Whitepaper:
RF Attacks in Private Cellular Networks

OneLayer Whitepaper: RF Attacks in Private Cellular Networks

Table of Contents

Introduction

As the digital infrastructure of our world becomes increasingly reliant on mobile telecommunications, Long-Term Evolution (LTE) stands as a pivotal technology in this evolution, enabling high-speed wireless communication for a myriad of devices and applications. Despite the advancements and benefits brought forth by LTE networks, they harbor intrinsic vulnerabilities, particularly in the domain of Radio Frequency (RF) attacks. These vulnerabilities are not just technical loopholes but significant security challenges that, despite being relatively well-known, remain dauntingly difficult to mitigate. The complexity of these vulnerabilities and the lack of comprehensive solutions underscore the critical nature of understanding and addressing RF attacks in LTE and its successor technologies, including 5G.

RF attacks exploit fundamental weaknesses in the LTE protocol, affecting both downlink and uplink communication channels. The repercussions of such exploits are far-reaching, with potential outcomes ranging from network disruption and degradation of service to severe breaches of confidentiality and data integrity. The intricacies of these attacks and their exploitation methods reveal a stark reality: current security measures and protocols, even those designed for newer technologies like 5G, are yet to offer foolproof protection against these vulnerabilities.

The intricacies of RF attacks and their exploitation methods reveal a stark reality: current security measures and protocols, even those designed for newer technologies like 5G, are yet to offer foolproof protection against these vulnerabilities.

The significance of RF vulnerabilities takes on an added dimension within the context of private cellular networks. In these environments, the associated risks of RF attacks are markedly elevated. Private networks, often tailored for specific industrial, corporate, or

specialized use cases, present unique security challenges. The confidentiality, integrity, and availability of data and services in these networks are of paramount importance, making the mitigation of RF attacks not just a technical issue but a critical business imperative. Additionally, the pivotal shift in the scale of LTE networks in the private networks market introduces the cell as a much more fragile point of failure from the private operator's perspective. As the private network ecosystem continues to evolve as an emerging market, the importance of addressing RF vulnerabilities becomes increasingly critical. The stakes are higher, the potential impacts are more severe, and the need for a deeper understanding and strategic mitigation is more urgent.

This whitepaper aims to shed light on the specific vulnerabilities that RF attacks exploit in LTE networks, with a focus on detailing the mechanics of various attacks at the bits and bytes level. Through a comprehensive examination of these vulnerabilities and their exploitation methods, we seek to provide a nuanced understanding of the threat landscape. Furthermore, by highlighting the elevated risks in private cellular networks, this document underscores the imperative for industry professionals to prioritize the mitigation of RF attacks. As we delve into the analyses of specific downlink and uplink attacks - our goal is to equip cybersecurity professionals with the knowledge and insights needed to safeguard their networks against these sophisticated threats, ensuring the security and reliability of LTE communications in the private cellular networks' domain.

Background on LTE Architecture and Security

The architecture of Long-Term Evolution (LTE) networks is intricately designed to facilitate high-speed data and voice communications across vast distances. Central to understanding LTE and its vulnerabilities, especially in the context of RF attacks, is familiarizing oneself with key terminologies and components:

- User Equipment (UE): The devices used by end-users to access the network, ranging from smartphones and tablets to IoT devices.
- Radio Access Network (RAN): The part of the network that sets up a connection between the UE and the core network through radio waves. In the context of LTE, this is specifically referred to as the Evolved UMTS Terrestrial Radio Access Network (E-UTRAN).
- Core Network: The backbone of the LTE network, known as the Evolved Packet Core (EPC), responsible for routing calls and data, maintaining user sessions, and delivering services such as voice over LTE (VoLTE).

LTE Security Mechanism

LTE incorporates several security mechanisms designed to protect the integrity, confidentiality, and availability of communications:

- Encryption safeguards data confidentiality by encoding the data exchanged between the UE and the network, typically using advanced algorithms like AES.
- Integrity Protection ensures that the data sent across the network is not tampered with, applying specifically to signaling data between the UE and the network.

- Authentication involves a mutual verification process between the network and the UE, ensuring that both parties are legitimate and authorized to communicate.

Vulnerabilities Exploited by RF Attacks

RF attacks exploit certain vulnerabilities unique to the wireless and open-air nature of LTE communications. A critical point of vulnerability lies in the fact that some messages exchanged between the RAN and the UE are unencrypted and lack identification. This lack of protection makes it relatively straightforward for a malicious actor to "fake" messages in both the uplink and downlink directions without needing to intercept the communication as a man-in-the-middle.

The open-air channel through which LTE operates allows for the possibility that if a malicious signal is broadcasted with sufficient strength or precision (matching the correct frequency and timing), it can be perceived by the legitimate UE or RAN as authentic. This susceptibility means that practically any malicious actor with close physical proximity to the targeted cell can launch impactful attacks on the network without requiring an authorized device. The implication here is significant, especially for private networks, as it suggests that the security and integrity of LTE communications can be compromised by merely having physical access to the network's operational vicinity.

The ease with which these attacks can be initiated, coupled with the fundamental challenge of securing open-air communications, underscores the urgent need for enhanced security measures. As we progress to analyze specific RF attacks in the next sections, we will focus on the vulnerabilities they exploit, how attackers could leverage these weaknesses and the potential impacts on both public and private LTE networks. This exploration aims to deepen the understanding of LTE's security challenges and highlight the critical importance of protecting against RF vulnerabilities in an increasingly connected world.

To better understand RF attacks in LTE, a clear explanation of the key concepts and channels involved in LTE communication is essential. This foundation is critical for delving into the specific attacks that exploit vulnerabilities in the LTE protocol.
When a UE powers on or moves into a new LTE network's coverage area, it initiates an attach request to gain access to the network's services.

