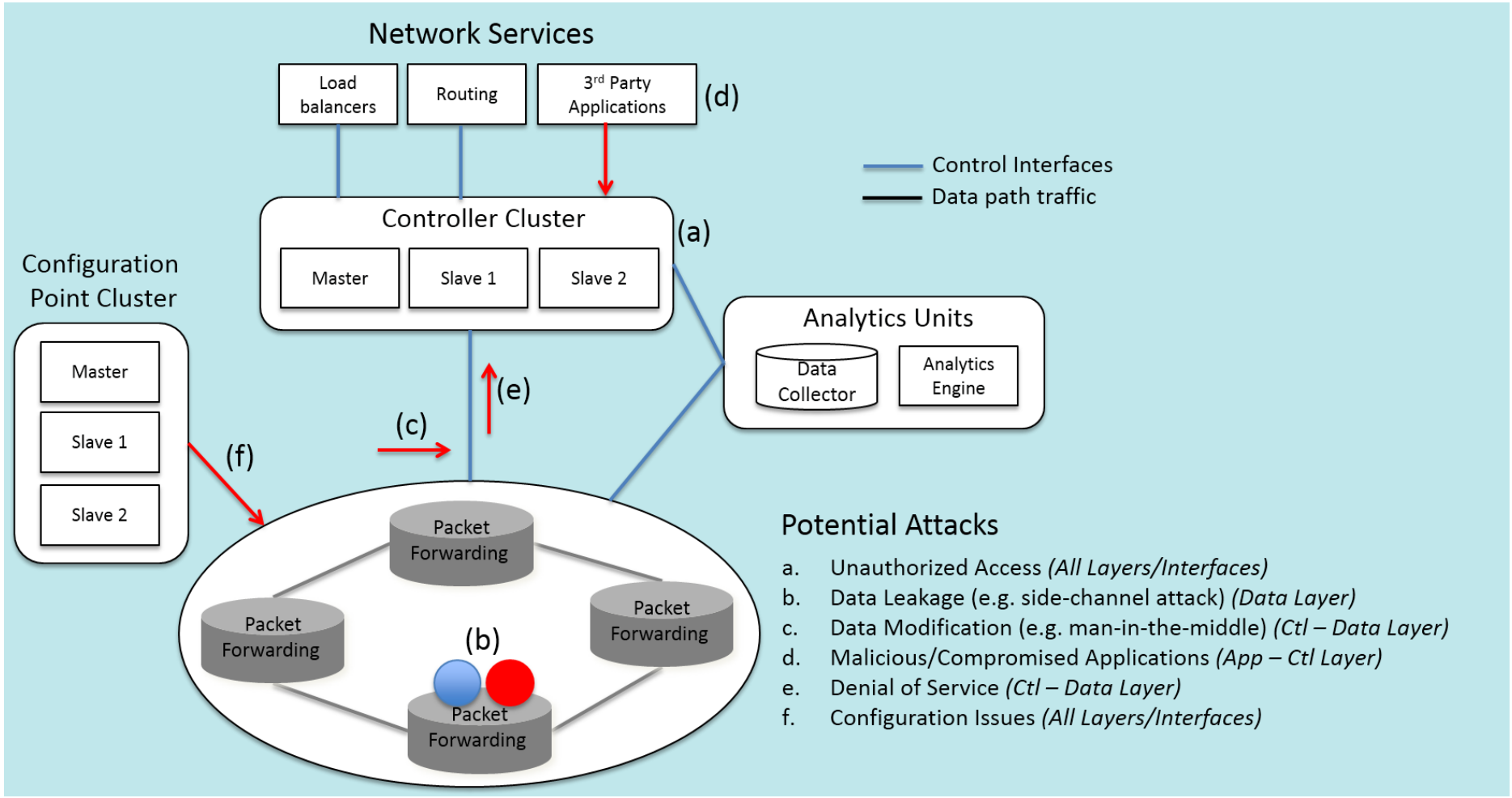

CSIT
CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES
TRAILING THE SNAIL:
SDN CONTROLLER
SECURITY EVOLUTION

SDN Overview



S. Scott-Hayward, S. Natarajan and S. Sezer, "A Survey of Security in Software Defined Networks," *IEEE Communications Surveys and Tutorials*, Vol. 18, No.1, pp.623-654, Jan. 2016

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Some controller security 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?

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Approach

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

Objectives:

- 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

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

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.

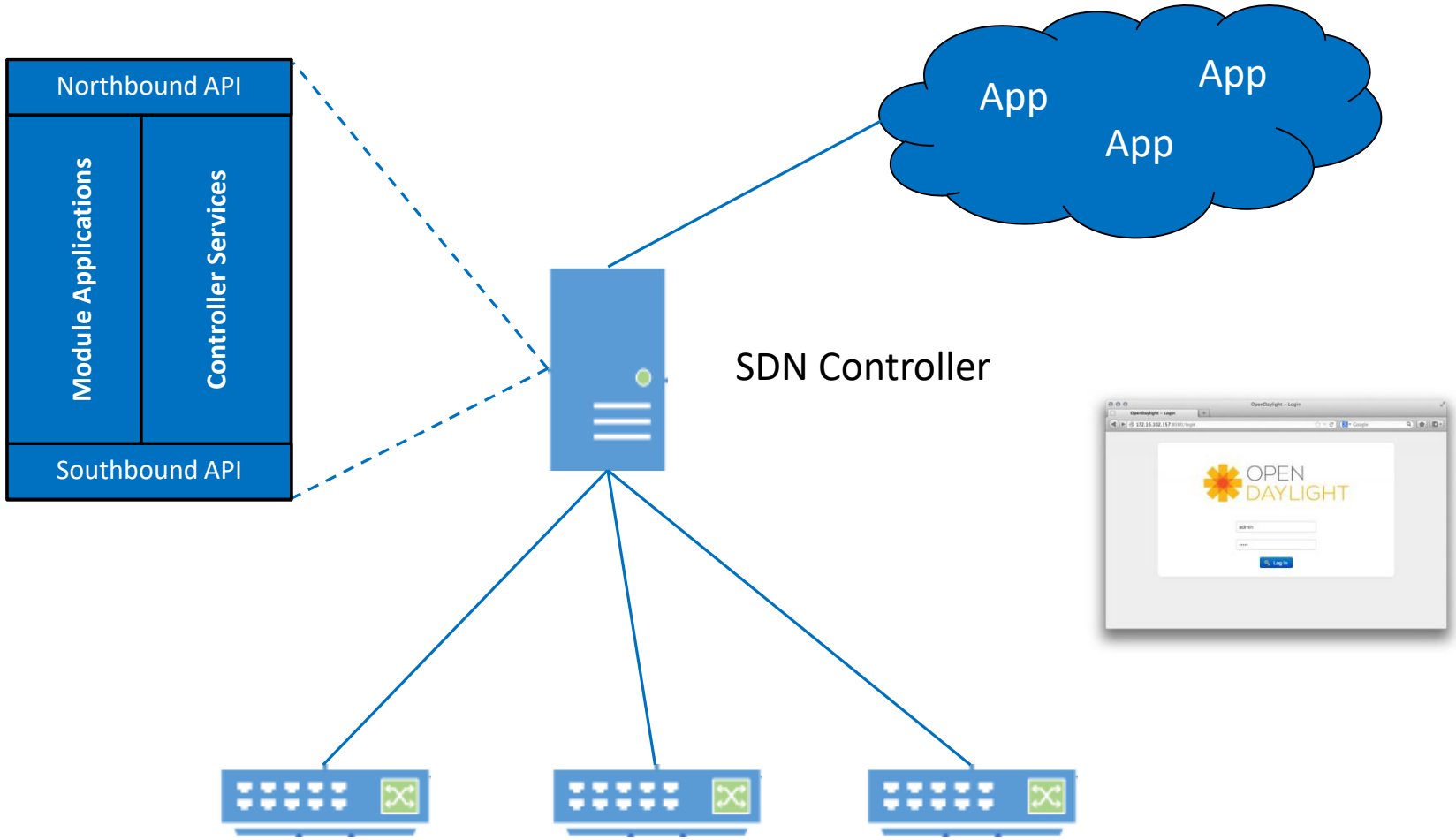
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

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, 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)

