JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

11100 Johns Hopkins Road
Laurel, MD 20723-6099

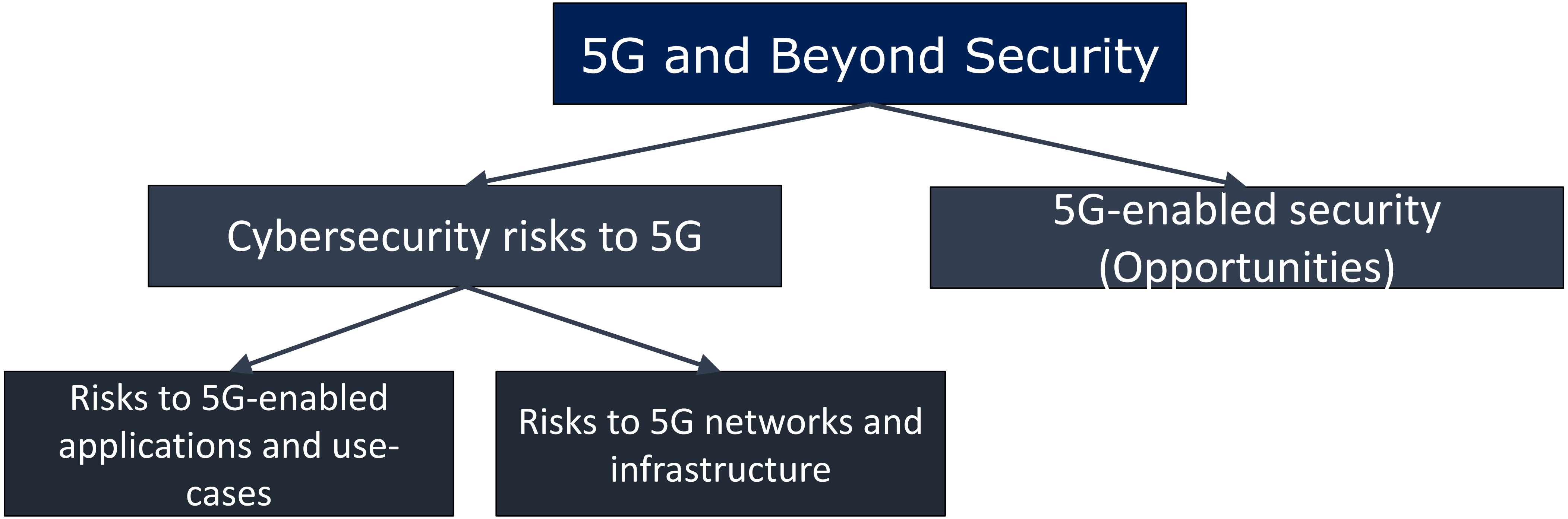
5G and Beyond Security Challenges and Opportunities – A System Approach

Ashutosh Dutta, Ph.D. Ashutosh.Dutta@jhuapl.edu, +1 908-642-8593

Acknowledgement – IEEE Future Networks Initiative, Security Working group

IEEE

5G & Beyond: Security Perspective



The progress of the 5G and beyond revolution may well be hindered if security issues are not tackled early on while the systems are being designed, standardized and deployed.

