Security Challenges & Opportunities in Software Defined Networks (SDN)

June 30th, 2015

SEC2 2015
Premier atelier sur la sécurité dans les Clouds

Nizar KHEIR
Cyber Security Researcher
Orange Labs Products and Services

orange™

Understanding the SDN Concept
Analogy with the operating system

Applications

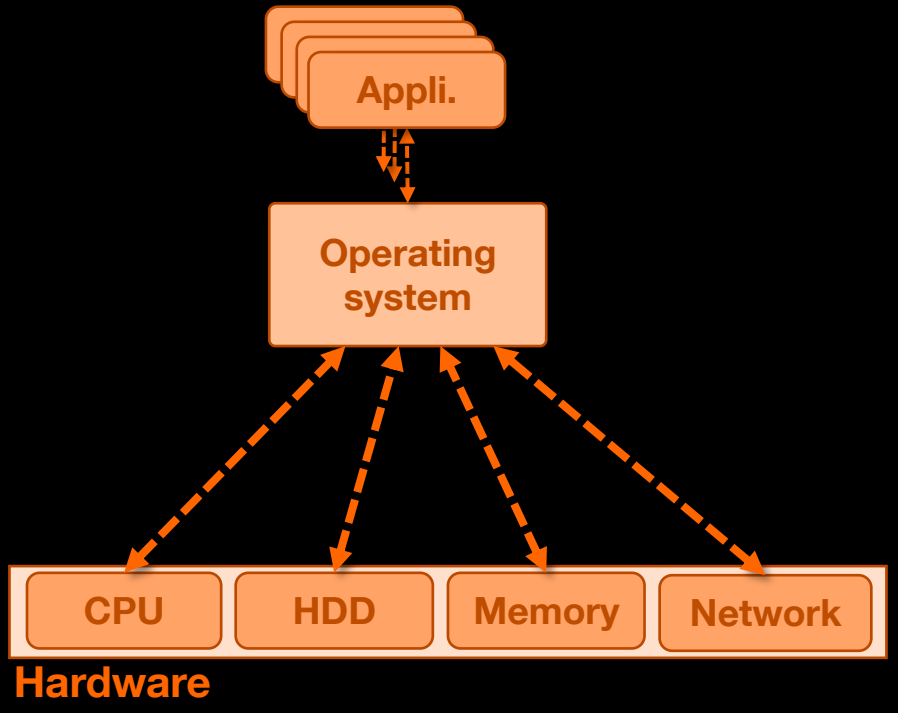
Supply value added services that leverage the main physical assets for the underlying system

Operating system

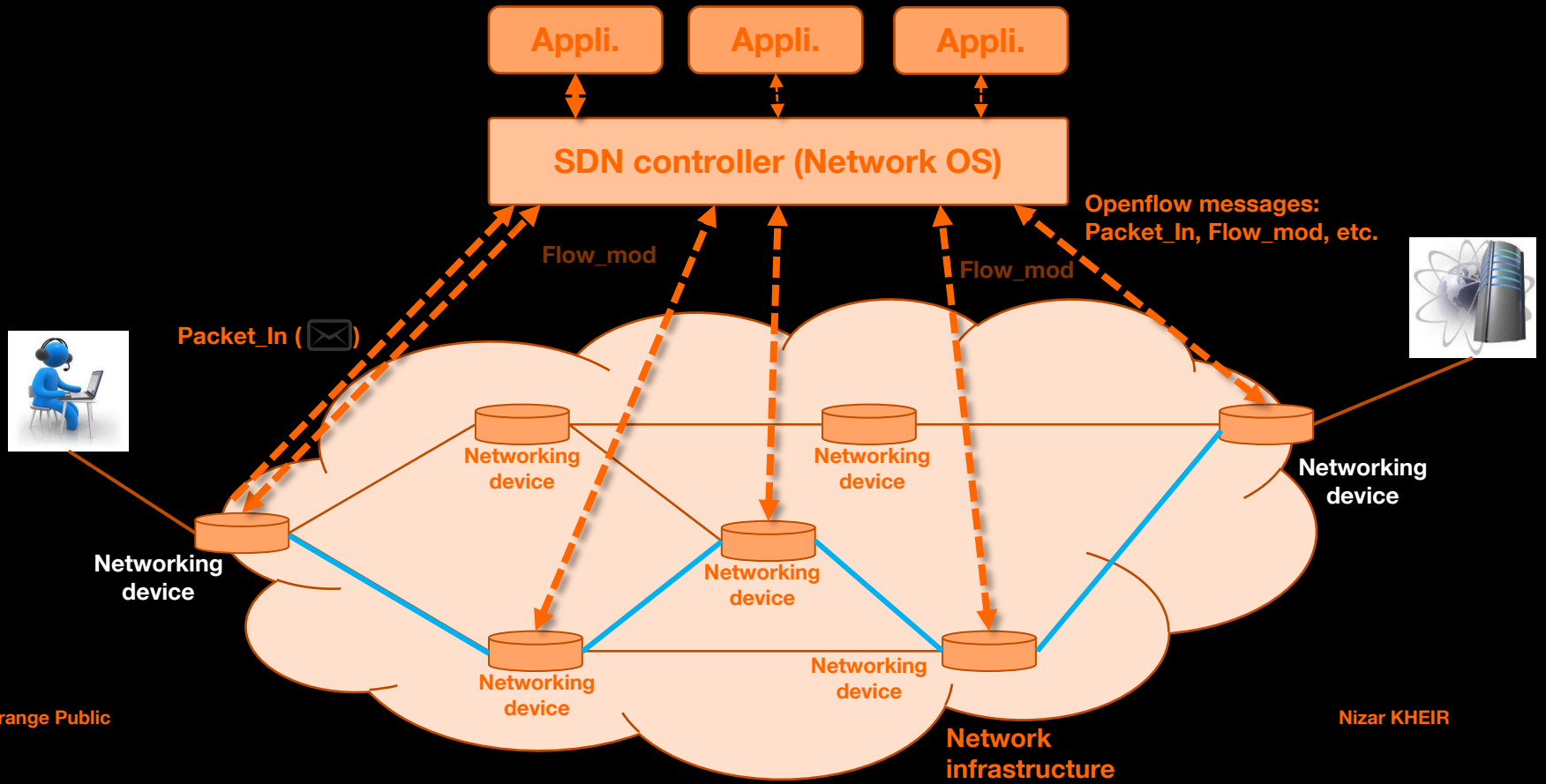
Provides a mediation layer between the application logic and the physical hardware. It may be accessed through dedicated APIs and system calls

