XECURITYPULSE

2025

HIJACKED SIGNALS

WHY CELLULAR SECURITY IN THE 5G ERA IS AT RISK

XECURITYPULSE

TABLE OF CONTENTS

XECURITYPULSE

ABOUT THE AUTHOR

TAHA SAJID, CISSP, MSC

FOUNDER OF XECURITY PULSE

A world-renowned cybersecurity expert, Taha Sajid is also a driving influence in developing technologies. Principal Architect and Founder of Xecurity Pulse, he has significantly influenced the trajectory of cybersecurity via his projects in Telecom, Zero Trust, AI, and Blockchain. He is skilled in securing vital infrastructure, introducing AI-driven security structures, and transforming blockchain security.

Taha is the author of The Blockchain Security Handbook, a definitive guide to understanding and mitigating risks in blockchain ecosystems. Beyond his technical expertise, he is a mentor, an EB1A coach, and an Infosec Board Member who is dedicated to directing the future generation of cybersecurity experts. Respectable consultant and award-winning leader, he regularly works with field pioneers to advance invention and protect the digital realm.

Through his work as a LinkedIn Instructor and thought leader, he highlights his devotion to learning and information-sharing, therefore guaranteeing that cybersecurity and new technologies remain accessible and impactful. Through his strategic vision and relentless pursuit of excellence, Taha continues to shape the global security landscape.

XECURITYPULSE

FOREWORD

IMRAN SALEEM

TELECOM SECURITY EXPERT | MEMBER OF GSMA CVD (POE)

Imran Saleem is a seasoned Security Researcher with nearly two decades of experience in telecom and cybersecurity. He has served as a cybersecurity consultant for Fortune 100 companies and has shared his expertise at major conferences such as RSA, DeepSec, Besides, Black Hat, and HITB. His contributions to industry bodies like the GSMA and the 3GPP Security Working Group, along with his role as a member of the GSMA Panel of Experts, underscore his influence in the field.

Recognized for his impactful work, Imran Saleem has earned acknowledgment from GSMA and peers alike. His deep insights into digital security and commitment to advancing industry standards continue to inspire professionals navigating the evolving challenges of cybersecurity and telecom.

XECURITYPULSE

ABSTRACT

IN THIS AGE OF HYPERCONNECTIVITY, CELLULAR NETWORKS ARE THE HIDDEN ARTERIES OF OUR DIGITAL CULTURE.

Seemingly strong 4G and 5G infrastructures hide vulnerabilities under the surface that could trouble the very foundation of worldwide communication. The sophisticated environment of cellular security is explored in this report, revealing previously unknown vulnerabilities in LTE and 5G core deployments that could subject networks to fresh attack vectors, from broad denial-of-service attacks to covert data breaches. By analyzing real-life cases and emerging threat intelligence, we investigate how adversaries leverage standardized protocols and changing network designs.

The report also describes a tactical roadmap comprising embracing zero-trust infrastructures, integrating AI-driven anomaly detection, and supporting industry-wide cooperation. In essence, our analysis calls for a change in cellular security approaches, we propose a proactive, powerful model that can respond to and counteract the advanced cyber attacks of tomorrow.

XECURITYPULSE

INTRODUCTION

Imagine a city where every bus, building, and streetlight is connected by invisible digital strings that create a continuous information flow keeping the contemporary world running. This is the domain of cellular networks, a hidden infrastructure that links daily billions of devices. Behind this flawless connectivity, however, are weaknesses that can be abused by someone with vicious intentions.

This report contradicts the widely held idea that cellular networks are impenetrable defenses. In reality, the very designs that facilitate our worldwide communications could also be their most serious flaw. Essential for technologies like 5G, standardized protocols and up-to-date, cloud-generated designs may produce unanticipated security gaps which have the potential to interfere with communications on a vast scale, leaving whole regions abruptly cut off.

This report reveals the concealed weaknesses of cellular networks by delving into the inner mechanics of modem telecom systems. Our goal is to highlight these weaknesses and give a roadmap for the creation of a more stable future for cellular connectivity.

