CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Queen's University Belfast

# SDN Security

## COINS Summer School

Dr. Sandra Scott-Hayward

23 August 2015

@CSIT_QUB

# Controller Security

# ONOS, OpenVirtex Questions

Are the application-controller transactions secured?
Are the controller-controller transactions secured?
How are application conflicts resolved?
How does a controller connect to the network?
How are applications/tenants isolated?
How are keys allocated, managed and where are they stored?
How are threats detected and handled?
Can the network state be identified at any point in time?
What information is stored for controller clustering and where?

# Problem Description

Increase in components and interfaces for the evolved SDN implementation increases the security challenges of the SDN controller design.

Objective:

- Identify requirements of a secure, robust, and resilient SDN controller;
- Analyse state-of-the-art open-source SDN controllers with respect to the security of their design;
- Provide recommendations for security improvements

# Definition of ‘Security’

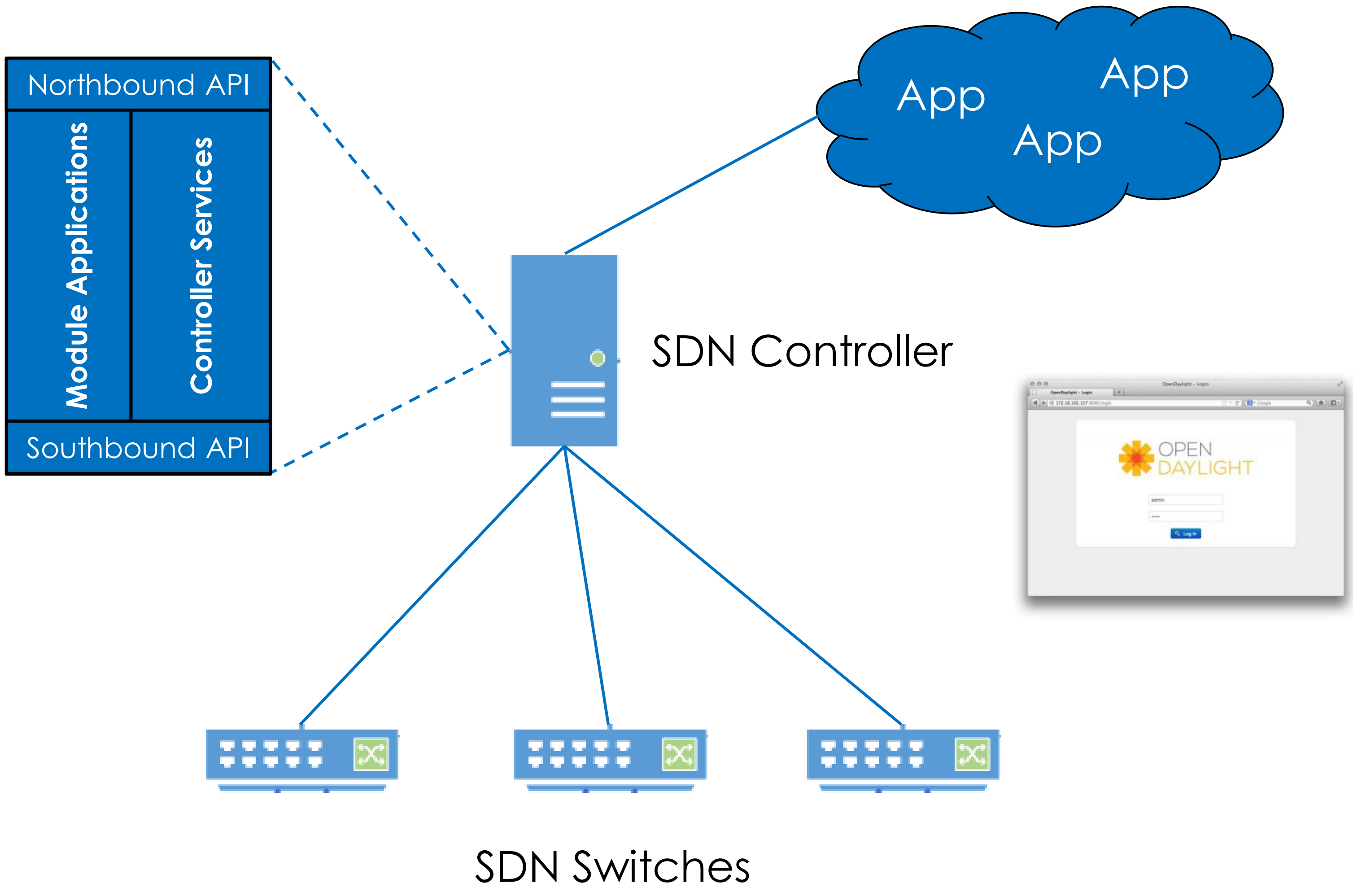
Secure, Robust and Resilient (referred to as ‘security’):

