ONOS Security:

Security-mode

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)

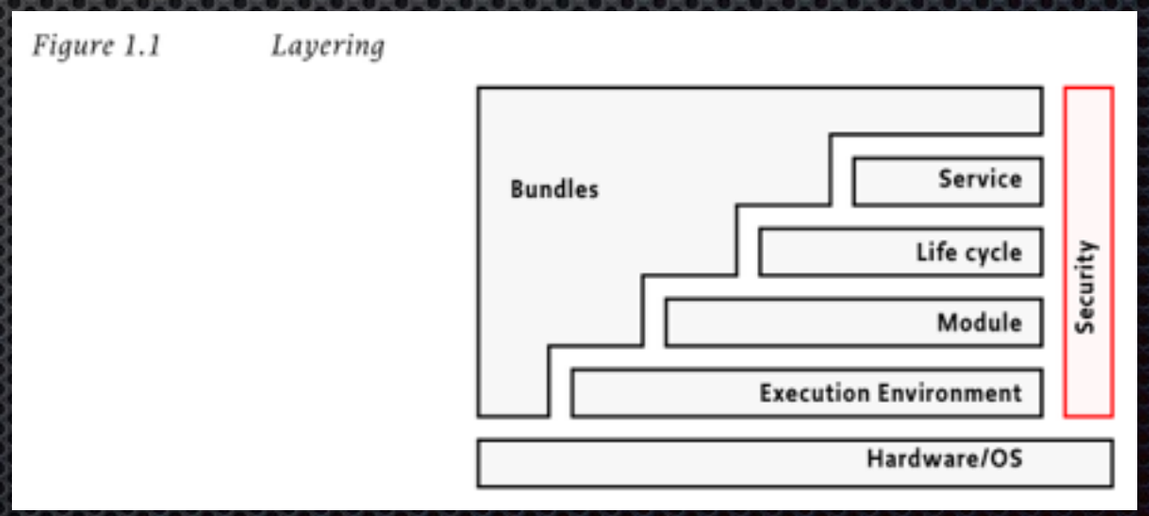
Feb. 13th 2015

Outline

- Implementation plan
- ONOS application permissions
- Agenda

Implementation plan

- **The OSGi Security Layer**
  - “It provides the infrastructure to deploy and manage applications that must run in fine-grained controlled environments” [1]
- and we are going to leverage its functionalities



Reference: [1] OSGi Service Platform Release 4 Version 4.3 Core Specification

Implementation plan

(1) Bundle-level Role-based Access Control

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

- OSGi permission types [2]
  - **PackagePermission**
    - Controls which packages a bundle is allowed to import and/or export
  - **BundlePermission**
    - Controls which bundles a bundle is allowed to require

ONOS architecture: well-designed

easy to specify which packages/bundles should be available to ONOS apps

Reference:
[2] Hall, Richard, et al. OSGi in action: Creating modular applications in Java. Manning Publications Co., 2011.

Implementation plan

(2) Application-level Role-based Access Control

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

- OSGi permission types [2]
  - **ServicePermission**
    - Controls which services a bundle is allowed to publish and/or use

ONOS architecture:
well-designed

AdminServices
and
regular Services

Reference:
[2] Hall, Richard, et al. OSGi in action: Creating modular applications in Java. Manning Publications Co., 2011.

