ESTD 1845

QUEEN'S
UNIVERSITY
BELFAST

Network Security Architecture – Part 2

Dr. Sandra Scott-Hayward

CSC3064 Lecture 05

School of Electronics, Electrical Engineering and Computer Science

Session Overview

□ Software Defined Network (SDN) Architecture – Example of a Security Analysis

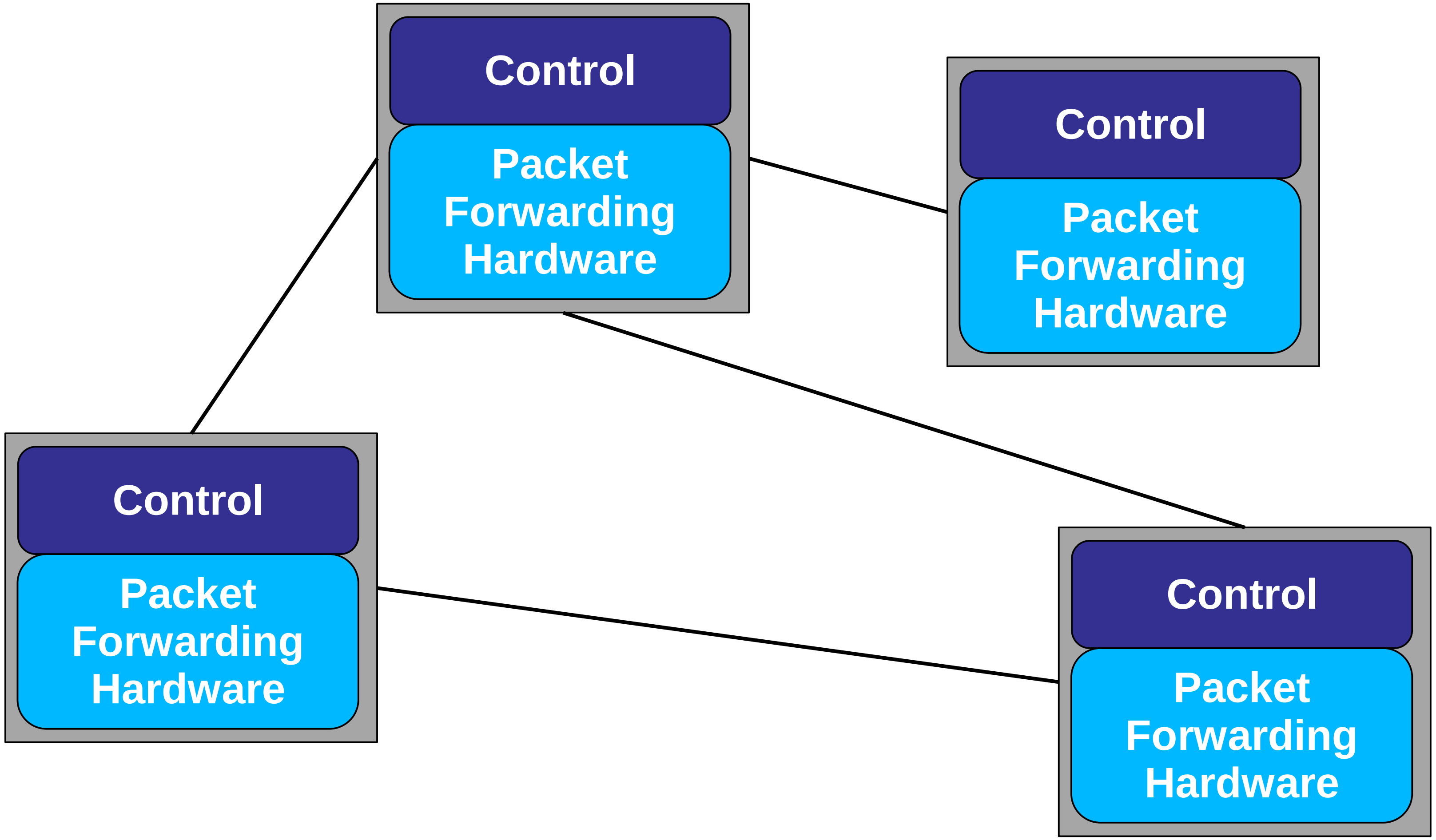
References:

