Agenda

A: Security threats in mission critical networks
B: How the threats are addressed in TETRA systems?
C: Security mechanisms in TETRA
D: Preventing fraud and misuse
E. Summary
A: Security threats in mission critical networks
Five domains of information security

**Authenticity**
- The person is who he claims to be

**Confidentiality**
- Information is protected

**Integrity**
- The same correct data delivered to all recipients

**Availability**
- Information is always available

**Non-repudiation**
- Original source of information is always traceable
Possible attacks, threats & risks (1)

Message related threats:
- Eavesdropping the air interface, microwave links, …
- Eavesdropping in equipment rooms
- Eavesdropping with stolen radios
- Masquerading, false transmitters
- Replay of recorded old messages
- Personnel loyalty risks
Possible attacks, threats & risks (2)

System related threats:
- Jamming
- IP network attacks, denial of service
- Accidental damage to cables etc
- Vandalism, sabotage
- Natural disasters
- Equipment/system faults

User related threats:
- Traffic monitoring & analysis, monitoring of user density
B: How the threats are addressed in TETRA systems?
Authenticity

Authentication
- Radio terminals
- Dispatchers, network administrators
- Applications
- Playback of recorded air interface stream prevented
  - hyperframe number repeats only after 22 days

Authorisation
- Authenticated users can be authorised for different types of access or activities
- Administration rights
- Communication rights
- Managed group memberships

Only authorised persons can join communication
Confidentiality

Air Interface Encryption
– Between the terminal and base station

End-to-End Encryption
– Between the terminals end-to-end
– Infrastructure cannot open the messages
– Also fixed terminals like dispatcher workstations

Encryption within the infrastructure
– Transfer and storing of security information in system

Authentication Key Distribution
– Secure transfer from terminal factory to system

Physical security
– Protected security modules to handle sensitive data
Integrity

Transmission across air interface
  – Channel coding, error correction

Network elements
  – Transmission between network elements; protocols with error detection and re-transmission capability
  – Security information shall be noticed especially
  – Data recovery mechanisms; consistent data in different databases
  – Uncontrolled software cannot be used in the network elements

Dispatching data
  – Tracking the status of the radio terminals to give correct picture
  – Information on talk group members and activity always intact
  – Periodic registrations

Correct data delivered to everybody
Availability

Fault tolerant computing
- Recovery system
- Automatic replacement of faulty unit – no service breaks

Transmission link monitoring
- Automatic resending, rerouting and recovery

Priority access
- Defined important users always have access to the system
- Control channel load management
- Priorities, pre-emption
- Emergency calls are handled with special care

Base station fall-back capability

Direct Mode Operation
Non-repudiation

Recording and playback
  – Archive recording of all control room traffic
  – Monitoring of subscribers/one-to-one calls

Logging of management events
  – Logon passwords of administrator or dispatcher
  – All actions are written to system log
  – Actions can be traced

Accounting capability
  – Call Detailed Records (CDR) log all the used resources
  – Can be used also for billing, capacity planning etc.
C: Security mechanisms in TETRA

- **Digital transmission**
  - Modulation and frame structure
  - ACELP vocoder not “readable”

- **Authentication**
  - Authenticates the user
  - Can authenticate the system

- **Air Interface Encryption**
  - Protects the air link
  - Protects signalling and identities

- **End-to-End Encryption**
  - Protects the transmission lines
  - Protects inside equipment rooms
Digital transmission
Modulation and frame structure
ACELP vocoder not “readable”

Complementary measures:
- Terminal Disable/Enable
- Key protection
- Jamming detection
- VPN

Authentication
Authenticates the user
Can authenticate the system

Air Interface Encryption
Protects the air link
Protects signalling and identities

End-to-End Encryption
Protects the transmission lines
Protects inside equipment rooms

<table>
<thead>
<tr>
<th>CLASS</th>
<th>AUTHENTIC</th>
<th>ENCRYPT</th>
<th>OTAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Option</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>Option</td>
<td>Static</td>
<td>Option</td>
</tr>
<tr>
<td>3</td>
<td>Yes</td>
<td>Dynamic</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Authentication

- Prevents unauthorized access to TETRA network
- Based on specific secret code both in the radio terminal (MS) and in the TETRA network (SwMI)
- During registration the network automatically verifies that the radio terminal’s secret code matches with the one stored in the network
  - Failure to match stops the registration
- The secret code (K) is never transmitted over the air.
- Different authentication methods in TETRA:
  - SwMI authenticates the MS
  - MS authenticates the SwMI
  - Mutual authentication
Air interface encryption

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
- CCK can be cell specific to reduce commonality

