CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

ATTACKS AND VULNERABILITIES IN SDN

Secure Communications Network

Confidentiality

Integrity

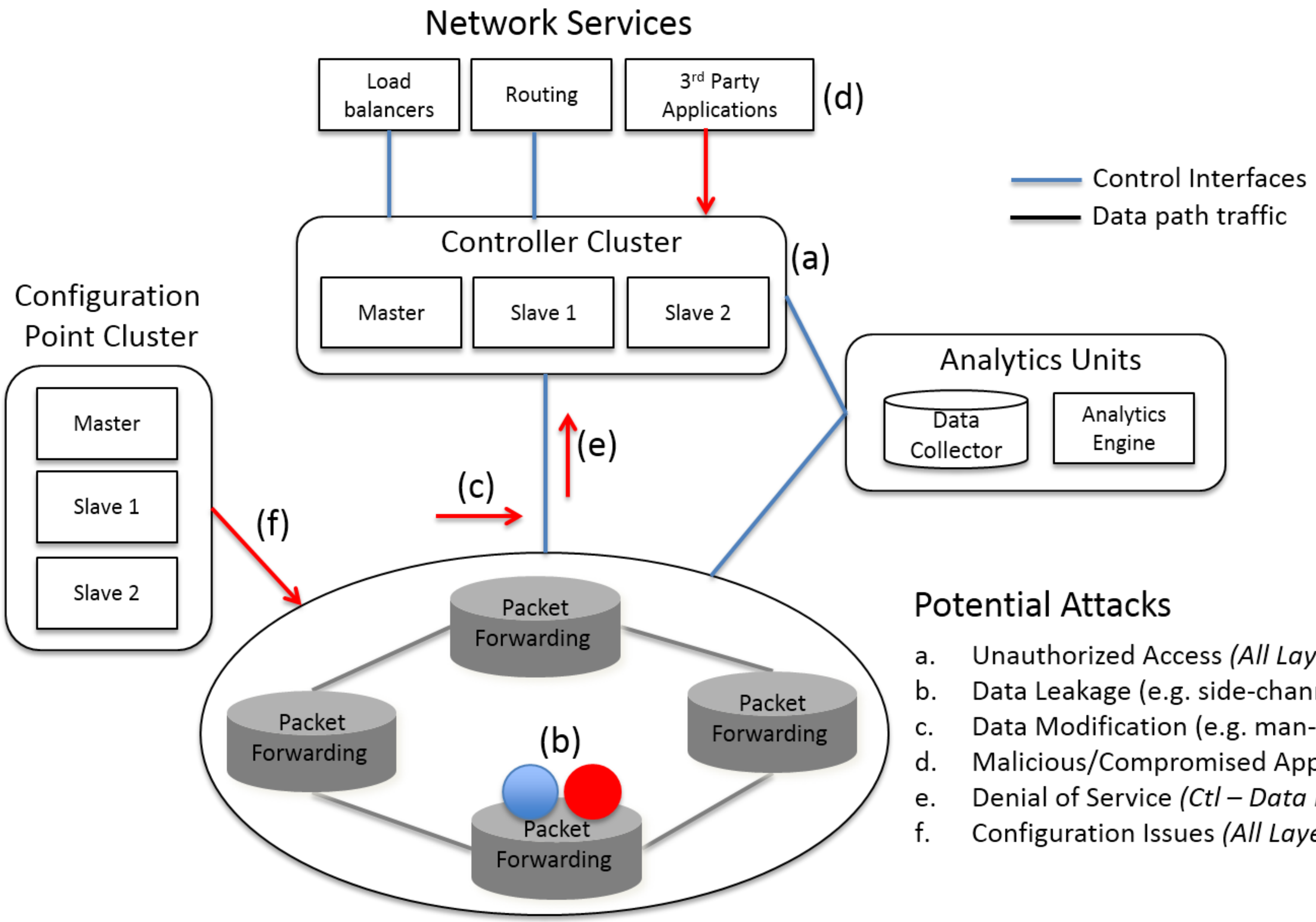
Availability of Information

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)*

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

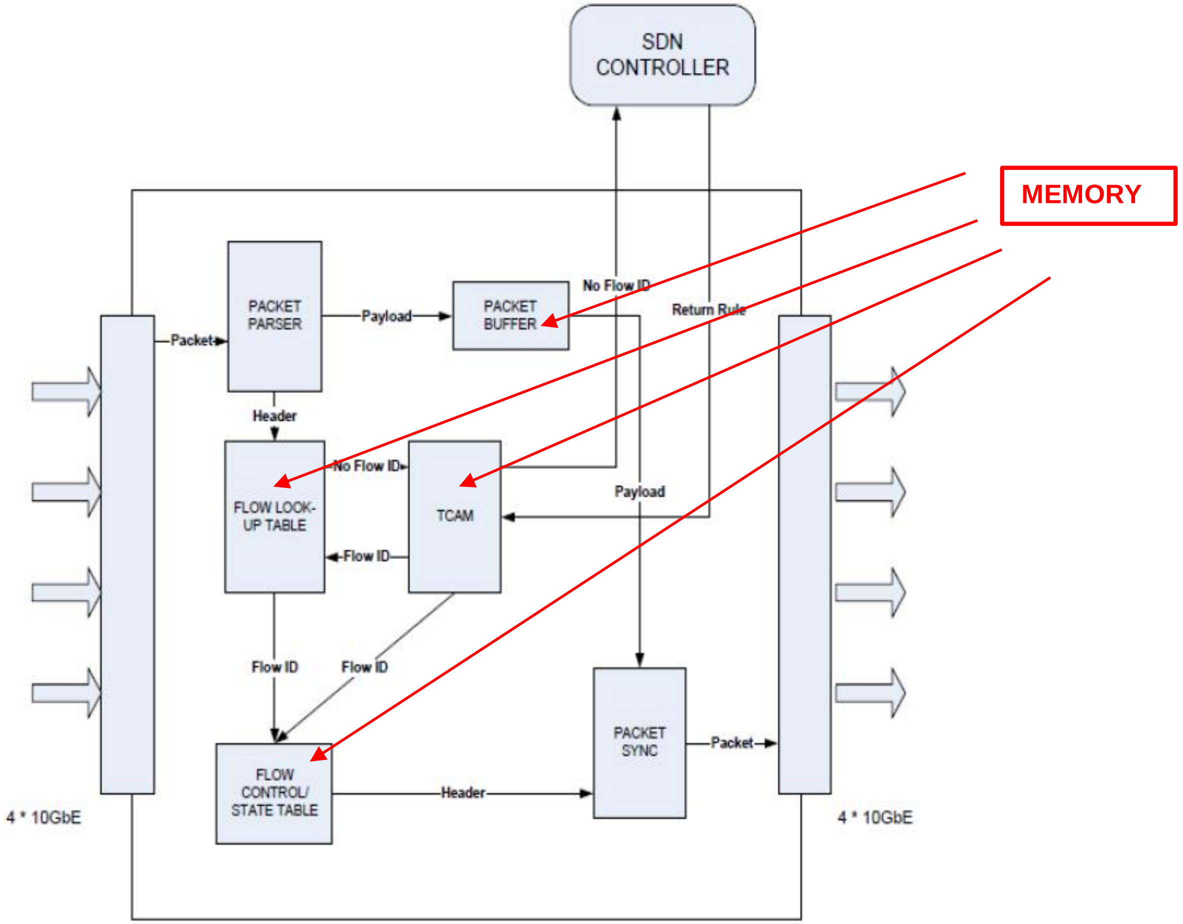
Categorization of Security Issues

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

Security Challenges with SDN

Increased potential for Denial of Service:

- Switch Buffer
- Flow Table
- State Table
- Data Flows/Processes



R. Kloti, ‘Openflow: A Security Analysis’, Swiss Federal Institute of Technology Zurich, Zurich, Switzerland, 2013.

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

