



**QUEEN'S
UNIVERSITY
BELFAST**

CSIT

**CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES**



TRAILING THE SNAIL: SDN CONTROLLER SECURITY EVOLUTION



DR. SANDRA SCOTT-HAYWARD, QUEEN'S UNIVERSITY BELFAST
ONOS SECURITY AND PERFORMANCE BRIGADE WORKSHOP, 11 APRIL 2018

Centre for Secure Information Technologies (CSIT)

CSIT is the UK's Innovation and Knowledge Centre for Cybersecurity



CSIT CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES

Centre for Secure Information Technologies (CSIT)

Member of the UK **CYBER GROWTH
PARTNERSHIP** (CGP) STEERING BOARD

90 PEOPLE

DIRECTOR, 16 ACADEMICS
16 ENGINEERS, 5 BUS. DEV.,
15 PDRAs, 29 PhDs, IT/Clerical 9

8 Spin-outs created, start-ups/scale-ups supported

Nucleated the Belfast Cyber Cluster (now 38
companies with >1,200 new jobs)

**HOST THE ANNUAL WORLD CYBER SECURITY
TECHNOLOGY RESEARCH SUMMIT**

PART OF RESEARCH
COUNCILS UK RCUK

**PARTNERSHIP IN
CONFLICT CRIME
AND SECURITY
RESEARCH
PROGRAMME**

EST. 2009

BASED IN THE ECIT INSTITUTE
QUEEN'S UNIVERSITY BELFAST

INITIAL FUNDING OVER £30M

£30M

Additional £15M won in competitive
tendering

IN 2015, PHASE 2 CORE FUNDING OF
£14M SECURED, WHICH (OVER NEXT
5 YEARS) WILL LEVERAGE

>£38M

CSIT CENTRE
FOR SECURE
INFORMATION
TECHNOLOGIES

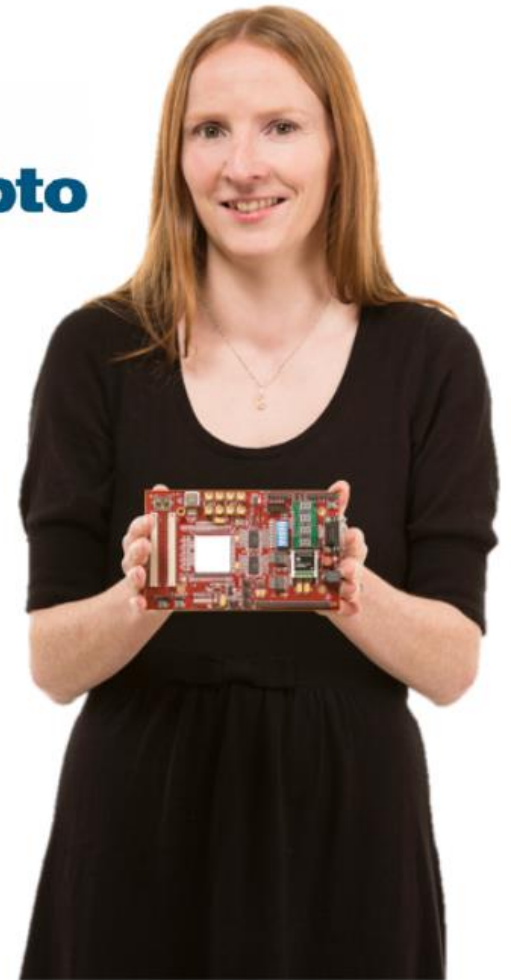


THE QUEEN'S ANNIVERSARY PRIZES
FOR HIGHER AND FURTHER EDUCATION
2015

Research Area: Data Security

Professor Máire O'Neill - Research Director

- **Quantum Safe Cryptography**
 - *Physically secure efficient quantum-safe hardware and software designs, leads H2020 €3.8M SAFEcrypto Project*
- **Cryptographic hardware and software architectures**
 - *Including lightweight crypto*
- **Physical Unclonable Functions for M2M and IoT authentication**
 - *Strong PUF, Software PUF, resistance to SCA/Modelling attacks*
- **Side Channel Analysis**
 - *Including Machine Learning /Deep Learning SCA*
- **Hardware Trojan detection**



Research Area: Networked Systems Security

Professor Sakir Sezer - Research Director

- **Network Security**
 - *Intrusion detection, WEB security, DDoS detection*
- **Virtual Networks**
 - *including Software Defined Network security*
- **Cloud Computing Security**
 - *VM security , secure segregation, hypervisor security etc.*
- **Mobile & IoT security**
 - *Security policy enforcement, Android Malware etc.*
- **Critical Infrastructure Security**
 - *SCADA, Smart Grid intrusion prevention etc.*
- **Malware/Botnet defence**
 - *Obfuscation strategies, detection algorithms, reverse engineering*



Research Area: Security Analytics and Event Mgmt.

