SOFTWARE DEFINED NETWORKING AND SECURITY

CHAPTER 5 SDN AND NFV SECURITY

Dijiang Huang, Ankur Chowdhary, and Sandeep Pisharody

OUTLINE

- NFV Security Overview
- NFV Security Classification and Attacks
- NFV Security Countermeasures
- SDN Security Overview
- SDN Attacks Classification and Examples
- SDN Security Countermeasures
- OpenFlow switch and OpenFlow Protocol Security

NFV SECURITY OVERVIEW

NFV SECURITY BASICS

- NFV consists of two main function blocks - (1) NFV Management and Network Orchestrator (MANO) (2) NFV Infrastructure (NFVI)
- Security compliance using standard authentication, authorization and encryption mechanisms.
- NFV security policy enforcement.
- Security against Internal and External attacks.

NFV THREAT VECTORS

Threat Vector	Description	Impact
VNF Service Flooding	• DNS lookup based attacks. • DDoS in dataplane.	Availability
Application Crashing	Malformed packets sent by the attackers to the running services.	Availability
Eavesdropping	Attackers targeting sensitive data and control plane information.	Confidentiality
Data-Exfiltration	Unauthorized access to sensitive user profile data.	Confidentiality
Data and Traffic Modification	• Man-in-the-Middle (MITM) on network traffic. • DNS redirect to modify sensitive data.	Integrity
Control Network and Network Elements	• Exploitation of protocol vulnerabilities. • Implementation flaws. • Management plane vulnerabilities.	Control

NFV SECURITY GOALS

- Establish a secure baseline of guidance for NFV operation.
- Define areas of consideration for differentiation of security requirements of NFV and non-NFV systems.
- Provide guidelines for operational environment supporting interfaces with NFV systems and operations.

NFV SECURITY GOALS

- Ensure proper data-authentication of NFV workloads.
- Standard authorization mechanisms for NFV functions and capabilities.
- Well defined and secured mechanism for VNF lifecycle management – VNF deletion, workload migration, VNF configuration and patch management.

NFV SECURITY CLASSIFICATION AND ATTACKS

NFV SECURITY CLASSIFICATION

- Security domains of NFVI can be classified into networking, compute and hypervisor domains.
- ETSI classifies the security domain of NFV into Intra-VNF security and Extra-VNF security.
- Intra-VNF security pertains to security between VNFs. The communication path between VNFs is not restricted to network-level.
- Extra-VNF security scope includes security of physical infrastructure, external services and environment.