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 $\textit{field}_1$ 10), (goto 2) }
1	6	[0,19]	[6,8]	[0,19]	{ (forward) }
2	[10,12]	[0,19]	[0,12]	[0,19]	{ (set $\textit{field}_3$ 6), (forward) }

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

SDN Control Plane Attacks – Service Chain Attack

Control Message Drop

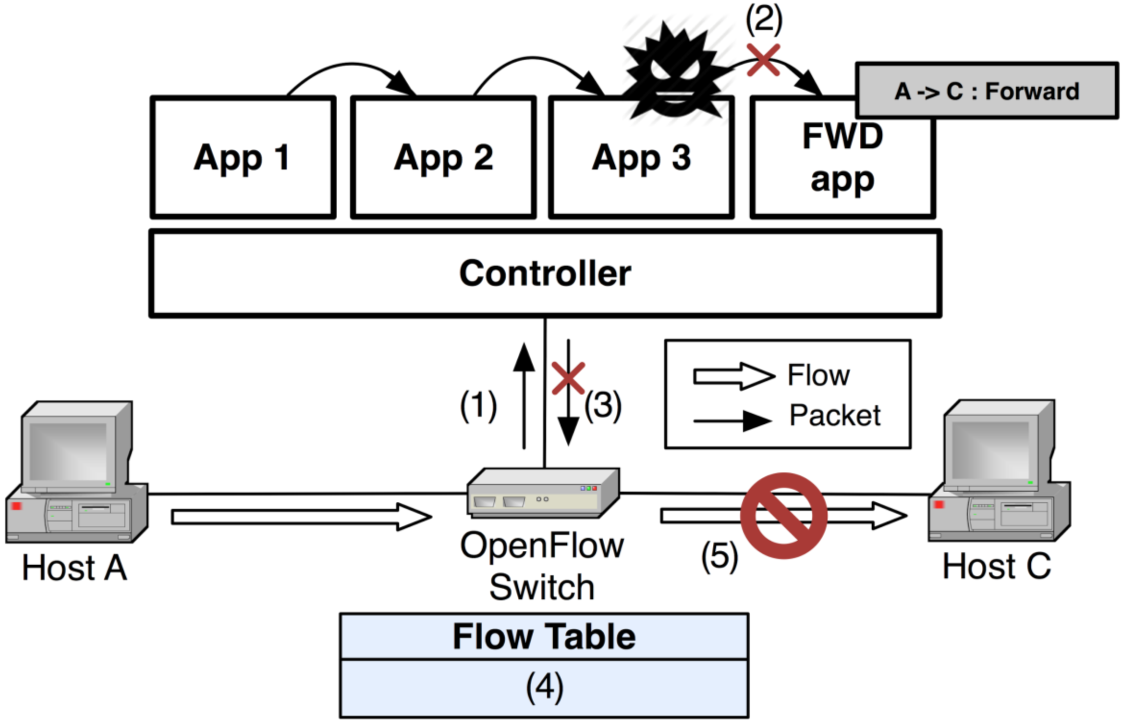
(1) Packet-In to Controller; Pkt-In passed to App 1, App 2, App 3 as per service chain;

(2) App 3 (malicious) drops Pkt-In w/out passing to FWD app;

(3) FWD app does not reply to Pkt-In;

(4) No flow rule installed in OF switch;

(5) Host A cannot communicate with Host C



Infinite Loop Attack

App 3 programmed to fall into an infinite loop leading the controller instance to freeze.