Key Pillars of "5G and Beyond" Security

SDN Security

Cloud RAN Security

Edge Cloud Security

Open Source / API Security

Network Slicing Security

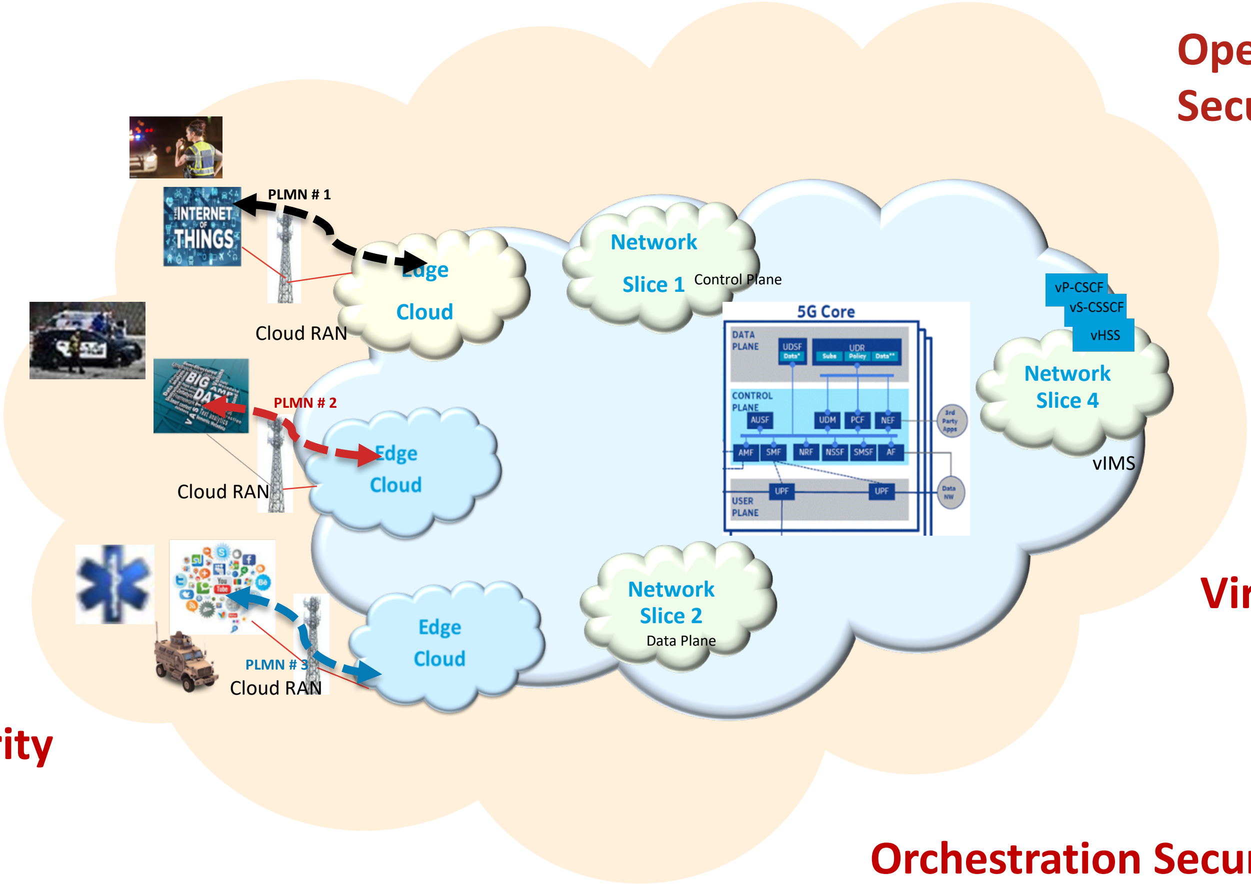
Supply Chain Security

Virtualization Security

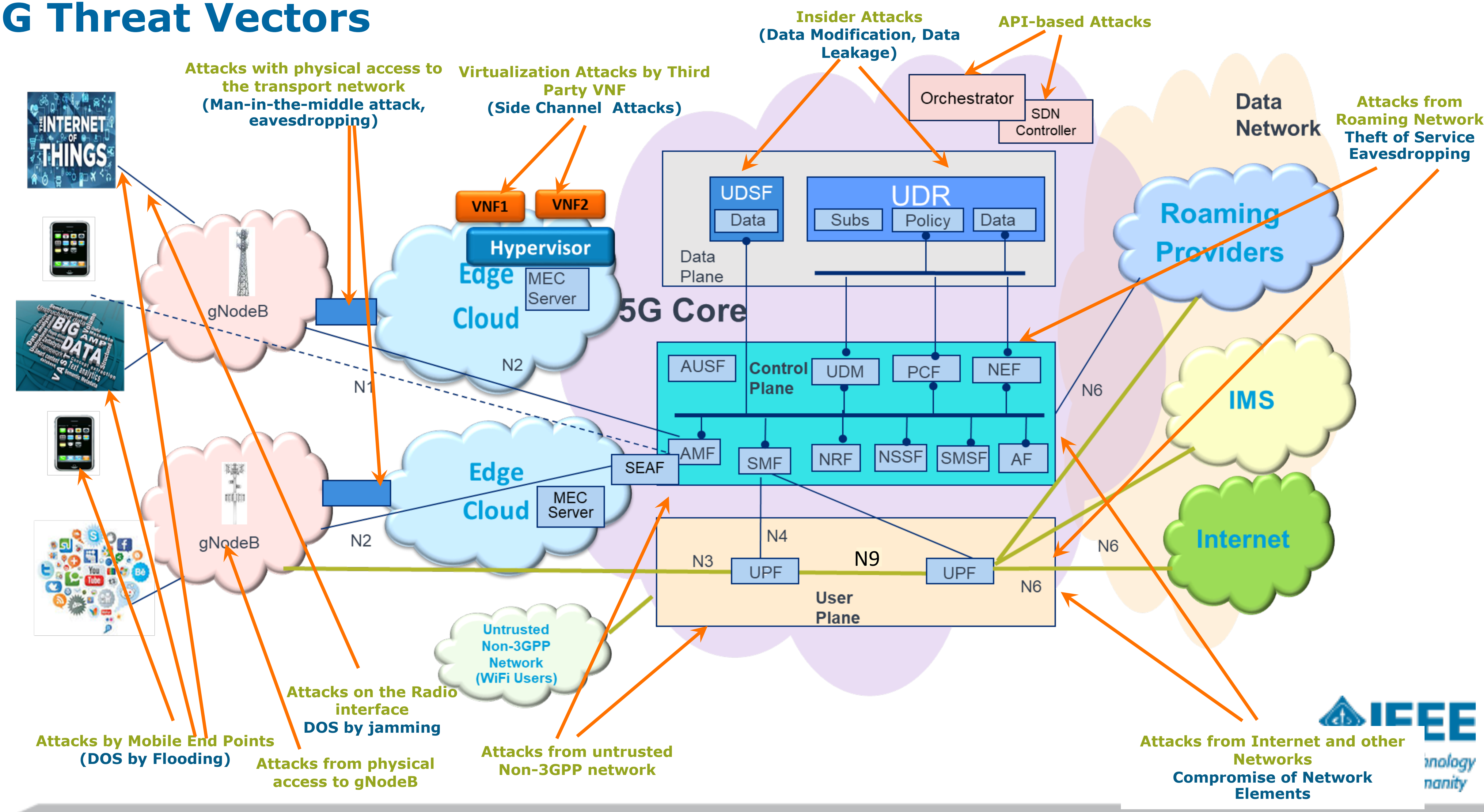
Predictive Security

Orchestration Security

Data Security and Privacy



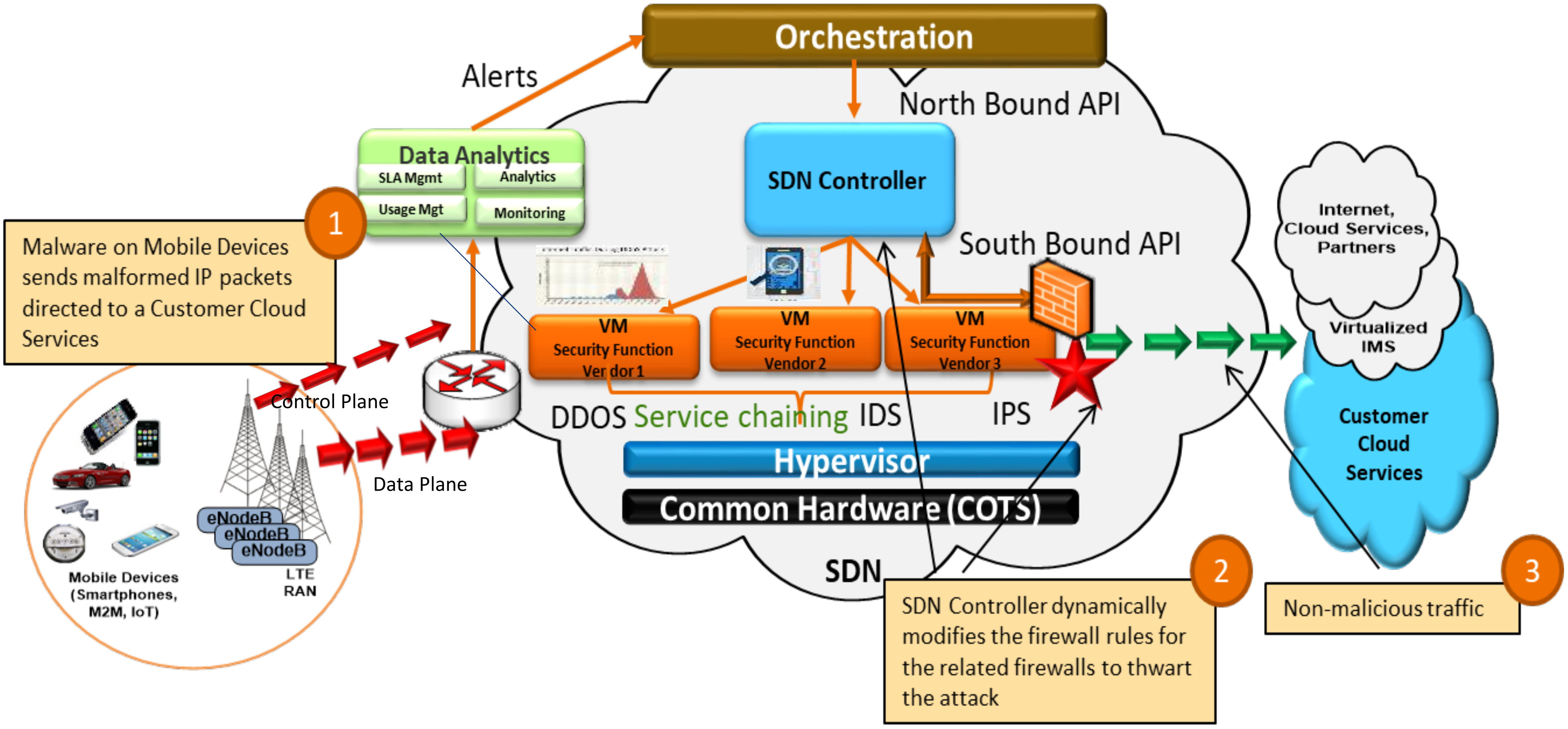
5G Threat Vectors



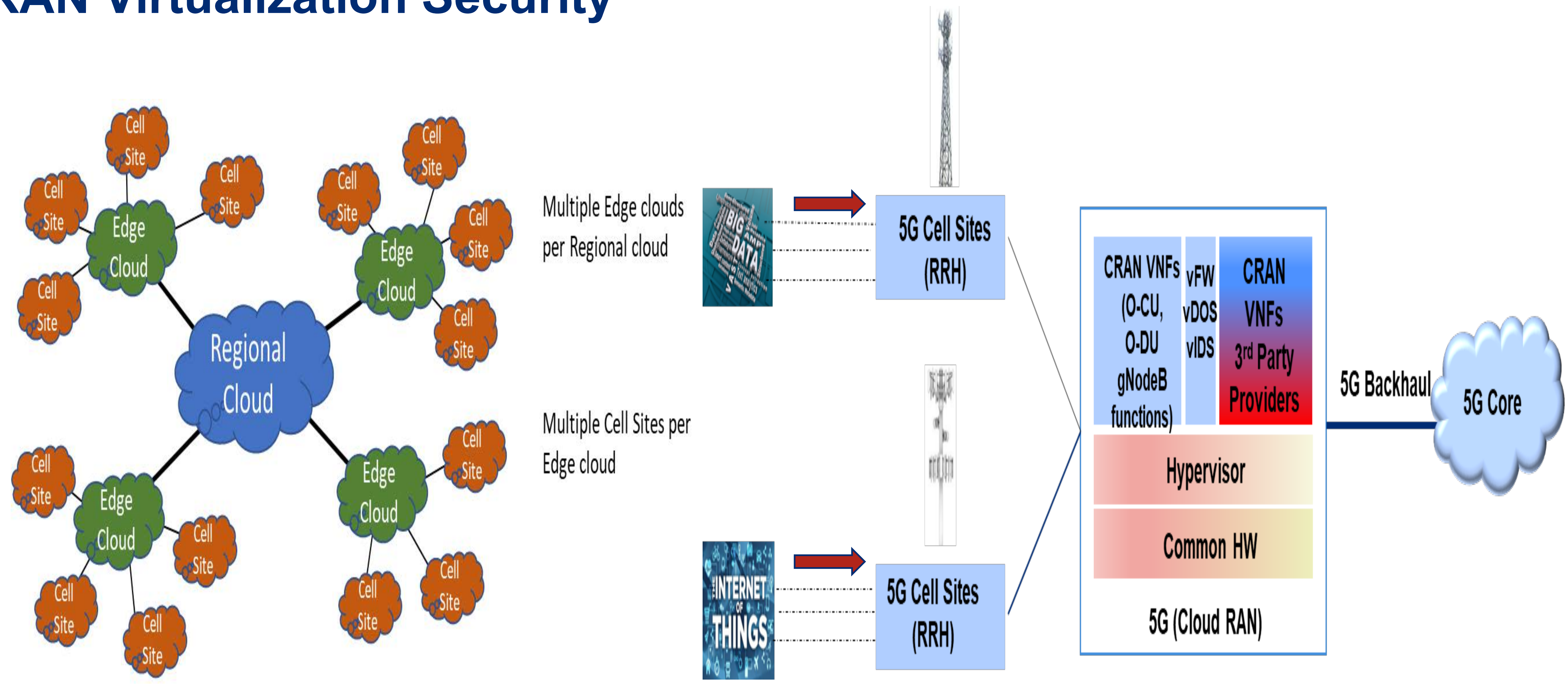
5G Threat Taxonomy

Category	Threat	Attack Description
Loss of Availability	Flooding an interface	Attackers flood an interface and network assets (AMF, AUSF) resulting in DDoS condition on the signaling plane (e.g. multiple authentication failure on N1, N2 interface)