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

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

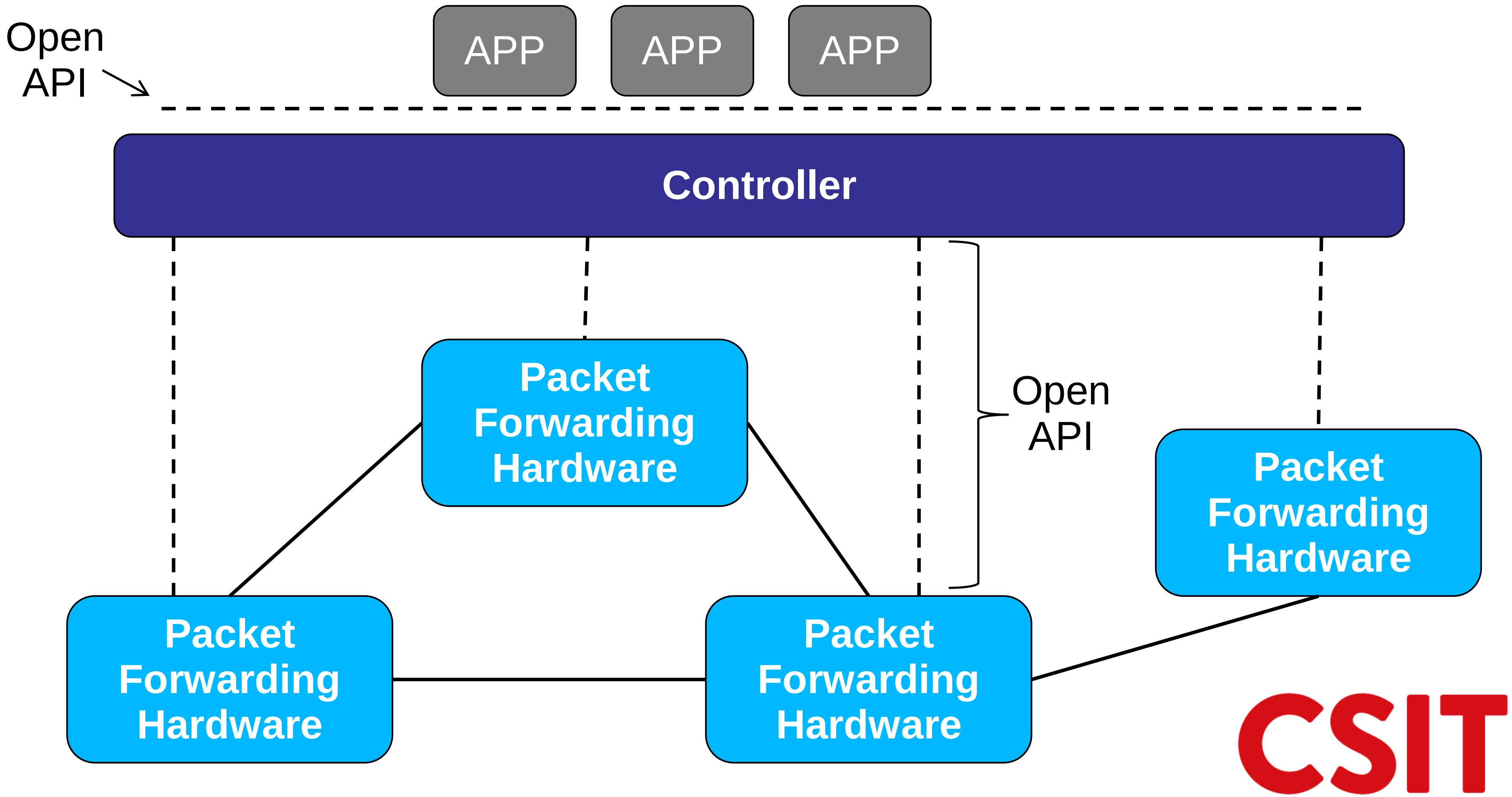
Traditional Network

Control and Data Planes combined in Network Elements:


Control
Packet Forwarding Hardware
Control
Packet Forwarding Hardware
Control
Packet Forwarding Hardware
Control
Packet Forwarding Hardware

