Security Assessment of Tetra Protocol

Samiksha Subodh Bedekar
Concordia University
Montreal, Canada

Aakanksha Nigudkar
Concordia University
Montreal, Canada

Subhra Rajesh Singh
Concordia University
Montreal, Canada

Nidhi Bose
Concordia University
Montreal, Canada

***Abstract*— This survey gives us a comprehensive security analysis of the TETRA (Terrestrial Trunked Radio), developed by the European Telecommunications Standards Institute (ETSI), which is extensively utilized by government agencies, police, emergency services, and military operators, as well as in critical infrastructure settings. The survey emphasizes the critical nature of authentication and safeguarding privacy, the cryptographic primitives handling authentication and encryption in TETRA have long been shielded from public overview, hindering independent duties of its claimed protection. The survey achieves objectives demonstrating the reverse engineering feasibility of unveiling the secret cryptographic primitives and providing an evaluation of their robustness within these specified protocols. The researchers have identified five significant security vulnerabilities in TETRA, out of which two of them are deemed to be critical and revealing vulnerabilities related to perfect forward secretiveness and the unlinkability of mobile radio subscribers. TETRA serves as a vital standard for professional users in different sectors. The lack of user unlinkability poses a threat, enabling adversaries to track user movement, especially in sensitive operations, other vulnerabilities included compromised message confidentiality and threats associated with group communications. The researchers propose an enhanced privacy-preserving protocol resistant to such attacks by suggesting firmware updates for mobile stations and end-to-end encryption. The TETRA protocol faces multiple challenges like key exposure, replay, and man-in-the-middle attacks necessitating further scrutiny and improvements. The papers in the survey also highlight future security enhancements to guarantee resilience against threats, emphasizing the ongoing need for research to strengthen TETRA security.**

Keywords—TETRA, Authentication, Radio, Encryption, Vulnerability.

I. INTRODUCTION

The Terrestrial Trunked Radio, also known as the TETRA protocol, represents a highly sophisticated and mission-critical digital mobile communication standard tailored to meet the requirements of professional users and organizations. Developed as a successor to traditional analog radio systems, TETRA has emerged as a robust, standardized solution, primarily used by public safety and emergency services like police, fire, and paramedics, as well as various other entities in the realm of transportation, utilities, and industrial sectors. TETRA's technology ensures the clarity and security of voice communication, rendering it superior to analog alternatives. Moreover, it encompasses a wealth of features designed to address the unique demands of professional users, including efficient utilization through time-division multiple access (TDMA), encryption mechanisms to protect communication from eavesdropping, support for group communication, emergency functionalities such as dedicated distress buttons, and the ability to transmit data alongside voice for information sharing. TETRA is known for its ability to support both point-to-point and point-to-multipoint communication, and it also incorporates digital data transmission, but at a relatively low data rate. The system consists of essential components such as TETRA base stations, Mobile stations (radios), a Core network, dispatchers, and management systems, all working in concert to create a dependable, secure, and efficient communication ecosystem. TETRA Mobile Stations (MS) operate in two modes: direct-mode operation (DMO) and trunked-mode operation (TMO). DMO enables communication in situations where network coverage is absent, and it offers the capability to relay messages through a sequence of TETRA terminals, known as DMO gateways or DMO repeaters. Primarily, TETRA places a strong emphasis on security, offering authentication for both terminals and infrastructure, along with air interface and end-to-end encryption to protect against eavesdropping.[9][10]

As a globally standardized protocol, TETRA offers interoperability and compatibility, ensuring seamless communication even among different manufacturers and systems. It also supports one-to-one communication, providing an extended range due to network utilization. TETRA terminals can function as mobile phones with direct connections to other TETRA users or the Public Switched Telephone Networks (PSTN). TETRA excels in several ways compared to other technologies. Its lower frequency provides an extended range and broad geographic coverage with fewer transmitters, reducing infrastructure costs. During voice calls, there's no interruption while moving between network sites, ensuring continuity of communication even in cases without a network. Furthermore, it supports point-to-point functions, which were traditionally absent in analog emergency services radio systems, offering a one-to-one trunked 'radio' link between sets without requiring control room intervention. Unlike cellular technologies, TETRA is versatile, enabling one-to-one, one-to-many, and many-to-many communication modes, all vital for public safety and professional users. TETRA's security features and rapid deployment solutions for disaster relief further enhance its appeal, making it a vital component of mission-critical communication networks. It plays a pivotal role in guaranteeing the timely and secure exchange of information for both routine operations and emergency responses and continues to evolve to address emerging challenges and incorporate new features, thus remaining a cornerstone for professional users who rely on secure and efficient communication for their vital functions.[9][11]

II. BACKGROUND

A. *Need for TETRA Security*

As TETRA security is a crucial aspect of the Private/Professional Mobile Radio (PMR) market, the need for its security arises from the fact that suppose a malicious attacker manages to monitor police radio frequencies and this unsecured communication system can compromise the safety of law enforcement personnel and the success of their confidential operations. We need security solely to address these concerns by providing a range of security mechanisms that will ensure confidentiality, integrity, and availability of communication.

The fundamental security service in TETRA is strong authentication, which basically means that a secret is shared between a terminal and the network's Authentication Centre (AuC). This authentication is both explicit and implicit, and this will help ensure that only authorized users can access the system. In addition to authentication, TETRA security focuses on the encryption of air-interface traffic, which ensures that eavesdroppers cannot intercept and decipher the communication. TETRA security also demands the need for anonymity, which is particularly important for specialist users who often carry highly secure and classified communications. Anonymity is supported in the standard TETRA security mechanisms, which ensure that all authentication is done between the base station and the network and not directly between the network and the user.

Another important aspect is the need for enhanced confidentiality. Specialist users often require a higher level of confidentiality and TETRA security addresses this need by providing end-to-end encryption. This encryption ensures that the communication between two TETRA base stations is encrypted, even if it passes through the network.

In conclusion, security in the TETRA protocol is a fundamental requirement and is essential to safeguard communications, protect sensitive data, and ensure the effective operation of public safety and emergency services.[4]

B. *Architecture of Tetraburst Protocol*

The TETRA network structure comprises of multiple system components and interfaces. Its primary focus is on Switching and Management Infrastructure (SwMI) within the TETRA system. It does not standardize the internal interface of TETRA networks and it is upon the manufacturers to customize it. This gives the manufacturers the freedom to customize the internal network interface to optimize the internal network according to their needs.

