Taxonomic Modeling of Security Threats in Software Defined Networking

Jennia Hizver
PhD in Computer Science

UBM Tech

Agenda

- SDN Adoption Rates
- SDN Attack Surface
- SDN Threat Model
- Attack Examples
- Threat Mitigation

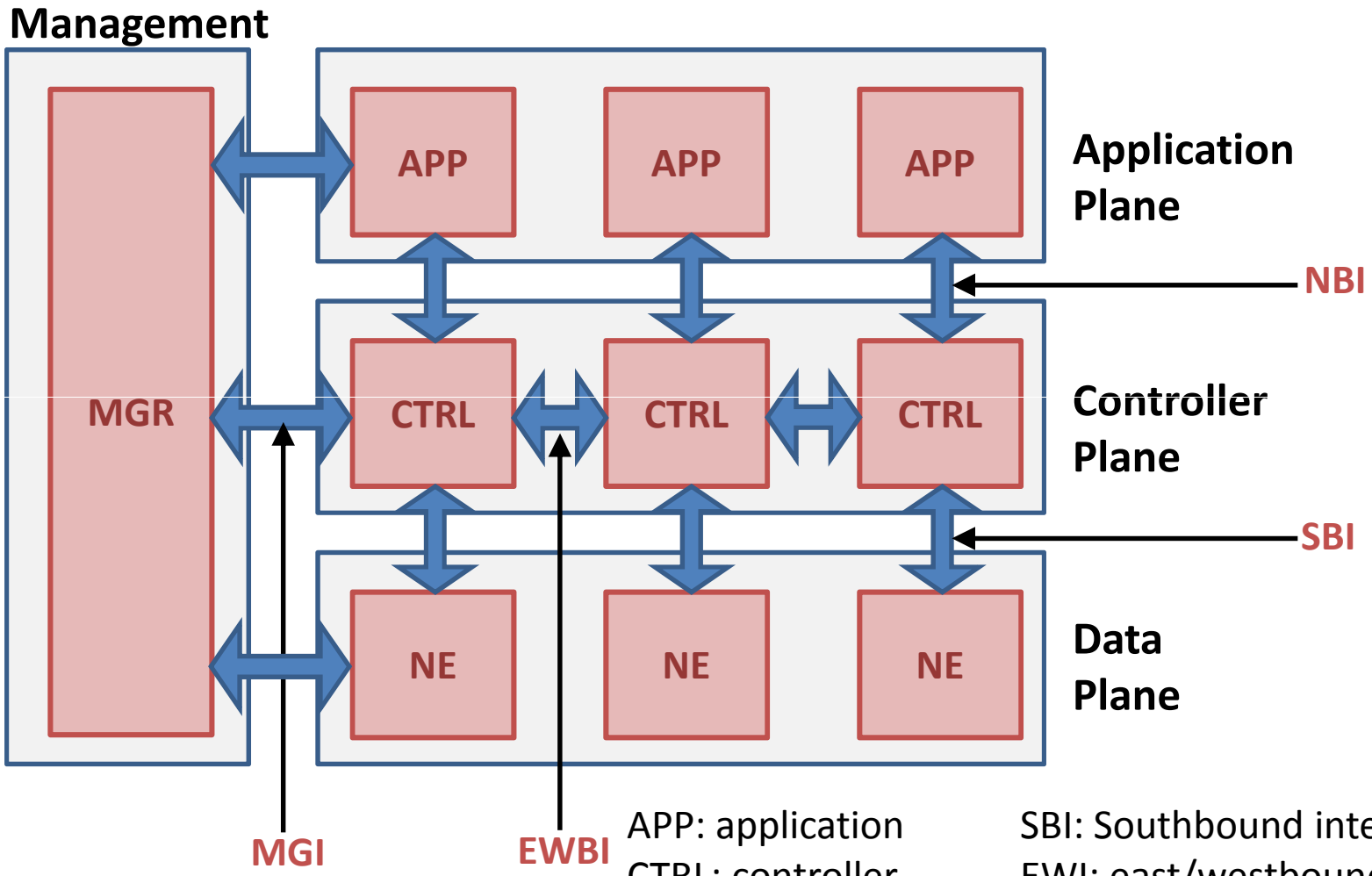
SDN Adoption Rates

- By the end of 2016, more than 10,000 enterprises worldwide will have deployed SDN in their networks (Gartner, 2014)
- 75% of the surveyed companies planned on SDN deployments in the next 5 years (Gartner, 2014)
- The worldwide SDN market will reach $8 billion by 2018 (International Data Corporation, 2014)

Security of SDN

- Limited knowledge on SDN vulnerabilities, threats, and attacks
- Increased architecture complexity => increased risk
- Vendors jumping on the SDN bandwagon => no time for secure SDLC
- No existing SDN threat identification framework

