The Critical Communications Association

Security and **F**raud **P**revention **G**roup

Maintaining TETRA Security

An SFPG paper, for use within TCCA.

March 2020

TCCA SFPG Secretariat

Marjan Bolle, email: SFPG@TCCA.info

MAINTAINING TETRA SECURITY

Introduction

TETRA security mechanisms are well documented and are capable of protecting the communications of the most demanding users. However, any security measure needs to be regularly managed to maintain its effectiveness. This paper gives a brief overview of the aims of the mechanisms, and provides some areas for consideration in using these to maintain a secure communication system.

TETRA security functions

The security functions of TETRA include authentication, air interface encryption, end to end encryption and a secure disabling facility. These are built on top of other standardized air interface functions which permit access to a system to be controlled, and which regulate the facilities available to each Mobile Station (MS). It is worth considering what each of the security functions contributes to overall system security, and the steps that should be taken in managing and maintaining the security of a secure TETRA system.

Access control and authentication

TETRA authentication ensures that all MSs that use a system are valid subscribers to that system, and that the MS can be assured that the system itself is authentic. A first step in access control to a system is restricting access to MSs that are provisioned in a subscriber database. Authentication provides additional control: to prevent a valid MS being cloned, a secretly provisioned authentication key is used to validate the MS on registration, and because the keys are provisioned in controlled environments, stored securely in the MS and never revealed, cloning is effectively prevented. The same secret key also allows the MS to verify that the system is genuine.

It is important that authentication is fully provisioned for all MSs, and it is recommended that MSs are configured to require mutual authentication. The list of valid subscribers must be continuously maintained. MSs that are lost, stolen or taken out of service need to be removed from the system database, or flagged as out of service. Otherwise, an MS that is still active with a valid authentication key provides a means of accessing the system, whether in the hands of an intended user or not. One measure against misuse is to require a PIN to be entered on the MS when it is switched on: this mitigates against lost or stolen MSs being used inappropriately. A further defence against a lost or stolen MS is the enable/disable mechanism – see later. If TETRA equipment that contains an authentication key (or other keys) is sent outside its organization for service or repair, the organization may want to delete the authentication key (and any other keys) as a matter of security policy before sending the equipment out, and to replace the authentication key (and other keys) before the equipment is put back into service.

Air interface encryption

Air interface encryption protects against eavesdropping at the radio link between MSs and base stations in Trunked Mode, or between MSs in Direct Mode. It is intended to make this link more difficult to break than an attack on the network itself. Dynamic keys are established by the authentication process, and longer life static and group keys are also used to protect in Direct Mode, in fallback situations and to differentiate between groups.

As far as is known, the air interface encryption in TETRA has never been broken. However, there have occasionally been instances of TETRA communications being eavesdropped, and the content revealed to the press or to other organizations. The most common causes of this are stolen MSs that have fallen into the wrong hands, or cases where encryption was not configured correctly and was not switched on, or where the secure TETRA network was patched to an insecure network, e.g. an analogue FM or AM network used for interoperability or air to ground communication.

It is therefore important that the network is configured correctly, with encryption enabled for all users. Even having a few users without encryption can cause a breach in security if unencrypted users communicate with encrypted users. Although the digital nature of TETRA transmissions might once have been considered to give some basic level of privacy, free software and cheap hardware (e.g. USB TV receiver sticks for around €10 to €20) allow anyone to eavesdrop on an unencrypted network with very little effort.

Connections to insecure networks need to be considered very carefully and avoided if possible; and users need to be aware of any circumstances where their communications could be relayed in clear.

Keys need to be changed regularly. The authentication and encryption mechanisms allow frequent changes of the dynamic keys (daily if needed). Over The Air Rekeying (OTAR) can be used to change the static and group keys, and should be configured to provide regular key change periods. If a compromise is suspected where an MS and its keys have been lost, further key changes can be initiated by use of the OTAR mechanisms, and that MS can be disabled.

The encryption algorithms are standardized, but not available in the public domain. MSs containing the TEA2 algorithm, used for European government and public safety use, are controlled and must be managed and disposed of in accordance with the Confidentiality and Restricted Usage Undertakings published by ETSI and agreed with the TEA2 custodian.

End to end encryption

End to end encryption provides a further layer of security in addition to air interface encryption. It protects communications at all points in the network. The encryption algorithm can be selected by the end user organization, with a key length suitable for its needs. The Over The Air Key management (OTAK) system can be owned and managed by the end users, independently of the TETRA network operator.

End to end encryption keys need to be managed, and changed regularly. MSs that have been lost or stolen, or taken out of service temporarily or permanently need to be excluded from communications by deleting keys, or disabling. Changing the keys in other MSs should be considered to avoid compromise where an MS cannot be accounted for.

Operationally, a user may communicate with some users and groups using end to end encryption, and with other users and groups without end to end encryption. It is important that a user is always aware of the security employed in each call, for example by enabling an alert on the MS when end to end encryption is not in use. Patching decrypted end to end encrypted communications to users without end to end encryption (e.g. to a telephone network) should be avoided, or only done in exceptional circumstances and where the end to end encrypted users have been warned (e.g. verbally) about loss of security.

If end to end encrypted MSs are used for communications of the highest security classifications, it is important that an accounting regime is put in place to keep track of these MSs, so that any loss of an MS, even if temporary, can be taken into account by key management. MSs sent for service or repair, or taken out of service, should have their keys erased first. If the algorithm is considered sensitive, or if there are any concerns about erasure of key material, there may be a need to destroy the hardware responsible for end to end encryption (which may be the entire MS itself) by a suitable procedure when the MS is taken out of service.

Secure enable and disable

TETRA also provides a means to securely disable an MS over the air, temporarily or permanently, which can include erasure of some or all keys. This is another tool for a system manager to ensure that lost, stolen or stored MSs are excluded from communications. A temporarily disabled MS can be enabled over the air once the MS has been verified and needs to be put back into service.

Upgrades and updates

When a TETRA system is put into service, it is important that the system and MS configuration apply the required security functionality. Once a system is running, the supplier will normally make updates and upgrades available for system and MS software, which can add functionality and improve security. Security patches to operating systems and updates to anti-virus definitions are examples of regular updates. The network operator should apply these updates as soon as is possible, to maintain the system in a secure state.

The TETRA standard itself has been continuously improved and has had new functionality added over the years. The TETRA network operator may find that new facilities would be of use to improve the security of their network, and may wish to consider upgrading accordingly.

Summary

TETRA provides layers of security which protect the communications of the most demanding users. However, the measures provided by TETRA need to be implemented and managed throughout the lifetime of the system to ensure that security is maintained. Every TETRA system needs to have operational and security policies in place to ensure that security is not left to chance. TCCA SFPG Recommendations can help provide guidance in the areas that should be considered in such policies. SFPG Recommendations are available from SFPG@TCCA.info.

Information on the control and management of equipment containing the TEA2 algorithm can also be obtained from SFPG@TCCA.info.

The TETRA standard itself is continuously maintained and improved, to ensure that the mechanisms specified remain up to date, and are interoperable between different suppliers of networks and MSs.