CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Queen's University Belfast

SDN Security

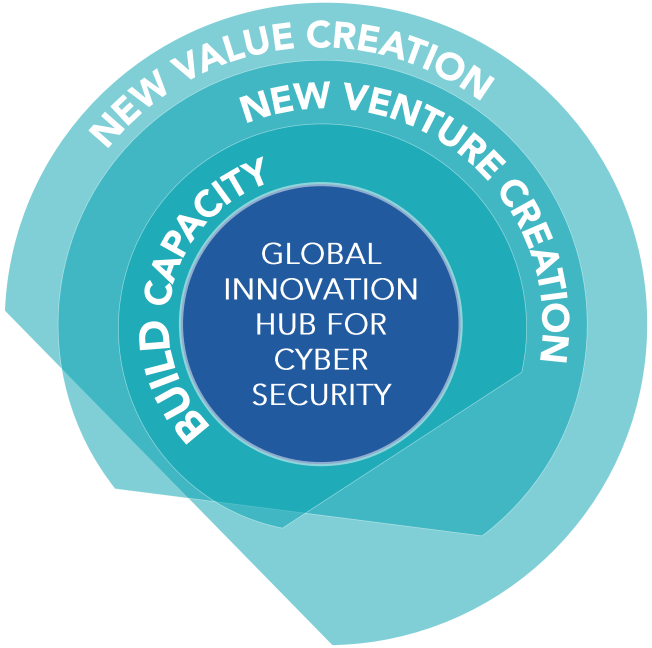
Open Networking Korea, Seoul

Dr. Sandra Scott-Hayward

19 November 2015

@CSIT_QUB

Centre for Secure Information Technologies



Est.2009, Based in The ECIT Institute

Initial funding over £30M (CSIT 2 - £38M)

80 People
- Researchers
- Engineers
- Business Development

Largest UK University lab for cyber security technology research

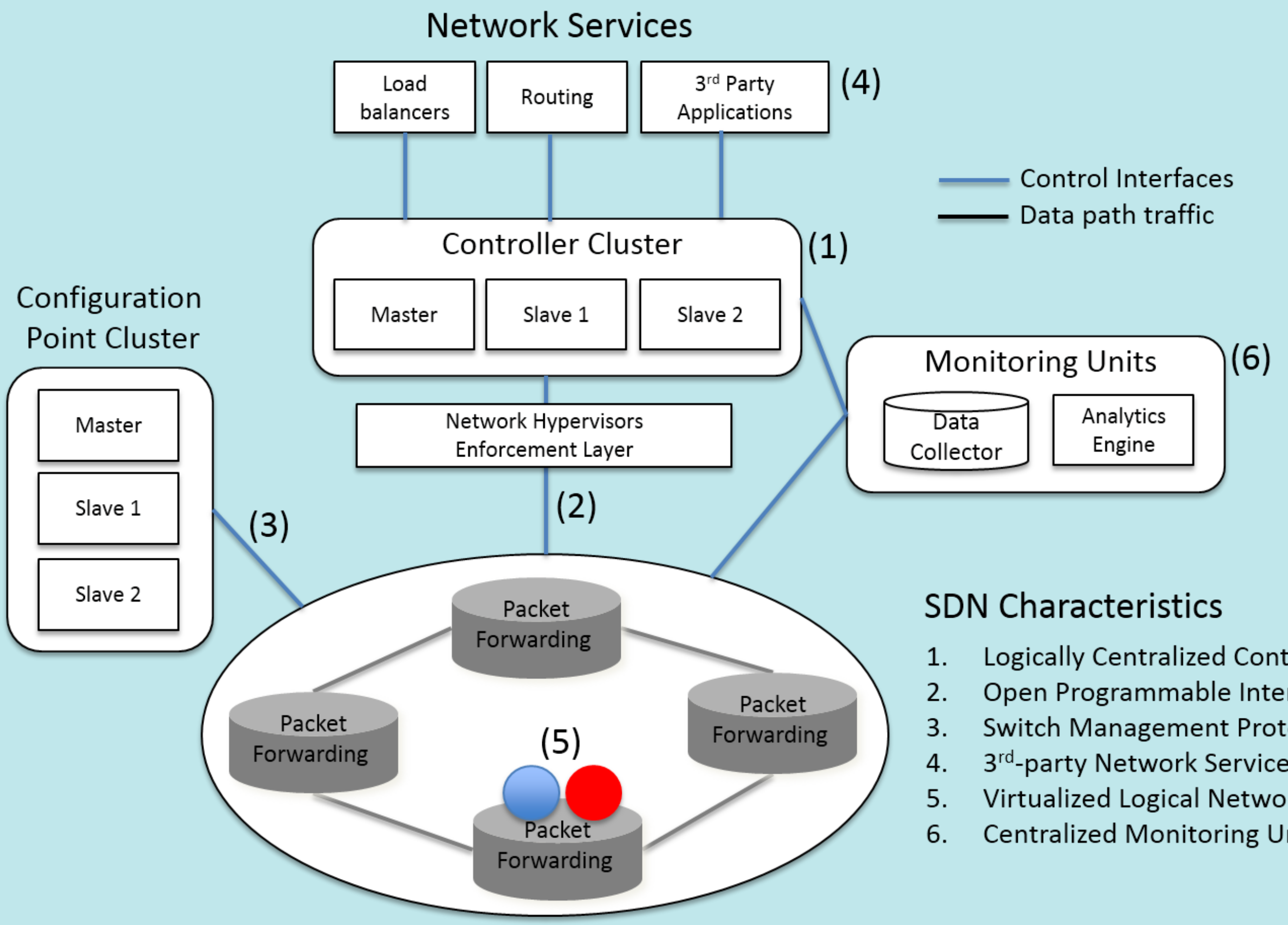
GCHQ Academic Centre of Excellence

Industry Informed
- Open Innovation Model

Strong international links
- ETRI, CyLab, GTRI, SRI International
- Cyber Security Technology Summit

SDN Security …

SDN Characteristics



SDN Characteristics

1. Logically Centralized Control
2. Open Programmable Interfaces
3. Switch Management Protocol
4. 3rd-party Network Services
5. Virtualized Logical Networks
6. Centralized Monitoring Units

S. Scott-Hayward, S. Natarajan, S. Sezer, ‘A Survey of Security in Software Defined Networks’, IEEE Communications Surveys & Tutorials, 2015.