XECURITYPULSE

FAULTY FREQUENCIES:

MAPPING HIDDEN RISKS IN CELLULAR SECURITY

Operating on highly standardized protocols, cellular networks allow for worldwide device and network Interoperability. Although this standardization allows for natural interaction, it also establishes a predictable template that opponents might learn and take advantage of. Recent investigations uncovered 119 security vulnerabilities in various LTE and 5G core implementations, ranging from open-source platforms like Open5GS, Magma, and OpenAirInterface to proprietary systems such as Athonet and SD-Core.

Operators are exposed to threats such as denial-of-service (DoS) attacks, data interception, and unauthorized access to subscriber data due to these weaknesses. Their occurrence in outdated as well as actively maintained infrastructure is especially concerning. This implies a fundamental problem in how cellular security is addressed, with gaps in secure coding practices, inadequate testing of edge cases, and the rapid rollout of new technologies without comprehensive risk assessments. Cellular networks transitioning to 5G broaden their attack surface, hence opening chances for exploitation never present before.

XECURITYPULSE

KEY VULNERABILITIES AND EXPLOITATION SCENARIOS

The vulnerabilities identified in cellular cores can be grouped into several categories, each with distinct implications for network operators and users:

DENIAL-OF-SERVICE ATTACKS ON CORE COMPONENTS

Cellular cores rely on specialized functions like the Mobility Management Entity (MME) and Serving Gateway (SGW) to handle network traffic and subscriber mobility. Attackers can exploit vulnerabilities in these components to launch DoS attacks, overwhelming the system with malicious traffic. Unlike traditional DoS attacks, which target specific websites or services, these attacks disrupt entire cellular networks, rendering communication impossible in affected areas.

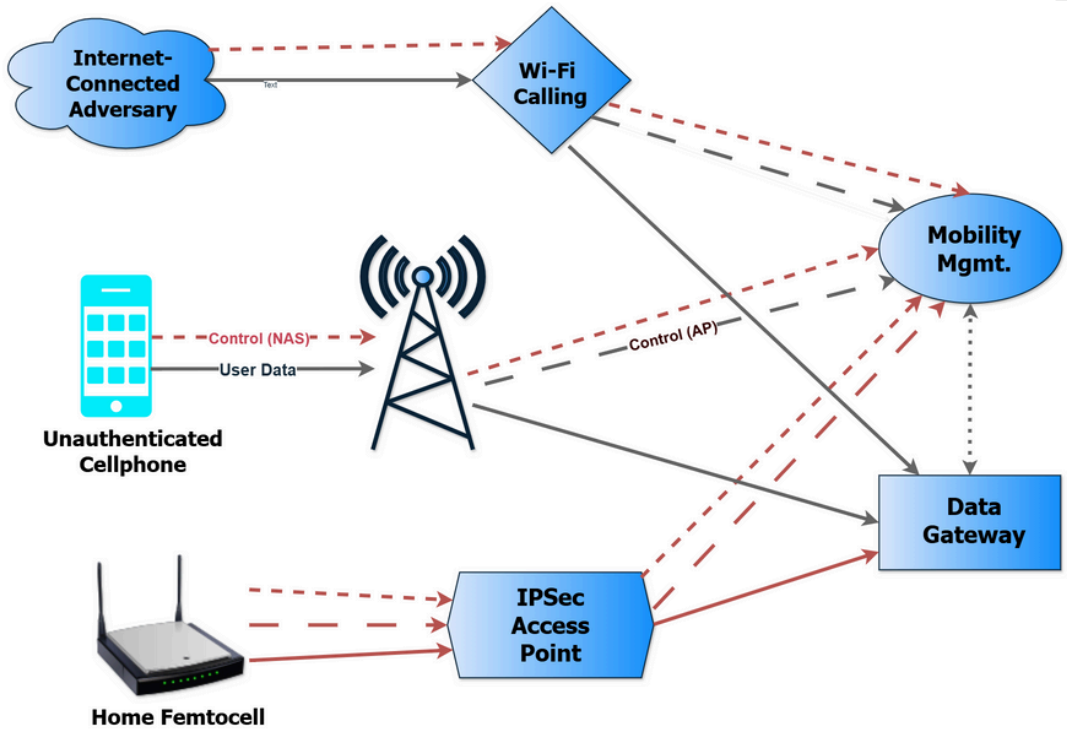
REMOTE CODE EXECUTION

Some vulnerabilities enable attackers to execute arbitrary code within the cellular core. This could allow them to manipulate network traffic, intercept sensitive data, or even compromise subscriber information. Remote code execution is particularly dangerous as it grants adversaries control over critical network functions.