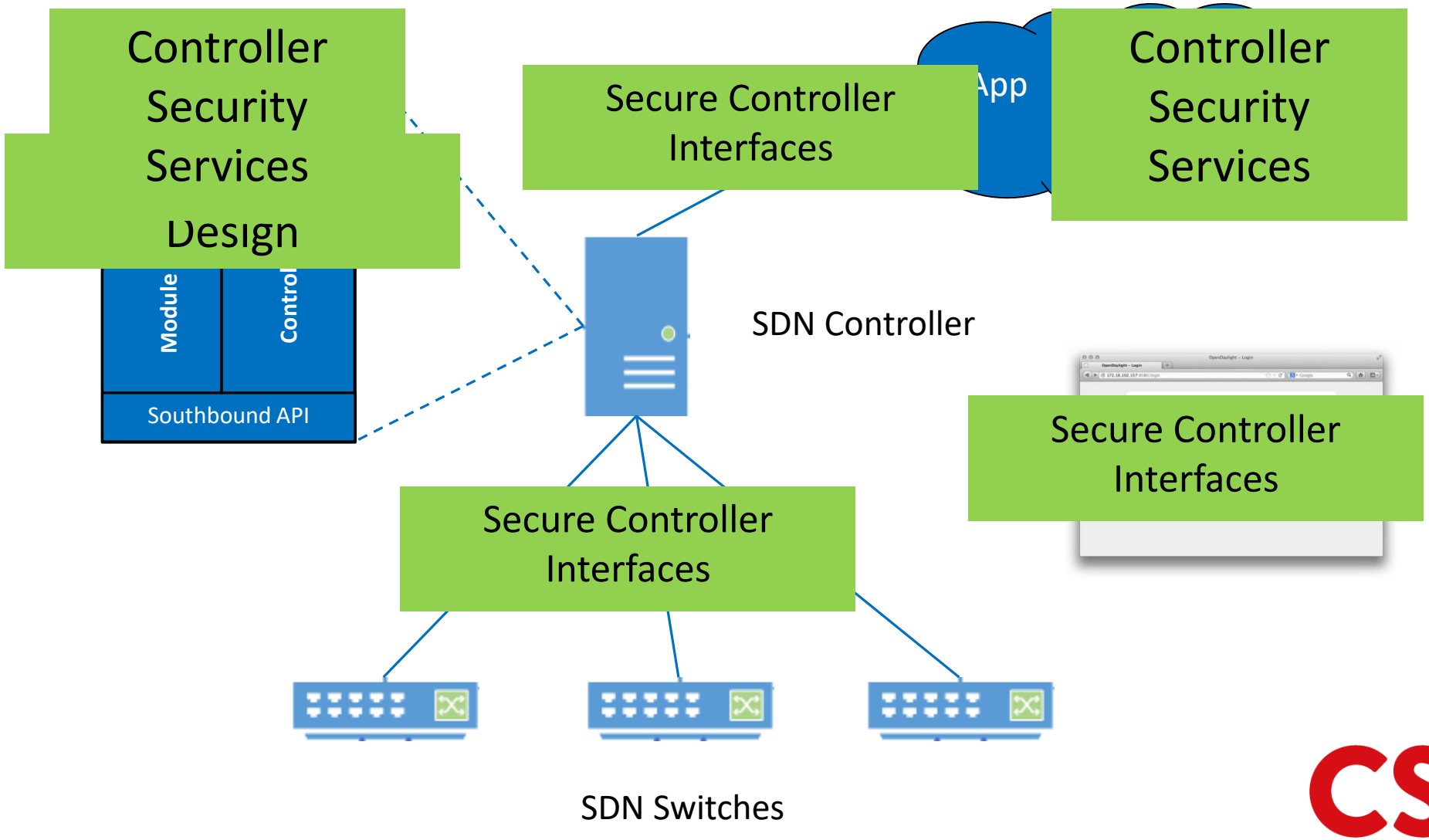
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Security Attributes



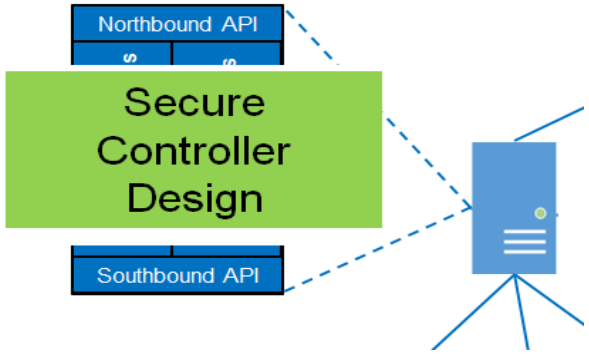
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Security Attributes



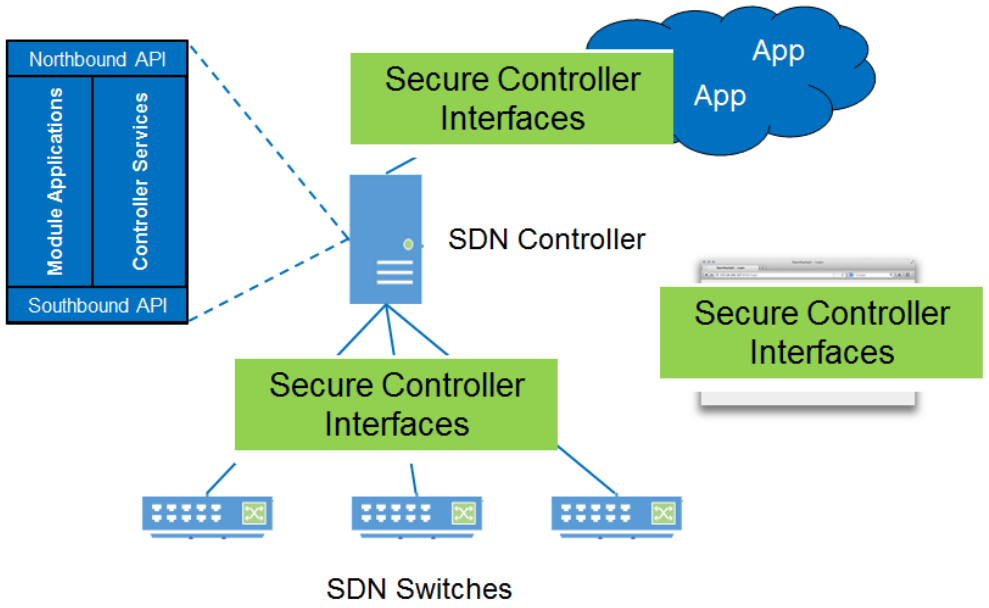
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Secure Controller Design



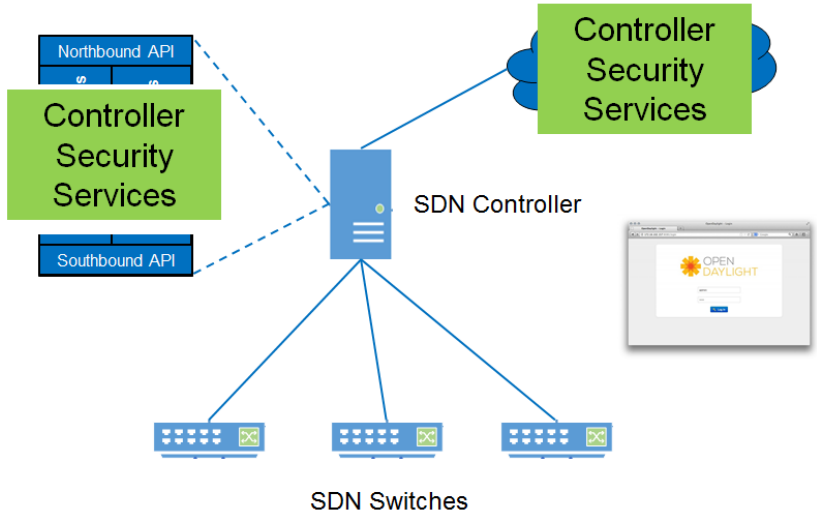
Controller	ONOS	ODL	ROSEMARY	Ryu	SE-Floodlight
Control Process (Application) Isolation	✗	✗	✓ (micro-NOS)	✗	✓ (Privilege-Based)
Implementation of Policy Conflict Resolution	✓ (Data-Store)	✗	✗	✗	✓ (Algorithm)
Multiple Controller Instances – Resilience	✓ (Clustering)	✓ (Clustering)	✗	✗	✗
Multiple Application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

Secure Controller Interfaces



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

Controller Security Services



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

Recommendations

Recommendations for Future Security Improvements:

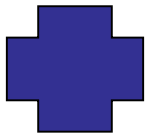
1. Design with Software Security Principles
2. Secure Default Controller Settings
3. Application Future-Proofing