<table>
<thead>
<tr>
<th>CLASS</th>
<th>ENCRYPT</th>
<th>AUTHENTIC</th>
<th>OTAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No</td>
<td>Option</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>Static</td>
<td>Option</td>
<td>Option</td>
</tr>
<tr>
<td>3</td>
<td>Dynamic</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Individual calls and group call uplink use individual keys
Group call downlink uses common key
Over The Air Re-keying (OTAR)

OTAR is needed in encrypted TETRA systems: CCK, SCK, GCK

CCK OTAR mechanism:
- CCKs are generated by the infrastructure
- One CCK is used in one or more cells
- CCK should be random and change frequently
- SwMI indicates in downlink the version of CCK to be used
- SwMI delivers CCK to MS individually, encrypted with DCK
- MS activates the new CCK when change happens in SwMI

Also SCK and GCK have OTAR mechanisms

OTAR is transparent to user
## Standard TETRA AIE algorithms

<table>
<thead>
<tr>
<th>PURPOSE</th>
<th>ALGORITHM</th>
<th>DISTRIBUTION &amp; CONTROL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>TAA1</td>
<td>General use, exportable</td>
</tr>
<tr>
<td>General encryption</td>
<td>TEA1</td>
<td>General use, exportable</td>
</tr>
<tr>
<td>European police encryption</td>
<td>TEA2</td>
<td>European police use, strict export control</td>
</tr>
<tr>
<td>General Public safety encryption</td>
<td>TEA3</td>
<td>Public Safety use outside Europe, strict export control</td>
</tr>
<tr>
<td>General encryption</td>
<td>TEA4</td>
<td>General use, exportable</td>
</tr>
</tbody>
</table>

Note 1: End user licence must be obtained for use of the algorithms – from custodian
Note 2: Export licence must be obtained for export of algorithms – from ministry
Export control information available at [www.wassenaar.org](http://www.wassenaar.org)
TETRA Key Distribution

Authentication key (K) is unique to terminal and known by the network, must be kept in secrecy

K must not be seen by human eyes to be secure

1. Terminal factory generates K’s for each REF (= radio serial number) in encrypted file and shows only the REF’s to operator
2. The encrypted REF-K file is loaded in the network
3. Operator programs TETRA number (ITSI) for each REF in the radio and in the system
4. Only the Authentication Module of the system knows the K for each ITSI, when the module is properly encrypted, nobody has seen K

Procedures defined in SFPG Rec 01 and TIP TTR001-14
End-to-end encryption

For most users the Class 3 AIE security is adequate
E2EE Protects messages across untrustworthy infrastructure
Protects the traffic only → should be used together with Air Interface Encryption to protect also user identities and signalling
TETRA gives possibility for national E2EE algorithms
Currently SFPG Recommendation covers example implementations with the popular 64 bit IDEA and 128 bit AES algorithms
Crypto module implementations in radios can vary

Questions to be considered before investing to E2EE:
- What is our main reason to use E2EE, against which threat?
- Does that justify the extra investment and operation cost?
D: Preventing fraud and misuse
To protect your system

Security is much about policy and processes

Countermeasures
- Implementation of TETRA security features
- Fraud detection systems and policies

Policies and guidelines
- Security Policy
- Security organization and security responsibilities
- Assets classification and control
- Personnel security
- Physical and environmental security
- Risk management
  - Potential attacks and countermeasures analysed
  - Especially interfaces to/from TETRA system analysed
  - Security audits
Security guideline documents

TETRA MoU Security and Fraud Prevention Group SFPG

- Recommendation 01, edition 4 'TETRA Key Distribution' (PUBLIC) and Annex on 'End-to-End Key Distribution' (R)
- Rec 02, edition 4 - End-to-End Encryption + Informative Annexes on IDEA and AES algorithms (R)
- Permanent Document 03, edition 2 - TETRA System Threat Analysis and Classification (R)
- Rec 04 - Implementation and Use of Security Features (R)
- Rec 06, edition 2 - Management of Long Life Air Interface Keys - GCK and SCK (R)
- Rec 07 - End-to-End Encrypted Short Data Service (R)
- Rec 08, edition 2 - Using a Smart Card for End-to-End Encryption (R)

(R) = Restricted to TETRA Association members and under NDA
E. Summary

1. Security functions are built in the TETRA standard from the beginning – they come as part of the package
2. Authentication prevents uncontrolled access
3. Air interface encryption protects both signalling and traffic
4. Key management comes without extra user effort
5. End-to-end encryption protects against system internal threats

Security is about much more than technology, it is about people and processes as well
Security must be analysed, planned and built in the operating procedures
Thank you!

www.etsi.org

www.tetramou.com

risto.toikkanen@eads.com