**Project Scope and Objectives Document: Securing 5G Network Slicing**

**1. Problem Statement**

**General Problem**

**5G networks leverage network slicing to create multiple virtual networks over shared infrastructure, allowing different services to operate independently. However, this flexibility introduces critical security risks, including:**

* **Cross-slice attacks where one compromised slice can be used to infiltrate another.**
* **Unauthorized access, leading to potential data breaches and service manipulation.**
* **SS7 vulnerabilities inherited from legacy network interconnections, enabling location tracking, SMS hijacking, and call redirection.**
* **Denial-of-Service (DoS) attacks, which can disrupt mission-critical slices (e.g., healthcare, autonomous driving, financial services).**

**Specific Problem in This Project**

**While existing 5G security measures address basic access control and encryption, they do not fully mitigate cross-slice attacks or SS7 vulnerabilities.  
Additionally, real-time security frameworks that can autonomously detect and respond to 5G slice attacks are lacking.**

**This project will design and implement an AI-driven security framework that:**

* **Isolates 5G slices to prevent unauthorized lateral movement.**
* **Detects anomalies caused by SS7 exploitation or slice intrusion using AI/ML techniques.**
* **Implements real-time threat response mechanisms to mitigate attacks before they cause damage.**

**2. Project Objectives**

**Main Objective**

**Develop a secure network slice management framework that protects 5G slices from cyber threats, particularly cross-slice attacks and SS7-based vulnerabilities.**

**Specific Objectives**

1. **Implement slice isolation mechanisms to prevent lateral movement between slices.**
2. **Develop AI/ML-based anomaly detection for real-time threat identification.**
3. **Secure SS7 interconnections, mitigating location tracking, SMS hijacking, and DoS attacks.**
4. **Provide real-time security monitoring with alerts and automated responses.**
5. **Deploy an automated threat response system that actively blocks detected attacks.**

**3. Project Methodology**

**To achieve these objectives, the project follows a three-phase methodology:**

**Phase 1: Security Analysis & Simulation Setup (Weeks 3-4)**

* **Simulate 5G network slicing using OpenAirInterface or srsRAN.**
* **Implement SDN (Software-Defined Networking) and NFV (Network Function Virtualization) to manage slices and enforce security policies.**
* **Introduce SS7 vulnerabilities in a controlled testbed to analyze potential attack vectors.**

**Phase 2: Threat Detection & AI-Based Security (Weeks 5-8)**

* **Deploy AI-driven anomaly detection for monitoring traffic patterns in different slices.**
* **Use packet analysis tools (Wireshark, Splunk) to capture malicious traffic.**
* **Train ML models (TensorFlow, Scikit-Learn) to detect cross-slice intrusions and SS7 exploitation.**

**Types of AI Models to be Used**

**To enhance the security framework, various AI/ML models will be utilized for threat detection:**

* **Supervised Learning Models (e.g., Decision Trees, Support Vector Machines) to classify known attack patterns.**
* **Unsupervised Learning Models (e.g., Autoencoders, K-Means Clustering) to detect unknown anomalies in network traffic.**
* **Deep Learning Models (e.g., Recurrent Neural Networks - RNN, Long Short-Term Memory - LSTM) to analyze temporal patterns in attack behavior.**
* **Reinforcement Learning (RL) Models to adapt security responses dynamically based on observed attack behavior.**

**Phase 3: Defense & Automated Mitigation (Weeks 9-10)**

* **Deploy slice-specific security policies using SDN controllers.**
* **Implement real-time mitigation techniques for SS7-based threats and DoS attacks.**
* **Test and evaluate the framework’s effectiveness under simulated attack scenarios.**

**4. SS7 Mitigation & Security Layers**

**The SS7 security countermeasures will be integrated into a multi-layered security approach:**

1. **Perimeter Security (Network Level)**
   * **SS7 Firewalls to detect and block unauthorized requests.**
   * **AI-based threat intelligence to monitor anomalies in SS7 signaling.**
2. **Slice-Specific Protection (Isolation & Access Control)**
   * **Strict authentication for inter-slice communication.**
   * **Role-Based Access Control (RBAC) to prevent unauthorized access to sensitive slices.**
3. **Real-Time Detection (AI-Driven Monitoring)**
   * **Packet inspection and anomaly detection to flag suspicious SS7 traffic.**
   * **Automated pattern recognition to detect potential SS7 exploitation attempts.**
4. **Automated Response (Threat Mitigation)**
   * **Automated blocking of detected SS7 threats (e.g., unauthorized location tracking, SMS hijacking attempts).**
   * **Dynamically adjusting slice parameters (e.g., reducing attack surface for a compromised slice).**
   * **Deploying AI-driven countermeasures (e.g., creating honeypot slices to trap attackers).**

**5. Tools & Technologies**

|  |  |  |
| --- | --- | --- |
| Category | Tools | Purpose |
| 5G Simulation | **OpenAirInterface, srsRAN** | **Simulate network slicing environments** |
| Security Monitoring | **Wireshark, Splunk** | **Capture and analyze traffic logs** |
| Threat Detection | **TensorFlow, Scikit-Learn** | **Implement AI-based anomaly detection** |
| SS7 Testing | **SS7 attack tools (SIGTRAN testbeds)** | **Simulate SS7 vulnerabilities** |
| SDN/NFV Management | **OpenDaylight, ONAP** | **Manage slices and enforce security policies** |

**6. Automated Threat Response Mechanisms**

**Upon detecting an anomalous event, the framework will automatically execute predefined countermeasures based on the threat type.**

|  |  |
| --- | --- |
| Threat Type | Automated Response Actions |
| Cross-Slice Attack | **Isolate affected slice, reconfigure SDN rules to block unauthorized traffic.** |
| Unauthorized Access Attempt | **Enforce MFA, temporarily suspend suspicious accounts, trigger real-time alerts.** |
| SS7 Location Tracking Attack | **Block unauthorized SS7 location queries, log attack sources for analysis.** |
| SMS Hijacking Attempt | **Reroute SMS authentication to app-based MFA, notify the user of potential compromise.** |
| Call Interception Attack | **Activate encryption on affected call routes, block unauthorized call redirections.** |
| DoS Attack on a Slice | **Rate-limit traffic, shift high-priority services to redundant slices, blacklist malicious IPs.** |

**The automated response mechanism will be driven by AI-assisted decision-making, ensuring real-time mitigation without manual intervention.**

**7. Expected Outcome & Contribution**

**Expected Outcome**

**At the end of the project, we will have a fully functional security framework that: ✅ Provides real-time slice security monitoring.**

**1) Detects anomalous activities in network slices.  
2) Mitigates SS7-based attacks before they can impact 5G services.  
3) Ensures slice isolation to prevent lateral movement attacks.  
4) Deploys automated countermeasures to secure critical slices.**

**Contribution to the Field**

**Bridging SS7 security with 5G slice protection, addressing a key security gap.  
Introducing an AI-driven threat detection approach tailored for 5G slicing.  
Improving real-time response capabilities in modern network security frameworks.  
Enhancing automation in security enforcement, reducing reliance on manual intervention.**