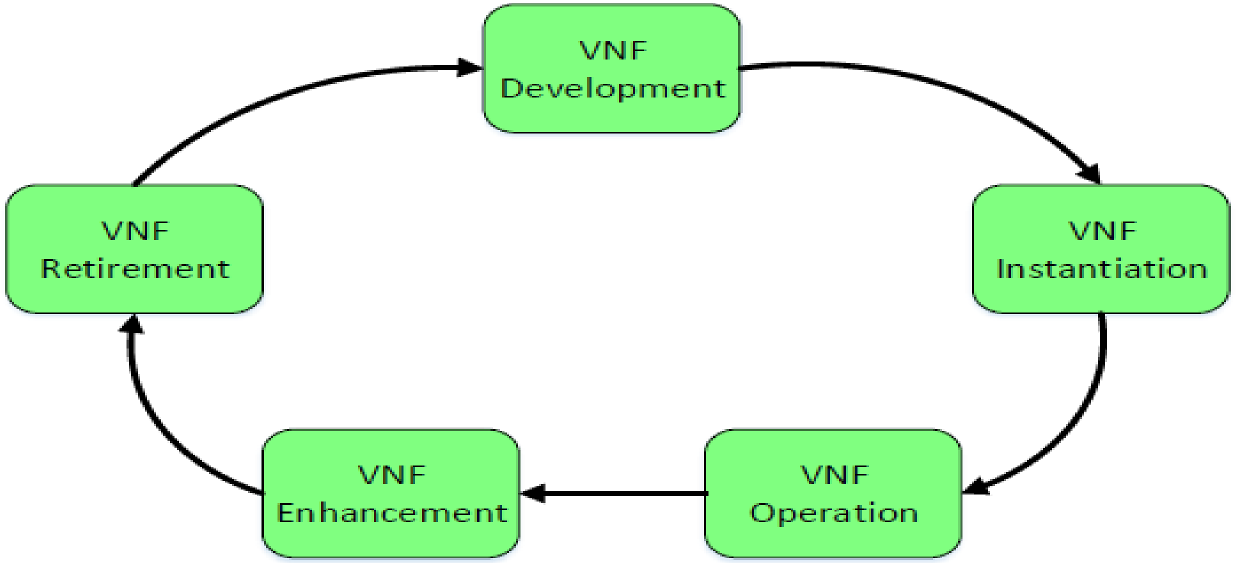
INTRA-VNF SECURITY CHARACTERISTICS

- Secured orchestration for and between VNFs.
- Security mechanism in the Intra-VNF communication and attack-resilience.
- Service Chaining capabilities should be enforced if available.
- Security and virtual appliances need to be configured as part of traffic flow.
- Flows between VNFs are often not through layer 3 firewall or any other security enforcement point.

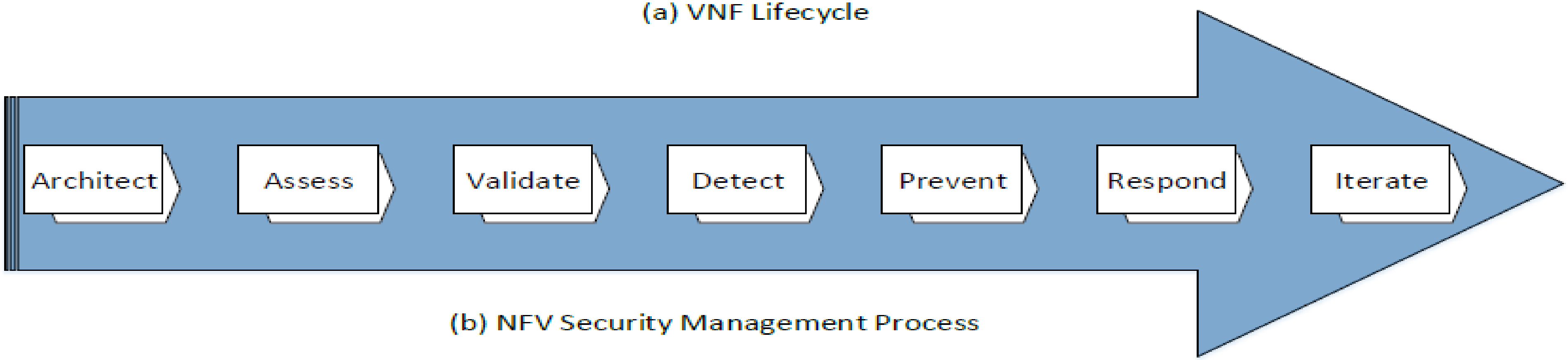
EXTRA-VNF SECURITY CHARACTERISTICS

- NFV deployment spans across several regulatory and jurisdiction domains.
- Extra-VNF security should have ability to administer cross-border and domain requirements.
- Multiple SLA and QoS requirements across regulatory domains should be satisfiable.
- Authentication, authorization, and accounting across NFV domains, humans and system entities should be enforced.

