White Paper

Security in WiMAX 802.16-2009 networks

January 2011
Rev A4

*Security in data Networks is day by day a more important issue to have into account, specially in wireless Networks. This document is intended to describe the mechanisms established by the IEEE 802.16-2009 standard (**WiMAX**) to completely guarantee the security in communications. For that purpose, concepts such as X.509 certificates, digital signatures or dynamic keys will be explained.*

Wi-Fi (802.11a/b/g) is a very popular technology and it has generated a kind of distrust regarding to Security in wireless networks. Despite it is a very different technology compared to WiMAX, but since both are wireless technologies, a comparison between security implementation in WiMAX and Wi-Fi standard will be performed in this document, which will explain the security mechanisms implemented by Wi-Fi and why it is a more vulnerable technology than WiMAX.

INTRODUCTION

Basic security concepts in data Networks

When talking about Security in any kind of data network, three aspects need to be guaranteed:

- **Confidentiality**: it ensures that one message has not been read by anyone except than from the genuine receiver. For instance, a credit card number must be kept confidentially when it is sent through the Internet. An example of confidentiality mechanism is the data encryption: an encrypted message may only be read if a key which is only known by the sender and the receiver is applied to the message.
- **Authentication**: authentication is the verification of a claimed identity. For instance, when using a bank account, it is mandatory that only the real owner of the account may operate with it. There are several resources for providing authentication. One of the most common is a simple user/password-based system.
- **Integrity**: information must remain complete and free of accidental or deliberate manipulations. Integrity ensures that data is complete and precise and that it is not modified during the transmission from sender to receiver. Data integrity is intended, for instance, to guarantee that a electronic transference is performed with exactly the desired amount of money. An example of mechanism for ensuring data integrity is the digital signature in an email, an encryption method that guarantees the authorship of the message and the non-manipulation of its content.

Why is Security so important in WiMAX?

Security is always important in data networks, but it is particularly critical in wireless networks, and more specifically in those scenarios for which WiMAX technology has been designed, for many reasons:

- In wired networks, it is complicated to infiltrate illegally since a physical connection with cable is required. WiMAX is a wireless technology, and data are transmitted by means of radio waves through the air.
- WiMAX is an outdoor technology able to cover areas of several km^2. These relatively large areas are potentially exposed to an unauthorized access.
- WiMAX was not designed as a Local Area Network (LAN) technology. It was orientated to MAN/WAN networks. It is an operator technology intended to provide simultaneous service to multiple users. Therefore, users must not be able to access another users' information.
- As happens in every network, if someone strange gets into our own cell, there are always some risk that may be considered. For instance, our Internet connection may be used, computers and files may be observed, or information may be *sniffed* (e-mails, passwords,...). Having absolute control over the network access is therefore a critical issue.
- If a wireless unauthorized infiltration is already quite dangerous in a personal network, it has even worst consequences in a corporative, governmental or even military deployment, which are typical WiMAX scenarios. Most critical applications and environments require maximum security guarantees, and WiMAX must be able to provide that.

SECURITY IN WIMAX NETWORKS (IEEE 802.16-2009)

Introduction

Aware of the challenges and needs of security it would have to face, the *IEEE 802.16-2009* standard authors made a great effort to achieve a truly secure wireless technology. WiMAX defines on its protocol-stack a security sub-layer specifically dedicated to provide privacy, confidentiality and authentication to the final users. WiMAX security system is based on the principles of **Authentication** and **Encryption**, which make it a practically invulnerable technology nowadays.

Besides, this technology itself makes possible a more controlled and more secure medium access. These issues will be explained below.

Authentication

As already described, Authentication is used to guarantee the secure access, avoiding unauthorized users using the wireless connection. The *IEEE 802.16-2009* standard defines two authentication philosophies:

- **OSA (*Open System Authentication*):** the user makes an authentication request associated to its MAC address. Afterwards, the Base Station (BS) sends a reply message accepting or denying the query. The BS will only (and optionally) filter by MAC address.
- **SKA (*Shared Key Authentication*):** in this system shared keys are used for the authentication process. These keys must be known by both sides of the communication to guarantee a more secure authentication. These authentication mechanisms are described below.

For Shared Key Authentication, WiMAX defines the **PKM** (*Privacy Key Management*) protocol. This protocol allows the Subscriber Station (SS) to exchange keys and obtain information from the BS. PKM is also in charge of another issues like keys refresh, periodical re-authorization, etc. The Authentication process between BS and SS may be simply described as follows:

1) A SS sends a **PKM** (*Privacy Key Management*) message requesting for authentication to the BS and including its **X.509 digital certificate**. This certificate is unique for every unit and may not be falsified. Thus, it identifies univocally the CPE and avoids attacks based on MAC supplanting.
2) BS proceeds with the authentication procedure and verifies the certificate, checking the **digital signature** of the manufacturer, which is included in the certificate.
3) If the X.509 certificate is accepted, the BS generates the **Authentication Key** (AK) and **encrypts it** by means of the **1024 bits public-key**, contained in the X.509 certificate itself.