SDN Attack Surface



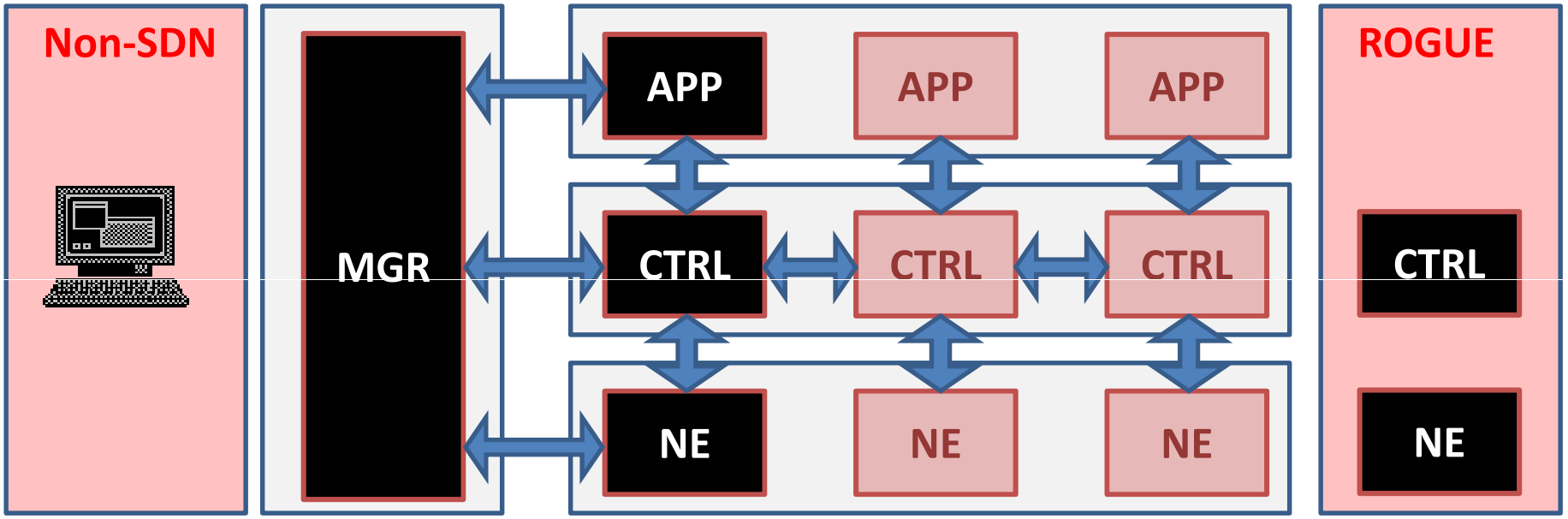
APP: application
CTRL: controller
NE: network element
MGR: manager

SBI: Southbound interface
EWI: east/westbound interface
NBI: northbound interface
MGI: management interface

SDN Threat Characterization

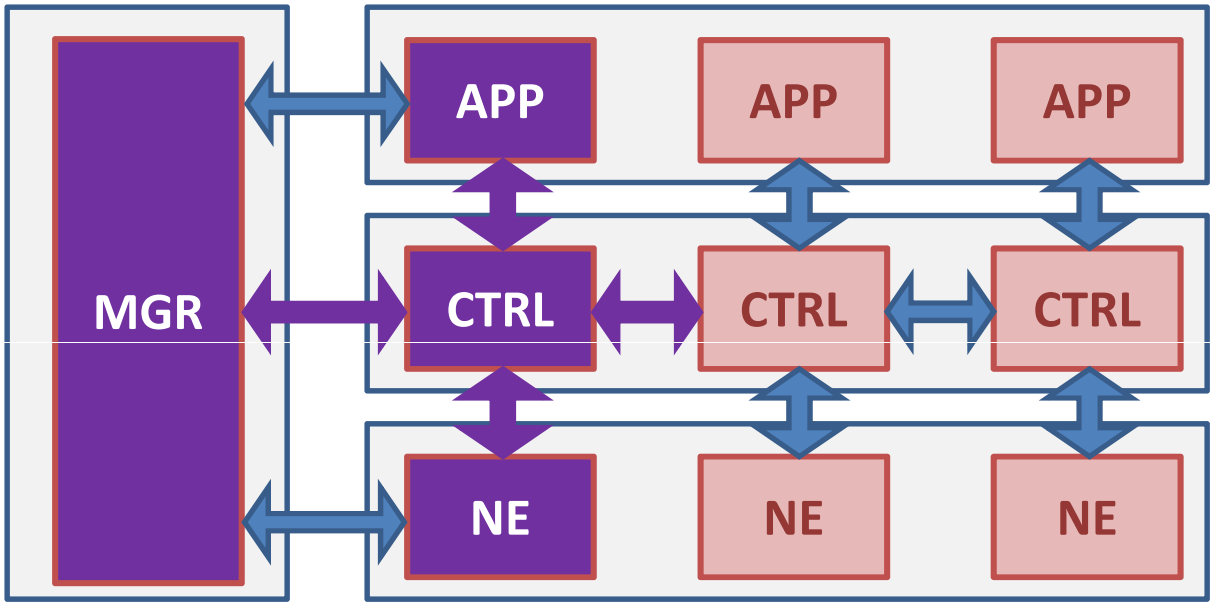
- Threat source - source triggering the vulnerability
- Vulnerability source - a SDN component where the vulnerability arises
- Threat action - by which a threat is carried out