NFV SECURITY LIFECYCLE



(a) VNF Lifecycle



(b) NFV Security Management Process

NFV TARGETABLE COMPONENTS

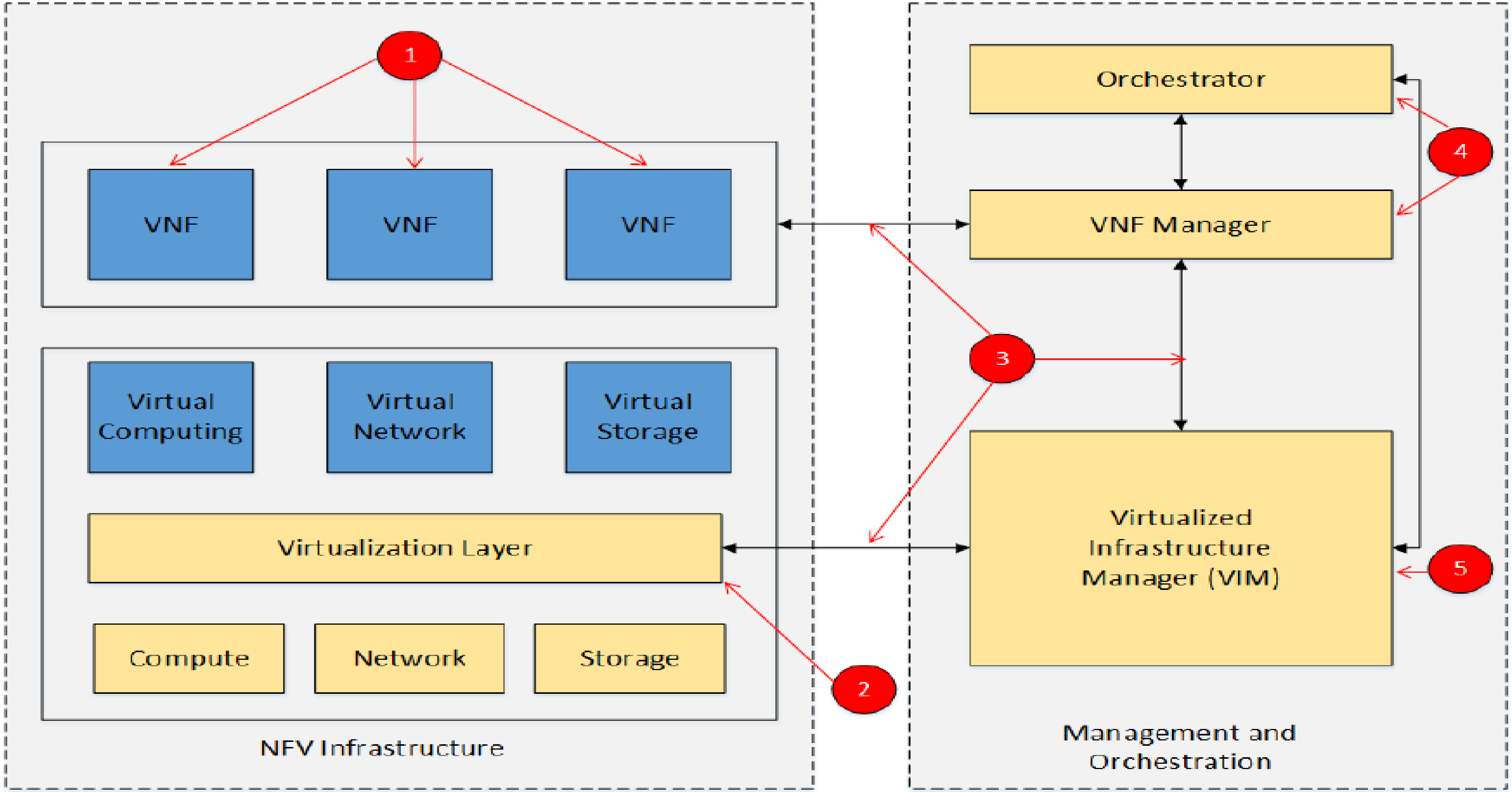
1. Virtual Network Functions: Suffer from software vulnerabilities, such as Buffer Overflow, DoS. They can be attack source or target.
2. Virtualization Layer: Security attacks such as VM privilege escalation, CPU resource monopolization, VM monitoring attacks.
3. MANO Communication: MITM attacks on the communication between NFV MANO and NFVI.

NFV TARGETABLE COMPONENTS

4. VNF Manager/ Orchestrator: NFV over OpenStack can be subjected to vulnerability exploitation, e.g., ephemeral storage vulnerability CVE-2013-7130.

5. Virtualized Infrastructure Manager (VIM): Attacks can target VM. Ruby vSphere console in VMWare vCenter Server suffers from privilege escalation vulnerability CVE-2014-3790.