This process involves several key steps and utilizes various channels and messages to establish a secure and efficient connection:

1. Searching for a Network: The UE initiates its connection to the LTE network by scanning for available signals, focusing on the Physical Broadcast Channel (PBCH). The PBCH transmits the Master Information Block (MIB), a fundamental set of data about the network, including bandwidth and the configuration of the Physical Hybrid ARQ Indicator Channel (PHICH). This information is critical for the UE to correctly synchronize with the network's frequency and timing, a prerequisite for any further communication. Without accurately processing the MIB, the UE is unable to align its signal with the network, effectively preventing any form of communication with the Radio Access Network (RAN).
2. System Information Acquisition: Upon successfully detecting a network and decoding the MIB, the UE's next step involves gathering more comprehensive system information, primarily through System Information Blocks (SIBs), starting with SIB1. The Physical Downlink Control Channel (PDCCH) carries Downlink Control Information (DCI) that indicates the scheduling of SIB1 (and other SIBs) on the Physical Downlink Shared Channel (PDSCH). This scheduling information is essential for the UE to know when to listen for SIBs, which contain detailed operational parameters like access policies, tracking area codes (TAC), and the scheduling of other SIBs. The UE locates these DCI messages within the Common Search Space (CSS) on the PDCCH, a process crucial for understanding the network setup and how to engage with it for service access. Accurate reception and processing of SIBs through the accurate guidance of DCIs from the CSS

enable the UE to complete its network attachment process and ensure proper service communication with the RAN.

3. Random Access Procedure: To initiate communication with the network, the UE sends a preamble on the Physical Random-Access Channel (PRACH). This step is critical for establishing an uplink synchronization with the network and requesting an initial resource allocation for further signaling. Without preamble, the RAN does not allocate dedicated resource allocation for further communication, which is essential to send user-plane traffic over the network.
4. Initial Connection Setup: Following the random-access procedure, the RAN allocates resources to the UE for sending the attach request message. This allocation and the direction to use the Physical Uplink Shared Channel (PUSCH) are communicated through DCI messages on the PDCCH. The UE-specific search space on the PDCCH is used here, directing the UE to the resources allocated specifically for it. This precise allocation allows the UE to transmit its attach request, marking a critical step towards establishing a successful network connection.
5. Security Procedures and Context Setup: Once the attach request is received, the network initiates security procedures, including authentication and encryption setup, to secure communication between the UE and the network. This involves exchanging messages that ensure both parties are legitimate, and that data transmitted over the air interface will be encrypted.
6. Completion of Attach Process: After the security procedures, the network assigns a Temporary Mobile Subscriber Identity (TMSI) to the UE and sends it the attach accept message. This message is transmitted over the Physical Downlink Control Channel (PDCCH) and informs the UE of its successful attachment to the network, including parameters for its network access and services.
7. Ongoing Communication: After the initial connection setup, the UE and the network engage in ongoing communication to maintain and optimize the connection. The Physical Uplink Control Channel (PUCCH) plays a crucial role in this phase by carrying uplink control information from the UE to the network. This includes acknowledgments of downlink data reception (ACK/NACK), scheduling requests (SR) for uplink data transmission resource allocation, and Channel

Quality Indicator (CQI) reports. These messages are vital for the dynamic management of network resources and the adaptation of transmission parameters to ensure efficient and reliable communication.

RF Attacks in LTE: Technical Overview

Given the open nature of the radio interface in LTE networks, where basic multiplexing relies on frequency and time, an attacker, by precisely tuning into the correct time and frequency, can exploit vulnerabilities in the air interface. The critical concepts outlined previously serve as a foundation for identifying these vulnerabilities and understanding their significant impact on network integrity. The openness of these communication channels, coupled with the lack of encryption and secure identification in certain critical procedures, dramatically simplifies the task for malicious actors with physical proximity to the network. By manipulating these unsecured channels and processes, attackers can significantly disrupt network operations. Recognizing the susceptibility of these key network elements to interference is essential for grasping the potential scale of disruption that can be inflicted upon the network's normal functioning.

Downlink Attacks

1. Common Search Space Exhaustion: Floods the PDCCH with noise or false DCI messages, preventing specific or several UEs from receiving correct SIB scheduling information – which is crucial for network connectivity and configuration.
2. MIB Blocking: By interfering with the PBCH, attackers can prevent the reception of the MIB for legitimate UEs, disrupting UEs from correctly accessing and configuring themselves for the network.
3. SIB1 Blocking: Disrupts the UE's reception of System Information Block Type 1 (SIB1) by interfering with its broadcast on the Physical Downlink Shared Channel

(PDSCH). This prevents the UE from acquiring essential network operational parameters and access policies, which are crucial for successful network attachment and configuration.

4. TAU Storm Initiation: Injection of incorrect Tracking Area Codes (TACs) within SIB1, misleading legitimate UEs to perform excessive Tracking Area Updates (TAU). This flood of unwarranted TAUs generates a signaling storm, straining and potentially overwhelming network resources.
5. TPC Faking: The TPC Faking attack involves the transmission of counterfeit Transmission Power Control (TPC) commands to the User Equipment (UE), misleading it into significantly elevating it transmit power. This malicious adjustment induces premature battery exhaustion and disrupts the cellular network's power control algorithms, potentially degrading overall communication quality and system efficiency.