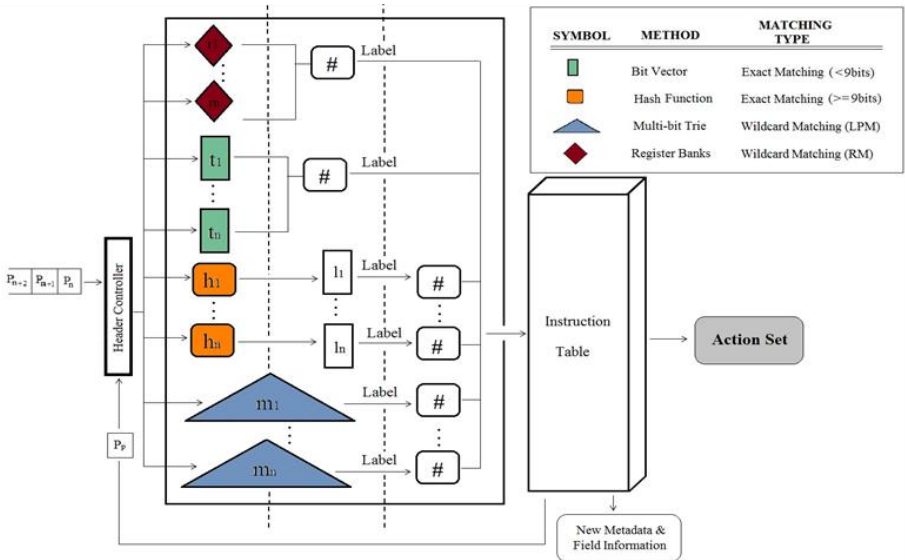
Dr Paul Miller - Research Director

- **Deep learning neural networks**
 - *Android malware detection*
- **Graph Mining**
 - *Network Intrusion Detection and Insurance Fraud Detection*
- **Event Reasoning**
 - *Alert correlation for total network defence*
- **Multimedia content analysis**
 - *Open source intelligence, cyber-physical security*