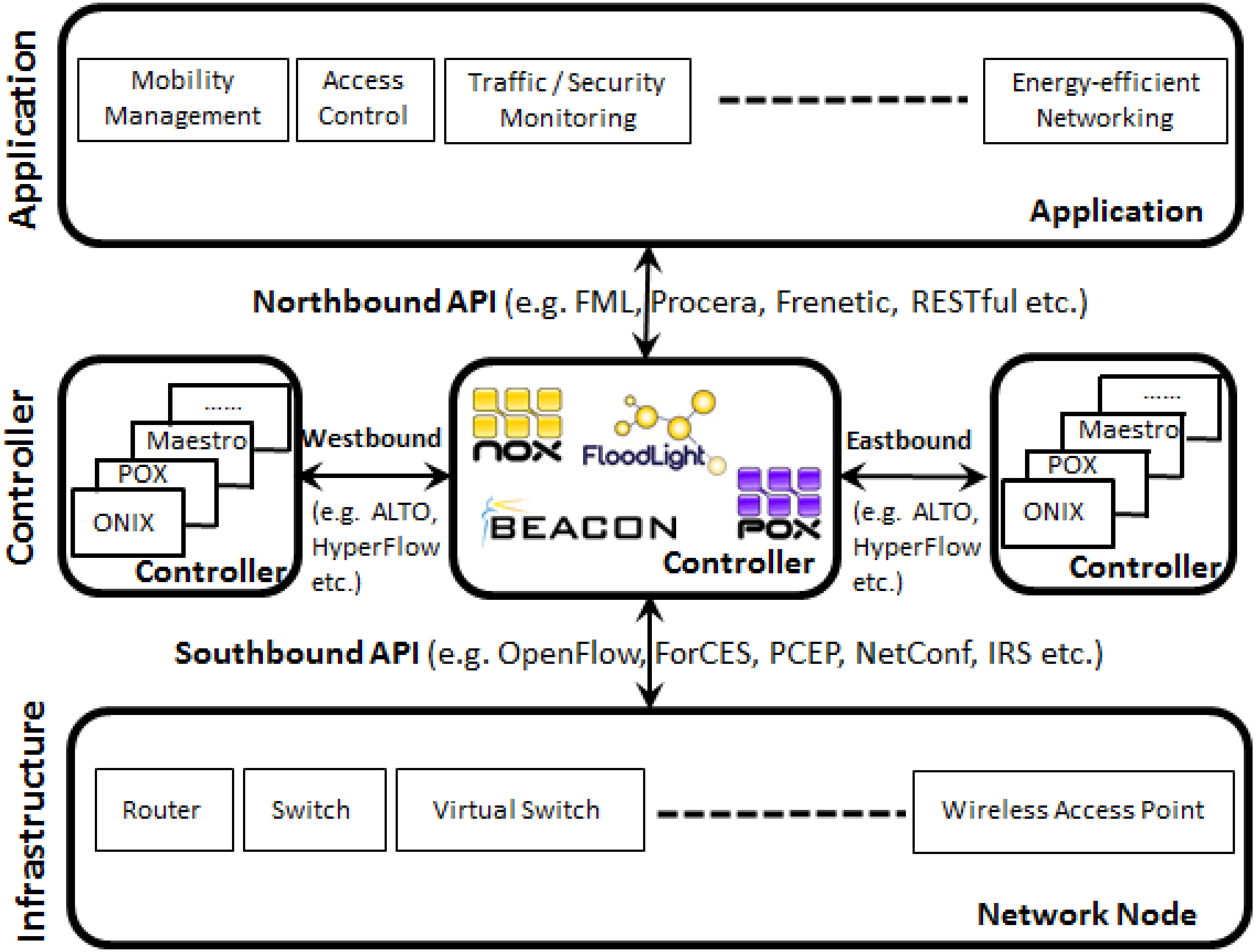
Software Defined Network

Separation of Control and Data Planes:

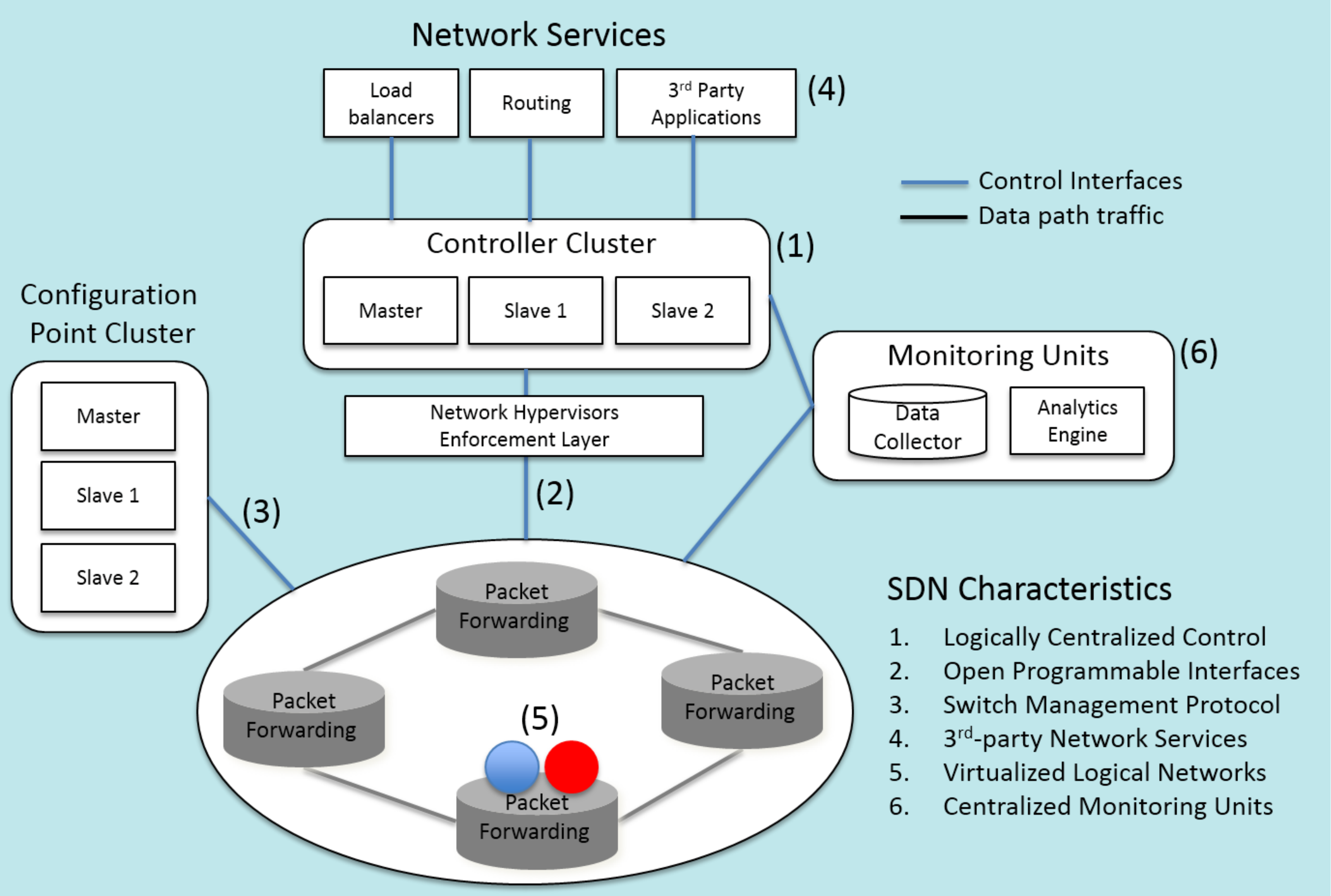


Open API
APP
APP
APP
Controller
Packet Forwarding Hardware
Open API
Packet Forwarding Hardware
Packet Forwarding Hardware
Packet Forwarding Hardware

