Cybersecurity Threats in 5G Networks and Telecom Infrastructure

Satya Geetri (2023202015)
Soham Ghosh (2023202011)
Pooja Rani (2024204019)

5G Network and its Security Frameworks

The following frameworks used in 5G networks have been analyzed:

- 3GPP Security Framework (SA3) for 5G
- NIST 5G Cybersecurity Framework
- Zero Trust Security Model for 5G

3GPP Security Framework (SA3) for 5G

Key security aspects of the framework are:

- Authentication & Key Management (5G AKA): **Mutual authentication** between user device, serving network and home network is present.
- User Plane Integrity Protection: Ensures **end-to-end data integrity** using cryptographic mechanisms.
- Network Slicing Security: **Slice isolation** prevents cross-slice attacks.
- Enhanced Subscriber Privacy: **IMSI encryption** (IMSI → SUCI) prevents message tracking.

Risk Assessment of 3GPP Security Framework for 5G

Key Risks & Vulnerabilities:

- **Unauthorized Access & Key Compromise**
- **Man-in-the-Middle (MitM) Attacks**
- **Cross-Slice Attacks**
- **Supply Chain Attacks**
- **Location Tracking & IMSI Catcher Alternatives**

Risk Mitigation of 3GPP Security Framework for 5G

Accept low-impact threats (e.g., minor service disruptions).

Use SUCI encryption instead of IMSI to prevent identity exposure.

Zero Trust Architecture (ZTA) for continuous authentication.

Cybersecurity insurance for DDoS & data breaches.

Business Continuity for 3GPP SA3 Framework in 5G

Business Impact Analysis (BIA)

- **Critical Functions:** Authentication, key management, network slicing security, user plane protection.
- **Impact of Failure:** Service disruptions, cross-slice compromises, and network downtime affecting telecom, businesses, and emergency services.
- **RTO & RPO:** Authentication recovery < 1 hour; no data loss for keys.

Business Continuity for 3GPP SA3 Framework in 5G

Business Continuity Strategies

- **Redundant Authentication Infrastructure** – Deploy geographically distributed authentication systems.
- **Network Slicing Isolation** – Implement strict access controls.
- **DDoS Mitigation** – Deploy traffic filtering & rate limiting.
- **Zero Trust** – Require continuous authentication & least privilege access.

NIST 5G Cybersecurity Framework

Key security controls of the framework are:

- **Supply Chain Risk Management (SCRM):** Protects 5G infrastructure from third-party risks.
- **Zero Trust Architecture (ZTA):** Enforces strict authentication, least privilege access, and network segmentation to prevent unauthorized access.
- **Endpoint & Device Security:** Secures 5G-connected devices with strong device authentication.

Risk Assessment of NIST 5G Cybersecurity Framework

Key Risks & Vulnerabilities:

- **Supply Chain Attacks**
- **Insider Threats**
- **IoT Botnets & DDoS**
- **Unauthorized Access**
- **Firmware Tampering**

Risk Mitigation of NIST 5G Cybersecurity Framework

Accept unpatchable legacy device risks.

Eliminate high-risk suppliers by enforcing strict vendor policies.

Implement Zero Trust & continuous monitoring.

Cyber insurance for DDoS losses.

Business Continuity for NIST 5G Cybersecurity Framework

Business Impact Analysis (BIA)

- **Critical Functions:** Zero Trust, supply chain security, IoT endpoint protection
- **Impact of Failure:** Network-wide compromise, 5G infrastructure disruption, unauthorized access & data breaches
- **RTO:** 2-4 hours (supply chain)
- **RPO:** 15 min (security updates)

Business Continuity for NIST 5G Cybersecurity Framework

Business Continuity Strategies

- **Secure Supply Chain** – Enforce vendor risk assessments & firmware integrity validation.
- **Zero Trust Security** – Implement MFA, continuous authentication & micro-segmentation.
- **AI-Driven Threat Detection** – Use ML models for DDoS & unauthorized access mitigation.
- **IoT Security Hardening** – Ensure secure boot, hardware authentication & regular updates.

Zero Trust Security Model for 5G

Key principles used in the framework are:

- **Micro-Segmentation**: Divides the 5G network into isolated segments.
- **Least Privilege Access:** Ensures users, devices, and applications only get the minimum access needed for their functions.
- **Continuous Monitoring & AI Detection:** AI-driven anomaly detection for real-time threat mitigation.

Zero Trust Security Model for 5G

Major cybersecurity risks in 5G and how Zero Trust mitigates them

Identity Spoofing Attacks:

- Hackers forge credentials to gain unauthorized access to **5G network slices**.
- This can lead to **data breaches and service disruptions**.

Micro-Segmentation Bypass:

- Attackers **exploit misconfigurations** in network policies to **move laterally** between different network slices.
- This can allow them to access **restricted telecom services and critical data**.

