



Connected Doesn't Mean Protected

Securing Cellular IoT: What Every Executive Needs to Know

This is a whitepaper of the GSMA IoT Community

This briefing provides business executives with a high-level overview of how to enhance security and robustness in cellular IoT deployments.

Drawing on GSMA's IoT Security Guidelines (FS.60), it classifies security threats, mitigation strategies, and best practices by relevance and importance across three key domains: Devices, Mobile Networks, and Applications.

Overview of Accountability per industry role

Accountability by Security Domain			
ENTITY	 DEVICE SECURITY	 NETWORK SECURITY	 APPLICATION SECURITY
Device OEM	✓	⚠ (limited)	✗
Cellular Module Provider	✓	✓	✗
Chipset Provider	✓	✗	✗
eUICC Manufacturer	✓	✓	✗
Mobile Network Operator	✗	✓	✗
Application Developer	✗	✗	✓
IoT Service Provider	✗	✗	✓
Backend Service Provider	✗	✗	✓
✓ Primary Responsibility Accountable ⚠ Partial Responsibility ✗ Not Typically			

Device-Related Security



High-Priority Threats and Mitigations

1	 Unauthorized Access	 Risk: Compromised devices can leak data or be hijacked (e.g., for botnets).	 Mitigations: Strong authentication, secure provisioning, encrypted credentials, and identity lifecycle management.
2	 Malware Infections/ Code Injection	 Risk: Malicious code can lead to persistent compromise or lateral movement.	 Mitigations: Secure boot, firmware signing, runtime integrity checks, secure update delivery.
3	 Physical Tampering	 Risk: Physical access can expose credentials or allow hardware attacks.	 Mitigations: Tamper-evident design, use of tamper-resistant, hardware secure elements (e.g., eSIMs), secure storage for keys.

Best Practices

- ✓ Carry out regular firmware updates with rollback protection.
- ✓ Implement secure decommissioning processes.
- ✓ Use hardware security modules (HSMs), tamper-resistant elements (e.g. eSIMs/iSIMs, secure elements) for cryptographic functions (and not SoftSIM).

Mobile Network-Related Security



High-Priority Threats and Mitigations

1	 Spoofing/Impersonation of Network Entities	 Risk: Enables man-in-the-middle (MitM) attacks and fake base stations.	 Mitigations: Mutual authentication using SIM/eSIM, network certificate validation.
2	 Data Interception/ Eavesdropping	 Risk: Unencrypted transmissions can expose confidential or sensitive data.	 Mitigations: 3GPP-standard encryption, TLS/DTLS protocols, VPN tunnelling for sensitive traffic.
3	 Signaling Attacks (e.g., Denial of Service)	 Risk: Can degrade or block device connectivity.	 Mitigations: Rate limiting, network traffic profiling, anomaly detection systems.

Best Practices

- ✓ Continuously monitor network.
- ✓ Implement and update SIM-based security algorithms (e.g., MILENAGE).
- ✓ Use operator-grade firewalls and intrusion prevention systems.

Application-Related Security



High-Priority Threats and Mitigations

1	 Insecure APIs	 Risk: Common point of exploitation for data exfiltration or service manipulation.	 Mitigations: Strong authentication, input validation, access control, rate limiting.
2	 Data Breaches	 Risk: High regulatory and reputational impact.	 Mitigations: End-to-end encryption, secure data storage, logging and monitoring.
3	 Weak Authentication / Authorization	 Risk: Leads to unauthorized access to critical systems.	 Mitigations: Role-based access control (RBAC), least privilege, Multi-Factor Authentication (MFA).

Best Practices

- ✓ Secure Software Development Life Cycle (SDLC) processes.
- ✓ Penetration testing and regular vulnerability assessments.
- ✓ Incident response planning and data breach notification protocols.

Security Management Key Recommendations



- ✓ **Adopt a Holistic Security Model:** Integrate security across devices, networks, and application layers.
- ✓ **Invest in Lifecycle Security:** Include secure design, deployment, maintenance, and decommissioning.
- ✓ **Prioritise by Risk and Business Impact:** Focus first on high-impact, high-likelihood threats.
- ✓ **Partner with Trusted Ecosystem Players:** Ensure your vendors, operators, and integrators follow GSMA and industry best practices.
- ✓ **Stay Informed:** Monitor threat intelligence feeds and participate in IoT security working groups.

Priority Heatmap Overview

THREAT CATEGORY	THREAT		IMPACT	LIKELIHOOD
 DEVICE	 Unauthorized Access			
 DEVICE	 Malware Infections/Code Injection			
 DEVICE	 Physical Tampering			
 NETWORK	 Spoofing/Impersonation of Network Entities			
 NETWORK	 Data Interception/Eavesdropping			
 NETWORK	 Signaling Attacks (e.g., Denial of Service)			
 APPLICATION	 Insecure APIs			
 APPLICATION	 Data Breaches			
 APPLICATION	 Weak Authentication/Authorization			

Further Reading: Full GSMA IoT Security Guidelines (FS.60):

<https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/wp-content/uploads/2024/07/FS.60.pdf>

GSMA Head Office

1 Angel Lane
London
EC4R 3AB
UK

Email: info@gsma.com