Secure Communications Network

Confidentiality

Integrity

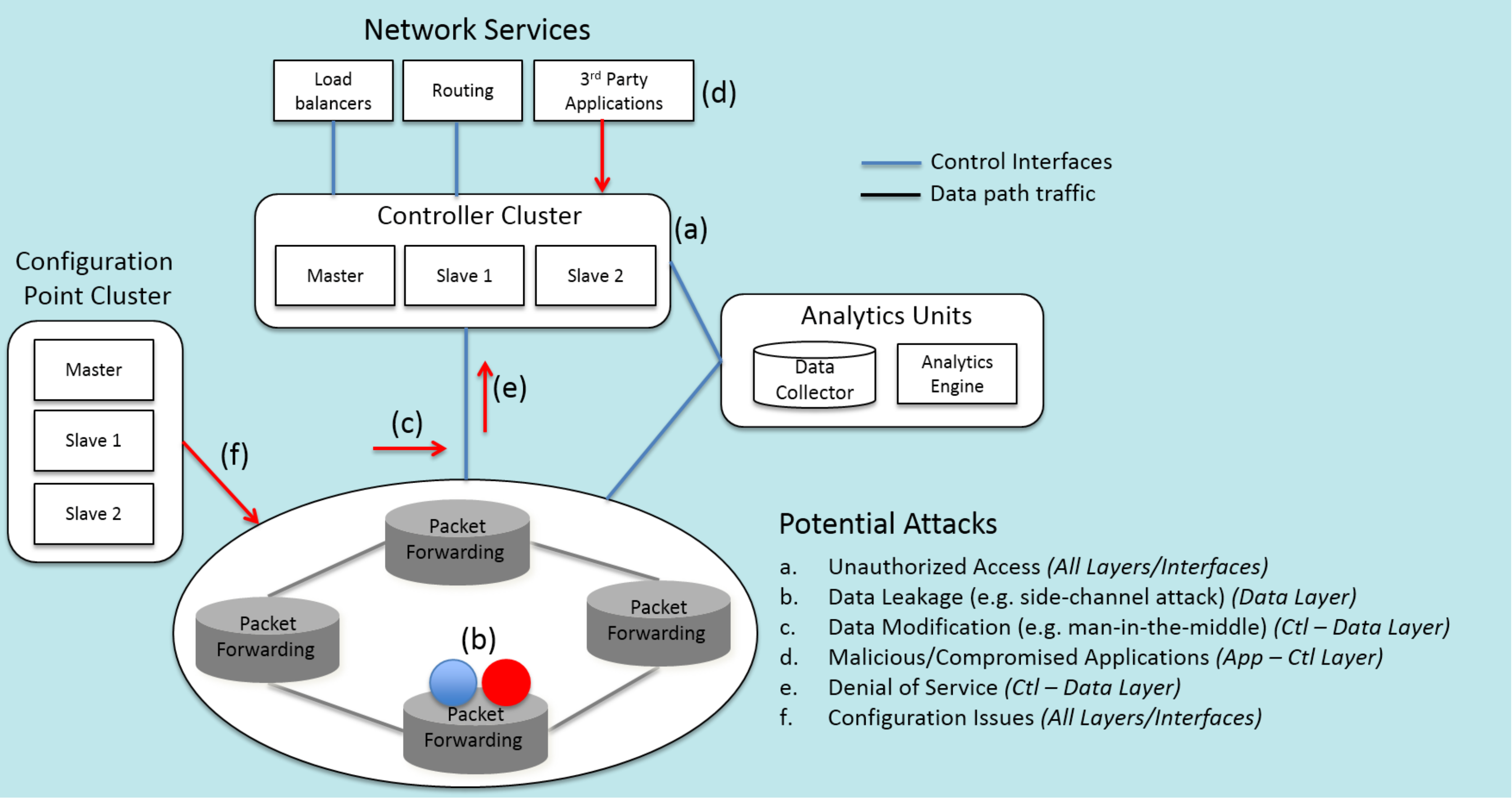
Availability of Information

Authentication

Non-repudiation

=> Secure data, network assets and communication transactions

SDN Potential Attacks and Vulnerabilities



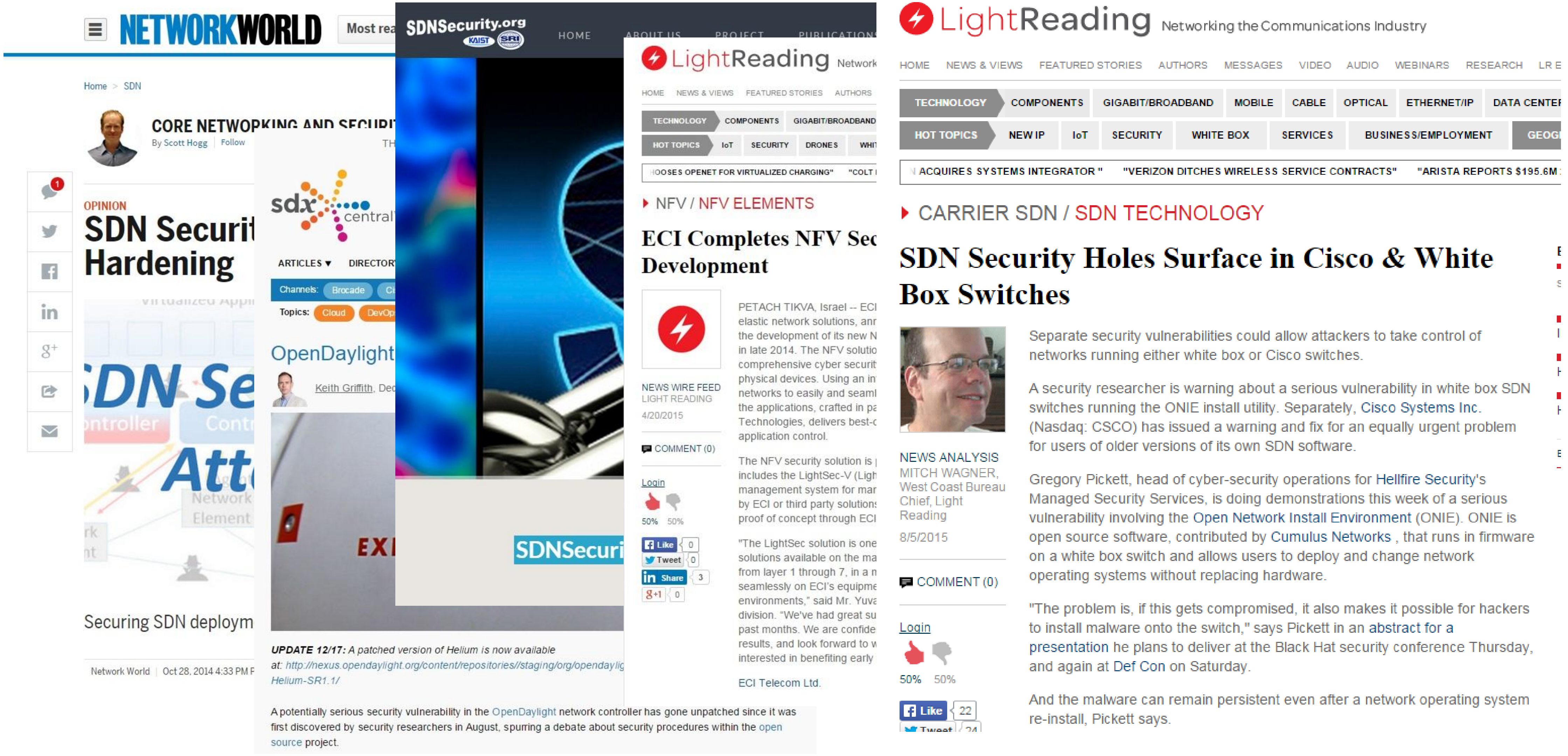
Potential Attacks

a. Unauthorized Access *(All Layers/Interfaces)*
b. Data Leakage (e.g. side-channel attack) *(Data Layer)*
c. Data Modification (e.g. man-in-the-middle) *(Ctl – Data Layer)*
d. Malicious/Compromised Applications *(App – Ctl Layer)*
e. Denial of Service *(Ctl – Data Layer)*
f. Configuration Issues *(All Layers/Interfaces)*

Categorization of Security Issues

Security Issue/Attack	SDN Layer Affected or Targeted				
	Application Layer	App-Ctl Interface	Control Layer	Ctl-Data Interface	Data Layer
Unauthorized Access e.g.					
• Unauthorized Controller Access/Controller Hijacking			X	X	X
• Unauthorized/Unauthenticated Application	X	X	X		
Data Leakage e.g.					
• Flow Rule Discovery (Side Channel Attack on Input Buffer)					X
• Credential Management (Keys, Certificates for each Logical Network)					X
• Forwarding Policy Discovery (Packet Processing Timing Analysis)			X	X	X
Data Modification e.g.					
• Flow Rule Modification to Modify Packets (Man-in-the-Middle attack)			X	X	X
Malicious/Compromised Applications e.g.					
• Fraudulent Rule Insertion	X	X	X		
Denial of Service e.g.					
• Controller-Switch Communication Flood			X	X	X
• Switch Flow Table Flooding					X
Configuration Issues e.g.					
• Lack of TLS (or other Authentication Technique) Adoption	X	X	X	X	X
• Policy Enforcement	X	X	X		
• Lack of Secure Provisioning	X	X	X	X	X
System Level SDN Security e.g.					
• Lack of Visibility of Network State			X	X	X

SDN Security … focus since Q4 2014



NETWORKWORLD

Most rea

Home > SDN

CORE NETWORKING AND SECURIT

By Scott Hogg | Follow

OPINION

SDN Securit Hardening

Securing SDN deploym

Network World | Oct 28, 2014 4:33 PM P

sdxcentral

ARTICLES ▾ DIRECTOR

Channels: Brocade Ci

Topics: Cloud DevOp

OpenDaylight

Keith Griffith, Dec

UPDATE 12/17: *A patched version of Helium is now available at: http://nexus.opendaylight.org/content/repositories//staging/org/opendaylig Helium-SR1.1/*

A potentially serious security vulnerability in the OpenDaylight network controller has gone unpatched since it was first discovered by security researchers in August, spurring a debate about security procedures within the open source project.

SDNSecurity.org KAIST SRI

HOME ABOUT US PROJECT PUBLICATIONS

SDNSecuri

LightReading Network

HOME NEWS & VIEWS FEATURED STORIES AUTHORS

TECHNOLOGY COMPONENTS GIGABIT/BROADBAND

HOT TOPICS IoT SECURITY DRONES WHI

OOSES OPENET FOR VIRTUALIZED CHARGING" "COLT I

NFV / NFV ELEMENTS

ECI Completes NFV Sec Development

NEWS WIRE FEED
LIGHT READING
4/20/2015

COMMENT (0)

Login

50% 50%

Like 0 Tweet 0 Share 3 +1 0

PETACH TIKVA, Israel -- ECI elastic network solutions, ann the development of its new N in late 2014. The NFV solutio comprehensive cyber securit physical devices. Using an in networks to easily and seaml the applications, crafted in pa Technologies, delivers best-c application control.

The NFV security solution is includes the LightSec-V (Ligh management system for mar by ECI or third party solutions proof of concept through ECI

"The LightSec solution is one solutions available on the ma from layer 1 through 7, in a n seamlessly on ECI's equipme environments," said Mr. Yuva division. "We've had great su past months. We are confide results, and look forward to w interested in benefiting early

ECI Telecom Ltd.

LightReading Networking the Communications Industry

HOME NEWS & VIEWS FEATURED STORIES AUTHORS MESSAGES VIDEO AUDIO WEBINARS RESEARCH LR E

TECHNOLOGY COMPONENTS GIGABIT/BROADBAND MOBILE CABLE OPTICAL ETHERNET/IP DATA CENTER

HOT TOPICS NEW IP IoT SECURITY WHITE BOX SERVICES BUSINESS/EMPLOYMENT GEOG

ACQUIRES SYSTEMS INTEGRATOR" "VERIZON DITCHES WIRELESS SERVICE CONTRACTS" "ARISTA REPORTS $195.6M

CARRIER SDN / SDN TECHNOLOGY

SDN Security Holes Surface in Cisco & White Box Switches

NEWS ANALYSIS
MITCH WAGNER, West Coast Bureau Chief, Light Reading
8/5/2015

COMMENT (0)

Login

50% 50%

Like 22 Tweet 24

Separate security vulnerabilities could allow attackers to take control of networks running either white box or Cisco switches.

A security researcher is warning about a serious vulnerability in white box SDN switches running the ONIE install utility. Separately, Cisco Systems Inc. (Nasdaq: CSCO) has issued a warning and fix for an equally urgent problem for users of older versions of its own SDN software.

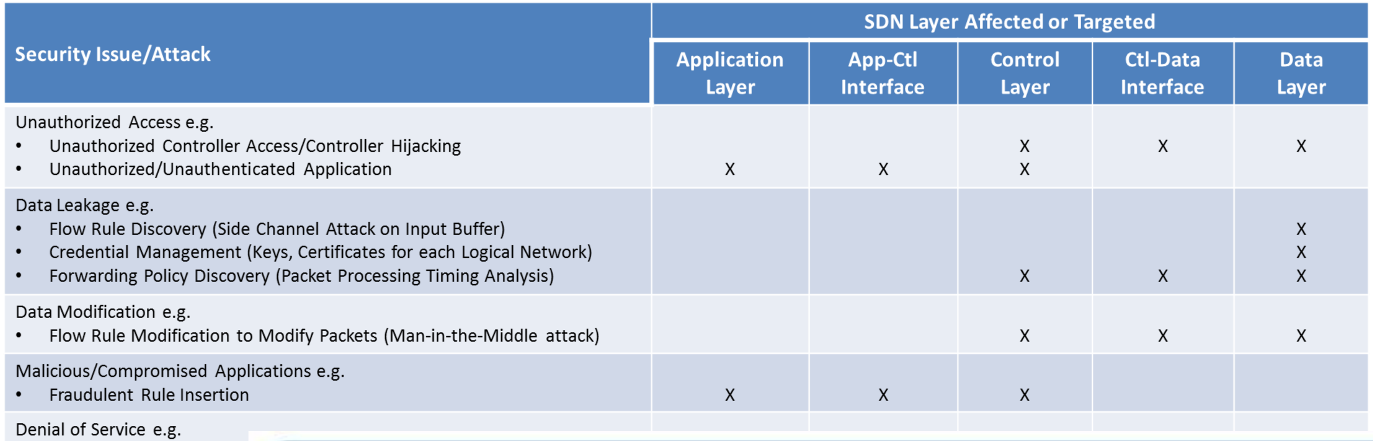
Gregory Pickett, head of cyber-security operations for Hellfire Security's Managed Security Services, is doing demonstrations this week of a serious vulnerability involving the Open Network Install Environment (ONIE). ONIE is open source software, contributed by Cumulus Networks , that runs in firmware on a white box switch and allows users to deploy and change network operating systems without replacing hardware.

