DECOIT

World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI) 2008

WiMAX-Security

Assessment of the security mechanisms in IEEE 802.16d/e

Prof. Dr.-Ing. Kai-Oliver Detken
Company: DECOIT GmbH
URL: http://www.decoit.de
URL2: http://www.detken.net
E-Mail: detken@decoit.de

Consultancy & Internet Technologies

DECOIT

Table of Content

- Fixed and Mobile WiMAX
- Security Association
  - Authorization Security Associations
  - Data Security Associations
  - Encapsulation Protocol
  - Privacy Key Management Protocol (PKM)
- Security mechanisms and weaknesses
- Mobile WiMAX security extensions and comparison
- Conclusions

DECOIT

Fixed and mobile WiMax definition

- **Fixed WiMax:** 802.16 is often called 802.16d, since that was the working party that developed the standard. It is also frequently referred to as “fixed WiMAX” since it has no support for mobility.
- **Mobile WiMax:** 802.16e is an amendment to 802.16 and is often referred to in shortened form as 802.16e. It introduced support for mobility, amongst other things and is therefore also frequently called “mobile WiMAX”.

DECOIT

WiMax technology

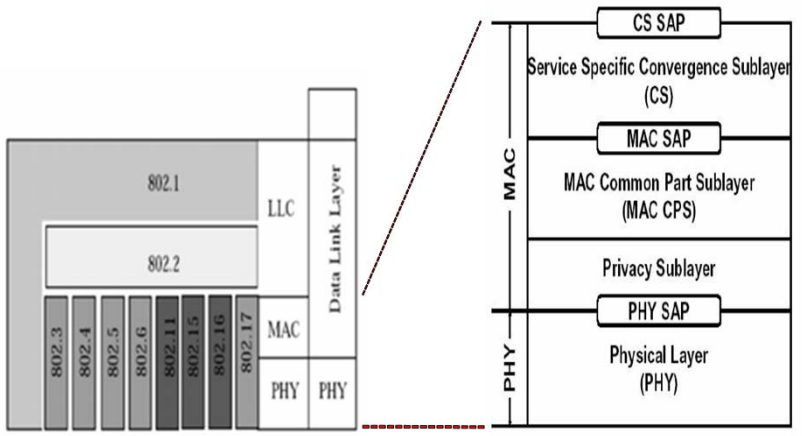
- Worldwide Interoperability for Microwave Access (WiMAX) defines a Point-to-Multipoint-Wireless network which operates within a range of 2 to 66 GHz
- Security is implemented in the so called Privacy Sublayer of the reference model
- The WiMAX security architecture uses numerous components and mechanisms
  - Digital certificate of the Subscriber Stations (X.509 standard, RFC-3280)
  - Security Associations
  - Encapsulation Protocol
  - Privacy Key Management Protocol
- WiMAX defines the layers PHY and MAC within ISO-OSI
  - The physical layer (PHY) handles signal connectivity, error correction, initial ranging, registration, bandwidth requests, and connection channels for management and data
  - The MAC layer manages connections and security

Security Association (1)

- A Security Association (SA) provides a set of security information by which secured communication between Subscriber Stations (SS) and Base Stations (BS) can be established
- By means of the SA, an SS is authorized for a WiMAX service
- There are three different SAs:
  - Primary: Management and data transport connections are mapped to these SAs and are secured according to the security mechanisms defined in the SAs
  - Dynamic: Dynamic SAs are dynamically generated by the BS and provided to the SS
  - Static: They are only initiated if the SS intends to use a new service and are dynamically terminated when data transfer in the service ends

Security Association (2)

- An SA, comprising a set of different security information, is described by a SA-descriptor
- This identifies the Primary SA, Static SA and Dynamic SA and contains the following information:
  - SAID (identifies the SA)
  - SA-Type (Primary, Dynamic or Static SA)
  - Cryptographic Suite: Data encryption, data authentication, and TEK encryption
- There are two SA-types:
  - Authorization Security Associations
  - Data Security Associations



Authorization Security Associations

- Authorization Security Associations are responsible for authorization of the SS. They are used by the BS in order to establish the Data SA between BS and SS. They consist of the following components
  - X.509-Certificate: Digital certificate serving for the identification of the SS.
  - Authorization Key (AK): Generated by the BS and used for the generation of the Key Encryption Keys (KEK), calculation of HMAC-Digests and HMAC-Digest verification on receiver side.
  - AK Sequence Number: Serves for the differentiation of successive AKs.
  - AK-Lifetime (32 Bit): Validity duration of an AK.
  - Key Encryption Key (KEK; 128 Bits): Used in the BS in order to encrypt the Traffic Encryption Key (TEK) from a Data SA and to transmit it. Furthermore, the SS uses the KEK to decrypt the encrypted TEKs, which is needed for data encryption.
  - HMAC-Digest: For the integrity check of exchanged key material. It is derived from the AK and guarantees, that SS and BS have the same AKs.
  - SA-Descriptor(s)

Data Security Associations

- Data SAs protect transport connections. They consist of the following security information:
  - SAID: SA-Identification
  - AK-Sequence Number
  - TEK-Parameter (two sets of key material), having the following values:
    - Traffic Encryption Key (TEK) for data encryption
    - TEK-Lifetime – remaining validity duration
    - 2-Bit TEK-Sequence Number
    - Initialisation Vector (IV) – a block of random numbers
    - Encryption algorithm (DES algorithm in CBC mode with 56-Bit keys, AES algorithm in CCM mode with 128-Bit keys)
  - HMAC-Digest

