SECURITY ASSESSMENT OF THE TETRA PROTOCOL

Oghenerukevwe Oyinloye
Institute of Information Systems and Engineering
Concordia University
Quebec,Canada
oghenerukevwe.oyinloye@mail.concordia.ca

Adithya Ananth
Institute of Information Systems and Engineering
Concordia University)
Quebec,Canada
adithya.ananth@mail.concordia.ca

Azeez Ogede
Institute of Information Systems and Engineering
Concordia University
Quebec, Canada
azeez.ogede@mail.concordia.ca

Seth Ekow Abaidoo
Institute of Information Systems and Engineering
Concordia University
Quebec, Canada
s_abai@live.concordia.ca

Divine Anyalamechi
Institute of Information Systems and Engineering
Concordia University
Quebec, Canada
d_anyale@live.concordia.ca

Vaishnavi Naikwade
Institute of Information Systems and Engineering
Concordia University
Quebec, Canada
vaishnavi.naikwade@mail.concordia.ca

***Abstract*—**

The Tetra protocol, integral to millions of deployed devices globally is assessed for its security and risk impact. In this study we investigated security of the tetra protocol thorough analysis and risk assessment focusing on its encryption algorithms, vulnerabilities, its impact on devices, data, network traffic, level of cryptanalysis, ease of exploitation, level of ease to discover the vulnerabilities, its scability impact on companies and countries. Despite the necessity for cryptographic protocols to be open for scrutiny, the replacement of insecure encryption algorithms with proprietary ones raises concerns about potential vulnerabilities. Through the evaluation of the Tetra protocol, multiple vulnerabilities are identified, including flaws in authentication procedures, weaknesses in air interface encryption, exploitable backdoors in encryption algorithms, and cryptographic scheme design flaws leading to user deanonymization. These vulnerabilities pose significant risks such as unauthorized access, data manipulation, deanonymization, and malleability attacks. In this report we presented attack surfaces that may ensue from the vulnerabilities and recommended mitigation strategies to address these threats. We concluded by highlighting potential vulnerabilities within the Tetra protocol given the secret of the encryption algorithm update after the recently discovered vulnerabilities.

Keywords*—*Tetra, protocol, security, assessment, encryption, architecture, vulnerabilities

1. INTRODUCTION

The development of the TETRA standard began in the early 1990s. It was driven by the need for a modern digital private mobile radio (PMR) system that could replace the aging analog systems used by emergency services and other professional users (such as police, fire, search and rescue and ambulance). The standard was designed to operate at the frequencies of 380-430 MHz, 450-470 MHz, and 800 MHz bands ensuring interoperability between different manufacturers' equipment [6]. It uses time-division multiple access (TDMA) with four 'slots' on a single carrier, with 25 kHz carrier spacing, to provide secure voice and data by the addition of optional encryption [1,2,3,4,5,7]. Between 2000 and 2010 tetra protocol evolved to provide enhanced data service (TEDs) and video transmission [1]
The TETRA protocol provides services, which include Direct Mode Operation (DMO) which allows direct communication between two or more radio terminals without the need for a base station or network infrastructure and the Trunked Mode Operation (TMO): this variant uses a centralized control channel to manage and allocate resources among multiple users, enabling efficient communication in a network.
Packet Data Service (PDS) that enables the transmission of data packets over the TETRA network, allowing for applications such as email, file transfer, and web browsing [8,9]

Tetra Protocol provides Security and Encryption using Various encryption and security mechanisms, which are available within the TETRA protocol to ensure secure communication and protect against unauthorized access [6].

Its' services are further divided into bearer services which provide information transfer between network interfaces using low layer functions and teleservices using complete capability system for communicating including terminal functions. [10], the main bearer services include [3,4,5,10]: - short Data Service (SDS): This allows for the transmission of short data messages between terminals and the network, like SMS in cellular networks; user status transmission used to transfer short, predefined messages; circuit switched data services in unprotected or protected mode and packet switched data services. [10]; teleservices include [9,11]- individual call, group call, broadcast call, acknowledged group call and DMO.

TETRA defines three security classes: Class 1—no encryption, Class 2—static cipher key encryption, and Class 3—dynamic cipher key encryption (with individual, common, or group cipher keys(GCK)), The GCK is not used directly. Rather, it is used as input to algorithm TA71 [5] together with the SCK (class 2) or

CCK (class 3) to generate the Modified Group Cipher Key (MGCK). In case the GCK for a group is not defined, the SCK or CCK is used instead. Cipher Key (CCK). Group conversations are supported through talk groups. Each talk group may optionally have a Group Cipher Key associated with it.. Over The Air Re-keying (OTAR) functionality, albeit largely out of scope, allows for new key material to be provided through the network Authentication in Classes 1 and 2 is optional but is required in Class [2,9].

II. ARCHITECTURE OF THE TETRA PROTOCOL NETWORK

Fig. 1 show the architecture of the tetra protocol network; a mobile station (which comprises the subscriber's physical equipment, a subscriber identity module (SIM) and a Tetra equipment identity (TEI) specified by the operator on each device) communicates with the line station over ISDN and the switching & management infrastructure as well as the network management unit that manages both local and remote functionalities. Tetra system has interfaces: radio air interface (l1), line station interface (l2), Inter-system interface (l3) which allows interconnection of Tetra networks from different manufacturers., Terminal equipment interface for a mobile station (l4), terminal equipment interface for a line station(l4'), network management interface (l5) and direct mode interface(l6).