	Crashing a network element	Attackers crash a network element (e.g., AMF) by sending malformed packets
Loss of Confidentiality	Eavesdropping	Attackers eavesdrop on sensitive data on control and bearer plane to retrieve user location and device details and sensitive user data
	Data leakage	Unauthorized access to sensitive data (e.g., user profile) stored in UDR, UDSF
Loss of Integrity	Traffic modification	Attackers modify information during transit in user plane interface N3 (SIP header modification, RTP spoofing)
	Data modification	Attackers modify data on network element (e.g., change the gNodeB configurations through admin interface)
Loss of Control	Control the network	Attackers control the network via protocol or implementation flaw
	Compromise of network element	Attackers compromise of network element via management interface
Malicious Insider	Insider attacks	Insiders make data modification on network elements, make unauthorized changes to NE configuration, etc.
Theft of Service	Service free of charge	Attackers exploits a flaw to use services without being charged

Security Function Virtualization - Security-As-a-Service – Predictive Security



RAN Virtualization Security



Ref: O-RAN Alliance White Paper

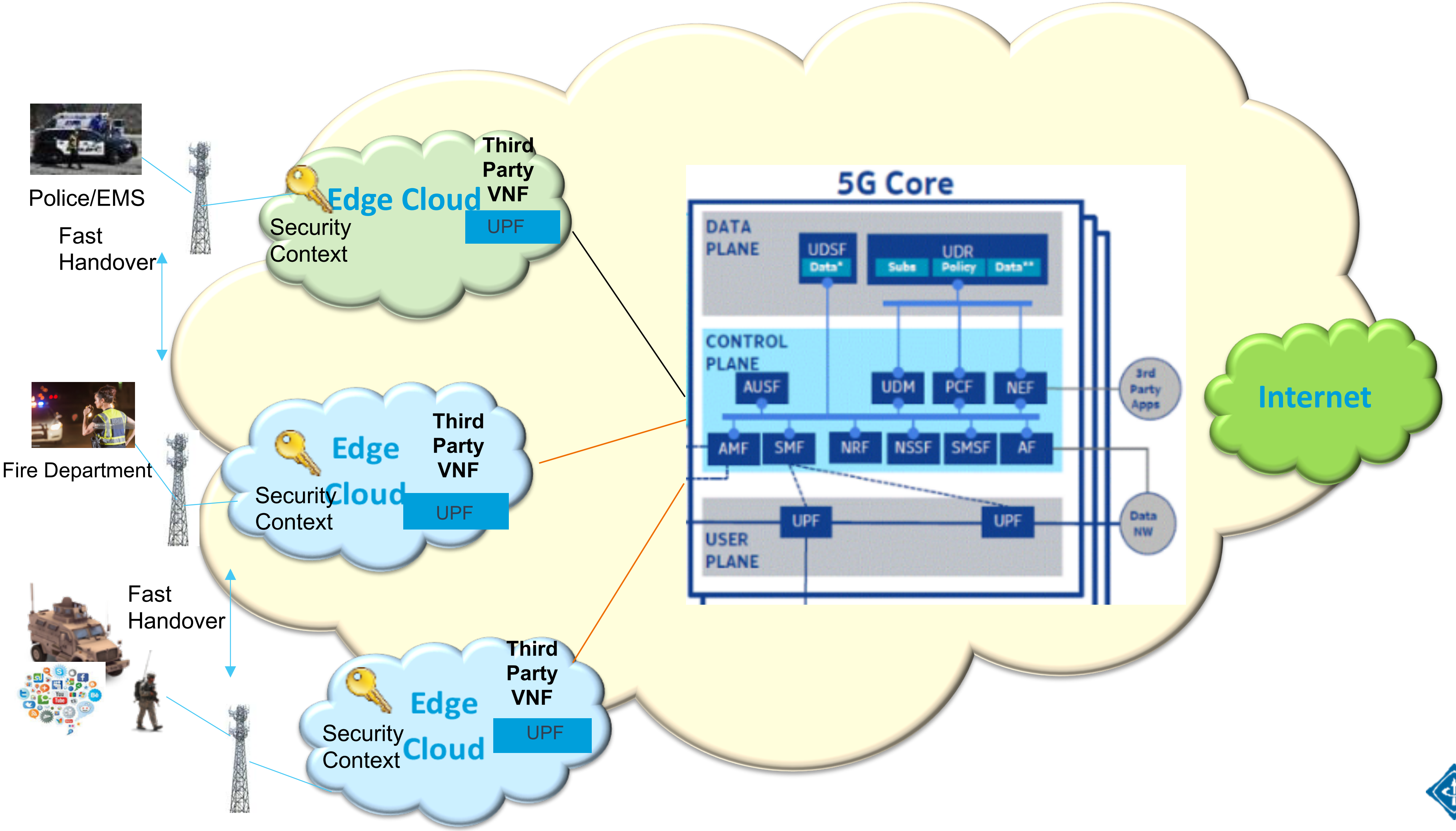
Cloud RAN - Security Opportunities, Challenges, Mitigation and Risks