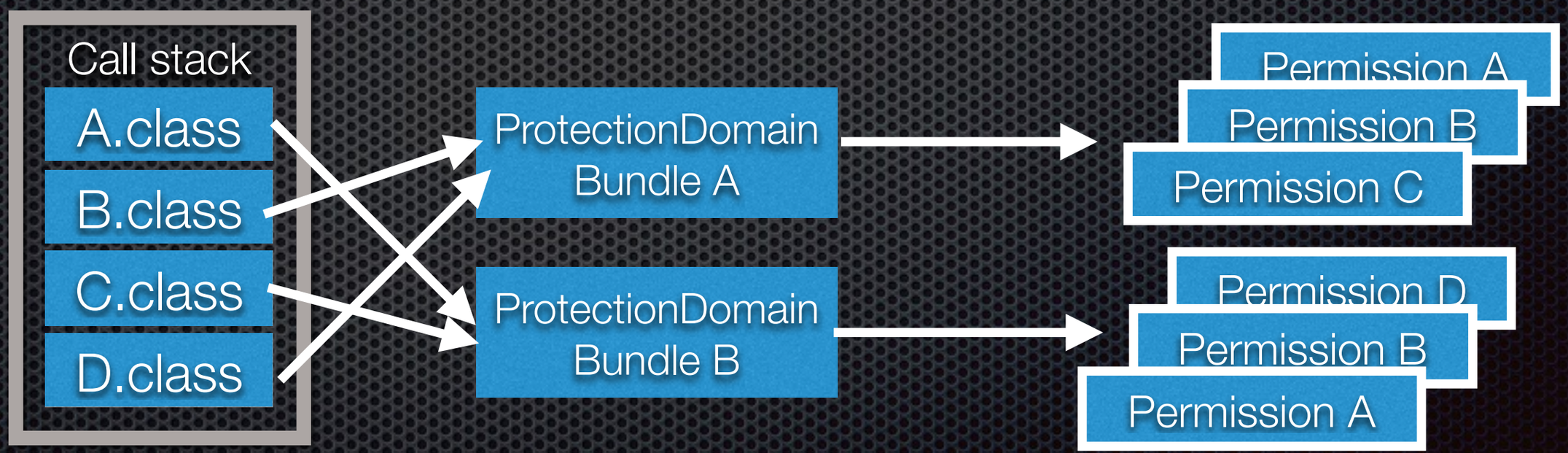
Implementation plan

(3) API-level Permission-based Access Control

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

+ Bundle local permission

- Logical representation of each type of network operation to be granted
- multiple APIs performing a similar network operation are mapped to one permission
- OSGi bundle protection domain [2]



Reference:
[2] Hall, Richard, et al. OSGi in action: Creating modular applications in Java. Manning Publications Co., 2011.

The app permissions: example usage

- **Reactive forwarding application (onos-app-fwd)**
  - Receive PACKET_IN events `PACKET_EVENT`
  - Check if the destination host is known `HOST_READ`
    - if unknown
      - flood via PACKET_OUT `PACKET_WRITE`
    - if known
      - find out the path `TOPOLOGY_READ`
      - install flow rules `FLOWRULE_WRITE`

ONOS app permissions
Version 0.1

Permission type	Description	Associated services
APP_INFORMATION	Allows an app to read application information	Application Service
APP_EVENT	Allows an app to receive application lifecycle events	Application Service
CLUSTER_WRITE	Allows an app to modify the cluster (e.g. add/remove ONOS node)	Leadership Service
CLUSTER_READ	Allows an app to read cluster information	Cluster Service Leadership Service
CLUSTER_EVENT	Allows an app to receive cluster events	Cluster Service Leadership Service
MASTERSHIP_WRITE	Allows an app to modify mastership role of the devices	Mastership Service
MASTERSHIP_READ	Allows an app to read various mastership information	Mastership Service
MASTERSHIP_EVENT	Allows an app to get notified of mastership events	Mastership Service
DEVICE_WRITE	Allows an app to modify devices	Device Service
DEVICE_READ	Allows an app to read device information	Device Service Device Clock Service
DEVICE_EVENT	Allows an app receive device events	Device Service
FLOWRULE_WRITE	Allows an app to add/remove flow rules	Flow Rule Service
FLOWRULE_READ	Allows an app to read flow rule information	Flow Rule Service
FLOWRULE_EVENT	Allows an app to receive flow rule events	Flow Rule Service
HOST_WRITE	Allows an app to modify host	Host Service
HOST_READ	Allows an app to read host information	Host Service Host Clock Service
HOST_EVENT	Allows an app receive host events	Host Service

DRAFT: subject to change

ONOS app permissions
Version 0.1

Permission type	Description	Associated services
INTENT_WRITE	Allows an app to issue/remove intents	Intent Service
		Intent Batch Service
INTENT_READ	Allows an app to read intent information	Intent Service
		Intent Batch Service
INTENT_EVENT	Allows an app to receive intent events	Intent Service
		Intent Batch Service
INTENT_EXTENSION	Allows an app to extend intent service	Intent Extension Service
LINK_READ	Allows an app to read link information	Link Service
LINK_EVENT	Allows an app to receive link events	Link Service
PACKET_WRITE	Allows an app to send/block packet	Packet Context
		Packet Service
PACKET_READ	Allows an app to read packet information	Packet Context
		Packet Service
PACKET_EVENT	Allows an app to handle packet events	Packet Service
STATISTIC_READ	Allows an app to access flow statistic information	Statistic Service
TOPOLOGY_READ	Allows an app to read path and topology information	PathService
		TopologyService
TOPOLOGY_EVENT	Allows an app to handle topology events	TopologyService
DATABASE_WRITE	Allows an app to modify database	Database Service
DATABASE_READ	Allows an app to read information from the database	Database Service

DRAFT: subject to change

Agenda

- Improve the permission model (~Feb.)
- Blackbird release (End of Feb.)
- Security-mode ONOS development (March ~ May)
  - Code contribution: either directly to the master or a dedicated branch
- Security-mode ONOS in Cardinal release (End of May.)

Thank you!

ON.LAB SRI International KAIST