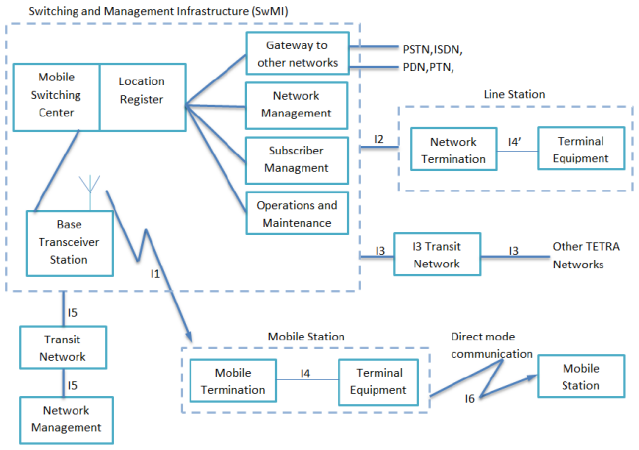

Fig. 1: Tetra network [9]

(a) TETRA CRYPTOGRAHIC PRIMITIVES

TETRA authentication and encryption are handled by secret, proprietary cryptographic primitives. Authentication, key derivation and distribution is implemented in the TETRA standard Authentication Algorithm set 1 (TAA1). A combination of stream ciphers and a family of block cipher designed for application with limited resources called tiny encryption algorithms (TEA) is used for achieving the protocol. [2] All TAxx are based on HURDLE* cipher, which is a 16-round Feistel cipher with 64-bit blocks and 128-bit key. All TBx based on XOR / addition and some blocks identical / related such as TA11 & TA41, TA12 &TA22 and TA11 &21 (which was reversed engineered). The TEA suite consists of four stream ciphers with 80-bit keys, providing mutual authentication between network elements and terminals, and the ability to securely manage keys and identities, end – to – end encryption and air interface encryption.

The shared key between the MS and BS can be generate) Authentication as shown in Fig. 2 from [8 cited in 9] (1) Authentication Code (AC), which is a pin code entered by the user, using the TB1 algorithm (2) UAK stored in the SIM card with the algorithm TB2 (3) Using both AC and UAK to generate K is the third method labeled TB3. The length of K, KS and KS' are all 128 bits. K will not be used directly in the authentication process but to generate session keys: KS and KS'.

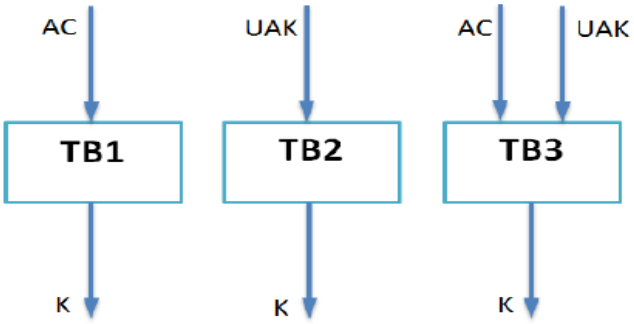

Fig.2: K generation [9]

(b) AUTHENTICATION PROCEDURE

[8,9] In TETRA, authentication services include the infrastructure may include authentication center and base station authentication of MS by Switching & Management Center (SwMI). Authentication of SwMI by MS and the mutual authentication is only done when the first one-way authentication is successful between them, which is usually initiated by the MS, as Illustrated in Fig. 3a &b.

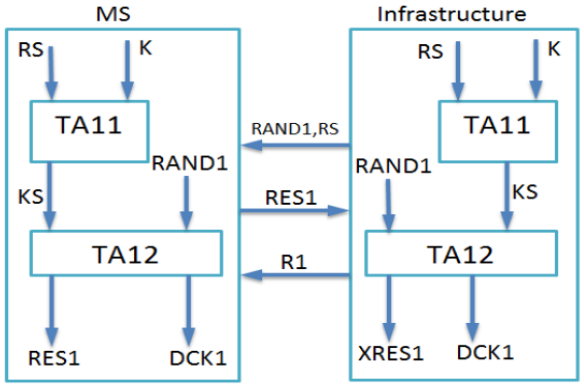

Fig.3a: Authentication procedure between infrastructure and MS [9]

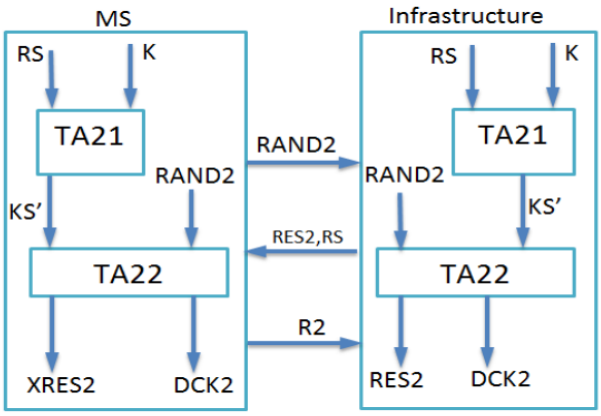

Fig.3b: Authentication procedure between MS and Infrastructure [9]