Security Opportunities	Security Challenges	Potential Mitigation Techniques	Risk Severity	Threat Likelihood
Programmability and Virtualization of RAN will adapt to dynamic nature of traffic and multi provider access SoftRAN (cRAN) in 5G networks will have **embedded DDoS detection and mitigation** functions **Dynamic Radio Resource Scheduling** significantly reduces the risk of jamming attacks targeting mission critical devices **Correlation of control plane and data plane traffic** will enable security monitoring of traffic via correlation	DDOS (Distributed Denial of Service) attack will result in resource starvation at cRAN Virtual Network Functions due to instantiation of additional vFirewalls	• Intelligent VM resource allocations • Capping of resources • Scale up functionality • Security monitoring at the edge	Medium	Medium
	VM (Virtual Machine) manipulation, Data exfiltration due to virtualization	• Hypervisor Separation • Hypervisor Hardening	High	Medium
	Programmable and Software RAN will increase the chance of Man-In-The-Middle Attack at the base station	• Traffic monitoring and closed loop orchestration will detect the attacks and mitigate these attacks	High	Medium
	Orchestration attack during scaling up and scaling down of VNFs in the cloud RAN	• Deploy detection and mitigation techniques for orchestration and API-based attacks	Medium	Low
	Jamming can be launched against control-plane signaling or user-plane data messages	• Deploy DDOS detection, IDS and vFirewall functions • Dynamic Service Chaining • Access Class Barring	Medium	Low

