MBMS Security

A Summary of three contributions

SA3-020533, 534 & 535

Ericsson

Ericsson is proposing that SA3 endorses the following working assumptions for MBMS Security:

1. SA3-020533 (*Security protocol*)
   i. Security protocol at application layer
   ii. IETF SRTP as security protocol for streaming
2. SA3-020534 (*Key Management*)
   i. IETF MIKEY using pre-shared keys and symmetric crypto
3. SA3-020535 (*Push Re-keying*)
   i. IETF MIKEY is potentially extended to support LKH (Logical Key Hierarchy)

Security Protocol @ application layer:

- In SA3-020363 Alcatel suggests that application layer security to be adopted given that scalability issues can be solved
- Trust model is between the Home Network, the Content Provider and UE/Subscriber
- Access independent i.e. it can be over GERAN, UTRAN and WLAN
- SRTP
  - has been developed under a long time in IETF AVT WG
  - is on AVT WG Last Call
  - implementations are available
  - for connection less transfer
  - is secure for unicast and multicast RTP applications
  - gives high throughput and low packet extensions
  - no PKI is required
  - compatible with IETF Multicast

Key management:

Scenarios

- Ten o'clock news
- MTV-like streaming
- Stock prices

Requirements

- Efficiency – Re-keying & Registration
- Scalability
- Reliability

Components

- Symmetric based vs. Asymmetric based
- Depending on scenario re-keying might not be needed by Logical Key Hierarchy technology

Key management

Available Schemes (All in IETF last call):

- GDOI – Group Domain of Interpretation
  - **Registration and re-keying**
  - **Supports IPsec only. Other protocols then new RFCs are required**
  - **Requires PKI**
- GSAKMP-Light – Group Security Association and Key Management Protocol
  - **Registration and re-keying**
  - **Requires PKI**
  - **Pre-shared keys possible but requires RFC**
- MIKEY – Multimedia Internet KEYing
  - **Registration with pre-shared keys**
  - **Simple and fast**
  - **Has the concept of ‘SPI’ and ‘SA-lifetime’. Several keys can be handled.**
  - **New algorithms can be included**

Re-keying by LKH:

Logical Key Hierarchy (Push from BM-SC):

- For the MTV Scenarios i.e. continuous streaming
- Re-keying regularly
- Unicast: Traffic Encryption Key potentially to every member indicidually. Not efficient
- Multicast: Send the Traffic Encryption Key to several members of a group simultaneously. When r members is leaving it requires O(r) messages rather than O(n) messages
- Support for LKH should be included in MIKEY