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Conclusion

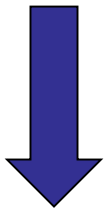
ONOS, OpenDaylight

High Availability, Performance



ROSEMARY, SE-Floodlight

Security, Resilience



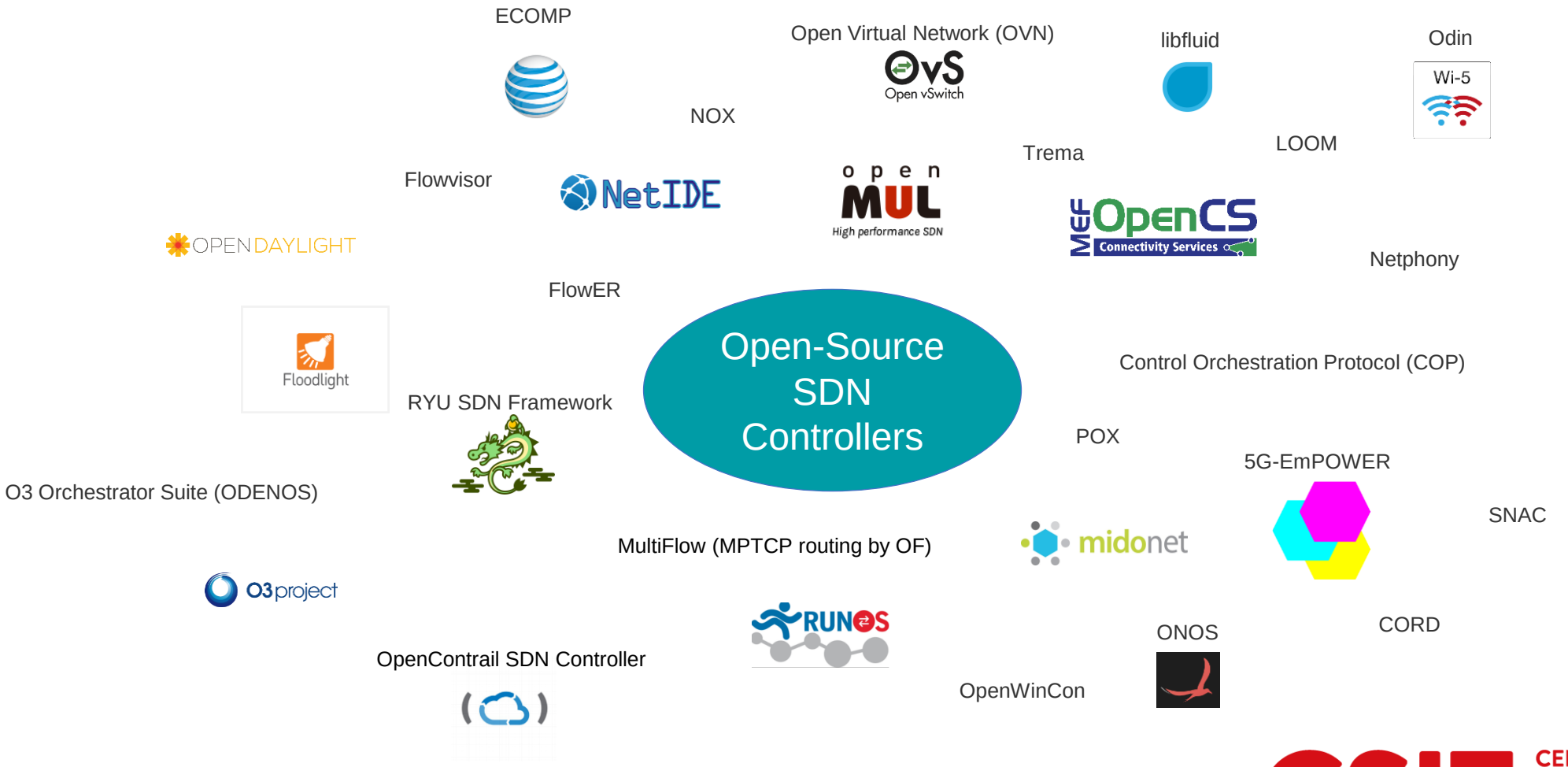
Next Evolution in SDN Controller Design …
Security, Robustness, and Resilience

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Fast-forward to 2018 …

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Open-source SDN Controllers



Source: https://wiki.sdn.ieee.org/display/sdn/SDN+Controllers+Catalogue

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

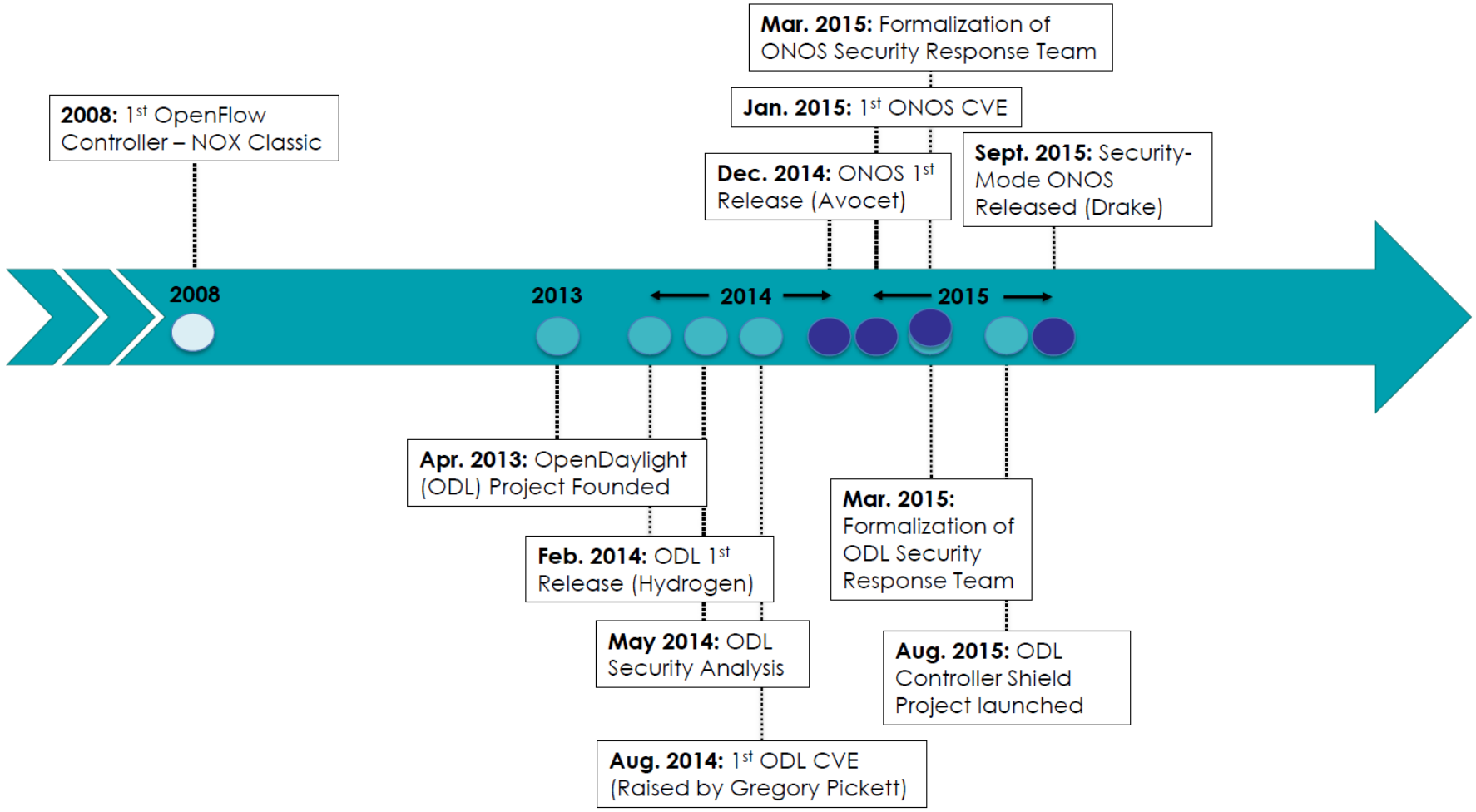
ONOS

Open Network Operating System

OPENDAYLIGHT

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

ODL and ONOS Security-related events



CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

CSIT
CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES

ONOS – Security Support

@ November 2017

Security

Created by David Jorm, last modified by Luca Prete on May 12, 2016

Reporting security issues

Please report any security issues you find in ONOS to: **security@onosproject.org**

Anyone can post to this list. The subscribers are only trusted individuals who will handle the resolution of any reported security issues in confidence. details of any embargo you would like to impose.

ONOS Security Response Team

Security Response Expert (s): David Jorm

Technical team: Technical Steering Team (Thomas Vachuska, Madan Jampani, Ali Al-Shabibi, Brian O'Connor, Jonathan Hart)

Test team: Suibin Zhang

ON.Lab: Bill Snow, Luca Prete

Security advisories

The security advisories page lists all security vulnerabilities fixed in ONOS.

Back to security advisories main page

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

ONOS – Security Support – Recent Activity

Security

Created by David Jorm, last modified by Thomas Vachuska on Mar 28, 2018

Reporting security issues

Please report any security issues you find in ONOS to: **security@onosproject.org**

Anyone can post to this list. The subscribers are only trusted individuals who will handle the resolution of any reported security issues in confidence. In your report, please note how you would like to be credited for discovering the issue and the details of any embargo you would like to impose.

ONOS Security Response Team

Security Response Expert (s): David Jorm

Technical team: Technical Steering Team (Thomas Vachuska, Brian O'Connor, Jonathan Hart, David Bainbridge, Jordan Halterman, Andrea Campanella, Yuta Higuchi)

Test team: Suchitra Vemuri

ONF: Bill Snow, Luca Prete

Security advisories

The security advisories page lists all security vulnerabilities fixed in ONOS.