Threat Sources



APP: application
CTRL: controller
NE: network element
MGR: manager

Vulnerability Sources

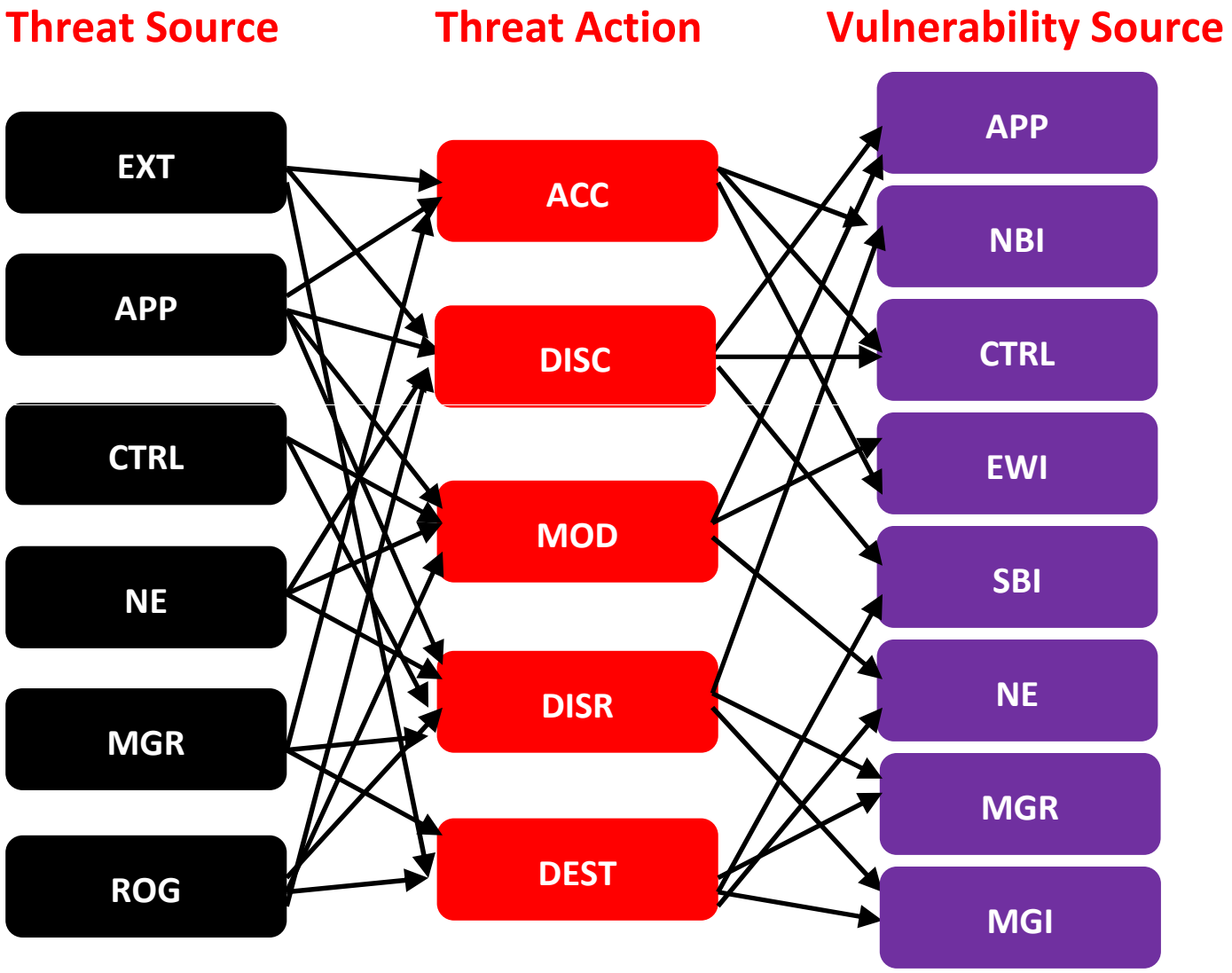


APP: application
CTRL: controller
NE: network element
MGR: manager

Threat Actions

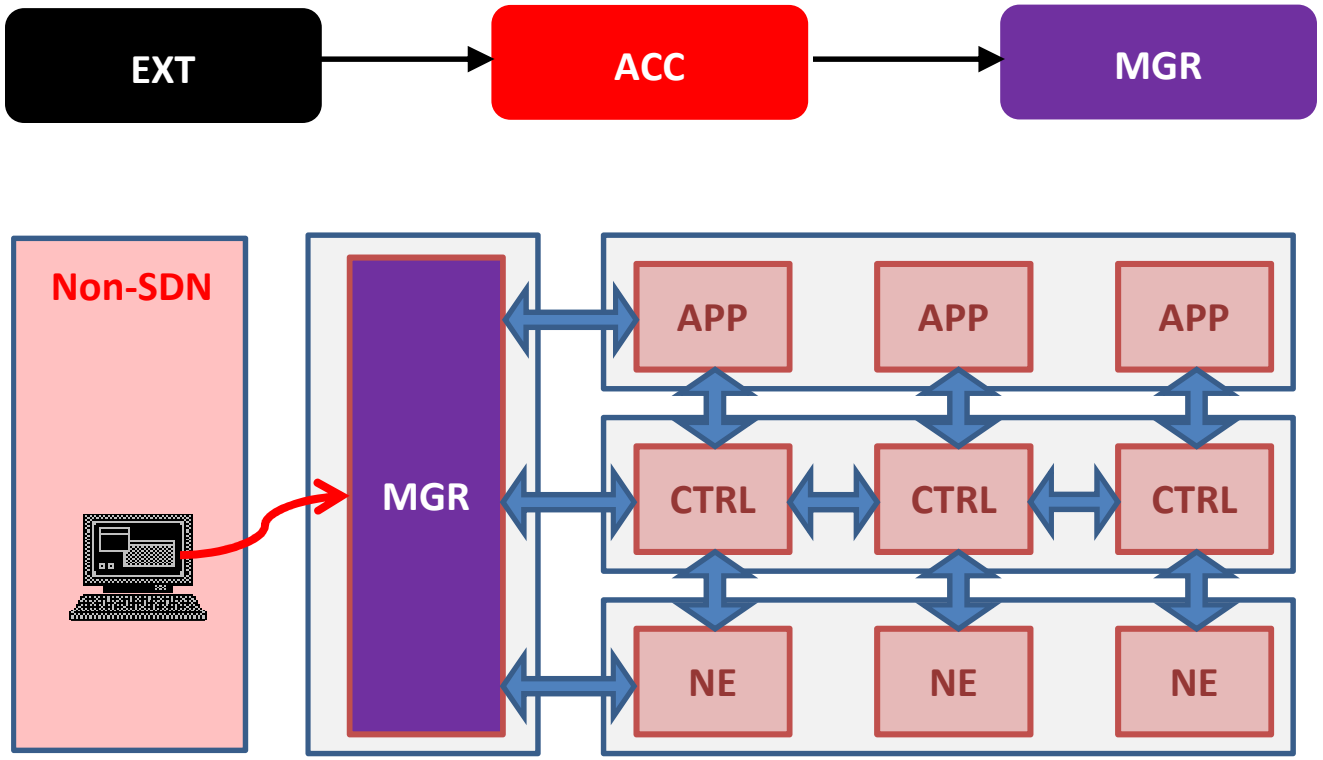
- "A threat is any event with the potential to adversely impact organizational operations and assets … through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service." - NIST Special Publication 800-30
- Threat Actions:
  - Unauthorized access (ACC)
  - Unauthorized disclosure (DISC)
  - Unauthorized modification (MOD)
  - Disruption of service (DISR)
  - Unauthorized destruction (DEST)

