The Vulnerability Analysis and Improvement of the TETRA Authentication Protocol

Yong-Seok Park*, Choon-Soo Kim*, Jae-Cheol Ryou**

*National Security Research Institute

**Internet Intrusion Response Technology Research Center, Chungnam National University

parkys@ensec.re.kr, jbr@ensec.re.kr, jcryou@home.cnu.ac.kr

***Abstract*—The TETRA system provides an authentication service which permits only the authorized terminal to access its network by verifying that the terminal equipment and the authentication center have the identical authentication key using challenge-response protocol. However, while TETRA standard 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. In this paper, we briefly describe TETRA standard authentication protocol defined by European Telecommunications Standards Institute (ETSI), followed by a brief description of authentication key generation/distribution/injection models during its authentication process. Then we analyze the threat of cloned terminals in the case of authentication key being exposed during the process of distributing to the authentication center. Finally we propose a new authentication protocol that can prevent cloned terminals that have cloned both ISSI and the authentication key from illegally accessing the network.**

***Keywords*— TRS, TETRA, authentication, authentication key, ISSI**

I. INTRODUCTION

Trunked Radio System (TRS) refers to the communication system in which multiple users share the limited radio frequency and it is comprised of such components as base station, mobile relay system and system management facility and so forth.

In Korea, the efforts for implementing government-directed wireless communication network that adopts the European TRS open standard, TETRA (TErrestiral Trunked RAdio) are being made in order to ensure the availability of unified wireless communication command system in case of emergency disaster situations [1].

As the world's only wireless digital open standard standardized by ETSI (European Telecommunications Standards Institute) that supports both PMR (Professional Mobile Radio) and PAMR (Public Access Mobile Radio), TETRA has already positioned itself solidly in the highly competitive open market for business-purpose mobile wireless communication industry and is currently being in use for public safety and disaster control networks all around the worlds. TETRA, being categorized as a control and command system utilized by disaster management authorities such as the military and the police, has been defined with a separate standard suitable for information security services with strict requirements [2-4].

The security functions of TETRA are classified, according to the security level, into authentication, Air Interface Encryption (AIE), and End-To-End Encryption (E2EE).

The authentication is the procedure which checks the sameness of authentication key (K) shared in advance between terminal and authentication center by using challenge-response protocol. The authentication function of the TETRA system ensures that the unauthorized terminal equipment cannot access its network illegally. However, though the TETRA standard authentication protocol is capable of blocking the terminal that wrongfully has copied terminal identifier called ISSI (Individual Short Subscriber Identity), the protocol is still remained with the vulnerability that it cannot protect from the terminal which has successfully obtained both a copy of ISSI and authentication key. Therefore the threat of illegally copied authentication key is not considered.

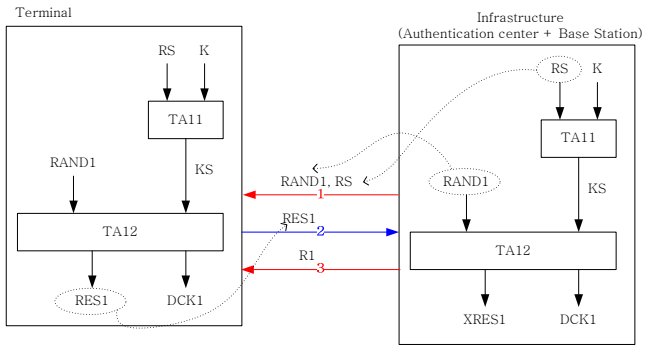
In this paper, the general description of the TETRA authentication protocol is provided and the authentication key generation, distribution and injection models used during its authentication process are explained. Next, the threat of the clone terminal caused by the exposure of the authentication key during its delivery process is analyzed. Finally, supposing the worst case scenario of a clone terminal as a result of authentication key exposure, we propose the new authentication protocol that is capable of blocking the illegal clone terminal from accessing the network.

II. THE ANALYSIS OF A TETRA AUTHENTICATION PROTOCOL

A. Authentication of a Terminal

The purpose of TETRA authentication service is to remove the threat of eavesdropping by illegal clone terminal. The TETRA authentication method is a symmetric secret key type.

