

FRESCO: Modular Composable Security Services for Software-Defined Networks

Seungwon Shin, [Phil Porras](#), [Vinod Yegneswaran](#), [Martin Fong](#),
Guofei Gu, and [Mabry Tyson](#)

SUCCESS LAB, Texas A&M and SRI International



Contents

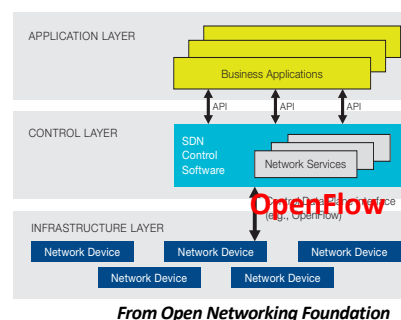
- Background
 - SDN and OpenFlow
- FRESCO
 - Design
 - Use cases
 - Evaluation
- Summary

Problem of Legacy Network Devices

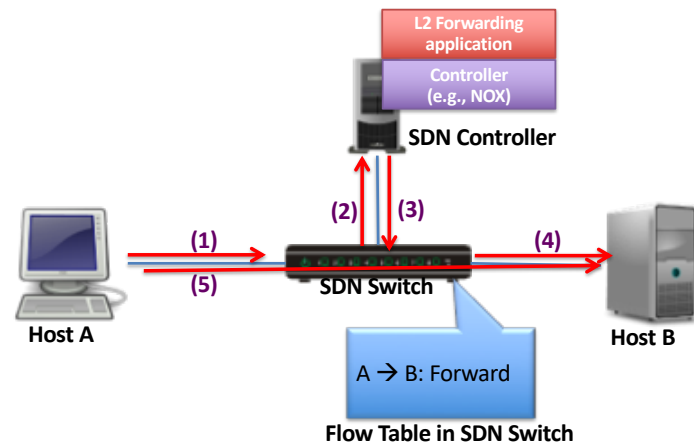
- Complicated and Closed platform
 - Complicated S/W and ASIC
 - Vendor specific
- Inflexible: Hard to modify (nearly impossible)
- Non-extensible: Difficult to support emerging technologies
 - E.g., VM mobility
- New proposal: Software Defined Networking
 - Separate the control plane from the data plane

Software Defined Networking (SDN)

- Three layers
 - Application layer
 - Application part
 - Implements logic
 - Control layer
 - Kernel part
 - Runs applications
 - Infrastructure layer
 - Data plane
 - Network switch or router



SDN Operation



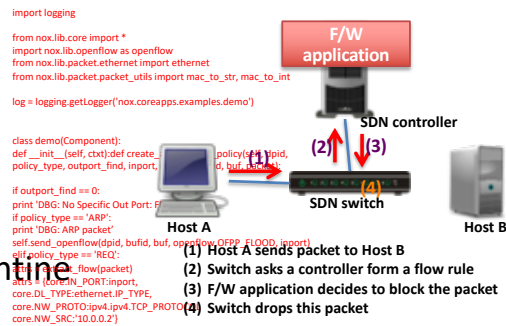
Killer Application of SDN?

- Reducing energy in data center networks
- Dynamic virtual machine migration in cloud networks
- diverse network applications
- What about security?
 - Can SDN enable new capabilities to improve network security?

Exemplar SDN Security Apps

- Security functions can be applications of SDN

- Firewall
- DDoS detection
- Scan detection
- Reflector net
- Tarpit
- Dynamic quarantine
- and more...



SDN Security App Development Challenges

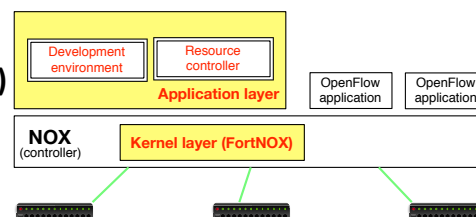
- However, it is not easy to create security apps in SDN
 - Security service creation and composition challenge
 - How do we simplify development of security applications?
 - Information deficiency challenge
 - E.g., TCP session, network status
 - Threat response translation challenge
 - How do we enforce security policies to the network devices?