Uplink Attacks

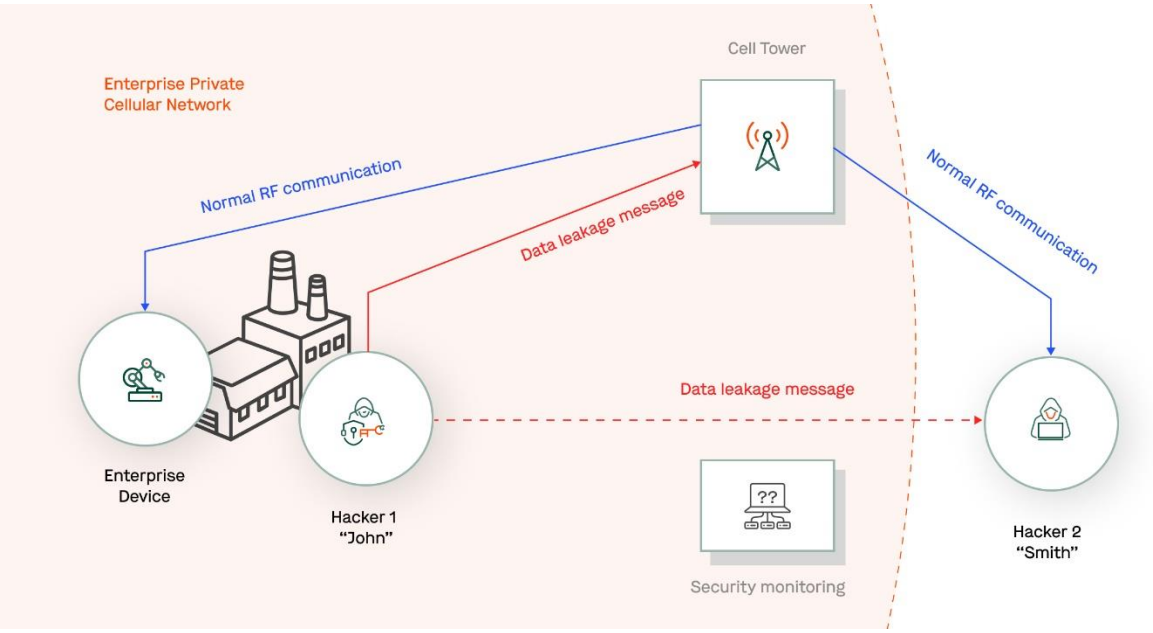
1. PRACH Exhaustion: Overloading the PRACH with excessive access attempts can deplete network resources, limiting the ability of legitimate UEs to establish connections.
2. HARQ Feedback Manipulation: Flood the PUCCH by disrupting ACK/NACK transmissions of HARQ, which results in falsely prompting retransmissions of user-plane communication that overload the network and degrade communication.
3. Scheduling Request Blockage: blocking UEs' scheduling requests on the PUCCH, preventing new uplink transmissions and straining network resource allocation.
4. Combined Uplink Attack: synergizes SR Blockage with PRACH Exhaustion by first obstructing UEs' uplink resource requests, thereby forcing them to retry connections via the PRACH. This influx of retries amplifies existing PRACH congestion creating a compounded effect that increases the PRACH overload.
5. Sparrow: manipulates random-access messages for covert transmission, embedding secret information within the standard communication framework, undetectable by conventional monitoring

Each of these attacks leverages specific vulnerabilities in the LTE protocol, exploiting the unencrypted and unprotected nature of essential control messages and channels. Understanding the technical mechanisms behind these vulnerabilities is crucial for developing effective countermeasures, particularly in the context of private cellular networks where the impact of these attacks can be significantly amplified. Let's delve into some of these attacks, to understand better their technical mechanism as well as their unique relevancy to the context of private cellular.

Case study 1: Sparrow

Introduction

The SPARROW attack leverages the LTE/5G random-access procedures and contention resolution mechanism to enable covert communication between devices. By exploiting the MAC layer's vulnerabilities, it facilitates the exchange of information without a proper network connection, IP packets or even core level signaling - evading detection and interception by security systems. This technique significantly impacts network security, offering a novel approach for clandestine communication across considerable distances, posing challenges for both detection and mitigation in private network contexts, particularly in environments requiring stringent security measures, like, for example – an internal Factory network.



Technical Overview

To deeply understand the SPARROW scheme, imagine two devices aiming for covert communication within an LTE/5G network. For the SPARROW attack to work, there must

be two devices that cooperate. Initially, one device, acting undercover, sends an RA message (Msg1) selecting a RACH preamble, starting the RA process without revealing its identity. Upon receiving Msg1, the cell sends RAR (msg2) which includes another temporary identifier (TC-RNTI) used for further communication.

The crux of SPARROW lies in Msg3, where the sending device encodes a secret message within the Contention Resolution Identity (CRI), a 48-bit field with 40 bits available for covert data. This message meant to resolve contention in the RA process, is sent back to the network, which then broadcasts the CRI in Msg4 as an acknowledgment. The cooperating device, aware of the agreed-upon RA-RNTI, decodes Msg2 to catch the TC-RNTI and listens for Msg4 to extract the secret message from the CRI, achieving stealth communication through this orchestrated misuse of RA messages.

To facilitate this exploitation, both participating devices must synchronize their actions within the network's operational framework. Normal RAR messages are monitored by both sides to synchronize on the relevant TC-RNTI identify and decode the intended communications amidst regular network traffic. This arrangement allows one device to encode data within the Contention Resolution Identity (CRI) during the Msg3 transmission, confident that the cooperating device, anticipating this signal, will decode the embedded information from Msg4. This strategy cleverly circumvents the network's limitations, particularly the complexity with detecting low level RF messages, the broadcast mechanism of the cell, and its inability to enforce backoff times reliably. Although there is a backoff mechanism in LTE, it purely trusts the UE to comply. A malicious UE can simply ignore backoffs, as the cell has no means to enforce it without strongly identifying the device across different RAs.

Within Private Networks Context

Private networks are usually highly secure. They serve sensitive or critical infrastructure and play as a gateway to the OT, IT or both networks. Therefore, the SPARROW attack in

the context of private networks is of extreme interest. Imagine an attacker intruding into a factory network. It was able to gather sensitive data from the operational network and now wants to leak it outside the internal network. Most organizations implement advanced security tools to either block or identify data leakage. Using SPARROW, intruders may leak sensitive data through stealth communication channels, undetected by regular security solutions. The range of the leak could even be outside the actual factory, as long as there's a signal of the RAN outside the factory territory.