http://sdnsecurity.org

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

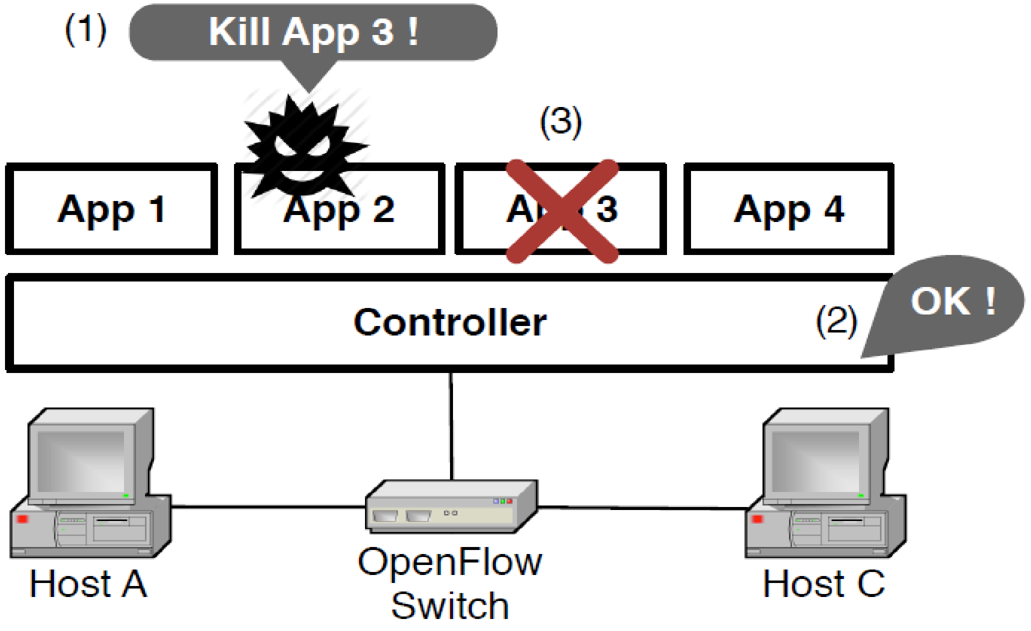
SDN Control Plane Attacks – Northbound API Abuse

Application Eviction

(1) App 2 (malicious) calls function to terminate App 3 via Northbound API;

(2) Controller accepts the App 3 termination request;

(3) Innocent App 3 terminated;



http://sdnsecurity.org

SDN Control Plane Attacks – Resource Exhaustion

Memory Leakage Attack

(1) App continuously allocates memory;

(2) System resource is increasingly consumed;

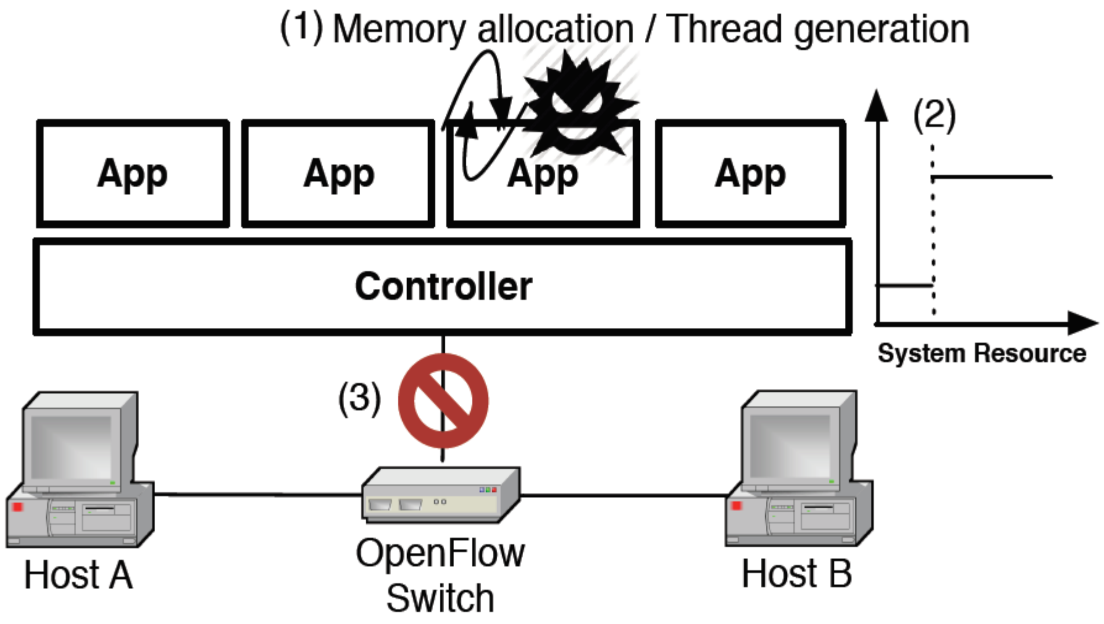
(3) Loss of control plane functionality and connection to data plane devices.

Create Thread Attack

(1) SDN App continuously generates threads'

(2) Computing power is increasingly absorbed;

(3) Loss of control plane functionality and connection to data plane devices.



http://sdnsecurity.org

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Open Network Install Environment (ONIE) Weaknesses

ONIE – Firmware for bare metal network switches

Weaknesses (Operating System) e.g.

- Privileged Accounts (No Root p/w, Doesn't force you to change it!)

Weaknesses (Installer) e.g.