"The problem is, if this gets compromised, it also makes it possible for hackers to install malware onto the switch," says Pickett in an abstract for a presentation he plans to deliver at the Black Hat security conference Thursday, and again at Def Con on Saturday.

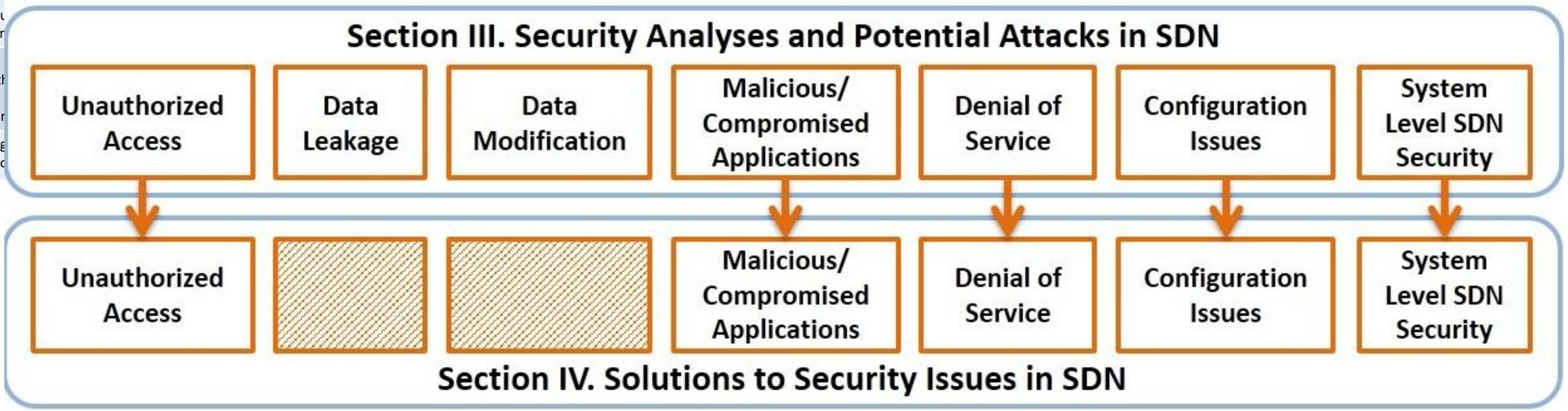
And the malware can remain persistent even after a network operating system re-install, Pickett says.

Solutions to Security Issues

Solutions to Security Issues - Analysis



Security Issue/Attack	SDN Layer Affected or Targeted				
	Application Layer	App-Ctl Interface	Control Layer	Ctl-Data Interface	Data Layer
Unauthorized Access e.g.					
• Unauthorized Controller Access/Controller Hijacking			X	X	X
• Unauthorized/Unauthenticated Application	X	X	X		
Data Leakage e.g.					
• Flow Rule Discovery (Side Channel Attack on Input Buffer)					X
• Credential Management (Keys, Certificates for each Logical Network)					X
• Forwarding Policy Discovery (Packet Processing Timing Analysis)			X	X	X
Data Modification e.g.					
• Flow Rule Modification to Modify Packets (Man-in-the-Middle attack)			X	X	X
Malicious/Compromised Applications e.g.					
• Fraudulent Rule Insertion	X	X	X		
Denial of Service e.g.					
• Controller-Switch Commu					
• Switch Flow Table Floodir					
Configuration Issues e.g.					
• Lack of TLS (or other Auth					
• Policy Enforcement					
• Lack of Secure Provisionir					
System Level SDN Security e.g					
• Lack of Visibility of Netwo					



Section III. Security Analyses and Potential Attacks in SDN
Unauthorized Access
Data Leakage
Data Modification
Malicious/ Compromised Applications
Denial of Service
Configuration Issues
System Level SDN Security
Unauthorized Access
Malicious/ Compromised Applications
Denial of Service
Configuration Issues
System Level SDN Security
Section IV. Solutions to Security Issues in SDN

Categorization of Security Solutions

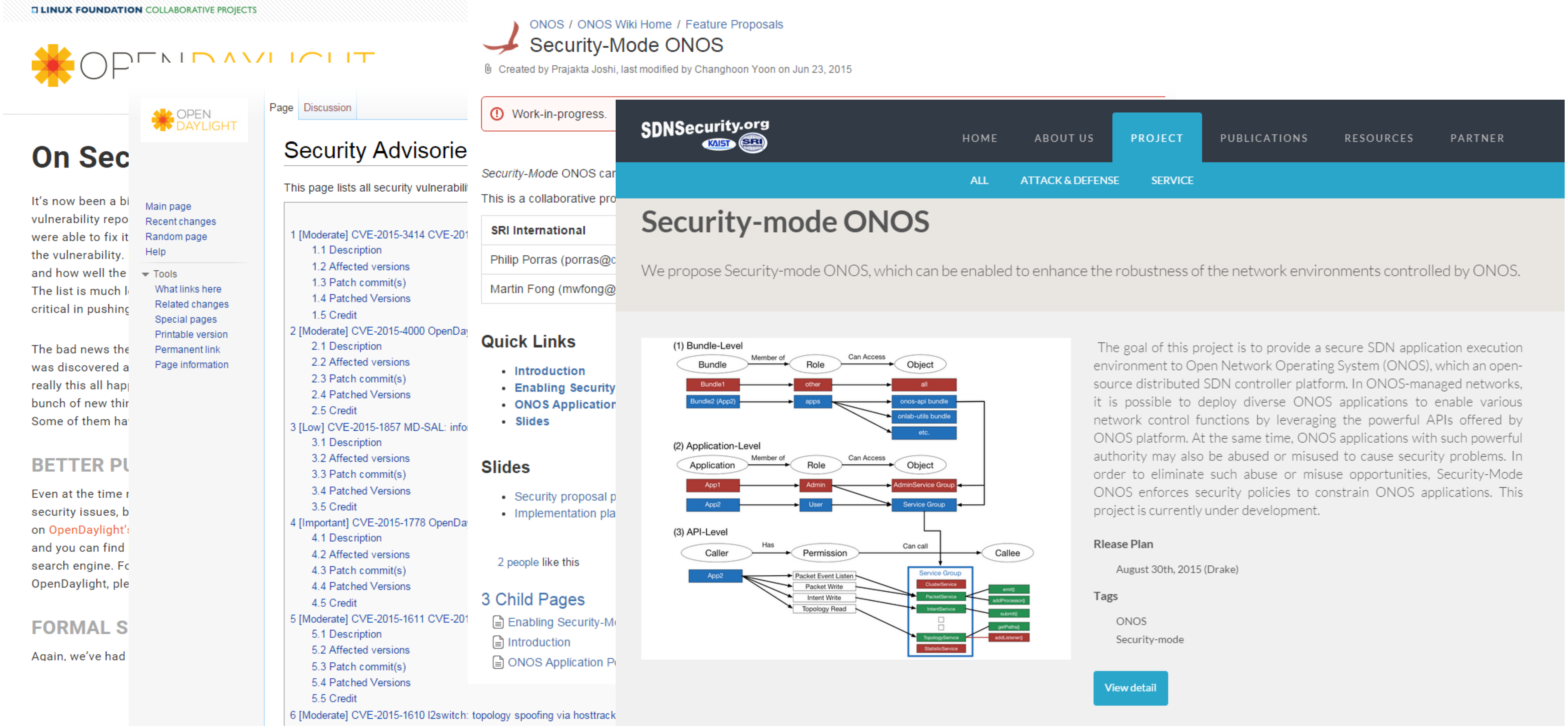
Solution to Security Issue	**Research Work**	**SDN Layer/Interface**				
		App	App-Ctl	Ctl	Ctl-Data	Data
Unauthorized Access	Securing Distributed Control, Byzantine-Resilient SDN			X	X	
	Authentication for Resilience			X		
	PermOF	X	X			
	OperationCheckpoint	X	X	X		
	SE-Floodlight	X	X	X	X	
	AuthFlow	X		X	X	X
Data Leakage						
Data Modification						
Malicious Applications	FortNox	X	X	X	X	
	ROSEMARY	X		X		
	LegoSDN	X	X	X		
Denial of Service	AVANT-GUARD, CPRecovery			X	X	X
	VAVE	X		X	X	X
	Delegating Network Security	X	X	X	X	X
Configuration Issues	NICE	X	X		X	
	FlowChecker, Flover, Anteater, VeriFlow, NetPlumber	X	X	X	X	
	Security-Enhanced Firewall, FlowGuard, LPM	X		X	X	X
	Frenetic, Flow-Based Policy, Consistent Updates	X	X	X	X	
	Shared Data Store	X		X	X	X
	Splendid Isolation		X	X		
	Verificare, Machine-Verified SDN, VeriCon		X	X	X	
System Level SDN Security	Debugger for SDN	X			X	
	OFHIP, Secure-SDMN				X	
	FRESCO	X	X	X	X	

SDN Controller Security

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)

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

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 r
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

- Main page
- Recent changes
- Random page
- Help

▾ Tools

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

Security Advisorie

This page lists all security vulnerabili

- 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 OpenDa
  - 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 can

