TETRA Security
Istanbul
February 2011

Brian Murgatroyd
Chairman ETSI TC TETRA
former chairman
Security and Fraud Prevention Group
(SFPG)

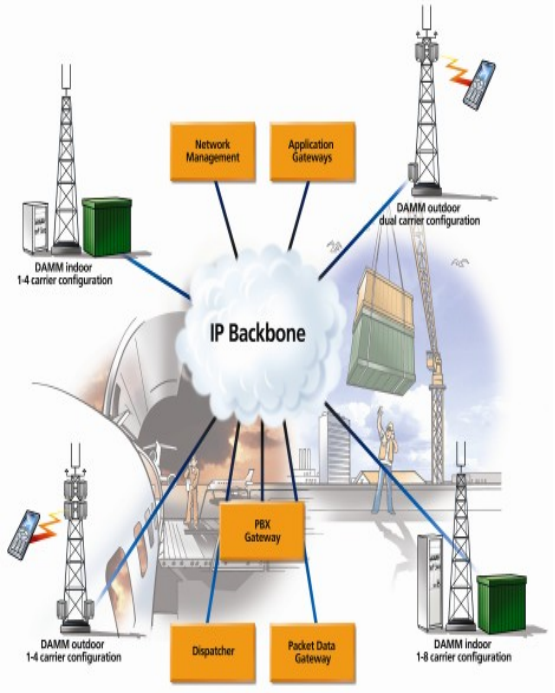
TETRA ASSOCIATION

Agenda

- Why do we need security countermeasures in communications systems?
- What are the practical security threats to TETRA systems?
- System security countermeasures
- Standard TETRA security features
  - Authentication
  - Air interface encryption
  - Terminal disabling
- Additional security measures
  - End to end encryption

Why is TETRA security important?

- Mission critical communications need security countermeasures to prevent data and intelligence falling into the hands of opponents and to maintain services when under attack
- GSM algorithm broken! Very active hacker group (Chaos Computer Club) are targetting systems. We know they are developing TETRA hacking equipment
- TETRA with no security allows an interceptor to find the terminals addresses and then register onto the system
- Tetra uses group communications and eavesdropping is much more serious than GSM
- Stealing a TETRA encryption key may reveal the communications of a large numbers of terminals
- End to end encryption allows users with widely varying needs to operate on a single system



Classes of Security Threats

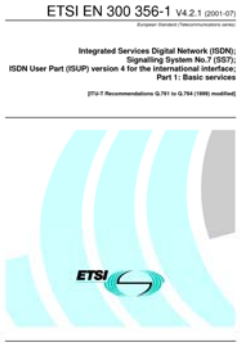
- **Availability.** **The most important threat type?**
  - Natural disasters, Denial of service(jamming, switching off network by illicit access)
- **Confidentiality.** **The best known threat?**
  - Eavesdropping, interception of radio path or network,
  - traffic analysis
- **Integrity.** **Is the terminal permitted on the network?**
  - 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 radio 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

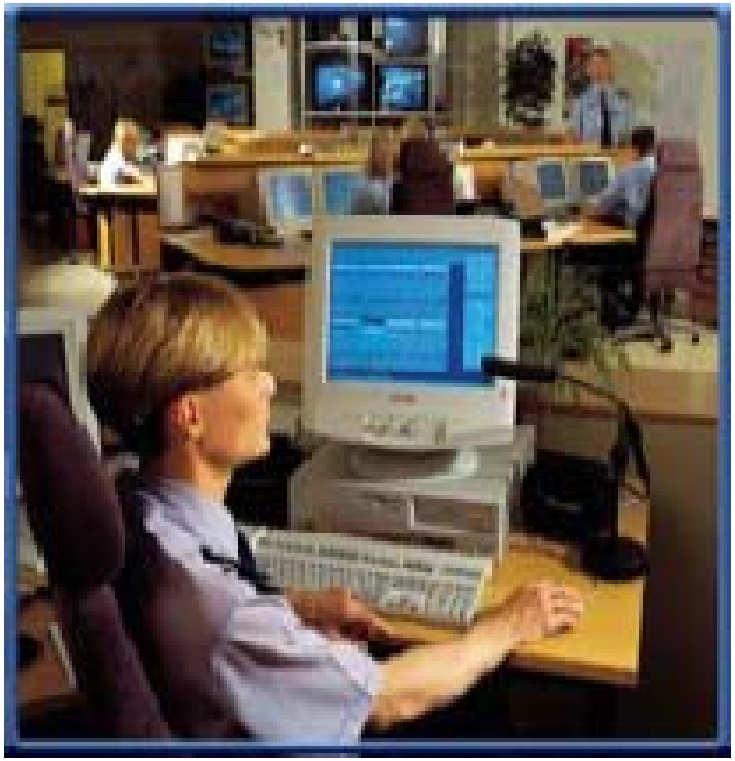
Importance of standardization in security countermeasures