Back to security advisories main page

2015 – 2 CVEs
2017 – 4 CVEs

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

ONOS – Projects/Applications

Project/Application	Proposal Date	Estimated Maturity
Security-Mode ONOS	Jan. 2015	Medium
Access Control based on DHCP	Jul. 2016	N/A
ACL	Jul. 2015	Low
AAA	Sept. 2015	Low

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

ONOS – Security-focused design

Version	Release Date	Security Features
Avocet (v1.0)	Dec. 2014	High Availability
Blackbird (v1.1)	Feb. 2015	
Cardinal (v1.2)	May 2015	
Drake (v1.3)	Sept. 2015	GUI and CLI require username and password login; REST interfaces require username and password; TLS support for inter-node communication; Configurable HTTPS for GUI and REST API; Security-Mode ONOS for application security
Emu (v1.4)	Dec. 2015	
Falcon (v1.5)	Mar. 2016	*[Automatic application security policy extraction using static analysis techniques (KAIST)];* SecurityGroup feature of OpenStack
Goldeneye (v1.6)	May 2016	
Hummingbird (v1.7)	Sept. 2016	*[New subsystem for anomaly detection (ATHENA) (SRI)];* Rate limit on port via NetConf (GEANT)
Ibis (v1.8)	Nov. 2016	
Junco (v1.9)	Feb. 2017	Implemented unit test for Security-Mode ONOS, Integrated Security (DELTA) tests into OnosSystemTest
Kingfisher(v1.10)	Jun. 2017	Added support of security group to Openstack/networking-onos and SONA
Loon (v1.11)	Sept. 2017	Enable TLS by default for intra-cluster communication
Magpie (v1.12)	Dec. 2017	
Nightingale (v1.13)	May 2018	

OPENDAYLIGHT

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

ODL – Security Support

Security:Main

Contents

[hide]

- 1 Reporting security issues
- 2 Security Response Team
  - 2.1 Current Members
  - 2.2 Audit Log of Changes
- 3 Security advisories
- 4 Secure engineering
- 5 Other Documents

2014 – 2 CVEs
2015 – 7 CVEs
2016 – 2 CVEs
2017 – 6 CVEs

Reporting security issues

Please report any security issues you find in OpenDaylight to: security@lists.opendaylight.org

Anyone can post to this list. The subscribers are only trusted individuals who will handle the resolution of any reported se
report, please note how you would like to be credited for discovering the issue and the details of any embargo you would

The OpenDaylight vulnerability management process is documented here.

Security Response Team

Current Members

- Robert Varga
- David Jorm
- Kurt Seifried
- Ryan Goudling
- Lori Jakab
- Stephen Kitt

They can be reached at the above private security mailing list.

Security:Advisories

This page lists all security vulnerabilities fixed in OpenDaylight. Each vulnerability is assigned a security impact rating on a four-point scale (low, moderate, important and critical). The versions that are affected by each vulnerability are also listed.

Contents

[hide]

- 1 [Moderate] CVE-2017-1000406 Password change doesn't result in Karaf clearing cache, allowing old password to still be used
  - 1.1 Description
  - 1.2 Affected versions
  - 1.3 Patch commit(s)
  - 1.4 Mitigations
  - 1.5 Credit
- 2 [Moderate] CVE-2017-1000357 Denial of Service attack when the switch rejects to receive packets from the controller
  - 2.1 Description
  - 2.2 Affected versions
  - 2.3 Patch commit(s)
  - 2.4 Mitigations
  - 2.5 Credit
- 3 [Moderate] CVE-2017-1000358 Controller throws an exception and does not allow user to add subsequent flow for a particular switch
  - 3.1 Description
  - 3.2 Affected versions
  - 3.3 Patch commit(s)
  - 3.4 Mitigations
  - 3.5 Credit
- 4 [Low] CVE-2017-1000359 Java out of memory error and significant increase in resource consumption
  - 4.1 Description
  - 4.2 Affected versions
  - 4.3 Patch commit(s)
  - 4.4 Mitigations
  - 4.5 Credit
- 5 [Low] CVE-2017-1000360 StreamCorruptedException and NullPointerException in OpenDaylight odl-mdsal-xsql
  - 5.1 Description
  - 5.2 Affected versions
  - 5.3 Patch commit(s)
  - 5.4 Mitigations
  - 5.5 Credit
- 6 [Moderate] CVE-2017-1000361 DOMRpcImplementationNotAvailableException when sending Port-Status packets to OpenDaylight
  - 6.1 Description
  - 6.2 Affected versions

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

ODL Security Support – Recent Activity

Reporting security issues

Please report any security issues you find in OpenDaylight to: security@lists.opendaylight.org

Anyone can post to this list. The subscribers are only trusted individuals who will handle the resolution of any reported security issues in confidence. In your report, please note how you would like to be credited for discovering the issue and the details of any embargo you would like to impose.

The OpenDaylight vulnerability management process is documented here.

Security Response Team

- Luke Hinds (Security Manager)
- Robert Varga
- Kurt Seifried
- Ryan Goudling
- Lori Jakab
- Stephen Kitt

Security advisories

The security advisories page lists all security vulnerabilities fixed in OpenDaylight.

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Summary of ODL Security Features, May 2014

Security Feature	Comment	Recommendation
Application Bundle Security	Bundles provide some level of isolation	Augment with bundle signature/permission verifiers at loadtime, bundle access security at runtime; Bundle authentication/authorization should be logged
OSGi Runtime Container Security - ODL Apache Karaf Distribution	Concerns with security footprint of Karaf	Make Karaf security documentation available to ODL developers and administrators
ODL Controller Plugins Security	Secure communication access to the controller; 5/13 plugins use secure versions of protocol	Provide secure access for 8 plugins, DDoS attack protection on plugin exposed ports, use a common crypto key storage, and support pluggable/built-in CA
AAA for External Users	Supports secure access via NB API	Provide role-based access control for external users, user access authentication, access protocol authorization, services/resource authorization, auditing access/authorization pluggable AAA service
Secure Device/Controller BootStrap Authentication and Authorization	Controller/Device Discovery is manual	Zero-touch bootstrap requirements - automatic device discovery and AAA support
Controller Clustering and Security	Clustering comms channel should be secure	Configure Jgroups AUTH and ENCRYPT support for security

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

ODL – Projects/Applications

Project	Proposal Date	Estimated Maturity
Defense4All	Aug. 2013	Medium
Secure Network Bootstrapping Interface	May 2014	High
AAA	Jun. 2014	High
Unified Secure Channel	Dec. 2014	High
Controller Shield	Aug. 2015	Low
Cardinal – ODL Monitoring as a Service	Mar. 2016	High

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

ODL – Security-focused design

Version	Release Date	Security Features
Hydrogen	Feb. 2014	Defense4All DDoS attack detection and mitigation tool
Helium	Sept. 2014	
Lithium	Jun. 2015	**New features for security and automation:** *Unified Secure Channel* eases secure communication between ODL and widely distributed networking equipment; *Time Series Data Repository (TSDR)* enables collection and analysis of large amounts of network activity; *Device Identification and Driver Management (DIDM)* provides end users the ability to discover, manage and automate a wide range of existing hardware in their infrastructure; *Persistence* ensures application-specific data is preserved over time or in the event of a catastrophe; *Topology Processing Framework* allows for filtered and/or aggregated views of a network, including multi-protocol, underlay/overlay
Beryllium	Feb. 2016	**New features for performance and scalability:** Stronger analysis and testing of clustering, applications that want to be cluster-aware can choose how to put data across the cluster; Fully support OpenStack High Availability and Clustering
Boron	Sept. 2016	*NetVirt project* enhanced support in OpenStack environments for IPv6, Security Groups (via OpenFlow configuration) and VLANs. *Cardinal* project monitors the health of the controller, delivered as a service to existing, deployed network monitoring and analytics tools. *Centinel* analytics engine enables end-to-end data collection and machine learning to support performance monitoring and bandwidth management across WAN links.
Carbon	May 2017	*NetVirt and Genius projects* integrate to dynamically create and manage tunnels and virtual network functions on demand.
Nitrogen	Sept. 2017	AAA bug fixes;
Oxygen	Mar. 2018	AAA bug fixes; USC bug fixes; Release notes highlight security considerations for each project

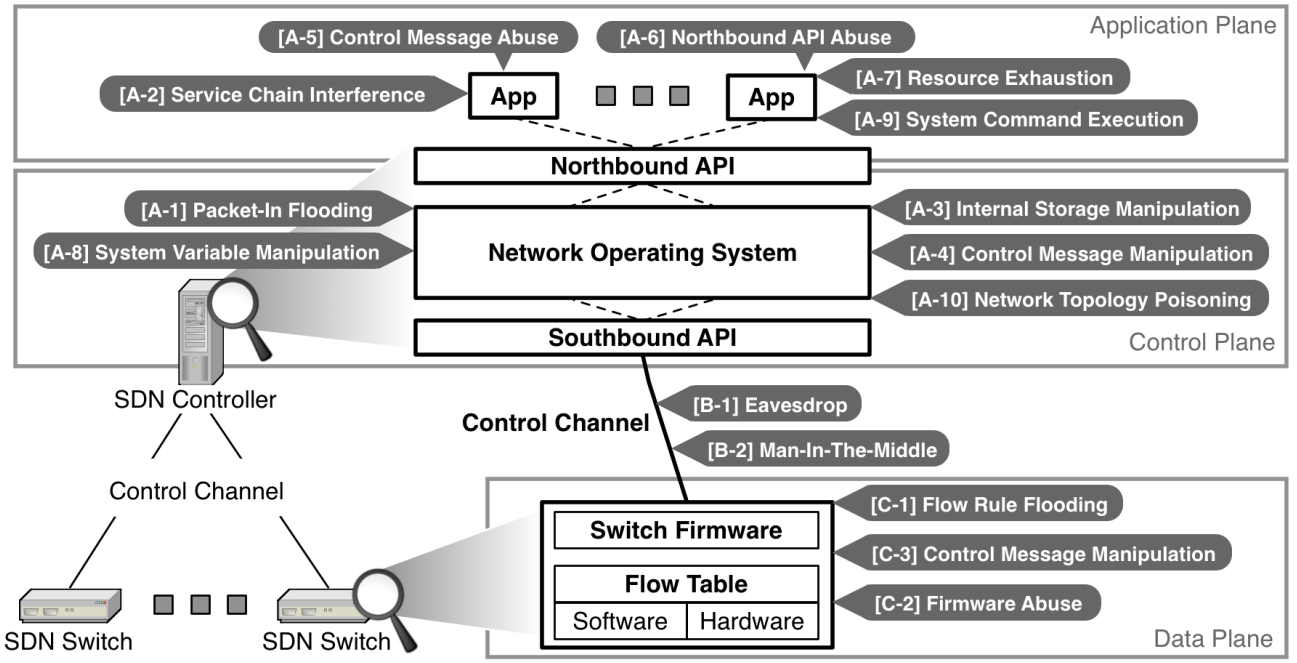
CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Delta - Motivation