Hardware

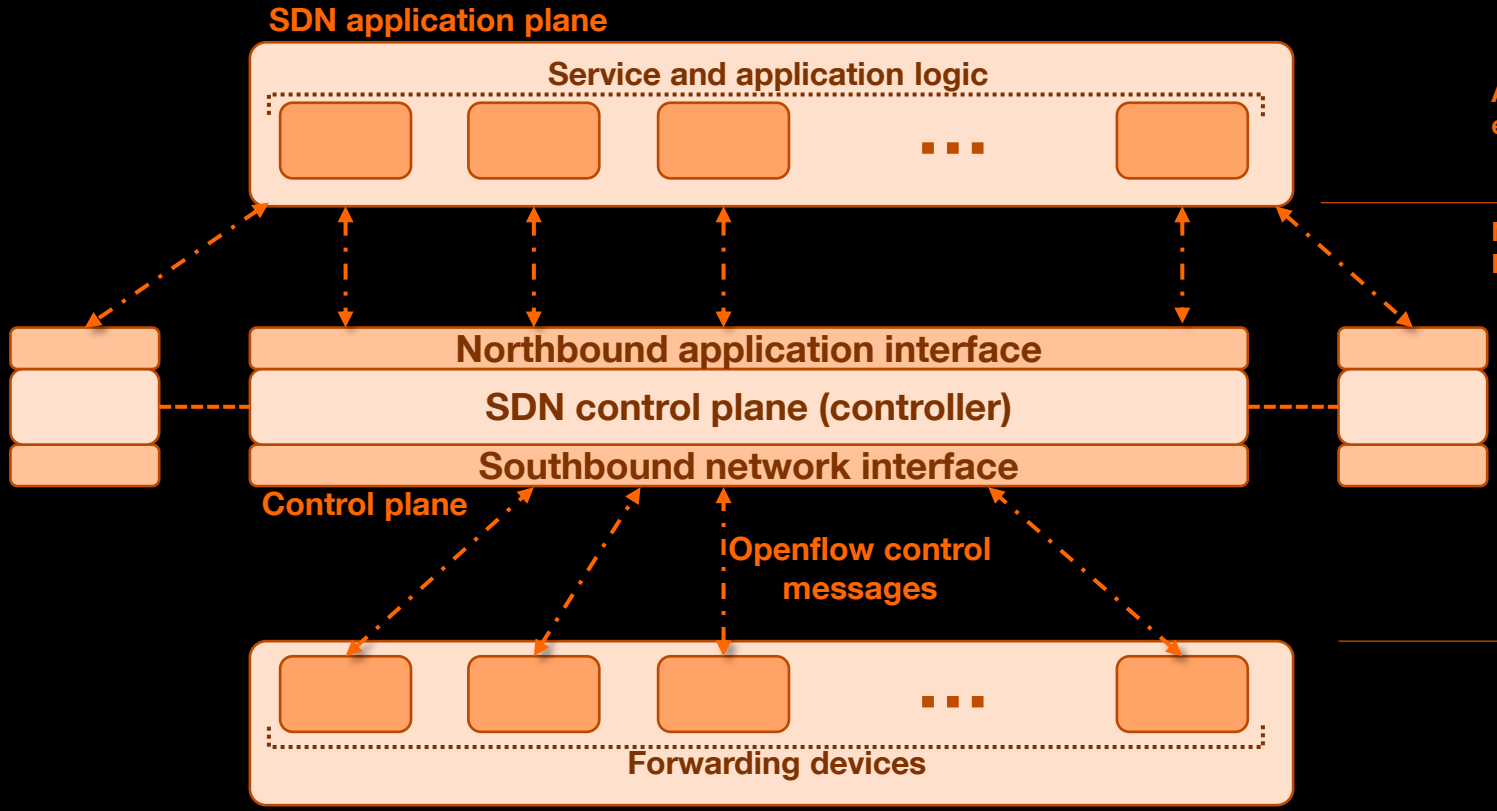
Supplies a collection of physical elements that make available both compute, data, and storage capabilities in order to execute the application logic