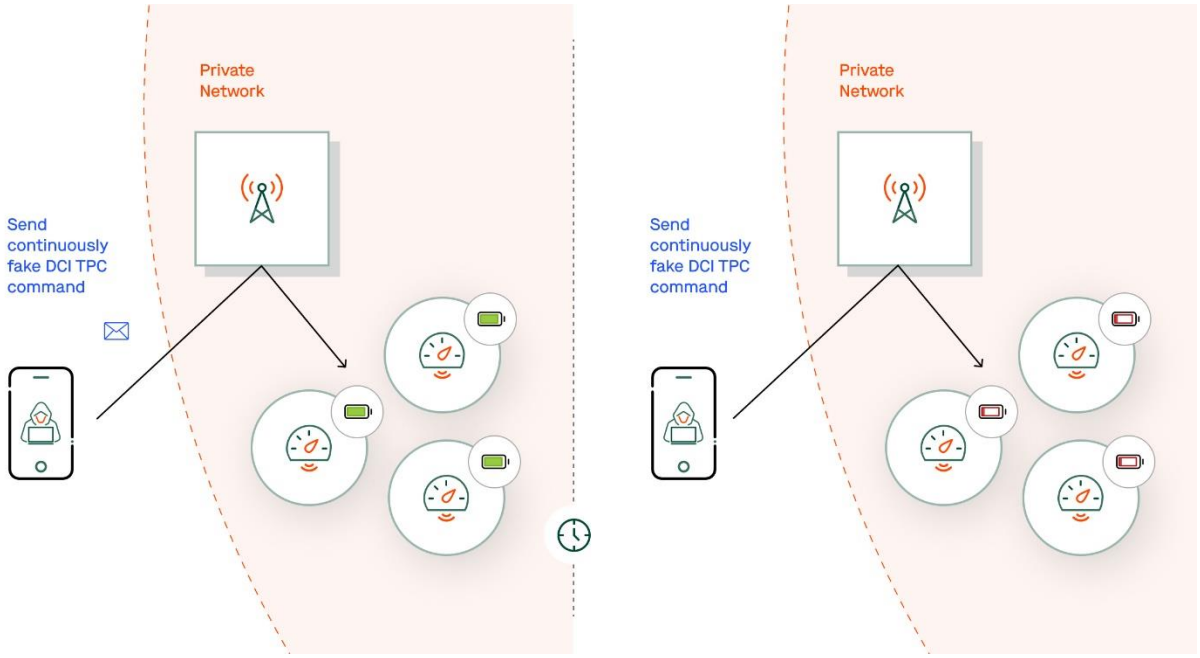
Using SPARROW, intruders may leak sensitive data through stealth communication channels, undetected by regular security solutions.

In contrast to public networks, private networks carry a heightened level of sensitivity that translates into a significant business concern rather than merely a technical nuance. While the SPARROW attack might not be deemed a substantial business risk in the context of public networks, its implications for private networks are far more serious. The specialized and often critical nature of data handled by private networks – as well as its interconnectivity with other sensitive networks - necessitates a more vigilant security posture, underscoring the importance of treating SPARROW and similar threats as pressing business risks that demand immediate and comprehensive mitigation strategies.

Case study 2: TPC Faking

Introduction

The TPC Faking attack constitutes a sophisticated threat vector against the integrity of cellular networks, specifically targeting the Transmission Power Control (TPC) mechanism that dynamically adjusts the transmission power of User Equipment (UE). By manipulating TPC commands, attackers induce UEs to unnaturally augment their transmission power, precipitating rapid battery drain and disrupting the network's power management protocols. This interference not only undermines communication quality and network efficiency but also jeopardizes the operational stability of private networks, where continuous device functionality and network reliability are paramount.



Technical Overview

The TPC Faking attack ingeniously exploits the LTE network's mechanism for managing the transmission power of User Equipment (UE) through a process that seems almost benign at its core but, in practice, unveils a significant vulnerability. At the heart of this exploit are the Transmit Power Control (TPC) commands, which are essential directives communicated from the network to the UE, dictating adjustments in the transmission power of the UE to optimize network efficiency, communication quality, and battery life. These TPC commands are embedded within specific DCI formats - namely formats 0, 3, and 3A - transmitted over the network's Physical Downlink Control Channel (PDCCH), a channel to which UEs are perpetually attuned, awaiting instructions.

The attack initiates when an adversary, having gained the capacity to inject DCI messages into the network, meticulously crafts and dispatches counterfeit DCI messages. These messages are carefully designed to mimic legitimate network commands but instruct UEs to increment their transmission power. The attacker does so by using the TPC command bits within the DCI, which tells the UE to increase its power usage. The deception does not rest on the complexity of the messages but on their indistinguishability from genuine commands and the UEs' inherent trust in the network's directives. As these fraudulent commands are transmitted over the PDCCH, they seamlessly integrate into the stream of legitimate network communication, effectively camouflaging their malicious intent.

What follows is a subtle yet relentless assault on the network's operational integrity. Each fake TPC command received coerces the UE into unnecessarily boosting its transmission power, a minor adjustment that, in isolation, appears inconsequential. However, the insidiousness of the attack lies in its persistence; through continuous delivery of these spurious commands, the attacker orchestrates a scenario where UEs are perpetually operating at elevated power levels. This not only precipitates a rapid depletion of the devices' battery life but also introduces a cascade of operational inefficiencies and interference with UEs of neighbor cells.

Moreover, the battery drain is affected not merely from the higher Tx power transmitted by the UE, but also because of the fabricated DCI messages – which prevent the UE from

returning to idle mode. The result is bypassing sophisticated battery saving modes such as the Connected DRX. The network, now cluttered with excessive and unwarranted transmissions, suffers from increased interference and battery drained UEs, which in turn degrades the quality of communication across the board.