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

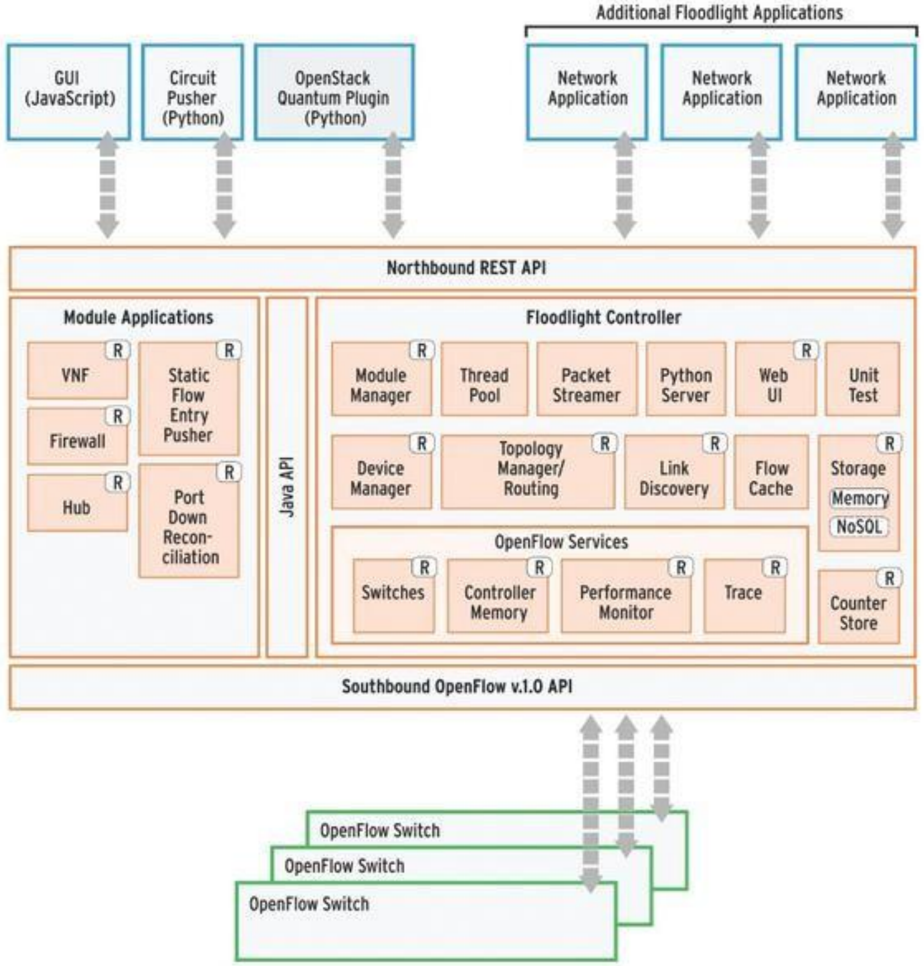
August 30th, 2015 (Drake)

Tags

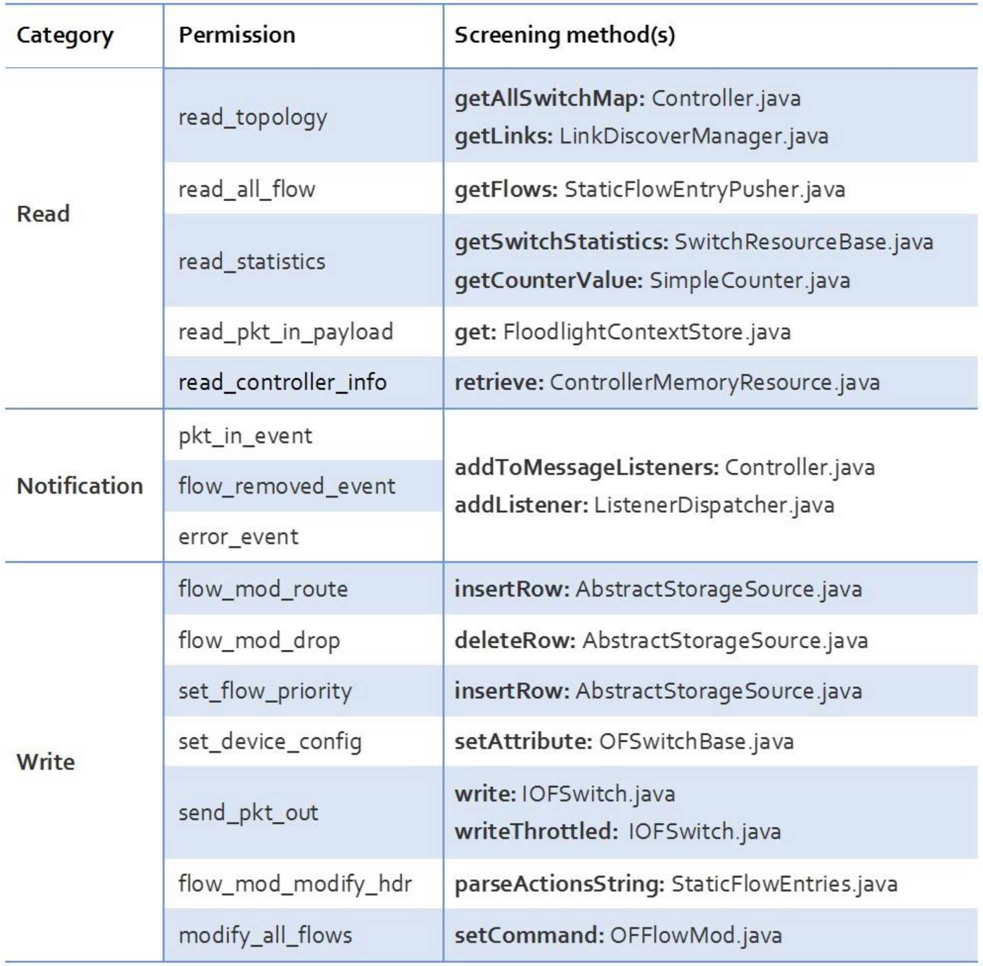
ONOS
Security-mode

View detail

SDN Application Control



OpenFlow Controller Article, Floodlight Architecture and Relationships, http://www.admin-magazine.com/

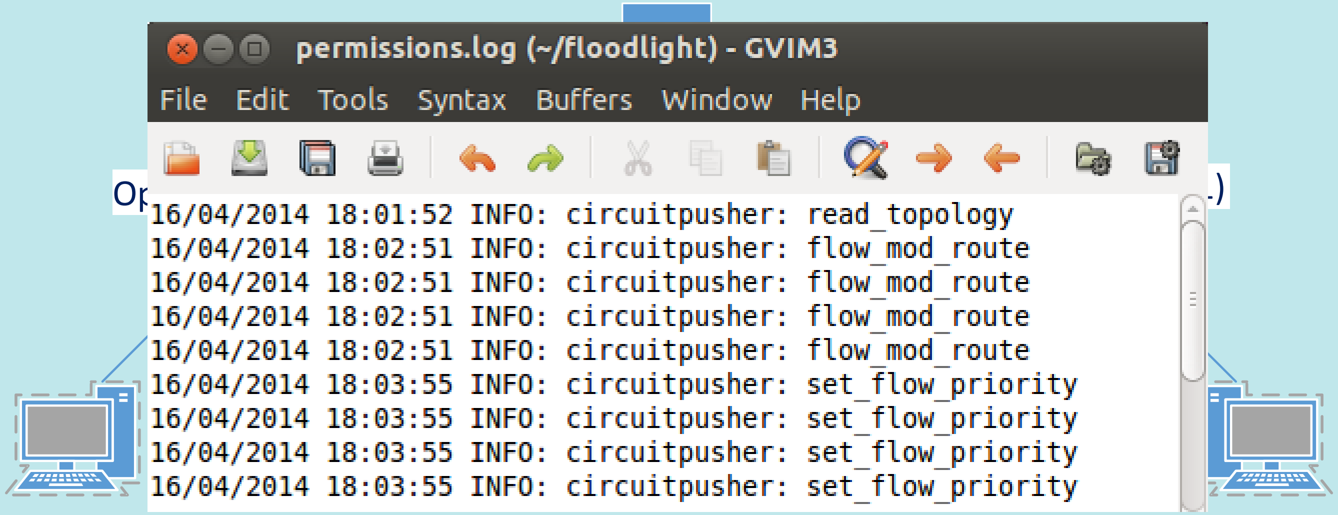


Category	Permission	Screening method(s)
Read	read_topology	**getAllSwitchMap:** Controller.java **getLinks:** LinkDiscoverManager.java
	read_all_flow	**getFlows:** StaticFlowEntryPusher.java
	read_statistics	**getSwitchStatistics:** SwitchResourceBase.java **getCounterValue:** SimpleCounter.java
	read_pkt_in_payload	**get:** FloodlightContextStore.java
	read_controller_info	**retrieve:** ControllerMemoryResource.java
Notification	pkt_in_event flow_removed_event error_event	**addToMessageListeners:** Controller.java **addListener:** ListenerDispatcher.java
Write	flow_mod_route	**insertRow:** AbstractStorageSource.java
	flow_mod_drop	**deleteRow:** AbstractStorageSource.java
	set_flow_priority	**insertRow:** AbstractStorageSource.java
	set_device_config	**setAttribute:** OFSwitchBase.java
	send_pkt_out	**write:** IOFSwitch.java **writeThrottled:** IOFSwitch.java
	flow_mod_modify_hdr	**parseActionsString:** StaticFlowEntries.java
	modify_all_flows	**setCommand:** OFFlowMod.java

OperationCheckpoint - CircuitPusher Example

CircuitPusher …"utilizes Floodlight REST APIs to create a bidirectional circuit, i.e. permanent flow entry, on all switches in route between two devices based on IP addresses with specified priority"

Floodlight (10.80.80.12)



permissions.log (~/floodlight) - GVIM3
File Edit Tools Syntax Buffers Window Help
Op
.)

