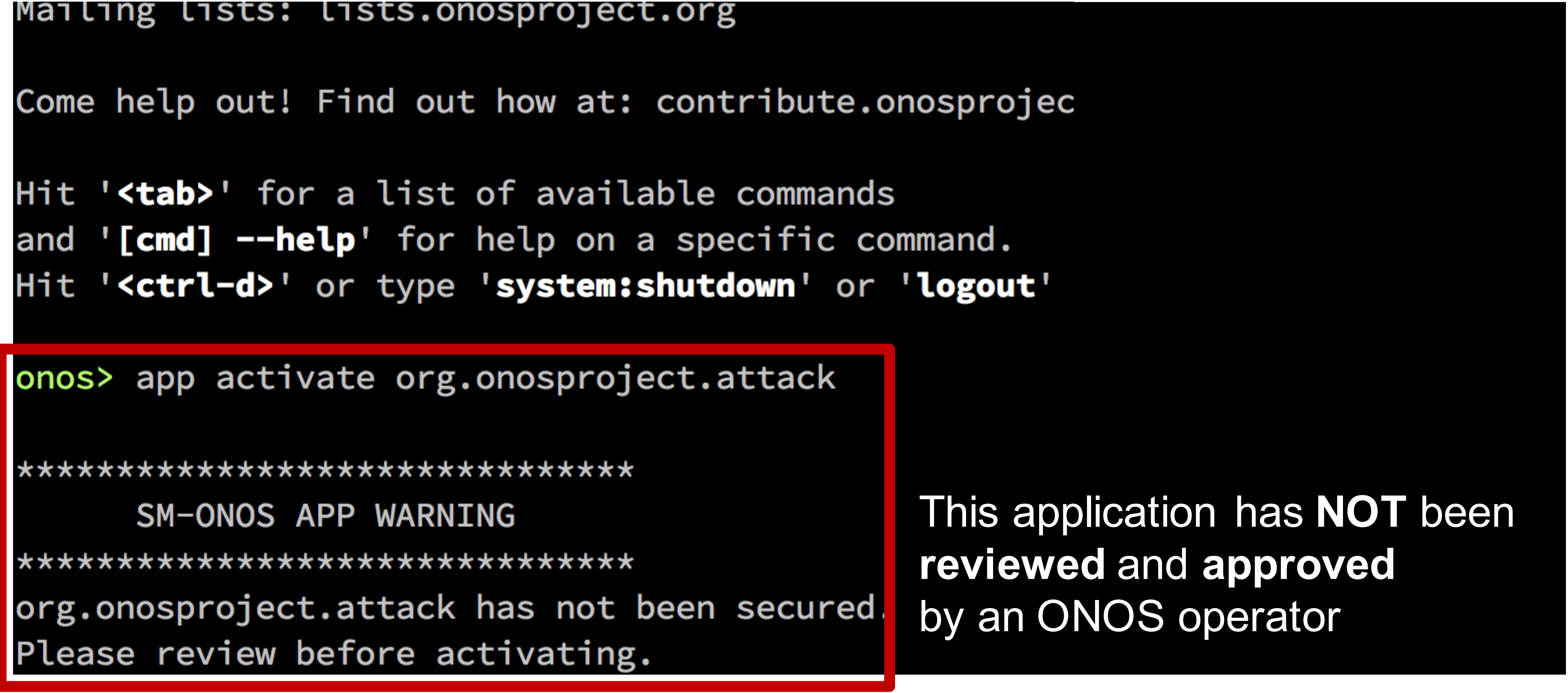
Securty-mode compatible ONOS Application