Many-To-Many Relationships



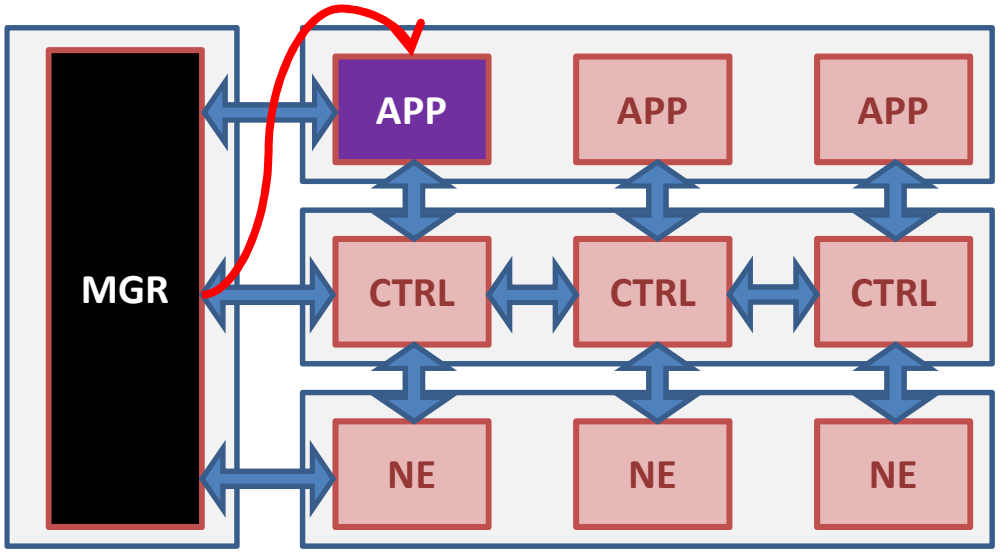
Unauthorized Access

An attacker conducts a password brute-forcing or password guessing attack



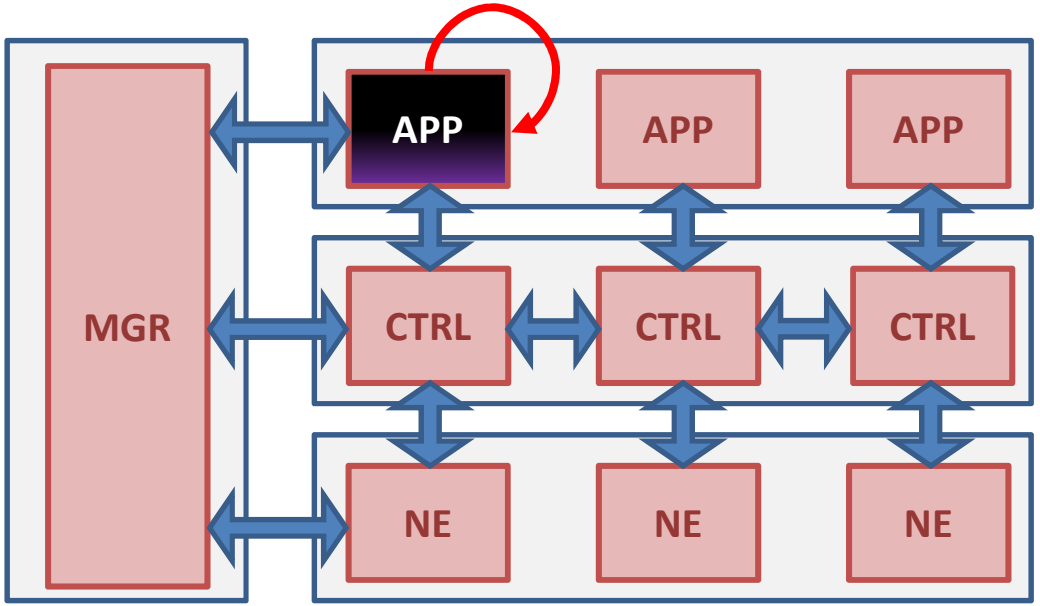
Unauthorized Access

An attacker exploits a software vulnerability to achieve unauthorized access



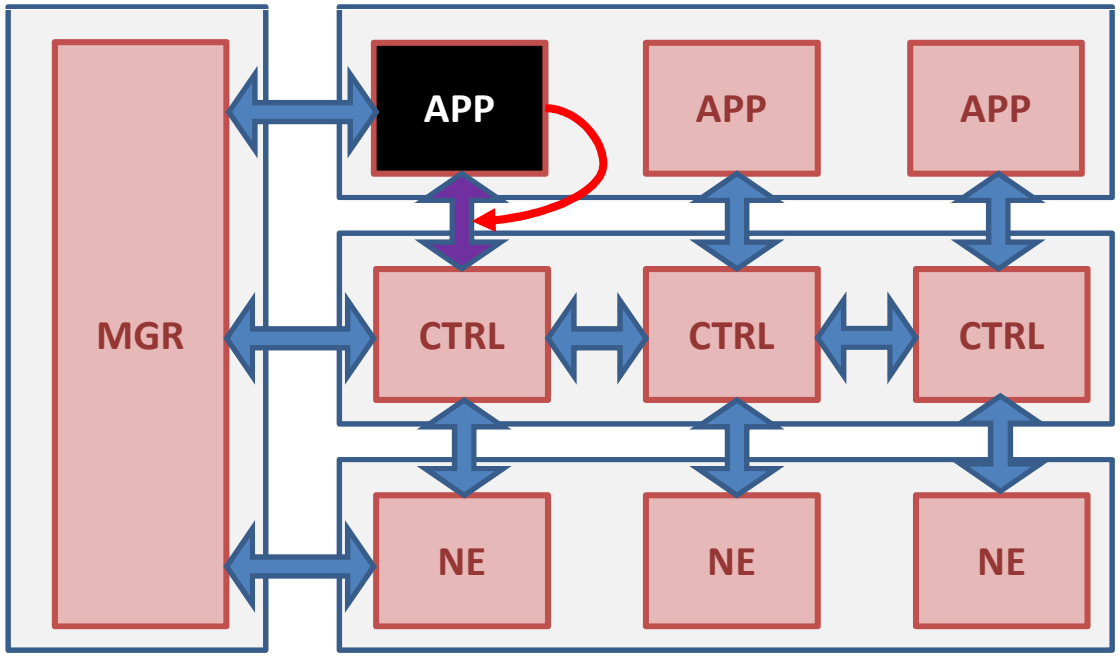
Disclosure of Information

An attacker scans the physical memory to extract flow rules



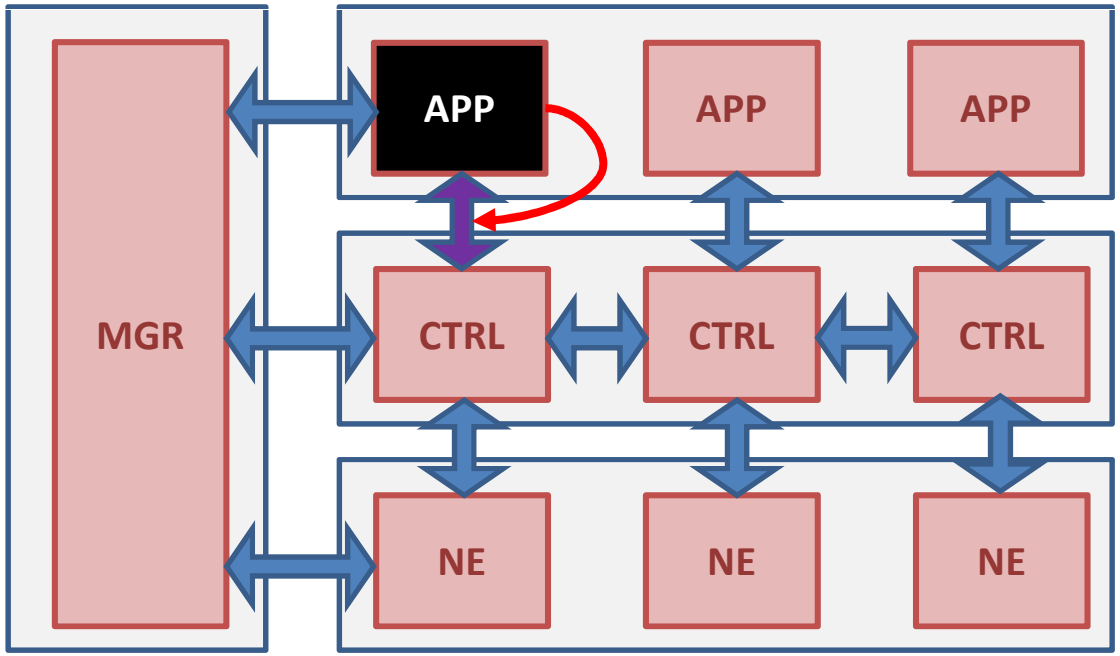
Disclosure of Information

An attacker exploits an API vulnerability to harvest information about flow rules