Encryption

After the BS authorizes the SS, additional encryption mechanisms are needed for assuring the data confidentiality and integrity . For this purpose, the SS sends to the BS a **request** for **encryption keys** called TEKs (*Traffic Encryption Keys*), which are sent by the BS in a response message. These messages are at the same time encrypted with a key that is only known by both parts. The algorithm used for encrypting the TEKs may be **3DES** (*Triple Data Encryption Standard*), **AES** (*Advanced Encryption Standard*), or **RSA**.

Once TEKs are known, several techniques may be used for data encryption: CBC(DES), CBC(AES), CTR (AES), CCM(AES).

Some of the advantages of the encryption mechanisms implemented by WiMAX (that are not implemented by other technologies) are:

- Use of very robust algorithms.
- Support of dynamic keys generation with a variable Time To Live.
- Independent encryption for each service flow allowed.

The objective of all these mechanisms is to guarantee confidentially in WiMAX networks.

X 509 digital certificates

A digital certificate is a digital document used by a reliable third-party certification authority for guaranteeing the true correspondence between the identity of a person or host, and its public key.

There are several formats for digital certificates, but one of the most popular standards is the **UIT-T X.509** (used also in the Spanish digital ID card, for instance). The certificate usually contains the name of the certificated entity, serial number, expiration time, a copy of the public key of the certificated owner (used for the verification of its digital signature) and the digital signature of the authorized certificate deliverer, so the receiver may verify that the deliverer has really established the association.

STATIC Keys: they are not renewed, highly vulnerable and easy to guess.

DYNAMIC Keys (WiMAX): they have a limited Time to Live. They are automatically changed and renewed, and they provide maximum security.

Extra security provided by WiMAX architecture

Regardless authentication or encryption mechanism, the design of the WIMAX standard itself implies an extra value when talking about security:

- Local Area Networks (LAN) were designed to interconnect "*friendly*" units in small environments, so they provide less robust security mechanisms (it is not usual that the potential "*enemy*" comes from inside the private LAN). On the contrary, WiMAX was not designed as a local network for providing access to the final user, but as a **MAN/WAN operator technology**, intended to connect a lot of users that may not be necessarily "*friends*". Since it is a large scale network, WiMAX technology itself was designed to ensure security with total guarantees.
- Medium Access is not random but completely **deterministic** and managed by a BS that acts like a, "*arbitrator*" controlling the transmissions all the time. Any unauthorized unit may indiscriminately transmit towards the BS or other SSs in the cell, flooding the radio medium. Thanks to it, DOS attacks (*Denial of Service*) are more difficult than in random-access technologies.

Solved questions about security in WiMAX

May an external host read the information travelling in my WiMAX network?

No. All the information travelling through the air is encrypted by the most robust encryption mechanisms (AES, 3DES…), based on dynamic keys. This fact guarantees the Confidentiality of the information.

May an external host access to the network?

No. Authentication is done by means of X.509 digital certificates and its respective digital signature, that corresponds to each one of the unit in the network univocally and may not be falsified.

May an external host perform "IP flooding" to the network? (invading massively the network with IP datagrams)?

No. WiMAX is an operator technology with deterministic access where the BS controls every transmission, so a *hacker* may never overwhelm any unit in the network.

COMPARISON WITH WI-FI (IEEE 802.11 a/b/g)

Authentication and Encryption

When a unit wants to access a Wi-Fi network, first thing needed is to associate with an Access Point (AP). Thus, it is the AP the one which **authenticates** the unit. The IEEE 802.11 standard considers the two Authentication philosophies: **OSA** and **SKA**. Besides Authentication, encryption mechanisms for guaranteeing confidentiality and data integrity are also added.

Most popular Authentication and Encryption systems defined in Wi-Fi are:

- **WEP** (*Wired Equivalent Privacy*): it is an authentication and encryption system that codifies data with a shared static key (64, 128 o 256 bits) before they are sent through the air. This key is exactly the same for every wireless station and for the AP. This technique has shown a huge vulnerability caused by several reasons (static key, initialization vector repeated and not encrypted, ...), which has led in a very easy-to-crack protection.
- **WPA** (*WiFi Protected Access*): it provides improvements respect WEP algorithm like dynamic generation of the access key. Basic networks frequently use a simpler version of WPA, called **WPA-PSK** (*Pre-Shared Key*), that implements the same shared key in every unit. WPA uses **RC4** as Encryption algorithm and **TKIP** (*Temporary Key Integrity Protocol*) as key management algorithm. To mention some defects, it may be said that TKIP has some vulnerabilities because it allows access to some of the messages from the AP to the network users.
- **WPA2**: it is a relative improvement of WPA and is the certificated version of IEEE 802.11i Standard. It uses **CCMP (AES)** (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol + Advanced Encryption Standard*) as encryption algorithm. Today, it is the most reliable security protocol in Wi-Fi, and it is implemented by a big part of the new Wi-Fi equipment. The disadvantage is that it may not be supported by more ancient equipment.