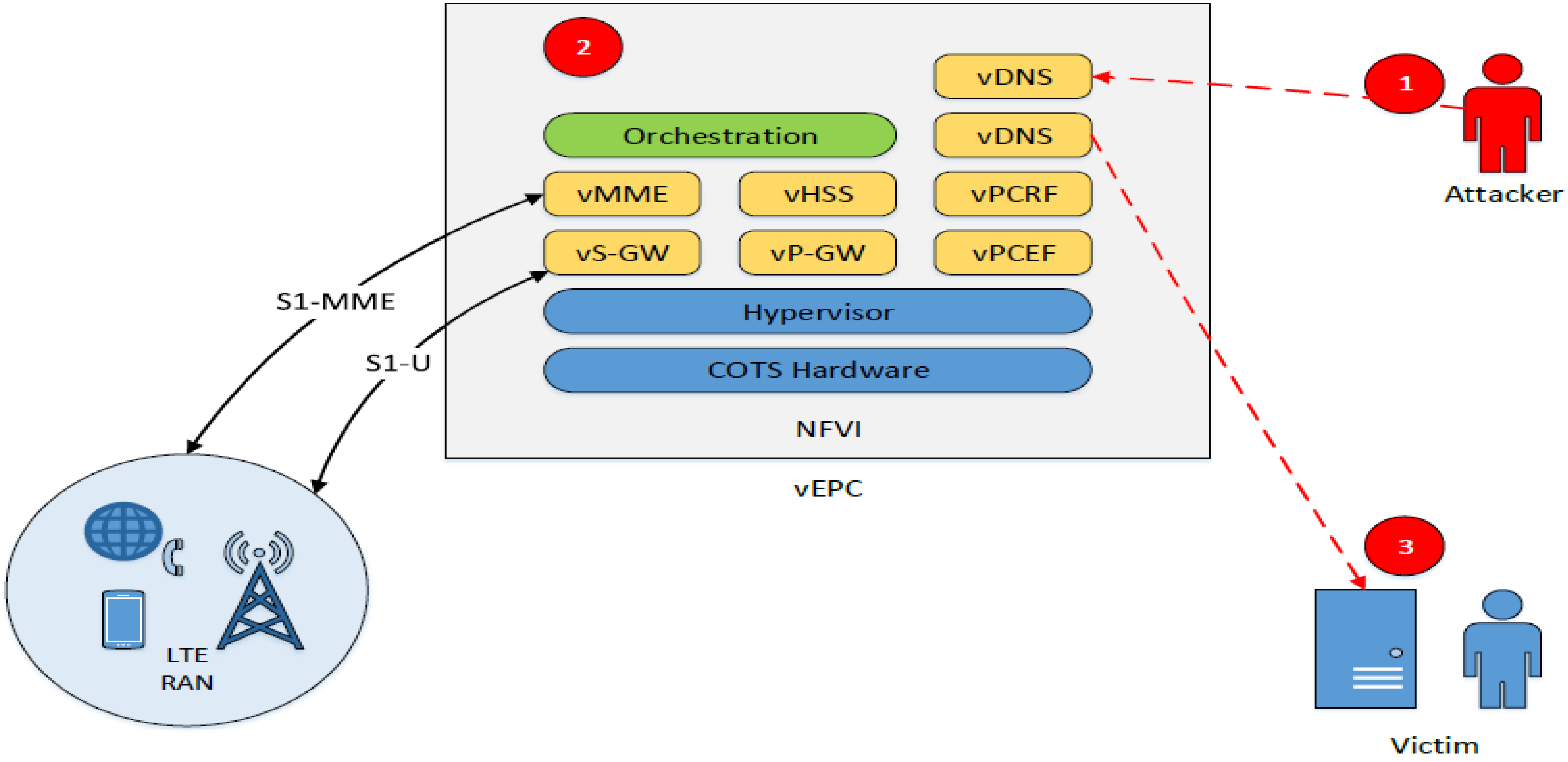
NFV TARGETABLE COMPONENTS



DNS AMPLIFICATION ATTACK

- Attack Goal: Network resource exhaustion or service availability impact.
- Attacker can target vulnerable VNFs using vulnerabilities such as remote code execution (RCE) to obtain command and control.
- The compromised VNF can serve as a proxy for launching DNS amplification attacks against other VNFs or hypervisor.