- Security countermeasures must be standardized otherwise there can be no interoperability between different terminal makes and infrastructure suppliers
- 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



Network Security

- IT security is vital in TETRA networks particularly ıf IP based
- All access points represent a potential threat
- Gateways are very vulnerable
- Firewalls required at **all** access points to the network
- Network staff and maybe users need security screening (vetting)



Important TETRA communications security countermeasures

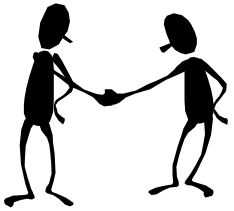
- Authentication - ensures only valid subscriber have access to the system and subscribers wi try and access the authorized system
- Air Interface Encryption – protects all signallin identity and traffic across the radio link
- Terminal disabling – ensures lost and stolen terminals are not a threat to 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

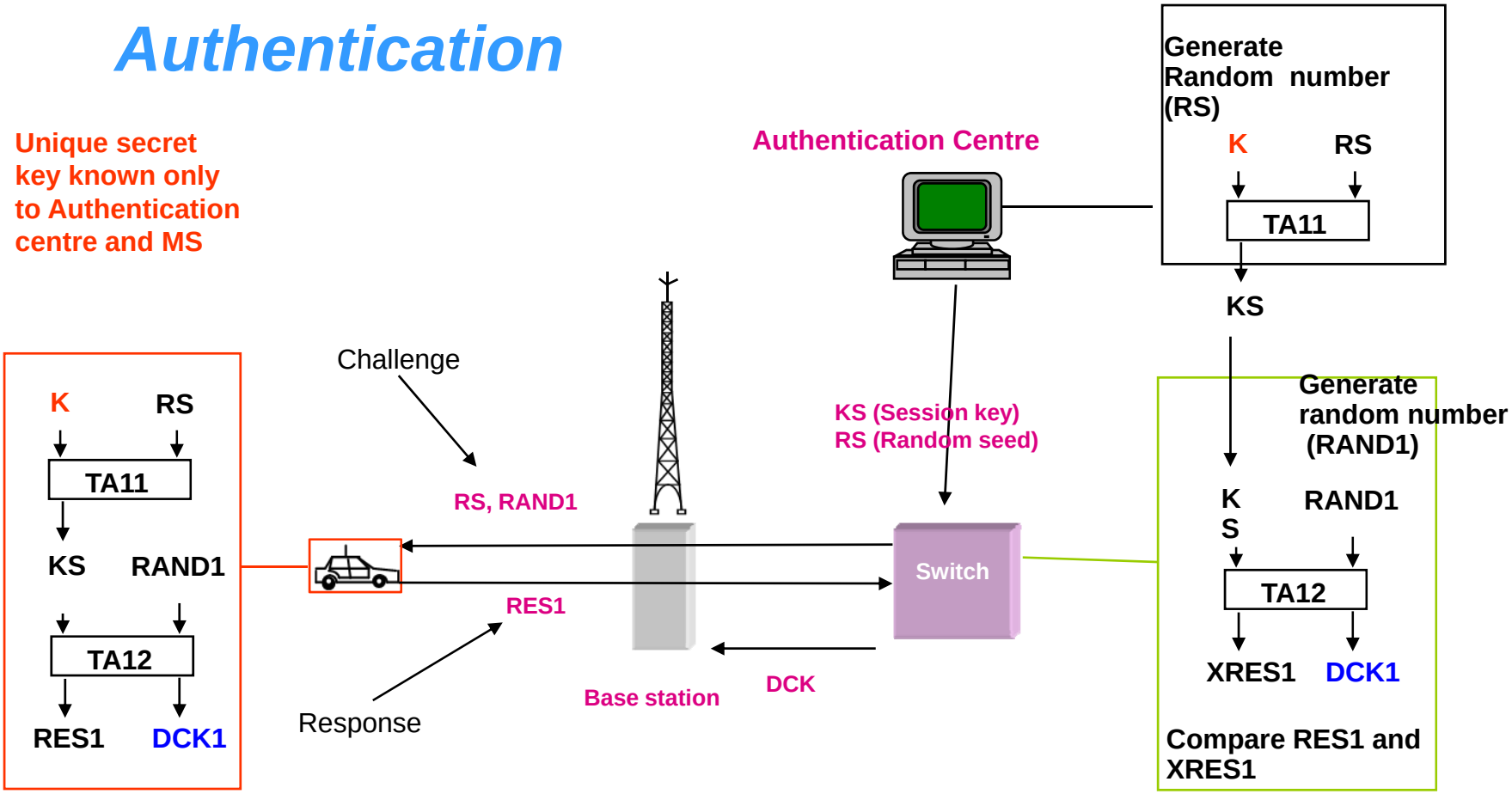
- Class 2: The static key (SCK) is loaded in all terminals, long lifetime. Always needed for DMO
- Class 3: The dynamic key (DCK) produced automatically in every authentication. Group call downlink encrypted with common (CCK) or group specific (GCK) key, loaded over the air
- Class 3 systems may fall back to class 2 under fallback conditions