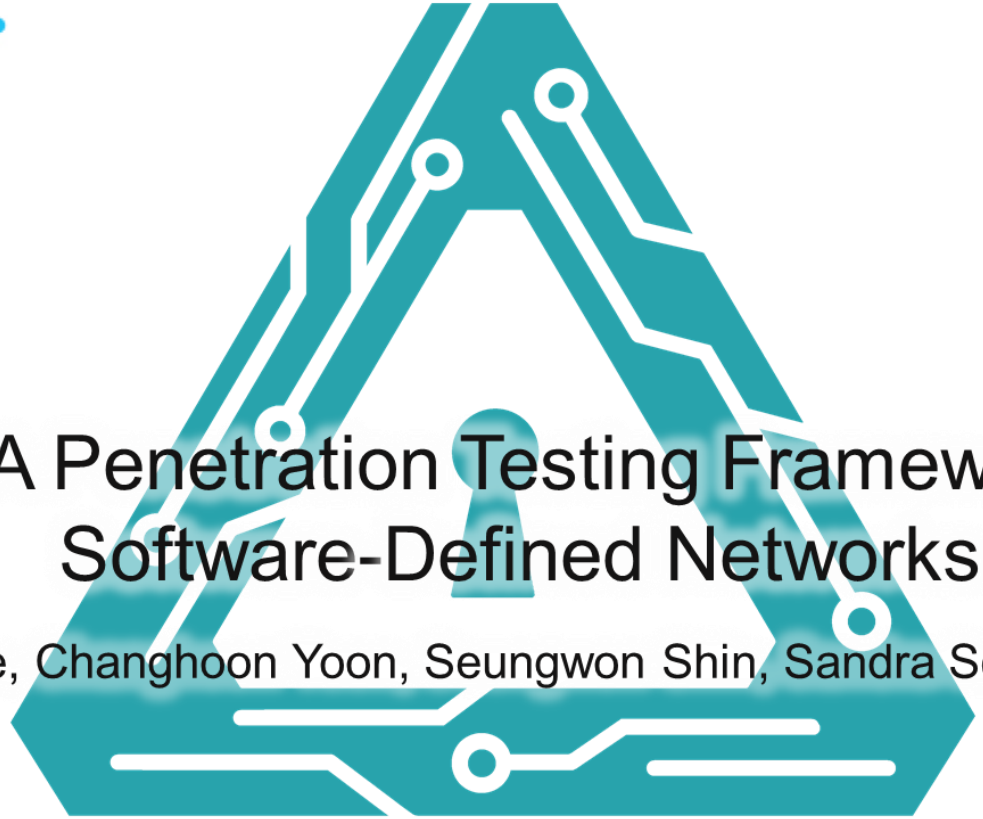
Why? Motivated by the potential security vulnerabilities in SDNs

What? Aim to simplify the detection of security issues in SDNs and **promote secure design, development and deployment of SDNs**

How? Test the security issues of both the OpenFlow protocol and SDN components (control/data plane and channel)



NS2 Network and System Security Laboratory KAIST CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES



Delta: A Penetration Testing Framework for Software-Defined Networks

Seungsoo Lee, Changhoon Yoon, Seungwon Shin, Sandra Scott-Hayward

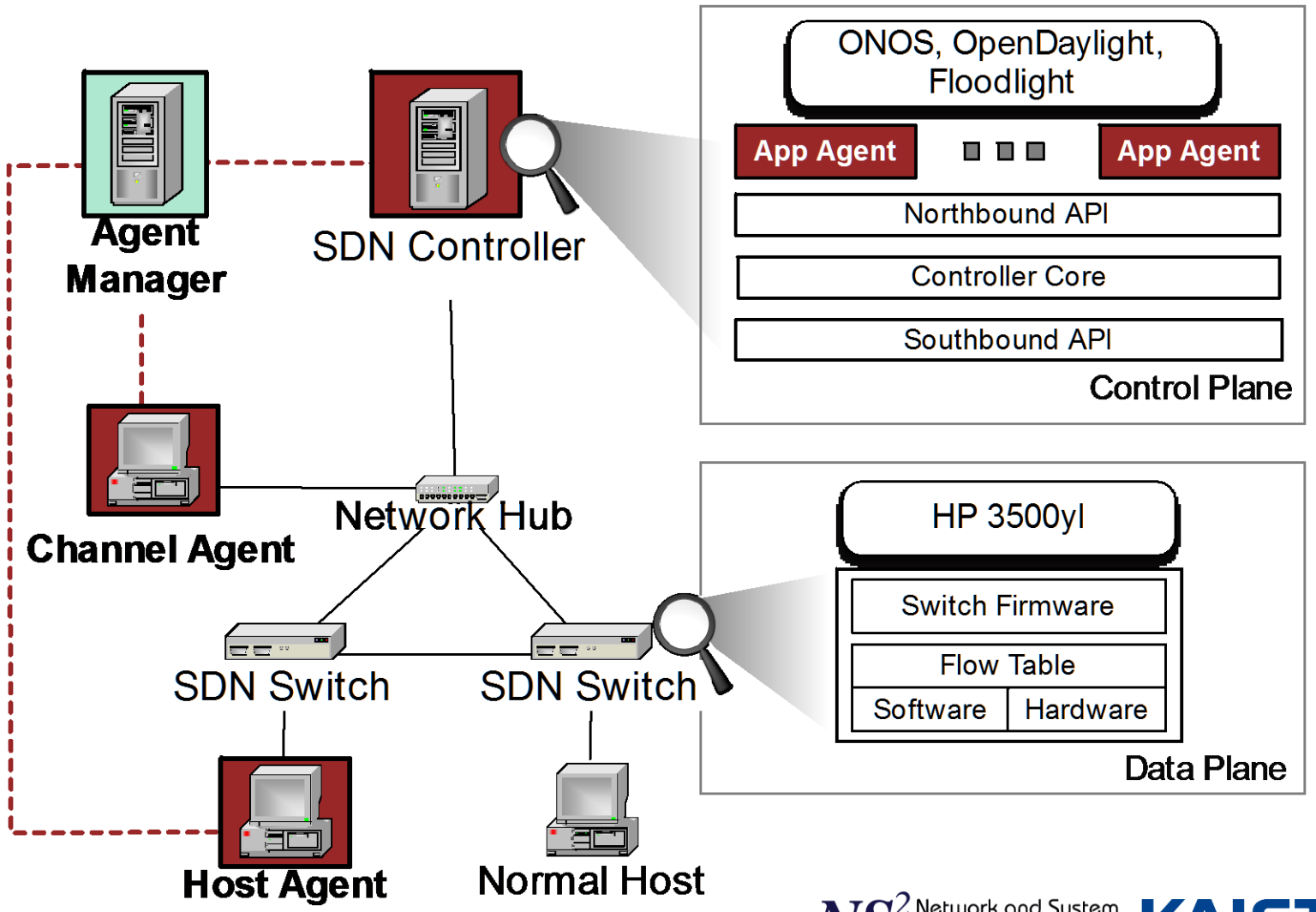
BEST IN SHOWCASE
SDN & OPENFLOW WORLD CONGRESS
OCTOBER 10-14, 2016
THE HAGUE, NETHERLANDS
SDN SOLUTIONS SHOWCASE