AI Evasion Attacks:

- Malicious actors manipulate **machine learning (ML) security models** to **evade detection**.
- This results in **false negatives**, allowing **hidden threats to persist undetected**.

IoT Device Exploits:

- Weak security in IoT devices can be used for **DDoS attacks**, flooding the **5G core network**.
- This can lead to **massive service disruptions** affecting millions of users.

How Zero Trust Reduces Risk in 5G

Highlights **core Zero Trust principles** and **how they proactively mitigate threats** in **5G security**.

1. **Continuous Authentication:**

Every request is validated using **biometric, behavioral, and multi-factor authentication (MFA)** before granting access.

2. **Micro-Segmentation:**

Each network slice is isolated using **dynamic policies** to **prevent unauthorized lateral movement**.

3. **AI-Powered Threat Detection:**

AI models analyze **traffic patterns in real-time** to detect **anomalies and malicious activities**.

4. **Zero Trust Policy Engine (ZTPE):**

Uses **policy-based access control** to **limit permissions** based on **user roles, session context, and risk level**.

Risk Mitigation Strategies for Zero Trust in 5G

A**ctionable solutions** to **secure 5G networks using Zero Trust**.

1. **AI-Powered Identity Verification:**

- Uses **biometrics, behavioral analytics, and MFA** to validate user identities.

2. **Automated Micro-Segmentation:**

- **Dynamic policy updates** ensure **secure network isolation**.

3. **Adversarial AI Testing:**

- **Continuous re-training of AI models** prevents evasion attacks.

4. **IoT Device Security Framework:**

- Enforces **device authentication** and **automated quarantine** for compromised devices.

Business Continuity Planning and Disaster Recovery Strategy for Zero Trust in 5G

1. **Dynamic Security Policies:**
   Security controls are **automatically updated** in response to **real-time threats**.

2. **Continuous Authentication & Monitoring:**
   Ensures **minimal downtime** in case of **breaches or failures**.

3. **Resilience Against IoT Attacks:**
   Self-healing security systems detect and mitigate **botnet threats**.

How Zero Trust disaster recovery ensures fast security response in **5G networks**.

1. **Automated Security Policy Rollback: Prevents misconfigurations** from impacting network authentication.
2. **Redundant AI-Based Threat Detection:** Uses **multi-layered AI models** to detect **cyber threats in real-time**.
3. **IoT Device Quarantine: Isolates compromised devices** to prevent **botnet-based attacks**.
4. **Zero Trust Adaptive Access Recovery: Restores authentication services** based on **risk-based policies**.

Telecom Networks Frameworks

- ISO/IEC 27001
- ETSI(European Telecommunications Standards Institute) EN 303 645
- NIST CSF(NIST CyberSecurity Framework)

ISO/IEC 27001 for 5G Networks

Overview:

Definition: ISO/IEC 27001 is an internationally recognized standard for Information Security Management Systems (ISMS).

- **Key Security Principles:** It is based on the **CIA Triad** (Confidentiality, Integrity, and Availability), ensuring secure handling of information.
- **Risk Management:** It follows a proactive approach to identifying vulnerabilities and mitigating risks.

Implementation Process: Organizations undergo certification through risk assessments, security controls, internal audits, and continuous improvement.

ISO Security Frameworks for 5G

- The **ISO/IEC 27001** framework provides a systematic approach to securing information systems through risk management, policy enforcement, and continuous monitoring.
- **ISO/IEC 27701** extends 27001 to address privacy information management, critical for telecom providers handling user data.
- **ISO/IEC 27017 & 27018** provide cloud security and privacy guidance, ensuring protection in cloud-based 5G infrastructure.
- These standards are essential in securing 5G networks against cyber threats while ensuring regulatory compliance.

Risk Assessment for ISO/IEC 27001 in 5G

Highlighting **major vulnerabilities in 5G networks** and how they **increase security risks** if **left unaddressed**.

- **Weak IAM Policies:** Overprivileged access → Insider threats, unauthorized access.
- **Unpatched Network Functions:** Delayed software updates → Exploitable vulnerabilities (CVE attacks).
- **Insecure APIs:** Lack of authentication → Enables unauthorized data extraction.
- **Insufficient Encryption:** Weak TLS/IPSec settings → Data breaches.
- **Lack of Continuous Monitoring:** No real-time detection → Persistent unauthorized access.

Likelihood and Impact Analysis:

- Risk levels are evaluated based on **how likely a threat is** and **its impact on telecom operations**.

Risk Scenario	Likelihood	Impact	Risk Score
Unauthorized network access due to weak IAM	High (1.0)	High (100)	100 (Critical)
DDoS attack on core telecom servers	Medium (0.5)	High (100)	50 (High)
Data leakage via misconfigured APIs	Medium (0.5)	Medium (50)	25 (Moderate)
Unpatched software vulnerabilities	High (1.0)	Medium (50)	50 (High)
Lack of encryption leading to eavesdropping	Low (0.1)	High (100)	10 (Low)

Risk Mitigation for ISO/IEC 27001 in 5G

ISO 27001-based security controls that protect 5G networks from major cyber threats.