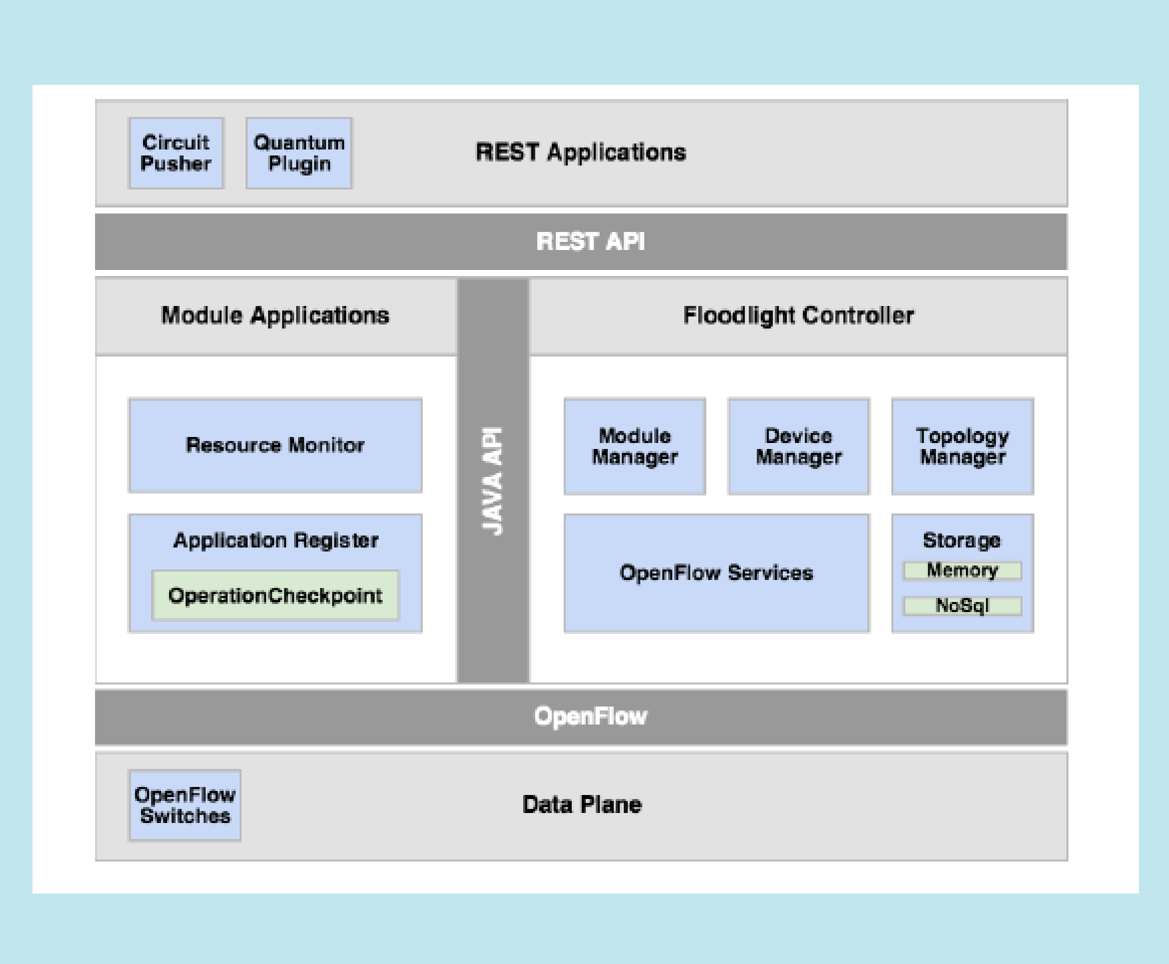
```
16/04/2014 18:01:52 INFO: circuitpusher: read_topology
16/04/2014 18:02:51 INFO: circuitpusher: flow_mod_route
16/04/2014 18:02:51 INFO: circuitpusher: flow_mod_route
16/04/2014 18:02:51 INFO: circuitpusher: flow_mod_route
16/04/2014 18:02:51 INFO: circuitpusher: flow_mod_route
16/04/2014 18:03:55 INFO: circuitpusher: set_flow_priority
16/04/2014 18:03:55 INFO: circuitpusher: set_flow_priority
16/04/2014 18:03:55 INFO: circuitpusher: set_flow_priority
16/04/2014 18:03:55 INFO: circuitpusher: set_flow_priority
```

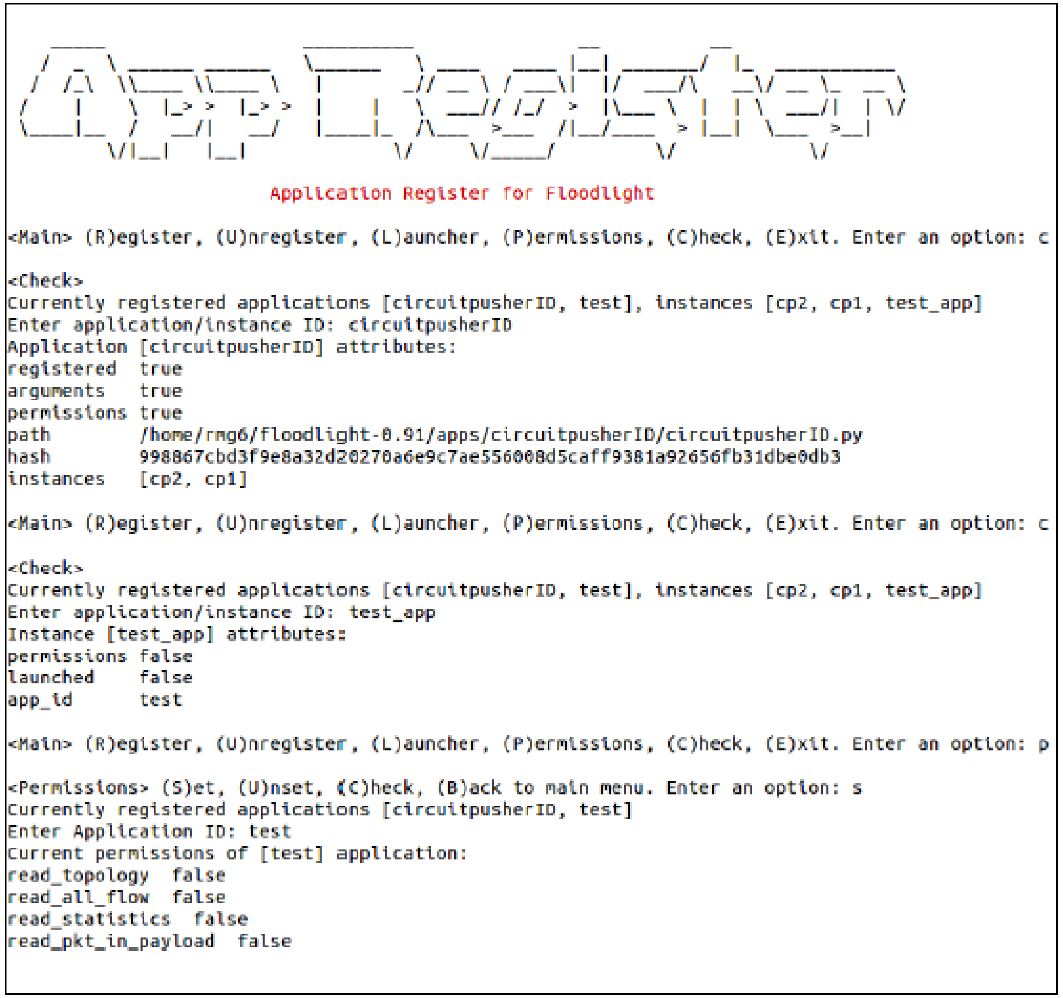
Host (10.80.81.45)

Host (10.80.81.55)

S. Scott-Hayward, C. Kane, S. Sezer, 'Operation Checkpoint: SDN Application Control', IEEE 22nd International Conference on Network Protocols (ICNP), 2014.

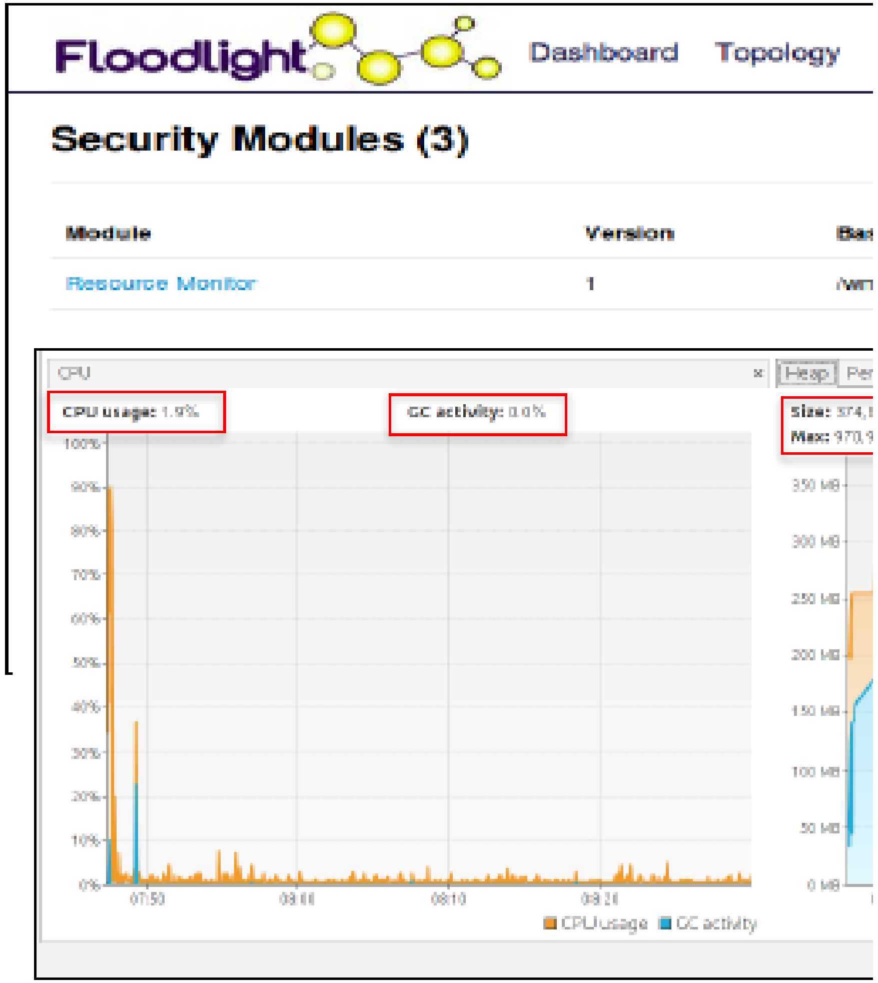
App Register/Resource Monitor





```
                    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/rmg6/floodlight-0.91/apps/circuitpusherID/circuitpusherID.py
hash        998867cbd3f9e8a32d20270a6e9c7ae556008d5caff9381a92656fb31dbe0db3
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: p

<Permissions> (S)et, (U)nset, (C)heck, (B)ack to main menu. Enter an option: s
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
```