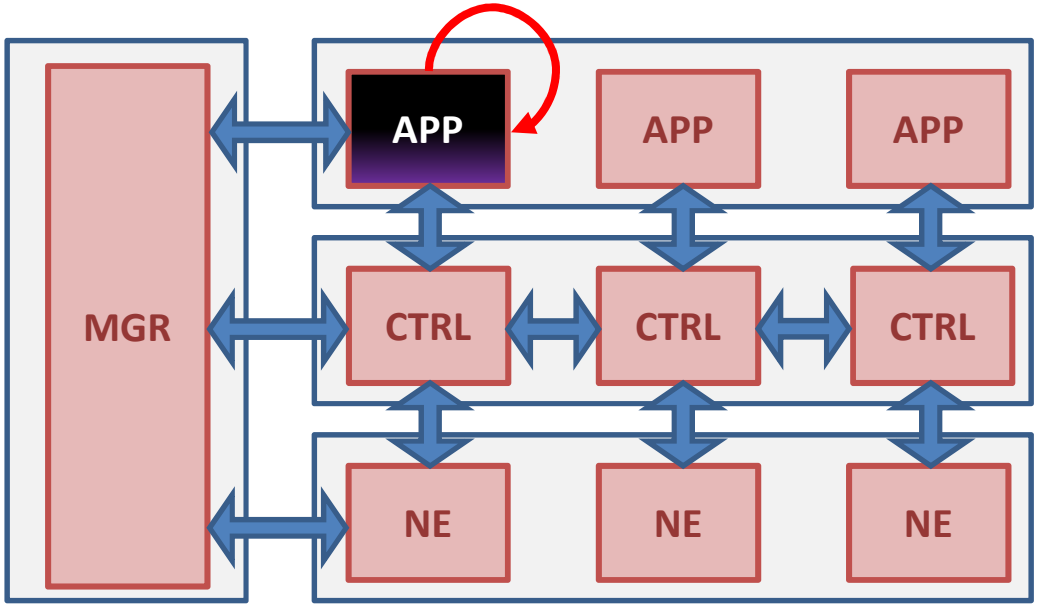
Unauthorized Destruction

An attacker exploits an API vulnerability to delete flows



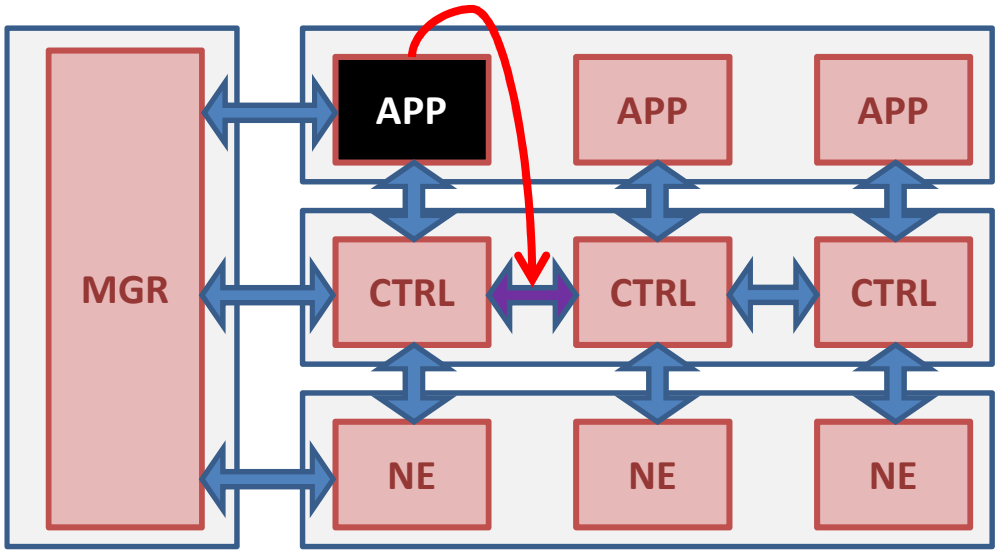
Unauthorized Access

An attacker with limited privileges exploits a software vulnerability to escalate her privileges