Mitigation Strategies for Identified Risks:

- **Unauthorized Access → Multi-Factor Authentication (MFA):** Enforce MFA for all logins to prevent unauthorized access.
- **DDoS Attacks on 5G → AI-Driven DDoS Protection:** Use AI-based detection (e.g., Cloudflare, Arbor Networks).
- **Supply Chain Attacks → Third-Party Security Audits:** Enforce ISO Annex A.15 policies for vendor security.
- **SIM Swap & Subscriber Data Theft → AI-Based Fraud Detection:** Monitor unusual SIM swap activities.
- **Cloud Security Misconfigurations → Zero Trust Enforcement:** Implement OAuth 2.0, TLS 1.3 for API authentication.

Implementing ISO/IEC 27001 Security Controls in Telecom

layered security approach for **telecom risk mitigation under ISO 27001**

- **Technical Controls:**
    a. **Role-Based Access Control (RBAC):** Restricts access to telecom systems based on job roles.
    b. **Encryption (AES-256, TLS 1.3, IPSec):** Protects sensitive subscriber data.
    c. **SIEM & Continuous Monitoring:** Uses Splunk, IBM QRadar to detect anomalies.
- **Operational Controls:**
    a. **Data Loss Prevention (DLP):** Blocks unauthorized data transfers (USB, email, cloud).
    b. **Intrusion Detection & Prevention (IDS/IPS):** Protects telecom signaling protocols (SS7, Diameter, SIP).
- **Management Controls:**
    a. **Incident Response Plan (ISO/IEC 27035):** Defines response for DDoS, data breaches.

Business Continuity & Risk Analysis in 5G

How **ISO 27001's BCP framework** ensures **5G network resilience against cyberattacks**.

Business Continuity Planning (BCP) ensures telecom resilience:

- **Minimizes downtime** for subscriber services.
- **Protects telecom infrastructure** from cyber threats.
- **Ensures compliance** with security regulations (ETSI, NIST, ISO).

Risk Analysis in BCP:

- **DDoS Attack on Core Network:** Mitigation → AI-driven rate limiting.
- **Cloud Misconfigurations:** Mitigation → Zero Trust security model.
- **5G Network Function Failure:** Mitigation → Failover mechanisms, redundancy.
- **SIM Swap Fraud:** Mitigation → AI-based anomaly detection.

ETSI EN 303 645

- Managing Cybersecurity Risk across variety of industries
- Device Security design for IoT Devices - Security Boot and firmware updates
- Data Encryption and Storage - encryption of data both in rest and in transit
- Cloud Connectivity - Secure API’s, Authentication mechanisms, Cloud firewalls and Network Segmentation

Risk Assessment of ETSI EN 303 645

Key Risks and Vulnerabilities

- Unauthorized access - Remote Exploitation of IoT Devices
- Unsecured Data - Data breaches and Man-in-the-middle attacks
- Outdated Firmware - exploitation of unpatched vulnerabilities and lack of secure update mechanism
- Privacy Violations

Risk Mitigation Strategies

- Device Authentication, Secure and strong passwords.
- Data Encryption, Access Control.
- Secure updates(Automated Patches and Updation), Cryptographic Signing.
- Anonymization, Consent Management

NIST Cybersecurity Framework (NIST CSF)

- Assist telecom companies in meeting and maintain the regulatory requirements and industry standards.
- Critical Infrastructure Protection
- Incident Detection and response - ensures necessary process for detecting, responding and recovering
- Risk Based approach with functions - Identify, Protect, Detect, Respond and Recover

Risk Assessment in NIST CSF

- DoS attacks, Outdated hardware/software. Unsecured Communication Protocols, poor device management
- Insufficient Encryption protocols, and weak authentication systems
- Lack of real time monitoring tools and network intrusions
- Data breaches, Data Loss and Reputation Damage

Risk Mitigation

- Regular Patching and hardware updates
- Strong access controls, Encryption and Multi Factor Authentication
- For monitoring we can have real time monitoring with threat intelligence sharing like IDS(Intrusion Detection System)
- Regular backups for Data loss and breaches.
- Ensuring critical systems can be quickly restored from backups.

- NIST CSF (Telecom) Aims for 99.9% to 99.999% uptime Focuses on overall network resilience, continuous monitoring, redundancy, and incident response. Helps telecom organizations recover quickly, minimizing downtime.

- ETSI EN 303 645 (IoT) Aims for 99.9% to 99.999% uptime Focuses on securing IoT devices, ensuring they operate securely and remain resilient in the network, preventing IoT-related downtimes that could impact service availability.