- Predictable URLS, No encryption or authentication for Installs

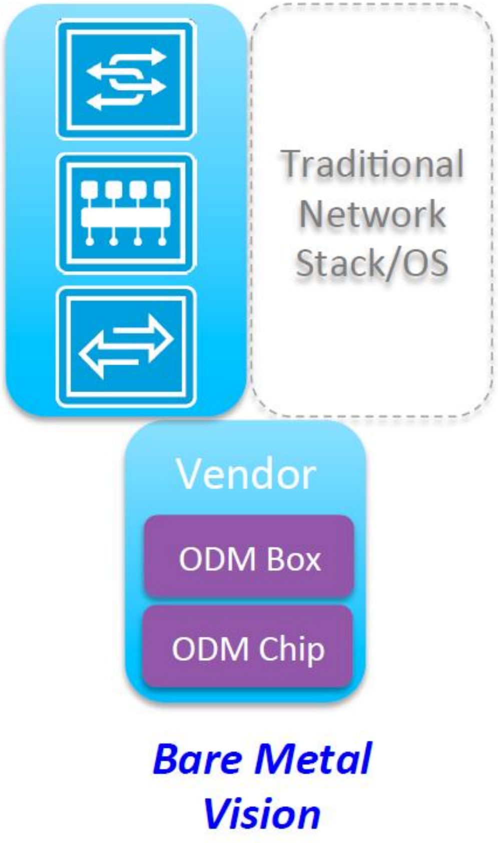
Weaknesses (Implementation) e.g.

- Exposed Partition, No Secure Boot

⇒ Compromise installations (via rogue dhcp server, IPv6 neighbour, TFTP)

⇒ Compromise It (forced reboot entry, sniffing/MITM)

⇒ Compromise It – Get past NOS, Modify ONIE, Into Firmware … forever!



Gregory Pickett, "Staying Persistent in Software Defined Networks," DefCon 23, Las Vegas 2015, https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/Speaker%20&%20Workshop%20Materials/Gregory%20Pickett/DEFCON-23-Gregory-Pickett-Staying-Persistant-in-Software-Def.pdf

ONIE-Compatible Network Operating System Weaknesses

ONIE – Compatible Distributions:

Open Network Linux, Switch Light, Cumulus Linux, MLNX-OS

Weaknesses (Agent) e.g.

- No encryption and no authentication, Out-Dated OpenSSL

⇒ Potential Topology, Flow, and Message Modification through Unauthorized Access

⇒ Potential Information Disclosure through Exploitation

- Run as root, Vulnerable Code

Gregory Pickett, "Staying Persistent in Software Defined Networks," DefCon 23, Las Vegas 2015, https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/Speaker%20&%20Workshop%20Materials/Gregory%20Pickett/DEFCON-23-Gregory-Pickett-Staying-Persistant-in-Software-Def.pdf

ONIE-Compatible Network Operating System Weaknesses

ONIE – Compatible Distributions:

Open Network Linux, Switch Light, Cumulus Linux, MLNX-OS

Weaknesses (Operating System) e.g.

- Out-Dated Bash, Default (and fixed) privileged accounts
- No forced change on default p/w, easy escape to shell, instant elevation

⇒ Potential full control of your network through Unauthorized Access

⇒ Potential compromise of firmware through Unauthorized Access

Gregory Pickett, “Staying Persistent in Software Defined Networks,” DefCon 23, Las Vegas 2015, https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/Speaker%20&%20Workshop%20Materials/Gregory%20Pickett/DEFCON-23-Gregory-Pickett-Staying-Persistant-in-Software-Def.pdf