Within Private Network Context

In the context of utility companies, the ramifications of the TPC Faking attack magnify due to the expansive and open nature of their private networks. These networks are not only vast, spanning large geographical areas, but also inherently accessible by the public, making them susceptible to unauthorized access and manipulation. The attack methodically targets this vulnerability, draining the battery of UEs that form the backbone of crucial infrastructure, such as the Advanced Metering Infrastructure (AMI) pivotal for utility companies.

The risk of battery depletion caused by a TPC Faking attack encompasses not only the immediate financial burden of widespread device maintenance and replacement but also the risk to the long-term ROI profile of infrastructures such as AMI (Automatic Metering Infrastructure).

AMI systems, integral to the modern utility infrastructure, rely heavily on cellular-connected smart meters for real-time data collection and management of utility services such as electricity, water, and gas. These meters are engineered for efficiency and longevity, minimizing the need for frequent physical maintenance.

However, the TPC Faking attack disrupts this balance. By compelling these devices to operate at unnecessarily high transmission power, the attack precipitates a rapid depletion of their battery life. This not only hampers the real-time operational capabilities of the AMI, leading to potential service disruptions and inaccurate billing but also poses significant logistical and financial challenges for the AMI vision.

The large-scale deployment of smart meters, designed with a 'set-and-forget' maintenance approach, becomes a critical vulnerability under the strain of the TPC Faking attack. Utility companies, which have invested heavily in the rollout of these smart meters across vast and often remote areas, find themselves facing the daunting task of replacing or servicing the compromised devices. This situation necessitates deploying costly workforce teams to physically access each affected meter, a process that is both time-consuming and financially burdensome. The logistical complexity of managing such widespread maintenance efforts can significantly disrupt the operational efficiency of utility services, leading to increased operational costs and potential delays in service provision.

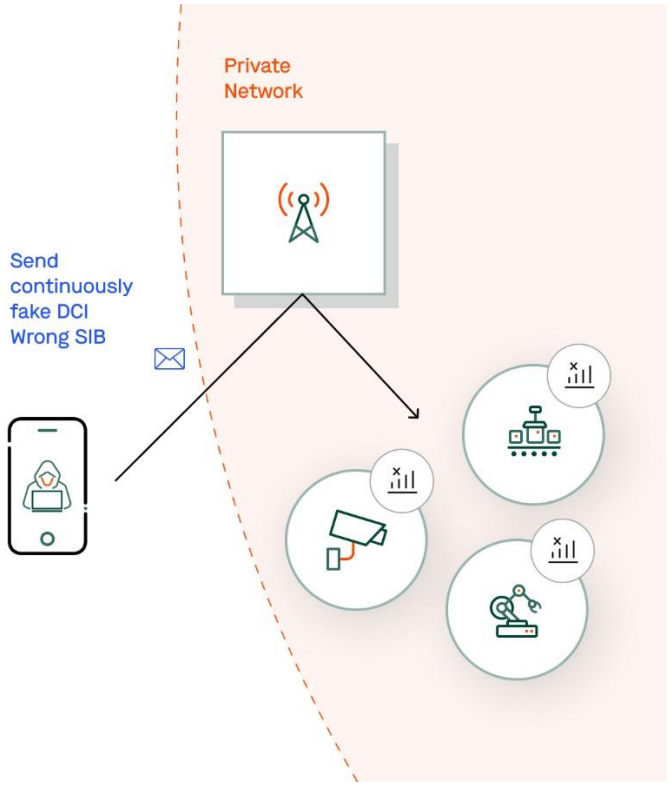
In comparing the impact of the TPC Faking attack on private versus public networks, it becomes evident that the stakes are significantly higher for private networks, particularly those operated by utility companies. While public network operators manage a broad spectrum of devices and prioritize core network integrity and average customer satisfaction, their direct responsibility for individual device battery life is highly limited if it exists at all.

However, private networks bear a much greater responsibility for the operational efficiency and longevity of connected UEs. The massive scale and critical nature of deployments like smart meters mean that any threat to device functionality, such as the rapid battery depletion caused by the TPC Faking attack, transcends a mere technical challenge to become a substantial business risk. This risk encompasses not only the immediate financial burden of widespread device maintenance and replacement but also the long-term ROI profile of those infrastructures.

Case study 3: Common Search Space Exhaustion

Introduction

The Common Search Space Exhaustion attack capitalizes on the cruciality of the SIBs for the network to work as expected. The attack targets the Physical Downlink Control Channel (PDCCH) to disrupt the communication of essential scheduling information to UEs. By inundating the PDCCH with spurious Downlink Control Information (DCI) messages, this attack hampers UEs' ability to receive vital System Information Blocks (SIBs), crucial for their operation within the network. This deliberate interference with network communication channels without the need to even be an authorized device in the network poses significant challenges to maintaining network reliability and security, especially in private networks where uninterrupted connectivity at the cell level is paramount.



Technical Overview

The Common Search Space Exhaustion attack is notably effective due to its simplicity and the minimal technical and RF resources required for its execution. This accessibility allows individuals with a fundamental grasp of LTE/5G network protocols to disrupt critical communications by flooding the PDCCH with false DCI messages. The narrow bandwidth utilized for DCI transmission compounds this issue, lowering the attack's barrier to entry and heightening its potential impact on private networks, where maintaining uninterrupted connectivity is crucial. This ease of execution underscores the urgency for network operators to address and mitigate such vulnerabilities.

The first strategy, termed "naïve DoS," is straightforward yet effective, involving the generation of intense interference at precise frequencies and timings aligned with the expected transmission of DCI messages. By synchronizing with the cell's DCI transmission schedule—a fundamental step for any UE to receive DCIs—the attacker strategically targets this critical, bandwidth-limited channel. This method exploits the inherent fragility of the cell, relying on the cell's over-dependency on the DCI narrow channel for proper function. It presents a tactically sound form of jamming that disrupts cell operation with minimal technical or RF resources, rendering it a formidable challenge to counteract.