SDN Architecture



SDN Characteristics



SDN Characteristics

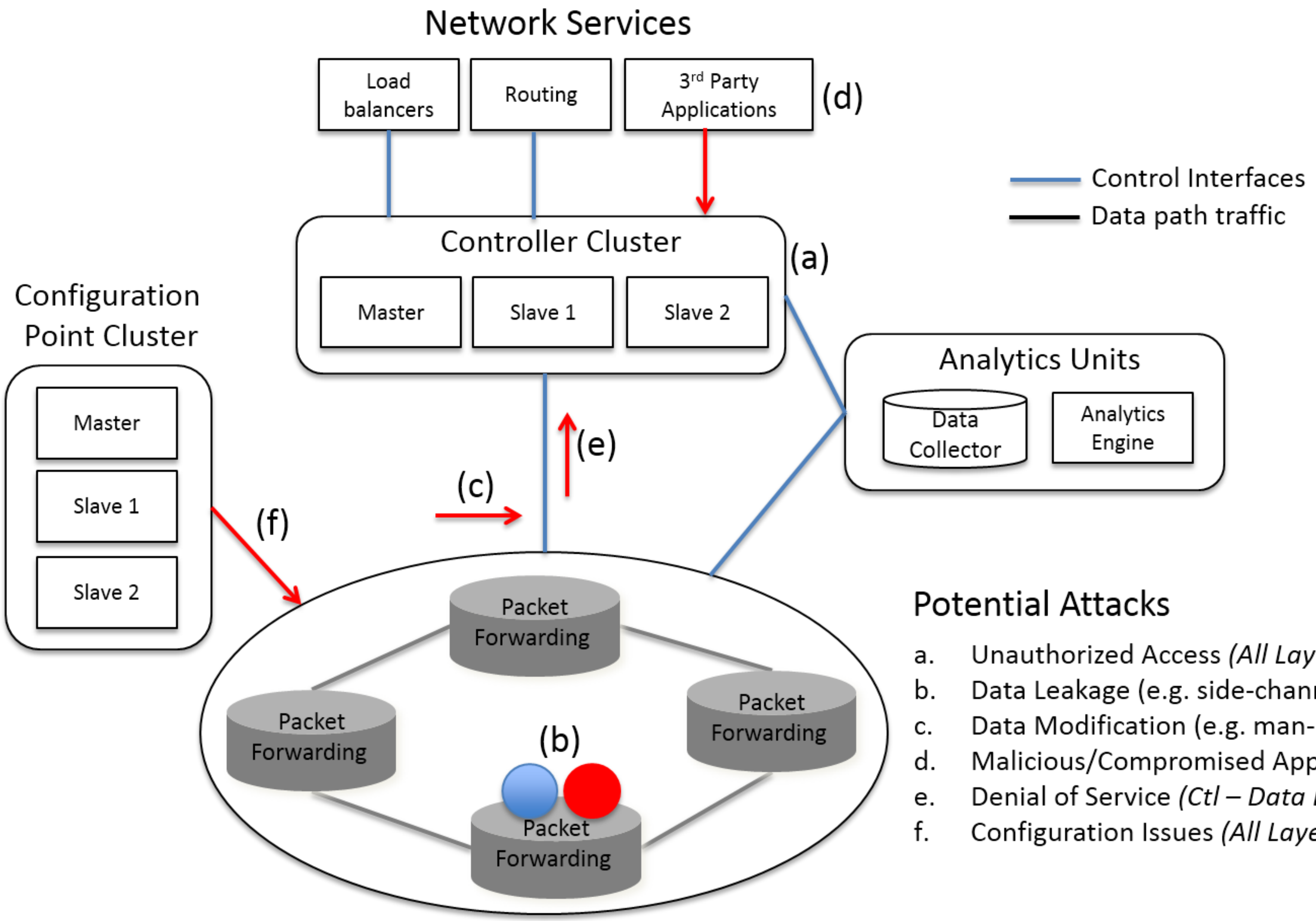
1. Logically Centralized Control
2. Open Programmable Interfaces
3. Switch Management Protocol
4. 3rd-party Network Services
5. Virtualized Logical Networks
6. Centralized Monitoring Units