SDN as a Network Operating System



Global SDN Architecture



Applications:
e.g. routing, QoS, security

Northbound interface: e.g. REST, Java (not sandardized)

Controller (topology management): e.g. NOX, OpenDayLight, FloodLight,

Southbound Interface :
e.g. OpenFlow standard

Network devices, e.g. Cisco, Juniper, Alcatel

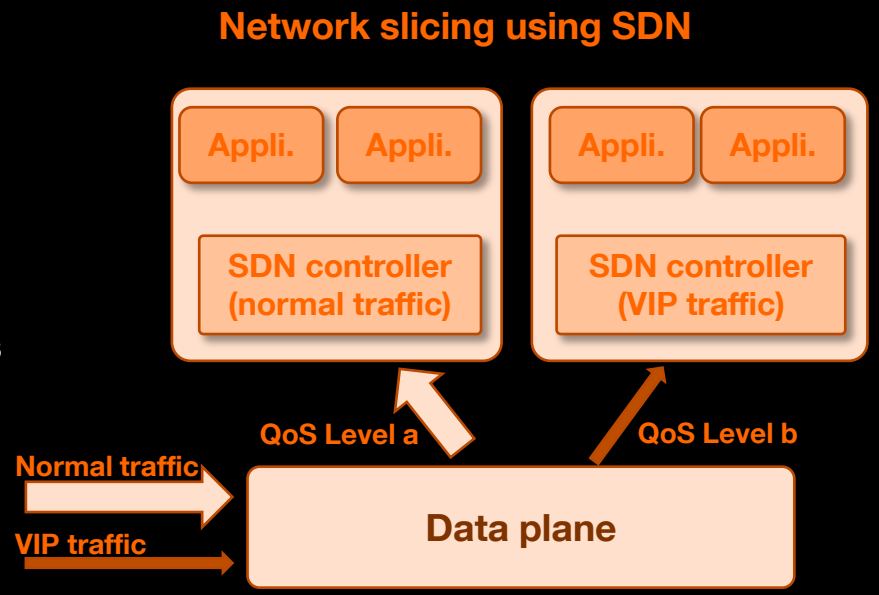
Common Benefits

Central management
Global routing policies instead of separate device configuration

Network abstraction layer
Dissociate network management from low level configuration

Adaptive/autonomic network management
Setup autonomous reaction strategies against failures and security incidents

Network slicing and isolated management
Segregate network traffic into different slices using isolated control logic



Security Challenges with SDN
Global risk overview

(1) Attacks in the data plane

- Common to legacy attacks

(2) Attacks on SDN devices

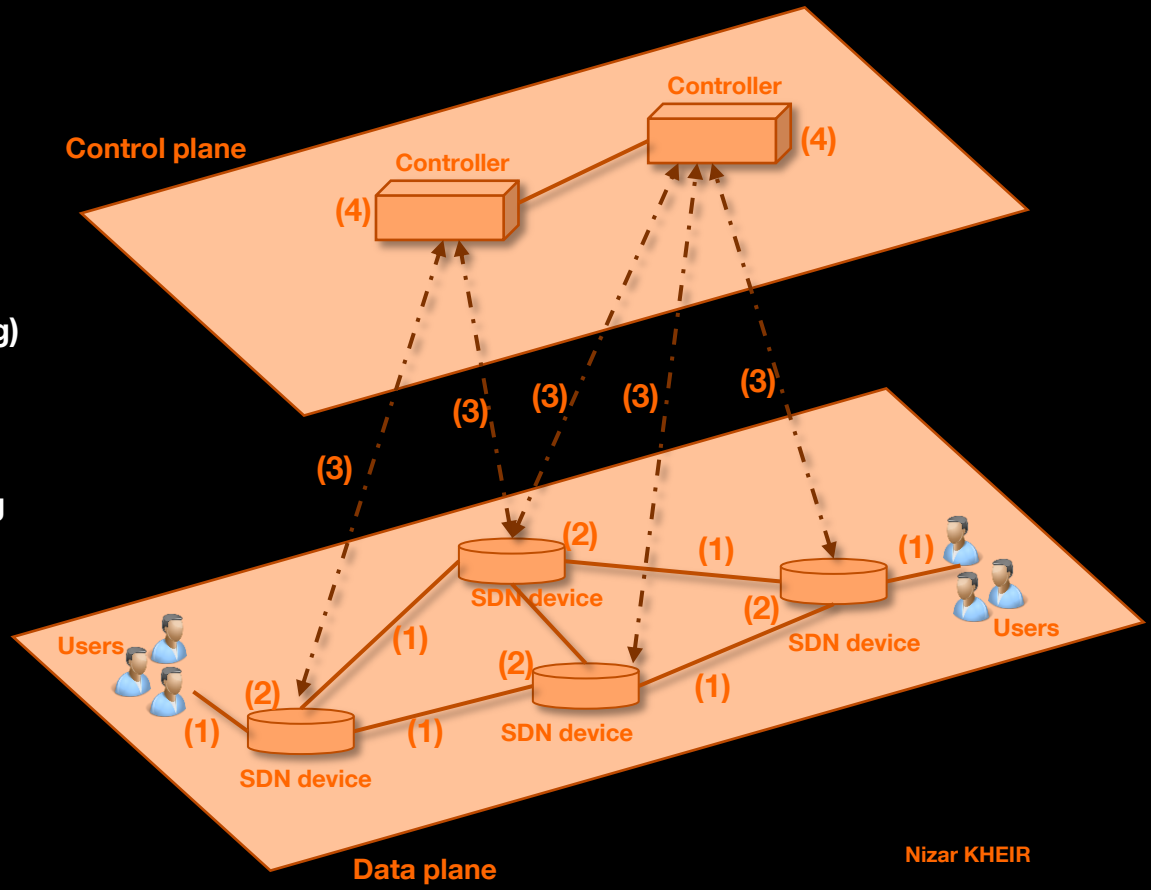
- Impact on data plane traffic
- Impact on control plane (LLDP tampering)