However, the attacker could go for more sophisticated strategies. One of the more sophisticated approaches is the semi-naïve DoS. In this strategy the attacker is crafting false DCI messages, which is an enabler to manipulate UEs into thinking it’s a legitimate cell. These false messages, mirroring legitimate DCI formats but filled with bogus information, are timed perfectly for injection into the PDCCH, targeting the common search space. Utilizing software-defined radios (SDRs), the attacker then broadcasts these messages, causing disruption. Since Common Search Space is used to pass critical information such as the SIBs, fabricated DCIs might make the UEs desynchronize with the cell and easily disrupt the communication between the UEs and the cell. This strategy diverges from simple jamming by intricately generating DCI messages that replicate legitimate formats yet contain misleading information. Such a smart strategy allows the attacker to initiate the attack even more easily than the naïve approach that is based on high noise.

Building on the semi-naïve DoS approach, the "targeted DoS" strategy refines it even further, by focusing on specific critical devices. By targeting the Specific Search Space instead of the Common Search Space, this method is less detectable and offers a stealthier alternative to broad-scale attacks. Thus, the targeting DoS makes it extremely challenging for IT teams to conduct root cause analysis due to the subtlety of the interference, as well as the fact most devices aren't affected.
Targeting specific devices, especially critical ones, can lead to significant operational impacts without the widespread "noise" of larger attacks. This precision disrupts key operations while potentially eluding detection, as operational anomalies might be dismissed as non-RF-related issues if other devices within the cell range remain unaffected.

The "targeted DoS" strategy tweaks the semi-naïve DoS approach by selectively crafting false DCI messages for a specific C-RNTI or a designated group of C-RNTIs via the Specific Search Space. The basic assumption for this attack would be to be able to track the C-RNTI of the targeted UE or UEs. This precise targeting ensures that only the chosen UEs will descramble and be misled by these fabricated DCI messages, directly impacting their operation within the network. This method allows for a discreet form of attack, limiting disruption to specific, critical devices and complicating detection and diagnosis efforts by IT teams, as the broader network remains unaffected.

The targeted DoS attack is possible due to how the Specific Search Space works technically. The core idea of the attack is to exploit the relationship between the C-RNTI identities and the Specific Search Space. C-RNTIs are temporary identifiers of the UE, and it allows to specifically direct DCI message to singular UE to command the UE what to do. UEs employ a brute-force mechanism, attempting to descramble all the DCI messages in the Specific Search Space with their C-RNTIs. Successful descrambling indicates for a message that was intended for them to receive – driving them to act upon descrambled DCI. Without getting too much into details, it is important to

mention that the brute-force mechanism is built in a predictable way, which allowing the attacker to send the message at a specific timing where it most likely wins any race with the base station. In other words, not only could the attacker craft fabricate DCI messages – it can exploit the UE's search mechanism to get priority over the cell.

Within Private Networks Context

Reflecting on these strategies within the context of private networks truly emphasizes their critical importance in this new emerging market. Private networks, which often support essential operations in sectors like manufacturing or utilities, cannot afford the disruptions of their critical devices. The potential impact on operations such as factory workflows or Advanced Metering Infrastructure (AMI) in utilities highlights a heightened need and expectation regarding the security of the cell. Public networks might tolerate a single dysfunctional cell, as their business context and incentives are different from private networks. The stakes for private network operators, especially in utility or manufacturing settings, demand constant vigilance to always ensure network availability and reliability at the cell level. To better understand why and the risks for each sector, let us dive into each scenario.

In factories, the reduced number of cells heightens the importance of each, meaning an attack like Common Search Space Exhaustion can have a much more pronounced and wider-reaching impact.

Utilities' networks, operating within publicly accessible areas, are a unique study case. They tend to use RAN-sharing architecture with public operators or deploy their own cells in residual areas. In any case, their cells are universally accessible in public places. With that said, their operational imperatives are starkly different. The uninterrupted functionality of their devices is non-negotiable, contrasting with the more flexible service expectations of public network operators. This scenario creates a pronounced fragility, as attackers can easily exploit the public accessibility of these cells to initiate disruptions. Given the critical nature of the services provided by utilities, such attacks not only pose a risk of significant operational disruption but also present lucrative opportunities for attackers seeking financial or geopolitical gain. The simplicity of launching a Common Search Space Exhaustion attack, coupled with the substantial

potential impact, underscores a critical security weakness in utilities' IT strategies, necessitating robust defenses against such threats.

Factories offer a unique security perspective, deploying cellular networks within enclosed, guarded areas, thus potentially limiting access more than utility setups. Despite the protected deployment within factories, the range of cellular networks often extends beyond these secured areas, potentially reaching public spaces. Thus, while not as openly accessible as utility networks, there is still a possibility for cell signals to be accessible from outside the factory's confines.

The smaller scale of factory networks makes each cell fundamentally vital to operations, contrasting with utilities where disruptions tend to be more localized, and one cell's failure isn't typically catastrophic at the network level. In factories, however, the reduced number of cells heightens the importance of each, meaning an attack like Common Search Space Exhaustion can have a more pronounced and wider-reaching impact, challenging IT and security teams with significant disruptions that are far from localized, emphasizing the elevated criticality of each cell to the network's overall functionality. Given the strategic positioning of cells within factory networks, even a single cell's signal extending into public spaces can present a vulnerability ripe for exploitation. An attacker targeting this cell could significantly disrupt factory operations by leveraging its vital role within the network's infrastructure. This scenario underscores the potential for even small-scale attacks to have outsized impacts, challenging the factory's operational continuity and highlighting the critical nature of securing each cell against such vulnerabilities.