The SwMI system components are linked through six specified interfaces, essential for ensuring compatibility, interconnection, and network management among the various system elements and networks. It consists of six major components like –

Individual TETRA network – This is a standalone TETRA network system, consisting of a local switching center, mobile switching center (MSC), base transceiver station (BTS), gateways, switches, operations, and management center (OMC), and the associated control and management facilities.

Mobile Station (MS) - The Mobile Station (MS) can be broken down into the mobile termination unit (MTU) and the related terminal equipment (TE). TETRA mobile devices can be classified based on their portability into two categories, hand-portable (or simply portable) and vehicle-mounted mobile (or simply mobile). Mobile stations are categorized into 4 classes based on attributes like power class and their capability. Regardless of their rated transmit power, they need to be capable of modifying their transmission power in accordance with the network's power control directives. The 4 classes are as follows -

- Vehicle mounted mobiles - Class 1: 30 watts, Class 2: 10 watts
- Hand-portable mobiles - Class 3: 3 watts, Class 4: 1 watt

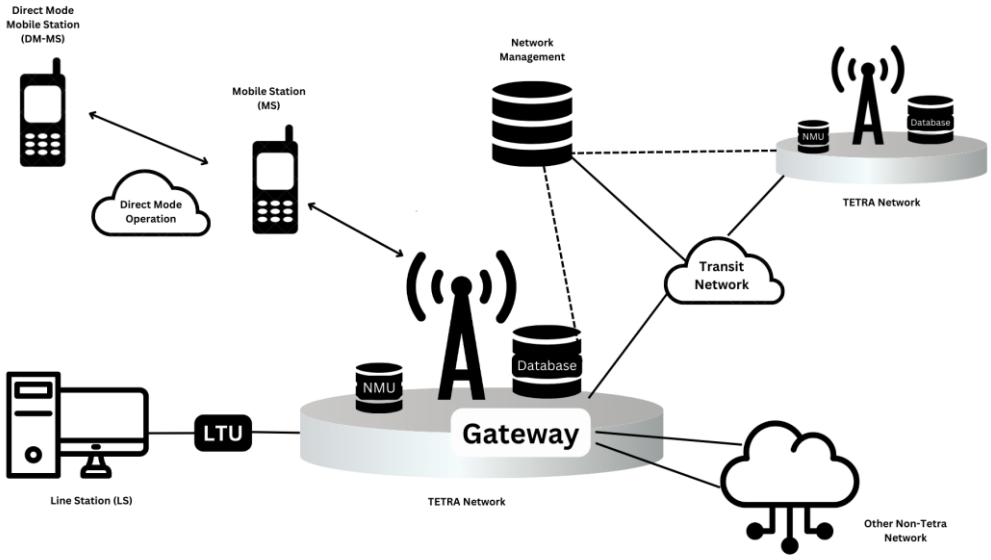

Fig. 1: Architecture of TETRA

There are three receiver classes based on their operating environments:

- Class A is designed for effective performance in urban settings and regions featuring hilly or mountainous terrain.
- Class B is tailored for optimal operation in urban and densely populated areas.
- Class E is intended to fulfill the stricter demands of quasi-synchronous systems.

Line Station (LS) - The line station (LS) consists of the line termination unit (LTU) and the related terminal equipment (TE). This configuration is commonly found in a control room console in a control room console terminal or dispatcher unit that connects to a TETRA SwMI via an ISDN network. The main difference between a mobile station (MS) and a line station (LS) is the transmission medium where the mobile termination unit (MTU) handles it for MS and the line termination unit handles it for LS.

Direct Mode Mobile Station (DM-MS) - This includes mobile devices that establish direct communication with one another without relying on the infrastructure, operating in a trunked mode. A mobile device configured for Direct Mode Operation (DMO) facilitates point-to-point or point-to-multipoint communication by utilizing the Direct Mode (DM) air interface. The TETRA standard outlines several options for expanding the fundamental mode of operation:

- Direct Mode Repeater MS: This extends the communication range beyond two DMO mobile devices.
- Dual Mode Switchable MS: This supports both TETRA DMO and trunked TETRA V+D (Voice + Data), enabling dual-watch mode.
- Direct Mode Gateway: This serves as a link between TETRA DMO and TETRA V+D modes.

The above options are utilized for different operating possibilities. These models are-

Direct Mode Mobile Station (DM-MS) - This enables two mobile devices to communicate directly using the DM air interface. This communication occurs in a "walkie-talkie" style, with the initiating DM-MS providing air interface synchronization and taking on the role of the master DM-MS.

- Dual Watch Mobile Station (DW-MS) - This is an extension of the DM-MS, capable of operating in both DMO and trunked V+D modes. A DW-MS can communicate with DM-MS or TETRA SwMI while simultaneously monitoring V+D or DM channels. During idle periods, a DW-MS can monitor both V+D and DM channels.
- Direct Mode Repeater (DM-REP) - It receives information from one DMO mobile station and retransmits it to another DMO mobile station.
- Direct Mode Gateway - This model serves as the connection between TETRA DMO and TETRA V+D modes. A DM-GATE bridges the protocol differences between DM and trunked V+D air interfaces.
- Direct Mode Repeater/Gateway - This model is a combination of repeater and gateway functionality. It can be achieved with a vehicle-based DM repeater and additional gateway capabilities for establishing a link to a TETRA V+D network.

Gateway - This facilitates the calls between the TETRA network and networks outside of the TETRA system like a public switched telephone network (PSTN). There is a need for a gateway because the external networks connected to the TETRA network employ information formats and communication protocols that are incompatible, necessitating some form of translation or conversion.

Network Management Unit - This unit offers local and remote network management capabilities, which are common in TETRA systems. They typically cover system management tasks related to fault monitoring, configuration, accounting, performance assessment, and planning. The TETRA network management specifications primarily focus on establishing a standard management interface and outlining general requirements for ensuring interoperability between various systems. The actual implementation of these management functions is the responsibility of network operators and equipment manufacturers.