SDN Security Research

Controller	Source	Version	Release	Architecture	Objective	Security Features
ONOS	ONLab	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)



```

Application Register for Floodlight

<Main> (R)egister, (U)nregister, (L)auncher, (P)ermissions, (C)heck, (E)xit. Enter an option: c

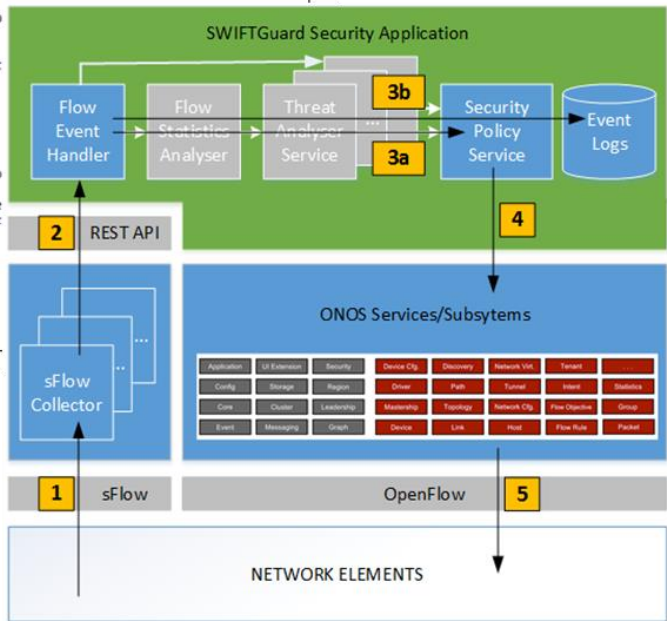
<Check>
Currently registered applications [circuitpusherID, test], instances [cp2, cp1, test_app]
Enter application/instance ID: circuitpusherID
Application [circuitpusherID] attributes:
  registered true
  arguments true
  permissions true
  path /home/rng6/floodlight-0.91/apps/circuitpusherID/circuitpusherID.py
  hash 998867cbd3f9e8a32d20270a6e9c7ae556008d5caff9381a9265dfb31dbe9db3
  instances [cp2, cp1]

<Main> (R)egister, (U)nregister, (L)auncher, (P)ermissions, (C)heck, (E)xit. Enter an option: c

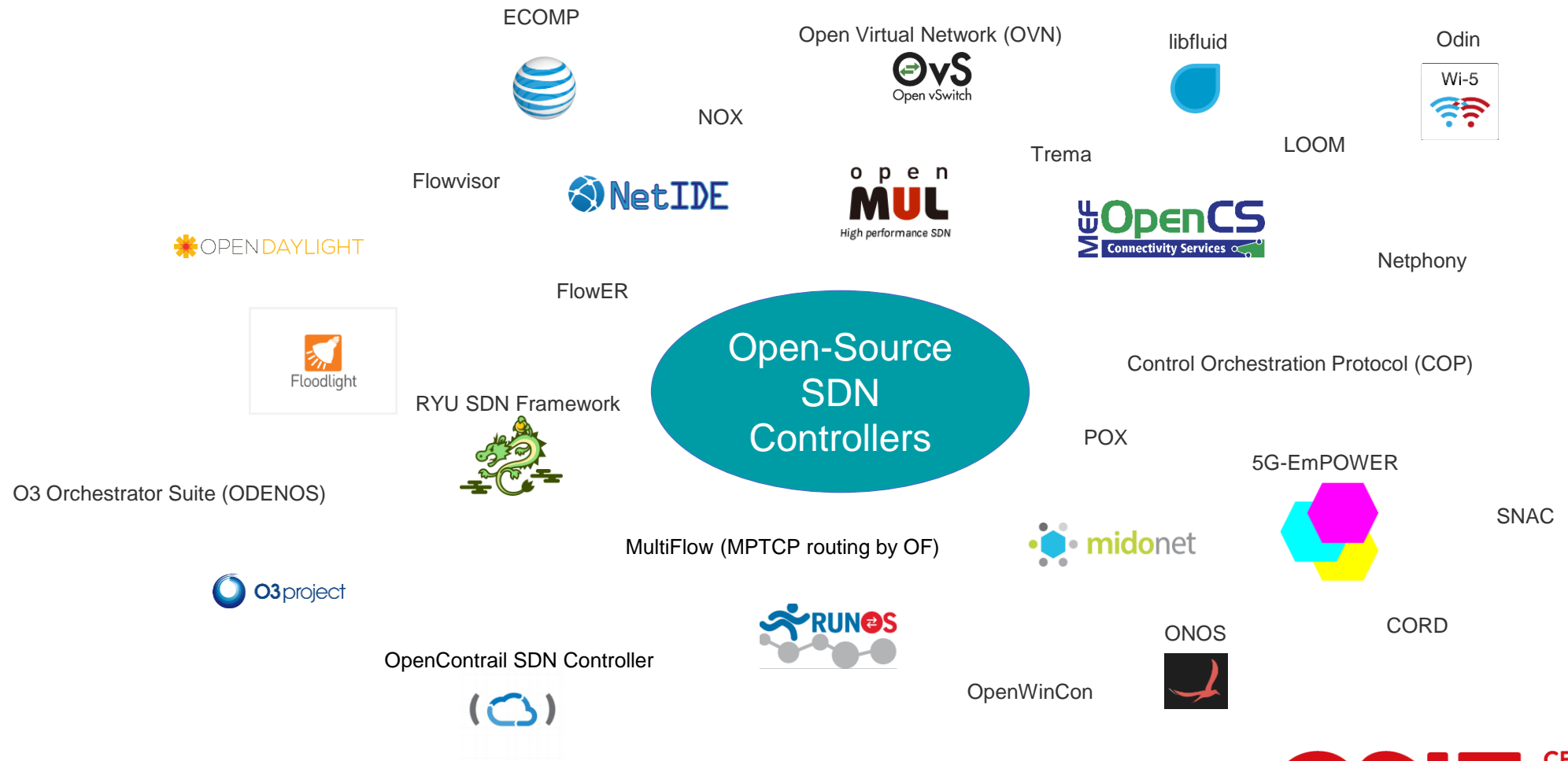
<Check>
Currently registered applications [circuitpusherID, test], instances [cp2, cp1, test_app]
Enter application/instance ID: test_app
Instance [test_app] attributes:
  permissions false
  launched false
  app_id test

<Main> (R)egister, (U)nregister, (L)auncher, (P)ermissions, (C)heck, (E)xit. Enter an option: c

<Permissions> (S)et, (U)nset, (C)heck, (B)ack to main menu
Currently registered applications [circuitpusherID, test]
Enter Application ID: test
Current permissions of [test] application:
  read_topology false
  read_all_flow false
  read_statistics false
  read_pkt_in_payload false
  