(3) Attacks on the control plane

- DDoS by flooding `packet_in` messages
- Topology poisoning via address spoofing (ARP, LLDP, IGMP)

(4) Attacks on the controller

- Malicious or untrusted applications
- Saturation of device forwarding tables
- Lack of isolation and conflict resolution

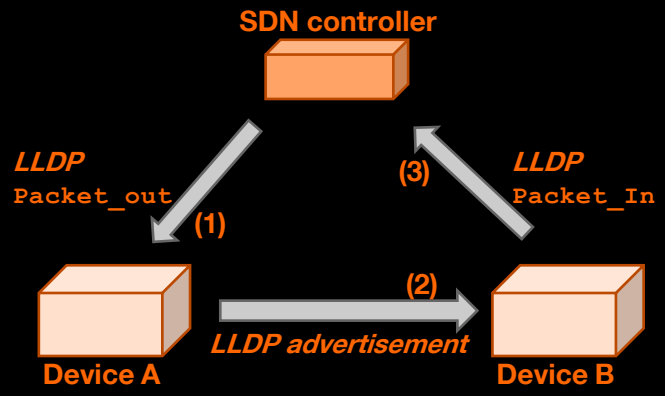


Topology Poisoning Attacks on SDN
Data plane link fabrication attack

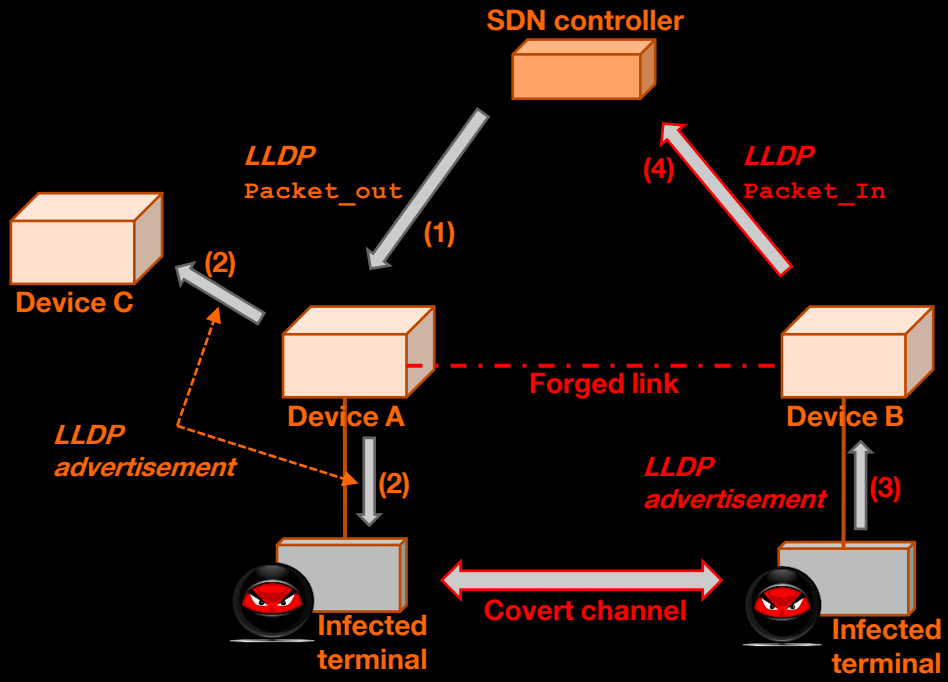
Threat model and constraints