FRESCO

- FRESCO is a new frame work that
 - Provides a new development environment for security applications
 - Effectively manages shared resources among security applications
 - Simplifies deployment of security policies
 - provides a set of 7 new intelligent security action primitives
 - E.g., block, deny, allow, redirect, and quarantine

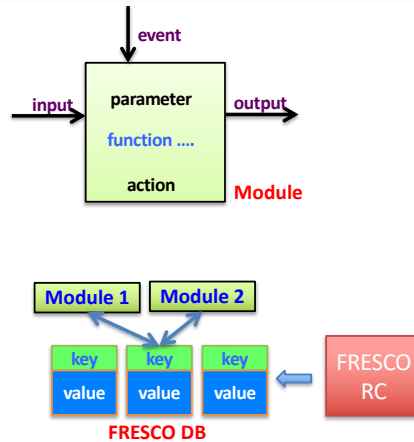
Architecture

- Component
 - **Application layer**
 - **Development env. (DE)**
 - **Resource controller (RC)**
 - Kernel layer
 - Security enforcement kernel
 - FortNOX
 - paper in HotSDN 2012



Development Environment

- FRESKO Module
 - Basic operation unit
- FRESKO DB
 - Simple database
 - (key,value) pairs
- FRESKO script
 - Define interfaces
 - Connect multiple modules



Development Environment

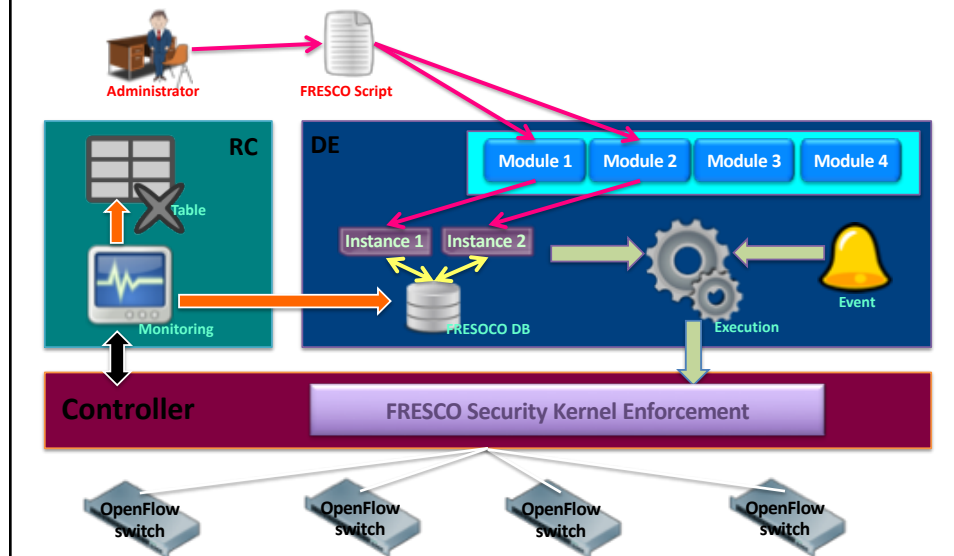
- FRESKO script
 - Format
 - **Instance name (# of input) (# of output)**
 - **type:** class of this module
 - **input:** input for this module
 - **output:** output of this module
 - **parameter:** define some variables
 - **event:** trigger a module
 - **action:** conduct this action

```
port_comparator (1)(1) {
  type: Comparator
  event: PUSH
  input: destination_port
  output: comparison_result
  parameter: 80
  action: -
}
```

Inspired by Click Modular Router

Robert Morris, Eddie Kohler, John Jannotti, and M. Frans Kaashoek. Proceedings of SOSP '99

Operational Scenario

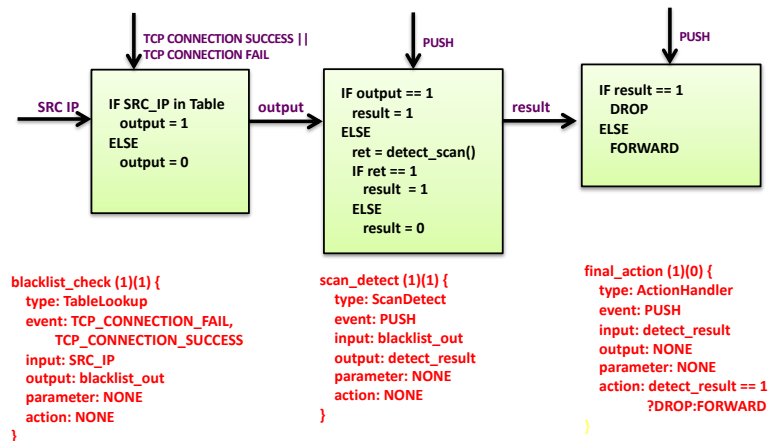


Implementation

- NOX (open source OpenFlow controller) based
 - Development environment
 - NOX based Python application
 - Resource controller
 - NOX based Python application
 - Security enforcement kernel
 - Modify NOX (C++)