DNS AMPLIFICATION ATTACK



DNS AMPLIFICATION ATTACK

- Step 1: Attacker spoofs the IP address of the victim and launches malicious DNS queries.
- Step 2: Multiple recursive DNS-servers send the response back to the victim. In effect victim receives amplified DNS response.
- Step 3: Service unavailability/ disruption.

NFV SECURITY COUNTERMEASURES

TOPOLOGY VERIFICATION AND ENFORCEMENT

- Network topology must be validated individually for different network segments as well as together.
- Topology validation is required at different levels such as physical topology, logical topology (GRE, VLAN).
- Network topology for data-plane, control plane and management plane should be validated.

TOPOLOGY VERIFICATION: DATA PLANE

- Intra-host communication
- Inter-host communication
- Communication between VNFs and physical equipment.

TOPOLOGY VERIFICATION: CONTROL AND MANAGEMENT PLANE

- Communication within MANO.
- Path between MANO and virtualized infrastructure.
- Paths between MANO and hardware.
- Paths between MANO and the managed VNFs.

VIRTUALIZATION PLATFORM SECURITY

- Boot Integrity Protection: Secure Boot.
- Prevents boot code tampering.
- Trusted boot can be integrated with VNF manager to provide VNF launch and installation phase validation.

NETWORK AND I/O SECURITY

- Fine-grained network boundary definition.
- Efficient QoS scheme to prioritize critical tasks in case of high workload demand.
- Fine-grained network segmentation.
- Resource isolation – a) Physical segregation of hardware resources b) VNF rate-limiting c) Resource distribution between competing demands.

AUTHENTICATION, AUTHORIZATION AND ACCOUNTING (AAA)

- AAA spans across infrastructure layer and network function layer.
- Authentication: Unauthenticated disclosure of user information.
- Authorization: Physical privilege escalation by wrapping unrelated identities.
- Accounting: Lack of accounting at different network infrastructure layers can allow attacker to oversubscribe NFVI resources.

AAA COUNTERMEASURES

- Authentication of VNF images.
- Authentication of users accessing NFV MANO function blocks.
- Updates to authorized users and managers in suspended/offline images.
- API authorization between function blocks.
- Real-time monitoring, logging and reporting.
- Full line rate traffic acquisition, classification and per-subscriber/user/application accounting.

DYNAMIC STATE MANAGEMENT AND INTEGRITY PROTECTION

- Dynamic State Management – Secure VM suspend, updating ACLs for suspended VMs, secured live migration.
- Dynamic Integrity Management – VNF encryption and secured cryptographic keys storage.
- Proper analysis of VNF keys and passwords in an event of crash and consequent crash events.

SDN SECURITY OVERVIEW

SDN SECURITY BASICS

- Centralized SDN design can introduce security challenges such as DDoS.
- Each SDN layer can have multiple attack vectors.
- The communication channel between the layers, i.e., application-control plane interface can be targeted by traffic modification and eavesdropping.