In this method one secret, the authentication key, shall be shared by each of the authenticating parties, and there should exist strictly two parties with knowledge of the secret. Authentication is achieved by the parties proving to each other knowledge of the shared secret. The authenticating parties are said to be the authentication center of the Switching and Management Infrastructure (SwMI) and the terminal. Fig. 1 shows the terminal authentication procedure.



K (128bit) : Authentication key distributed per terminal
RS (80bit) : Random value generated by authentication center used to generated session authentication key(KS)
KS (80bit) : Session authentication key used to identify terminal
RAND1 (80bit) : Random value generated per each authentication procedure by Base Station
RES1(32bit) : Authentication result that terminal replies to infrastructure

Figure 1. Authentication of a Terminal by Infrastructure

The authentication is done using a challenge- response protocol, with a session authentication key (KS) derived from an authentication key that shall be shared by the terminal and the infrastructure system. The session authentication key is provided by an authentication centre of the home system.

The computation of the session authentication key is carried out by an algorithm, TA11. The computation of the response is done by another algorithm, TA12, which at the same time shall produce a derived cipher key.

The SwMI generates a random number as a challenge RAND1. The terminal computes a response, RES1, and the SwMI computes an expected response, XRES1. A component of the derived cipher key is generated by this process, labeled DCK1. The SwMI on receipt of RES1 from the terminal shall compare it with XRES1. If the values are equal the result R1 shall be set to TRUE, else the result R1 shall be set to FALSE.

Using protocol analyzer, Fig. 2 shows the screen capture of authentication signaling message exchange process that starts with the actual TETRA mobile system terminal sending a location update demand message (U-LOCATION UPDATE DEMAND) to the base station during the terminal registration stage.

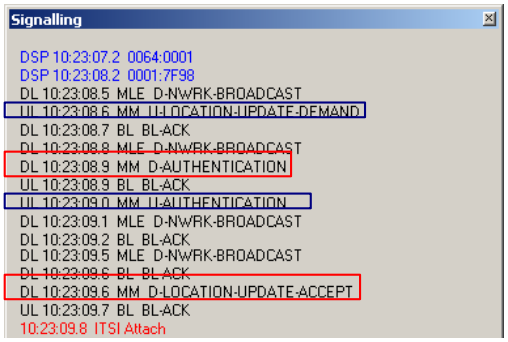


Figure 2. Authentication Signaling Message Exchange Process

The identity request signal (challenge) indicated by arrow number 1 of Fig. 1 associates with D-AUTHENTICATION of Fig. 2. The actual message of D-AUTHENTICATION that the protocol analyzer captured is shown below in Fig. 3.

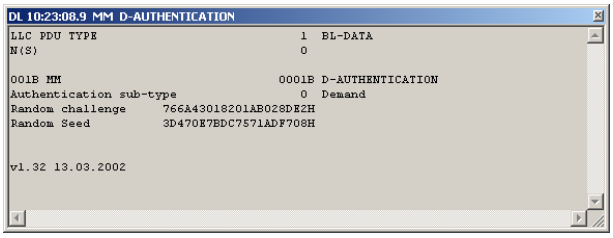


Figure 3. D-AUTHENTICATION Message

Subsequently, the response signal (response) indicated by arrow number 2 of Fig. 1 associates with U-AUTHENTICATION of Fig. 2. The actual message of U-AUTHENTICATION that the protocol analyzer captured is shown below in Fig. 4.

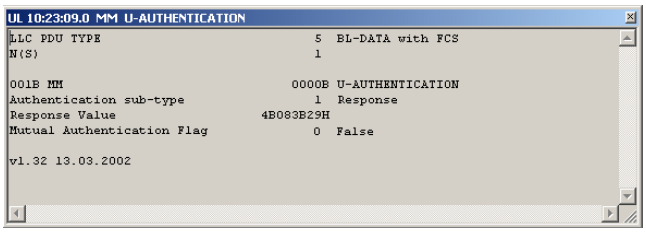


Figure 4. U-AUTHENTICATION Message

Finally, the authentication result signal (result) indicated by arrow number 3 of Fig. 1 associates with D-LOCATION UPDATE ACCEPT of Fig. 2. The actual message of that the protocol analyzer captured is shown below in Fig. 5. The authentication result field sets to TRUE (1) upon successful authentication.