https://github.com/OpenNetworkingFoundation/delta

NS2 Network and System Security Laboratory KAIST

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

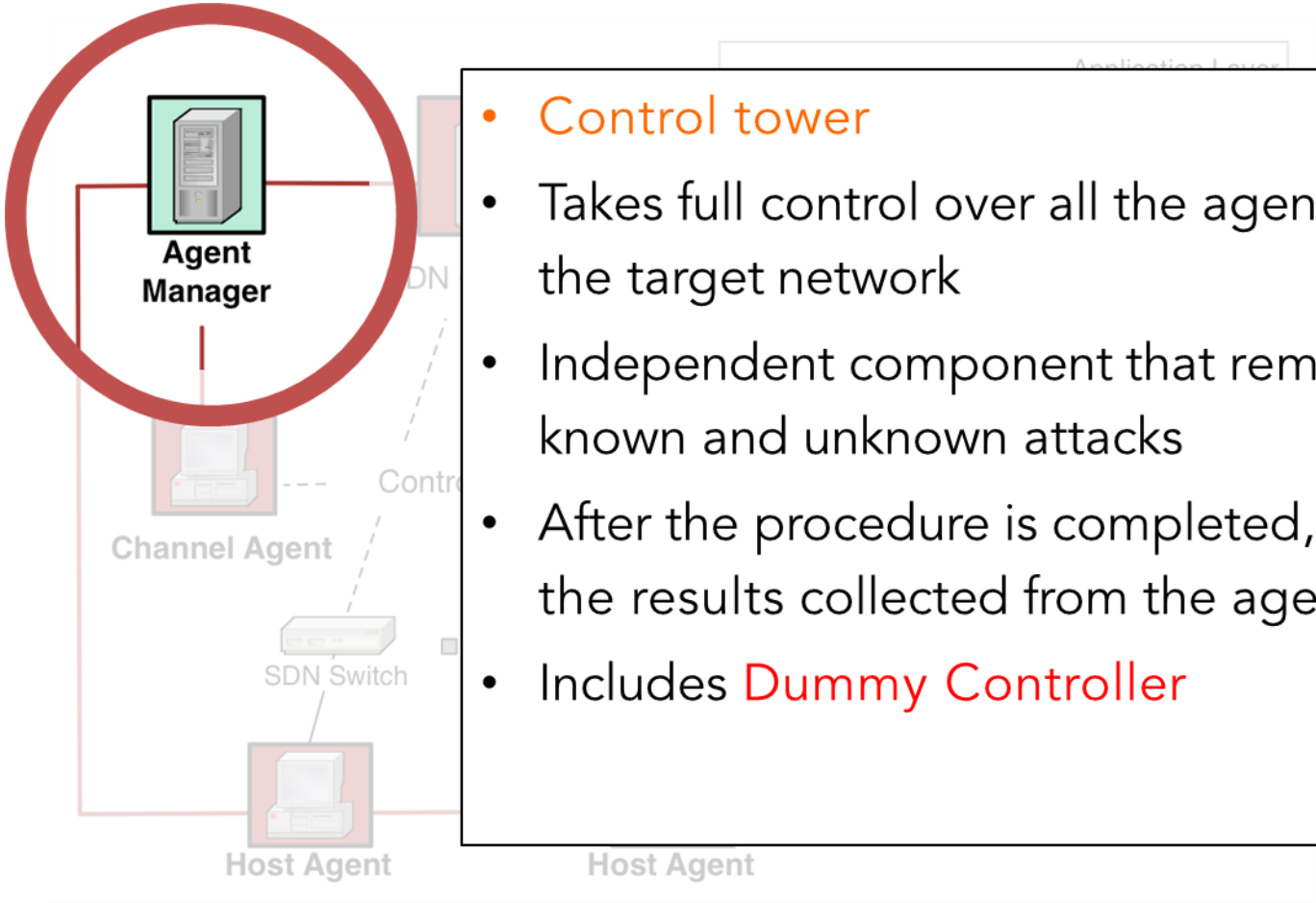
Delta - Framework



NS2 Network and System Security Laboratory KAIST

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

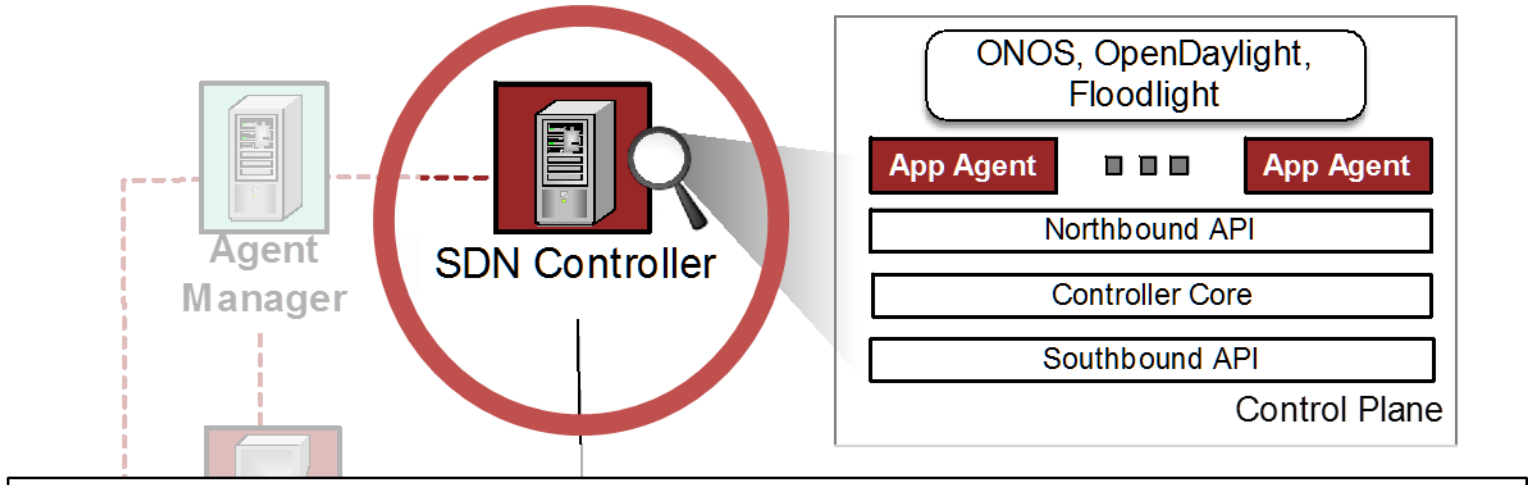
Delta – Agent Manager



- Control tower
- Takes full control over all the agents deployed to the target network
- Independent component that remotely launches known and unknown attacks
- After the procedure is completed, the AM analyzes the results collected from the agents
- Includes Dummy Controller

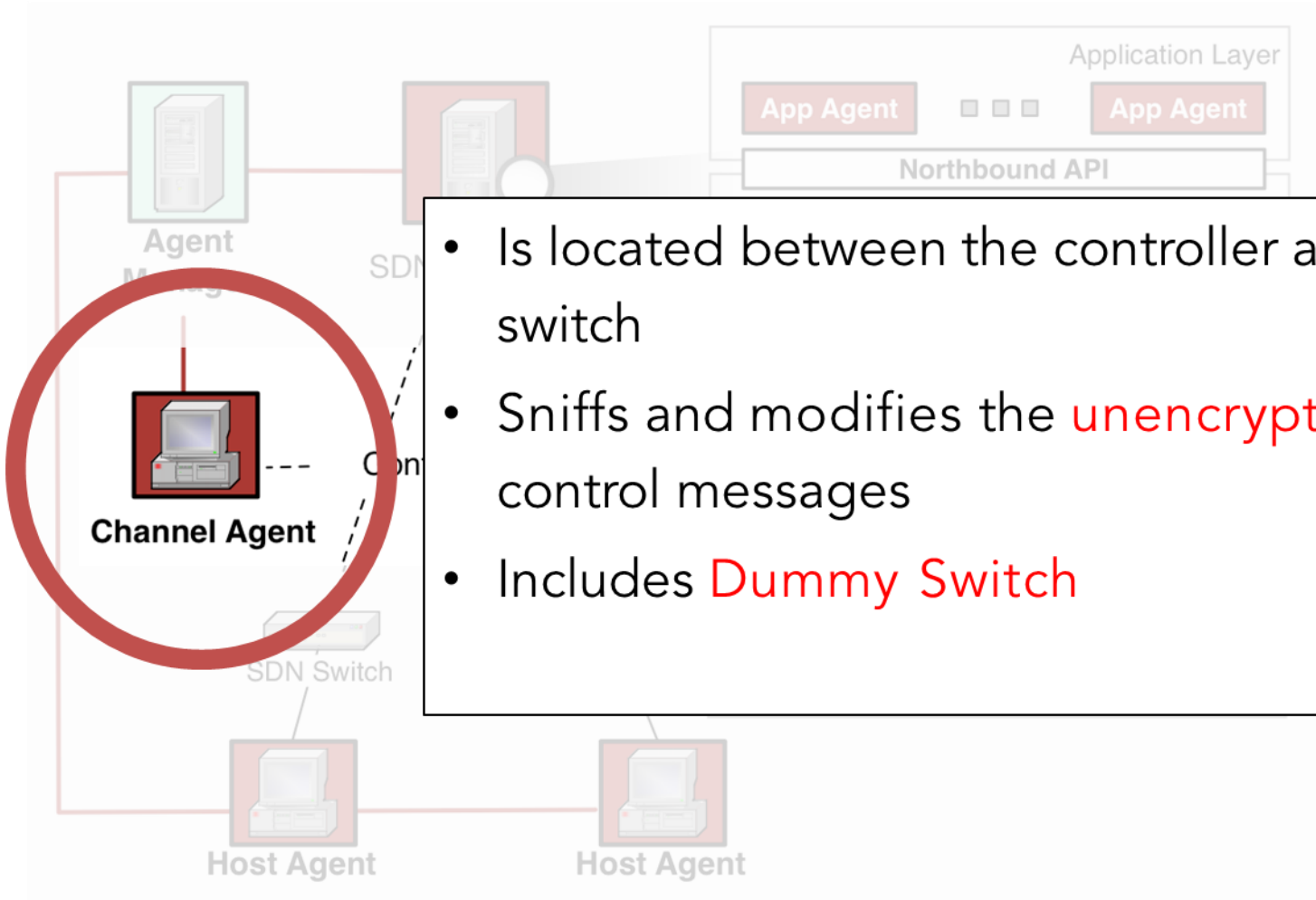
NS2 Network and System Security Laboratory KAIST CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Delta – Application Agent