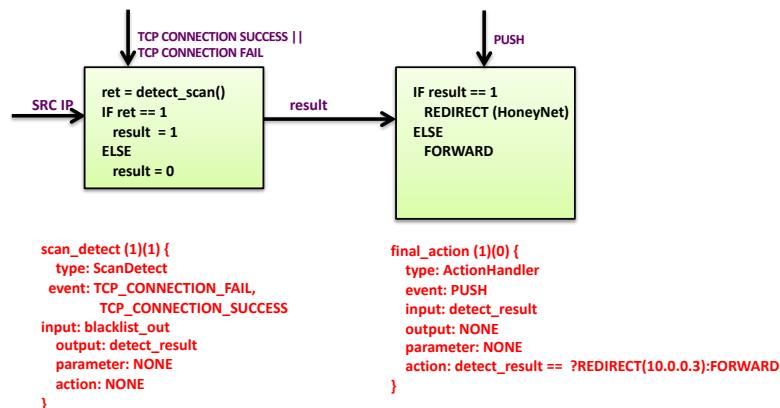
Example: Scan Detection

- Steps
 - Check blacklist → Threshold based scan detection → Drop or Forward



Example: Reflector Net

- Confuse network scan attackers
- Steps
 - Threshold based scan detection → Reflect or Forward



Evaluation

Source code length comparison

Algorithm	Implementation		
	Standard	OpenFlow	FRESCO
TRW-CB	1,060	741	66 (58 + 8)
Rate Limit	991	814	69 (61 + 8)

Results for Standard and OpenFlow are obtained in the following paper,
S. A. Mehdi, J. Khalid, and S. A. Khayam.
Revisiting Traffic Anomaly Detection Using Software Defined Networking, In Proceedings of Recent Advances in Intrusion Detection, 2011.

Flow rule setup time

	NOX	Simple Flow Tracker	Simple Scan Detector	Threshold Scan Detector	BotMiner	P2P Plotter Detector
Time (ms)	0.823	1.374	2.461	7.196	15.461	11.775

Please refer to our paper for the explanation of each test case

Summary and Future Work

- FRESCO
 - Create security applications easily
 - Deploy security applications easily
 - Focus on creating security applications
- Future work
 - Port FRESCO to other controllers for open source release
 - E.g., POX or Floodlight
 - Create more modules (now 16 basic modules)

More Information

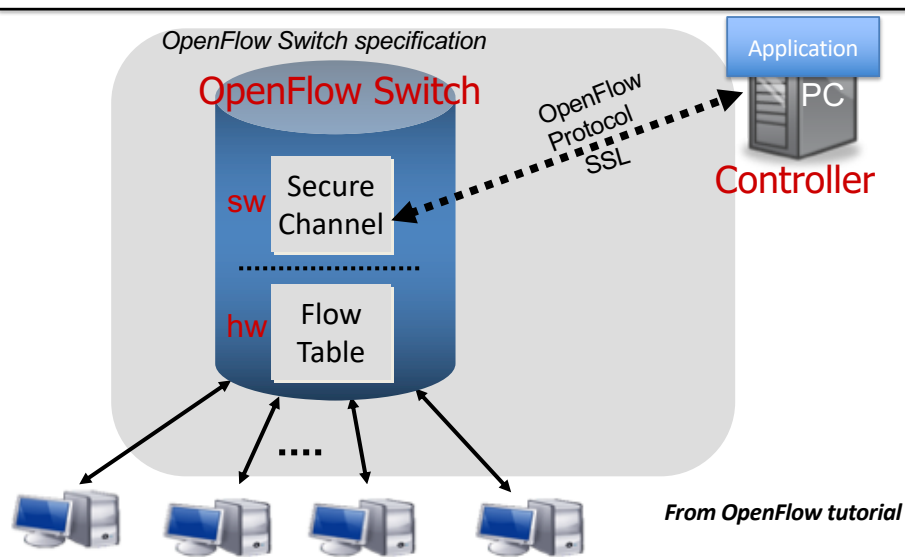
www.openflowsec.org

- Demo movies
 - Security Constraints Enforcement
 - Reflector Nets
 - Automated Quarantine

Thank you,
Question ?

Optional

OpenFlow Architecture



Resource Controller

- Monitor OpenFlow switches
 - Check current status of security policies
 - How many security policies are active
 - How many packets are matched to policies
 - And etc..
- Remove some old policies
 - Save some space for FRESCO security constraints
 - Garbage collection