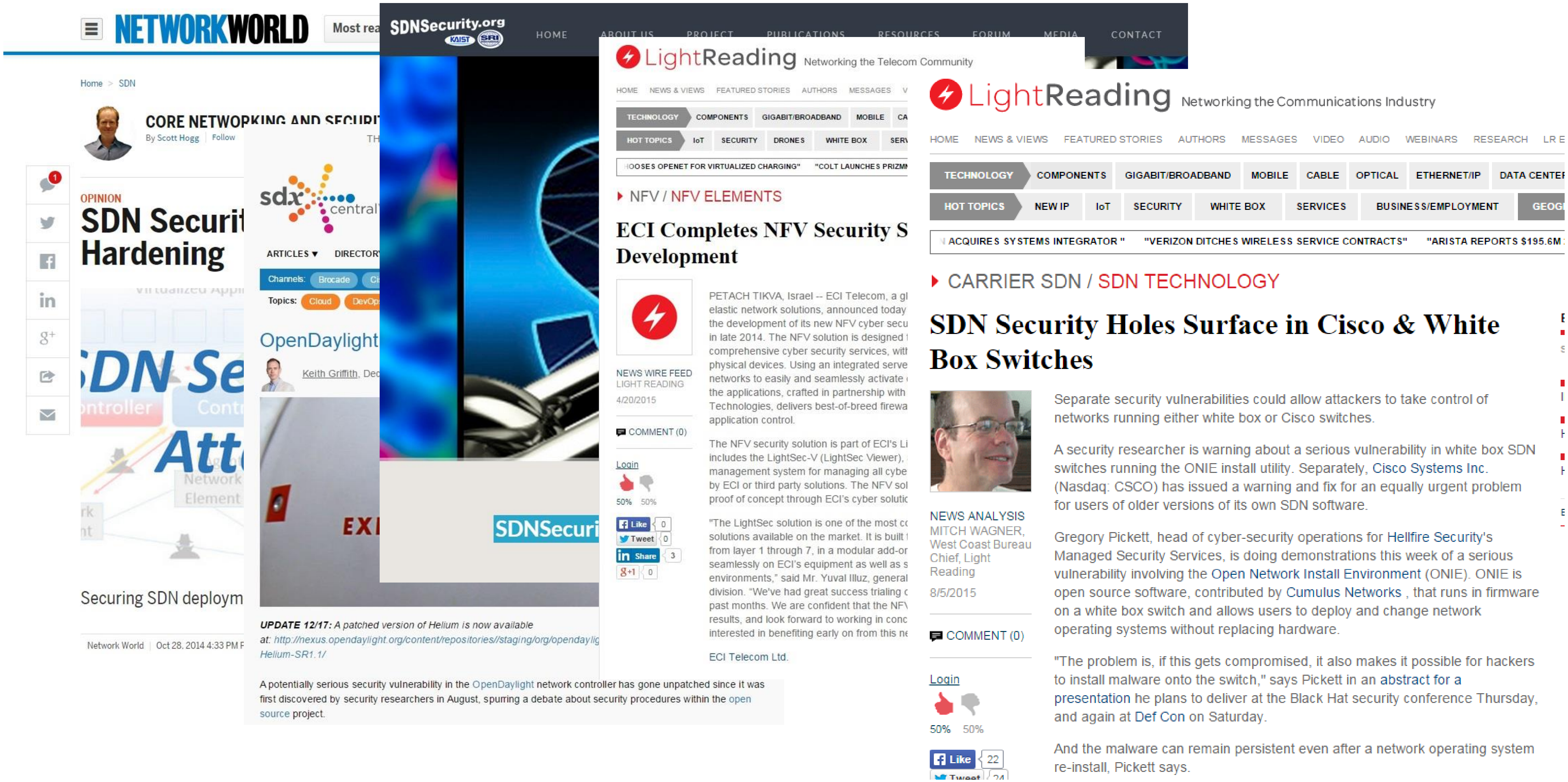
Available Solutions

Available Solutions:

- Hardware (Trusted Platform Module)
- Install Environment (Increase key entropy, force p/w change, sign installations)
- Network Operating Systems (changeable names, force p/w change, tighten shell access)
- Agents (use TLS, add encryption and authentication, coordinate certificate/key distribution)
- Enterprise Architecture (isolate management plane, audit switches)

Gregory Pickett, “Staying Persistent in Software Defined Networks,” DefCon 23, Las Vegas 2015, https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/Speaker%20&%20Workshop%20Materials/Gregory%20Pickett/DEFCON-23-Gregory-Pickett-Staying-Persistant-in-Software-Def.pdf

SDN Security … focus since Q4 2014



SDN Securit Hardening

Securing SDN deploym

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

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 RESOURCES FORUM MEDIA CONTACT
SDNSecuri

LightReading Networking the Telecom Community
HOME NEWS & VIEWS FEATURED STORIES AUTHORS MESSAGES V
TECHNOLOGY COMPONENTS GIGABIT/BROADBAND MOBILE CA
HOT TOPICS IoT SECURITY DRONES WHITE BOX SERV
HOOSES OPENET FOR VIRTUALIZED CHARGING" "COLT LAUNCHES PRIZM
NFV / NFV ELEMENTS

ECI Completes NFV Security S Development

NEWS WIRE FEED
LIGHT READING
4/20/2015

COMMENT (0)

Login
50% 50%
Like 0
Tweet 0
Share 3
g+1 0

PETACH TIKVA, Israel -- ECI Telecom, a gl elastic network solutions, announced today the development of its new NFV cyber secu in late 2014. The NFV solution is designed comprehensive cyber security services, with physical devices. Using an integrated serve networks to easily and seamlessly activate the applications, crafted in partnership with Technologies, delivers best-of-breed firewa application control.

The NFV security solution is part of ECI's Li includes the LightSec-V (LightSec Viewer), management system for managing all cybe by ECI or third party solutions. The NFV sol proof of concept through ECI's cyber solutic

"The LightSec solution is one of the most co solutions available on the market. It is built from layer 1 through 7, in a modular add-or seamlessly on ECI's equipment as well as s environments," said Mr. Yuval Illuz, general division. "We've had great success trialing c past months. We are confident that the NF results, and look forward to working in conc interested in benefiting early on from this ne

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
N 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.

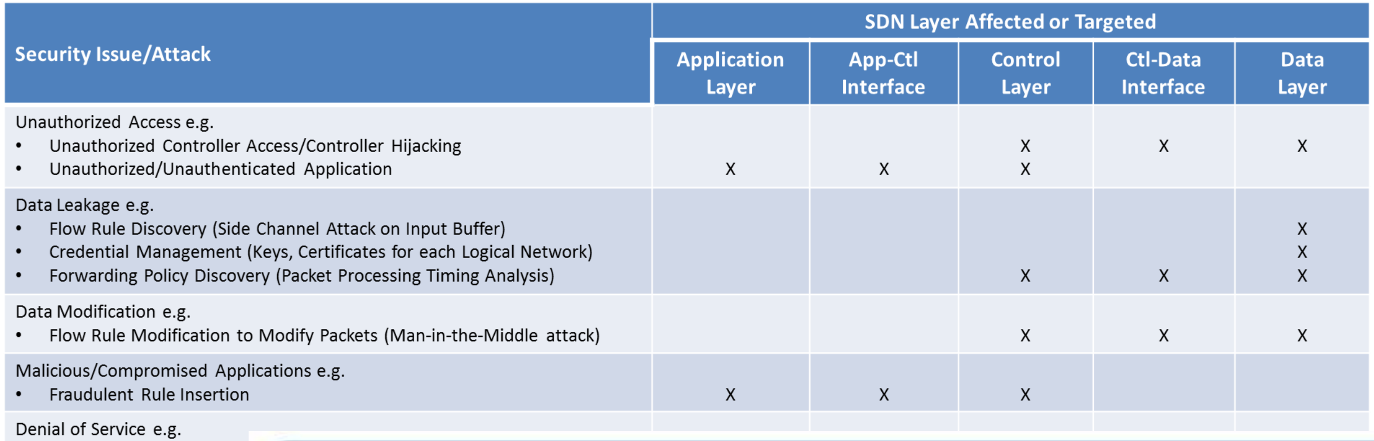
Gregory Pickett, head of cyber-security operations for Hellfire Security's Managed Security Services, is doing demonstrations this week of a serious vulnerability involving the Open Network Install Environment (ONIE). ONIE is open source software, contributed by Cumulus Networks , that runs in firmware 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.