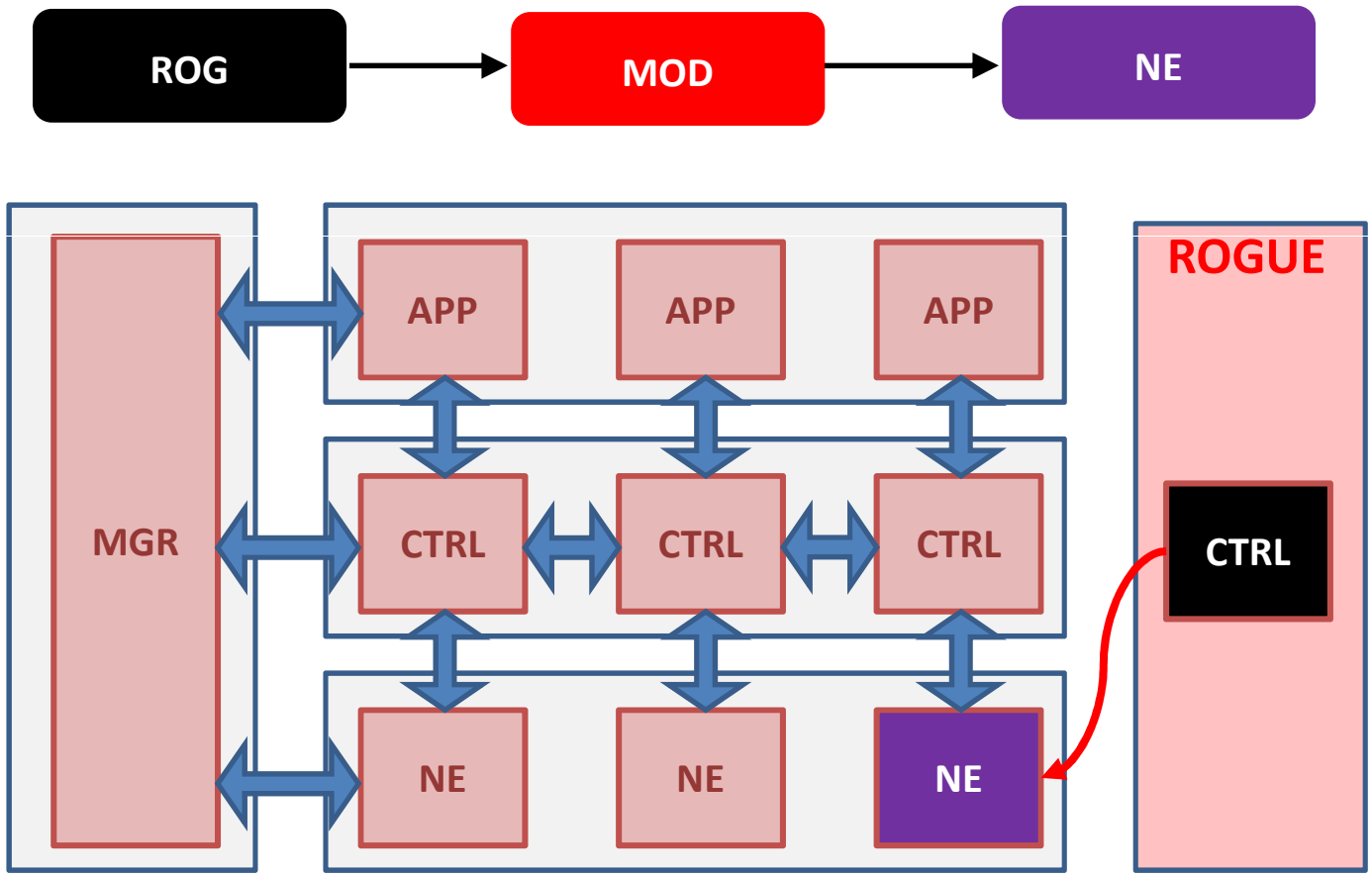
Disclosure of Information

An attacker intercepts communications to gain access to transmitted information



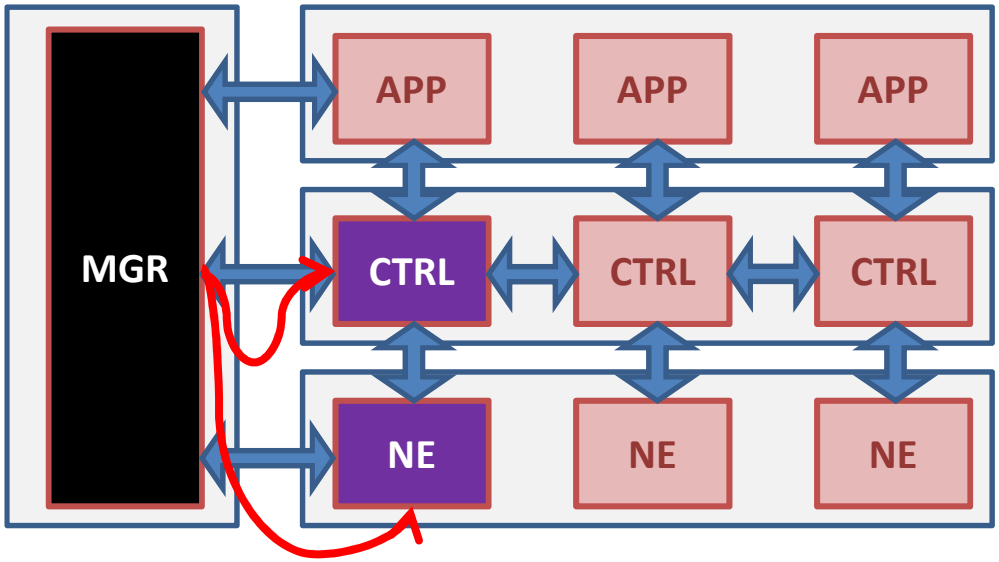
Unauthorized Modification

An attacker conducts an identity spoofing attack



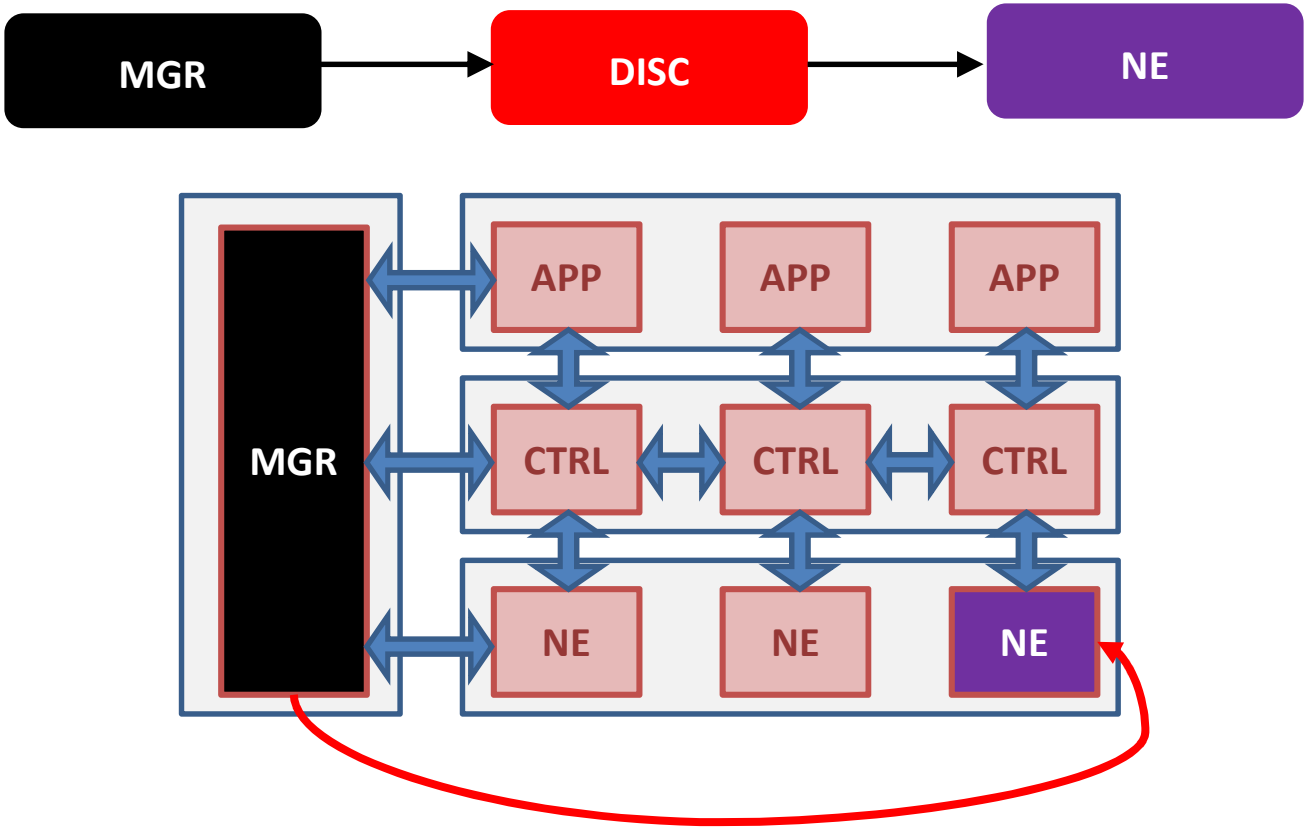
Disruption of Service

An attacker exploits a software vulnerability to cause DoS



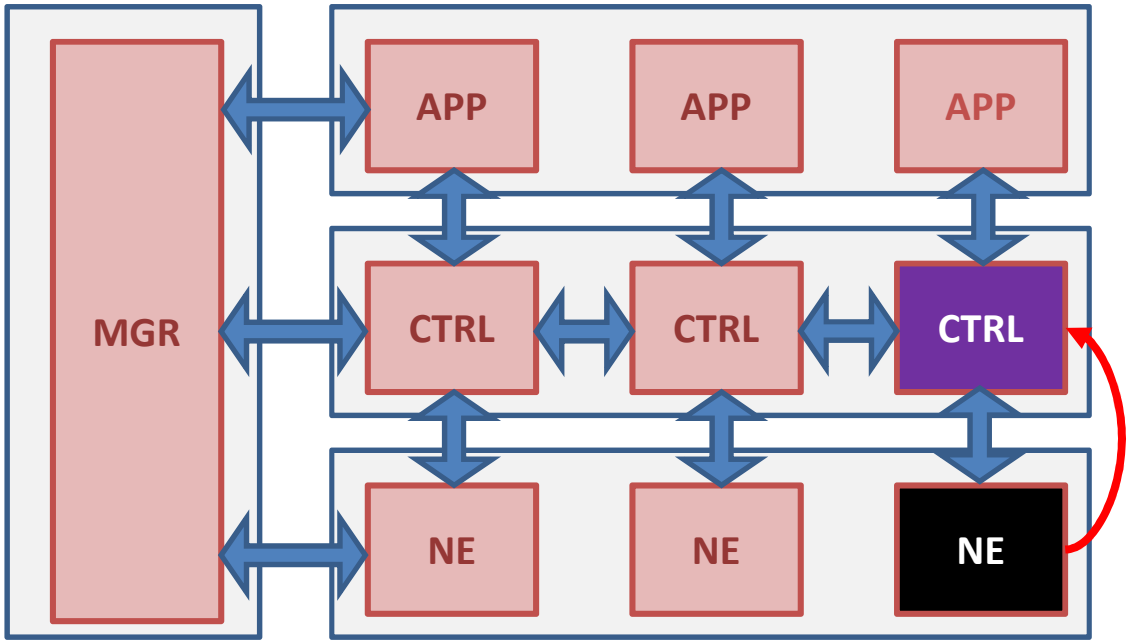
Disclosure of Information

A attacker tries to determine if a flow rule exists using a side channel attack



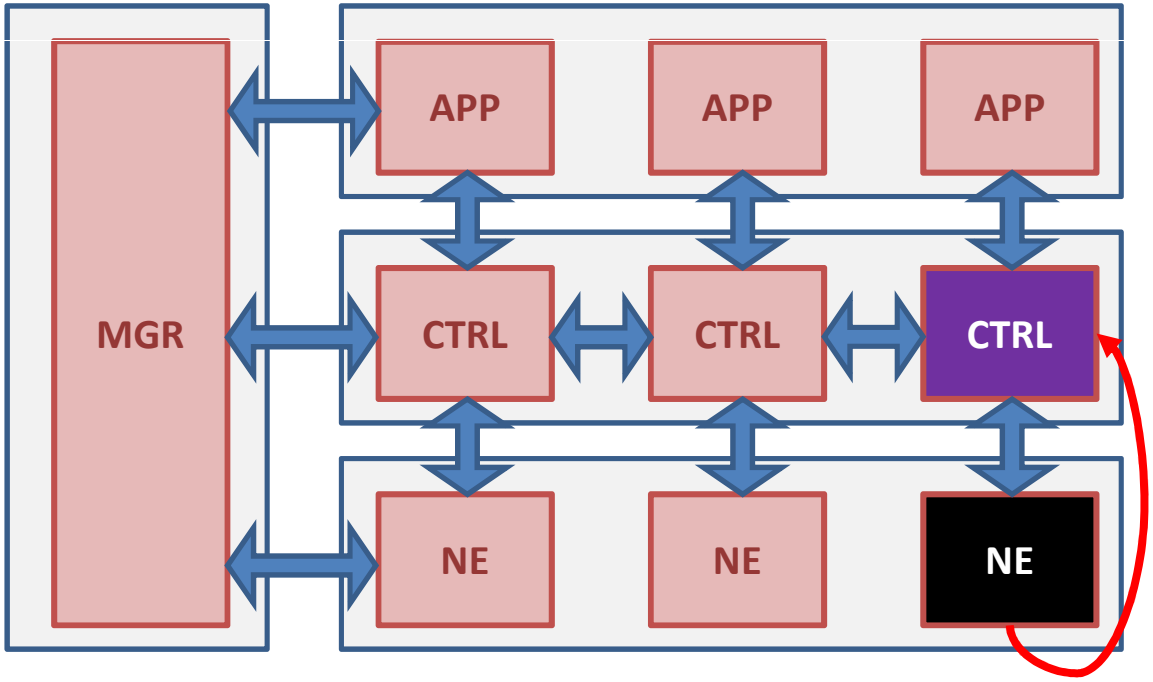
Disruption of Service

The attacker leverages a compromised network element to flood a controller



Unauthorized Modification

A malicious user attempts to poison the controller's view of the network topology



Threat Mitigation

- Determine what threats have to be mitigated
- Specify security requirements to address the threats
- Implement the mitigation measures

Threat Mitigation Examples

TH: Conduct brute force login attempts/password guessing attacks against the management console

SR: A management console shall not allow any user to successfully use a password guessing attack to gain unauthorized access