- SDN applications that conduct attack procedures
- The known malicious functions are implemented as an application agent library

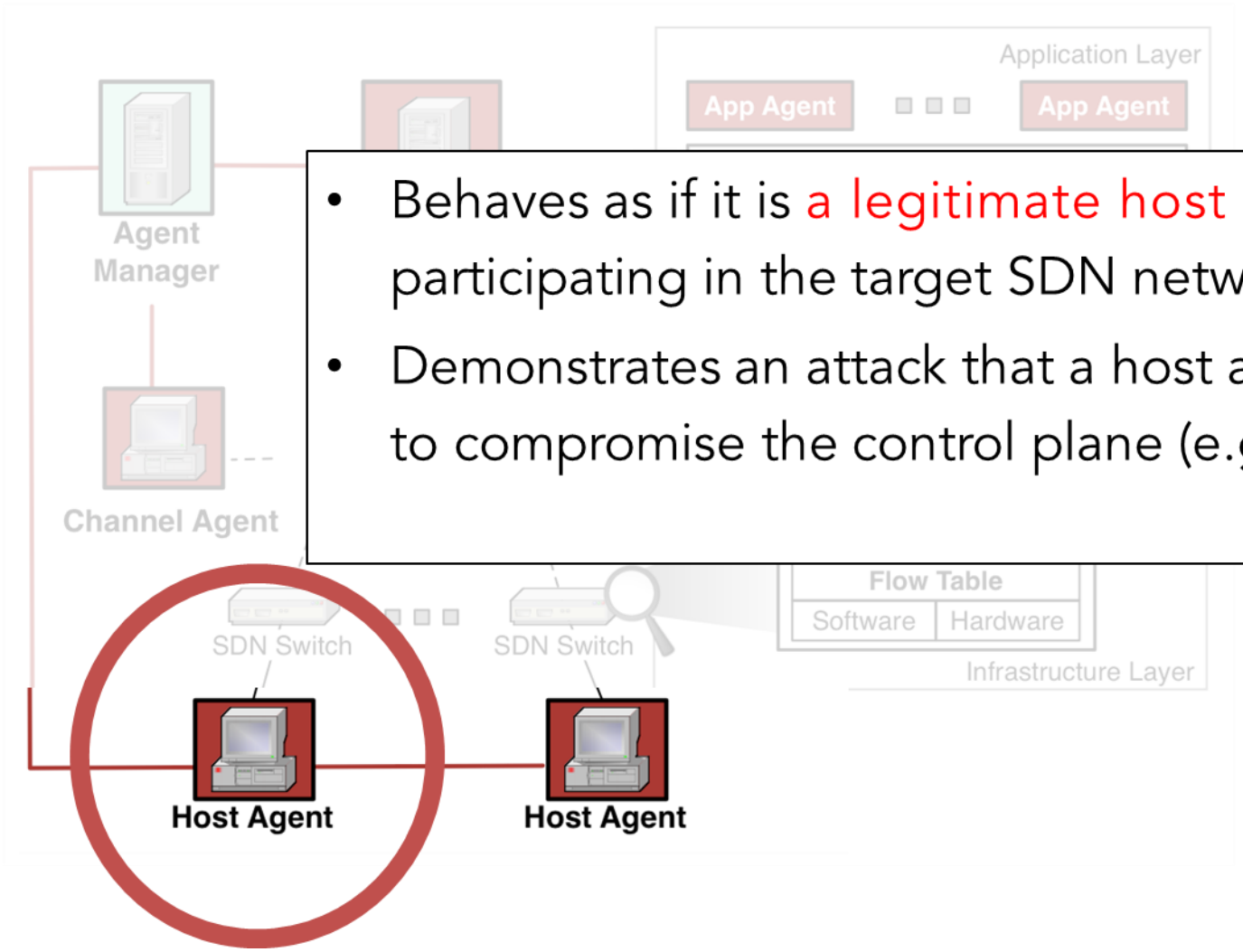
Delta – Channel Agent



- Is located between the controller and the switch
- Sniffs and modifies the unencrypted control messages
- Includes Dummy Switch

NS2 Network and System Security Laboratory KAIST CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Delta – Host Agent

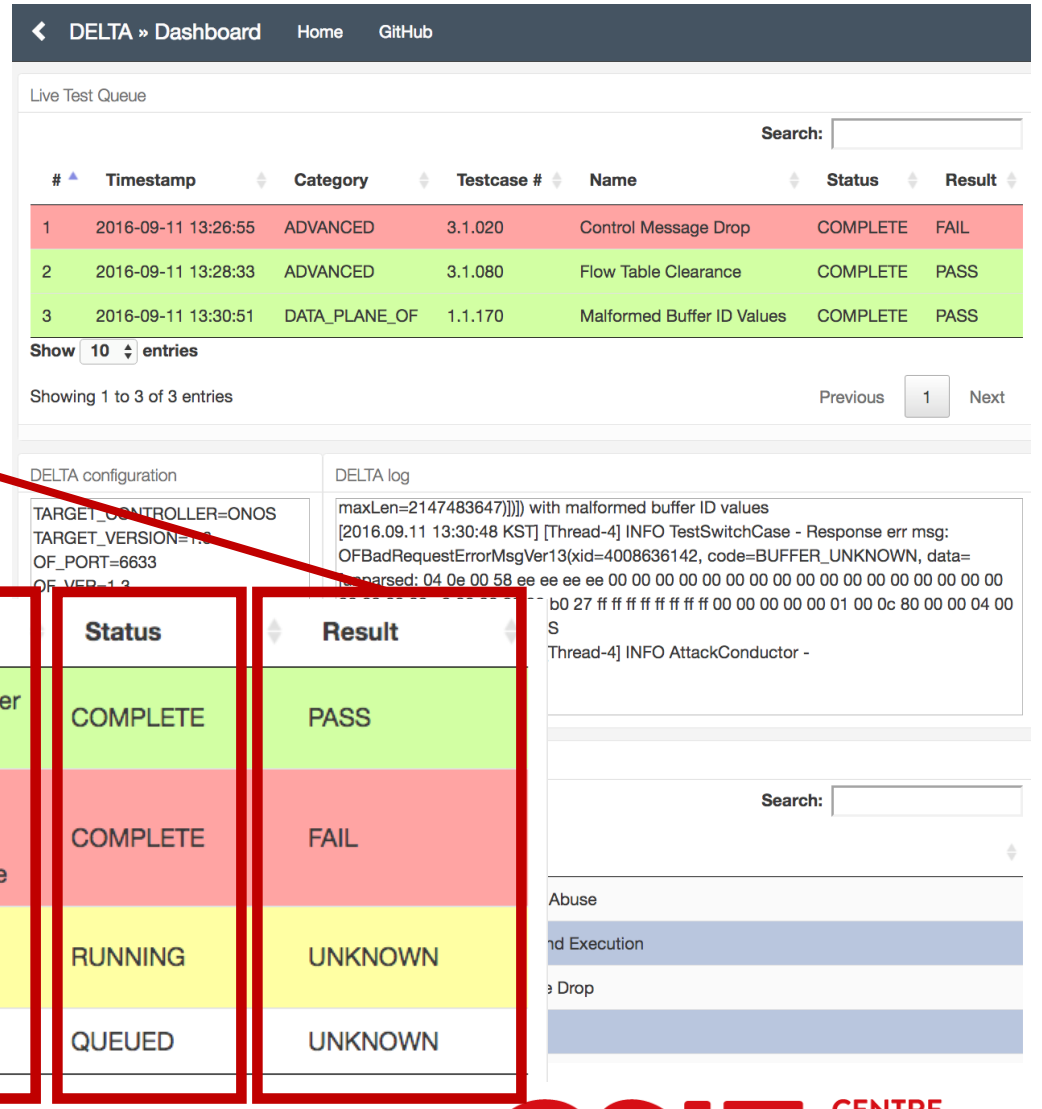


- Behaves as if it is a legitimate host participating in the target SDN network
- Demonstrates an attack that a host attempts to compromise the control plane (e.g. DDoS)

NS2 Network and System Security Laboratory KAIST CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Delta - Dashboard

- PASS (ATTACK FAIL)
- FAIL (ATTACK SUCCESS)



#	Timestamp	Category	Testcase #	Name	Status	Result
1	2016-09-12 08:56:26	DATA_PLANE_OF	1.1.030	Group Identifier Violation	COMPLETE	PASS
2	2016-09-12 08:56:57	CONTROL_PLANE_OF	2.1.020	Corrupted Control Message Type	COMPLETE	FAIL
3	2016-09-12 08:57:15	ADVANCED	3.1.100	Application Eviction	RUNNING	UNKNOWN
4	2016-09-12 08:57:14	ADVANCED	3.1.030	Infinite Loops	QUEUED	UNKNOWN

NS2 Network and System Security Laboratory KAIST

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Delta – Data Plane Security Tests