- Attacker controls only few virtual machines connected to the SDN network

Link Discovery in OpenFlow networks



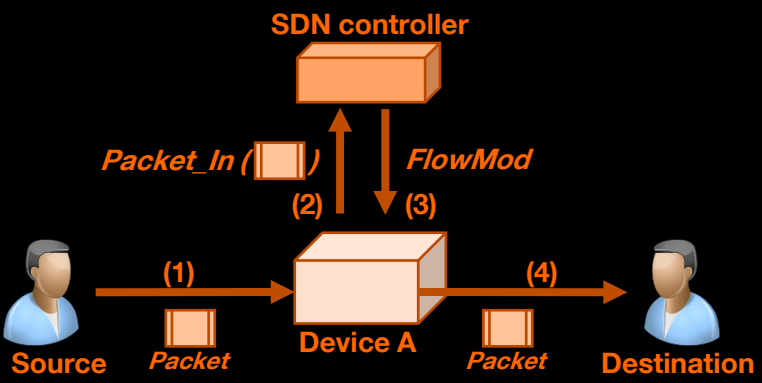
Link fabrication attack mechanism

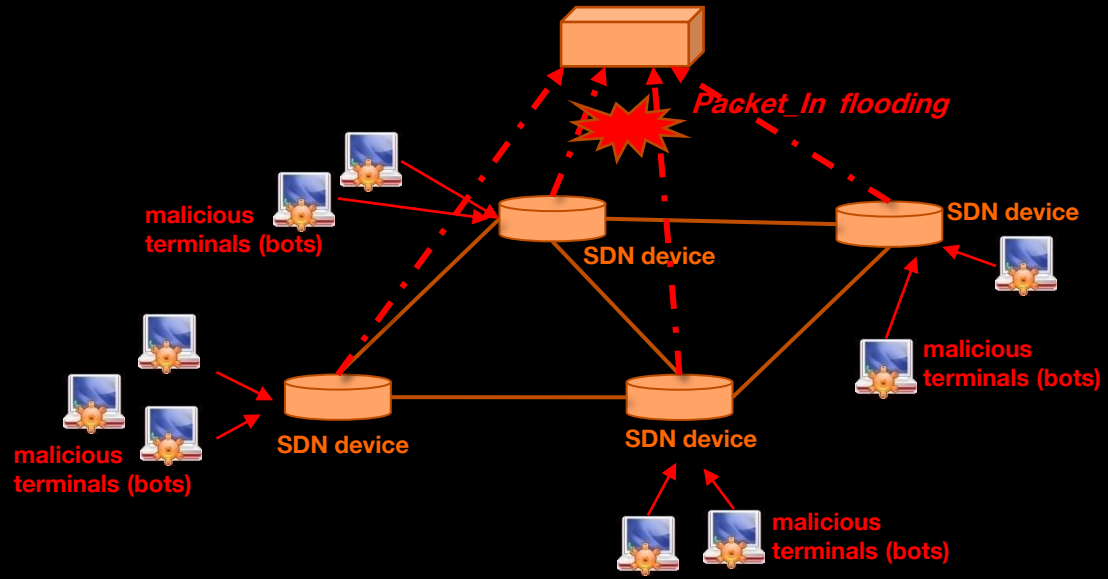


Control plane saturation attacks
Flooding the controller with `Packet_In` messages

Limited monitoring support for many security applications in openFlow

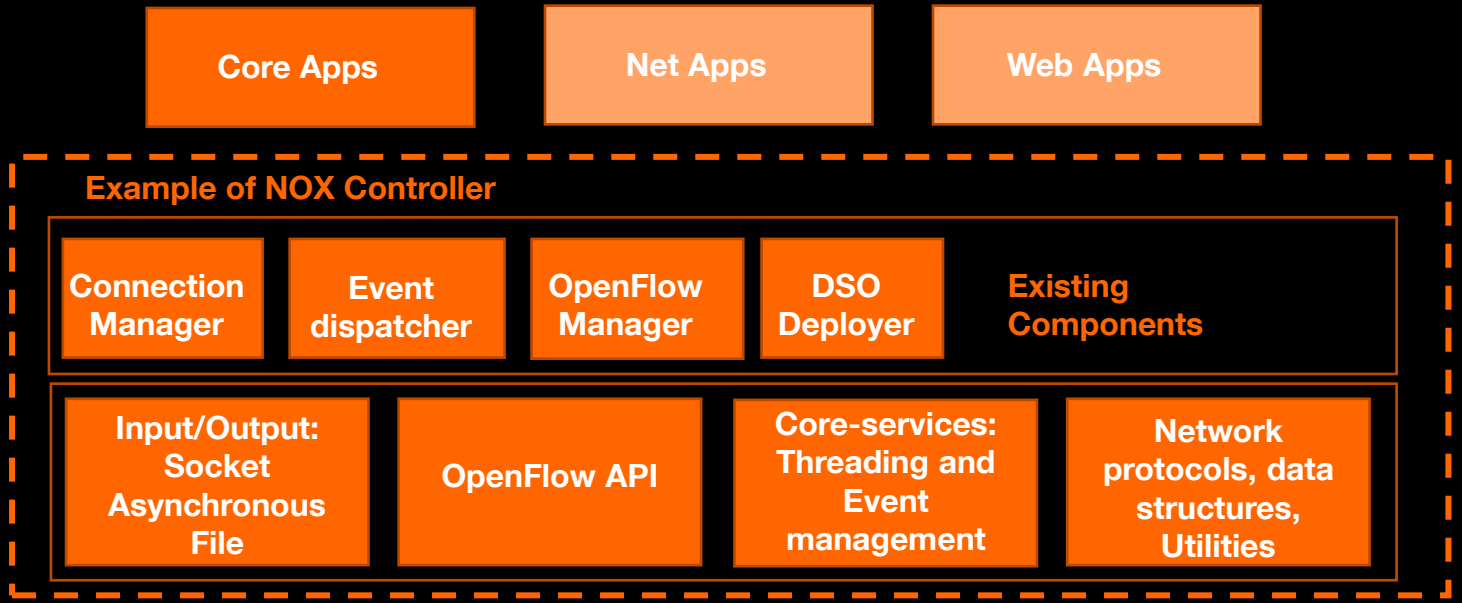
Inherent communication bottleneck between control and data planes, which enables control plane saturation attacks