MM: All vendor default passwords for management consoles should be changed

TH: Exploit a known information disclosure vulnerability in the NBI

SR: An application shall not allow any user to successfully exploit a vulnerability to access information which the user is not authorized to access

MM: All application server patches should be applied in a timely manner

.

Threat Mitigation Examples

TH: Conduct communications interception attack against the EWI

SR: The east/west bound interface shall not allow unauthorized users to eavesdrop on network communications between the controllers

MM: The east/west bound communication channels should be protected using strong cryptography

TH: Cause a denial of service on a controller

SR: A controller shall not allow any network element to successfully use a denial of service attack to reduce its availability

MM: Rate limiting and packet dropping at the controller plane to avoid denial of service attacks. Specific rules should be installed on the network elements where the attack is being originated.

High-Level Recommendations

- Allow only required ports and services in the controller
- Limit the number of accounts requiring direct access to the controller
- Implement HA controller architecture
- Integrate the SDN specific user accounts with the enterprise IM infrastructure
- Place the management interfaces in a dedicated virtual network segment
- Implement SDN patch management practices
- Use strong encryption to protect SDN communication channels
- Follow secure coding practices for all applications
- Validate NE flow tables against the controller to identify discrepancies
- Implement integrity checks on controllers
- Implement security monitoring and security policy enforcement of SDN elements
- Enable logging and audit trails

BlackHat Sound Bytes

- Our current knowledge on SDN threats and attacks is limited. To better anticipate potential SDN threats at the early design stage, enterprises could use the presented SDN threat model
- The proposed framework could be further extended by incorporating the details of specific SDN designs. It could also serve as a foundation for planning and carrying out SDN penetration tests
- The model enables comprehensive development of security requirements and mitigation measures to increase the state of preparedness in the event of attacks on SDN