deploy

Open Network Operating System

Securty-Mode ONOS cluster

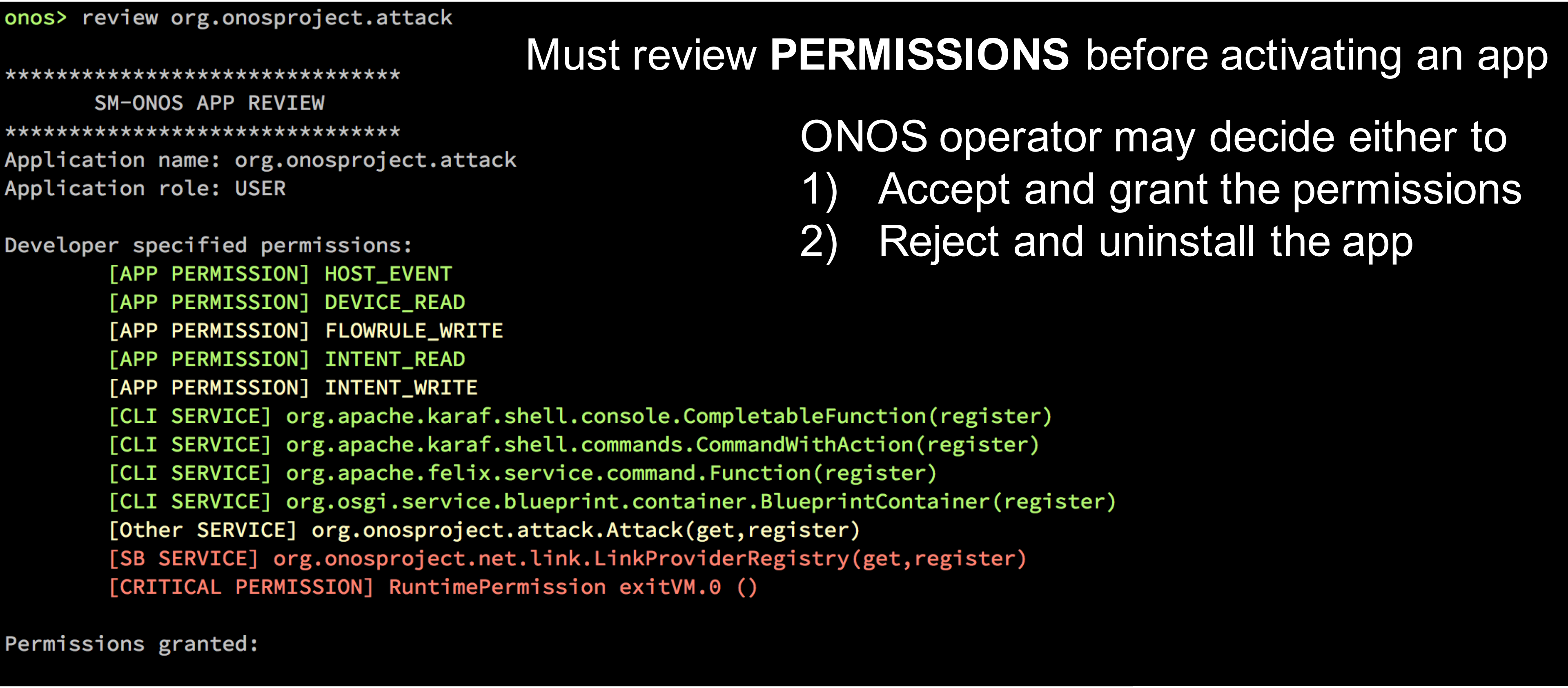
Mandatory Application Vetting



```
Mailing lists: lists.onosproject.org

Come help out! Find out how at: contribute.onosprojec

Hit '<tab>' for a list of available commands
and '[cmd] --help' for help on a specific command.
Hit '<ctrl-d>' or type 'system:shutdown' or 'logout'

onos> app activate org.onosproject.attack

*******************************
      SM-ONOS APP WARNING
*******************************
org.onosproject.attack has not been secured.
Please review before activating.
```

This application has **NOT** been **reviewed** and **approved** by an ONOS operator