Problems generated by Medium Access

Medium access in IEEE 802.11 b/g is based on **CSMA/CA** (*Carrier Sense, Multiple Access, Collision Avoidance)* protocol, in which units transmit when they think there is absence of other traffic in the shared medium. It is therefore a random and uncontrolled medium access. Having a limited radio-electric spectrum, a non authenticated user might flood the air with "rubbish traffic", a classical attack in Wi-Fi networks that may have different purposes, like DOS (*Denial of Service*) attacks or packet sniffing for capturing network traffic.

These kind of attacks may not be solved with more sophisticated encryption mechanisms, because they are inherent problems of random medium access technology itself, and as a consequence, avoiding them is not possible.

CONCLUSSIONS

The most interesting issues explained in the document will be summarized below:

1) Authentication

Authentication in WiMAX is very reliable thanks to the **X.509 certificates** and the **digital signatures**, that univocally define every user that is trying to enter the cell, as well as the **dynamic keys** that change periodically, and the **automatic re-authentication requests** in the BS. These certificates cannot not be falsified, and prevent any unauthorized unit entering the WiMAX cell.

WEP authentication and encryption technology using **static keys** has resulted as a big security failure in Wi-Fi, since it has become incredibly vulnerable. Any network using this system today is exposed to many types of *cracking* attacks. Despite WPA and WPA2 have solved a big part of the problems caused by WEP mechanism, Wi-Fi equipment must be quite modern to use them, so older network equipment may only support WEP. Besides, the truth is that, because of the lack of knowledge, many people keep using WEP without knowing its high risks.

2) Encryption

WiMAX uses basic block ciphers: **AES** and **DES**. The complexity of the algorithms is related to the way of selecting, transposing and relating the blocks in a message. In fact, and being strict, WiMAX uses CBC(DES), CBC (AES), CTR(AES), CCM(AES). It is not that these techniques are technologically superior to others (like Wi-Fi's), but that they are correctly used (they use **dynamic keys** that **expire after a time to live** and are **automatically renewed**, without repeating initialization vectors, encrypting every SS's service flow independently, etc...).

WEP and WPA in Wi-Fi have proved important vulnerabilities regarding encryption, and they may only perform a encryption comparable to in WiMAX by using **WPA2**.

3) Medium Access

Technology itself has a great impact in Security. WiMAX implements a totally **deterministic** Medium Access, permanently **controlled** by the BS. No station may transmit a single bit if it has not been previously allowed by the BS, so the radio spectrum is automatically controlled and many kind of attacks are avoided.

Other technologies, like Wi-Fi and its MAC layer based on CSMA/CA, use **random** and **uncontrolled** Medium Access, which leads in the possibility of any user flooding the air with traffic, even though it is not registered in the AP. This makes these networks more vulnerable to many DOS (*Denial Of Service*) attacks.

4) Operator technology: MAN/WAN vs LAN

WiMAX was not designed as a LAN technology, it was designed to be an **operator** technology for **MAN** or **WAN** (*Metropolitan*, *Wide-Area*) networks. This implies outdoor environments performance, big coverage areas, service to multiple independent users,… and therefore the standard developers were very aware of how important security was. WiMAX was thoroughly created to achieve a complete absence of any kind of vulnerability and a guarantee of Integrity, Confidentiality and Authentication by itself. In fact, WiMAX is nowadays used in military environments where maximum security is required.

Wi-Fi is a very different technology and it is intended for other purposes: it is directly orientated to everyone, pioneer in wireless networks and specially designed for small local networks, so it was born with lacks regarding Security aspects. Besides, its success has led in having millions of Wi-Fi stations all around the world, and it has become a low cost and affordable technology for most of the people. This has many advantages but implies some risks: when increasing the number of units it is obvious to think that more potentially *hackers* may appear. The hacker community specialized in breaking Wi-Fi networks is quite large and many applications are specifically designed for it, while WiMAX world, for the time being, is not suffering these issues.

5) Extra security not required

Lacks in Security in other technologies may be mitigated by using specific high level security protocols or additional equipment and servers: Radius, Kerberos, PAP(LDAP), EAP, … These "external" elements increase Security but require extra equipment and additional costs. If the standard itself already implements the necessary Security mechanisms, like WiMAX does, it would be easier and more cost-efficient to deploy a secure network without requiring any other methods.