Implementing a targeted DoS strategy within a private factory network could not just disrupt the entire manufacturing process but might also prove extremely challenging to detect and mitigate. This kind of attack, focused on critical devices, could turn into a long-term issue, possibly taking months or even years to fully resolve, despite having a strong cybersecurity team in place. Of course, replacing the device would not be a proper solution in the long-term, as the new devices could be as well targeted by the

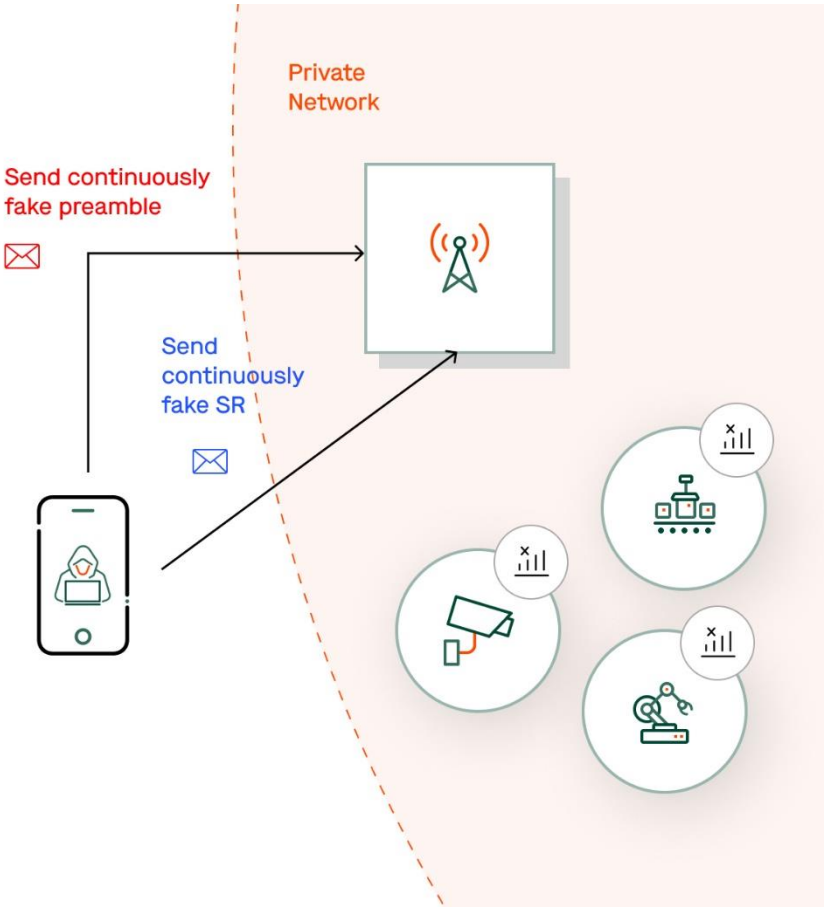
attacker whenever it chooses to, assuming the ability to keep the tracking of the device's C-RNTI, which is a basic assumption for the targeted DoS attack. Such a scenario is most likely the worst nightmare of the IT and security teams.

The extreme impact of this attack from the perspective of private networks, along with the relatively easy to initiate it, illustrates the outsized importance of this attack for private operators. Similarly to other attacks discussed in the white paper, while it might not be deemed a substantial business risk in the context of public networks, its implications for private networks are far more serious. The criticality of the devices served by the private network means each cell is a point of failure that must be protected.

Case study 4: Combined Uplink Attack

Introduction

The Combined Uplink Attack presents a sophisticated threat to LTE networks by exploiting two critical uplink processes: the Physical Random-Access Channel (PRACH) and the Scheduling Request (SR) mechanism on the Physical Uplink Control Channel (PUCCH). The Combined Uplink Attack uses two different attacks simultaneously to create a "perfect storm". Individually, PRACH Exhaustion and SR Blockage pose significant challenges; however, their combined exploitation results in the compounded effect which magnifies the impact, severely compromising network performance.



Technical Overview

The first attack is in the PRACH Exhaustion, which intricately exploits the LTE network's foundational process for managing initial communication requests of UEs to the cell. At the heart of this exploitation is the PRACH process, a critical channel designed for UEs to signal their intent to initiate communication, especially crucial for establishing uplink connections or when a device first seeks to connect to the network. The procedure commences with the UE selecting and sending a preamble—a short, predefined signal—on the PRACH, effectively notifying the cell of its request for network access. The transmission of this preamble, known as Message 1 (Msg1), marks the UE's first step in the random-access process, occurring at specified opportunities that align with the network's scheduling.

The vulnerability exploited by the PRACH Exhaustion attack lies in the deliberate and malicious flooding of the PRACH with an excessive volume of preamble transmissions meant to exhaust the allocated resources for receiving preambles. By doing so, the attacker significantly reduces the chance of UEs in the network to successfully initiate a radio connection with the cell. This strategic flooding aims to saturate the network's ability to process and respond to legitimate access requests, leading to delays or outright failures for genuine UEs attempting to establish communication. Even by itself, a PRACH Exhaustion attack may cause meaningful disruptions in the network’s efficiency and availability.

The second attack is the Scheduling Request (SR) Blockage, which focuses on the established connections' uplink data transmission process. This attack manipulates the mechanism through which User Equipment (UE) signals its need for uplink resources. In normal operations, when a UE has data ready to send but lacks the specific uplink resources to do so, it sends a Scheduling Request (SR) to the network's cell. This request is crucial—it's the UE's way of asking for bandwidth to transmit its data, and it's typically conveyed via the Physical Uplink Control Channel (PUCCH), a channel dedicated to carrying control information from the UE to the network.

The network, upon receiving an SR, allocates fixed uplink resources to the requesting UE, enabling it to transmit its data on the Physical Uplink Shared Channel (PUSCH). This

allocation process is meticulously managed to prevent collisions and ensure efficient resource distribution among all UEs requiring service. However, the SR Blockage attack disrupts this delicate balance by either flooding the network with fraudulent SRs or interfering with the signaling process itself. Attackers might generate a barrage of bogus SRs, effectively saturating the PUCCH with fake requests. Alternatively, they might disrupt the SR signaling pathway, making it difficult or impossible for legitimate SRs to reach the cell for processing.