- The controller is designed to reduce the risk of intrusion/attack at the network control layer;
- The controller is able to withstand errors in control layer logic;
- The controller is able to recover quickly from disruption and maintain an acceptable level of service in the face of faults.

# Selected SDN Controllers

| Controller | Source | Version | Release | Architecture | Objective | Security Features |
|---|---|---|---|---|---|---|
| **ONOS** | ON.Lab | Avocet 1.0.0 | 2014 | Distributed | High-availability, Scale-out, Performance | Security-mode ONOS proposed for v2 |
| **OpenDaylight** | OpenDaylight Project | Helium (Karaf 0.2.0) | 2014 | Distributed | Enterprise-Grade Performance, High Availability | AAA Service, Foundation of Security Group |
| **ROSEMARY** | KAIST,<br>SRI International | - | 2014 | Centralized | Robust, secure, and high-performance NOS | Process Containment, Resource Usage Monitoring, App Permission Structure |
| **Ryu** | NTT | 3.13 | 2012 | Centralized, Multi-Threaded | High quality controller for production environments | Secure control layer communication |
| **SE-Floodlight** | SRI International | Beta 2 | 2013 | Centralized | Security-enhanced version of Floodlight controller | Security enforcement kernel (AAA) |

# Security Attributes

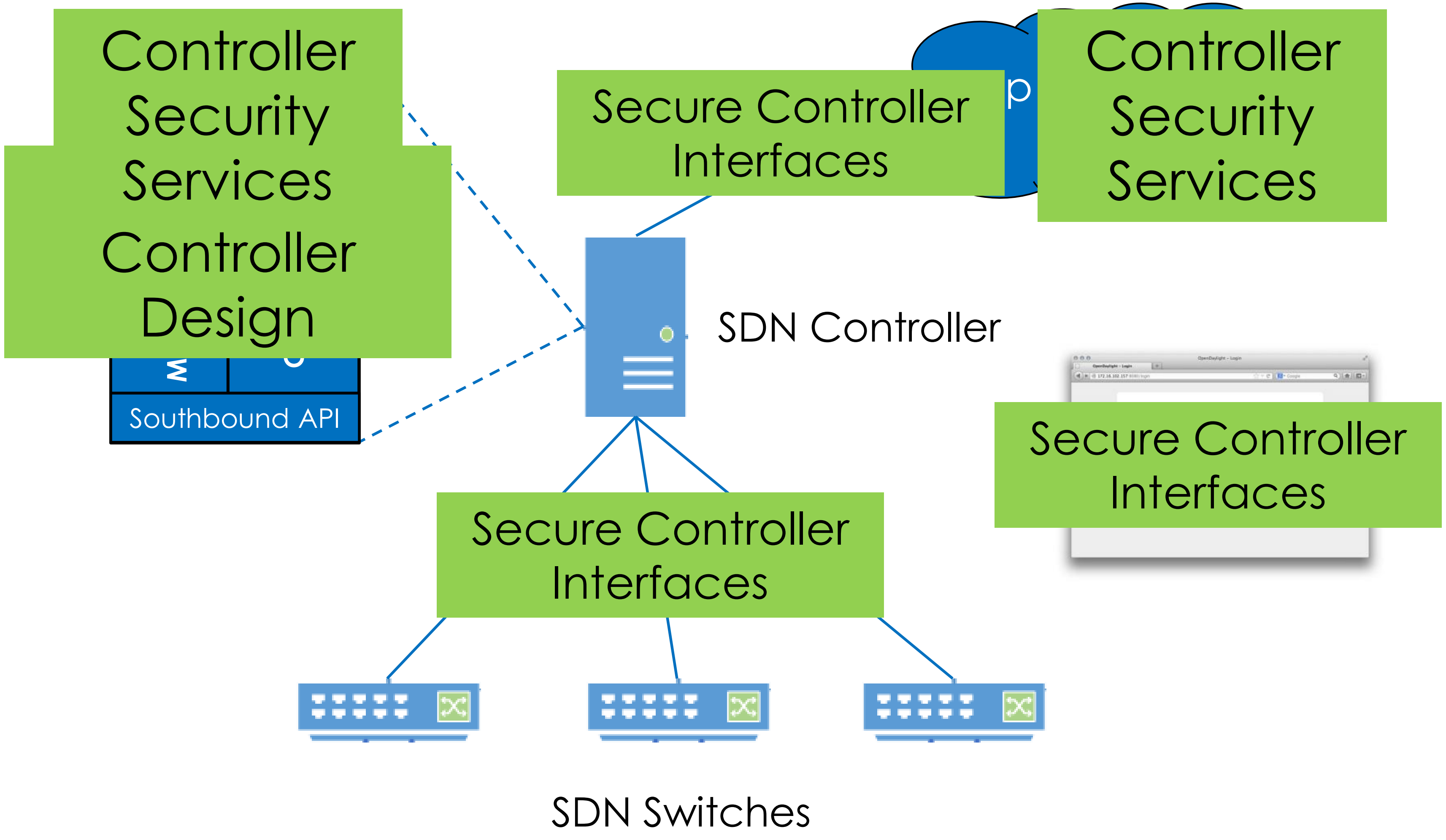


OpenDaylight - Login

172.16.102.157:8080/login

admin

# Security Attributes



Controller Security Services

Controller Design

Secure Controller Interfaces

Controller Security Services

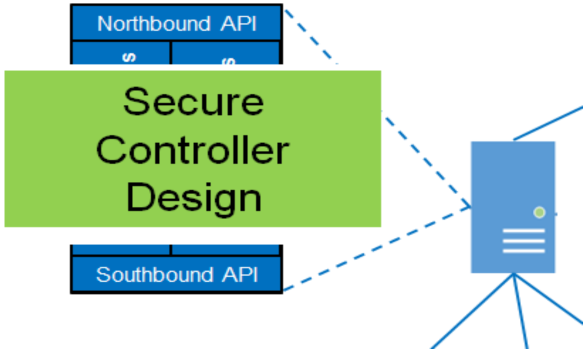
SDN Controller

Secure Controller Interfaces

Secure Controller Interfaces

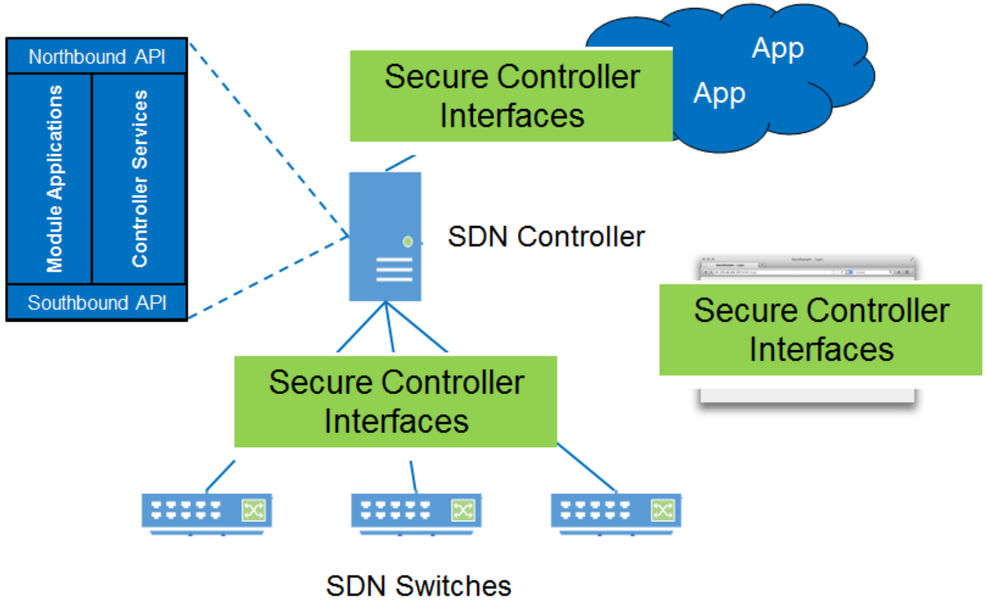
SDN Switches

# Secure Controller Design



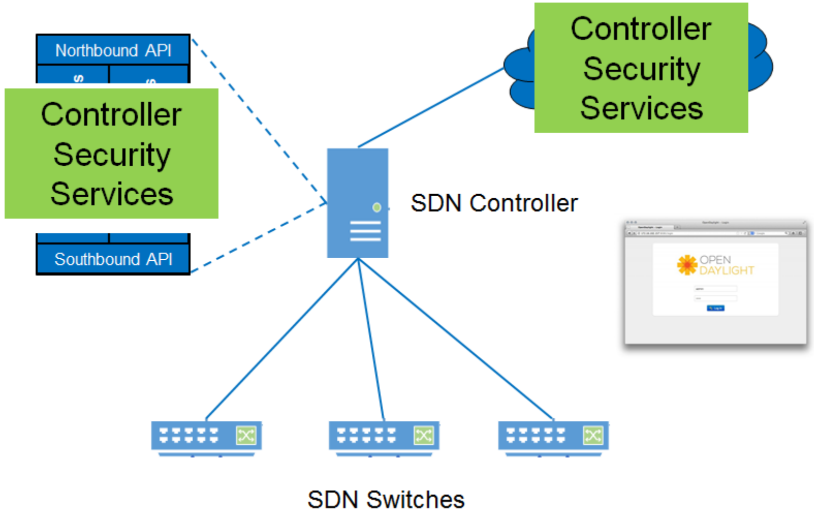
| Controller | ONOS | ODL | ROSEMARY | Ryu | SE-Floodlight |
|---|---|---|---|---|---|
| Control Process (Application) Isolation | ✘ | ✘ | ✓<br>(micro-NOS) | ✘ | ✓<br>(Privilege-Based) |