High Medium Low

IEEE

Mobile Edge Cloud Security

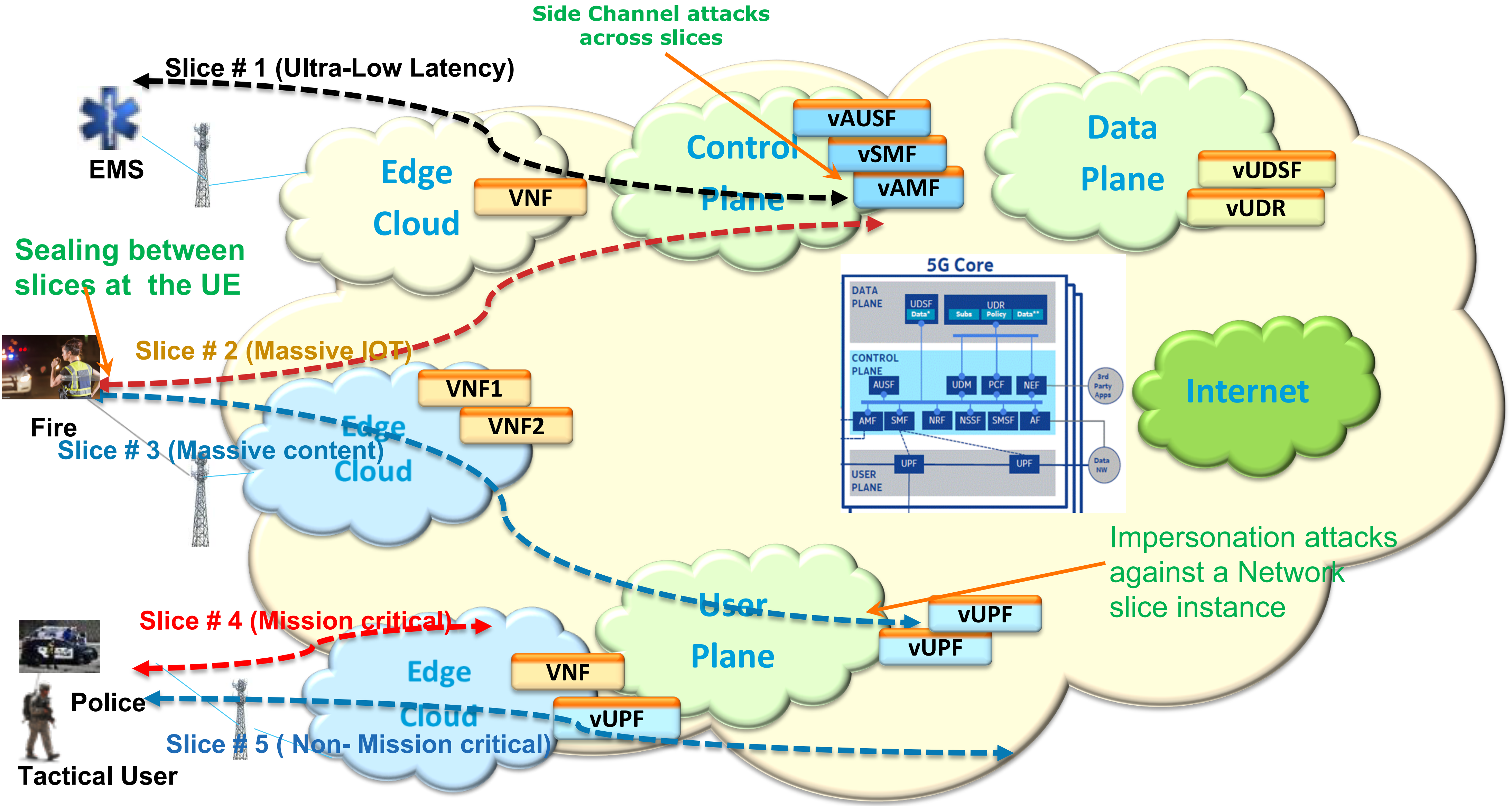


Mobile Edge Cloud - Security Opportunities, Challenges, Mitigation and Risks

Security Opportunities	Security Challenges	Potential Mitigation Techniques	Risk Severity	Threat Likelihood
Embed Security monitoring at the Edge of the network	Co-existence of the third party applications with the virtual network functions allow the hackers to infiltrate the platform	• Run both the edge computing applications and the network function(s) in robustly segregated virtual machines. • Higher priority for network functions	🔴	🟠
Application aware **performance optimization**	Storage of security context at the edge can lead to malicious spoofing attack	• Apply proper encryption mechanisms for the security context at the edge	🟠	🟠
Reduced latency by way of edge authentication for time sensitive applications	User plane attacks in mobile edge including cache poisoning, cache overwhelming	• Access Control • Hardening Mechanism • Investigate the new security implications	🟠	🟢
Secured and fast data offloading during handover	Spoofing, eavesdropping or data manipulation attack during context transfer	• Encrypted transfer of security context • IDS/IPS for proper monitoring and mitigation,	🟠	🟢
	Subscriber authentication within the visited networks leads to fraud and lack of control by home operator	• Reuse old security association (SA) while running AKA with the home network and acquiring a new security association. • Timely expiry of temporary security association • Proper authentication between DSS and UE	🔴	🟠