A 80-bit is a random seed (RS) used together with the authentication key K to generate a session key KS. The algorithm used is TA11 and performed by the home center. 80-bit random number RAND1 is generated by the infrastructure and sent to the MS as a challenge. The MS will compute its response, RES1 of 32-bits using the session key KS and the algorithm TA12, there by generating a derived cipher key (DCK1) which is a part of the (DCK). The infrastructure compares the RES1 and the response XRES1 (32-bits) as shown in Fig. 5 and authenticates if equal else does not [thesis]. The mobile station also does the same authentication procedure with the infrastructure but using the algorithms TA21 and TA22 respectively, so that the session keys will be different from the earlier session keys sent by the mobile station to the infrastructure, which in turn generates the other part of the derived cipher key DCK2.
The Tetra authentication process adds protocol information to the header as it goes through different protocol layers as shown in Fig. 4, which is used to initiate an authentication,

PDU Type	Authentication sub-type	Random Challenge (RAND1)	Random Seed (RS)	Proprietary element
4 bits	2 bits	80 bits	80 bits	...

Fig. 4: D-Authentication Demand [9]

PDU Type	Authentication sub-type	Response Value (RES1)	MAF	Random Challenge (RAND2)	Proprietary element
4 bits	2 bits	32 bits	1 bit	80 bits	...

Fig.5: U-Authentication Response [9]

So that a mutual authentication in tetra protocol involves three parties as shown in the algorithm 1 and Fig. 6 and the algorithm 1[9]: the authentication center (AuC), the mobile station (MS) and the base station (BS). A summarized message exchange between the parties in a mutual authentication is:
Algorithm1:
1. MS -AuC: UserID
2. AuC -BS: RS, KS, KS'
3. BS -MS: RAND1, RS
4. MS - BS: RES1, RAND2
5. BS-MS: RES2, R1
6. MS- BS: R2

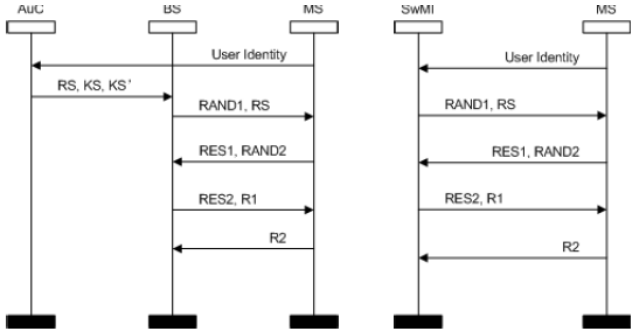

Fig.6: Protocol [9]

The security requirement for the authentication is given [9]:
1.For both roles, the long term shared symmetric key between MS and SwMI should not be revealed to an adversary (2) the session keys KS and KS' should not be revealed to an adversary (3) the derived cipher key (DCK) should not be revealed to an adversary (4) for both roles the claim of aliveness should hold (5) the MS and the SwMI should agree on all the value of variables exchanged (6) for both roles the requirement of non-injective synchronization should be satisfied.

III. REVIEW OF LITERATURE

(a) PLATFORMS USING TETRA PROTOCOL

TETRA (Terrestrial Trunked Radio) is widely used in various industries and sectors where reliable and secure communication is crucial. The TETRA protocol has been deployed in several sectors; it is extensively used by police forces, fire departments, and emergency medical services (EMS) for mission-critical communication, in transportation sectors such as railways, airports, and ports for operational communications, ensuring coordination between staff for smooth operations and emergency response, many utility companies, including electricity, gas, and water. Tetra helps in managing field operations, maintenance tasks, and responding to emergencies efficiently, utilized in the oil and gas industry for communication between field workers, operators, and control centers, ensuring safety and coordination in remote and hazardous environments, implemented in manufacturing plants, industrial sites, and construction projects for workforce communication, safety coordination, and managing logistical operations [12,13]
Another area where Tetra protocol is deployed is the devices, such as Handheld Radios: designed for rugged use in demanding environments. These devices often feature functionalities like GPS, voice recording, and emergency alerts; Mobile Radios: TETRA mobile radios are installed in vehicles such as police cars, ambulances, and utility trucks.

They provide seamless communication for mobile teams and integrate with other vehicle systems; base stations which are the backbone of the communication infrastructure, providing coverage and network connectivity. They are deployed strategically to ensure reliable communication across wide geographical areas; Infrastructure Equipment: these includes repeaters, antennas, dispatch consoles, and network management systems essential for operating and maintaining TETRA communication networks. Airbus, Motorola

Solutions, Hytera, Sepura and Rohill are major manufacturers of devices that use the tetra protocol [12,13]

(b) RELATED WORKS

Recent research has unveiled vulnerabilities, and possible attack surfaces for the tetra protocol and network; [14,15] described how location privacy may be broken, by localization employing antenna arrays and direction finding techniques on the physical layer on an unencrypted DMO, given the possibility to estimate the angle-of-arrival (AoA) of radio waves between the mobile station(MS) and base station(BS) transmissions, while transitioning from analogue to digital communication and maintaining of signaling by MB to BS even if they are not used actively. Their claim is based on the implementation of a localization attack of TETRA equipment based on AoA estimation of TETRA signals, a TETRA fuzzing framework for unencrypted DMO transmissions, and a demonstration of vulnerabilities that cause MS devices to crash, reboot or mute. Using their fuzzing framework, they replayed recorded physical layer signals and generated signals from upper layer TETRA bursts, implementing a straightforward jamming-based Denial of Service (DoS) by replaying a simple synchronization burst 2 times per second. During the jamming attack, both MSes were neither able to start voice calls nor to send text messages and were temporarily muted.