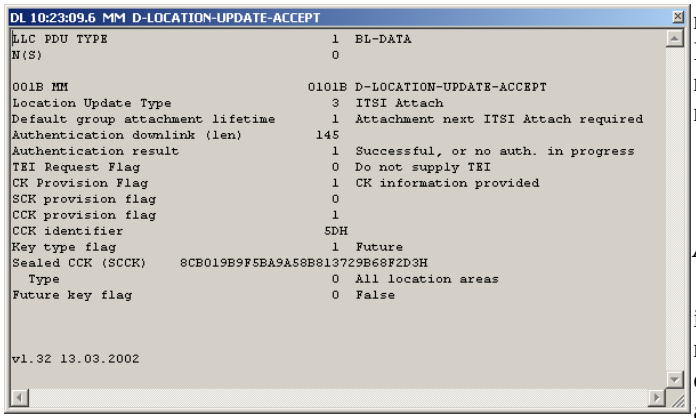
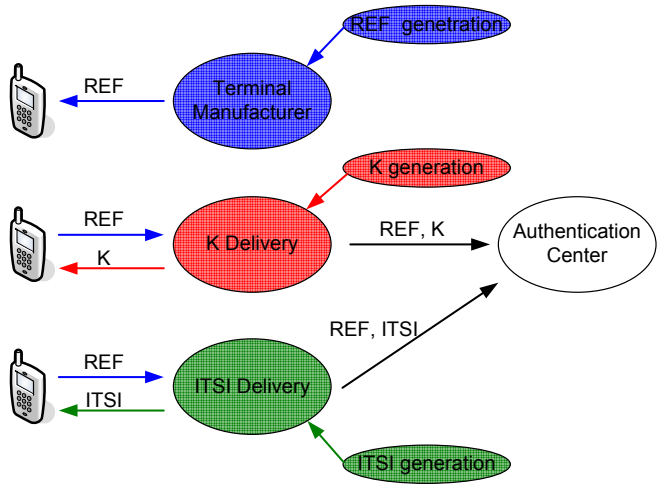


Figure 5. D-LOCATION UPDATE ACCEPT Message

B. Authentication Key Generation/Distribution/Injection Model

For successful terminal authentication, each terminal and authentication center must possess identical authentication key. Fig. 6 depicts the generation/distribution/injection models as proposed by TETRA MoU SFPG Recommendation 01 [5].



1. Terminal Manutacturer
 - Delivers terminal to K Delivery after generating REF and programming terminal
2. K Delivery
 - Generates K and programs onto terminal
 - Generates REF-K pair according to pre-defined file format and distributes to authentication center
 - Delivers terminal to ITSI Delivery
3. ITSI Delivery
 - Generates ITSI and programs onto terminal
 - Generates REF-ITSI pair according to pre-defined file format and distributes to authentication center

Figure 6. TETRA Authentication Key Generation/ Distribution/Injection Models

As shown in Fig. 6, authentication center database must have stored REF-K pair and REF-ITSI pair in order for the authentication center to determine which authentication key should be injected to which terminal. REF (Reference Number) here refers to the terminal serial number that the manufacturer provides and ITSI (Individual TETRA Subscriber Identity) refers to the terminal identification number that the network manager provides, which essentially is a phone number.

III. Analysis of Clone Terminal Threat in TETRA Network

A. Cloning ISSI Only Case

ISSI refers to the phone number as 6-digit (24-bit) terminal identification number which is country code (10-bit) and network code (14-bit) taken off from 48-bit ITSI. The number of ther terminal can be easily obtained. Therefore, whoever is accessable to the terminal program tool can easily create clone terminal with ISSI copied. However, by TETRA standard definition, the terminal that has copied only ISSI without the knowledge of other terminal's authentication key will be prohibited from network connection by the authentication protocol. Suppose A is a normal terminal and B is a clone terminal created with ISSI_A of A. A hacker would attempt to access the system with ISSI_A without knowing A's authentication key, K_A. If the clone terminal, B, is turned on, it transmits a location update demand message (U-LOCATION UPDATE DEMAND) to the network and tries to register itself (to the infrastructure system) as shown in Fig. 7.