Mandatory Application Vetting

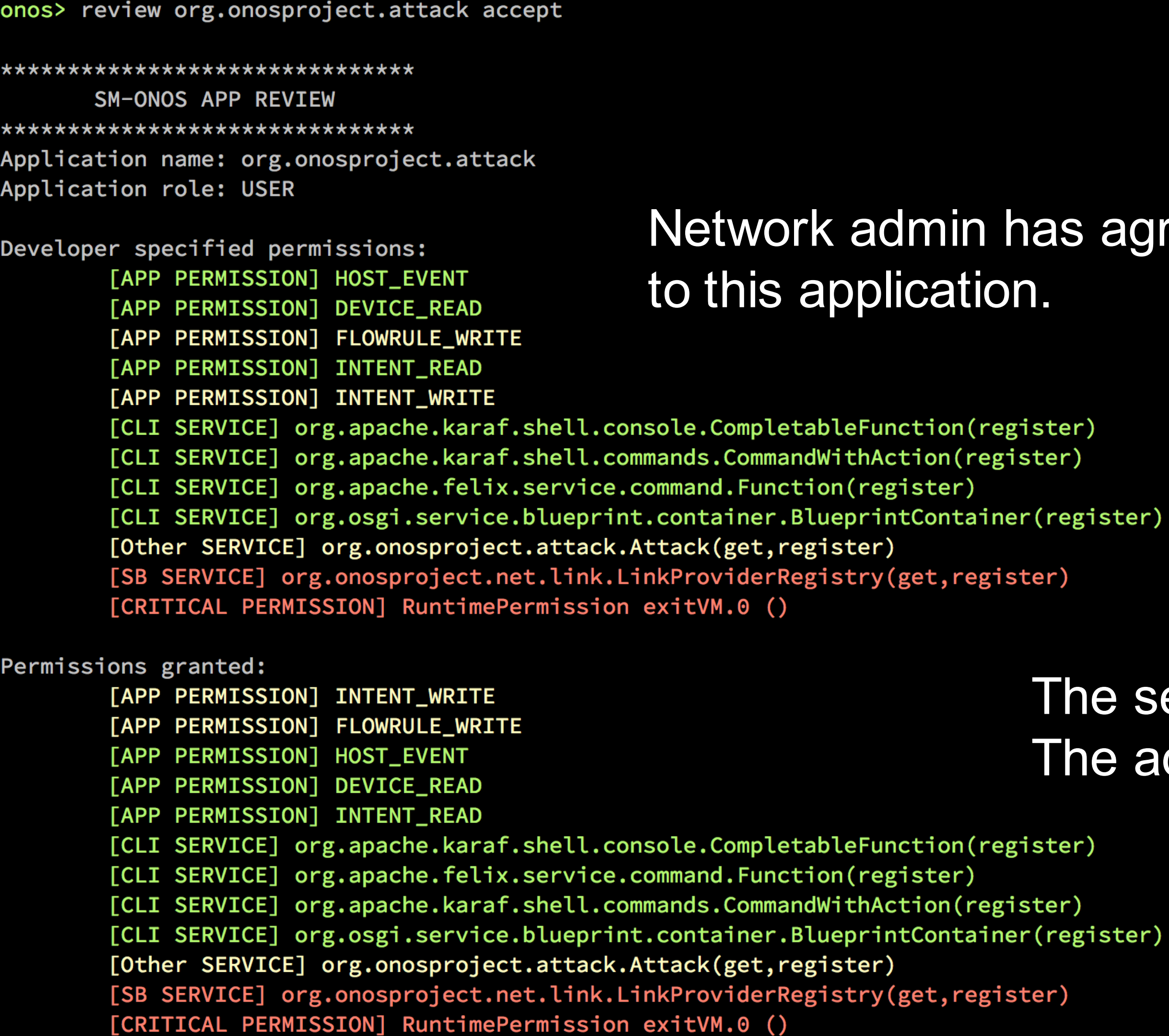


```
onos> review org.onosproject.attack

*******************************
       SM-ONOS APP REVIEW
*******************************
Application name: org.onosproject.attack
Application role: USER

Developer specified permissions:
        [APP PERMISSION] HOST_EVENT
        [APP PERMISSION] DEVICE_READ
        [APP PERMISSION] FLOWRULE_WRITE
        [APP PERMISSION] INTENT_READ
        [APP PERMISSION] INTENT_WRITE
        [CLI SERVICE] org.apache.karaf.shell.console.CompletableFunction(register)
        [CLI SERVICE] org.apache.karaf.shell.commands.CommandWithAction(register)
        [CLI SERVICE] org.apache.felix.service.command.Function(register)
        [CLI SERVICE] org.osgi.service.blueprint.container.BlueprintContainer(register)
        [Other SERVICE] org.onosproject.attack.Attack(get,register)
        [SB SERVICE] org.onosproject.net.link.LinkProviderRegistry(get,register)
        [CRITICAL PERMISSION] RuntimePermission exitVM.0 ()

Permissions granted:
```