TETRA utilizes a method of partitioning the radio spectrum into multiple channels that are then shared among multiple users. This is called trunking, and it allows people to talk to each other on the same radio without getting in each other's way. The channels used in TETRA range from voice channels to data channels and control channels, with voice channels providing voice communication and data channels providing data communication, while control channels are used to control and manage the system. The TETRA protocol offers a variety of additional features and services, including Group Calling, Emergency Calling, and Location-Based Services. Group Calling enables multiple users to communicate simultaneously, while Emergency Calling enables users to call a central control room in an emergency. Location-based Services enable users to locate their location through GPS or other location technologies. All in all, TETRA Protocol is intended to provide secure and dependable communication services to professional users who require top-notch communication services.[6]

III. CRYPTOGRAPHY OF TETRA

TETRA uses air as a medium of communication. The air interface is the RF (Radio Frequency) link between the MS and the BS. To provide confidentiality, the TETRA air interface is encrypted using one of the TETRA Encryption Algorithm (TEA) ciphers. Encryption provides confidentiality (protection against eavesdropping) as well as protection from signaling.

The encryption algorithms used in TETRA are TEA1 (TETRA encryption algorithm 1), TEA2 (TETRA encryption algorithm 2), TEA3 (TETRA encryption algorithm 3) and TEA4 (TETRA encryption algorithm 4).

- TEA1: TEA1 is a symmetric encryption algorithm (128-bit key) used in the early TETRA system. It is intended for commercial use and restricted export. It is the default and mandatory encryption algorithm for TETRA Encryption mode 1(E1). In E1, all voice and data traffic are encrypted using TEA1, and users cannot disable encryption. TEA1 is a proprietary encryption algorithm, and the details of its operation are typically not publicly disclosed to enhance security. While TEA1 provides a reasonable level of security, it is considered less secure than the subsequent TEA versions.
- TEA2: TEA2 is an enhanced version of the encryption algorithm designed to provide a higher level of security compared to TEA1 and it is used in national emergency services within Europe. It uses a 256-bit key for encryption. TEA2 is typically employed in TETRA Encryption Mode 2 (E2). In E2, encryption is optional, and users or user groups can choose whether to enable encryption or not.
- TEA3: TEA3 is another version of the TETRA encryption algorithm, introduced to provide even stronger security. It is used in Extra European Emergency Services. TEA3 uses a 256-bit key for encryption, like TEA2, but may have improved security features. TEA3 is also used in Encryption Mode 2 (E2), making encryption optional for users.
- TEA4: TEA4 represents the latest version of the TETRA encryption algorithm, developed to further enhance security. It is used in Commercial use and restricted exports as that of TEA1. Like TEA2 and TEA3, TEA4 uses a 256-bit key for encryption. As with the other TEA versions, TEA4 is typically used in Encryption Mode 2 (E2), where encryption remains optional.

The choice of which TEA version to use (TEA1, TEA2, TEA3, or TEA4) depends on network operators' security requirements and the specific regulations in place in each jurisdiction. While TEA1 may still be used in some legacy TETRA systems, there is a trend towards adopting stronger encryption methods like TEA2, TEA3, or TEA4 to ensure a higher level of security for TETRA communication, especially in critical applications like public safety and emergency services.

TETRA allows for two modes of air interface encryption.

- Encryption Mode 1 (E1): In this mode, encryption is mandatory, meaning that all voice and data traffic is encrypted using TEA1. Users have no option to disable encryption, ensuring a basic level of security.
- Encryption Mode 2 (E2): In this mode, encryption is optional which means users can choose to enable or disable it. If the user disables encryption mode E2, then voice and data traffic will be sent on clear. If encryption mode E2 is enabled, then voice and data traffic is encrypted using TEA2 which provides enhanced security compared to TEA1.

Encryption keys are used to encrypt and decrypt voice and data transmissions, ensuring that unauthorized parties cannot eavesdrop on or tamper with the content of messages. The Key Management Facility (KMF) is the centralized entity responsible for generating, distributing, and managing encryption keys. Encryption keys involved in TETRA communication are:

- Traffic Encryption Keys (TEKs): TEKs are used for encrypting voice and data traffic over the air interface. Each individual or group of TETRA users has their own unique TEK. These keys are periodically rotated or changed to enhance security.
- Key Encryption Keys (KEKs): KEKs are used to encrypt the TEKs themselves. This adds an extra layer of security. If an attacker needs to crack TEKs they would still need the KEKs to decrypt them. KEKs are typically stored securely within the TETRA devices.
- Network Management Keys (NMKs): NMKs are used for secure communication between the TETRA devices and the Key Management Facility (KMF). They ensure the confidentiality of key management processes and key exchange.

TETRA uses authentication to ensure that only authorized users can access the network and participate in secure communications. Users must have valid authentication keys (usually stored in their radios) to establish a connection with the TETRA network.

TETRA also uses a technique called frequency hopping to further enhance security. Frequency hopping involves changing the frequency of the radio signal rapidly and randomly during transmission. This makes it difficult for an attacker to intercept and decode the signal, as they would need to know the exact frequency at each moment in time.

In addition to encryption, and frequency hopping, TETRA also supports access control. Access Control Mechanism is used to ensure that users only have access to the resources they are authorized to use while restricting others. These combined security measures make TETRA a robust choice for organizations that require secure and reliable communication systems, especially in critical situations where the confidentiality and integrity of data are paramount. [3][16]

A. Attacks on TETRA

a) CVE-2022-24401: A security vulnerability or an attack scenario concerning the TETRA (Terrestrial Trunked Radio) communication system, particularly with respect to keystream reuse in encrypted traffic when utilizing the TEA (Tiny Encryption Algorithm) keystream generator.