App Register/Resource Monitor



Security Modules (3)

Module	Version	Bas
Resource Monitor	1	/wr

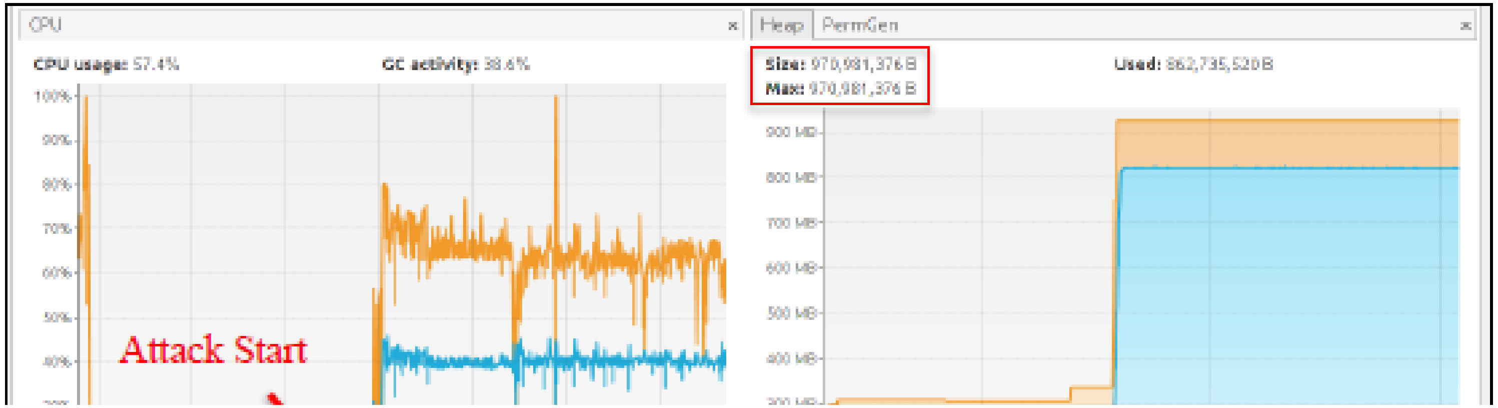
CPU usage: 1.9%

GC activity: 0.0%

Size: 374,

Max: 970,9

Floodlight Regular Reso



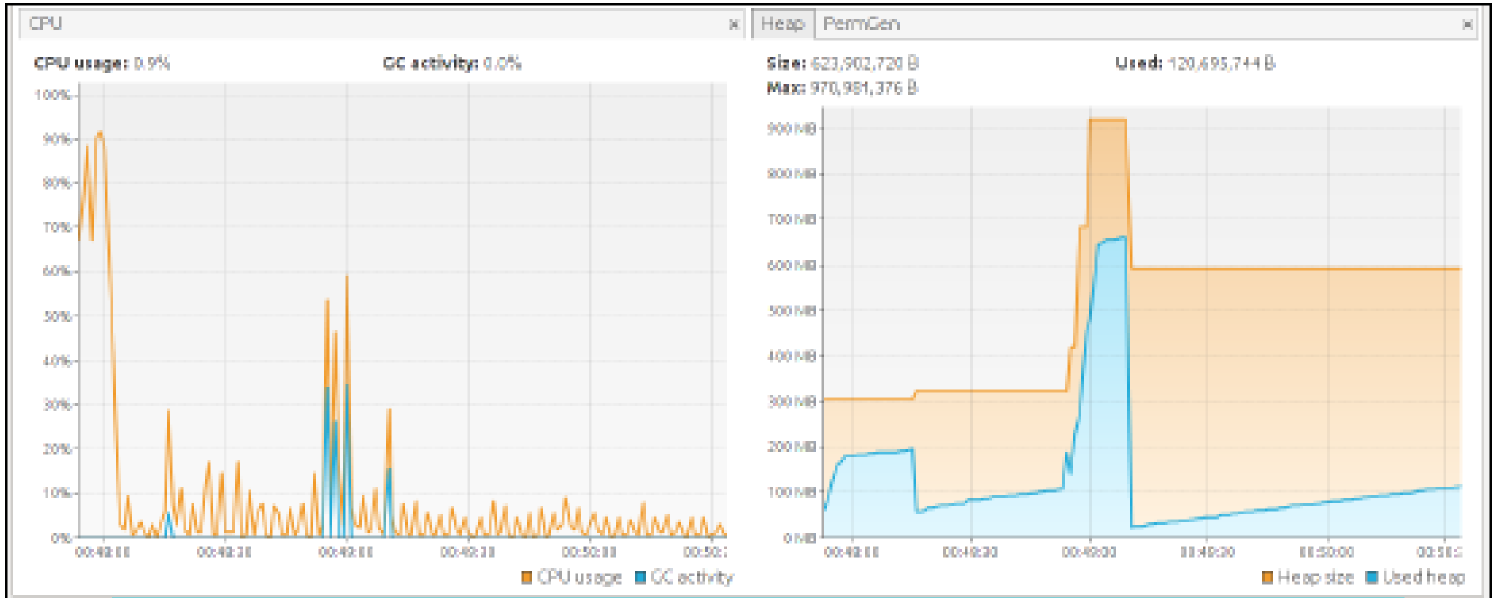
CPU usage: 57.4%

GC activity: 38.6%

Size: 970,981,376 B

Max: 970,981,376 B

Used: 862,735,520 B



CPU usage: 0.9%

GC activity: 0.0%

Size: 623,902,720 B

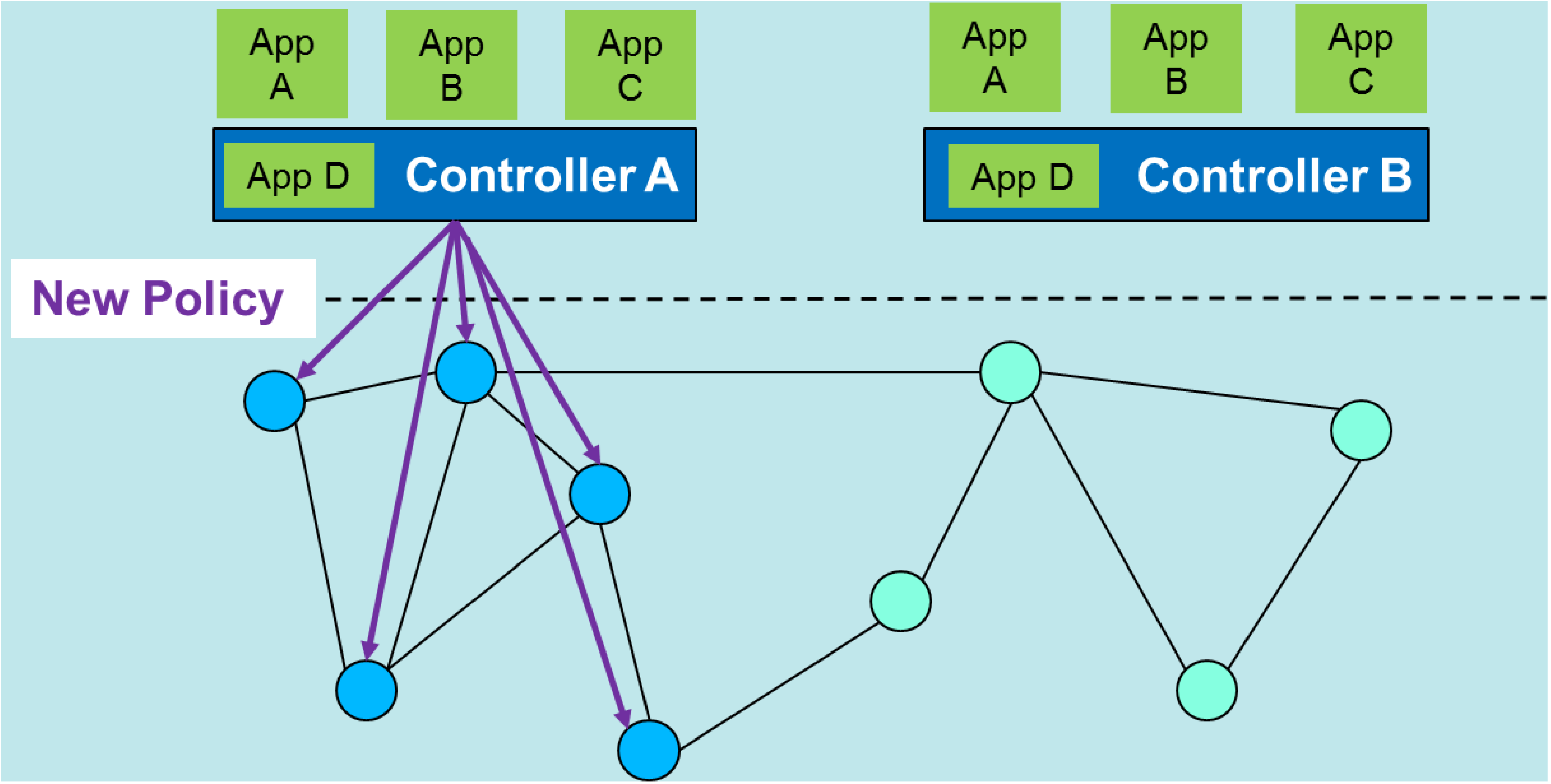
Max: 970,981,376 B

Used: 120,695,744 B

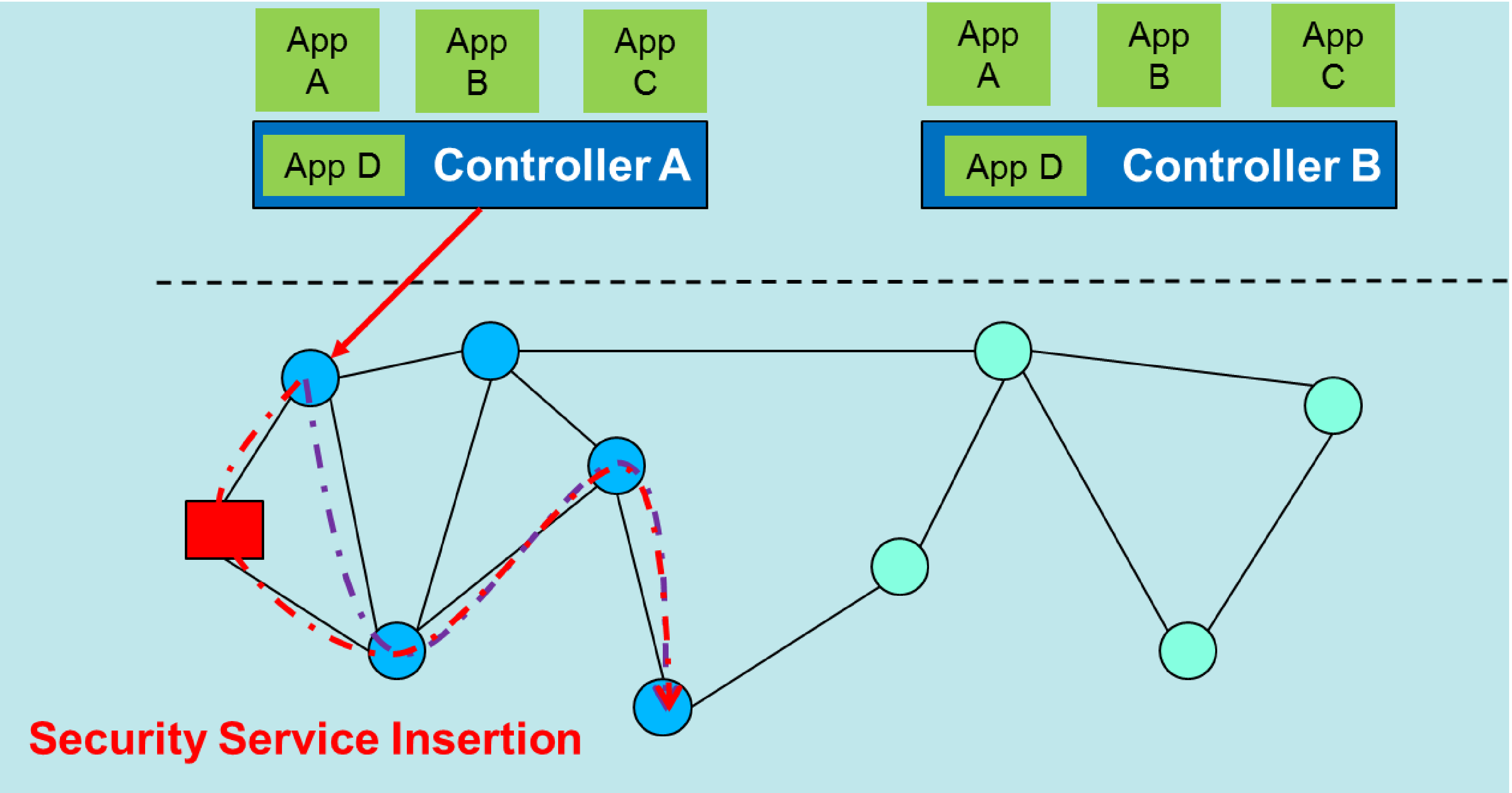
Memory Exhaustion Attack killed by Resource Monitor