SDN ATTACK CLASSIFICATION AND EXAMPLES

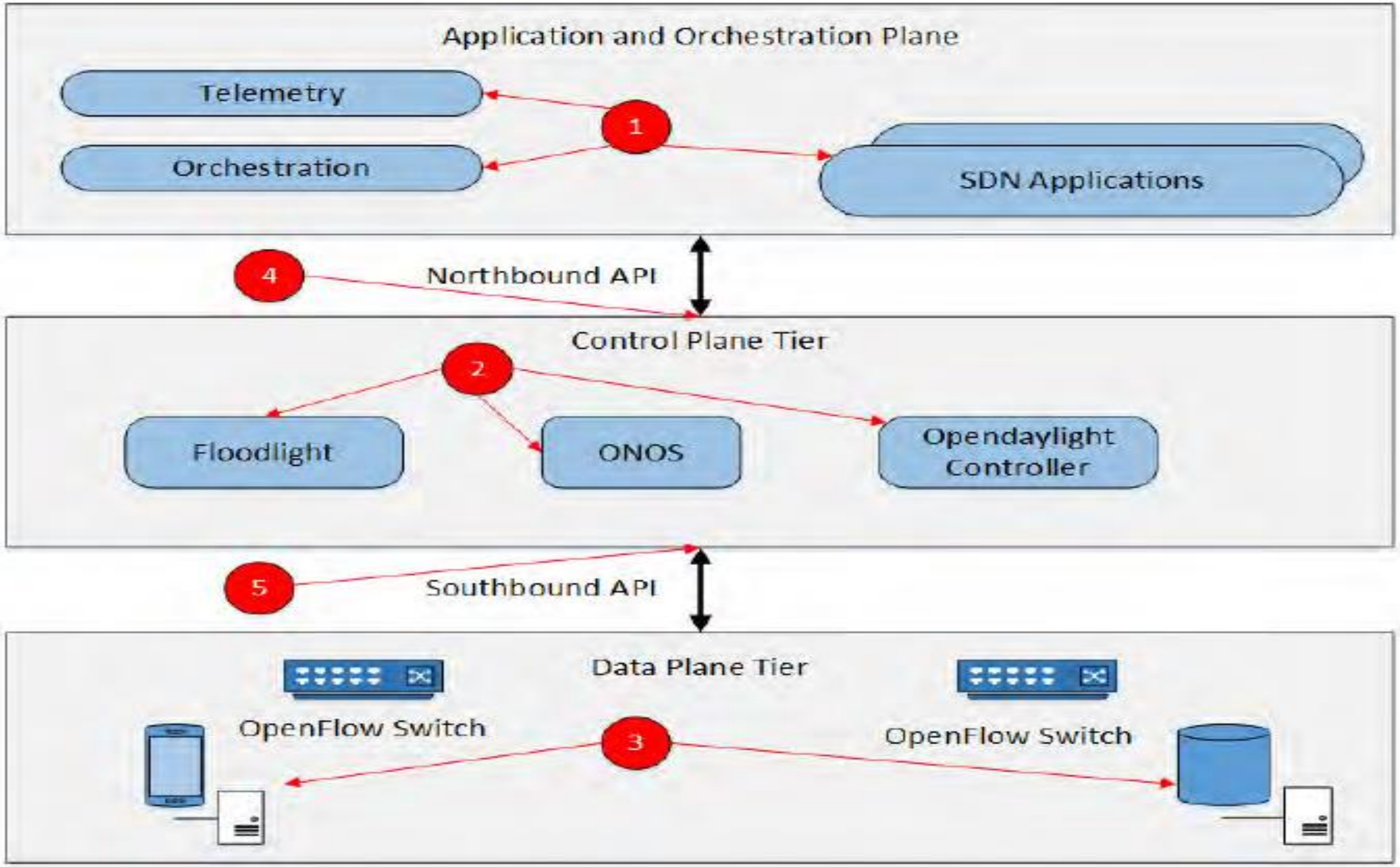
SDN TARGETABLE COMPONENTS

- Application Plane: SDN applications developed for orchestration and telemetry can have security vulnerabilities, e.g., Cross-Site Scripting (XSS).
- A compromised SDN application can infect rest of the network.
- Control Plane: Attacker can generate huge volume of traffic from spoofed IP address and send to controller.
- Switch controller communication can be saturated using forged traffic flows.

SDN TARGETABLE COMPONENTS

- Data Plane: Poison the global view of network by forging Link Layer Discovery Protocol (LLDP).
- Attackers can identify controller application logic by observing the delay between control-data plane communication.
- Communication Channel: Communication Channel between switches and controller (Southbound API), control-application tier (Northbound API) can be subjected to MITM attack.