Authentication

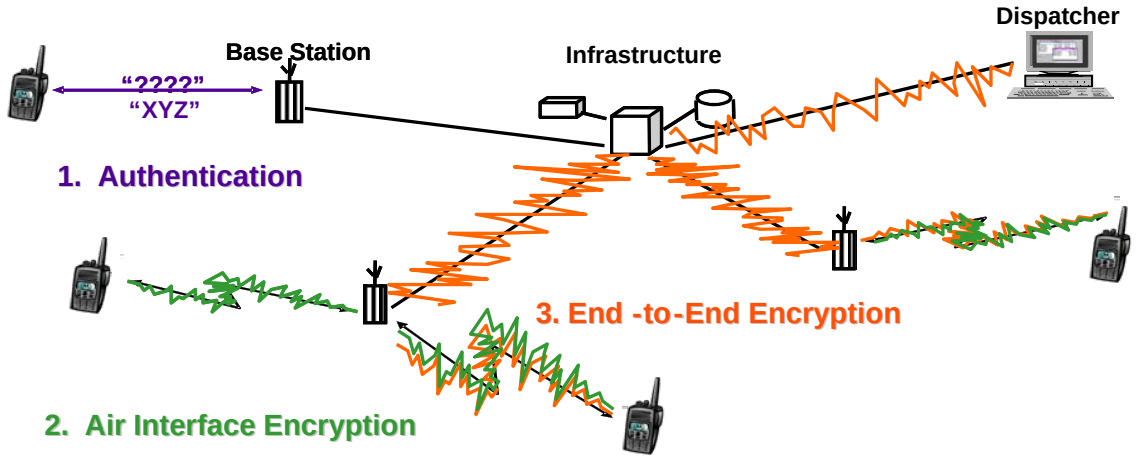


- Used to ensure that terminal is genuine and allowed on network
- Mutual authentication ensures that in addition to verifying the terminal, the SwMI can be trusted
- Authentication requires both SwMI and terminal have proof of unique secret key
- Successful authentication permits further security related functions to be downloaded

Authentication



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

Over The Air Re-keying (OTAR)

- Populations of terminals tend to be large and the only practical way to change encryption keys frequently is by OTAR
- This is done securely by using a derived cipher key or a session key to wrap the downloaded traffic key
- The security functionality is transparent to the user as the network provider would normally be responsible for OTAR and management of AI keys

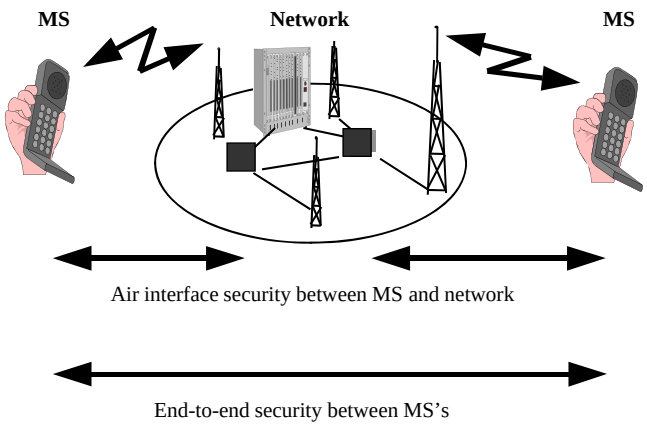
Standard air interface algorithms

- 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

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

End to end encryption



- Protects messages across an untrusted infrastructure
- Provides enhanced confidentiality over all parts of the network
- Protects
  - Voice services
  - SDS services
  - Packet data services
- Key management under control of user

Practical considerations for TETRA security

- Encryption is **easy** to implement
  - Some 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 from key management system
  - Must ensure connectivity is strictly controlled
  - Highly protected local security environment and sophisticated access control on Key Management System

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

- Air interface (AI) encryption alone and end to end encryption alone both have their limitations

- For most users AI security measures are completely adequate
- 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 confidentiality of user data right across the network

Questions

Thankyou