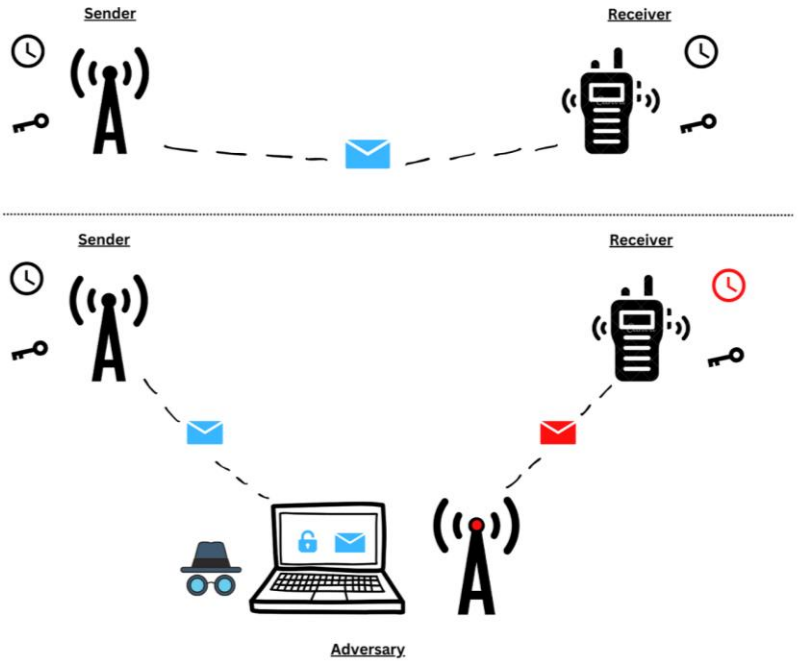

Fig 2: CVE-2022-24401 Attack

The vulnerability appears to be derived from the manner in which IVs are generated and maintained, which can be leveraged by an active actor to induce keystream reuse and decrypt encrypted traffic. System administrators and security professionals must be cognizant of security vulnerabilities such as this one to mitigate them, as they can have a detrimental effect on the security and confidentiality of encrypted communications within systems such as TETRA.

This attack scenario serves as a reminder of the need for reliable key management and intravenous (IV) generation within encryption systems. It is essential to generate IVs in a manner that prevents the formation of predictable patterns and the reuse of IVs across multiple messages or frames. Furthermore, robust authentication and integrity verification systems can help to protect against such attacks. Security researchers and organizations often work to identify and mitigate these types of threats to enhance the security of communication systems.

Figure 2, this attack works by spoofing unauthenticated frame number update messages which function to synchronize network time, in this manner, an attacker can recover keystreams corresponding to a specific moment in time t by collecting encrypted traffic of interest. An attacker can then attack any radio system with the shared keys at a later point in time to recover the key stream and decrypt the earlier collected traffic. An attacker can recover voice communication and inject data.

There are two main headers: the MAC header, which is transmitted in cleartext, and the LLC header which encodes the properties of the link layer. The MAC header is responsible for transmitting essential information such as the recipient's SSI, the encryption of the message, and the length of the message. The fill bits flag allows for flexibility in the length of messages, indicating whether they are padded. The LLC header, however, contains a variety of information, including the link layer type, the FCS (Frame Check Sequence) for error control, if the message requires confirmation, and if it contains a confirmation of a previous message. Additional information may be added to the LLC header depending on the type of the LLC PDU.

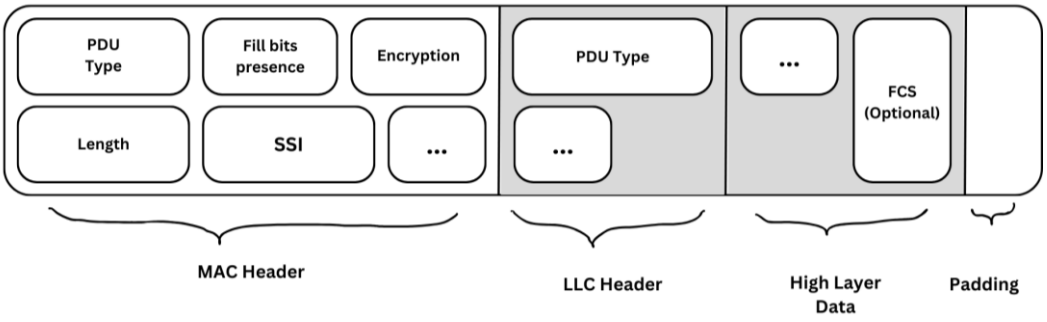

Fig. 3: Data Format for downlink air interface messages

The frame check sequence (FCS) is an element used for error detection in the protocol. If a valid FCS exists, it is verified and removed prior to the message being passed to higher-level protocol handler functions. The presence or absence of an FCS has the equivalent effect for these higher-level functions. The information also distinguishes between two link types, Basic Link and Advanced Link. For Advanced Link, the FCS is required, while for Basic Link it is optional. However, in the context of the information provided, the services that use the Basic Link are the primary focus, making the distinctions between the two link types less important. In summary, this information provides insight into the technical complexities of formatting and transmitting data over the air interface in a communication system context, highlighting the importance of headers such as MAC and LLC, and the FCS's role in ensuring data integrity.

Recovering uplink keystream

An attacker aims to decrypt an encrypted message (c) that was sent at a specific timestamp (t) using cryptographic keys that have not been updated. The attacker's approach involves impersonating a network entity (SwMI) and tricking a mobile station (MS) into reusing the Initialization Vector (IV) employed at the original time (t). This is achieved by sending synchronization (SYNC) and system information (SYSINFO) frames with timestamps set just before time t. When the MS, under the influence of the attacker, subsequently transmits a message (c') at the spoofed time (t), it is encrypted using the same keystream as the original target message (m). Therefore, any knowledge gained about the contents of c' directly translates into knowledge about m. This implies that if the attacker can determine the content and characteristics of c', they can infer the content of m. One critical aspect is the potential for high confidence in identifying parts or all of c' based on its length and its alignment within the observed communication stream. In many cases, the length and positioning of c' may be characteristic of certain types of communication, enabling the attacker to establish significant information about m.

This underscores the importance of robust security measures in communication systems to protect against impersonation attacks and the reuse of cryptographic parameters, such as IVs. It also emphasizes the significance of encryption and authentication mechanisms to thwart such adversarial attempts to gain access to confidential messages. In practice, to mitigate this type of vulnerability, implementing strong authentication, secure key management, and cryptographic protocols that prevent IV reuse is crucial for ensuring the confidentiality and integrity of communications.

Recovering downlink keystream

This method outlines information for recovering the downlink keystream in a communication system, despite the challenge posed by the SwMI's perception of time being beyond the attacker's control. Downlink keystream recovery is typically less straightforward than uplink recovery, but this approach demonstrates its feasibility by sending ciphertexts to the mobile station (MS) and observing its behavior in response.

