CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Queen's University Belfast

SDN Security

COINS Summer School

Dr. Sandra Scott-Hayward

23 August 2015

@CSIT_QUB

Attacks and Vulnerabilities in SDN

Confidentiality

Integrity

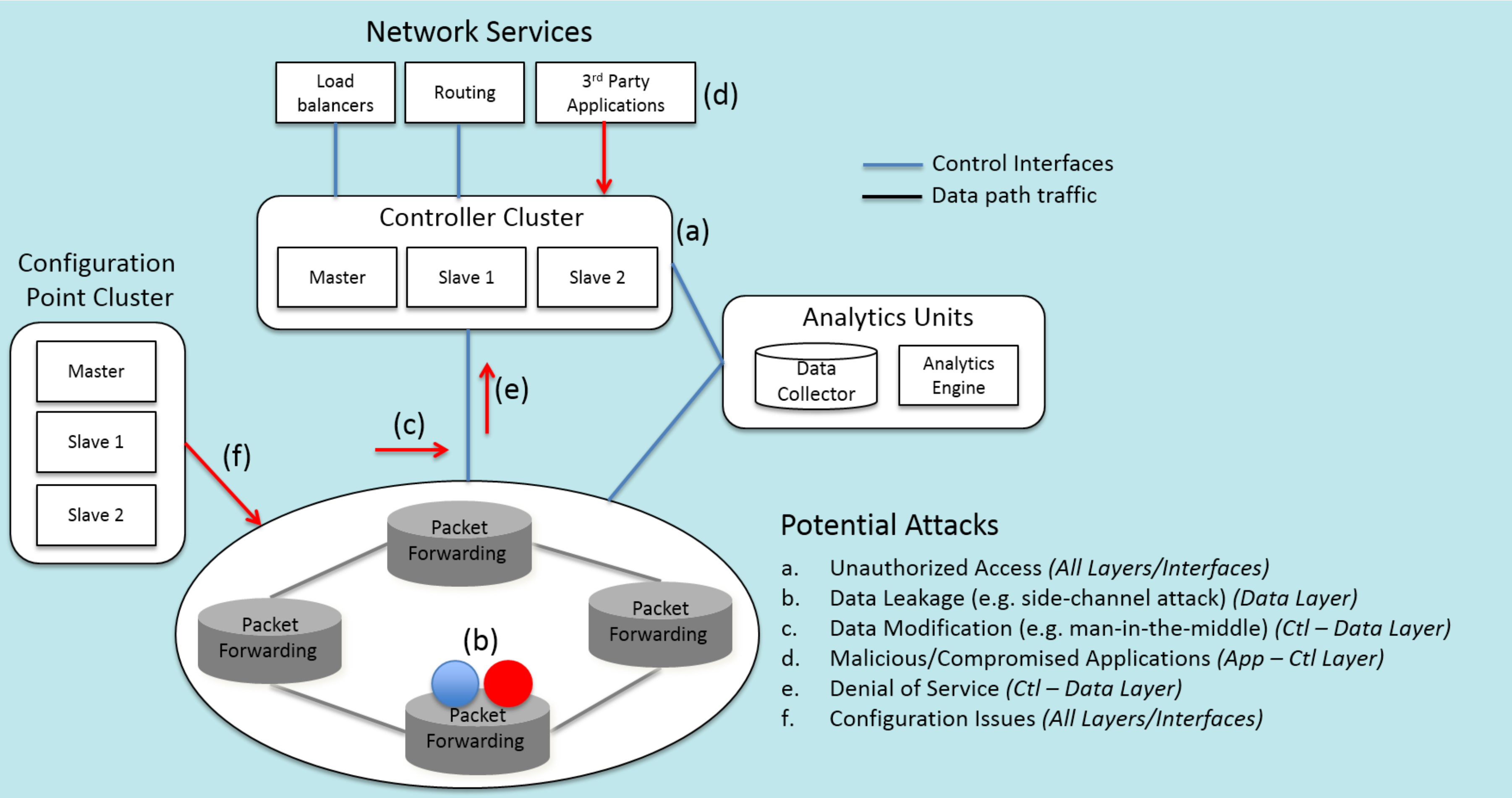
Availability of Information

Authentication