XECURITYPULSE

UNAUTHENTICATED DEVICE ACCESS

Cellular networks traditionally require devices to authenticate using SIM cards. However, certain flaws allow unauthenticated devices to send malicious packets directly to the core network. This opens the door to attacks that bypass traditional security measures, including those initiated from internet-based services like Wi-Fi Calling.



COMPROMISED BASE STATIONS AND FEMTOCELLS

As 5G networks increase, the deployment of small-scale base stations in public or semi-public locations increases. These stations can be compromised by attackers, who can then exploit vulnerabilities to communicate maliciously with the network core. This risk is compounded by the decentralized nature of modern cellular architectures, which rely on distributed components for scalability.

XECURITYPULSE

TOP VULNERABILITY ANALYSIS IN CELLULAR SECURITY

Modern cellular networks, especially open-source 5G implementations like Open5GS, Magma, and OpenAirInterface, are critical for research and innovation. However, these implementations also introduce vulnerabilities that attackers can exploit to compromise network security, intercept communications, and disrupt services. Below, we analyze five major vulnerabilities affecting these systems, with a focus on OpenAirInterface (5G).

1. NULL POINTER DEREFERENCE IN NGAP PROTOCOL (CVE-2024-24445) – DOS THROUGH FAULTY MESSAGE HANDLING

One of the most concerning flaws in OpenAirInterface's Next Generation Application Protocol (NGAP) is a null pointer dereference. This issue arises when the system attempts to process an unsupported protocol message and inadvertently accesses an invalid memory reference. The result? A system crash leading to denial-of-service (DoS) attacks.

```
void ngap_app::handle_receive(
        bstring payload, sctp_assoc_id_t assoc_id, sctp_stream_id_t stream,
        sctp_stream_id_t instreams, sctp_stream_id_t outstreams) {
    // ...

    // Handle the message
    (*messages_callback[ngap_msg_pdu->choice.initiatingMessage->procedureCode]
                       [ngap_msg_pdu->present - 1])(
        assoc_id, stream, ngap_msg_pdu);
    // ^ function pointer dereference of potentially null value

    // ...
```

◆ **Exploitation Scenario:** An attacker sends malformed NGAP messages containing unexpected procedure codes. The system fails to handle these messages properly, crashing the Access and Mobility Management Function (AMF), leading to service disruption.

◆ **Potential Impact:**

- Repeatedly exploiting this flaw can take down an entire 5G core network
- Attackers can target critical AMF components, affecting authentication, mobility, and session management

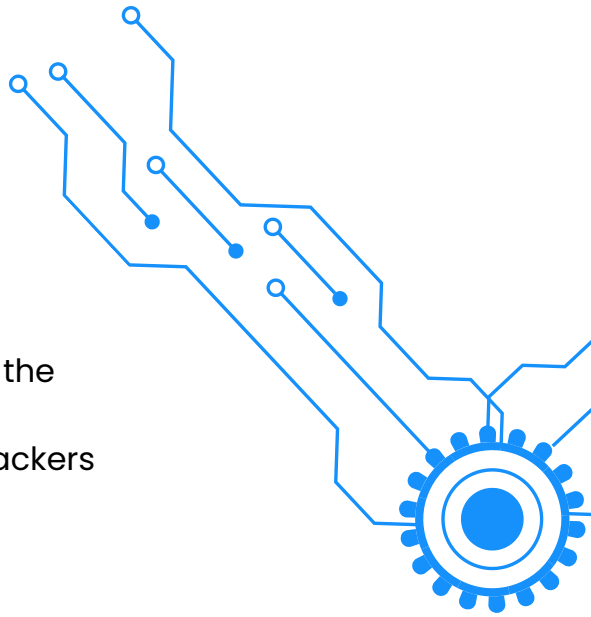
◆ **Mitigation Strategies:**

- Implement input validation and error handling to filter out malformed NGAP messages
- Use memory-safe programming techniques to prevent null pointer dereference crashes