🔴 High 🟠 Medium 🟢 Low

Network Slicing Security

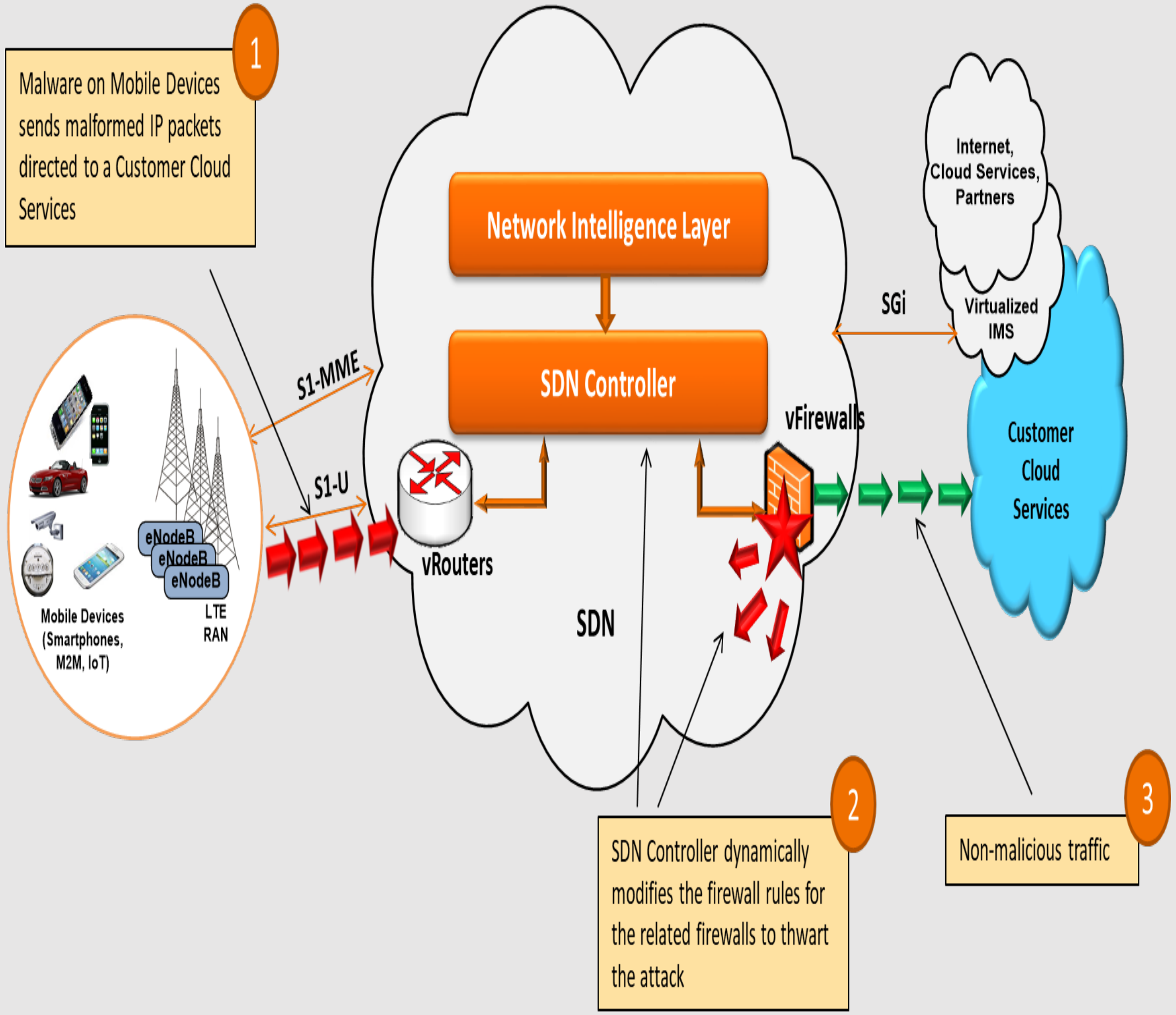


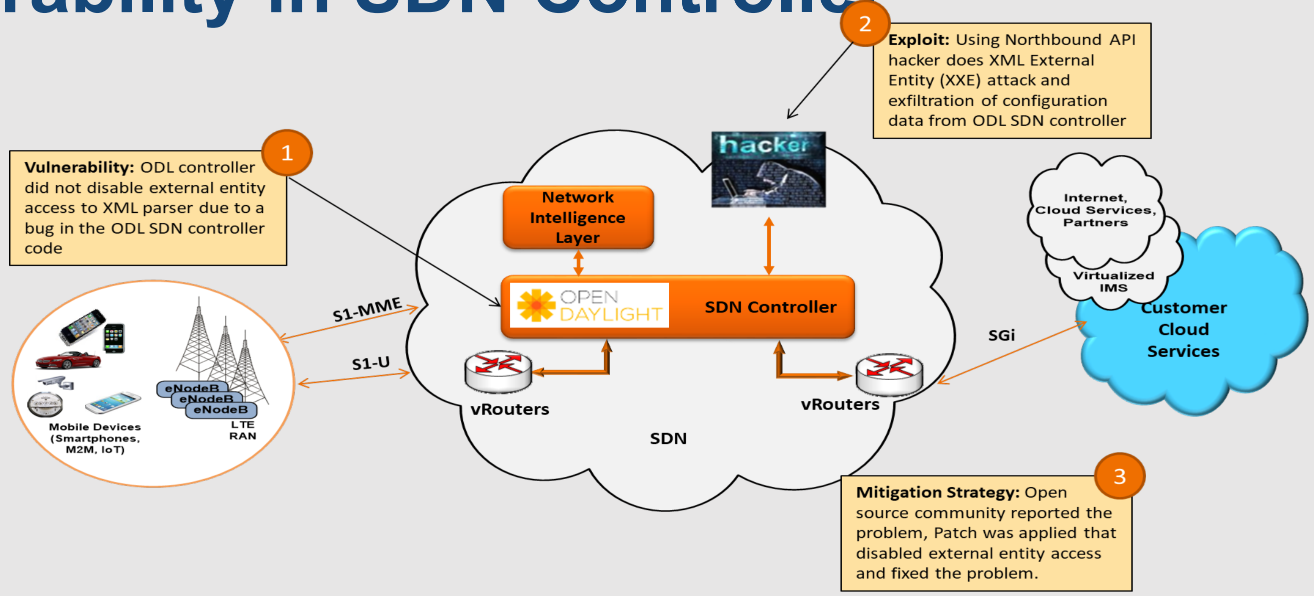
Network Slicing – Security Opportunities, Challenges, Mitigation, and Risks