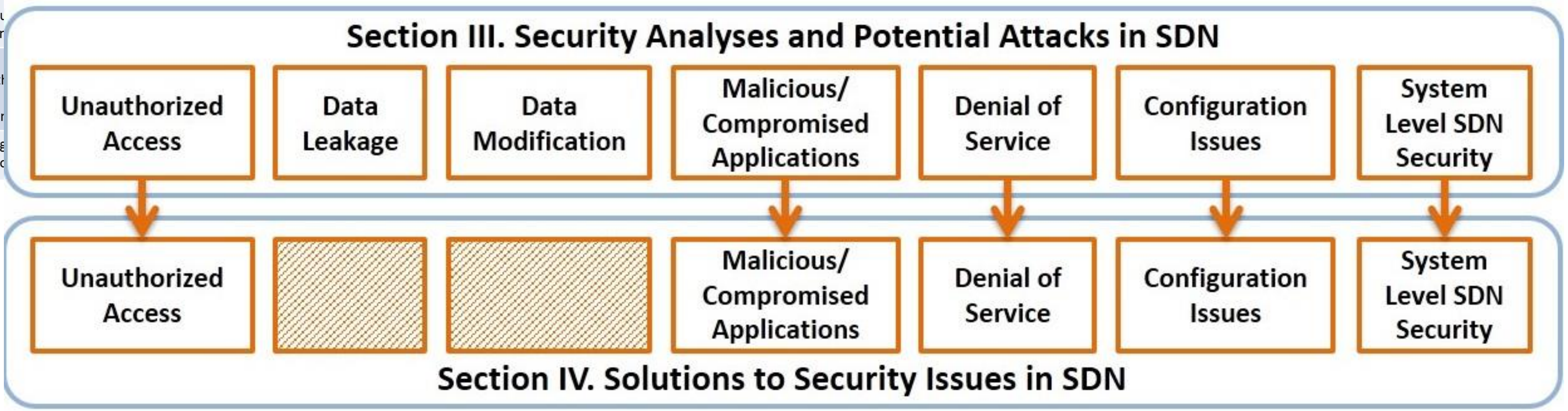
And the malware can remain persistent even after a network operating system re-install, Pickett says.

SOLUTIONS TO SECURITY ISSUES IN SDN

Solutions to Security Issues - Analysis



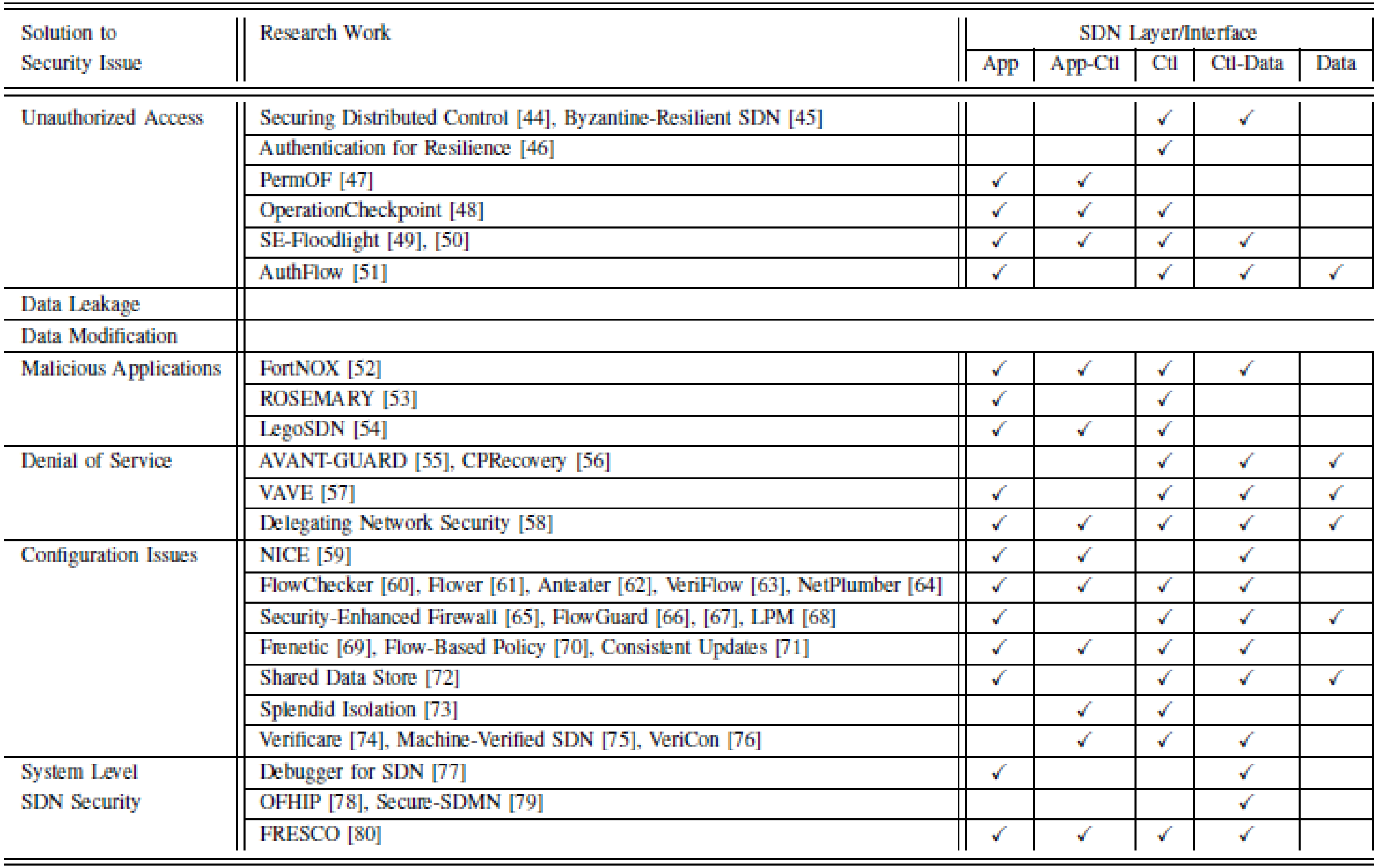
Security Issue/Attack	SDN Layer Affected or Targeted				
	Application Layer	App-Ctl Interface	Control Layer	Ctl-Data Interface	Data Layer
Unauthorized Access e.g. • Unauthorized Controller Access/Controller Hijacking • Unauthorized/Unauthenticated Application	 X	 X	 X X	 X	 X
Data Leakage e.g. • Flow Rule Discovery (Side Channel Attack on Input Buffer) • Credential Management (Keys, Certificates for each Logical Network) • Forwarding Policy Discovery (Packet Processing Timing Analysis)			 X	 X	 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