2. STACK-BASED BUFFER OVERFLOW IN PDU PROCESSING (CVE-2024-24450) – REMOTE CODE EXECUTION RISK

Another critical flaw exists in the PDU (Protocol Data Unit) Session Resource Setup Response handling function. A stack-based buffer overflow occurs when an attacker sends a specially crafted FailedToSetupList that exceeds the expected buffer size.

◆ **Exploitation Scenario:** A remote attacker with access to the N2 interface sends a maliciously large list of failed session setups. Since the function copies data into a fixed-size buffer without proper bounds checking, this can lead to memory corruption and potential remote code execution (RCE).



- **Potential Impact:**
  - Attackers could execute arbitrary code within the AMF, potentially taking full control
  - Could allow privilege escalation, enabling attackers to manipulate network sessions

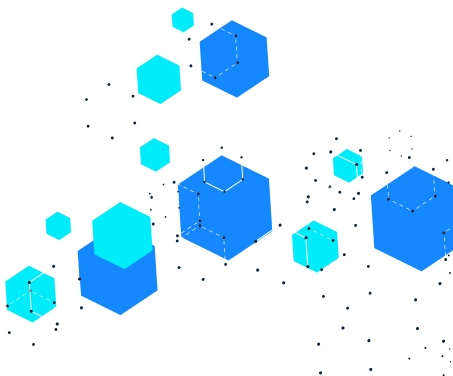
- **Mitigation Strategies:**
  - Enforce strict boundary checks on buffer sizes to prevent overflows
  - Implement memory-safe programming practices, such as using dynamic memory allocation instead of fixed buffers

```
int ngap_amf_handle_pdu_session_resource_setup_response(
        const sctp_assoc_id_t assoc_id, const sctp_stream_id_t stream,
        struct Ngap_NGAP_PDU* message_p) {
    // ...

    std::vector<PDUSessionResourceFailedToSetupItem_t> list_fail;
    if (!pdu_session_resource_setup_resp->getPduSessionResourceFailedToSetupList(
            list_fail)) {
        Logger::ngap().error(
            "decoding PduSessionResourceSetupResponseMsg "
            "getPduSessionResourceFailedToSetupList IE  error");
    } else {
        PduSessionResourceSetupUnSuccessfulTransferIE* UnSuccessfultransfer =
            new PduSessionResourceSetupUnSuccessfulTransferIE();
        uint8_t buffer[BUFFER_SIZE_512];
        // ^ static buffer of 512 bytes allocated
        memcpy(
            buffer, list_fail[0].pduSessionResourceSetupUnsuccessfulTransfer.buf,
            list_fail[0].pduSessionResourceSetupUnsuccessfulTransfer.size);
        // ^ static buffer copied in data from buffer that could have more than 512 bytes

        // ...
    }

    // ...
}
```



XECURITYPULSE

3. UNINITIALIZED MEMORY ACCESS IN RADIO CAPABILITY HANDLING (VULN-B03) – DATA LEAKAGE THREAT

The OAI AMF contains a flaw in its Radio Capability Indication message processing, where it accesses uninitialized memory. This vulnerability arises because the system does not properly initialize the radio capability structure before use, leading to potential information leaks.

- **Exploitation Scenario:** An attacker crafts a malformed Radio Capability Indication message that causes the system to return uninitialized memory content. This could leak sensitive device data, including network parameters and user authentication details.