The objective is to expand the knowledge of a known keystream (ks) at a specific time (t) by constructing a message (m) at the Logical Link Control (LLC) layer with the same bit length as ks plus one bit. This concept is referred to as "keystream expansion." The constructed message (m) is of type BL-DATA with FCS as its Protocol Data Unit (PDU) type, indicating the presence of the FCS checksum and requiring acknowledgment upon correct reception. The actual contents of m are irrelevant and are filled with zeroes. Additionally, m concludes with the FCS checksum computed over its contents.

To create the expanded keystream (ks'), a zero bit is appended to the known keystream (ks), resulting in ks' = ks ∦ 0. The encrypted message (c) is then generated as c = m ⊕ ks'. The process continues by sending spoofed synchronization (sync) and system information (sysinfo) frames, setting the MS's timestamp to slightly precede t, and transmitting message c exactly at time t. Depending on whether the FCS is correct, and, by extension, whether the newly added zero bit in ks' is the correct keystream bit, the MS will either emit an acknowledgment or silently discard the message. In either case, the attacker learns a keystream bit. This procedure is repeated continuously until the entire downlink keystream at time t is eventually learned. This method highlights the potential vulnerabilities in communication systems and the importance of strong encryption, authentication, and integrity mechanisms to protect against keystream recovery attacks. It also emphasizes the need for robust security measures to mitigate the risks associated with the exploitation of communication protocol behaviors.[2]

b) CVE-2022-24402: This is a major security issue with regard to the TEA1 Keystream Generator. It appears that the key register initialization function of the generator reduces the length of the key to only 32 bits, which significantly weakens the system's security. This is due to the fact that modern cryptographic attacks can be quickly brute-forced with current computing power. Therefore, it is recommended to use keys that are longer and more complex, ideally closer to the full length of 80 bits. Furthermore, key management practices such as secure key generation and storage should be adhered to reduce the risk of a key compromise. The overall conclusion is that the implementation of a truncated key in TEA1’s keystream generator poses a risk to the system’s ability to withstand cryptographic attacks and indicates a need for a more robust key management strategy to address potential security vulnerabilities.

Recovering full keys

This is a fundamental security vulnerability in the TETRA encrypted system, particularly when it comes to the handling of encryption keys. This vulnerability is due to the compression of the extended key (EGK) into a 32-bit length,

which not only reduces the length of the key but also presents a number of serious security risks. This compression function assigns a reduced EGC to each channel within the network, each of which has its own EGC. The two main consequences of this vulnerability are that a reduced EGC on a particular channel allows for encryption and decoding operations only within that channel. More importantly, if an attacker can access the entire 80-bit EGC (DCK, SCK, CCCK, or MGCK), they are able to gain complete control over the network's communications, allowing for unauthorized decryption, interception, and even the forging of communications.

The complexity of the attack is further exacerbated by the fact that it is relatively simple. The compression function has specific properties that allow an attacker to generate a large number of candidate keys efficiently. The attack complexity is 2^48, which is indicative of the vulnerability's severity. To be successful in the attack, the attacker must be able to distinguish between correct key guesses and incorrect ones. The attack approach involves recovering three different reduced ECCs from different cell or carrier frequencies. The network information transmitted to the compression function is different for each of these. The attacker then iterates over the potential pre-image of the first reduced ECC. The inverse of TB5 is then applied and the resulting key is verified to generate the other two reduced ECCs after applying TB5 again with varying network information parameters. Finally, the attacker is able to determine the entire 80-bit key. This information highlights a fundamental vulnerability within TETRA's encryption system, wherein a decrease in the bit length of the Encryption Key (ECK) can result in a network-wide breach of security if the attacker is able to recover the entire key. To mitigate this risk, it is necessary to reevaluate TETRA's key compression function, as well as the general key management procedures within the system, in order to protect the security and confidentiality of network communications. Implementing more robust encryption protocols and key management procedures are necessary to effectively mitigate this risk.[2]

c) CVE-2022-24404: The lack of cryptographic integrity check in air-interface encrypted TETRA traffic poses a major and concerning security risk. Securing data is as important as its confidentiality in secure communication systems, and a cryptographic integrity check (MAC or checksum) is essential for the recipient to be able to verify that the data has not been altered during transmission. Without such a mechanism in the encryption strategy of TETRA, the data is vulnerable to potential attacks that could compromise its integrity, potentially leading to far-reaching repercussions. Stream ciphers are a form of encryption that works by combining a keystream with plaintext to create a ciphertext. While stream ciphers provide a means of safeguarding data, they do not provide a means of verifying its accuracy after decryption. This is especially problematic when an active adversary is able to intercept and manipulate the encrypted ciphertext. A malicious actor with the ability to intercept and alter data in transit can take advantage of this vulnerability to alter the encryption code bit by bit. By manipulating individual bits of the encryption code, they can manipulate the decoded plaintext and potentially corrupt it, misinterpret it, or even inject malicious content into it. In other words, they can alter the intended communication and cause confusion, disinformation, or even use the compromised data for malicious purposes.

Furthermore, the absence of cryptographic integrity controls not only compromises data integrity but also data confidentiality. By manipulating the encryption code and observing the corresponding alterations in the decoded data, an attacker may gain insight into the contents or patterns of encrypted information that should remain confidential.

To effectively address this critical problem, it is essential to implement a reliable cryptographic integrity check within TETRA. This check is intended to identify any unauthorized changes or attempts to tamper with data while it is being transmitted. Generally, this can be achieved through the use of HMACs or encrypted encryption modes that combine encryption with integrity checks. These techniques can help to guarantee the integrity of data and quickly identify and reject any attempts to tamper. Maintaining the security of communications systems is a continuous process. Regular changes and revisions of encryption algorithms, protocol specifications, and key management procedures are necessary to address known weaknesses and potential threats, thus safeguarding the system in the long term. To sum up, the lack of cryptographic integrity checks in encrypted traffic within TETRA airspace poses a significant risk to data integrity, as it allows active adversaries to tamper with data. Effective integrity checks are essential to prevent unauthorized modifications and protect the integrity and confidentiality of communications and should be implemented as a best practice to enhance the security of all communication systems, particularly in cases where the integrity of data is of utmost importance.