```



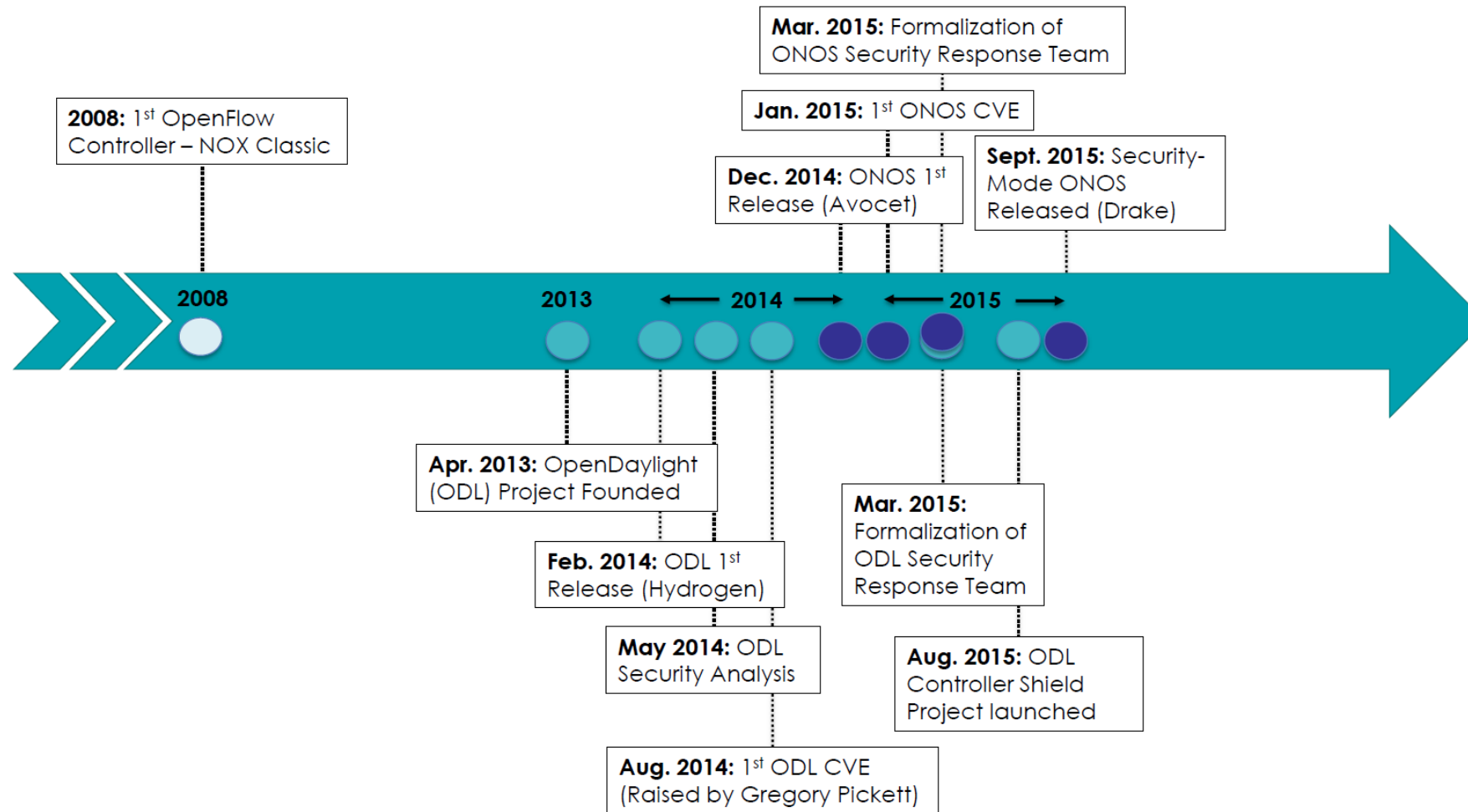
Open-source SDN Controllers



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



ODL and ONOS Security-related events



Features of a secure, robust, and resilient SDN Controller

Secure Controller Design

Control Process (Application) Isolation

Implementation of Policy Conflict Resolution

Multiple Controller Instances – Resilience

Multiple Application Instances – Resilience

Secure Storage

Secure Controller Interfaces

Secure Control Layer Communication

GUI/REST API Security

Controller Security Services

IDS/IPS Integration

Authentication and Authorization

Resource Monitoring

Logging/Security Audit Service

S. Scott-Hayward, “Design and deployment of secure, robust, and resilient SDN Controllers”, IEEE Conference on Network Softwarization (NetSoft), April 2015.



ONOS – Security Support

Security

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

@ November 2017

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](#)

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)

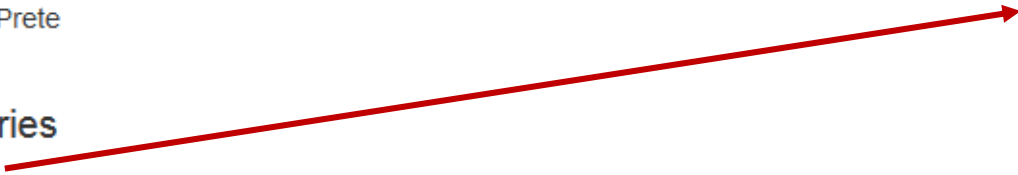
Test team: Suchitra Vemuri

ONE: 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

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

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	<i>[Automatic application security policy extraction using static analysis techniques (KAIST)]; SecurityGroup feature of OpenStack</i>
Goldeneye (v1.6)	May 2016	
Hummingbird (v1.7)	Sept. 2016	<i>[New subsystem for anomaly detection (ATHENA) (SRI)]; Rate limit on port via NetConf (GEANT)</i>
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	



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 security issue. If you would like to be credited for discovering the issue and the details of any embargo you would like to request, please note how you would like to be credited for discovering the issue and the details of any embargo you would like to request.

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-xsq
 - 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

ODL Security Support – Recent Activity

[About](#) [Charter](#) [What We Do](#) [Use Cases and Users](#) [Ecosystem & Solutions](#) [Technical Community](#) [Support OpenDaylight](#)

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.

Getting Started for
Developers >

Security

IP Policy >

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

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

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: <i>Unified Secure Channel</i> eases secure communication between ODL and widely distributed networking equipment; <i>Time Series Data Repository (TSDR)</i> enables collection and analysis of large amounts of network activity; <i>Device Identification and Driver Management (DIDM)</i> provides end users the ability to discover, manage and automate a wide range of existing hardware in their infrastructure; <i>Persistence</i> ensures application-specific data is preserved over time or in the event of a catastrophe; <i>Topology Processing Framework</i> 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	<i>NetVirt project</i> enhanced support in OpenStack environments for IPv6, Security Groups (via OpenFlow configuration) and VLANs. <i>Cardinal</i> project monitors the health of the controller, delivered as a service to existing, deployed network monitoring and analytics tools. <i>Centinel</i> analytics engine enables end-to-end data collection and machine learning to support performance monitoring and bandwidth management across WAN links.
Carbon	May 2017	<i>NetVirt and Genius projects</i> 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

