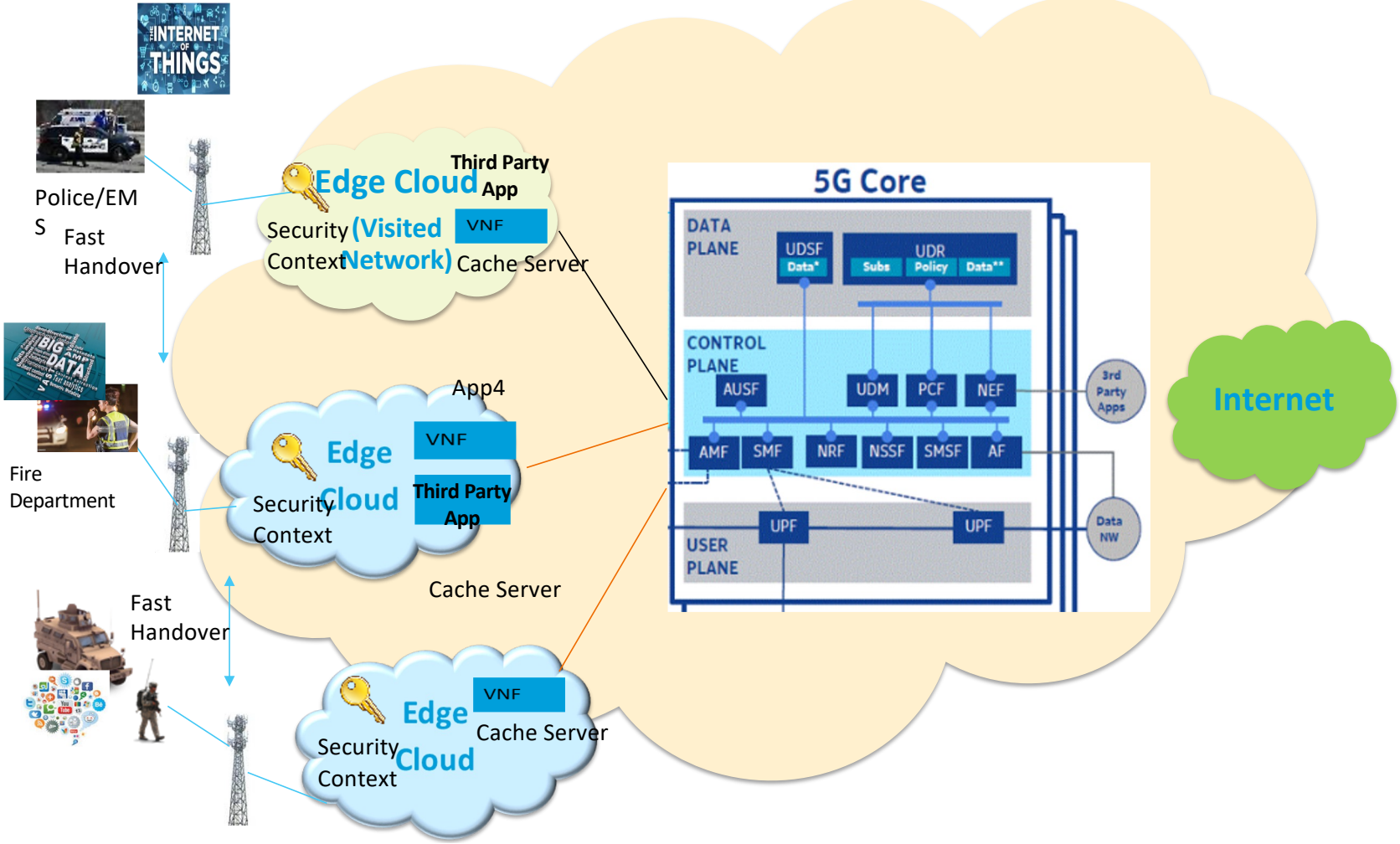
Mobile Edge Security



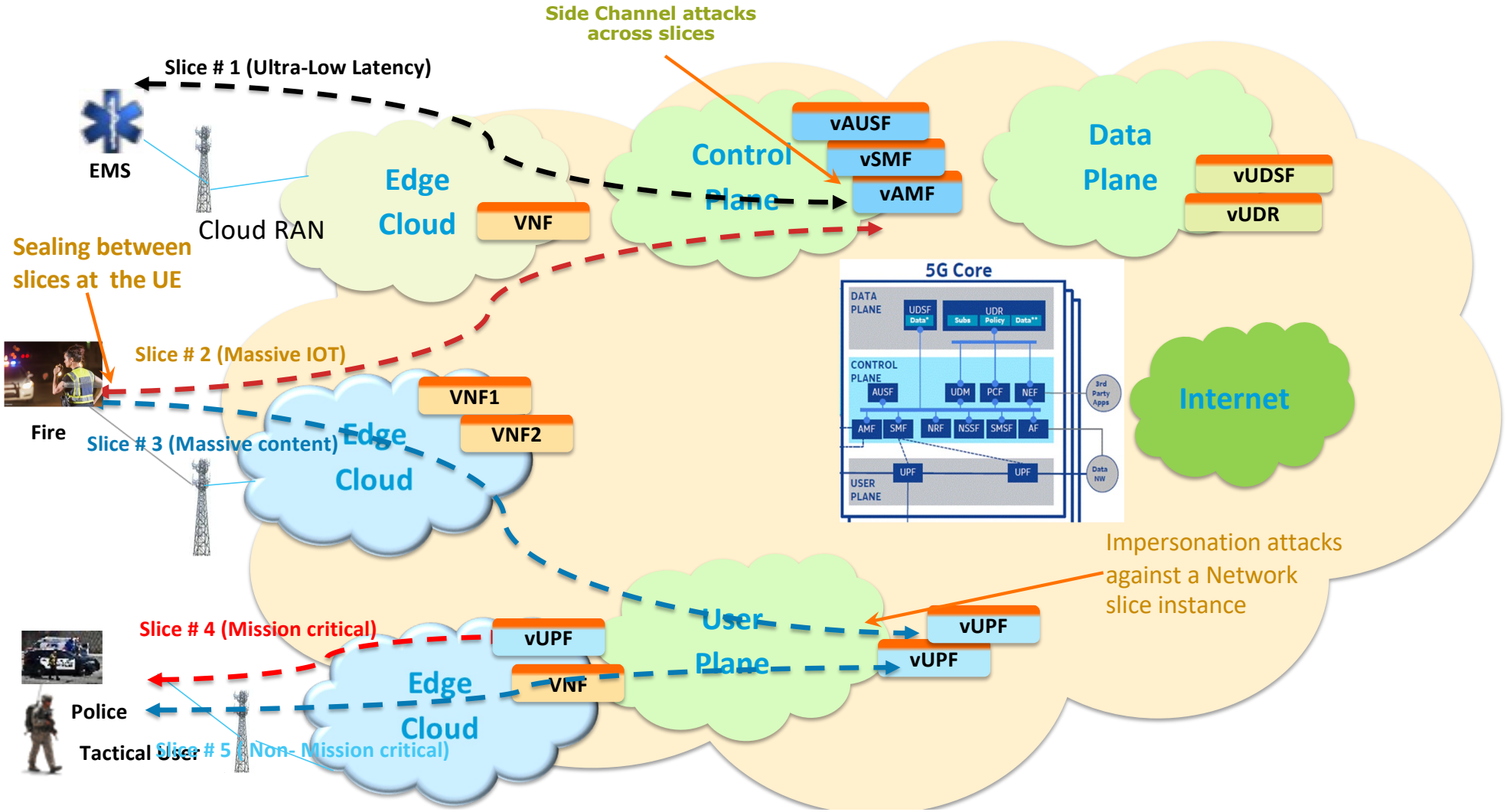
Mobile Edge Cloud Opportunities, Security Challenges, and Mitigation

5G Capabilities	Potential Security Challenges	Potential Mitigation
• **Server Computation at the edge of the network** • **Security Context at the Edge of the network** • **MEC Servers provide caching, local processing and application aware optimization** • **Reduced handover time and Data off-loading** • **Reduced Latency for authentication for time sensitive applications**	• If third party applications are run on the same platform as network functions, there are risks of poorly designed applications that allow the hackers to infiltrate the platform	Run both the edge computing applications and the network function(s) in robustly segregated virtual machines.
	• Sensitive security assets are compromised at virtualized functions at the edge. Man-In-The-Middle Attack at the Mobile Edge Server	Sensitive Security Assets stored at the mobile edge should be encrypted
	• Persistent caching of old Security Association by both the UE and visited network will weaken security by way of cache poisoning, cache overwhelming	Understand the security implications and take measures to protect these caches.
	• Attacker can gain connectivity or carry out a spoofing, eavesdropping or data manipulation attack during context transfer	Encrypted transfer of security context, IDS/IPS for proper monitoring and mitigation, proper security level
	• Subscriber authentication within the visited network gives rise to additional security vulnerabilities at the edge of the network.	Reuse old security association (SA), while in the meantime running AKA and acquiring a new security association. Delegate some of the HSS functions to the visited network such as Delegated Subscriber Server (DSS).