Encapsulation Protocol

- The Encapsulation Protocol enables encryption of data packets between BS and Subscriber Stations (SS)
- Therefore, it defines the cryptographic suites (cryptographic identifiers) for specifying encryption and authentication methods supported by the SS
- They are presented to the BS in form of a list of consecutive cryptographic suites
- A set consists of the packet data encryption/authentication algorithm and the encryption algorithm for the TEK
- Out of this list the BS selects a single suite and applies it for the Primary SA of the requesting SS

Privacy Key Management Protocol (PKM)

- PKM is responsible for normal authorization of the Subscriber Stations (SS), periodic re-authorization and reception/renewal of key material
- This protocol is comparable to a conventional Client-/Server-model where the SS (as PKM client) requests key material from the BS, which functions as PKM server
- With this mechanism the client (and thus each SS) only receives key material for those services the client is allowed respectively authorized for
- With the extension IEEE 802.16e of the standard the protocol has been modified and is denoted as PKM Version 1. With further modifications it was transformed to Version 2, which supports mobile SS exclusively in point-to-multi-point networks

Security mechanisms

- Authentication and authorization of the Subscriber Stations (SS) and the subsequent data encryption are based on a two-stage combination of symmetrical and asymmetrical encryption methods and PKM
- Communication between the SS and BS takes place in three phases:
  - Phase I: SS Authorization
  - Phase II: Exchange of Key Material
  - Phase III: Encrpytion of the Data Stream

Fixed WiMAX weaknesses (1)

- Authentication of the Subscriber Station (SS)
  - Lack of mutual authentication between SS and BS: SS authenticates itself through its certificate, however, the BS does not!
  - The attacker can generate his own Authorization Reply Message containing a self-generated Authorization Key and thus gain control over the communication of the attacked SS. This is a typical Man-in-the-Middle-Attack.
  - The BS can fall victim to a replay-attack by which the attacker intercepts an Authorization Request Message from an authorized SS and stores it.
  - DoS-attacks against the SS are also possible by repeatedly send Authorization Response Messages to the BS, burdening the BS with the effect that this declines the real/authentic SS.

Recommendations (1)

- Authentication of the Subscriber Station (SS)
  - Replay attacks: equip the Authorization Request Message with a time stamp together with a signature of the SS
  - An authentication of the BS could be achieved if a certificate of the BS is attached to the Authorization Reply Message
  - An alternative to the time stamp would be using a nonce by which the SS can be sure, that the Authorization Reply Message is the corresponding response to the Authorization Request Message. But the BS can not recognize whether the Authorization Request Message has been sent recently or is an old message
  - Nonce and time stamp are two essential methods for the verification of the timeliness (freshness) of messages

Fixed WiMAX weaknesses (2)

- Key Material Exchange Phase
  - After completion of the authorization phase, the SS requests key material (TEKs), necessary for data encryption. For this purpose, it periodically sends Key Request Messages referring to one of its valid SAIDs.
  - The BS replies with a Key Reply Message containing valid key material for the given SAID.
  - One potential replay-attack is possible due to the Key Sequence Number of the TEK, which has a length of only two Bits!
  - An attacker is able to capture TEK messages and replay them to gain information needed in order to decrypt data traffic.

Recommandations (2)

- Key Material Exchange Phase
  - Increasing the sequence number length: a bigger amount of TEK Sequence Numbers can be generated and transmitted within the longest validity duration of the Authorization Keys
  - Using 70 days as highest duration of an AK and 30 minutes as the smallest duration of a TEK, a Data SA could theoretically consume 3.360 TEKs over a complete AK-Lifetime

Mobile WiMAX security extensions (1)

- Authentication and Authorization
  - **Mutual Authentication:** PKMv2 introducing mutual authentication, giving both stations the possibility to check each other's identity.
  - **Authentication of User Data:** AES in CCM-Mode
  - **Control Message Protection:** AES based CMAC, or HMAC schemes
  - **Authorization:** generation of the Authorization Key (AK) within the Authorization Phase leads to a higher security level

Mobile WiMAX security extensions (2)

- **TEK 3-Way Handshake:** Mobile WiMAX improves the key material exchange procedure by means of the PKMv2 SA-TEK 3-Way Handshake either during initial authentication or handover
- **Encryption of Data:** IEEE 802.16e allows data encryption in four different ways. But the generic MAC header, MAC Management Messages, and the optional CRC-checksum are transmitted in plaintext.
- **Encryption of Keys:** TEK-encryption within PKMv2 can be carried out in four ways (3DES, RSA, AES-128 ECB, AES-128 Key Wrap)

Comparison 802.16d with 802.16e

- More development of security features has been invested in the security architecture of the newer standard IEEE 802.16e (Mobile WiMAX)
- Compared to IEEE 802.16d it is by far more secure and the improvements are obvious
- Most of the shortcomings have been eliminated
- By adding encryption methods and by introducing mutual station authentication, Mobile WiMAX can be judged as much more secure

DECOIT

Conclusions

- IEEE 802.16d provides a security architecture which basically secures the wireless link using different components such as X.509-certificates, Security Associations (SA), encryption methods, the Encapsulation Protocol, and the Privacy Key Management Protocol (PKM)
- IEEE 802.16d is mainly vulnerable in two phases:
  - Authentication
  - Key exchange phase
- Suggestions for countermeasures made by security analysts and researchers have to be considered respectively implemented in products
- Alternatively, the security mechanisms from IEEE 802.16e should be deployed in IEEE 802.16d implementations
- If applicable, users or network operators should deploy IEEE 802.1e

Thank you!

...for your attention.

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
Tel.: 0421-596064-0
Fax: 0421-596064-09

Consultancy & Internet Technologies