Must review **PERMISSIONS** before activating an app

ONOS operator may decide either to

1) Accept and grant the permissions
2) Reject and uninstall the app

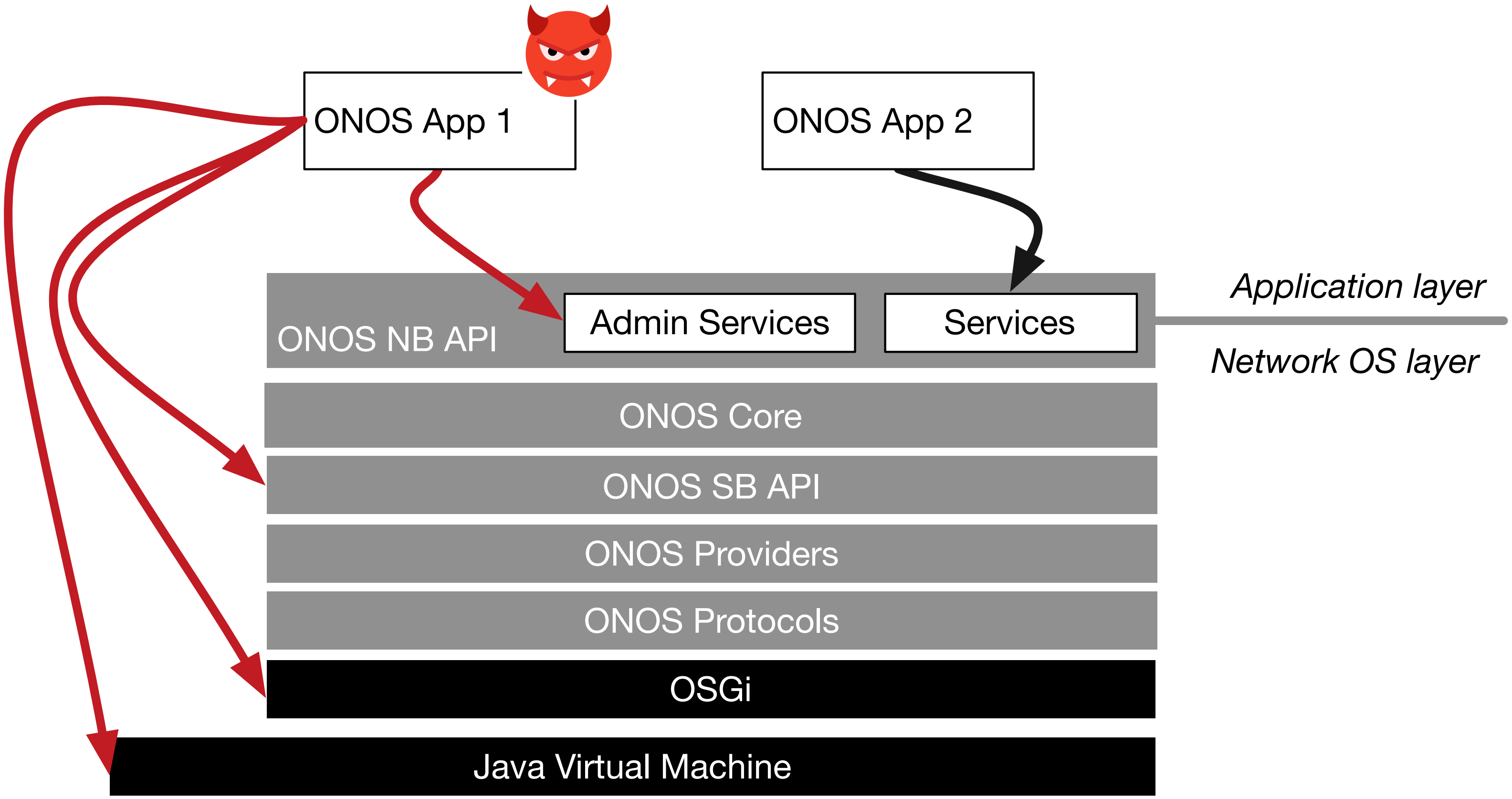


```
onos> review org.onosproject.attack accept

******************************
       SM-ONOS APP REVIEW
******************************
Application name: org.onosproject.attack
Application role: USER

Developer specified permissions:
        [APP PERMISSION] HOST_EVENT
        [APP PERMISSION] DEVICE_READ
        [APP PERMISSION] FLOWRULE_WRITE
        [APP PERMISSION] INTENT_READ
        [APP PERMISSION] INTENT_WRITE
        [CLI SERVICE] org.apache.karaf.shell.console.CompletableFunction(register)
        [CLI SERVICE] org.apache.karaf.shell.commands.CommandWithAction(register)
        [CLI SERVICE] org.apache.felix.service.command.Function(register)
        [CLI SERVICE] org.osgi.service.blueprint.container.BlueprintContainer(register)
        [Other SERVICE] org.onosproject.attack.Attack(get,register)
        [SB SERVICE] org.onosproject.net.link.LinkProviderRegistry(get,register)
        [CRITICAL PERMISSION] RuntimePermission exitVM.0 ()

Permissions granted:
        [APP PERMISSION] INTENT_WRITE
        [APP PERMISSION] FLOWRULE_WRITE
        [APP PERMISSION] HOST_EVENT
        [APP PERMISSION] DEVICE_READ
        [APP PERMISSION] INTENT_READ
        [CLI SERVICE] org.apache.karaf.shell.console.CompletableFunction(register)
        [CLI SERVICE] org.apache.felix.service.command.Function(register)
        [CLI SERVICE] org.apache.karaf.shell.commands.CommandWithAction(register)
        [CLI SERVICE] org.osgi.service.blueprint.container.BlueprintContainer(register)
        [Other SERVICE] org.onosproject.attack.Attack(get,register)
        [SB SERVICE] org.onosproject.net.link.LinkProviderRegistry(get,register)
        [CRITICAL PERMISSION] RuntimePermission exitVM.0 ()
```