Potential Security Opportunities/Benefits

- **The Edge provides an opportunity to embed security detection and mitigation functions to stop and isolate attacks before they can impact other parts of the 5G network.**

Network Slicing Security



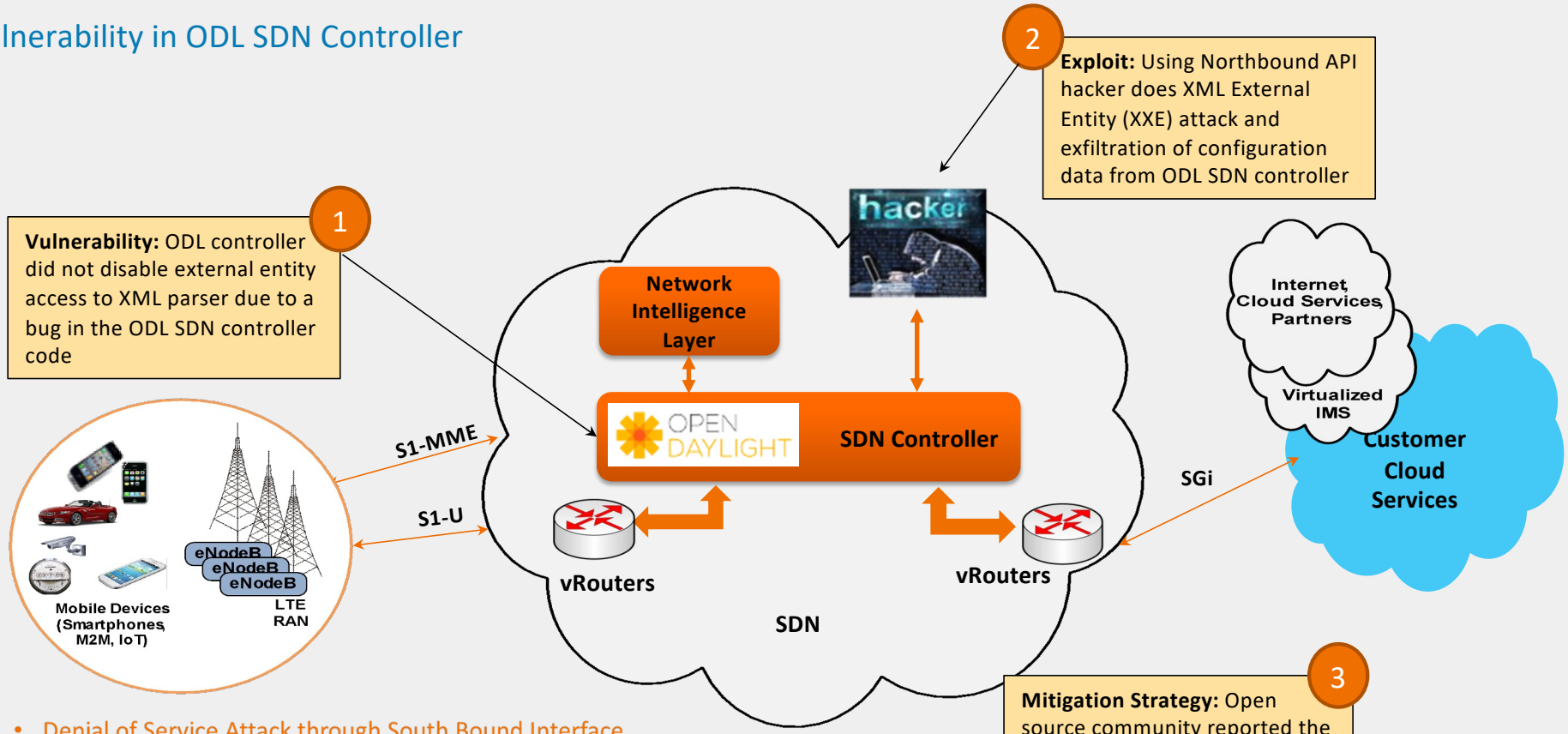
Network Slicing – Opportunities, Security Challenges, and Potential Mitigation