[d] reported to have verified TETRA authentication protocol using the Scyther analysis tool. They showed that the integrity of the exchanged messages can be manipulated to violate the key agreement of the protocol. Also, showed how two key agreements and availability attacks impact the protocol. They proposed to use message authentication code on the exchanged messages to avoid such attacks. They noted that these vulnerabilities do not really threaten the TETRA network since entities check the equality of their keys before the beginning of communications.

[1,16,17] an analysis using ProVerif and Scyther analysis tools in various aspects such as authentication, anonymity, forward secrecy etc. showed a Lack of perfect forward secrecy that allows an attacker to discover the previous session keys given the long-term key k. it also suffices for the attacker to get the transmitted RS in a previous session. Using algorithm TEA1, s/he can compute session key KS by having the long-term key k and the intercepted RS [1] However, the authors believe that this vulnerability cannot be fixed unless public key encryption which is hard to deploy is used. They further showed an attack against TETRA that TETRA authentication protocol lacks perfect un-link ability property required by mobile radio subscribers outside the network. Lack of user un-link ability lets the attacker track the physical movement of users which is highly undesirable, especially in military operations seen in the authentication protocol between the mobile terminals and authentication server (SwMI) [1]. Despite the use of temporary identities ATSI to avoid the linkability of TETRA subscribers, the execution of the authentication protocol paves the way for the attackers to trace TETRA subscribers, as an active attacker can intercept the authentication triplet (Rs, RAND1, RES1) sent and received by the SwMI respectively to the victim mobile station MSv. The intercepted authentication challenge (RS,RAND1) is sent later by the attacker to a number of MSs to find the original MSv. Due to the fact that the output of TA12 depends on (RAND1,K,RS) the attacker is able to distinguish any mobile station from the one the authentication challenge was originally sent to (MSv). Upon reception of the replayed (RS, RAND1) the victim mobile station, MSv will give the same RES1 as the one given before, while other MSs give different values for RES1 due to the different pre-shared keys they have. The implementation of few false base stations would then allow an attacker to trace the movements of a victim mobile station, resulting in a breach of the subscriber untraceability [1]

[1] proposed not sending challenges RAND1, RS explicitly, instead, they should be computed secretly by both parties using a Random Generating Function (RGF) seeded from the common pre-shared key k i.e. (RS, Rand1, Rand2) =RGF(k) for the first session. For the next sessions the RGF produces the new challenges (Rs', Rand1', Rand2') seeded from the previous challenges namely Rand1, Rand2 i.e. (Rs', Rand1', Rand2') = RGF (Rand1, Rand2). (RAND2 is used for the authentication of SwMI by MS). As before SwMI computes XRES1 by itself using algorithm TA21 to compare it with received RES1. Upon the equality of the two terms, the MS is authenticated and SwMI sends R1 (True) to MS. The same scenario holds for the mutual authentication of MS and SwMI. In this case, challenges such as RAND1, RAND2, RS are not transmitted in the protocol.

While this approach seems better, we believe that using a shared random generating function does not handle the issue of session key replay attack, which was the first problem in the first instance provided in the review of [1].

[14] reported TETRA's vulnerability to reactive jamming by design, because the protocol is designed to have long synchronization periods and the sender's identity is transmitted. [18] Intelligent Intentional Electromagnetic Interference (IEMI) was used to test the resilience of Terrestrial-Trunked Radio (TETRA) against intelligent intentional electromagnetic interference (IEMI) with low amplitude, preventing mobile stations from initiating communications with the many base stations thus disrupting the network without detection. This specifically targets the modulation scheme based on $\pi/4$ Differential Quadrature Phase Shift Keying (QPSK) and the susceptibility to interference from both continuous wave signals and QPSK-modulated signals. The authors note that when TETRA systems are faced with intelligent jamming via the manipulation of time-slotted ALOHA protocol and access assignment channel (AACH) by corrupting each block in AACH an attacker can force mobile stations to wait indefinitely for the AACH to be decoded with an IEMI signal of 10 dBm lower than the intended signal, a large Error Vector Magnitude (EVM) can still be created.

IV. RECENTLY ESTABLISHED AND ANALYSIS OF TETRA VULNERAB ILITIES

In this section we discuss vulnerabilities and analysis that have been established based on research on the CVE-2022-24400 - 22404[2]:

To carry out their research they investigated firmware and categorized them as those with presumably encryption, high

entropy data section used to embed the Tetra protocol cryptographic primitive, noting that in all cases where such a high-entropy section is absent, the device itself and its SoC are produced by the same manufacturer, suggesting that the algorithm may be implemented in hardware in the SoC.
[2] reported the following vulnerabilities of the tetra protocol haven broken the TEA1 cryptographic algorithms as described in table 1

Table I Recent tetra protocol break-out [2]