The recommendation to Implement End-to-End Encryption (E2E) is an effective means of mitigating the security and privacy risks associated with the transmission of data in communication systems. E2E encrypts data on the sender's end and only decrypts it on the recipient's end. This means that, even if an attacker were to intercept the data while it is in transit, they would not be able to decrypt its contents without the corresponding decryption key. As a result, the encryption of the communication would protect its confidentiality and integrity, making it difficult for adversaries to manipulate or intercept the data. In addition to E2E, Operational Security (OPSEC) compensating controls (OPSEC) are beneficial for reinforcing overall security. By conducting a comprehensive risk assessment, organizations are able to tailor their OPSEC practices to the specific threats and vulnerabilities they are facing. This allows for the identification of weaknesses in the security posture and the development of tailored measures to address those vulnerabilities. It is essential to bear in mind that, while encryption is highly effective in safeguarding data in transit, it may not be sufficient to address all security issues. OPSEC measures can complement encryption by addressing additional aspects of security, including physical access control, staff training, and security incident response.

In conclusion, the recommended mitigation is to use encryption to protect against data interception and manipulation, however, it should be incorporated into a comprehensive security strategy, which includes operational security practices that are tailored to risks and vulnerabilities. Such a layered approach to security enables organizations to address a wider range of security issues and maintain a strong defense against threats.[2]

d) CVE-2022-24403: The security implications of using a cryptographic scheme to conceal radio identities are of utmost importance. Cryptographic schemes are a fundamental element of modern communication networks and are designed to protect user privacy and anonymity. However, if the cryptographic scheme is weak in design, it can open the door to attacks that could de-anonymize and monitor users, thus compromising user privacy and security. The vulnerability of the cryptographic scheme means that it does not provide the necessary security measures to protect user identities. This leads to the risk of de-anonymization, in which the identity of anonymous users is revealed. Attackers can take advantage of the inadequacies of the cryptographic scheme to reverse the encryption process, thus revealing the identity of the user. This is not only a violation of user privacy but also exposes individuals to the risk of intrusive surveillance, harassment, or other forms of surveillance.

The use of de-anonymization to monitor and track users can have serious repercussions for individuals' security and privacy. This allows adversaries to track and monitor users' activities, which can be used for malicious purposes or to violate personal liberties. In short, a weak cryptographic system can undermine the fundamental principles of privacy and security in a communication system. To reduce this risk, it is essential to strengthen the cryptographic scheme used to mask radio identities. This may involve adopting more powerful encryption algorithms, refining key management procedures, and conducting thorough security audits and evaluations to identify and address vulnerabilities. Another important factor in addressing this issue is raising user awareness. Educating users on potential risks, the importance of privacy safeguards, and the value of unique passwords can help to strengthen their own security in the system. To sum up, the existence of a low-level cryptographic scheme in the obfuscation of radio identities constitutes a serious risk to the privacy and security of users and the communication system. The design of the cryptographic scheme, the implementation of stringent security protocols, and the awareness of users are all necessary steps to mitigate this vulnerability and ensure the continued safeguarding of user identity and privacy within the communication system.

In order to address the vulnerability of the cryptographic scheme used to obfuscate radio identities, the recommended mitigation measure is a long-term transition to TAA2. Moving to TAA2 is likely to involve the implementation of more secure encryption algorithms, better key management procedures, and improved security mechanisms. To minimize disruption to the communication system and improve its security, it is important to plan and execute the migration process carefully. Additionally, compensating controls should be implemented in the interim to ensure a strong security posture. A comprehensive risk assessment should be conducted to assess the risks related to subscriber identity management. By adapting OPSEC measures to specific vulnerabilities and threats, organizations can maintain a strong security posture and improve their communication system security.

The overall conclusion is that the combination of long-term migration to TAA2 and compensating controls via OPSEC adjustments provides a comprehensive approach to enhancing security and privacy in the communication system. This approach addresses both short-term security threats and long-term enhancements, providing a strong defense against attacks that could de-legitimize and monitor users. This approach is in line with best practices in the information security domain, where a layered approach is typically the most effective means of mitigating risks and maintaining a high level of protection.[2]

e) CVE-2022-24400: The authentication algorithm flaw, which allows malicious actors to set the DCK to 0, is a critical security issue in a communication system. Although the immediate consequences may be minor, the potential consequences are not to be disregarded. This vulnerability presents a risk of authenticity loss and partial confidentiality loss in communications and is therefore a matter of serious concern. This vulnerability highlights the importance of unpredictability in the authentication process, such as the ability of the attacker to selectively select values for parameters such as RS and predict RS RAND2. By strategically selecting values for RS RAND1 and RS RAND2 and using XOR operations the attacker can make RS DCK become an ALL-ZERO key. This vulnerability should be addressed, and authentication security measures enhanced to ensure the integrity and confidential nature of communication within the system. Additionally, it points to potential issues with random number generation in radios which can affect the security of the entire system. The attack allows the attacker to authenticate a session with the Mobile Station using an All-Zero DCK but does not allow the attacker to decrypt the real communication between the Mobile Station and the legitimate SWMI.

The low-severity nature of this flaw does not detract from its significance. However, it is important to note that even a low-level vulnerability can be exploited by malicious actors, which in this case could include malicious actors with the intention of disrupting or compromising communications. The DCK is a key component of the authentication process that is intended to verify the identity of users and the security of their communications. In order to address this vulnerability and reduce the risks associated with it, a multi-pronged approach should be adopted. The primary priority should be to update radio firmware as soon as a fix is issued. Firmware updates typically include patches and security improvements to address known vulnerabilities. Staying up-to-date with firmware updates can help protect an organization's communication systems from being exploited by adversaries. Adopting End-To-End Encryption (E2E) is also an effective mitigation measure. E2E encrypts data on

the sender's end and decodes it on the recipient's end, making it almost impossible for an attacker to eavesdrop or manipulate the data while it is in transit. This extra layer of security significantly increases the confidentiality and integrity of data, thus reducing the impact of the flaw.