5G Capabilities	Potential Security Challenges	Potential Mitigation
• **Network slicing enables service differentiation and meeting end user SLAs.** • **Allocates appropriate amount of network resources to a specific slice based on service (e.g. IOT, Priority services)** • **Overcomes all the drawbacks of "DiffServ-based" QoS solution.** • **Enables the operators to provide networks on an as-service-basis that minimizes CAPEX and OPEX.** • **A single network can offer various services based on the requirements of the user and various use cases.** • **Vastly improves operational efficiency and time to market for the delivery of 5G network services.**	Controlling Inter-Network Slices Communications	Proper security mechanism to ensure operations within expected parameters and security needs
	Denial of service to other slices – attacker may exhaust resources common to multiple slices,	Capping of resources for individual slices, Ring-fencing resources for individual slices to guarantee minimum level of resource
	Attacker attacks the resources in slice A and in turn slice B's resources get exhausted	Ring-fence the network resource for security protocols so that the slice has always has the ability in spite of resource exhaustion in other slices.
	Side Channel attacks across slices extract information about cryptographic keys	Avoid co-hosting the slices that have very different levels of sensitivity on the same hardware. Hypervisor hardening
	If UE is attached to several slices. UE may receive sensitive data via one slice and publish data via other slice.	Security mechanisms to address this should exist in the network and potentially in UE.
	Impersonation attacks against a Network slice instance within an operator network	All virtual functions within a Network Slice instance need be authenticated and their verified.

Potential Security Opportunities/Benefits

- **Network Slicing provides a native approach to isolate highly sensitive contexts or applications which would be very beneficial for several security use cases.**
- **Slice specific SLAs enable a context-aware orchestration and optimization of security virtual functions.**

Security Vulnerability in ODL SDN Controller



- Denial of Service Attack through South Bound Interface
- REST API Parameter Exploitation – North Bound API
- North Bound API Flood Attack
- MAN-IN-THE MIDDLE ATTACK/Spoofing
- Protocol Fuzzing – South Bound
- Controller Impersonation – South Bound

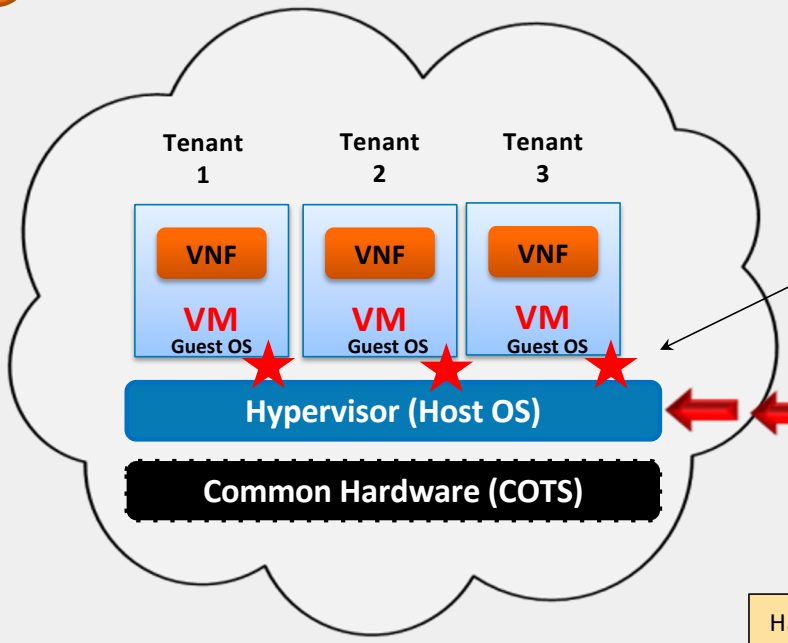
IEEE

Security Challenges from Virtualization

Hypervisor Vulnerabilities

To prevent this type of attack, we must:
- Conduct security scans and apply security patches
- Ensure the Hypervisor is hardened and minimized (close vulnerable ports)
- Ensure the access to the Hypervisor is controlled via User Access Management,

3



Malware compromises VMs:
- VM/Guest OS manipulation
- Data exfiltration/destruction