CVE	Vulnerability	Impact	Severity/Actor
CVE-2022-24400	A flaw in the TETRA authentication procedure allows a MITM adversary that can predict the MS challenge RAND2 to set session key DCK to zero	Loss of authenticity / partial loss of confidentiality	Low/Active
CVE-2022-24401	The Air Interface Encryption (AIE) keystream generator relies on the network time, which is publicly broadcast in an unauthenticated manner. This allows for decryption oracle attacks.	Loss of confidentiality / authenticity	Critical / Active
CVE-2022-24402	The TEA1 algorithm has a backdoor that reduces the original 80-bit key to a key size which is trivially brute-forceable on consumer hardware in minutes.	Loss of confidentiality / authenticity	Critical Passive / Active
CVE-2022-24403	The cryptographic scheme used to obfuscate radio identities has a weak design that allows attackers to deanonymize and track users.	User deanonymization	High/Passive
CVE-2022-24404	Lack of ciphertext authentication on AIE allows for malleability attacks.	loss of authenticity	High/Active

The key initialization function, in tetra whose key length is reduced from 80-bit key into 32-bit while returning the challenge response can be exploited by attackers, by communication interception and possible data Injection.
A major problem leading from the improper implementation of the stream cipher; without the randomization of the initialization vector (IV) and the use of some properties of the frame such as current time and sequence number to generate the Initialization vector [3,19].

Another area described is the possibility of sequence replay attack, where an attacker can replay a previous sequence number and the system resets to such a previous session, something the system shouldn't be doing, hence forcing the system to reset to that initialization vector (because the system assumes something went wrong), this return to a previous session can be exploited allowing an attacker review information/carry out other malicious act because of the re-use of the IV [1,2].
Another issue is the actual implementation of the cryptographic algorithm which are hand crafted crypto and not public for scrutiny as the weak key system would have been pointed out if it were publicly scrutinized [3,19].

The key TEA1 which uses 80bits but selects 32bits from the 80bits in actual implementation allows the protocol to be vulnerable to brute-force with only 2^ 32bits attempts.

[2] The method of truncating the key from 80bits to 32bits was done to allow for reconstruction of the original 80bits, which is a bad practice following the principle of one-way trap door expected of such high used protocol. [7] also mentioned a small x-box whose activities are yet to be determined (a backdoor) been problem itself as it can be exploited by either the provider or an attacker for malicious activities. Depending on infrastructure and device configurations, these vulnerabilities allow for real time decryption, harvest-now-decrypt-later attacks, message injection, user deanonymization, or session key pinning.

V. OUR SECURITY ANALYSIS AND RISKS ASSESSMENT OF TETRA PROTOCOL

In this section we discuss our analysis and risk assessment in two main parts: the analysis of the algorithm and the impact of the vulnerabilities [2].
One thing that is known about crypto is that it must be open for scrutiny, but replacing the unsecure encryption algorithm with another set of propriety algorithms goes again to show that there are likely vulnerabilities with the new set of encryption algorithms tetra protocol developers has introduced to overcome the challenges of the just discovered vulnerable protocol and the fear of such discovery. Evaluating tetra protocol as presented in [9].
Algorithm1[9]:
1. MS -AuC: UserID
2. AuC -BS: RS, KS, KS'
3. BS -MS: RAND1, RS
4. MS - BS: RES1, RAND2
5. BS-MS: RES2, R1
6. MS- BS: R2

From algorithm 1, we see that the tetra protocol does not apply any seen encryption to protect the exchange of RES1, RAND2, RES2, R2, R1 between the MS and BS leaving the possibility of reflection attack, if an attacker can pose as the MS.

CVE-2022-24400: A flaw in the TETRA authentication procedure allows a MITM adversary that can predict the MS challenge RAND2 to set session key DCK to zero

This vulnerability allows an attacker to replay a previous session on a device, potentially gaining unauthorized access or manipulating data stored on the device. Additionally, the attacker could manipulate data transmitted over the network from these devices, leading to potential data breaches or unauthorized access to sensitive information. Bypassing any authorization checks present in the system. Attackers can look at places where user specific data is retrieved (e.g. search screens) and determine whether the key for the item being looked up is controllable externally. The system with this flaw will be vulnerable to modification attacks, eavesdropping attacks, MITM attacks, usurpation attacks. This vulnerability is very easy to exploit. Access control checks for specific user data or functionality can be bypassed. Horizontal escalation of privilege is possible (one user can view/modify information of another user). Due to the unencrypted nature of messages sent at the point of authentication sent between MS and infrastructure, this derived key could be easily set to 0 for not updated devices. And replicated on all devices in that network if a botnet is used to propagate the takeover. Since cryptographic primitives are not publicly available it will take a long period of time to evaluate the security vulnerability even with powerful machines, but with the presence of a not patched device on a network, and an attacker is able to get into the network, making weakness of this algorithm will be discoverable. The threat will be continuous reproducible if the authentication procedure on tetra protocol between the MS and BS remain unencrypted and the ATSI is not revised to ensure unlinkability. This threat will still exist in companies if the only option to handle the flaw is the replacement of the affected devices, most companies will not want to replace these devices due to the cost of such replacement of infrastructure, leaving the threat management to the users/client. Most clients will also not want a change in the cost of service and will prefer the availability of other security patch options to handle the current flaw. These options may or may not be effective.