- **Potential Impact:**
  - Attackers can extract internal memory data, potentially revealing security-sensitive information
  - Could be combined with other exploits to gain deeper system access

- **Mitigation Strategies:**
  - Ensure all memory allocations are properly initialized before being accessed
  - Implement strict input validation for Radio Capability messages

XECURITYPULSE

4. AUTHENTICATION BYPASS VIA WEAK NGAP HANDLING – UNAUTHORIZED NETWORK ACCESS

A logic flaw in the NGAP authentication procedure enables attackers to bypass authentication checks and gain unauthorized access to the network.

◆ **Exploitation Scenario:** By manipulating NGAP messages, an attacker can trick the AMF into skipping authentication steps, allowing them to impersonate a legitimate user or device.

◆ **Potential Impact:**

- Unauthorized devices can access the 5G core network without authentication
- Attackers can spoof SIM identities, leading to identity theft and service hijacking

◆ **Mitigation Strategies:**

- Strengthen authentication mechanisms with additional security checks
- Implement behavioral anomaly detection to detect suspicious authentication patterns

5. NETWORK SLICE ISOLATION FAILURE – CROSS-SLICE SECURITY BREACH

5G networks introduce network slicing, a technology that allows multiple virtual networks to run on shared infrastructure. However, in some implementations, weak slice isolation allows attackers to move laterally between network slices, creating serious security risks.

◆ **Exploitation Scenario:** A hacker gains access to a low-privilege slice (e.g., public IoT services) and exploits vulnerabilities to access a high-privilege slice (e.g., emergency services, private enterprise networks).

- **Potential Impact:**
  - Attackers can steal sensitive data from other slices
  - A compromise in one slice could lead to system-wide network breaches
- **Mitigation Strategies:**
  - Enforce strict access controls and segmentation between slices
  - Regularly audit and monitor slice communications for anomalies

As 5G networks evolve, so do the threats targeting them. The vulnerabilities discussed highlight the urgent need for stronger security measures in open-source 5G implementations like Open5GS, Magma, and OpenAirInterface. Attackers are actively looking for weaknesses in protocol handling, memory management, and authentication mechanisms to gain unauthorized access.

XECURITYPULSE

KEY TAKEAWAYS FOR SECURE 5G DEPLOYMENTS:

- **Input Validation –** Prevent malformed messages from triggering vulnerabilities
- **Memory Safety –** Address null dereferences, buffer overflows, and uninitialized memory use
- **Authentication Hardening –** Strengthen device and user authentication mechanisms
- **Network Isolation –** Ensure strict segmentation between different 5G network slices

By proactively identifying and mitigating these risks, we can build resilient, secure, and future-proof 5G networks that protect users, data, and infrastructure from emerging cyber threats.

XECURITYPULSE

THE ROLE OF EMERGING TECHNOLOGIES IN CELLULAR SECURITY

The transition to 5G and the increasing adoption of edge computing, IoT devices, and network slicing introduce new security challenges. While these technologies promise greater efficiency and lower latency, they also expand the attack surface:

- **Network Slicing Risks**

5G networks leverage network slicing to create virtualized, isolated networks for specific use cases, such as autonomous vehicles or smart cities. However, improper configuration or exploitation of vulnerabilities in the slicing mechanisms can lead to cross-slice attacks, where a breach in one slice compromises others.

- **IoT Device Vulnerabilities**

The proliferation of IoT devices connected to cellular networks exacerbates security risks. Many IoT devices lack robust security measures, making them easy targets for attackers. Once compromised, these devices can be used as entry points to launch broader attacks on the network core.

- **Edge Computing Challenges**

By processing data closer to the source, edge computing reduces latency but also decentralizes security responsibilities. Ensuring consistent security across distributed edge nodes is a significant challenge for network operators.

XECURITYPULSE

PROACTIVE STRATEGIES FOR CELLULAR SECURITY

Addressing the vulnerabilities in cellular networks requires a holistic approach that combines technical, organizational, and regulatory measures. Below are some actionable strategies to enhance cellular security:

- **Comprehensive Vulnerability Management**

Network operators must implement robust vulnerability management programs that prioritize regular patching and updates. Collaboration between operators and vendors is essential to ensure that vulnerabilities are identified and remediated quickly.