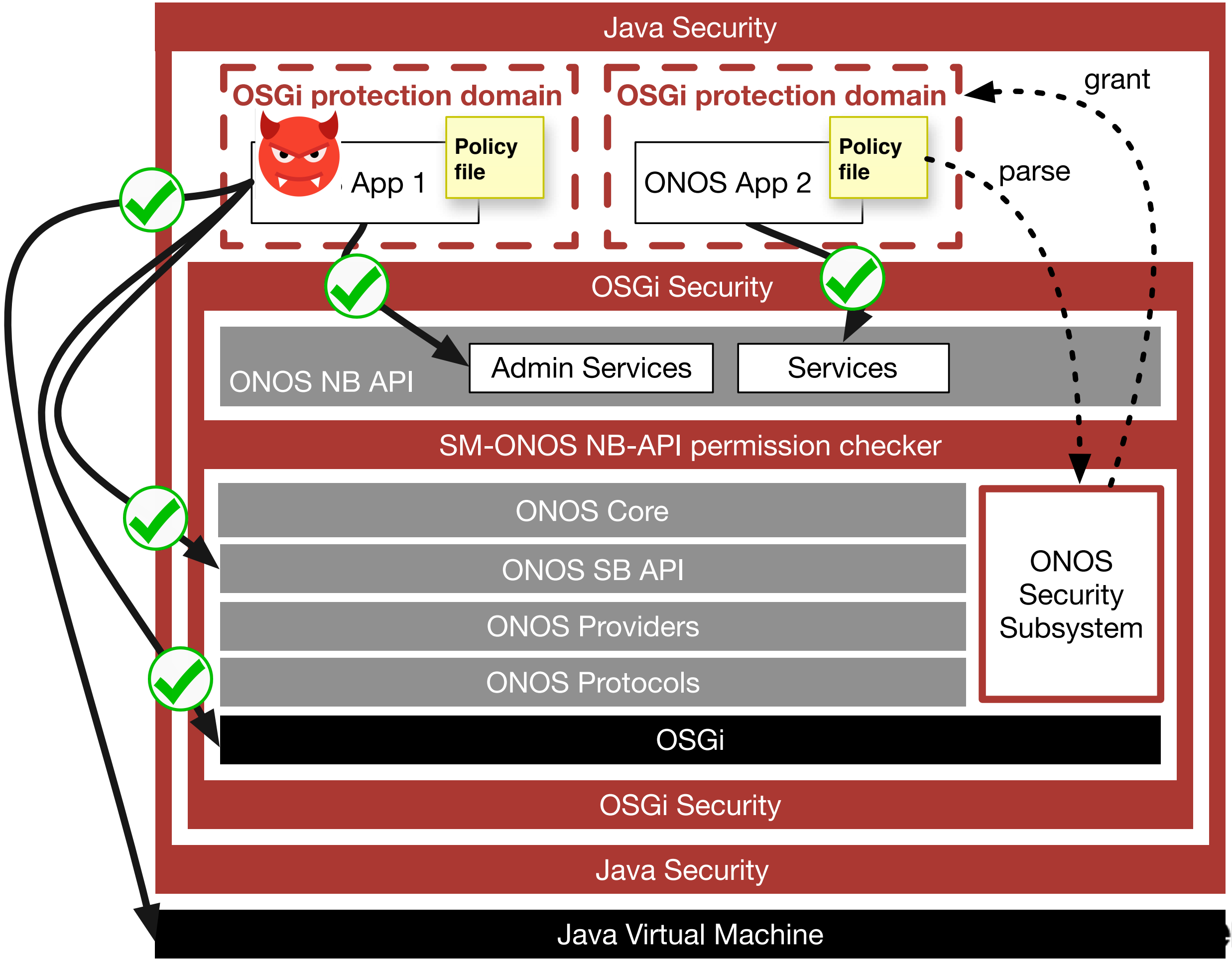
Network admin has agreed to grant the permissions to this application.