Defending SDNs from malicious applications
Security Enforcement within SDN controllers

No effective mechanisms to enforce access control and conflict resolution among SDN applications

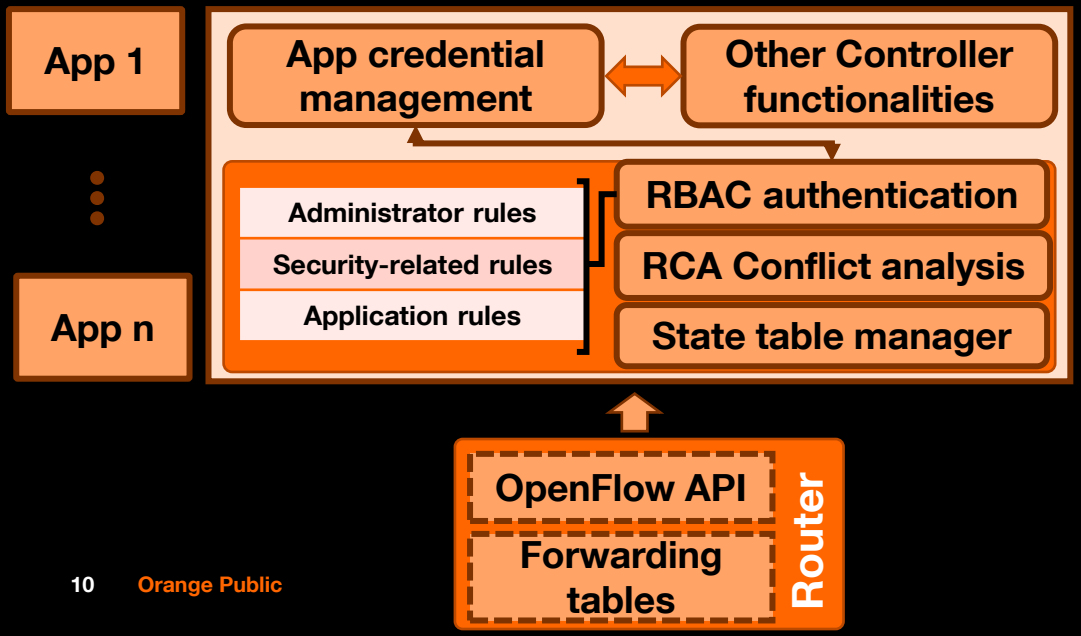


No built-in Access control management and conflict handling

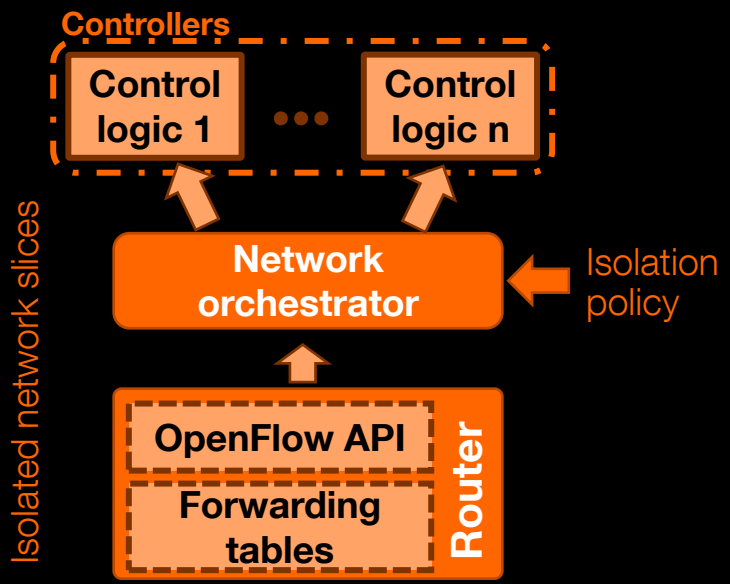
Defending SDNs from malicious applications (cont'd)
Security Enforcement within SDN controllers

Two competing directions for enforcing security and access control in SDN architectures