CVE-2022-24401: The Air Interface Encryption (AIE) keystream generator relies on the network time, which is publicly broadcast in an unauthenticated manner. This allows for decryption oracle attacks

Despite the LLC header and further payload getting encrypted by TEAx keystream generator (KSG) TETRA messages have no cryptographic auth/integrity guarantee with CRC16 on lower MAC layer and Optional CRC32 on LLC layer, TEAx keystream generators depend on key and on network time, there is a need to guarantee different keystream used each time since network time broadcast in unencrypted, unauthenticated manner − SYNC and SYSINFO frames, no further cryptographic integrity checks − Any encrypted data is taken at face value.

having devices on a network that can serve as decryption oracle will result in attack of other devices that should not be exposed to the attacker, this will further lead to possible theft of confidential data via that network or possible denial of service by those or passive attack as copy of company resources. With the ability to decrypt the communication stream, an attacker can intercept and eavesdrop on sensitive data transmitted over the network. This could include confidential information, personal data, financial transactions, or any other type of sensitive data being communicated. In addition to intercepting data, an attacker might also tamper with the intercepted data before allowing it to reach its intended destination. This could involve modifying the content of messages, injecting malicious code or commands, or altering transaction details, leading to unauthorized actions or compromises. Users' privacy could be compromised as their personal information and communication become exposed to unauthorized parties. This could lead to various privacy violations, including identity theft, surveillance, or blackmail. Devices communicating over the compromised network could be targeted for further exploitation. This could involve installing malware, gaining unauthorized access to the device, or using it as a pivot point to launch attacks on other devices or systems within the network.

If the Air Interface Encryption (AIE) keystream generator relies solely on network time that is publicly broadcasted in an unauthenticated manner, it introduces vulnerabilities that can lead to various levels of cryptanalysis and attacks on transmitted data. The attacker can submit ciphertexts to the system and observe the corresponding decrypted plaintexts, thus gaining information about the encryption keys or keystream used. Attackers might exploit weaknesses or predictability in the network time protocol to derive information about the keystream or encryption keys. For instance, if the network time follows a predictable pattern or is not sufficiently random, it could be exploited to mount timing attacks. This could involve analyzing patterns in the keystream or exploiting weaknesses in its generation algorithm. If the network time is not properly secured or authenticated, attackers could manipulate or replay network time data to trick the system into using previously generated keystreams. This could enable replay attacks where previously intercepted ciphertexts are replayed to the system to gain unauthorized access to plaintext data.

The difficulty of exploiting the decryption oracle vulnerability depends on several factors, including the strength of generation, the attacker's capabilities, and the availability of resources, but with the availability of tools that scan networks for open and unencrypted data, a targeted network with this vulnerability will be easily discovered despite patches available except the protocol is revised to provide use an encrypted timestamp. Sophisticated cryptographic algorithms and proper implementation practices can make such attacks significantly harder to execute. the encryption algorithm, the randomness and unpredictability of the keystream

Once the weakness is understood and the necessary information is accessed, the attacker needs to have the ability to exploit it. This might involve developing tools or scripts to intercept and analyze the network time data and exploit the decryption oracle. The impact of exploiting this weakness would also affect the discoverability. If successful exploitation leads to significant consequences such as unauthorized access to sensitive information or disruption of services, it's more likely that the weakness would be discovered and exploited. The discoverability of the security weakness depends on a combination of technical knowledge, access to resources, and the potential impact of exploitation.

If these conditions are met, the weakness could be discovered and exploited. However, if the weakness is not well-known or actively sought after, it might remain undiscovered for an extended period as with the Tetra protocol

Since the network time is publicly accessible and not securely authenticated, attackers can repeatedly exploit vulnerabilities or weaknesses in the AIE keystream generation process. This means that threats, once identified and understood by attackers, can be continuously exploited or reproduced as long as the underlying vulnerabilities remain unaddressed.

The prevalence of this threat in the industry or similar companies depends on various factors such as the specific implementation of AIE, the security practices of the organizations deploying it, and the level of scrutiny given to potential security vulnerabilities.

To mitigate these threats, it's crucial for organizations to implement robust authentication mechanisms for network time synchronization and to regularly assess and update their encryption systems to address known vulnerabilities. Additionally, employing additional layers of security such as end-to-end encryption can further protect sensitive data from decryption oracle attacks.

CVE-2022-24402: The TEA1 algorithm has a backdoor that reduces the original 80-bit key to a key size which is trivially brute-forceable on consumer hardware in minutes

Devices utilizing TEA1 for encryption are vulnerable to attacks that exploit this backdoor. Adversaries could potentially gain unauthorized access to sensitive information stored or transmitted by these devices. It undermines the confidentiality and integrity of the data processed by such devices. The level of cryptanalysis and attacks that can be performed on transmitted data would include attacks such as brute-force attacks so that any confidentiality provided by TEA1 encryption would be effectively nullified; Known-plaintext attacks- If the attacker has access to plaintext-ciphertext pairs, they could exploit the backdoor to deduce the encryption key more easily, facilitating decryption of other ciphertexts; Chosen-plaintext attacks- they can use this knowledge along with the backdoor to mount chosen-plaintext attacks, which may further compromise the security of the system. The ease of exploitability of the backdoor in the TEA1 algorithm depends on several factors: awareness, technical Skill, access to Resources. The presence of countermeasures or mitigations against the backdoor can affect its exploitability. If security measures are in place to detect or prevent attacks exploiting the backdoor, it may significantly increase the difficulty of successful exploitation have significant implications for the security of systems relying on it for encryption. Remediation efforts might involve patching the algorithm to remove the backdoor, replacing it with a more secure algorithm, or implementing additional security measures to mitigate the risks posed by the weakness.