| Implementation of Policy Conflict Resolution | ✓<br>(Data-Store) | ✘ | ✘ | ✘ | ✓<br>(Algorithm) |
| Multiple Controller Instances – Resilience | ✓<br>(Clustering) | ✓<br>(Clustering) | ✘ | ✘ | ✘ |
| Multiple Application Instances – Resilience | ✘ | ✘ | ✘ | ✘ | ✘ |
| Secure Storage | ✓ | ✓ | ✓ | ✓ | ✓ |

# Secure Controller Interfaces



| Controller | ONOS | ODL | ROSEMARY | Ryu | SE-Floodlight |
|---|---|---|---|---|---|
| Secure Control Layer Communication | ✗ | ✓<br>(D-CPI) | ✗ | ✓<br>(D-CPI) | ✓<br>(D-CPI, A-CPI) |
| GUI/REST API Security | ✗ | ✓<br>(weak) | n/a | ✗ | ✗ |

# Controller Security Services



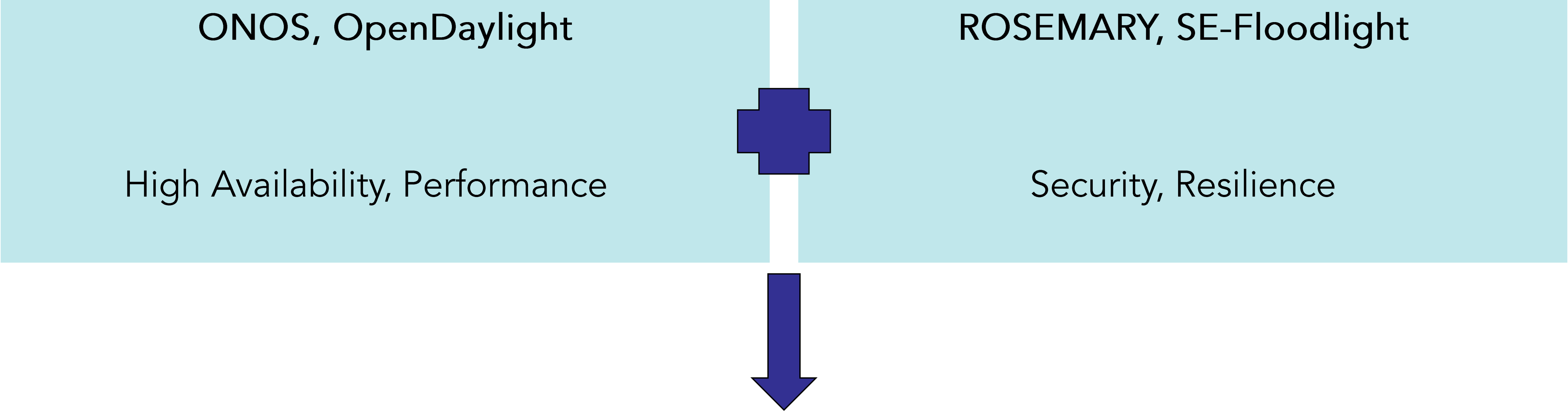
| Controller | ONOS | ODL | ROSEMARY | Ryu | SE-Floodlight |
|---|---|---|---|---|---|
| IDS/IPS Integration | ✗ | ✓<br>(Defense4All) | ✗ | ✓<br>(Snort) | ✓<br>(BotHunter, Sec. Actuator) |
| Authentication and Authorization | ✗ | ✓ | ✓ | ✗ | ✓ |
| Resource Monitoring | ✗ | ✗ | ✓ | ✗ | ✗ |
| Logging/Security Audit Service | ✓ | ✓ | ✓ | ✓ | ✓ |