Secure Communications Network

Confidentiality
Integrity
Availability
Controlled Access
Accountability

=> 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)*

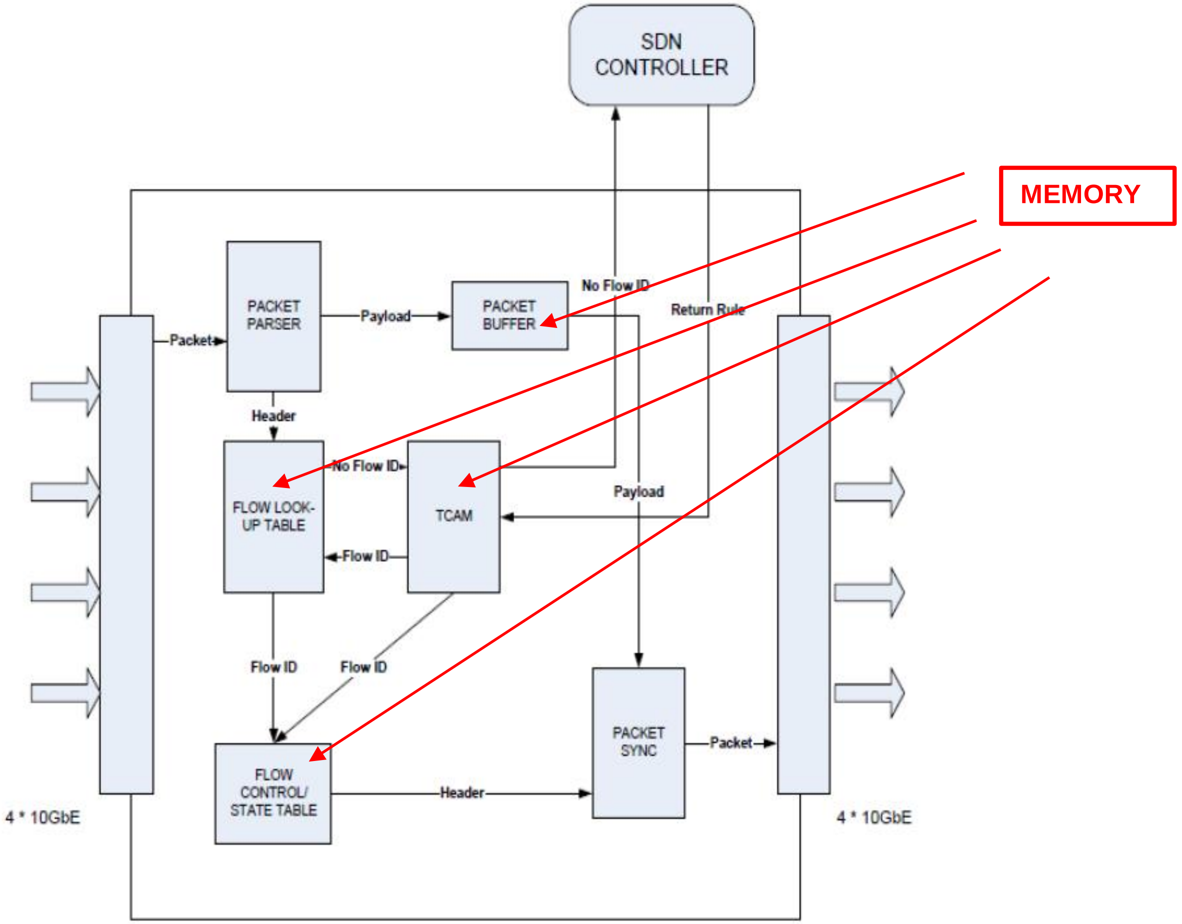
Categorization of Security Issues

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

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 $field_1$ 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 – Service Chain Attack

Control Message Drop

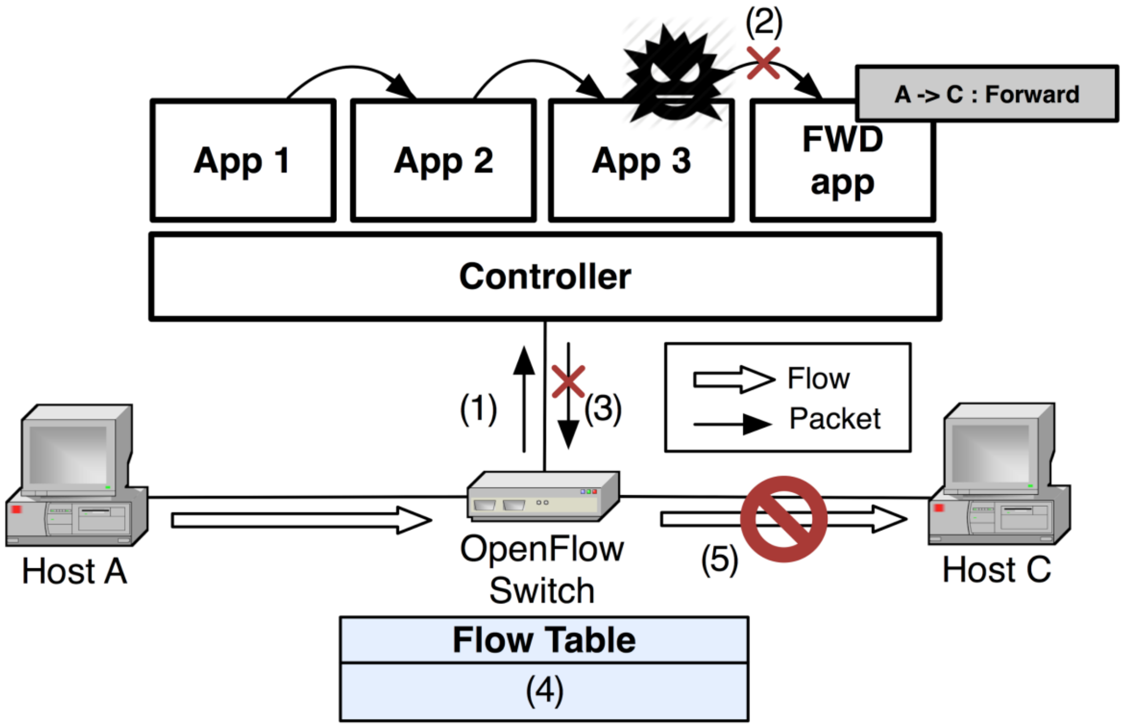
(1) Packet-In to Controller; Pkt-In passed to App 1, App 2, App 3 as per service chain;