Non-repudiation

=> Secure data, network assets and communication transactions

SDN Potential Attacks and Vulnerabilities

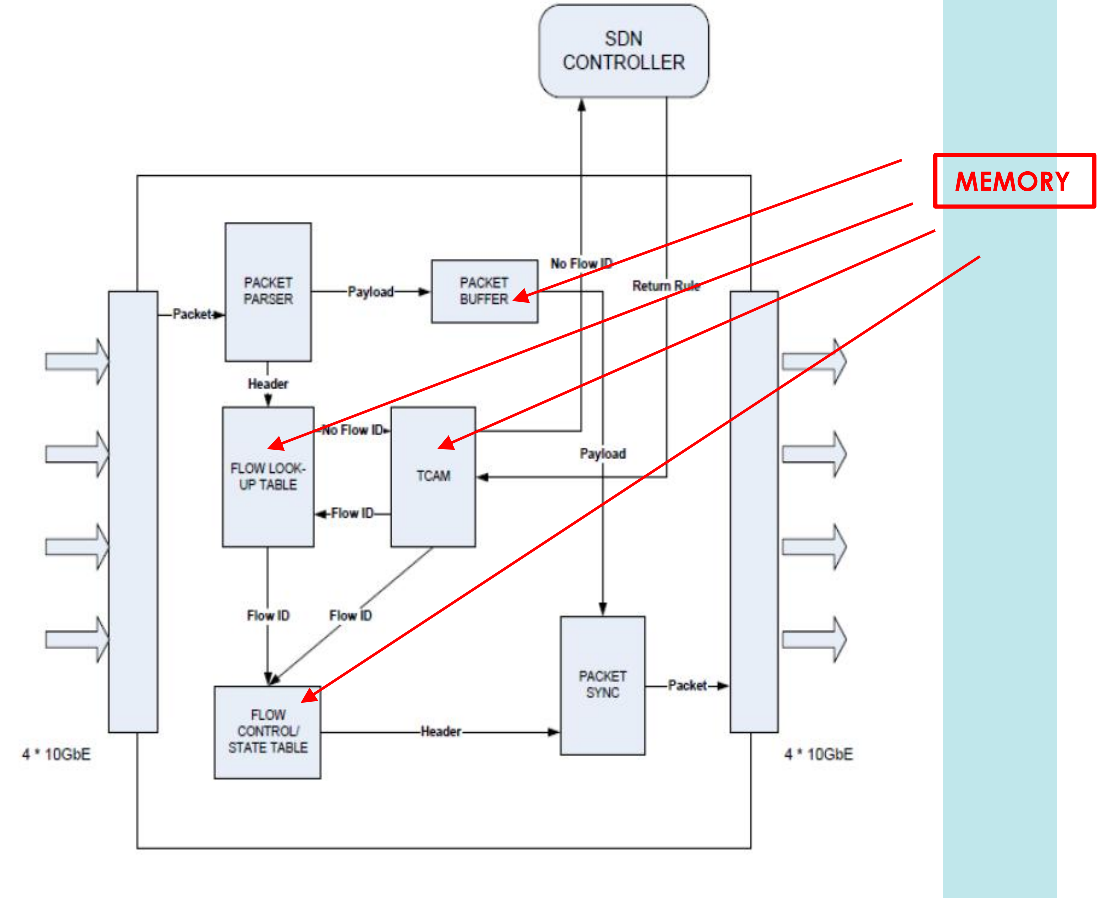


Categorization of Security Issues

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

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.