# Recommendations

Recommendations for Future Security Improvements:

1. Design with Software Security Principles
2. Secure Default Controller Settings
3. Application Future-Proofing

# Conclusion



ONOS, OpenDaylight

High Availability, Performance

ROSEMARY, SE-Floodlight

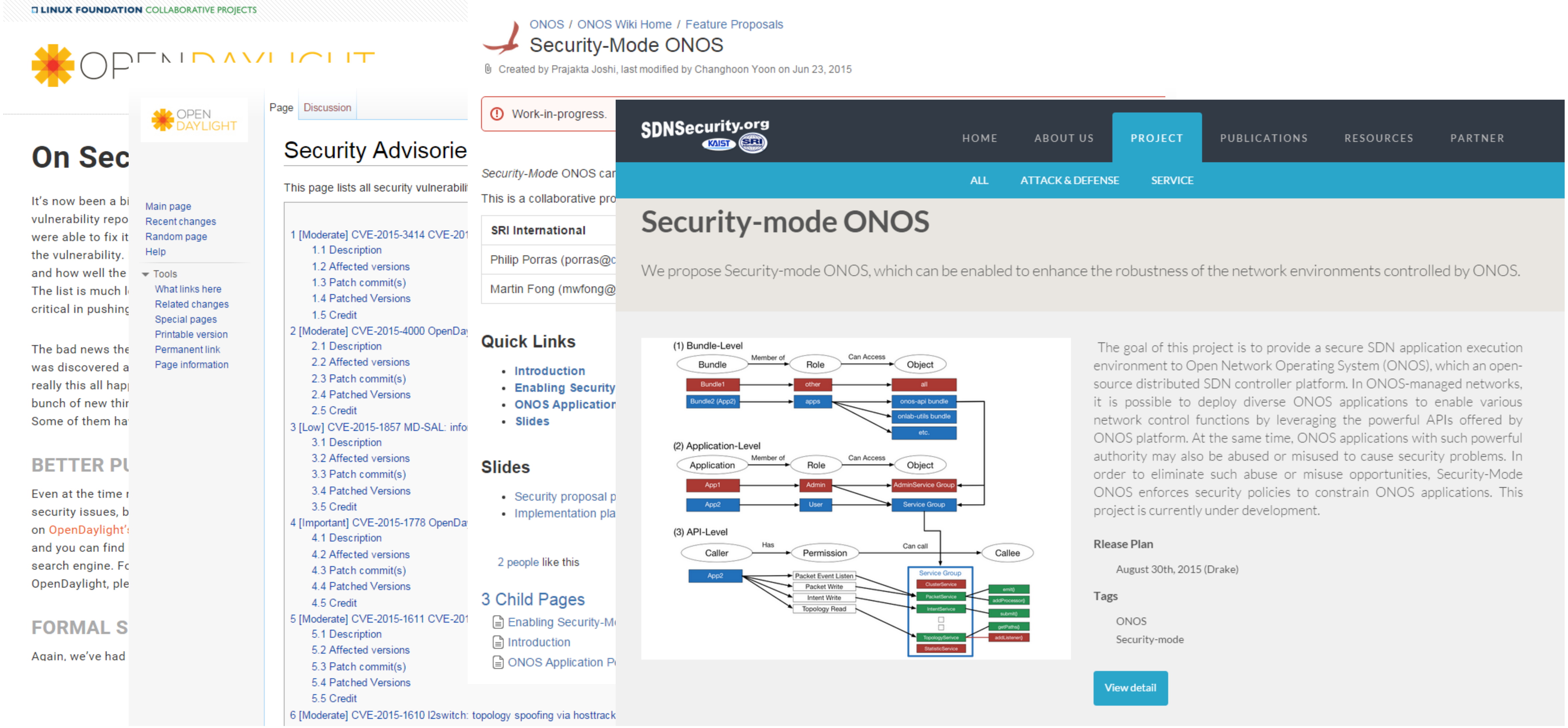
Security, Resilience

**Next Evolution in SDN Controller Design …**
**Security, Robustness, and Resilience**

# Controller Security Rating

## DEMO

# Controller Security Breaches/Developments



LINUX FOUNDATION COLLABORATIVE PROJECTS

OPENDAYLIGHT

On Sec

It's now been a bi
vulnerability repo
were able to fix it
the vulnerability.
and how well the
The list is much l
critical in pushing

The bad news the
was discovered a
really this all hap
bunch of new thir
Some of them ha

BETTER PU

Even at the time i
security issues, b
on OpenDaylight's
and you can find
search engine. Fo
OpenDaylight, ple

FORMAL S

Again, we've had

OPEN DAYLIGHT

Page | Discussion

Security Advisorie

This page lists all security vulnerabili

- Main page
- Recent changes
- Random page
- Help

Tools

- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information

1 [Moderate] CVE-2015-3414 CVE-201
 1.1 Description
 1.2 Affected versions
 1.3 Patch commit(s)
 1.4 Patched Versions
 1.5 Credit
2 [Moderate] CVE-2015-4000 OpenDay
 2.1 Description
 2.2 Affected versions
 2.3 Patch commit(s)
 2.4 Patched Versions
 2.5 Credit
3 [Low] CVE-2015-1857 MD-SAL: info
 3.1 Description
 3.2 Affected versions
 3.3 Patch commit(s)
 3.4 Patched Versions
 3.5 Credit
4 [Important] CVE-2015-1778 OpenDa
 4.1 Description
 4.2 Affected versions
 4.3 Patch commit(s)
 4.4 Patched Versions
 4.5 Credit
5 [Moderate] CVE-2015-1611 CVE-201
 5.1 Description