(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

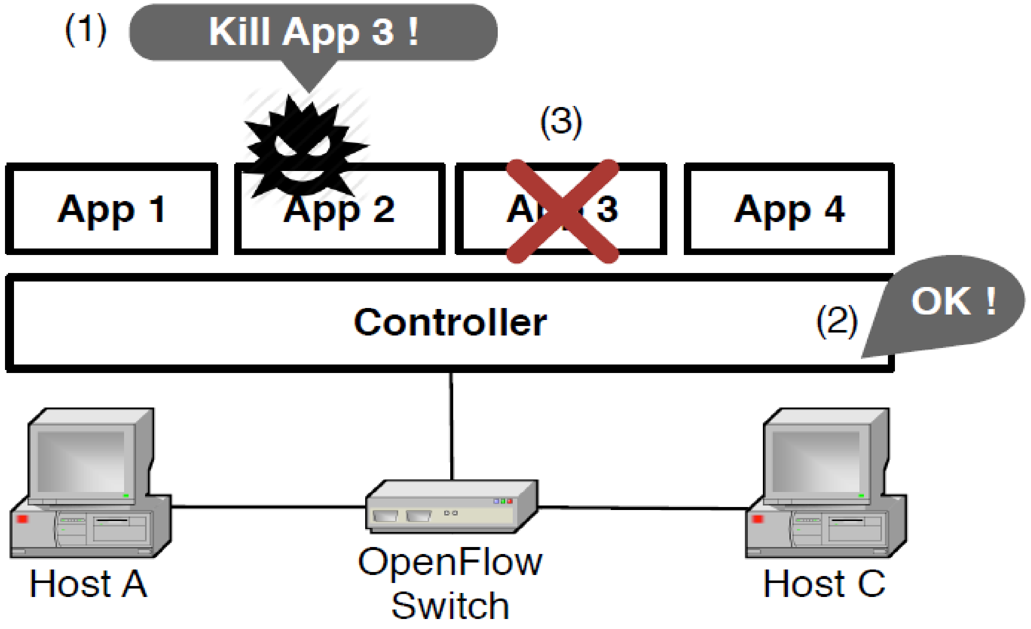
SDN Control Plane Attacks – Northbound API Abuse

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

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

SDN Control Plane Attacks – Resource Exhaustion

Memory Leakage Attack

(1) App continuously allocates memory;

(2) System resource is increasingly consumed;

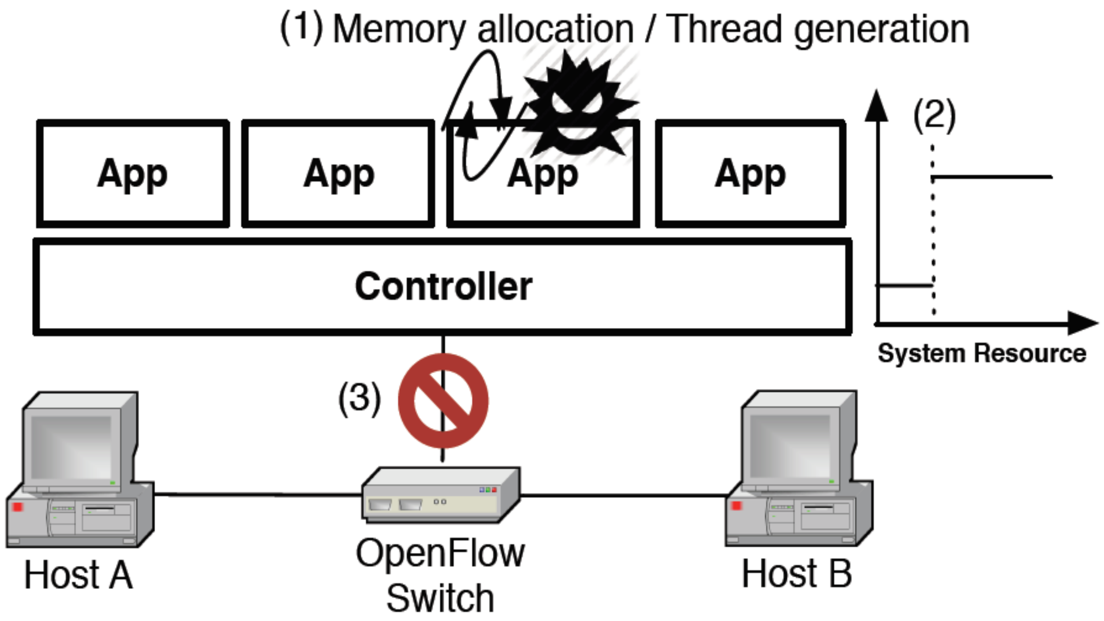
(3) Loss of control plane functionality and connection to data plane devices.