In terms of the reproducibility of this threat, it appears to be a continuous one rather than a one-time occurrence. Once the existence of such a backdoor is discovered, it poses an ongoing risk to any systems or applications that rely on TEA1 for encryption. The threat persists as long as the backdoor remains exploitable, potentially allowing attackers to decrypt sensitive information protected by TEA1.

The continuous nature of this threat underscores the importance of promptly addressing vulnerabilities in encryption algorithms and regularly updating cryptographic systems to mitigate emerging risks.

CVE-2022-24403: The cryptographic scheme used to obfuscate radio identities has a weak design that allows attackers to deanonymize and track users

Part of TAA1, called TA61Encrypts 24-bit TETRA addresses and the Encrypted identities change only when network key changes. TA61 is vulnerable to meet-in-the-middle attack − Recovers value of c − Complexity: 248 with 3 identity pairs leading to instant deanonymization. Attackers can exploit easily TA61 (the primitive responsible for identity encryption), allowing attackers to deanonymize traffic (passive attack) by identifying three pairs' identities with their encrypted equivalent, which can be obtained by observing unencrypted authentication in which both encrypted and unencrypted identities are used [2]

Such weak cryptographic schemes can compromise the privacy of users by allowing attackers to deanonymize them. Users may be concerned about their identities being exposed, especially if they are involved in sensitive or confidential activities. Deanonymization can lead to the exposure of sensitive information associated with radio identities. This could include location data, communication patterns, and other metadata that attackers could exploit for malicious purposes. The cryptographic schemes can make network traffic more susceptible to surveillance and monitoring by malicious actors. Deanonymization of users within the network could also enable attackers to manipulate network traffic, impersonate users, or perform other malicious activities without detection. The protocol will be vulnerable to traffic analysis even if the cryptographic scheme itself remains unbroken, weaknesses in the obfuscation of radio identities may still allow attackers to perform traffic analysis. By observing patterns in the communication, such as timing, frequency, or size of messages, attackers may be able to infer information about the identities or activities of users. Other attacks include Known-Plaintext Attack, Chosen-Plaintext Attack to deduce encryption keys or other sensitive information. The ease of exploitability of a cryptographic scheme weakness that allows for deanonymization, and user tracking depends on a combination of factors related to the attacker's capabilities, available resources, and the effectiveness of mitigation measures in place. Organizations should prioritize addressing such weaknesses promptly to mitigate the risk of exploitation by malicious actors.

Reverse Engineering: In some cases, attackers may reverse engineer the software or protocols used in radio systems to uncover weaknesses in the cryptographic scheme. By analyzing the implementation details and behavior of the system, attackers may identify vulnerabilities that could be exploited to deanonymize and track users.

CVE-2022-24404: Lack of ciphertext authentication on AIE allows for malleability attacks

A malleability attack allows a possible attacker to alter ciphertext in a way that when decrypted results in a related or known plaintext, these types of attacks take advantage of a lack of authentication for the origin message, weakness when a product does not validate or incorrectly validates the integrity check values or "checksums" of a message which can prevent the detection of data that has been modified or corrupted in transmission, or Message integrity violation due to the alteration of command-and-control signals which affects the integrity and trust worthiness of the communications within critical infrastructure.

Device Security: Devices relying on AIE for encryption may become vulnerable to malleability attacks. Without proper ciphertext authentication, an attacker could tamper with encrypted data packets in transit, modifying their contents in a way that the changes are not detected by the recipient. This can lead to various security breaches, such as injecting malicious code or commands into the data stream, disrupting communication, or compromising the integrity of transmitted information. This poses risks to critical operations, including those in sectors such as telecommunications, finance, healthcare, and public safety. Malleability attacks on AIE can undermine the security of network traffic within organizations or across communication networks. By tampering with encrypted packets, attackers can potentially bypass security controls, evade detection mechanisms, or launch more sophisticated attacks such as data exfiltration, injection of malware, or interception of sensitive information. This jeopardizes the confidentiality, integrity, and availability of network resources and services, compromising the overall security posture of the network infrastructure. Without proper authentication and safeguards against tampering, individuals' privacy rights may be violated, and confidential data may be exposed to unauthorized parties, leading to reputational damage, regulatory penalties, or legal liabilities.

To mitigate the impact of malleability attacks on AIE, organizations need to implement robust cryptographic protocols that incorporate ciphertext authentication mechanisms, such as digital signatures or message authentication codes (MACs). Additionally, deploying intrusion detection and prevention systems (IDPS), network monitoring tools, and encryption key management practices can help detect and mitigate malleability attacks, safeguarding devices, data, and network traffic from unauthorized tampering and exploitation. Regular security assessments, vulnerability scans, and penetration testing should also be conducted to identify and remediate vulnerabilities in AIE implementations and ensure the resilience of cryptographic protections against emerging threats.