- **Stronger Authentication Mechanisms**

Mutual authentication between devices and the network is critical to prevent unauthorized access. Advanced methods like Public Key Infrastructure (PKI) and digital certificates can provide stronger security than traditional SIM-based authentication.

- **Advanced Threat Detection**

Deploying AI-driven anomaly detection systems can help identify unusual traffic patterns indicative of ongoing attacks. These systems can provide real-time alerts, enabling operators to respond quickly and mitigate damage.

- **Supply Chain Security**

The hardware and software components of cellular networks often come from diverse sources, creating potential supply chain vulnerabilities. Operators must conduct thorough audits of their supply chains to identify and address security risks.

XECURITYPULSE

PROACTIVE STRATEGIES FOR CELLULAR SECURITY

- **Security-by-Design**

The adoption of secure coding practices and rigorous testing during the development of cellular infrastructure is essential. This includes the use of fuzz testing, penetration testing, and code audits to identify vulnerabilities before deployment.

- **Public-Private Collaboration**

Governments, regulatory bodies, and private sector organizations must work together to establish standards and frameworks for cellular security. Information sharing on emerging threats and vulnerabilities can enhance collective defenses.

XECURITYPULSE

FUTURE DIRECTIONS IN CELLULAR SECURITY

The following trends are likely to shape the future of cellular security:

- **Post-Quantum Cryptography**

The advent of quantum computing poses a threat to existing encryption algorithms used in cellular networks. Research into post-quantum cryptographic solutions is essential to future-proof network security.

- **Zero-Trust Architecture**

Adopting a zero-trust approach to cellular security can help mitigate risks by assuming that all devices and network components are potentially compromised. This involves continuous monitoring, strict access controls, and micro-segmentation.

- **Decentralized Security Models**

Blockchain technology offers the potential for decentralized security solutions, such as tamper-proof audit trails and distributed authentication mechanisms. These innovations could enhance the resilience of cellular networks.