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

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 [44], Byzantine-Resilient SDN [45]			✓	✓	
	Authentication for Resilience [46]			✓		
	PermOF [47]	✓	✓			
	OperationCheckpoint [48]	✓	✓	✓		
	SE-Floodlight [49], [50]	✓	✓	✓	✓	
	AuthFlow [51]	✓		✓	✓	✓
Data Leakage						
Data Modification						
Malicious Applications	FortNOX [52]	✓	✓	✓	✓	
	ROSEMARY [53]	✓		✓		
	LegoSDN [54]	✓	✓	✓		
Denial of Service	AVANT-GUARD [55], CPRecovery [56]			✓	✓	✓
	VAVE [57]	✓		✓	✓	✓
	Delegating Network Security [58]	✓	✓	✓	✓	✓
Configuration Issues	NICE [59]	✓	✓		✓	
	FlowChecker [60], Flover [61], Anteater [62], VeriFlow [63], NetPlumber [64]	✓	✓	✓	✓	
	Security-Enhanced Firewall [65], FlowGuard [66], [67], LPM [68]	✓		✓	✓	✓
	Frenetic [69], Flow-Based Policy [70], Consistent Updates [71]	✓	✓	✓	✓	
	Shared Data Store [72]	✓		✓	✓	✓
	Splendid Isolation [73]		✓	✓		
	Verificare [74], Machine-Verified SDN [75], VeriCon [76]		✓	✓	✓	
System Level SDN Security	Debugger for SDN [77]	✓			✓	
	OFHIP [78], Secure-SDMN [79]				✓	
	FRESCO [80]	✓	✓	✓	✓	

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Mitigating SDN Architecture threats using standard technologies

E.g. SANE Security Analysis (similar OpenFlow Threat Analysis within ONF SecWG)

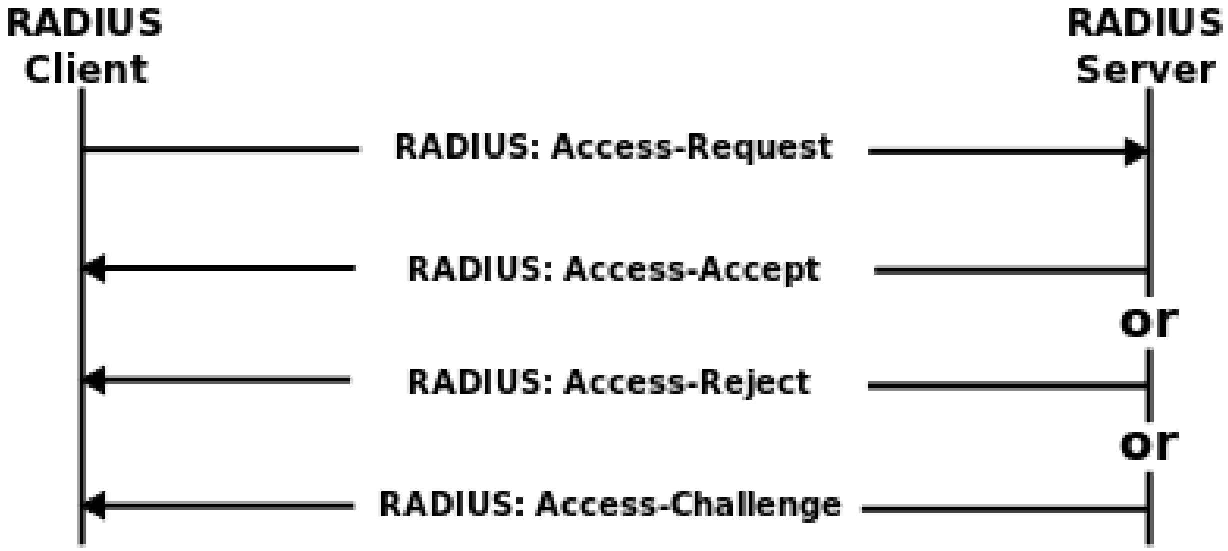
Threat Type	Data Flows	Data Stores	Processes	Interactors
Spoofing				-
Tampering	X[1]	X[2]		
Repudiation			X[4]	X[4]
Information Disclosure	X[1]	X[2,3]		
DoS	-	-	-	
Elevation of Privilege			X[5]	

[1]mitigated with IPSec, [2]mitigated with ACLs, [3]mitigated by not storing secrets, [4]auditing trails in logfile, [5]run with least privileges