VI. Conclusion

One thing that is known about crypto is that it must be open for scrutiny but replacing the unsecure encryption algorithm with another set of propriety algorithms as have been done, goes again to show that there are likely vulnerabilities with the new set of encryption algorithms and a fear of such discovery is present. Knowing that Propriety encryption algorithms are not secure. From the assessment of [2], we conclude that tetra protocol may be vulnerable to:

Eavesdropping: Despite encryption features in TETRA, if encryption keys are compromised or if outdated encryption algorithms are used, attackers could potentially eavesdrop on TETRA communications.

Denial of Service (DoS): TETRA systems may be vulnerable to DoS attacks, where an attacker floods the system with illegitimate requests or traffic, causing it to become overwhelmed and unavailable to legitimate users.

Man-in-the-Middle (MitM) Attacks: If attackers can intercept and manipulate TETRA traffic, they could potentially insert themselves as a middleman between communicating parties, eavesdropping on or altering the communication.

Weaknesses in Encryption: If TETRA systems are not properly configured or if outdated encryption algorithms are used, it could lead to vulnerabilities in the encryption mechanism, allowing attackers to decrypt intercepted communications.

Physical Security: TETRA infrastructure components such as base stations and control centers need to be physically secure. Unauthorized access to these components could compromise the entire system's security.

Radio Interference: TETRA operates in radio frequency bands, which could be subject to interference from other radio devices or intentional jamming by attackers, affecting communication reliability.

Insider Threats: Insider threats pose a risk to TETRA systems. Malicious insiders with access to system components could abuse their privileges to compromise the integrity, confidentiality, or availability of the system.

Lack of Security Updates: Failure to regularly update TETRA infrastructure with security patches and firmware updates could leave systems vulnerable to known exploits and vulnerabilities.

Social Engineering: Attackers could exploit human vulnerabilities through social engineering techniques to gain unauthorized access to TETRA systems or sensitive information.

Backdoor Exploitation: Undocumented or overlooked backdoors in TETRA equipment or software could be exploited by attackers to gain unauthorized access or control over the system.

REFERENCES

[1] Zahednejad, Behnam & Azizi, Mahdi & Student, P. (2020). An Improved Privacy Preserving TETRA Authentication Protocol Seyyed Morteza pournaghi.

[2] Carlo Meijer, Wouter Bokslag and Jos Wetzels (2023) All cops are broadcasting: TETRA under scrutiny, Midnight Blue accessed at https://www.tetraburst.com/

[3] Liu, M., & Li, H. (2023, July). A Formal Analysis of Emergency Communication System Based on Model Checking. In *2023 IEEE 13th International Conference on Electronics Information and Emergency Communication (ICEIEC)* (pp. 22-26). IEEE.

[4] ETSI. Terrestrial trunked radio (TETRA); security; synchronization mechanism for end-to-end encryption. ETSI ES 202 109 V1.1.1, 2003.

[5] ETSI. Terrestrial trunked radio (TETRA); voice plus data (v+d); part 7: Security. ETSI EN 300 392-7 V3.5.1, 2019.

[6] Karapantazis, S., & Pavlidou, F.-N. (Eds.). (2015). Security and Privacy in the Digital Era: A Practical Guide to Cybersecurity and Privacy. Springer.

[7] Liu Siqian, Li Hai, Wang Luman, Song Qizhu, Wang Junfeng, Chen Guocheng, "Design and implementation of TETRA call analysis software", 2014 IEEE 5th International Conference on Software Engineering and Service Science, pp.220-223, 2014.

[12] Reports from market research firms such as Frost & Sullivan, IHS Markit, and Technavio often provide insights into the TETRA market, including device usage, manufacturers, and industry sectors.

[13] Radio Resource International, Critical Communications Today, and MissionCritical Communications frequently cover developments in the field of professional mobile radio (PMR) and TETRA technology

[14] Pfeiffer, M., Kwiotek, J. P., Classen, J., Klose, R., & Hollick, M. (2016). Analyzing TETRA location privacy and network availability. In Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices (pp. 117-122).

[15] Ozimek, I and Gorazd. K, "SCADA system using TETRA communication network," Recent advances in computers, computing and communications, pp. 164-166, 2002.

[8] ETSI Technical Standard ETSI EN 300 392-7 V2.1.1 (2001-02): Terrestrial Trunked Radio (TETRA); Voice plus Data; Part 7: Security

[9] Shuwen Duan (2013) Security Analysis of TETRA; Masters' thesis, Norwegian University of Technology

[10] Dunlop, J., Girma, D., & Irvine, J. (1999). Digital mobile communications and the TETRA system (Vol. 1). Wiley.

[11] Walke, B. H. (2002). Mobile Radio Networks: Networking, Protocols and Traffic Performance. Wiley.

[16] Yong-Seok.P,Kim.S, "The vulnerability analysis and improvement of the TETRA authentication protocol," in The 12th International Conference on Communication Technology (ICACT), 2010.

[17] MullaZadeh.M,Farash.S, "formal verification of TETRA authentication protocol with automated tools," cyber and electronics defense magazine, no. 4, pp. 109-129, 2017.

[18] Tanuhardja R. R. , van de Beek S., Bentum M. J. and Leferink F. B. J. ,(2015) "Vulnerability of Terrestrial-Trunked Radio to Intelligent Intentional Electromagnetic Interference," in IEEE Transactions on Electromagnetic Compatibility, vol. 57, no. 3, pp. 454-460

[19]https://youtu.be/Fy3Odmdny0?si=AaZABwmjuMGC45Zm accessed January 30, 2024