**Vulnerabilties:**

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.

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”*. This vulnerability will allow the attacker to gain access to the network and thereby provide the ability to eavesdrop on communication.

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

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.

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.

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.

Citations:

* 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.
* Terrestrial Trunked Radio," [Online]. Available: <https://en.wikipedia.org/wiki/Terrestrial_Trunked_Radio>
* "TETRA," [Online]. Available: <https://www.etsi.org/technologies/tetra>.
* TETRA:BURST," [Online]. Available: <https://www.tetraburst.com/>
* Zahednejad, Behnam & Azizi, Mahdi & Student, "An Improved Privacy Preserving TETRA Authentication Protocol Seyyed Morteza Pournaghi," 2020.