SDN Security Enhancements

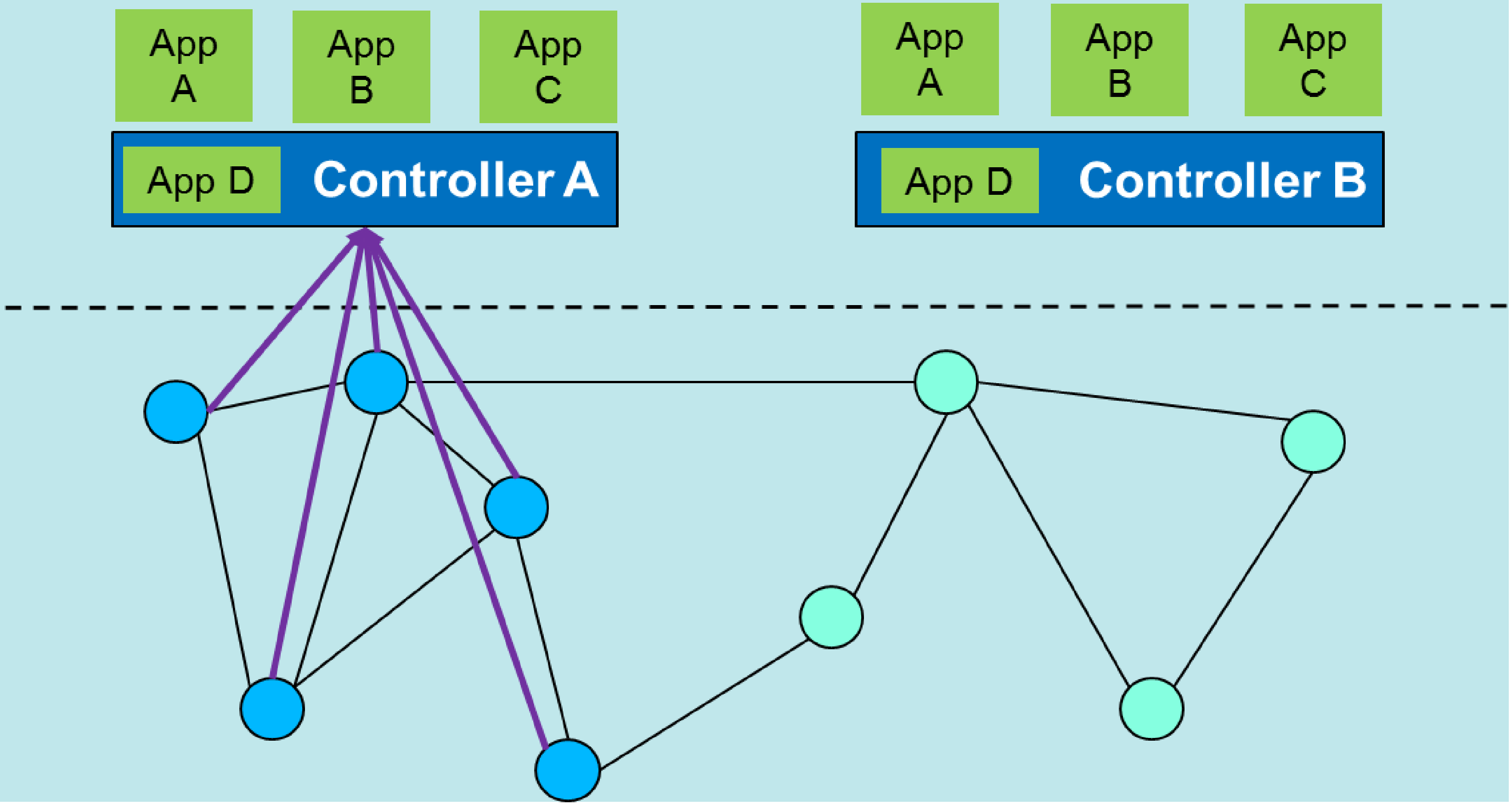
SDN Security Enhancements



SDN Security Enhancements



Network Forensics – Monitoring and Analysis

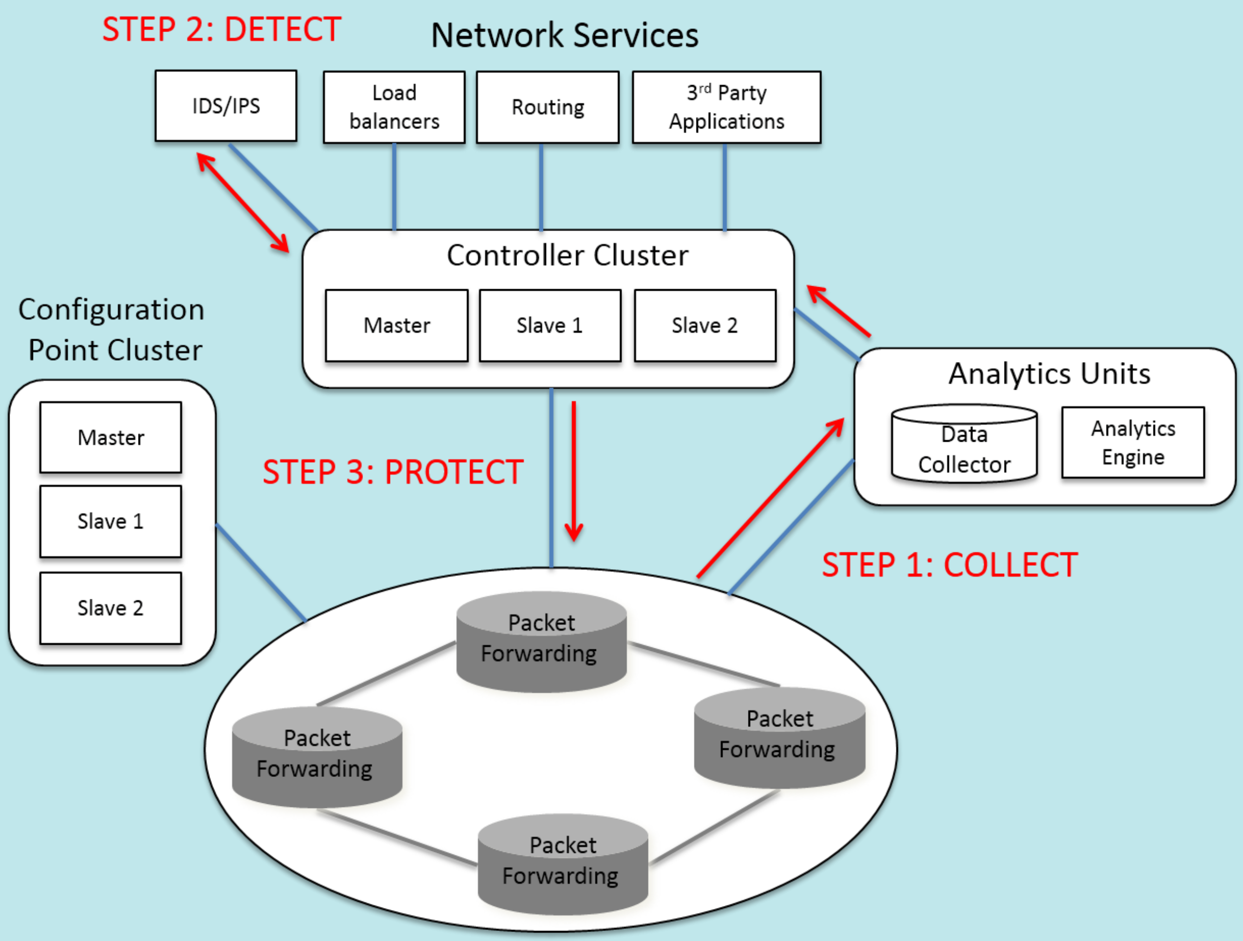


SDN Security Feedback Control

Step 1: Collect Network Statistics

Step 2: Detect anomalies or intrusions in the network

Step 3: Insert flow rules to protect the network

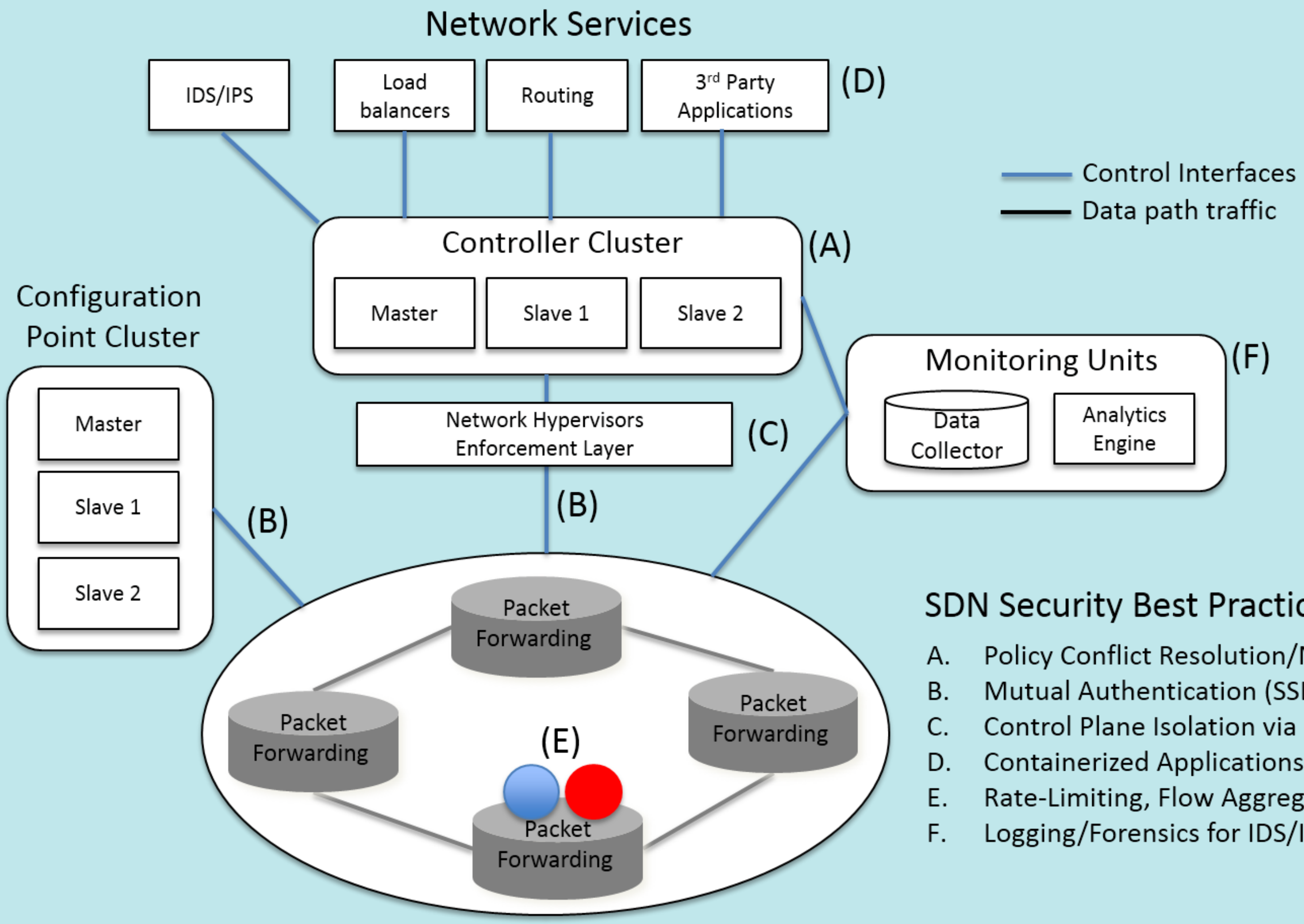


Categorization of Security Enhancements

Security Enhancement	Research Work	SDN Layer/Interface				
		App	App-Ctl	Ctl	Ctl-Data	Data
Collect, Detect, Protect	Combining OpenFlow/SFlow, Active Security	X		X	X	X
	Learning-IDS (L-IDS), NetFuse, OrchSec	X		X	X	X
	Cognition	X	X	X		
Traffic Analysis & Rule Updating	Resonance	X		X	X	X
	AVANT-GUARD, Pedigree, OF-RHM			X	X	X
	SDN-MTD	X		X	X	X
	NICE:NIDS, SnortFlow, SDNIPS, ScalableIDS	X		X	X	
	Revisiting Anomaly Detection	X		X	X	
	Fuzzy Logic SDN IDS	X		X	X	X
DoS/DDoS Protection	Lightweight DDoS	X		X	X	
	CONA, DDoS Defender, DDoS Blocker	X		X	X	X
Security Middleboxes – Architecture and Services	Slick, FlowTags	X	X	X	X	X
	SIMPLE-fying Middlebox	X		X		X
	OSTMA			X	X	X
	Covert Channel Protection	X		X	X	X
	OpenSAFE, CloudWatcher	X	X	X	X	
	Secure-TAS				X	X
	Secure Forensics				X	X
AAA	AAA SDN			X	X	X
	C-BAS	X	X	X	X	X
Secure, Scalable Multi-Tenancy	vCNSMS, OpenvNMS, Tualatin	X		X	X	X
	NetSecCloud	X		X		

Recommended Best Practices

Recommended Best Practices



SDN Security Best Practices

A. Policy Conflict Resolution/Network Invariant Detection
B. Mutual Authentication (SSL/TLS) – Access Control
C. Control Plane Isolation via Slicing
D. Containerized Applications - Access Control
E. Rate-Limiting, Flow Aggregation, Short Timeouts
F. Logging/Forensics for IDS/IPS

Industry/Standards Groups

Forum	Group Name	Launch Date	Objective	Proposed Output
ETSI	NFV Security Experts Group	Mar. 2013	Design security into NFV from the start and ensure security accreditation bodies address NFV	Document existing solutions/recommended practices and identify subsequent research requirements
ONF	Security Working Group	Apr. 2013	Define security requirements for OpenFlow SDN architecture	SDN Security Standards Documents Threat Model/Analysis Document
ITU-T	Study Group SG11/SG13 (SG17)	Jun. 2013	Contribute to standardization of SDN	Recommendations