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

Mitigating SDN Architecture threats using standard technologies

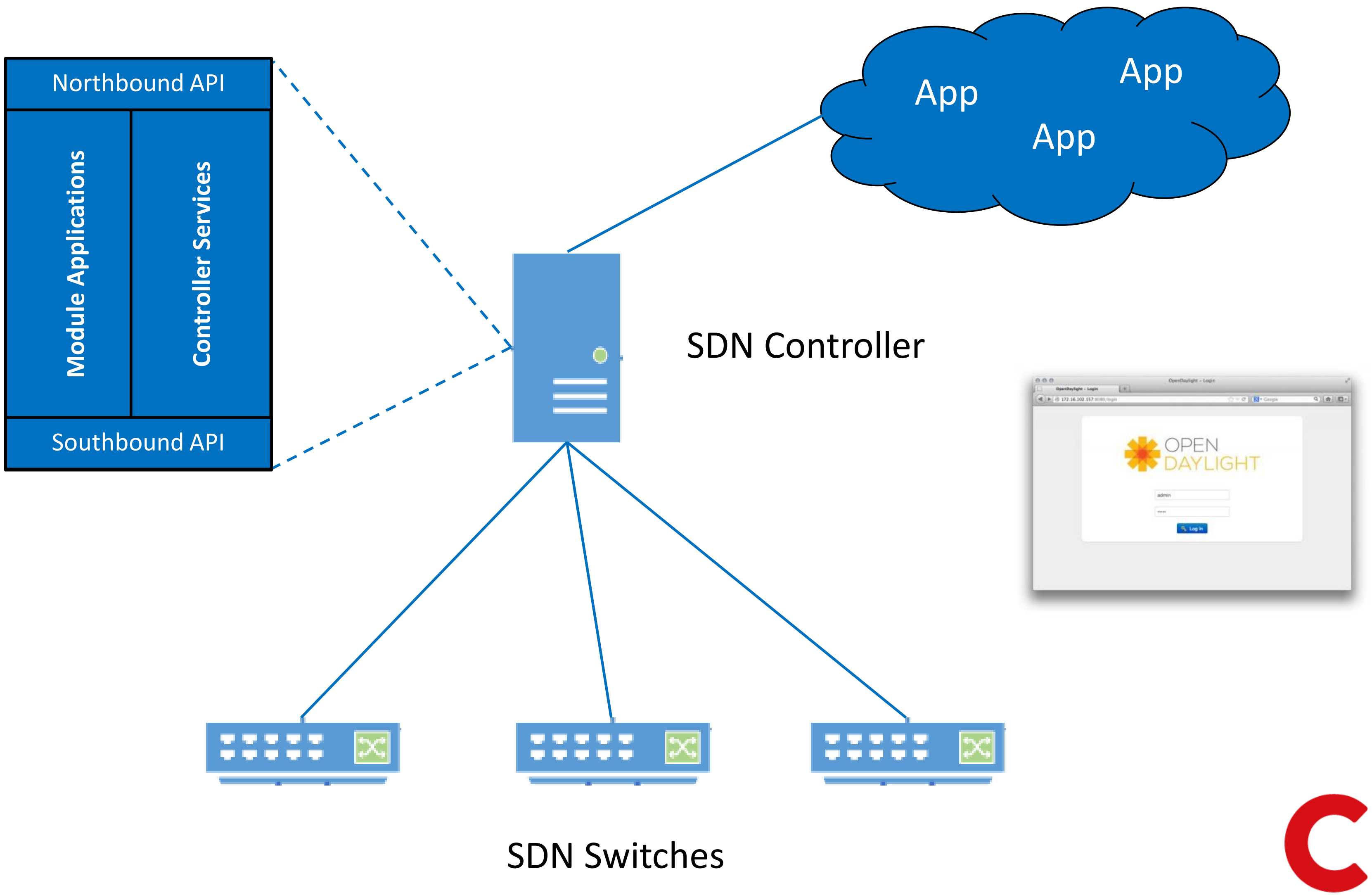
Example OpenFlow (SDN communication protocol) Threat Analysis