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 *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 CONTROL PLANE ATTACKS

DEMO

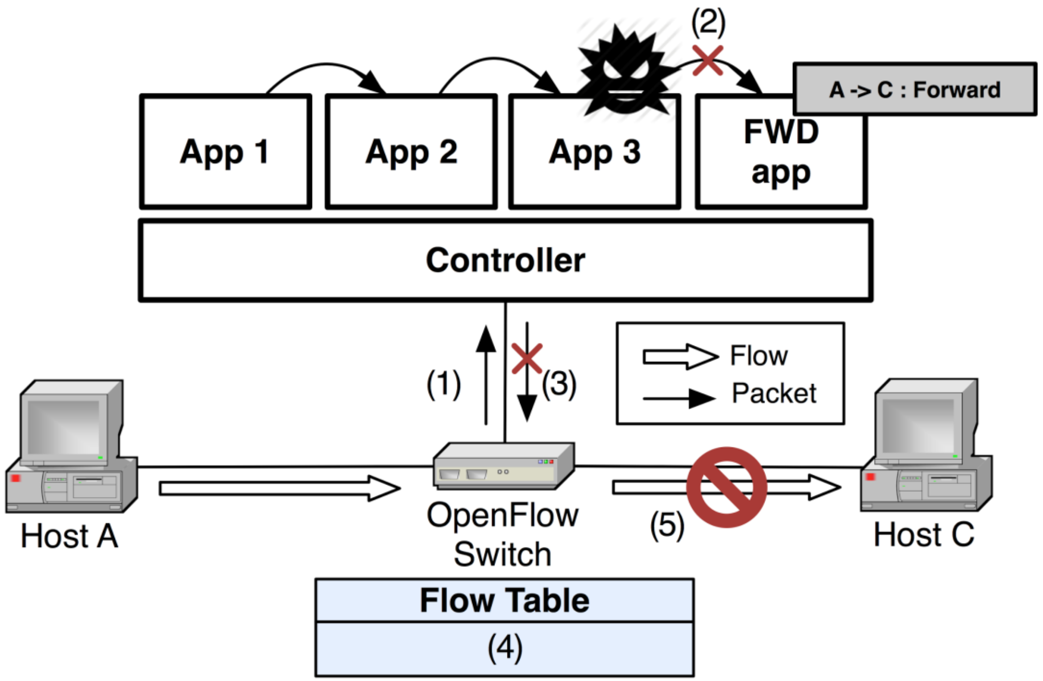
http://sdnsecurity.org

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