For the long term, it is recommended to migrate to TAA2, as TAA2 is likely to be a more secure and resilient protocol that addresses the authentication algorithm's vulnerabilities. Although this may not be the immediate solution, it should be a priority to plan for the migration. It is possible to employ compensating controls to reduce the risk. For example, by disabling radios with an unacceptable firmware update schedule, only devices with current security measures can be allowed to function. This can help to isolate vulnerable radios, thus preventing them from introducing potential security threats into the system. To address the authentication algorithm flaw that enables attackers to reset the DCK value to zero, a comprehensive strategy is necessary. This includes updating radio firmware as soon as possible, implementing End-to-End encryption, and potentially transitioning to Taa2 in the long term. Additionally, compensating measures such as the disabling of radios with insufficient firmware updates can be employed to further protect the communication system. Although the vulnerability is classified as low, it is important to be proactive and comprehensive in order to protect authenticity and confidentiality.[2]

IV. Vulnerability Analysis

In the context of the reuse of keystreams, TETRA relies on the initialization vector (IV) to generate unique keystreams for encryption. These IVs cycle every 23 days. However, the vulnerability becomes apparent when malicious actors can tamper with the synchronization of these parameters between mobile stations (MS) and the Switching and Management Infrastructure (SwMI). Attackers can exploit this vulnerability in two primary ways. First, by impersonating the SwMI and manipulating synchronization frames, they can deceive an MS into reusing a specific IV, enabling the recovery of keystreams for uplink message decryption. Second, while recovering downlink keystreams is more challenging due to time synchronization dependencies, attackers can gradually regain the entire downlink keystream by manipulating ciphertexts and observing the MS's responses. Group communication isn't immune to this threat either, as attackers can adapt the same approach with some adjustments. Practical experiments validated this vulnerability, and mitigations include updating mobile station firmware to implement frame counter sanity checks. However, the effectiveness of these patches depends on their widespread adoption, making the network vulnerable until all devices are updated or replaced. Alternatively, deploying end-to-end encryption or other secure communication methods can bolster security in TETRA communications. In essence, this vulnerability jeopardizes the integrity of encryption keystreams in the TETRA system, potentially compromising message confidentiality and overall security. Countermeasures involve firmware updates and the consideration of alternative encryption methods to safeguard communications effectively. [2]

The TEA1 stream cipher, a fundamental component of TETRA networks, faces a notable vulnerability due to its key compression mechanism. It initially compresses an 80-bit encryption key down to a 32-bit key register, significantly reducing its security. This flaw paves the way for a man-in-the-middle attack that not only permits full decryption of captured traffic but also enables the encryption of counterfeit messages. It also makes it possible to recover the complete 80-bit key, exploiting the weaknesses in key compression, which could potentially facilitate the creation of forged sealed messages. Experimental results demonstrate the efficiency of these attacks, particularly when leveraging GPUs. To mitigate these risks, a transition to the more secure TEA2 is recommended. However, such a migration might prove challenging in certain scenarios, as it necessitates device replacement or firmware updates and lacks a secure transition period. [2]

The TA61 algorithm used for identity encryption also possesses some vulnerabilities by not fully supporting the HURDLE block cipher. This can be also exploited through an MITM attack that allows the attacker to recover the secret by obtaining 3 pairs of SSI and ESI. This will help the adversary to impersonate as the TETRA MS and thereby jeopardizing the encryption of the user identities. To address this issue, suggested mitigations include modifying TA61 by increasing the size of the secret and the encryption procedure.[2]

The Session Key Pinning vulnerability discussed in the above section, pertains to the derivation of a session key, DCK, through challenge/response mechanisms. The vulnerability arises when predictable values for RAND2 are employed, leading to an all-zero DCK, effectively allowing an authentication bypass. The security of DCK relies on the unpredictability of RAND2, a critical factor inadequately emphasized in TETRA specifications. Radios with subpar random number generation may be susceptible to this type of attack. To address this issue, potential mitigations include revising the authentication handshake to eliminate the vulnerability or enforcing measures to prevent the use of predictable RAND2 values. Fortunately, these mitigations can be implemented while maintaining protocol compliance.

The TEA3 S-box vulnerability concerns the behavior of TEA3, a cipher used in non-EU countries. An analysis of TEA3's S-box reveals that it doesn't conform to the standard S-box design practices, with specific indices mapping to the same value, and a particular value not appearing. To improve its security and align it with TEA1 and TEA2, it's suggested to change one entry in the S-box. This deviation from the standard S-box design practices raises concerns about the overall security of TEA3. Due to compatibility issues, it is recommended to refrain from using TEA3 until a more comprehensive security assessment is conducted, ensuring its safety in practical applications.[2]

The security analysis of the TETRA protocol reveals several more vulnerabilities that organizations and agencies should

consider while implementing this standard. Some are discussed as follows:

Lack of message integrity: The integrity of the messages exchanged in the TETRA protocol can be manipulated by violating the key agreement of the protocol. This vulnerability can be exploited to launch key agreement and availability attacks. If an attacker is successful in such an attack, they can gain access to sensitive information and compromise user privacy.[5]

Impersonation or Clone terminal attack: In cases where, if the secret key of the TETRA authentication protocol is revealed to an adversary, they can impersonate as an authorized user or infrastructure. This can lead to unauthorized access to sensitive information and compromise user privacy. *"While the TETRA authentication protocol is able to block cloned terminals that have cloned a terminal identifier called Individual Short Subscriber Identity (ISSI), it is currently unable to prevent the illegal use of cloned terminals that have cloned both ISSI and the authentication key"* [1]. This vulnerability will allow the attacker to gain access to the network and thereby provide the ability to eavesdrop on communication.[1]

Lack of perfect forward secrecy / Key exposure: Another critical vulnerability the protocol additionally lacks to prevent is perfect forward secrecy, meaning that if in the process the secret key is obtained by the adversary, then they will be able to decrypt all past and future communications. This is because the session key is derived from the secret key and a random number (RAND1) exchanged during the authentication process. If an attacker obtains the secret key, they can use it to derive the session key and decrypt all previous and future communications. The lack of perfect forward secrecy is a serious vulnerability because it means that the compromise of the secret key can lead to the compromise of all past and future communications. This can be particularly problematic in situations where sensitive information is being transmitted, such as in military or law enforcement operations. On the other hand, the protocol also uses a shared secret key between the terminal and the authentication center to authenticate the terminal. This key is generated, distributed, and injected into the terminal and the authentication center during the authentication process. The key distribution process involves transferring the key from the key generator to the authentication center. This process can be vulnerable to attacks that expose the authentication key. For example, if the key file storage medium is misplaced during the delivery process, the authentication key can be exposed to attackers. Similarly, if the key file storage medium is not properly secured during the delivery process, attackers can intercept and steal the key. If the authentication key is exposed, attackers can use it to clone legitimate terminals and gain unauthorized access to the network.[5]