ETSI ISG Network Functions Virtualization Security Expert Group (http://www.etsi.org/technologies-clusters/technologies/nfv)
Open Networking Foundation Security Working Group. (https://www.opennetworking.org/technical-communities/areas/services)
ITU-T SG13 Future Networks - Questions Under Study. (http://www.itu.int/en/ITU-T/studygroups/2013-2016/13/Pages/questions.aspx)

Recent Work:

- Principles and Practices for Securing Software Defined Networks
- Recommendations to Extensibility WG – Updates to OpenFlow Switch Specification v1.3.5
    - Specify that a secure version of TLS is recommended (EXT-525)
    - Clarify certificate configuration of the switch (EXT-304)
    - Specify that malformed packet refer to those in the datapath (EXT-528)
    - Specify how to deal with malformed OpenFlow messages (EXT-528)
    - Specify that counters must use the full bit range (EXT-529)
- Threat Analysis
- Florence: Security Assessment Tools for SDN

Thank You!
Questions?

Policy Conflict Resolution

Problem:

Verify that the current state of flow rules inserted in a switch's flow table(s) remain consistent with the current network security policy.

Evaluate the table against the non-bypass property: *every packet that goes from source IP [5,6] to destination IP 6 must be dropped* - (1) Coverage Violation, (2) Modify Violation (Src 5, Dst 7)

Flow Table	Condition				Action Set
	Field 1 Src IP	Field 2 Src Port	Field 3 Dst IP	Field 4 Dst Port	
1	5	[0,19]	6	[0,19]	{ (drop) }
1	5	[0,19]	[7,8]	[0,19]	{ (set field_1 10), (goto 2) }
1	6	[0,19]	[6,8]	[0,19]	{ (forward) }
2	[10,12]	[0,19]	[0,12]	[0,19]	{ (set field_3 6), (forward) }

SDN Application Control

Fundamental security challenge is the ability for a malicious application to access network state information and manipulate network traffic for nefarious purposes.

Weaknesses in current approach:

- No authentication of RESTful API commands
- No scheme to ensure rules installed do not overlap or interfere with one another
- Applications do not have to provide identity information
- No application regulation or behaviour inspection after installation

Potential Solutions:

- Rule conflict detection and correction
- Application identification and priority enforcement
- Malicious activity detection and mitigation