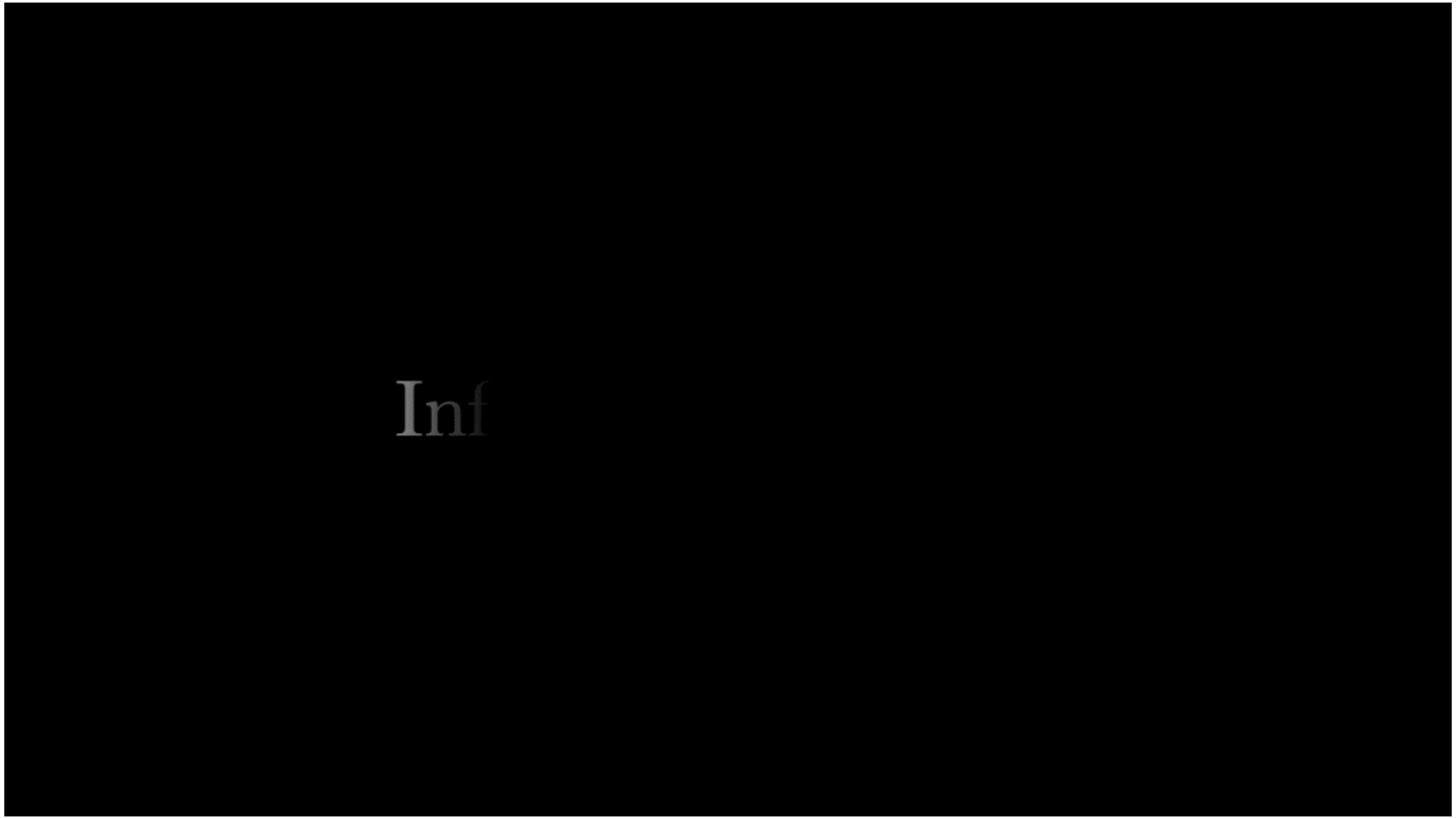
App 3 programmed to fall into an infinite loop leading the controller instance to freeze.



Service Chain Attack – Control Message Drop

http://sdnsecurity.org

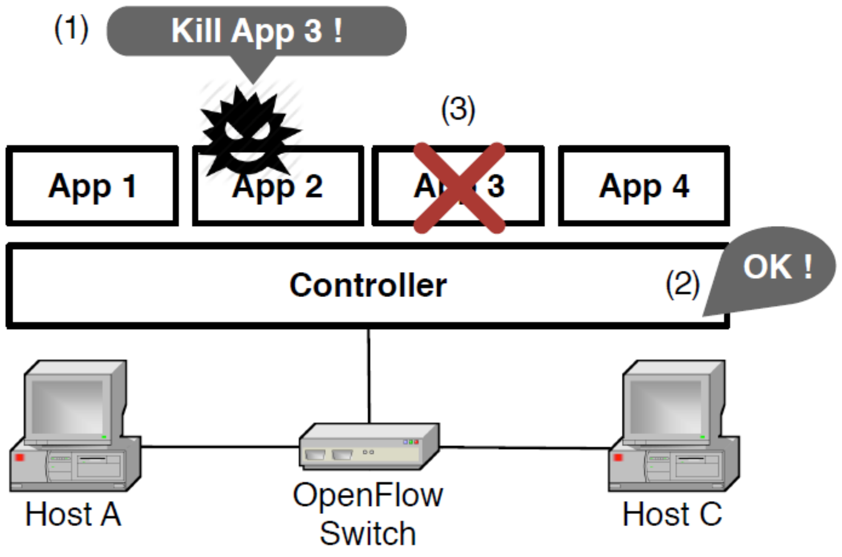
Service Chain Attack – Infinite Loop Attack



