TETRA Security for Poland

Brian Murgatroyd

TETRA ASSOCIATION

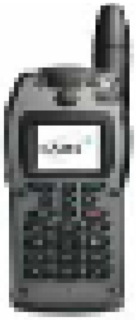
former Chairman
Security and Fraud Prevention Group
(SFPG)

Agenda

- Practical security threats to mission-critical TETRA systems
- System security countermeasures to handle threats
- Standard TETRA security features
  - Authentication
  - Air interface encryption
  - Terminal disabling
- Additional security measures
  - End to end encryption

Importance of standardization in security countermeasures

- Security countermeasures must be standardized otherwise their can be no interoperability between terminal makes
- TETRA has a mature set of standards and interoperability testing regime to assure users they can safely procure terminals of any compliant supplier
- The TETRA association Security & Fraud Prevention Group (SFPG) have recommendations that give explicit guidance on applying security standards and in particular on the use of end to end encryption which is not included in the ETSI standards



Classes of Security Threats

- **Availability. The most important threat type?**
  - Natural disasters, Denial of service(jamming, switching off network by illicit access)
- **Confidentiality. The best known threat?**
  - Eavesdropping, interception of radio path or network,
  - traffic analysis
- **Integrity?**
  - Unauthorized terminals and users allowed on the system
  - Messages can be replayed at later date. Data may be altered during transmission

Practical communications security threats to mission critical TETRA systems

➢Thousands of theoretical threats to communications systems

➢Very important that **expensive** security countermeasures are targeted only on real and important threats

➢Not all threats need to be protected against because:

- Maybe too expensive
- Unlikely to occur
- Other non technical solutions available

➢Outstanding threats need to be properly identified and risk managed by the system/data owners

Practical considerations for TETRA security

- Encryption is **easy** to implement
  - Algorithms available freely on internet

- Encryption is **difficult** to implement securely
  - Correct application of security functions requires experience
  - Need to protect against extraction of secret keys in terminals
  - Traffic encryption keys need storing in encrypted form or in secure environment

- Efficient key management is the most important aspect of a secure radio system
  - Need to protect against extraction of keys
  - Ensure connectivity is strictly controlled
  - Highly protected local security environment and sophisticated access control on Key Management System

Main TETRA security countermeasures

- 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
- Terminal disabling – ensures lost and stolen terminals are not a threat to the network security
- End-to-End Encryption – protects user’s data all the way through the system with high levels of confidentiality

TETRA Air interface security classes

Class	Encryption	OTAR	Authentication
1	No	No	Optional
2	Static key	Optional	Optional
3	Dynamic key	Mandatory	Mandatory

- Class 2:

The static key (SCK) is loaded in all terminals, long lifetime

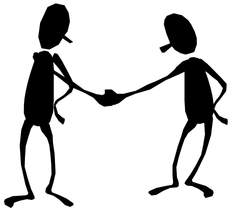
Always needed for DMO and base station Fall-back operation

- Class 3:

The dynamic key (DCK) produced automatically in every authentication

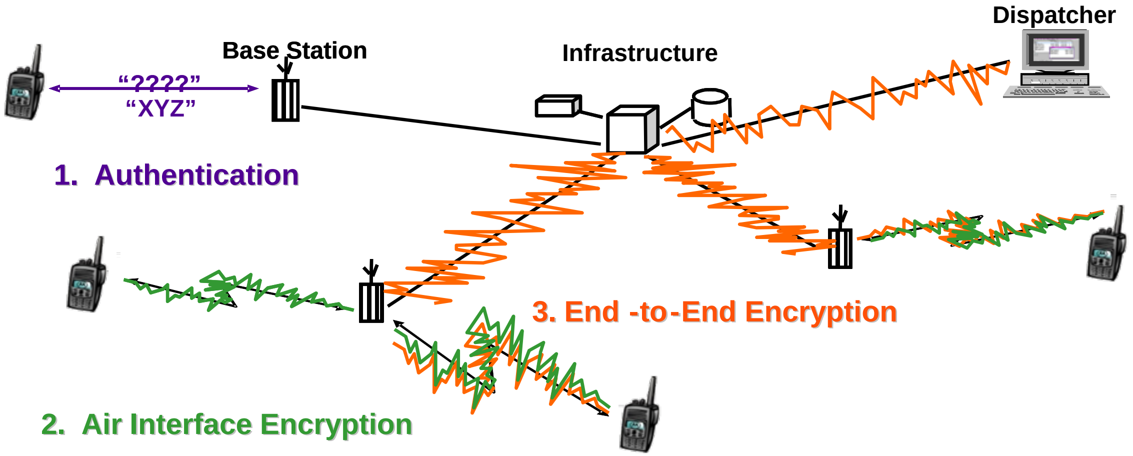
Group call downlink encrypted with common (CCK) or group specific (GCK) key, loaded over the air