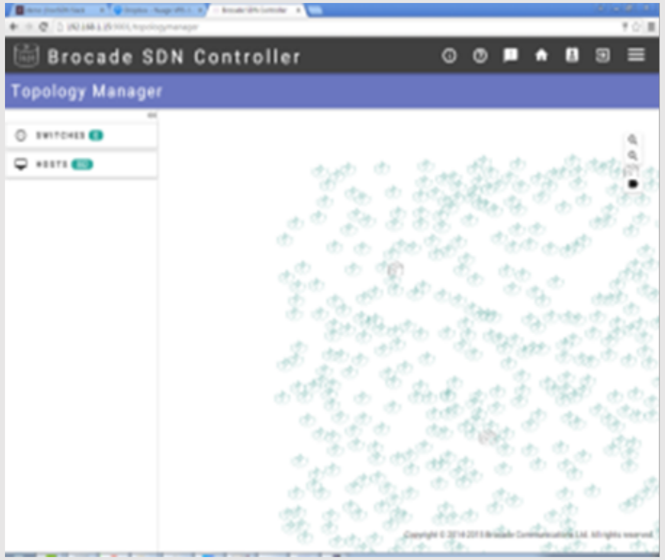
Security Opportunities	Potential Security Challenges	Potential Mitigation	Risk Severity	Threat Likelihood
Network slicing enables service differentiation and meeting end user SLAs. **Isolates highly sensitive contexts or applications** from other non-critical applications Slice specific SLAs enable a **context-aware orchestration and optimization** of security virtual functions. **Slicing reduces security overhead** by avoiding additional layer of authentication	Different security protocols or policies in different slices results in higher probability of attack	• Adequate isolation of slices with different security levels • Separate authentication of a UE accessing multiple slices at once	Medium	Low
	Denial of service to other slices resulting in resource exhaustion	• Capping of resources for individual slices • Ring-fencing resources for individual slices	High	Medium
	Side Channel attacks across slices extract information about cryptographic keys	• Avoid co-hosting the slices with different levels of sensitivity on the same hardware • Hypervisor hardening	High	Low
	Sealing between slices when the UE is attached to several slices	• Security monitoring mechanisms should exist in the network and potentially in UE.	High	Medium
	Impersonation attacks against a network slice instance within an operator network	• All virtual functions within a Network Slice instance need to be authenticated and their integrity verified.	Medium	Low

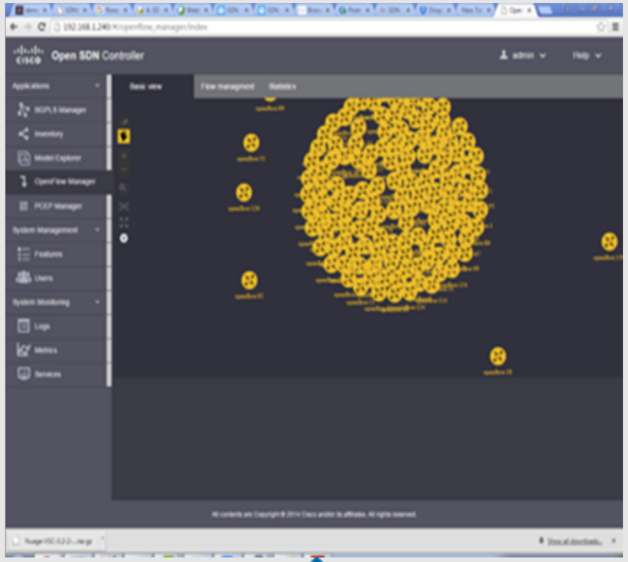
High Medium Low

Security Opportunities and Vulnerability in SDN Controller









SDN Controller – Security Opportunities, Challenges, Mitigation, and Risks

Security Opportunities	Potential Security Challenges	Potential Mitigation Techniques	Risk Severity	Threat Likelihood
SDN controller provides resilience to the attack and overload **Enhances programmability and adaptability** for the network routers and firewalls **Facilitates dynamic service chaining for** closed loop automation **Provides Dynamic Security Control mechanism** to stop attacks on signaling plane and data plane	Denial of service attack through South Bound Interface	• Security monitoring • Access control	Medium	Low
	REST API Parameter Exploitation (North Bound API)	• API Authentication • SDN controller Code Scanning • System Logging and Auditing	High	Medium
	North Bound API Flood Attack	• API Monitoring • Closed Loop Automation	Medium	Low
	Man-In-The Middle Attack (Spoofing Attack)	• SDN Scanner • Closed Loop Automation	High	Medium
	Protocol Fuzzing Attack (South Bound API)	• Hardening mechanism for SDN Controller	Medium	Low
	Controller Impersonation (South Bound API)	• Access Control • API monitoring	High	Low

High Medium Low

Security Opportunities and Challenges and Virtualization Management

Security Opportunities	Potential Security Challenges	Potential Mitigation	Risk Severity	Threat Likelihood
Provides resiliency in the event of DDOS attack Closed loop automation	Lack of visibility into Network Traffic	API-based monitoring Embed security monitoring in the Hypervisor	Medium	Medium
Multi-tenant operation	Execution of VMs with different Trust levels	Firewalls should be used to isolate VM groups from other groups for east-west traffic	High	Medium
Sharing of resources to support priority applications	VNF Catalog is compromised	Apply encryption for Data at Rest Harden Access Control	High	Medium
Ability to scale up and scale down the network based on the load by way of orchestration	Communication between VNF Catalog, Orchestrator, and Virtual Infrastructure Manager is compromised	API Security Hardening Security monitoring	Medium	Medium
Distributed inventory control	Wrong placement of VNF	Verification of VNF placement API Security	High	Low

High Medium Low

Summary

- Future Network needs to be programmable, resilient, and flexible to support emerging applications with variant KPIs

- 5G network gives rise to additional security pillars that offer both in-built security opportunities, and new challenges
  - Opportunities: Resiliency, Automation, Isolation of mission critical applications, edge detection
  - Challenges: Side Channel attacks, inter-slice communication, resource starvation, orchestration attacks

- Implement best current practice to augment security controls to mitigate the risks associated with new threats

- A systematic approach to threat analysis and threat taxonomy is essential to understanding associated risks and mitigation techniques

- Collaboration among operators, vendors, regulators and academia is essential

- Standards, Testbeds and POCs act as catalyst for 5G deployment

JOHNS HOPKINS

APPLIED PHYSICS LABORATORY