Information element	Length
PDU type	4
Location update type	3
Request to append LA	1
Cipher control	1
Ciphering parameters	10
Class of MS	24
Energy saving mode	3
LA information	
SSI	24
Address extension	24
Group identity location demand	
Group report response	
Authentication uplink	
Proprietary	

Figure 7. Information of U-LOCATION UPDATE DEMAND Message

Once the network receives the location update demand message, it retrieves the ISSI value embedded in the message and it starts its authentication process by searching from the authentication center database for the authentication key that matches with the associated ISSI. In this process, since the clone terminal B does not know the authentication key K_A of the normal terminal A, the clone terminal B cannot calculate the correct response value RES1 that matches with the XRES1 value calculated from the network. As a result, the clone terminal B is not allowed to be registered on the network.

B. Cloning both ISSI and authentication key Case

Fig. 6 shows that REF-K pair and REF-ITSI pair are delivered to the authentication center on/offline. In case of most of today's TETRA systems, REF-K pairs and REF-ITSI pairs are generated according to the specified file format and delivered to the authentication centers via portable storage

mediums such as CD-ROM [5]. During the process of delivering key files to the authentication center, since no separate standard has yet been prepared to specify the maintenance of confidentiality, there exists a risk of authentication key leakage through such events as the misplacement of key file storage mediums during delivery processes.

Likewise, in case of the authentication key misplacement and both ISSI and K being cloned, the authentication protocol defined by TETRA standard cannot prevent these cloned terminals from accessing the network. The following simulation elicits the problem of a cloned terminal that successfully cloned both ISSI and K passing the authentication process and connecting to the network.

1) Simulation Environment Setting

- Leave three terminals, A, B, and C that support authentication and wireless cryptographic features turned off
- Program terminal A with ISSI_A and K_A and terminal B with ISSI_B and K_B.
- Make terminal C a cloned terminal of terminal A by programming ISSI_A and K_A.

2) Simulation

- Turn on terminal A and B and confirm a normal registration at site 1.
- Using terminal protocol analyzer, confirm that both terminal A and B have successfully received U-LOCATION UPDATE ACCEPT message (Fig. 5). This means that the terminals have successfully authenticated and, as a result, both terminal A and B have generated separate DOKs. The DOK that terminal A currently possess is called DOK_A.
- Send group-call from terminal A and confirm that terminal B receives encrypted group-call. Then send group-call from terminal B and confirm that terminal A receives encrypted group-call. This shows that both terminals are now available for group communication using DOK and COK keys.
- Roam terminal A to site 2. Terminal A is tacitly authenticated. SwMI provides DOK_A_1 to site 2 and removes DOK_A_1 from site 1.
- Send group-call from terminal A and confirm that terminal B receives encrypted group-call. Then send group-call from terminal B and confirm that terminal A receives encrypted group-call.
- Turn on cloned terminal C and register onto site 1. Verify that the terminal C that cloned both ISSI and K of terminal A is registered as if identical to terminal A at the SwMI. Therefore, the SwMI authenticates terminal C explicitly. Terminal C now possesses DOK_A_2. The SwMI removes DOK_A_1 from site 2 while terminal A still has DOK_A_1.
- Send group-call from cloned terminal C. Confirm that terminal B receives the encrypted group-call. Send group-call from terminal B. Confirm that cloned terminal C receives the encrypted group-call. This shows that cloned terminal passes an authentication process and that the protocol does not prevent the illegal use of the cloned terminal that has masqueraded as a normal terminal A.

IV. A New Authentication Protocol that Protects from Cloned Terminals

As examined earlier, there exists a serious problem with the current TETRA standard authentication protocol of not being able to prevent cloned terminals with ISSI and K wrongfully cloned from accessing the network. The root cause of this problem is with the fact that the REF value, which is used as a serial number that uniquely identifies each terminal, is not delivered to the infrastructure network but rather to ISSI only (see Fig. 7 for location update demand message). Since the network must check for the relationship between ISSI and K, if the cloned terminal possesses both ISSI and K, the the network cannot acknowledge it. Therefore, in order to resolve this issue, this paper proposes a new authentication method as shown in Fig. 8.