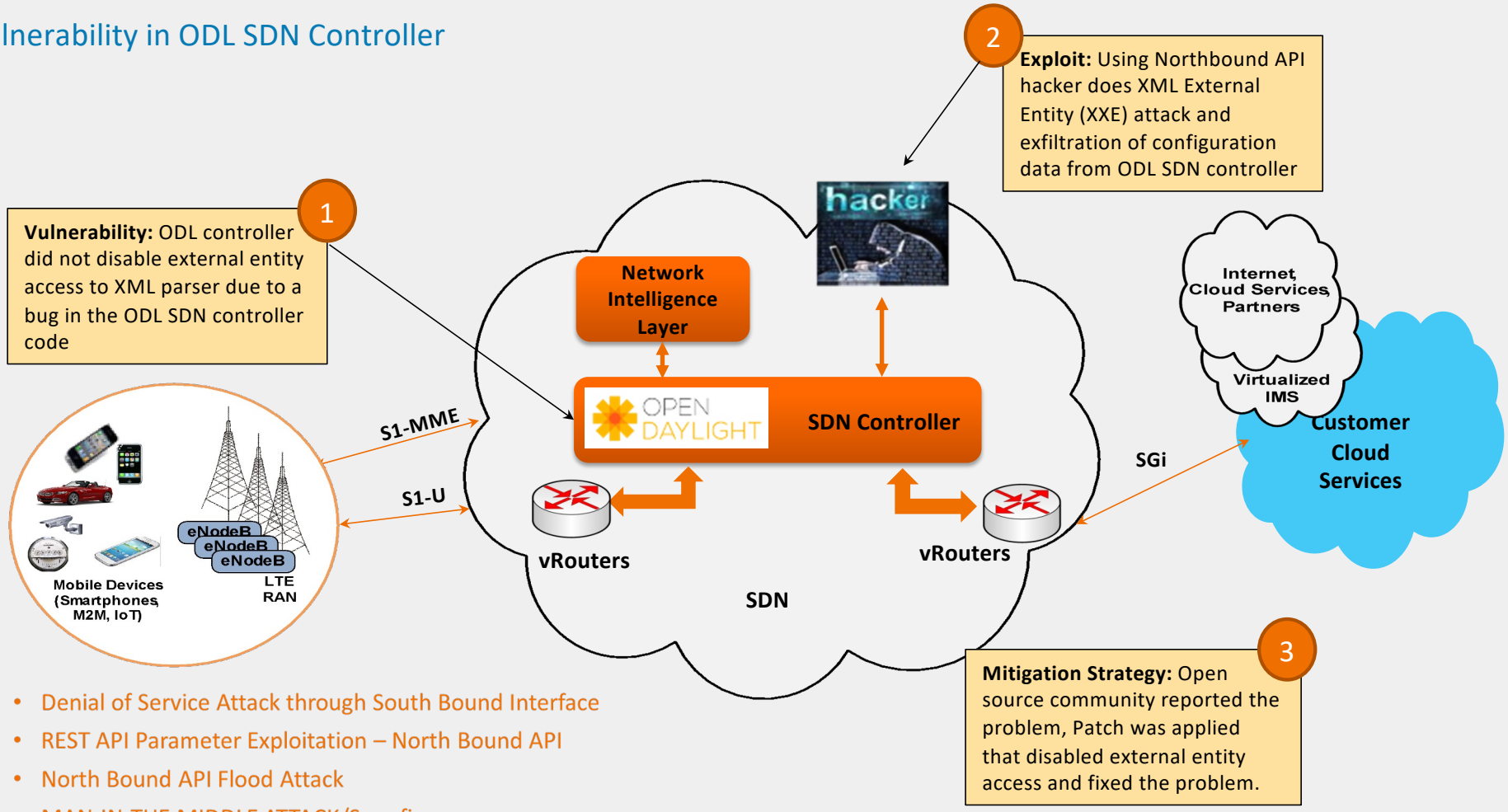
2

Hacker exploits a vulnerability in the Open Source code and infects the Hypervisor with a Malware