Replay attacks: As we know, the protocol uses a challenge-response mechanism to authenticate the terminal or the Mobile station (MS). The authentication center sends a random challenge to the MS, and the MS responds with a response value that is calculated using the authentication key and the challenge. If the response value matches the expected value, the MS is authenticated and granted access to the network. In a replay attack, an attacker intercepts a legitimate authentication message and replays it to gain unauthorized access to the network. The attacker does not need to know the authentication key to launch a replay attack. Instead, the attacker simply intercepts the authentication message and replays it to the authentication center. If the authentication center accepts the replayed message, the attacker gains unauthorized access to the network.[1]

Man-in-the-middle: The TETRA is vulnerable to Man-in-the-middle (MITM) attacks in which, the attacker intercepts the authentication messages and modifies them to gain unauthorized access to the network. The attacker can modify the challenge or response values to bypass the authentication process and gain access to the network. For example, the attacker can intercept the challenge sent by the authentication center to the TETRA MS and modify it to a different value. The TETRA MS will then calculate the response value using the modified challenge and send it back to the authentication center. The authentication center will accept this modified response value and eventually grant the attacker access to the network.[1]

Lack of Anonymity: The TETRA protocol fails to provide anonymity to its users in some cases. The lack of anonymity can be particularly problematic in situations where sensitive information is being transmitted, such as in military or law enforcement operations.[5]

V. Future Scope

The need for continued research and analysis into the security of terrestrial trunked radio (TETRA) communications systems is important. While significant security issues have been identified, the passage emphasizes that there is still a great deal of potential for further research and analysis. The main areas of focus are the evaluation of current TETRA encryption solutions, such as those used to mitigate known vulnerabilities, as well as a more in-depth analysis of the more unusual cipher structures, such as TEA3 and TEA4.

Additionally, it is important to consider upcoming security enhancements that promise to withstand cryptanalysis in the future, as these enhancements will likely be treated as confidential, thus necessitating a higher level of examination to guarantee their robustness and security, especially in cases where sensitive communications may be involved. In conclusion, the passage emphasizes the need for ongoing research in order to strengthen the security of the TETRA systems and ensure their resilience to the ever-evolving threat landscape.

VI. Conclusion

In summary, the Tetra protocol security evaluation has been a thorough investigation into the resilience and weaknesses of this important communication standard. We have learned a great deal about the protocol's advantages and disadvantages by carefully examining its architecture, cryptographic techniques, attacks, and vulnerabilities. The

assessment of potential threats, including denial-of-service attacks, man-in-the-middle attacks, replay attacks, spoofing, and eavesdropping has given rise to a more sophisticated knowledge of the security posture.

Our findings draw attention to both the positive parts of the Tetra protocol, such as its encryption algorithms and safe key management, and the areas that still need improvement, including its vulnerability to specific kinds of attacks and possible locations of exploitation. The discourse surrounding the detected vulnerabilities emphasizes the significance of ongoing enhancement and adjustment considering changing security measures.

REFERENCES

[1] Yong-Seok Park, Choon-Soo Kim, and Jae-Cheol Ryou, "The Vulnerability Analysis and Improvement of the TETRA Authentication Protocol," in *The 12th International Conference on Advanced Communication Technology (ICACT)*, Phoenix Park, 2010.

[2] Carlo Meijer, Wouter Bokslag, and Jos Wetzels, "All cops are broadcasting: {TETRA} under scrutiny," in *32nd USENIX Security Symposium (USENIX Security 23*, Anaheim, CA, USENIX Association, 2023, pp. 7463--7479.

[3] Leif Nilsen, "Development of Cryptographic Standards for Telecommunications," in *TELEKTRONIKK*, Oslo, Telenor, pp. 13-20.

[4] D. W. Parkinson, "TETRA Security," *BT Technology*, pp. 81-88, 2001.

[5] Zahednejad, Behnam & Azizi, Mahdi & Student, "An Improved Privacy Preserving TETRA Authentication Protocol Seyyed Morteza Pournaghi," 2020.

[6] John Dunlop, "TETRA System Architecture, Components and Services," in *Digital Mobile Communications and the Tetra System*, 2013, pp. 161-204.

[7] B. Zahednejad, M. Azizi and M. Pournaghi, "A Novel and Efficient Privacy Preserving TETRA Authentication Protocol," *14th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)*, pp. 125-132, 2017.

[8] H. P. Riess, "Cryptographic security for the new trans-European trunked radio (TETRA) standard," *IEEE Colloquium on Security and Cryptography Applications to Radio Systems*, pp. 3/1-3/5, 1994.

[9] "Terrestrial Trunked Radio," [Online]. Available: https://en.wikipedia.org/wiki/Terrestrial_Trunked_Radio.

[10] "TETRA," [Online]. Available: https://www.etsi.org/technologies/tetra.

[11] "TETRA:BURST," [Online]. Available: https://www.tetraburst.com/.

[12] Tsay, "Security Analysis of the Terrestrial Trunked Radio (TETRA) Authentication Protocol," 2013.

[13] (NCSC-NL), "CVE-2022-24400 Detail," 2023. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2022-24400.

[14] Attacks, "Vulnerabilities," 2023. [Online]. Available: https://news.ycombinator.com/item?id=36848157.

[15] F. V. Labs, "New TETRA: BURST Vulnerabilities Enable Attackers to Intercept and Inject Critical Radio Traffic – How to Mitigate Risk," 2023. [Online]. Available: https://www.forescout.com/blog/new-tetraburst-vulnerabilities-how-to-mitigate-risk/.

[16] TETRA Encryption Algorithm. (2023). Retrieved from Crypto Museum: https://www.cryptomuseum.com/crypto/algo/tea/#:~:text=The%20TEA%20algorithms%20are%20used,authentication%2C%20key%20derivation%20and%20OTAR