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
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

- **Orchestration Security**
- **Virtualization Security**
- **Edge Cloud Security**
- **Cloud RAN Security**
- **Supply Chain Security**
- **Predictive Security**
- **Data Security and Privacy**
- **SDN Security**
- **Open Source / API Security**
- **Network Slicing Security**
- **Virtualization Security**
- **Orchestration Security**
5G Threat Vectors

Attacks by Mobile End Points
(DOS by Flooding)

Attacks with physical access to the transport network
(Man-in-the-middle attack, eavesdropping)

Virtualization Attacks by Third Party VNF
(Side Channel Attacks)

Attacks from physical access to gNodeB

Attacks from untrusted Non-3GPP network

Insider Attacks
(Data Modification, Data Leakage)

API-based Attacks

Orchestrator

SDN Controller

UDSF

UDR

UDM

PCF

NEF

AUSF

Control Plane

UPF

User Plane

N3

N4

N9

N6

IMS

Internet

Data Network

Roaming Providers

5G Core

MEC Server

SEAF

SMF

NRF

NSSF

SMSF

AF

N1

N2

N5

N6

5G Core

Hypervisor

VNF1

VNF2

gNodeB

N2

N2

N1

Attacks from Internet and other Networks
Compromise of Network Elements

Attacks from roaming Network
Theft of Service Eavesdropping

Globally Untrusted Third Party

Globally Untrusted Third Party

Attacks on the Radio interface
DOS by jamming

Untrusted Non-3GPP Network (WiFi Users)
## 5G Threat Taxonomy

<table>
<thead>
<tr>
<th>Category</th>
<th>Threat</th>
<th>Attack Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of Availability</td>
<td>Flooding an interface</td>
<td>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)</td>
</tr>
<tr>
<td>Crashing a network element</td>
<td>Attackers crash a network element (e.g., AMF) by sending malformed packets</td>
<td></td>
</tr>
<tr>
<td>Loss of Confidentiality</td>
<td>Eavesdropping</td>
<td>Attackers eavesdrop on sensitive data on control and bearer plane to retrieve user location and device details and sensitive user data</td>
</tr>
<tr>
<td></td>
<td>Data leakage</td>
<td>Unauthorized access to sensitive data (e.g., user profile) stored in UDR, UDSF</td>
</tr>
<tr>
<td>Loss of Integrity</td>
<td>Traffic modification</td>
<td>Attackers modify information during transit in user plane interface N3 (SIP header modification, RTP spoofing)</td>
</tr>
<tr>
<td></td>
<td>Data modification</td>
<td>Attackers modify data on network element (e.g., change the gNodeB configurations through admin interface)</td>
</tr>
<tr>
<td>Loss of Control</td>
<td>Control the network</td>
<td>Attackers control the network via protocol or implementation flaw</td>
</tr>
<tr>
<td></td>
<td>Compromise of network element</td>
<td>Attackers compromise of network element via management interface</td>
</tr>
<tr>
<td>Malicious Insider</td>
<td>Insider attacks</td>
<td>Insiders make data modification on network elements, make unauthorized changes to NE configuration, etc.</td>
</tr>
<tr>
<td>Theft of Service</td>
<td>Service free of charge</td>
<td>Attackers exploits a flaw to use services without being charged</td>
</tr>
</tbody>
</table>
Security Function Virtualization - Security-As-a-Service – Predictive Security

1. Malware on Mobile Devices sends malformed IP packets directed to a Customer Cloud Services

2. SDN Controller dynamically modifies the firewall rules for the related firewalls to thwart the attack

3. Non-malicious traffic
RAN Virtualization Security

Ref: O-RAN Alliance White Paper
<table>
<thead>
<tr>
<th>Security Opportunities</th>
<th>Security Challenges</th>
<th>Potential Mitigation Techniques</th>
<th>Risk Severity</th>
<th>Threat Likelihood</th>
</tr>
</thead>
</table>
| Programmability and Virtualization of RAN will adapt to      | DDOS (Distributed Denial of Service) attack will result in resource starvation at     | • Intelligent VM resource allocations  
| dynamic nature of traffic and multi provider access          | cRAN Virtual Network Functions due to instantiation of additional vFirewalls         | • Capping of resources  
|                                                              |                                                                                      | • Scale up functionality  
|                                                              |                                                                                      | • Security monitoring at the edge                                                            | High          | Low                |
| SoftRAN (cRAN) in 5G networks will have embedded DDoS       | VM (Virtual Machine) manipulation, Data exfiltration due to virtualization           | • Hypervisor Separation  
| detection and mitigation functions                           |                                                                                      | • Hypervisor Hardening                                                                         | Medium        | Medium             |
| Dynamic Radio Resource Scheduling significantly reduces the   | Programmable and Software RAN will increase the chance of Man-In-The-Middle Attack   | • Traffic monitoring and closed loop orchestration will detect the attacks and mitigate these  | High          | Medium             |
| risk of jamming attacks targeting mission critical devices   | at the base station                                                                   | attacks                                                                                     |               |                    |
| Correlation of control plane and data plane traffic will    | 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          | High          | Medium             |
| enable security monitoring of traffic via correlation         |                                                                                      |                                                                                                 |               |                    |
|                                                              | 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                                                                       | High          | Medium             |

- High
- Medium
- Low
Mobile Edge Cloud Security

![Diagram of Mobile Edge Cloud Security](image_url)
### Mobile Edge Cloud - Security Opportunities, Challenges, Mitigation and Risks

<table>
<thead>
<tr>
<th>Security Opportunities</th>
<th>Security Challenges</th>
<th>Potential Mitigation Techniques</th>
<th>Risk Severity</th>
<th>Threat Likelihood</th>
</tr>
</thead>
</table>
| **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 | ♺️            | ♼️               |

**Legend:**  
- ♺️: High  
- ♼️: Medium  
- ♻️: Low
Network Slicing Security

Sealing between slices at the UE

Side Channel attacks across slices

Impersonation attacks against a Network slice instance

Slice # 1 (Ultra-Low Latency)
Slice # 2 (Massive IOT)
Slice # 3 (Massive content)
Slice # 4 (Mission critical)
Slice # 5 (Non-Mission critical)
## Network Slicing – Security Opportunities, Challenges, Mitigation, and Risks

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

<table>
<thead>
<tr>
<th>Threat Likelihood</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
</table>
Security Opportunities and Vulnerability in SDN Controller

1. Malware on Mobile Devices sends malformed IP packets directed to a Customer Cloud Services

2. SDN Controller dynamically modifies the firewall rules for related firewalls to thwart the attack

3. Non-malicious traffic

Vulnerability: ODL controller did not disable external entity access to XML parser due to a bug in the ODL SDN controller code

Exploit: Using Northbound API, hacker does XML External Entity (XXE) attack and exfiltration of configuration data from ODL SDN controller

Mitigation Strategy: Open source community reported the problem, patch was applied that disabled external entity access and fixed the problem.
# SDN Controller – Security Opportunities, Challenges, Mitigation, and Risks

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

- **High**
- **Medium**
- **Low**
### Security Opportunities and Challenges and Virtualization Management

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