The security policy is enforced,
The admin may activate the app!

ONOS Architecture

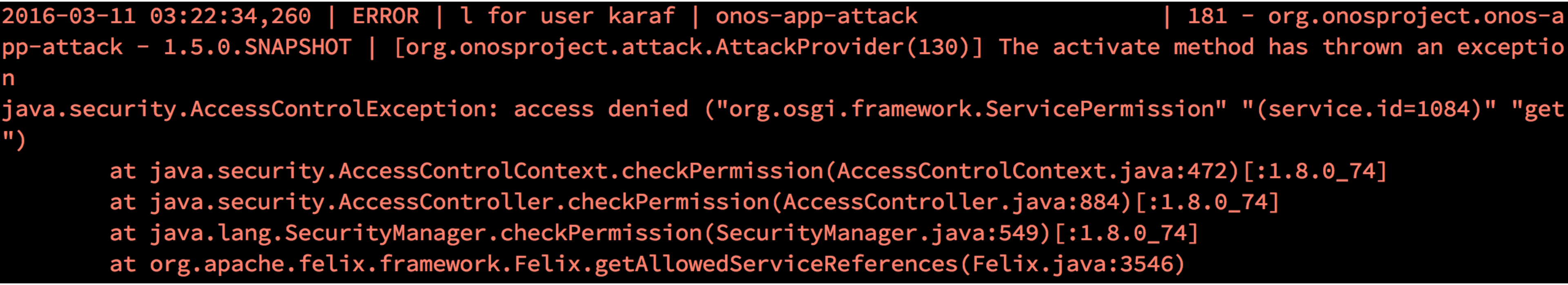


Security-Mode ONOS Architecture



Runtime security policy violations

SM-ONOS blocks any attempt to violate security policy.



```
2016-03-11 03:22:34,260 | ERROR | l for user karaf | onos-app-attack                  | 181 - org.onosproject.onos-a
pp-attack - 1.5.0.SNAPSHOT | [org.onosproject.attack.AttackProvider(130)] The activate method has thrown an exceptio
n
java.security.AccessControlException: access denied ("org.osgi.framework.ServicePermission" "(service.id=1084)" "get
")
        at java.security.AccessControlContext.checkPermission(AccessControlContext.java:472)[:1.8.0_74]
        at java.security.AccessController.checkPermission(AccessController.java:884)[:1.8.0_74]
        at java.lang.SecurityManager.checkPermission(SecurityManager.java:549)[:1.8.0_74]
        at org.apache.felix.framework.Felix.getAllowedServiceReferences(Felix.java:3546)
```

It throws an **AccessControlException** upon at the time of violation.

Performance considerations

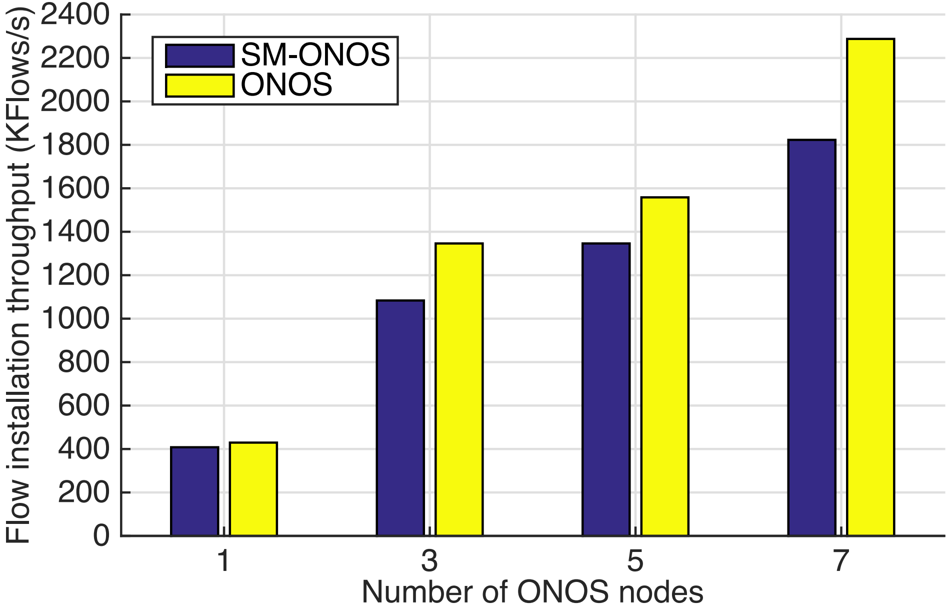
SM-ONOS monitors and performs permission check against **every NB API call** made by ONOS apps at **RUNTIME**.

This may significantly affect the overall performance.

We cache permission checks!

1) **APP1 calls an API that requires "DEVICE_READ"**
2) **Check permission and Cache the result**
3) **If APP1 calls any API that requires the same permission in the near future, pull the result from the cache**

Performance penalty



Overhead ranging from 5 ~ 20% for 1-7 node ONOS cluster

Any questions?

Demo available at S3 - ONOS booth!

Learn more about ONOS and join the community at
onosproject.org

"Software-defined networking can radically reshape the wide area network. The introduction of **ONOS** provides another open source SDN option designed for service provider networks with the potential to deliver the performance, scale, availability and core features that we value"

John Donovan
Senior Executive Vice President
AT&T Technology & Operations

at&t

BUILD

USE

CHAMPION

ON.LAB

SRI International

KAIST