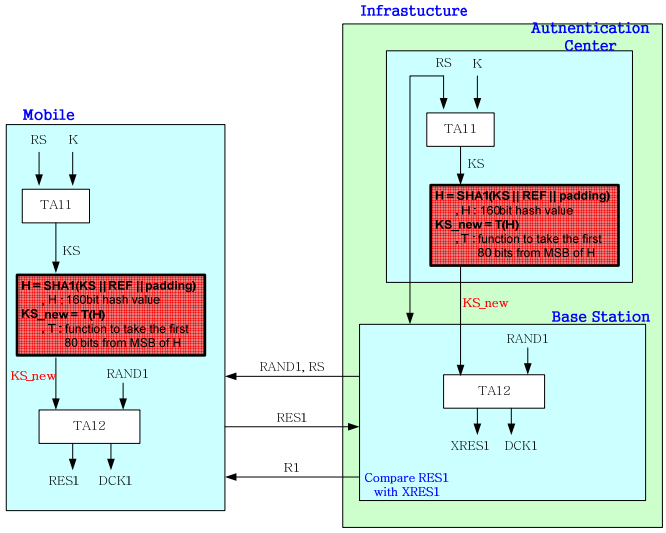


Figure 8. A New Protocol Blocking the Network Access of Terminal that the Authentication Key is Copied

The suggested protocol implements the use of REF to which the existing authentication process does not refer. Instead of using the 80-bit session authentication key, KS, in the existing protocol, the new process generates a session authentication key, KS_new, as the following.

The new authentication protocol applies KS and REF as input values from SHA1 hash algorithm. Then, KS_new value is determined by applying function T which takes the 80 MSB bits from the 160-bit hash value, H which is a SHA1 output. Instead of the KS value, the KS_new value is now used as an input to the existing authentication algorithm, TA12.

Since REF is a value that terminal manufacturer generates and stores on the permanent security identified memory from the point of terminal shipment, it is impossible to modify from an external programming equipment. Therefore, even for the cloned terminal that has cloned ISSI and authentication key , by

implementing the procedure of checking REF, the suggested protocol does not allow the cloned terminal onto the network because, if REF value is incorrect, it cannot produce the same response value, RES1 that equals XRES1 that the network calculates.

V. CONCLUSION

TETRA standard provides its authentication service by allowing only the authorized terminals to access the network to mitigate the risk of conversation eavesdropping, masquerade attacks and other security attacks from cloned terminals. However, the risk of the authentication key being exposed while the key is distributed to the authentication center still exists. That is, this also suggests that there exists a vulnerability of the protocol not to block the cloned terminal that has successfully copied both ISSI and the authentication key onto the network. In this paper, having described TETRA standard authentication protocol and authentication key generation/distribution/injection models, we have confirmed through simulation that the current TETRA standard authentication protocol cannot prevent the illegal use of cloned terminals that has successfully cloned the authentication key. In order to reslove this critical issue, we have proposed a new authentication protocol that applies REF during the authentication process with the purpose of disallowing any cloned terminal that has cloned both ISSI and authentication key successfully. The proposed authentication protocol can be applied with a simple software upgrade on authentication center and terminal side without having to revise any authentication-related signal message standard defined in TETRA standard, maintaining the existing authentication framework.

ACKNOWLEDGMENT

"The third author of this research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency)" (NIPA-2009-(C1090-0902-0016))

REFERENCES

[1] NEMA, "Request For Proposal for Korean Government Radio Network", 2005.
[2] ETSI EN 300 392-7 V2.2.1, "Terrestrial Trunked Radio(TETRA); Voice plus Data(V+D); Part 7 : Security", September 2004.
[3] ETSI EN 302 109 V1.1.1, "Terrestrial Trunked Radio(TETRA); Security: Synchronization mechanism for end-to-end encryption", October 2004.
[4] TETRA MoU SFPG Recommendation 02 edition 4, "End-to-End Encryption", October 2004.
[5] TETRA MoU SFPG Recommendation 01 edition 4, "TETRA Key Distribution", February 2006.