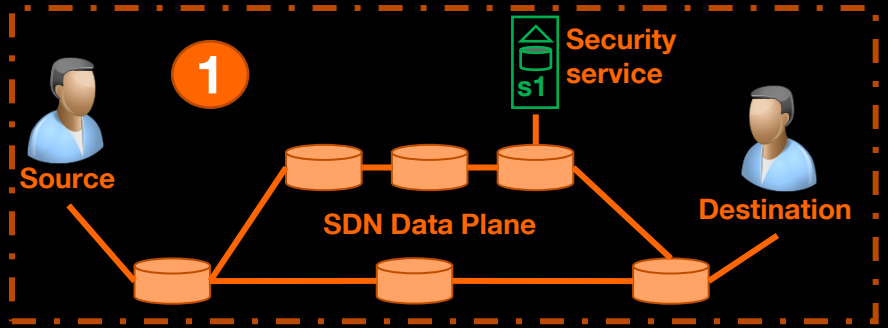
Security enforcement kernel



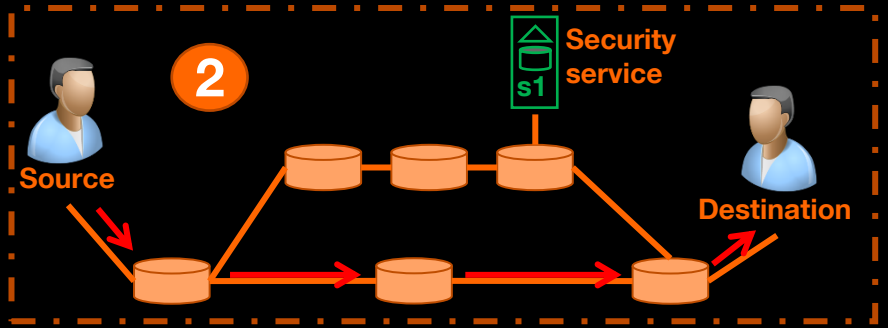
Seamless network slicing



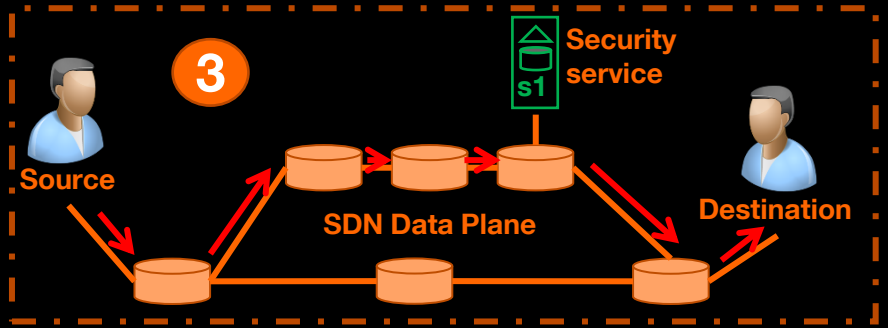
What about SDN security applications (cont'd) ?
Dynamic and lightweight composition of security services



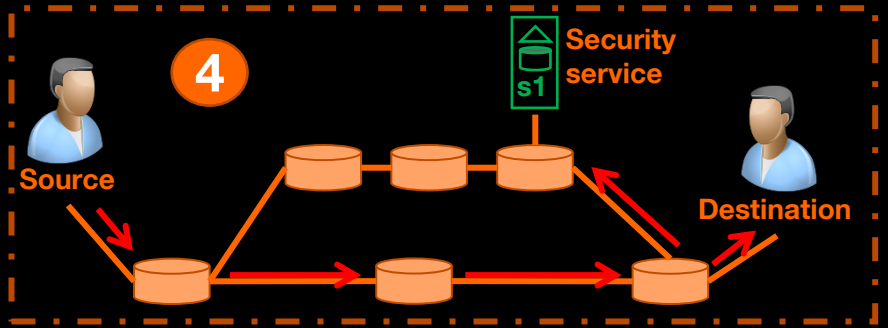
(a) Network topology



(b) No security service – Shortest path routing



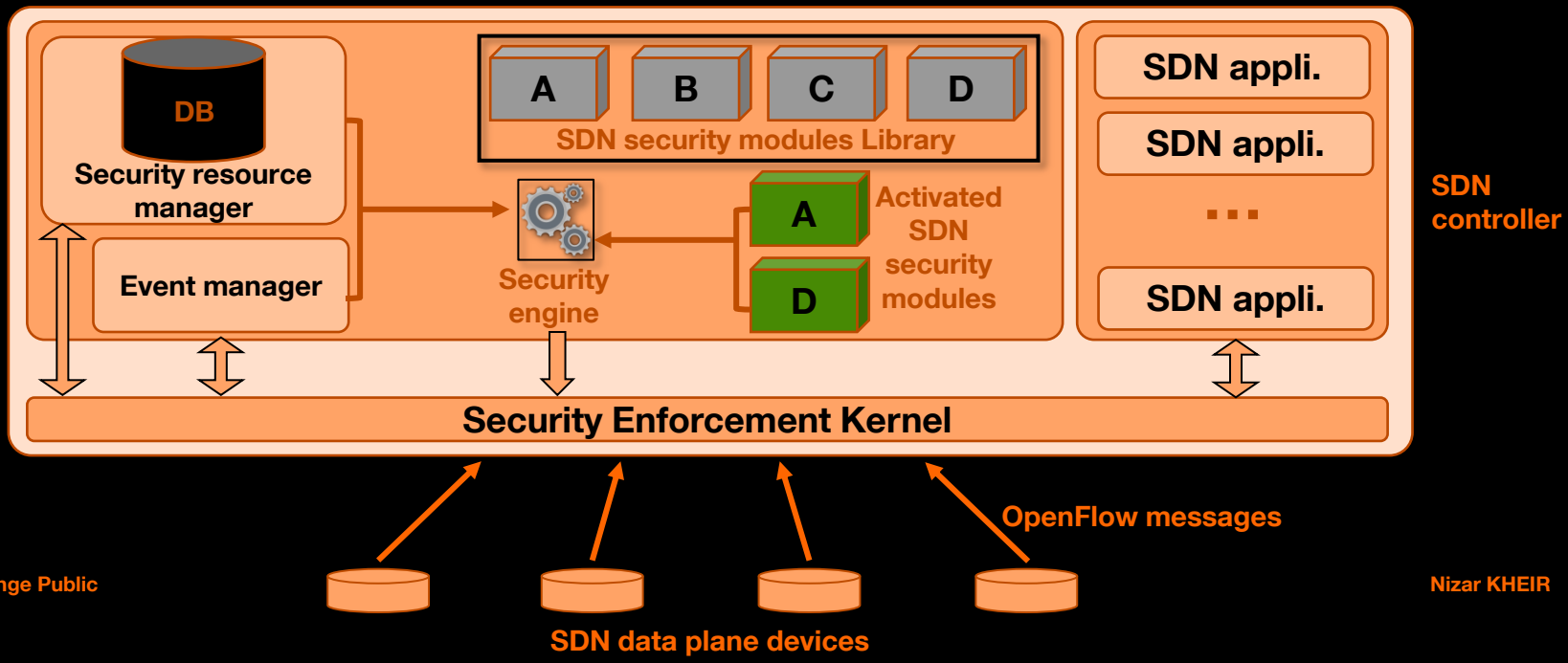
(c) Subscribed Security service – Shortest path through