SDN TARGETABLE COMPONENTS



SDN THREAT VECTORS

Security Attack	**SDN Layer Affected**				
	App Layer	App-Ctrl Interface	Ctrl Layer	Ctrl-Data Interface	Data Layer
Unauthorized Access					
Unauthorized Control ler Access			✓	✓	✓
Unauthenticated Application	✓	✓	✓		
Data Leakage					
Flow Rule Discovery					✓
Forwarding Channel Discovery					✓

SDN THREAT VECTORS

Security Attack	**App Layer**	**App-Ctrl Interface**	**Ctrl Layer**	**Ctrl-Data Interface**	**Data Layer**
Data Modification					
Flow Rule Modification			✓	✓	✓
Malicious Applications					
Fraudulent Rule Insertion	✓	✓	✓		
Controller Hijacking			✓	✓	✓
Denial of Service					
Controller –Switch Flooding			✓	✓	✓
Switch Flow Table Flooding					✓

SDN THREAT VECTORS

Security Attack	**App Layer**	**App-Ctrl Interface**	**Ctrl Layer**	**Ctrl-Data Interface**	**Data Layer**
Configuration Issues					
Lack of TLS			✓	✓	✓
Policy Enforcement Issues	✓	✓	✓		

SDN THREAT VECTORS

- TV1 Fake Traffic Flows: Malicious users can target TCAM switches and exhaust switch capacity.
- TV2 Switch Specific Vulnerabilities: Network switches can have vulnerabilities, such as Juniper OS (CVE-2018-0019), allows remote attacker to crash mib2d process, resulting in DoS attack.
- Attacker can also deviate traffic to steal information.
- TV3 Control Plane Communication Attack: Compromise of CA Server can lead to control plane subjugation.

SDN THREAT VECTORS

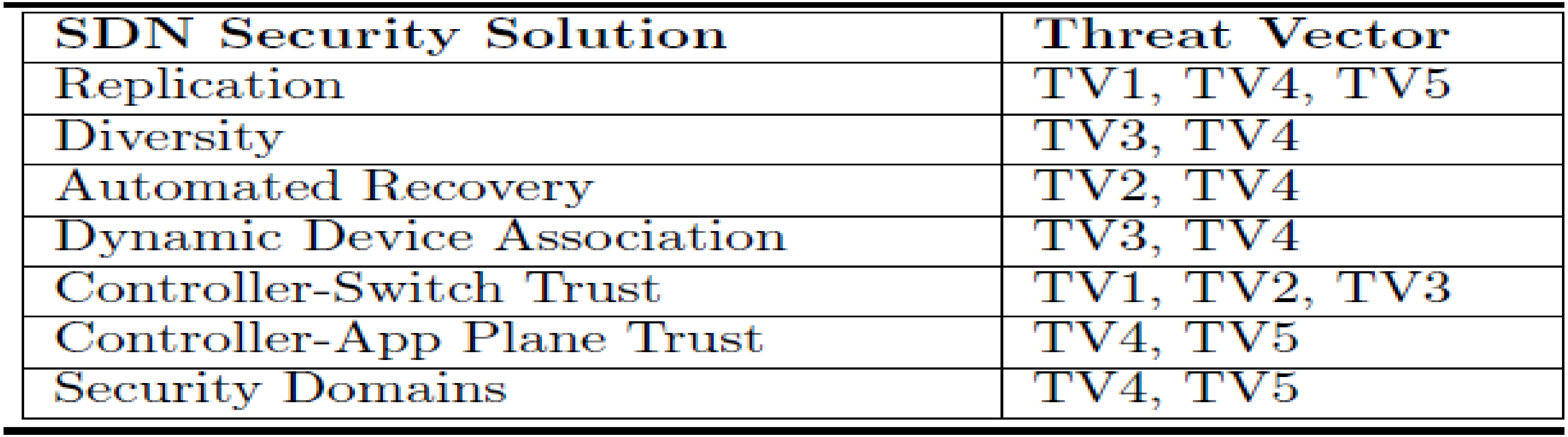
- TV4 Controller vulnerabilities: SDN controller ONOS suffers from remote DoS (CVE-2015-7516). The attacker can cause NULL pointer dereference by sending specially crafted Ethernet frames – Jumbo Frame (0x8870).
- TV5 Lack of Trust between controller and management plane: There is no built-in trust management framework.

SDN DATA PLANE ATTACKS

- Side Channel Attacks: Attacker can observe the processing time of the control plane to learn network configuration.
- Denial-of-Service (DoS): Data plane devices can send connection request to switch and saturate the switches.
- Topology Poisoning: Attacker can capture and forge LLDP packets to trigger response from switch to controller, and utilize the modified topology to launch MITM attack.