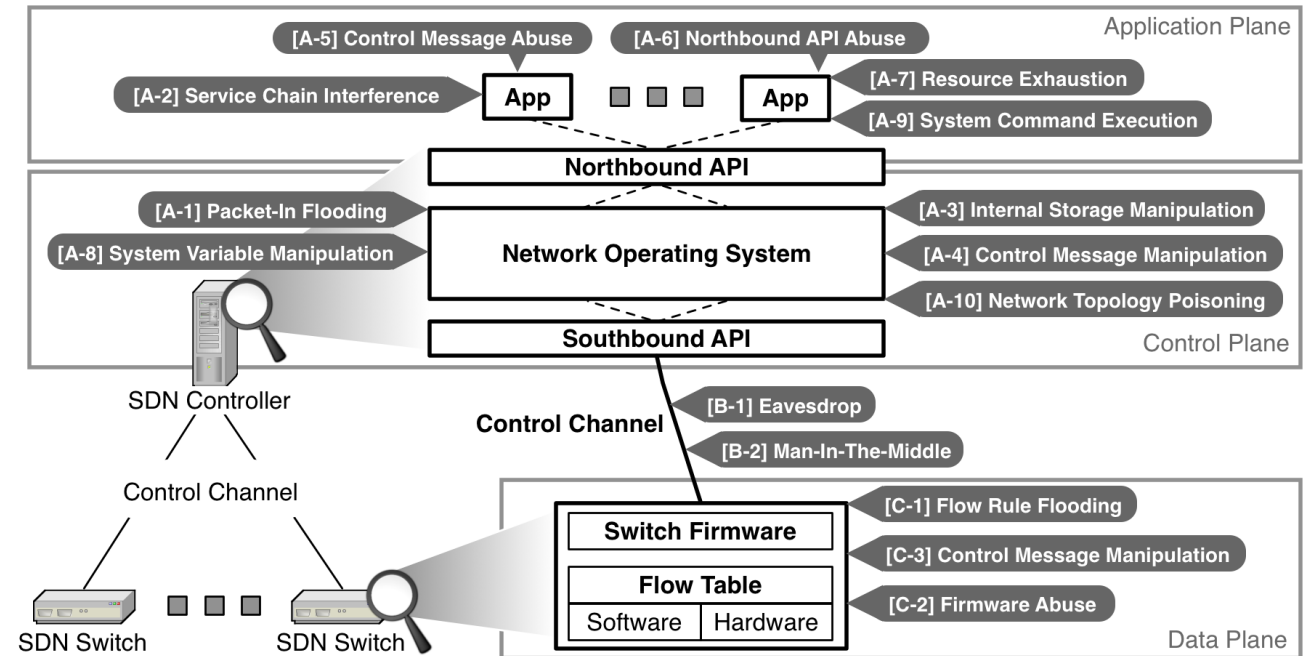
Delta - Motivation



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)





Delta: A Penetration Testing Framework for Software-Defined Networks

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



<https://github.com/OpenNetworkingFoundation/delta>



Delta - Dashboard

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

DELTA » Dashboard

Home

GitHub

Live Test Queue

Search:

#	Timestamp	Category	Testcase #	Name	Status	Result
1	2016-09-11 13:26:55	ADVANCED	3.1.020	Control Message Drop	COMPLETE	FAIL
2	2016-09-11 13:28:33	ADVANCED	3.1.080	Flow Table Clearance	COMPLETE	PASS
3	2016-09-11 13:30:51	DATA_PLANE_OF	1.1.170	Malformed Buffer ID Values	COMPLETE	PASS

Show 10 entries

Showing 1 to 3 of 3 entries

Previous1Next

DELTA configuration

DELTA log

TARGET_CONTROLLER=ONOS
TARGET_VERSION=1.0
OF_PORT=6633
OF_VER=1.2

maxLen=2147483647))))) with malformed buffer ID values
[2016.09.11 13:30:48 KST] [Thread-4] INFO TestSwitchCase - Response err msg:
OFBadRequestErrorMsgVer13(xid=4008636142, code=BUFFER_UNKNOWN, data=
parsed: 04 0e 00 58 ee ee ee 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
b0 27 ff ff ff ff ff ff ff ff 00 00 00 00 00 01 00 0c 80 00 00 04 00
S
Thread-4] INFO AttackConductor -

Search:

Abuse

nd Execution

Drop

#	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

Delta – Data Plane Security Tests

<i>Data Plane Security Evaluation</i>			
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		✓

Delta – Data Plane Security Tests

<i>Data Plane Security Evaluation</i>			
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	✓	

Delta – Control Plane Security Tests

<i>Control Plane Security Evaluation</i>			
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	✓	✓	✓	✓	✓	✓	✓

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	✓	✓	✓	✓	✓	✓	✓

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

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.

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>

Thank you

s.scott-hayward@qub.ac.uk

www.csit.qub.ac.uk