1

IEEE

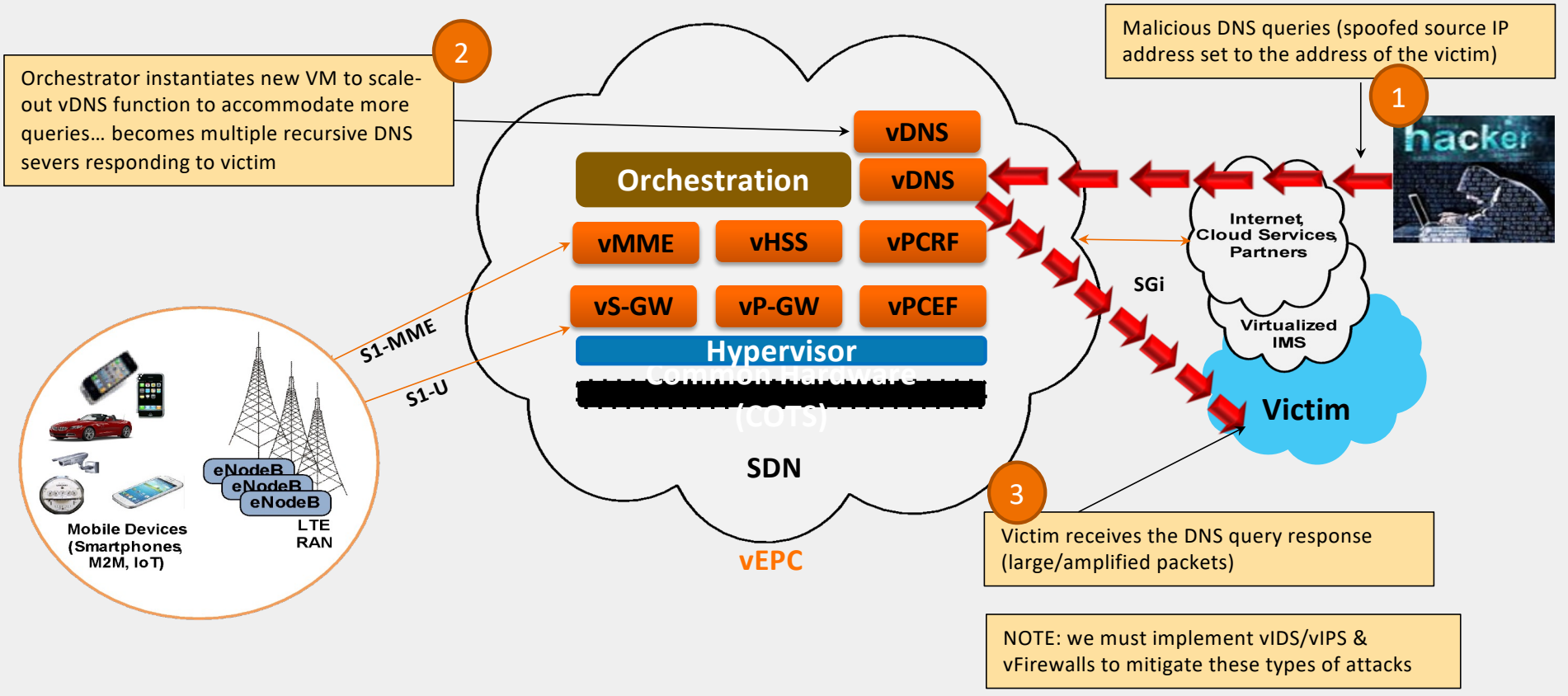
Security Vulnerability in ODL SDN Controller



- Denial of Service Attack through South Bound Interface
- REST API Parameter Exploitation – North Bound API
- North Bound API Flood Attack
- MAN-IN-THE MIDDLE ATTACK/Spoofing
- Protocol Fuzzing – South Bound
- Controller Impersonation – South Bound

IEEE

DNS Amplification Attacks Enhanced by Elasticity Function



Relevant SDN/NFV/5G Standards

Forum	Focus
IETF	Network Virtualization Overlay, Dynamic Service Chaining, Network Service Header
3GPP	Mobility and Security Architecture and Specification
ETSI ISG NFV	NFV Platform/Deployment Standards – Security, Architecture/Interfaces, Reliability, Evolution, Performance
IEEE	IEEE 802.11 ax/ac/ay. There are 42 societies to contribute to 5G Eco System
ONF	OpenFlow SDN Controller Standards
OPNFV	NFV Open Platform/eCOMP/OPNFV Community TestLabs
Open Air Interface (OAI)	5G Open Source Software Alliance
OpenDaylight	Brownfield SDN Controller Open Source
ONOS	OpenFlow SDN Controller Open Source
Open RAN Alliance	Open and Interoperable RAN Virtualization
KVM Forum	Hypervisor
NSF PAWR Testbed	COSMOS (NYC), POWDER-RENEW (Salt Lake City), RENEW (NCSU)
Linux Foundation	Operating System, Container Security
ITU	The ITU Telecommunication Standardization Sector coordinates standards for telecommunications
ATIS/NIST/FCC/CSA	Regulatory Aspects of SDN/NFV

Open Source Networking / SDO Landscape