 5.2 Affected versions
 5.3 Patch commit(s)
 5.4 Patched Versions
 5.5 Credit
6 [Moderate] CVE-2015-1610 l2switch: topology spoofing via hosttrack

ONOS / ONOS Wiki Home / Feature Proposals

Security-Mode ONOS

Created by Prajakta Joshi, last modified by Changhoon Yoon on Jun 23, 2015

Work-in-progress.

*Security-Mode* ONOS car

This is a collaborative pro

| SRI International |
|---|
| Philip Porras (porras@c |
| Martin Fong (mwfong@ |

## Quick Links

- **Introduction**
- **Enabling Security**
- **ONOS Application**
- **Slides**

## Slides

- Security proposal p
- Implementation pla

2 people like this

## 3 Child Pages

- Enabling Security-M
- Introduction
- ONOS Application P

SDNSecurity.org KAIST SRI

HOME | ABOUT US | PROJECT | PUBLICATIONS | RESOURCES | PARTNER

ALL | ATTACK & DEFENSE | SERVICE

## Security-mode ONOS

We propose Security-mode ONOS, which can be enabled to enhance the robustness of the network environments controlled by ONOS.

The goal of this project is to provide a secure SDN application execution environment to Open Network Operating System (ONOS), which an open-source distributed SDN controller platform. In ONOS-managed networks, it is possible to deploy diverse ONOS applications to enable various network control functions by leveraging the powerful APIs offered by ONOS platform. At the same time, ONOS applications with such powerful authority may also be abused or misused to cause security problems. In order to eliminate such abuse or misuse opportunities, Security-Mode ONOS enforces security policies to constrain ONOS applications. This project is currently under development.

**Rlease Plan**

August 30th, 2015 (Drake)

**Tags**

ONOS
Security-mode

View detail

# End Session 6