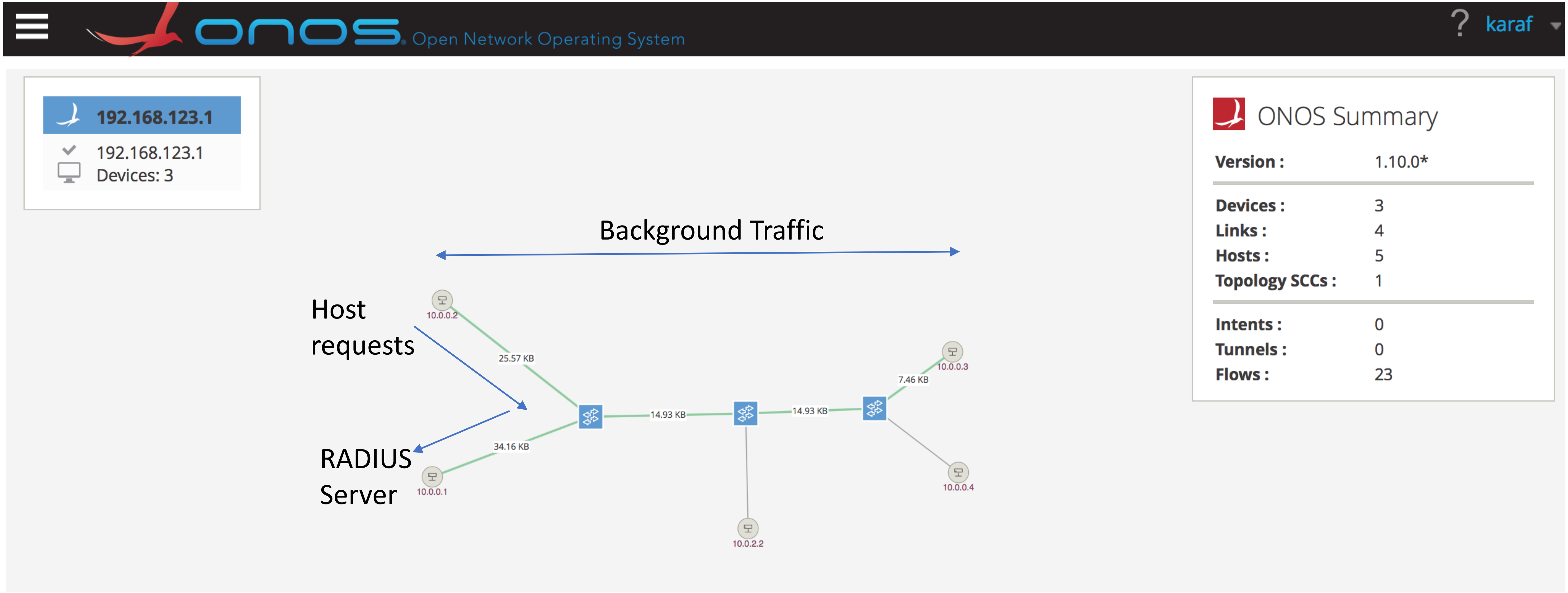
AAA in SDN

RADIUS AAA Server

- Authentication, Authorisation and Accounting
- RADIUS provides support for EAP



Integration of RADIUS into ONOS/Mininet - DEMO



192.168.123.1

192.168.123.1
Devices: 3

Background Traffic

Host requests

RADIUS Server

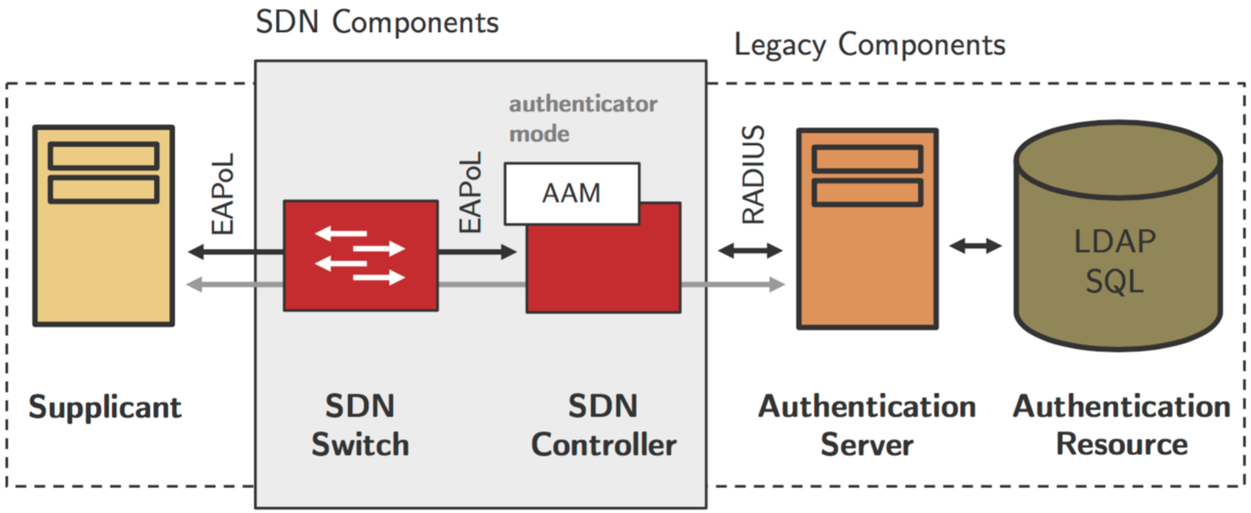
ONOS Summary

Version :	1.10.0*
Devices :	3
Links :	4
Hosts :	5
Topology SCCs :	1
Intents :	0
Tunnels :	0
Flows :	23

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

AAA in SDN

- Call to RADIUS server a 1 to 10 overhead
  - Bandwidth – extra payload content
  - Latency – extra routing; server processing
- One-time cost when new application uses NBI
- Alternative AAM in ONOS controller
  - Eliminates need for extra middleware boxes
  - What about performance impact on controller?



CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Agenda - Updated

Evening Session: 5pm – 7pm

1. SDN Controller Security evolution
   Demo- DELTA
2. Network Security Enhancements using SDN
3. SDN Monitoring and Security Applications
4. Application-aware VNSF Provisioning
5. Future Directions a.k.a. Buzzword Bingo ☺