Authentication



- Used to ensure that terminal is genuine and allowed on network
- Mutual authentication ensures that in addition to verifying the terminal, the SwMI can be trusted
- Authentication requires both SwMI and terminal have proof of unique secret key
- Terminals' secret keys are provisioned securely in accordance with SFPG Recommendation 01(Key distribution)
- Successful authentication permits further security related functions to be downloaded

Air interface encryption protection



- As well as protecting voice, SDS and packet data transmissions:
  - AI encryption protects voice and data payloads
  - Also protects signalling
  - Encrypted registration protects identities and gives anonymity to sensitive users
  - Protection against replay attack

Disabling of terminals

- Stolen and lost terminals can present a major threat to system security
- Disabling stops the terminal working as a radio and:
  - Permanent disabling removes all keys (including secret key)
  - Temporary disabling removes all traffic keys but allows ambience listening
- Relies on the integrity of the users to report losses quickly and accurately
- The network needs to be able to remember disabling commands to terminals that are not live on the network at the time of the original command being sent

Export control of crypto material

- All cryptographic material and terminals capable of encryption are subject to export control

- The export authority has to be satisfied that the key length and algorithms used are allowed to be exported to the end user

- Guidance is given in the Wassenaar arrangement www.wassenaar.org but the export control authority must be approached in all cases

Standard air interface algorithms

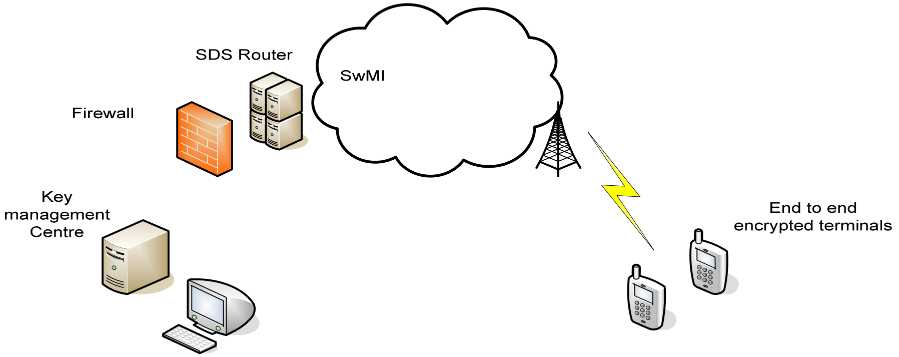
- Air interface encryption is designed to give the same degree of confidentiality as if a landline were used!
- The following algorithms have been designed for specific purposes
  - **TEA3**
    - For use by public safety and military organizations where TEA2 is not allowed. Strictly export controlled
  - **TEA2**
    - Only for use in Europe for public safety and military organizations. Strictly export controlled
  - **TEA1 and TEA4**
    - Generally exportable outside Europe. Designed for non public safety use
- Algorithms are “Secret” and (except TEA2) are owned by ETSI

End to end encryption

- End to end encryption is used for one of two reasons
  - It can protect user data messages across an untrusted infrastructure
  - If designed correctly it can provide enhanced confidentiality over all parts of the network
- Requires special terminals
  - e2ee on SIM card
  - or in tamper proof module
  - or in ASIC
- Protects
  - Voice services
  - SDS services
  - Packet data services
- Does not protect
  - Signalling
  - Identities
- Key management under control of user
  - Network provider has no knowledge of keys and key associations

Typical key management topography for e2e encryption

- Key management system must be in a secure environment
- Connectivity to LANs etc strictly controlled



- SDS type 4 service used for messaging
- All key management messages are encrypted
- Key load messages are always acknowledged so KMS knows which terminals have received the new keys
- All keys are stored in encrypted form on KMS

KMS functions

- Managing key associations
  - between talkgroups and traffic keys
- Re-keying radios
  - These need changing regularly
- Stunning/killing
  - Deletes traffic keys if stunned, deletes all keys if killed
- Logging-audit
  - Security rules insist on full accountability
- Interoperability

end-to-end encryption algorithms

- There are no ‘standard’ algorithms defined by SFPG but:
  - AES-128 has been adopted as the normally provided encryption algorithm for use with TETRA and test data and an example implementation has been produced. AES is license free
  - AES-256 has now been implemented by some terminal suppliers and gives a very high level of assurance for high levels of confidentiality protection
- Private algorithms may be implemented but there are restrictions on the export of cryptographic material and the export of equipment with a “hole” to insert cryptography
- Suppliers will be able to advise on the limitations and possibilities

Benefits of end to end encryption in combination with Air Interface encryption

- Both Air interface (AI) encryption and end to end encryption both have their limitations
- For most users AI security measures are completely adequate but the data is unencrypted within parts of the network and vulnerable to network operator eavesdropping
- Where either the network is untrusted, or the data is extremely sensitive then end to end encryption may be used in addition as an overlay.
- Brings the benefit of encrypting user addresses and signalling as well as user data across the Air Interface and high level of confidentiality of user data right across the network

Conclusion

- TETRA is designed for mission critical communications
- Security countermeasures built in from the start
- Extensive standardization has been undertaken resulting in a true multi-vendor terminal environment
- Network security is equally important!