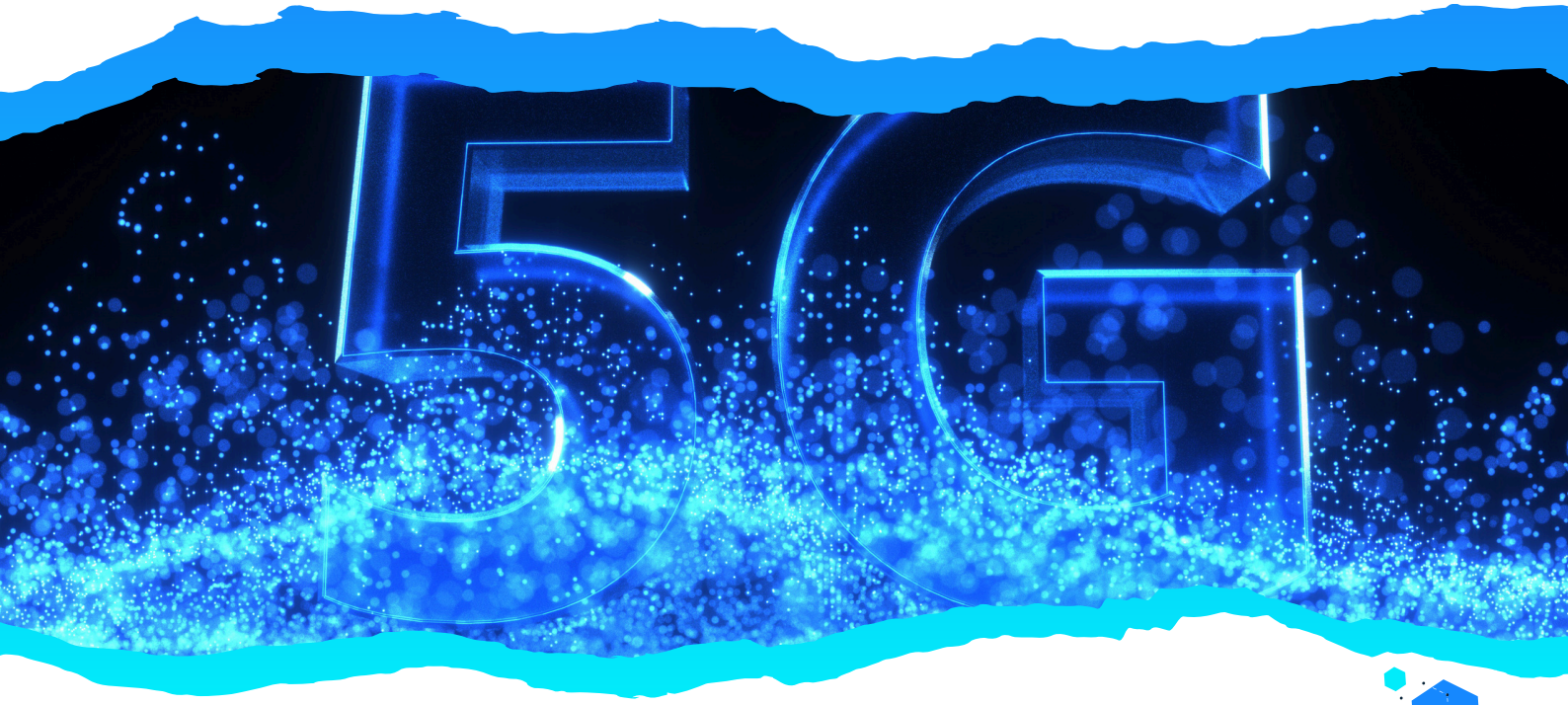
CELLULAR NETWORKS EVOLVE, SO MUST OUR APPROACH TO SECURITY

XECURITYPULSE

CONCLUSION

Deeply examining cellular flaws shows a terrain where major security gaps result from technical oversights in protocol usage and memory management. These problems are signs of a more general structural issue in modern open-source 5G deployments rather than isolated anomalies. Urging stakeholders to go beyond responsive measures, they compel a reevaluation of our present security policies. Bridging the gap between innovation and inherent risk calls for the rather keen use of strong verification techniques and layered defenses.

The aim going forward is to turn these weaknesses from points of failure into prospects for rebuilding our cellular system. This implies creating systems that are not only responsive to emerging threats but are designed with security as a foundational element. By adopting a more systematic, forward-thinking approach to protecting network integrity, we can transform mobile security to suit the requirements of a changing digital environment, thereby establishing our future on principles of resiliency and deliberate innovation.



XECURITYPULSE

REFERENCES

- **SecurityWeek. LTE & 5G Vulnerabilities Could Cut Entire Cities from Cellular Connectivity.**
  - https://www.securityweek.com/lte-5g-vulnerabilities-could-cut-entire-cities-from-cellular-connectivity/

- **ResearchGate. 5G Core Security: An Insider Threat Vulnerability Assessment.**
  - https://www.researchgate.net/publication/380264652_5G_Core_Security_An_Insider_Threat_Vulnerability_Assessment

- **ResearchGate. Security and Protocol Exploit Analysis of the 5G Specifications.**
  - https://www.researchgate.net/publication/331080692_Security_and_Protocol_Exploit_Analysis_of_the_5G_Specifications

- **MDPI. Security Vulnerabilities in 5G Non-Stand-Alone Networks: *A Systematic Analysis and Attack Taxonomy.***
  - https://www.mdpi.com/2624-800X/4/1/2

- **National Security Agency. *Mobile Device Best Practices.***
  - https://media.defense.gov/2021/Sep/16/2002855921/-1/-1/0/MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3%20-%20COPY.PDF

- **ACM Digital Library. New Vulnerabilities in 4G and 5G Cellular Access Network Protocols: *Exposing Device Capabilities.***
  - https://dl.acm.org/doi/10.1145/3317549.3319728

- **Infosec Institute. Cellular Networks and Mobile Security.**
  - https://www.infosecinstitute.com/resources/network-security-101/cellular-networks-and-mobile-security/

XECURITYPULSE

2025

THANK YOU!

XECURITY-PULSE
SUPPORT@XECURITYPULSE.COM
HTTPS://XECURITYPULSE.COM/