(d) Subscribed Security service – Multi-shortest paths with passive monitoring

What about SDN security applications ?
Seamless and autonomic security incident management

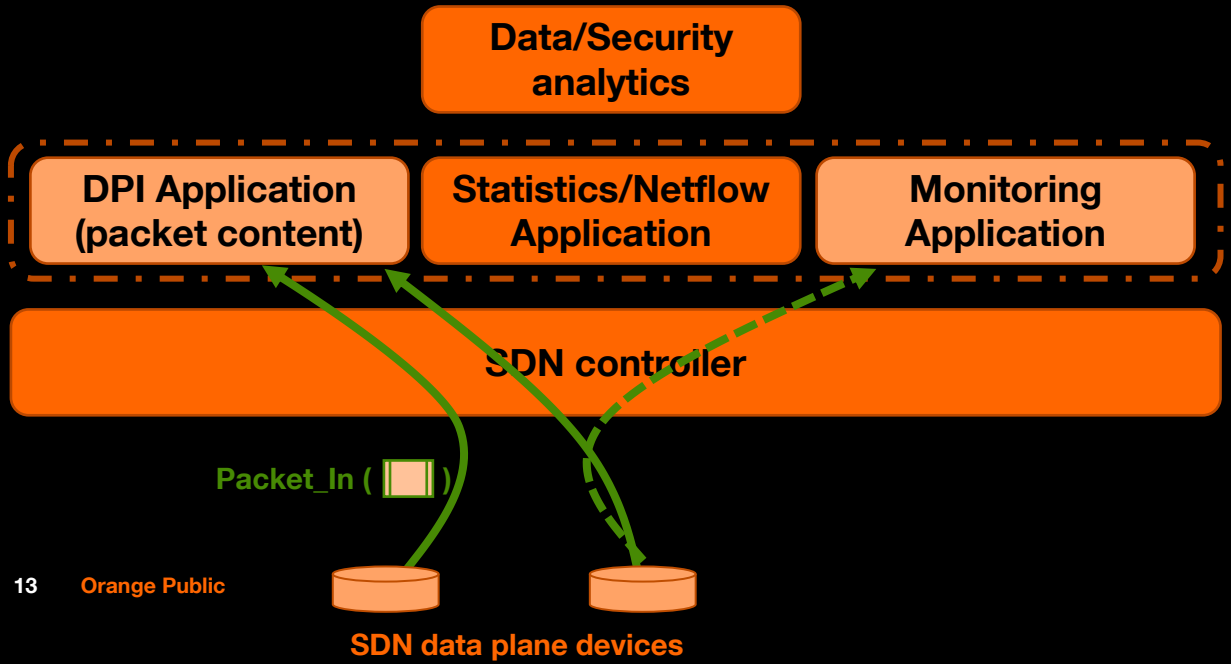
Enhancing SDN capabilities by introducing a framework for the modular composition of event-driven security services



Network security monitoring in SDN
Open issues and questions

A security monitoring framework as an SDN application

Packet content is sent to the DPI application using `Packet_In` messages



Pros:

- Straightforward approach (Leverage inherent SDN)
- No intelligence required for data plane devices

Cons:

Bottleneck since all traffic is forwarded to the controller (at least first packets of a flow)

Conclusion

SDN security challenges have sparked multiple research efforts in the recent years

- Resilience of SDN control plane => Avoid bottlenecks & single points of failure
- Management of SDN control plane => Detect and handle poisoning attacks
- Security and reliability of SDN data plane => Diagnose failures and data plane attacks
- Open innovation ecosystem => Enable isolation & security enforcement

But also several opportunities in terms of enhancing autonomic security monitoring

- Bridge the longstanding gap between detection and remediation of security incidents
- Network layer abstraction, which enables comprehensive security management and dissociates security mechanisms from low level configuration

Thank you

June 30th, 2015

SEC2 2015

Premier atelier sur la sécurité dans les Clouds

nizar.kheir@orange.com

orange™