Data Plane Security Evaluation			
Test No.	**Test Name**	**In Progress**	**Completed**
1.1	**Single Controller:**		
1.1.10	Port Range Violation		✓
1.1.11	TTP Port Range Violation	✓	
1.1.20	Table Number Violation		✓
1.1.30	Group Identifier Violation		✓
1.1.40	Meter Identifier Violation		✓
1.1.50	Table Loop Violation		✓
1.1.60	Corrupted Control Message Type		✓
1.1.70	Unsupported Version Number (bad version)		✓
1.1.80	Malformed Version Number (supported but not negotiated version)		✓
1.1.90	Invalid OXM – Type		✓
1.1.100	Invalid OXM – Length		✓
1.1.110	Invalid OXM – Value		✓
1.1.120	Disabled Table Features Request		✓
1.1.130	Handshake without Hello Message		✓
1.1.140	Control Message before Hello Message (Main Connection)		✓
1.1.150	Incompatible Hello after Connection Establishment		✓
1.1.160	Corrupted Cookie Values		✓
1.1.170	Malformed Buffer ID Values		✓

NS² Network and System Security Laboratory KAIST CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Delta – Data Plane Security Tests

Data Plane Security Evaluation			
Test No.	**Test Name**	**In Progress**	**Completed**
1.2	**Multiple Controllers:**		
1.2.10	Slave Controller Violation		✓
1.2.20	Corrupted Generation ID	✓	
1.2.30	Auxiliary Connection – Terminate when main connection is down	✓	
1.2.40	Auxiliary Connection – Initiate Non-Hello	✓	
1.2.50	Auxiliary Connection – Unsupported Messages	✓	

Delta – Control Plane Security Tests

Control Plane Security Evaluation			
Test No.	**Test Name**	**In Progress**	**Completed**
2.1	**Single Controller:**		
2.1.10	Malformed Version Number (supported but not negotiated version)		✓
2.1.20	Corrupted Control Message Type		✓
2.1.30	Handshake without Hello Message		✓
2.1.40	Control Message before Hello Message (Main Connection)		✓
2.1.50	Multiple main connection request from same switch		✓
2.1.60	Un-flagged Flow Remove Message notification		✓
2.1.70	TLS Support		✓
2.1.71	Startup Behaviour with Failed TLS Connection	✓	
2.1.72	Handling Invalid Authentication Credentials	✓	
2.1.73	Handling Control Packet Modification	✓	
2.1.80	Auxiliary Connection Mismatch with main connection	✓	

NS2 Network and System Security Laboratory KAIST CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Delta – Control Plane Security Tests

Control Plane Security Evaluation			
Test No.	**Test Name**	**In Progress**	**Completed**
2.2	**Multiple Controllers:**		
2.2.10	Master/Equal controller disabled packet-in type	✓	
2.2.20	Slave controller disabled control messages	✓	
2.2.30	Auxiliary Connection request without main connection	✓	
2.2.40	Improper Slave Bad Request Error Message	✓	

Delta – Advanced Security Tests

△ : in progress
✓ : completed
N/A : not applicable

Advanced Security Evaluation								
		In Progress / Completed						
Test No.	**Test Name**	**Floodlight**		**ONOS**			**OpenDaylight**	
3.1	**Single Controller:**	**0.91**	**1.2**	**1.1**	**1.6**	**1.9**	**Helium-sr3**	**Carbon**
3.1.010	Packet-In Flooding				✓			
3.1.020	Control Message Drop	✓	✓	✓	✓	✓	✓	✓
3.1.030	Infinite Loops	✓	✓	✓	✓	✓	✓	✓
3.1.040	Internal Storage Abuse	✓	✓	✓	✓	✓	✓	✓
3.1.050	Device Inventory Table Flooding				△			
3.1.060	Switch Identification Spoofing				✓			
3.1.070	Flow Rule Modification	✓	✓	✓	✓	✓	✓	✓
3.1.080	Flow Table Clearance	✓	✓	✓	✓	✓	✓	✓
3.1.090	Event Listener Unsubscription	✓	✓	N/A	N/A	N/A	✓	✓
3.1.100	Application Eviction	N/A	N/A	✓	✓	✓	✓	✓
3.1.110	Memory Exhaustion	✓	✓	✓	✓	✓	✓	✓
3.1.120	CPU Exhaustion	✓	✓	✓	✓	✓	✓	✓
3.1.130	System Variable Manipulation	✓	✓	✓	✓	✓	✓	✓
3.1.140	System Command Execution	✓	✓	✓	✓	✓	✓	✓

NS² Network and System Security Laboratory KAIST CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Delta – Advanced Security Tests

△ : in progress
✓ : completed
N/A : not applicable

Advanced Security Evaluation								
		In Progress / Completed						
Test No.	**Test Name**	**Floodlight**		**ONOS**			**OpenDaylight**	
3.1	**Single Controller:**	**0.91**	**1.2**	**1.1**	**1.6**	**1.9**	**Helium-sr3**	**Carbon**
3.1.150	Host Location Hijacking				△			
3.1.160	Link Fabrication				✓			
3.1.170	Eavesdrop				✓			
3.1.180	Man-In-The-Middle				✓			
3.1.190	Flow Rule Flooding	✓	✓	✓	✓	✓	✓	✓
3.1.200	Switch Firmware Abuse	✓	✓	✓	✓	✓	✓	✓

NS² Network and System Security Laboratory KAIST CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Delta – Demo/Video

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Delta – Test Results

Test No.	Test Name	Floodlight		ONOS			OpenDaylight	
3.1	**Single Controller:**	**0.91**	**1.2**	**1.1**	**1.6**	**1.10**	**Helium-sr3**	**Carbon**
3.1.010	Packet-In Flooding	F	F	F	F	F	F	
3.1.020	Control Message Drop	F	F	F	F	F	F	
3.1.030	Infinite Loops	F	F	F	F	F	F	
3.1.040	Internal Storage Abuse	F	F	F	F	P	F	
3.1.050	Device Inventory Table Flooding	N/A						
3.1.060	Switch Identification Spoofing	F	F	P	P	P	F	
3.1.070	Flow Rule Modification	F	F	F	F	P	F	
3.1.080	Flow Table Clearance	F	F	F	F	F	F	
3.1.090	Event Listener Unsubscription	F	F	P	P	U	F	
3.1.100	Application Eviction	P	P	F	F	F	F	
3.1.110	Memory Exhaustion	F	F	F	F	P	F	
3.1.120	CPU Exhaustion	F	F	F	F	P	F	
3.1.130	System Variable Manipulation	F	F	P	P	F	F	
3.1.140	System Command Execution	F	F	F	F	F	F	
3.1.150	Host Location Hijacking	N/A						
3.1.160	Link Fabrication	F	F	F	P	U	F	
3.1.170	Eavesdrop	F	F	F	F	F	F	
3.1.180	Man-In-The-Middle	F	F	F	F	F	F	
3.1.190	Flow Rule Flooding	F	F	F	F	F	F	
3.1.200	Switch Firmware Abuse	F	F	F	F	P	F	

S. Secci, K. Attou, DC. Phung, S. Scott-Hayward, D. Smyth, S. Vemuri, You Wang, "*ONOS Security and Performance Analysis (1st report)*", Informational report, Open Networking Foundation, Sept. 2017

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Delta – Test Results

Flow Type	*Attack Code*	*Attack Name*	*Controller*		
			ONOS	*OpenDaylight*	*Floodlight*
Symmetric Flows	SF-1	Switch Table Flooding [11]	X	X	O
	SF-2	Switch Identification Spoofing [10]	X	O	O
	SF-3	Malformed Control Message [37]	X	O	O
	SF-4	Control Message Manipulation [35]	O	O	O
Asymmetric Flows	AF-1	Control Message Drop [35]	O	O	O
	AF-2	Control Message Infinite Loop [35]	O	O	O
	AF-3	PACKET_IN Flooding [21], [38], [40]	O	O	O
	AF-4	Flow Rule Flooding [8], [38], [45]	O	O	O
	AF-5	Flow Rule Modification [35]	O	O	O
	AF-6	Switch Firmware Misuse [35]	O	O	O
	AF-7	Flow Table Clearance [35]	O	O	O
	AF-8	Eavesdrop [35]	O	O	O
	AF-9	Man-In-The-Middle [35]	O	O	O
Intra-Controller Control Flows	CF-1	Internal Storage Misuse [39]	O	O	O
	CF-2	Application Eviction [39]	O	O	N/A
	CF-3	Event Listener Unsubscription [39]	N/A	O	O
Non Flow Operations	NF-1	System Command Execution [39]	O	O	O
	NF-2	Memory Exhaustion [39]	O	O	O
	NF-3	CPU Exhaustion [39]	O	O	O
	NF-4	System Variable Manipulation [35]	X	O	O

Lee, Seungsoo, Changhoon Yoon, Chanhee Lee, Seungwon Shin, Vinod Yegneswaran, and Phillip Porras. "DELTA: A security assessment framework for software-defined networks." In *Proceedings of NDSS*, vol. 17. 2017.

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Conclusion

Increasing focus on security within both controller communities

BUT

Lack of integration of security as a core feature of the controller

Article available at: https://arxiv.org/abs/1711.08406

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES