Security-Mode ONOS

Changhoon Yoon

KAIST
Security-Mode ONOS?

1) Application layer access control
   • A network application permission-enforce model for managing distributed ONOS applications

2) Application auditing
   • Provide operators with explicit insight and control over the ONOS core services and APIs used by each ONOS application
Motivation

• Powerful authority granted to ONOS applications
  - Direct network manipulation
  - Data exfiltration (IP theft)
  - Denial of service
  - anything is possible!

• Applications cannot be trusted
  - Third-party applications (from untrusted source) may contain malicious/buggy code
Motivating examples

• System command execution – Denial of Service

(1) System.exit(0)
Motivating examples

- Southbound API access

ONOS node 1
ONOS node 2
ONOS node N

Applications
Northbound API
Distributed Core
Southbound API
Providers
Protocols

Global Network View

(1) sw1 disconnected

sw1
sw2
sw3
Motivating examples

- Persistent switch disconnection event generation

Inconsistent global network view
Motivating examples

- Administrative API access
Motivating examples

• Host and device removal
Permission Model

1) Bundle-level role-based access control
   - If a bundle is an application bundle,
     ONLY grant least permissions required (least-privileged)
     (e.g., system command execution, Southbound API access are restricted)

2) Application-level role-based access control
   - If application has ‘USER’ role,
     Administrative NB API access is restricted

3) API-level permission-based access control
   - An application can access a NB API,
     ONLY IF it has the required permission
Security Policy File

Provides a clear view of application intrinsic
Security-Mode ONOS (SM-ONOS)

• The BIG picture
Secure application activation

• In **Security-Mode**, an ONOS operator MUST…
  1) review application security policy
  2) agree and accept security policy
      … prior to activating an application

• Upon the policy acceptance, policy is *immediately*
enforced to the application bundles

• ONOS operator should be able to go through the secure
  app activation process ANYWHERE in the cluster!
Secure application activation

- Extend existing application state machine

![Application State Machine (in ONOS)](image)

- An application can only be activated, if ‘Security State’ of the application is ‘SECURED’

![Application State Machine (in Security-Mode ONOS)](image)
Security State of Application

- SM-ONOS maintains Security State of each application (via Strongly consistent / RAFT-based consistent store)

- **Security States**
  - **INSTALLED**: Application has been installed
  - **REVIEWED**: Security policy has been reviewed by ONOS operator
  - **SECURED**: Security policy has been accepted and enforced
  - **POLICY_VIOLATED**: Application has violated security policy
Distributed security policy enforcement

• Application subsystem enables ‘Cluster-wide’ application installation/activation

• Application security policy **MUST be consistently** enforced to distributed applications!

• **How?**
  - Consistent distributed store
Distributed security policy enforcement

- Security policy and state information
  - synchronized using strongly consistent store
- Security policy violation events
  - synchronized using eventually consistent store
Application security policy enforcement

• How to locally enforce security policy?
  - Leverage both Java and OSGi security framework
Summary

• New application layer access control
• Secure application activation mechanism
• Distributed application security policy enforcement
Thank You
“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