http://sdnsecurity.org

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

Northbound API Abuse – Application Eviction

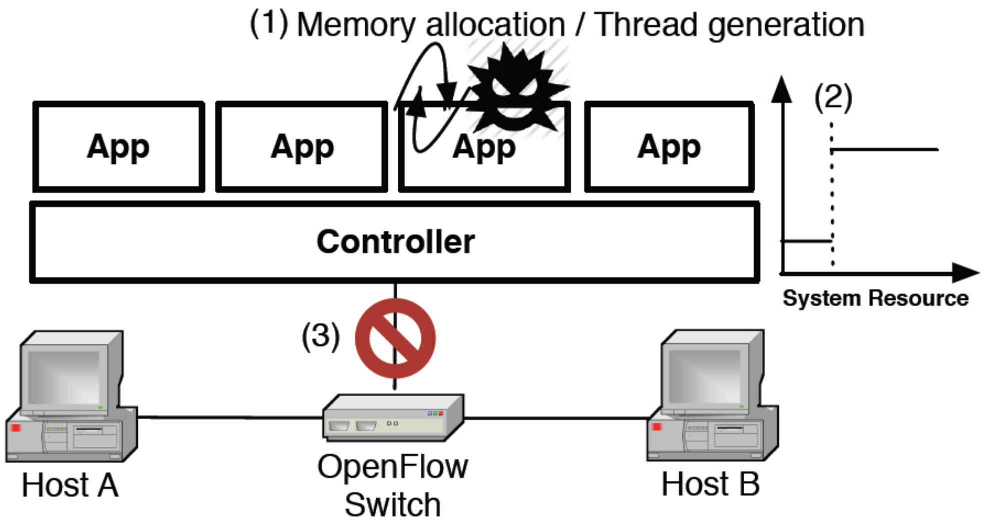
http://sdnsecurity.org

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.



Resource Exhaustion – Memory Leakage Attack

http://sdnsecurity.org

Resource Exhaustion – Create Thread Attack

http://sdnsecurity.org

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!)

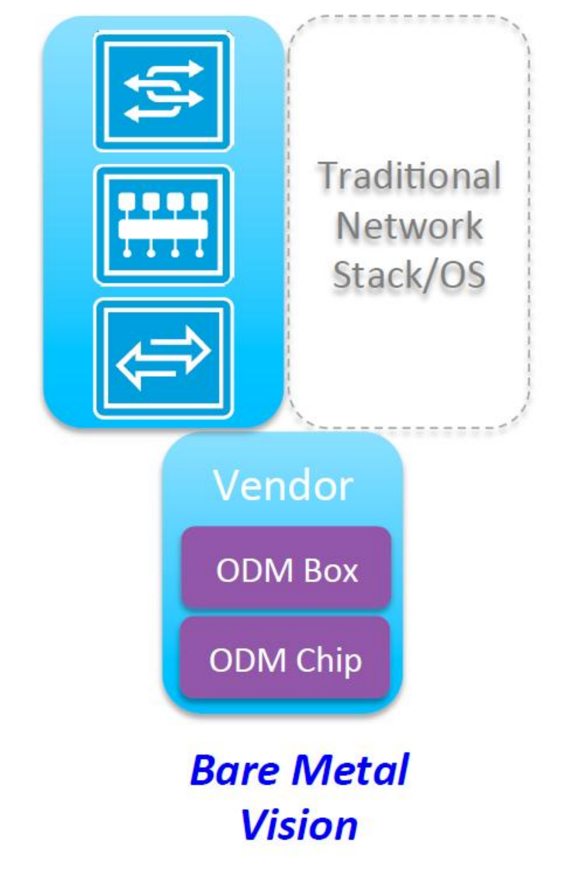
Weaknesses (Installer) e.g.