SDN SECURITY COUNTERMEASURES

SECURE AND DEPENDABLE SDN SECURITY SOLUTION



SDN Security Solution	Threat Vector
Replication	TV1, TV4, TV5
Diversity	TV3, TV4
Automated Recovery	TV2, TV4
Dynamic Device Association	TV3, TV4
Controller-Switch Trust	TV1, TV2, TV3
Controller-App Plane Trust	TV4, TV5
Security Domains	TV4, TV5

SECURE AND DEPENDABLE SDN SECURITY SOLUTION

1. Replication at application plane and control plane can help in dealing with high-traffic volume.
2. Diversity of controller software improves robustness and intrusion tolerance. Since there are only a few intersecting vulnerabilities between diverse software, common security issues can be reduced using this technique.
3. Automated Recovery using efficient proactive and reactive security mechanism such as alternate versions of controller in an event of failure providing similar functionality.

SECURE AND DEPENDABLE SDN SECURITY SOLUTION

4. Dynamic Device Association can help in automatically shifting to alternate controller in an event of failure. This also helps in providing efficient load-balancing.

5. Controller-Switch Trust using whitelisting of trusted switches and public-key infrastructure (PKI) can be used for trust management. The behavior of device (normal or anomalous) can also be considered while establishing trust.

SECURE AND DEPENDABLE SDN SECURITY SOLUTION

6. Controller-App Plane Trust using mutual trust, delegated-trust (3rd party CA) can help in preventing authentication and authorization violation attacks.

7. Security Domains can help in segmenting network into trust boundaries and quarantining the threat only to the infected network segment or trust domain.

DATA PLANE ATTACK COUNTERMEASURES

- Side channel attacks can be prevented by using timeout proxy on data plane to normalize the control plane delay. The response duration can also be randomized.
- Denial of Service (DoS) attacks can be countered using a TCP-Proxy to respond to send SYN-ACK for TCP half-open connections. Flow classification can be used to distinguish malicious and benign traffic.

DATA PLANE ATTACK COUNTERMEASURES

- Topology Poisoning Attacks can be prevented using information of neighboring devices and other packet statistics.
- If the neighboring device of an host is located at one-hop distance, the device is regarded as a host.
- Dynamic Monitoring and probing can also help reconstructing network topology.

OPENFLOW SWITCH AND OPENFLOW PROTOCOL SECURITY

OPENFLOW SECURITY ISSUES

Attack Vectors

- Passive Eavesdropping on data, control plane traffic.
- Replay attacks with non-authentic data/control plane messages, MITM attacks.

Target/Goals

- Obtaining Sensitive information in protocol messages.
- Tenant, network topology information.
- Reference data on devices implementing OpenFlow switch flow tables.

OPENFLOW COMPONENTS ATTACK COUNTERMEASURES

Component	Security Issue	Candidate Countermeasure
Physical Port	Fake Physical Port for traffic analysis.	Link state monitoring and network change tracking at controller.
Logical Ports	Port tunnel ID missing in port statistic messages.	Control based tunnel ID checking.
Reserved Ports	Controller unable to collect reserved port information.	Enable API for controller to query ports.
Counters	Counter rollback out of control.	Control-flow table synchronization.
Connection Setup	TLS protection for TC header missing.	TCP-AO for header protection, switch management protocol for key and certificate management.

OPENFLOW COMPONENTS ATTACK COUNTERMEASURES

Component	Security Issue	Candidate Countermeasure
Encryption	Message Communication authentication missing.	Multiple types of authentication and encryption protocols should be present.
Multiple Controllers	Security Policy conflict between controllers.	Mutual authentication and synchronization across controllers. Role based authentication.
Auxiliary Connections	Lack of verification mechanisms against invalid DPID.	Alert mechanism in controller when invalid DPID is present. Use authentication for auxiliary and main connections.

CITE THIS WORK

```
@book{huang2018software,
title={Software-Defined Networking and Security: From Theory to Practice},
author={Huang, Dijiang and Chowdhary, Ankur and Pisharody, Sandeep},
year={2018},
publisher={CRC Press}}
```