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

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

SDN Controller - Security Attributes



OpenDaylight - Login

OpenDaylight - Login

172.16.102.157:8080/login

Google

OPEN DAYLIGHT

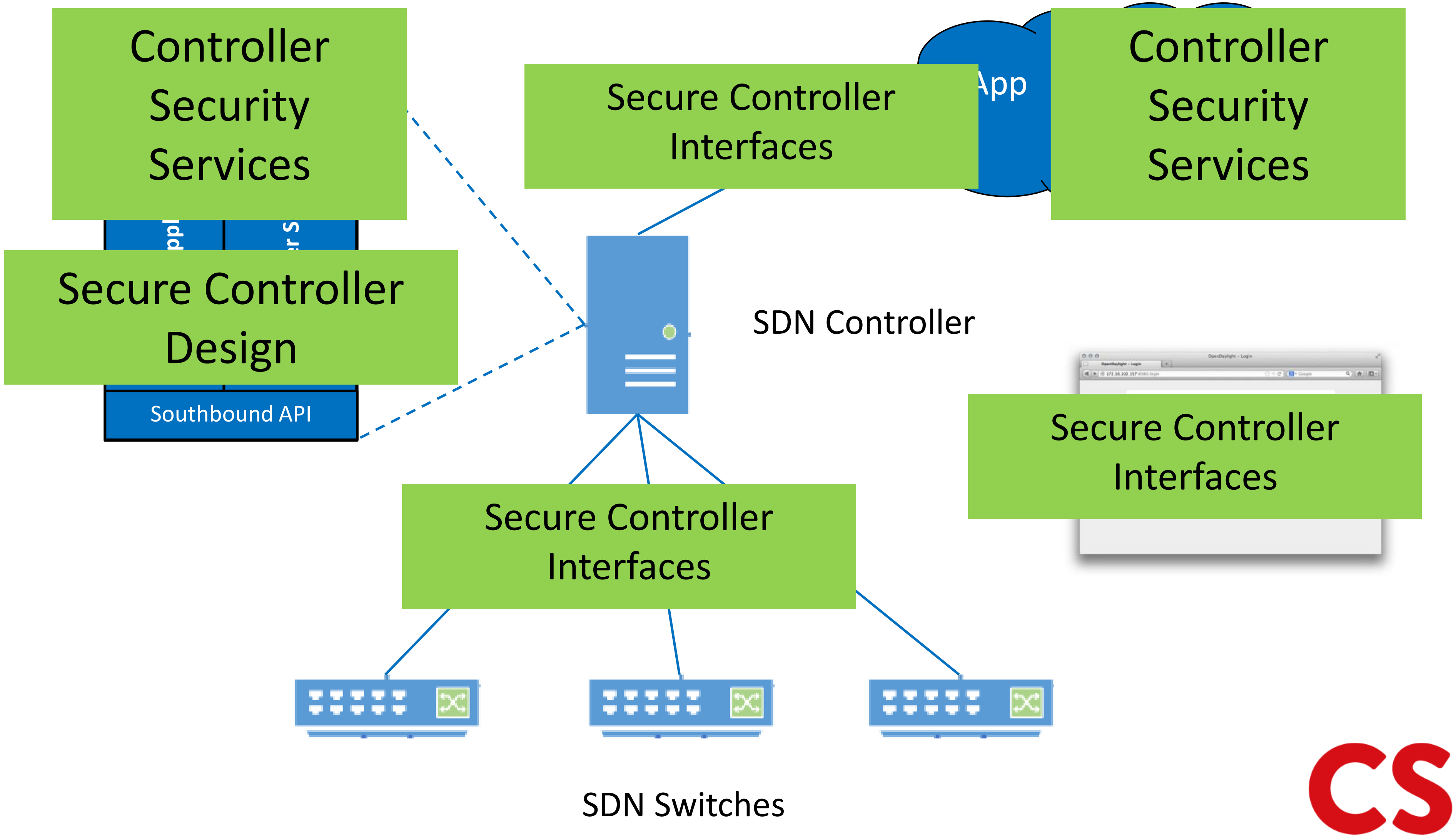
admin

•••••

Log In

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

SDN Controller - Security Attributes


Controller Security Services
Secure Controller Interfaces
App
Controller Security Services
Secure Controller Design
Southbound API
SDN Controller
Secure Controller Interfaces
Secure Controller Interfaces
SDN Switches

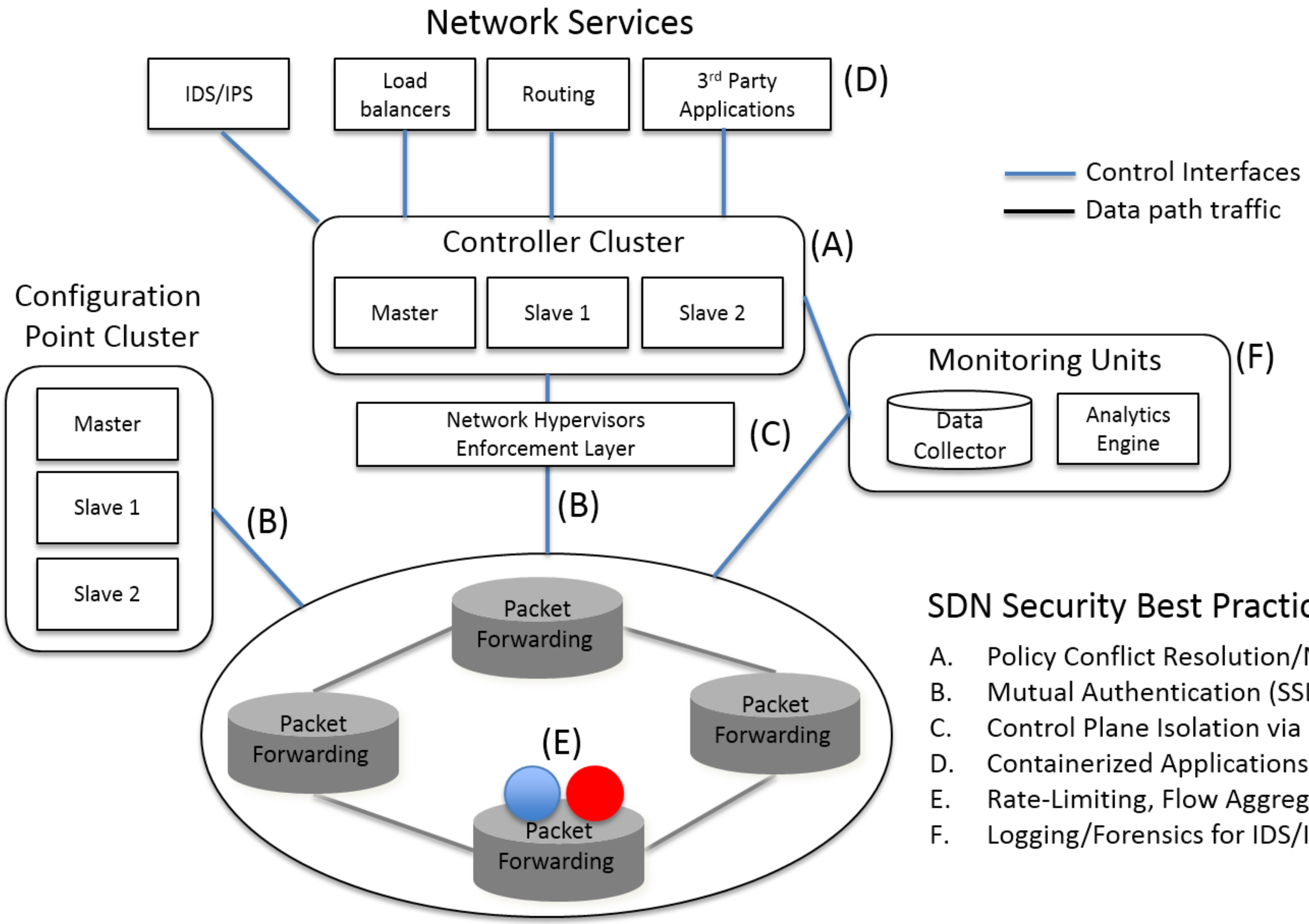
Features of a secure, robust, and resilient SDN Controller

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

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

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Summary

- Example of network security analysis applied to the Software Defined Network architecture
  - Categorization of security Issues
  - Mitigation of threats using standard security technologies
  - SDN Controller security features
  - Recommended SDN security best practices

Questions?

Next Session: Security of Internet Protocols – Part 1

Friday, 25 January 2019

QUEEN'S UNIVERSITY BELFAST