TETRA Security

Security mechanisms in TETRA, and how to ensure that the solution is secure...

Iain Ivory
Motorola
What we want to achieve with Security

- **Confidentiality**
  - No one can eavesdrop on what we are saying

- **Authenticity**
  - The people we are talking to are the right people
  - The wrong people can’t try and join us

- **Integrity**
  - The information gets there completely intact

- **Availability**
  - Communications are possible where and when they are needed

- **Accountability (Non repudiation)**
  - Whoever said something, can’t deny it later
Threats to communication and the threats to security

• **Message related threats**
  – interception, eavesdropping, masquerading, replay, manipulation of data

• **User related threats**
  – traffic analysis, observability of user behaviour

• **System related threats**
  – denial of service, jamming, unauthorized use of resources
Key Functions of TETRA Security

- TETRA has several security features allowing most customers' security needs to be met in a cost efficient way.
  
  - **Authentication** - ensures only valid subscriber units have access to the system and subscribers will only try and access the authorized system.

  - **Air Interface Encryption** – protects all signalling, identity and traffic across the radio link.

  - **End-to-End Encryption** - protects information as it passes through the system.
Authentication

- Authentication provides proof identity of all radios attempting use of the network.
- Radio can authenticate the network in turn, protects against ‘fake base stations’ etc.
- A session key system from a central authentication centre allows highly secure key storage.
  - Secret key need never be exposed.
- Authentication process derives air interface key (TETRA standard) – automatic key changing!
Radio Security Provisioning And Key Storage

- TETRA MoU SFPG Recommendation 01 provides a standardised format for importing authentication and other air interface encryption keys

- Use of Recommendation 01 files will allow multi vendor terminal supply

- Separation of logical key programming step from factory can allow all keys to be loaded in country
  - Meets national security requirements
**What is Air Interface Encryption?**

- **First level encryption used to protect information over the Air Interface**
  - Typically software implementation
  - Protects almost everything – speech, data, signalling, identities...

- **3 different Classes**
  - **Class 1**
    - No Encryption, can include Authentication
  - **Class 2**
    - Static Cipher Key Encryption, can include Authentication
  - **Class 3**
    - Dynamic Cipher Key Encryption
      - Individual Derived Cipher Key
      - Common Cipher Key
      - Group Cipher Key
    - Requires Authentication

- **Includes over the air key management protocols**
  - Allows seamless key management
The purpose of Air Interface Encryption

- Network fixed links are considered difficult to intercept.
- The air interface was considered vulnerable.
- Air Interface encryption was designed to make the air interface as secure as the fixed line connection.
Important properties of Air Interface encryption

• Many threats other than eavesdropping
  – traffic analysis, observance of user behaviour
• AIE protects control channel messages and identities as well as voice and data payloads
  – End to end encryption - if used alone - is insufficient (it only protects the voice payload)
• Continuous authentication
  – Encryption key generated from authentication process
• Encrypted registration protects ITSIs even at switch on
• Security classes can be changed in operation – essential for fallback measures if authentication cannot operate
End to end encryption in TETRA

• ETSI Project TETRA provides standardised support for end to end Encryption
  – ETSI EN302109 contains specific end to end specification
  – Ensures TETRA provides a standard alternative to proprietary offerings and technologies
  – Ensures compatibility between infrastructures and terminals

• Many organisations want their own algorithm
  – Confidence in strength
  – Better control over distribution

• TETRA MoU – Security and fraud Protection Group
  – Provides detailed recommendation on how to implement end to end encryption in TETRA

• The result – Standardisation and compatibility, with choice of algorithm
  – A big strength of TETRA
End To End Encryption

‘Standardisation’

- TETRA MoU SFPG Recommendation 02
  - Framework for end to end encryption
  - Recommended synchronisation method for speech calls
  - Protocol for Over The Air Keying
  - Sample implementations including algorithm mode and key encryption for IDEA, and AES in progress
  - DOES NOT specify implementation – can be implemented with module, software, SIM card etc..
  - DOES NOT provide module interface specification
Related Recommendations

- **TETRA MoU SFPG Recommendation 01**
  - Key transfer specification
  - Currently being updated to include end to end encryption key import formats

- **TETRA MoU SFPG Recommendation 07**
  - Short data service encryption
  - Currently being updated to reflect larger algorithm block sizes, e.g. 128 bits for AES

- **TETRA MoU SFPG Recommendation 08**
  - Framework for dividing encryption functionality between a SIM (smartcard) and a radio
  - No defined bit level interface (export control issue)

- **TETRA MoU SFPG Recommendation 11**
  - IP Packet data encryption
  - Work in process
  - Will provide a suitable means for high security packet data encryption, with commonality with voice encryption
Implementing TETRA security

- TETRA security measures are by no means the complete picture
- How well they are implemented – and how the implementation is evaluated is critical
- The rest of the network – what else connects to TETRA – is equally important
- The operational process and procedures equally provide countermeasures to the threats
Implementation considerations – Air Interface Encryption

• AIE should provide security equivalent to the fixed network

• There are several issues of trust here
  – Do I trust that the AIE has been implemented properly?
  – Does AIE always operate (during registration, in fallback modes etc)?
  – Do I trust the way that the network (or radio) stores keys?
  – Do I trust the fixed network itself or can someone break in?

• A strong AIE implementation and an evaluated network can provide essential protection of information

• An untested implementation and network may need reinforcing, for example with end to end encryption
Useful Recommendations

- TETRA MoU SFPG Recommendation 03 – TETRA threat analysis
  - Gives an idea of possible threats and countermeasures against a radio system
- TETRA MoU SFPG Recommendation 04 – Implementing TETRA security features
  - Provides guidance on how to design and configure a TETRA system
- Both documents are restricted access requiring Non Disclosure Agreement with SFPG
Assuring your security solution

• There are two important steps in assuring the security of the solution: Evaluation and Accreditation
• Evaluation of solutions should be by a trusted independent body
  – Technical analysis of design and implementation
• Accreditation is the continual assessment of risks
  – Assessment of threats vs solutions
    • Procedural and technical solutions
  – Should be undertaken by end user representative
Maximising cost effectiveness

• Evaluation can be extremely expensive – how to get best value for money?
• Establish the requirements in advance
  – as far as they are known – security is always a changing requirement!
• Look for suppliers with track record and reputation
• Look for validations of an equivalent solution elsewhere
• Consider expert help on processes and procedures
Summary: The essentials of a secure system

- A strong standard
- A good implementation
- Experienced supplier
- Trusted evaluation
- Continual assessment of threats and solutions
Security benefits in integrated system

• Common security measures for all services
  – Government approved security measures rather than just commercial level security
  – No need for users to worry about which data service is security cleared for which application

• The system availability and resilience are high for all services
  – Public data networks look attractive, but cannot provide the availability or the priority service levels

• Single evaluation and common accreditation issues for entire network
What security level do you want?

- TETRA Class 1
- TETRA Class 2
- TETRA Class 3
- TETRA w/ E2E algorithm on Smart Card
- TETRA w/ E2E SW algorithm in radio
- TETRA w/ E2E hardware solution using AES128
- TETRA w/ E2E hardware solution using own algorithm

TETRA is @ your Service
Thank You

www.Tetramou.com
www.ETSI.org
www.Motorola.com/Tetra
Iain.Ivory@motorola.com