The consequence of SR Blockage is immediate and disruptive: legitimate UEs find themselves unable to secure uplink resources. This impasse not only delays data transmission but, in severe cases, can prevent it altogether. The attack effectively silences legitimate UEs, rendering them unable to communicate their data needs to the network. This blockade on the PUCCH strains the network's resource allocation mechanisms and degrades the overall quality of service.

The Combined Uplink Attack leverages a synergistic approach by concurrently executing SR Blockage and PRACH Exhaustion strategies, thereby amplifying the disruptive impact beyond what each attack could achieve independently. Initially, the attack targets the Physical Uplink Control Channel (PUCCH) through SR Blockage, disrupting UEs' ability to request uplink resources. This obstruction forces UEs into a state where, unable to transmit data or secure necessary resources, they must revert to initiating the connection process again via the Physical Random-Access Channel (PRACH).

This redirection to the PRACH, induced by the initial SR Blockage, significantly increases the volume of allegedly legitimate access attempts on a channel already constrained by design to handle only a limited number of initiation requests. The sudden and abnormal spike in PRACH usage, driven by UEs attempting to re-establish their network connections, harmonized with the PRACH Exhaustion attack. The network cannot handle these simultaneous demands of both the victims of SR blockage and direct PRACH flooding generated by the attacker. struggles to allocate resources to the legitimate UEs,

the network's ability to set up radio connections is undermined. The compounded effect of this Combined Uplink Attack emerges into an extreme overload of network resources. This orchestrated approach highlights the vulnerability of LTE networks to attacks that exploit the interconnectedness of network protocols, revealing how coordinated disruptions can lead to exacerbated network failures.

Within Private Network Context

In the scenario of a small-scale factory network, characterized by its private LTE infrastructure serving a critical assembly of devices, the Combined Uplink Attack unveils a particularly daunting challenge. Such networks are designed to support the reliable operation of IIoT and OT devices integral to the factory's automation, manufacturing, and monitoring systems. These devices, crucial for the real-time oversight of production processes and safety protocols, rely on the unwavering reliability and timeliness of LTE-based communications to perform their functions effectively Indeed, the reliability and rapid communication offered by private LTE networks are key reasons manufacturers have shifted toward adopting them.

The strategic disruption caused by the Combined Uplink Attack undermines the factory's operational efficiency and poses significant safety risks.

When the factory's network falls victim to the Combined Uplink Attack, the repercussions are both immediate and severe. Initially, the SR Blockage component of the attack stifles the critical devices' attempts to communicate uplink data. This interference can lead to significant operational disruptions; for instance, sensors tasked with monitoring the condition of machinery might fail to transmit essential status updates, potentially leaving emerging issues undetected until they escalate into critical failures. As the attack progresses and its second phase, PRACH Exhaustion, begins to take effect, the situation worsens. The factory's devices, repeatedly attempting and failing to establish connections due to the overloaded PRACH, create a feedback loop of congestion. This intensifies the network's resource exhaustion, pushing it to a brink where maintaining any form of reliable communication becomes untenable.

Given the small scale of the factory's network, with a limited number of cells and possibly constrained by tighter resource allocations than larger, public networks, the compounded impact of the attack can swiftly lead to a near-complete operational shutdown. As each cell supports a high percentage of the network activity, and each device is critical for business continuity and safety – the individual cell emerges as a fragile single point of failure.

The strategic disruption caused by the Combined Uplink Attack not only undermines the operational efficiency of the factory but also poses significant safety risks. Critical alerts may be delayed, and automated safety mechanisms might fail to engage in time, increasing the risk of accidents and endangering both personnel and machinery. Beyond the immediate operational and safety concerns, the attack's impact on a small-scale factory network can have profound business implications. The loss of productivity, potential damage to equipment, and safety incidents can incur substantial financial costs, not to mention the possible long-term damage to the company's reputation and customer trust.

Similar to other attacks examined herein, the Combined Uplink Attack, though presenting a limited threat to public networks, could be catastrophic within the confines of private networks. The significance of each individual cell, coupled with the critical nature of every device connected to the network, fundamentally alters the perspective from which the potential impacts of these attacks must be assessed.

Conclusions

In this whitepaper, we've undertaken a thorough investigation into the critical vulnerabilities that plague LTE networks, with a particular emphasis on RF attacks and their profound impact on private cellular networks. Through a nuanced examination of LTE's architecture and its inherent security mechanisms, we've identified the network components most vulnerable to these attacks and delineated the specific vulnerabilities that RF attacks seek to exploit. Our comprehensive analysis spanned a spectrum of RF attacks, including both downlink and uplink strategies such as Common Search Space Blocking, MIB and SIB1 Blocking, TPC Faking, PRACH, and PUCCH Exhaustion, alongside the SPARROW and Combined Uplink Attacks. This exploration not only highlighted the intricate nature of these threats but also underscored the imperative for industry professionals to cultivate a deeper technical acumen. By delving into focused case studies, we've laid bare the real-world impacts these attacks can wield on private networks, spotlighting the paramount importance of implementing robust defenses against such vulnerabilities.

Moreover, our discussion illuminated the stark contrasts between public and private networks, particularly in terms of business necessities and the ensuing threat landscape. Public networks, given their scale and service obligations, face a distinct set of challenges and vulnerabilities compared to their private counterparts. This whitepaper has dissected these nuances, demonstrating the unique security needs private networks command due to their specific operational contexts. We've shown that RF attacks vary not only in their technical execution but also in their potential impacts, making certain attacks more pertinent to specific types of private networks. This variance underscores the necessity for a tailored approach to security, one that comprehensively addresses the particular vulnerabilities and business imperatives of private LTE networks. In conclusion, the evolving threat landscape demands vigilant, ongoing updates to security protocols and a sustained commitment to deepening our understanding of LTE vulnerabilities, ensuring the protection and resilience of network infrastructures against the sophisticated nature of RF attacks.