- 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

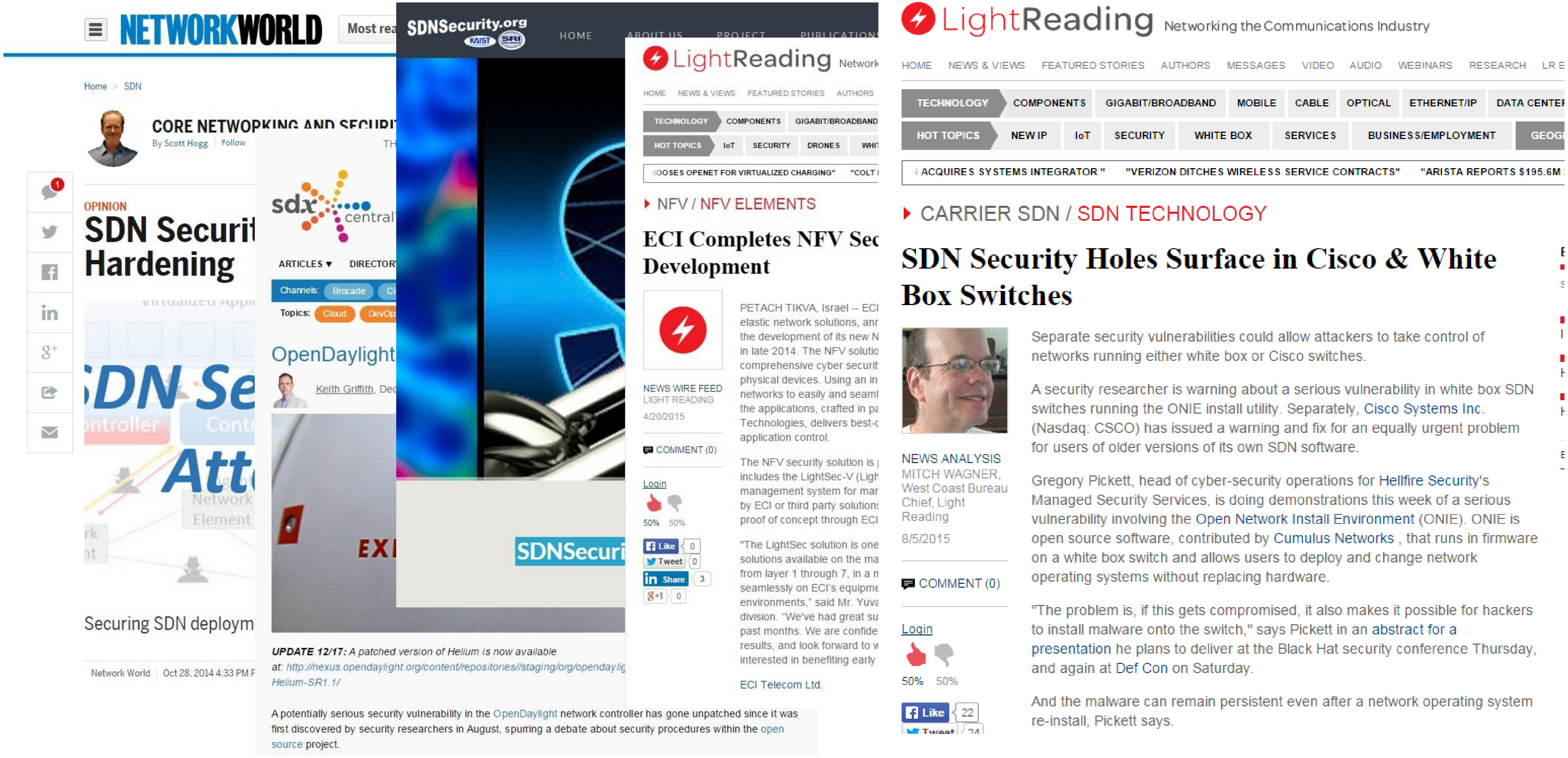
Gregory Pickett, "Staying Persistent in Software Defined Networks," DefCon 23, Las Vegas 2015, https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/Speaker%20&%20Workshop%20Materials/Gregory%20Pickett/DEFCON-23-Gregory-Pickett-Staying-Persistant-in-Software-Def.pdf

Available Solutions:

- 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



End Session 4