Day 6 research  
  
**Day 6: Research Existing Solutions & Identifying Gaps**

**Objective:**

Today, we will **analyze existing security solutions for 5G network slicing** and **identify gaps** that the project can address. Understanding what has already been developed will help ensure that the framework is innovative and fills a critical security gap.

**1. Research Current Security Solutions for 5G Network Slicing**

We will look at how companies, research institutions, and organizations are securing **5G slices** and **SS7 interconnections**.

**A. Security Solutions for Network Slicing**

|  |  |  |
| --- | --- | --- |
| Solution | Description | Limitations |
| Ericsson 5G Security | Implements slice-specific security policies and threat detection. | Primarily designed for enterprise-level security, not real-time AI-driven detection. |
| Huawei 5G Core Security | Uses SDN-based security policies for slice isolation. | Lacks AI-based anomaly detection; mainly rule-based. |
| Nokia NetGuard Security | Uses deep packet inspection (DPI) for real-time security monitoring in 5G slices. | Heavy reliance on DPI increases processing overhead. |
| OpenDaylight SDN Security | Provides dynamic network control and security policy enforcement for slices. | Does not integrate AI-driven threat detection. |

📝 **Observation:**

* Most existing solutions rely on **traditional rule-based security**, which can be **bypassed by advanced, evolving attacks.**
* **AI-based real-time detection is missing** in most solutions.
* **SS7 security is often ignored**, despite its relevance in legacy interconnections.

**B. Security Solutions for SS7 Protection**

|  |  |  |
| --- | --- | --- |
| Solution | Description | Limitations |
| AdaptiveMobile SS7 Firewall | Monitors and blocks suspicious SS7 requests. | Does not integrate 5G slicing security. |
| Positive Technologies SS7 Protection | Uses pattern recognition to detect SS7-based location tracking and SMS hijacking attacks. | Lacks real-time AI threat analysis. |
| GSMA SS7 Security Guidelines | Recommendations for securing SS7 interconnects in 5G networks. | Only provides guidelines, not active security solutions. |

📝 **Observation:**

* **Current SS7 security tools focus on filtering traffic**, but **lack AI-driven detection.**
* **No integration between SS7 security and 5G slice security exists.**
* **A unified framework to secure both SS7 and network slicing is missing.**

**2. Identify Gaps in Existing Security Solutions**

Based on our research, here are **key weaknesses in current solutions** that the project will address:

|  |  |
| --- | --- |
| Existing Weakness | Project’s Contribution |
| No real-time AI-powered anomaly detection for network slices. | Implement **AI-driven real-time monitoring** to detect cross-slice attacks. |
| No automated response mechanisms for threats. | Develop a system that **isolates compromised slices dynamically** upon detecting an attack. |
| SS7 security is not integrated with 5G slice security. | Create a framework that **secures SS7 signaling alongside network slicing.** |
| Existing solutions rely too much on DPI and static filtering. | Use **machine learning-based anomaly detection** instead of just rule-based filtering. |

**3. Define How the Project Will Innovate**

Here’s what makes the project **unique compared to existing solutions**:

**AI-Driven Anomaly Detection**

* **Unlike traditional rule-based systems**, the framework will use **unsupervised learning (Autoencoders, Isolation Forests)** to detect **zero-day threats** in network slices.

**Integrated SS7 & 5G Security**

* Unlike **firewalls that only filter SS7 traffic**, the framework will **proactively detect SS7-based attacks** that impact 5G slices.

**Automated Mitigation System**

* Instead of just **alerting administrators**, the system will **dynamically isolate infected slices, filter malicious traffic, and adjust security policies in real-time**.

**4. Resources for Today**

1. **Research Papers & Articles**
   * GSMA 5G Security Guidelines
   * IEEE Paper: "Security Challenges in 5G Network Slicing"
   * Whitepaper: "AI for 5G Cybersecurity" (Ericsson)
2. **Videos & Webinars**
   * **YouTube:** "Why AI is Needed for 5G Security"
   * **Webinar:** "5G Security Threats & Countermeasures"

**5. Deliverable for Today**

By the end of today, summarize:

1. **The main security solutions for 5G slicing and SS7.**
2. **What gaps exist in current solutions.**
3. **How the project fills these gaps and innovates.**