WiMAX Security – A Formal Analysis using Scyther tool

Kahya Noudjoud, Debbah Adel and Nacira Ghoualmi

***Abstract*—The** Worldwide Interoperability for Microwave Access (WiMAX) is a norm of computer network for long distance communication by radio wave, belonging to the family of 802.16 standards. The fact of using the free space as a broadcast channel for data makes wireless networks more vulnerable than wired networks. The former IEEE 802.16 standards used the Privacy and Key Management (PKM) protocol which had many critical drawbacks. In IEEE 802.16e, a new version of this protocol called PKMv2 is released. The security problems still persist and many additional flaws have emerged. In our paper we made a formal analysis of authentication protocol WiMAX (PKMv1 and v2) and proposed a new protocol more reliable and secure. The formal analysis has been conducted using a specialized model checker Scyther, which provides formal proofs of the security protocol.

***Keywords*—** IEEE 802.16, vulnerability, PKM, Analyze formal, Scyther tool.

I. Introduction

WORLDWIDE Interoperability for Microwave Access (WiMAX) was proposed to provide high speed data distribution through Wireless Metropolitan Area Networks (WMANs), with the advantages of rapid deployment, high scalability, and low upgrade cost. It also provides high throughput broadband connections over long distances. WiMAX also known as IEEE 802.16 standard for Metropolitan Area Networks. First published in 2002,802.16 [1] gives the specifications for the air interface allowing Point-to-Point and Point-to-Multipoint Broadband Wireless Access in the 10–66 GHz frequency band under LOS conditions. In 2004, IEEE 802.16d [2] was published to address the requirements of fixed BWA under NLOS conditions in 2–11 GHz. An amendment to IEEE 802.16d was published to address the provision of mobility in 2005 under the title Mobile WiMAX or IEEE 802.16e which also operates in 2-11 GHz band under NLOS conditions.

The security features of the IEEE 802.16 standard lie in the privacy sub-layer which is integral to the MAC layer of the system. The privacy sub-layer provides the Mobile Station (MS) with security capabilities and protects the Base Station (BS) from malicious attacks that may disrupt its services.

Kahya Noudjoud is in Networks and Systems Laboratory (LRS) Badji Mokhtar University, Annaba, Algeria

Debbah Adel is in Networks and Systems Laboratory (LRS) Badji Mokhtar University, Annaba, Algeria

Nacira Ghoualmi is in Networks and Systems Laboratory (LRS) Badji Mokhtar University, Annaba, Algeria.

Although the privacy sub-layer of the IEEE 802.16e- 2005 [3] standard has addressed weaknesses found in previous versions and has increased the overall security of the system, many more vulnerabilities still remain and causes the standard to be susceptible to attacks on its integrity and availability.

Many attacks are identified on Privacy Key Management (PKM) during authentication. The potential attacks that can be carried out are replay attack, DoS and man-in-the-middle attack which is generally applicable in a communication protocol when mutual authentication is absent [4].

In this paper, we present an overview of security flaws in the existing protocol (PKMv1 & v2), and propose a new protocol to take care of the security of MS and BS and the service availability. At first we give a full description of the PKM protocol (V1 and V2) then we analyze both protocols informally. Next we apply formal methods [5] on the authentication protocols using the Scyther tool [6] to extract extra holes or threat that might exist.

The proposed protocol will address some security issues which can be fatal to the entire communication process. This protocol will be also analyzed formally using scyther tool.

The rest of the paper is organized as follows. Section II presents a description of the protocol and provides an overview of existing attacks. In Section III, we formally verify the security of the PKMv1 and PKMv2 authentication protocols, using Scyther. Section IV introduces the proposed revised authentication protocol and his formal analysis. Section V concludes the paper.

II. WiMAX SECURITY

The IEEE 802.16 PKM protocol provide the authorization process and secure distribution of keying data from the BS (base station) to MS (mobile station). BS uses the protocol to enforce conditional access to network services. Privacy and Key Management (PKM) protocol uses X.509 digital certificates, RSA public-key algorithm, and strong encryption algorithm to perform key exchanges between SS and BS, at client/server model. IEEE 802.16 PKM employs two-tier key systems. The Authentication Protocol first authenticates SS to BS, establishing a shared secret (Authorization Key, AK) via public-key cryptography; then via Key Management Protocol, SS registers to the network, during which AK is used to secure the exchange of Transport Encryption Keys (TEK).

A. PKMv1Authentication Protocol

In the first version of the IEEE 802.16 standard, the authorization protocol used in PKM is basically 3 way handshake protocol between the MS and BS.

The MS sends a message to BS, which contains an X.509 certificate (identifying the MS's manufacturer). BS is using this message in order to decide if the particular MS is a trusted device. 802.16 design defines that all devices from a trusted manufacturer can be trusted. MS sends a second message without waiting for an answer from BS. This second message contains the MS's X.509 certificate and its public key, the MS's Security capabilities and its SAID (Security Association Identity). The X.509 certificates are used for the BS to know if the MS is authorized. MS's public key is used by the BS to form the reply message. If BS determines that the MS is authorized then it replies with a third message, which initiates an SA (security association) between the BS and MS. BS generates Authentication Key (AK) which encrypted with the MS's public key, a 4-bit sequence number, used to distinguish between successive generations of AKs, and a list of SAIDs which contains the identities and the properties of the SA list the MS authorized to access. If AK is used correctly, then MS gains the authorization to access the WMAN channel. The 802.16 designs assume that BS and MS share the secure AK.

B. Analysis of PKMv1 Attacks

The second message is sent in plaintext but eavesdropping is possible as the information is almost public and is preferred to be sent in plaintext to facilitate authentication. However, the BS may face a replay attack from an adversary who intercepts and saves the authentication messages sent by a legitimate MS previously.

An adversary eavesdropping the messages cannot derive the AK from message 3 as it does not have the corresponding private key. However, the adversary still can replay message 2 multiple times, thus either exhausts BS's capabilities or forces the BS to deny the MS who owns that MS's certificate Cert(MS) The reason is that, if BS sets a timeout value which makes the BS reject the authorization request from the same MS in a certain period, the legitimate request from the victim MS will also be ignored. In this case a denial of service attack occurs to the victim MS.

The obvious flaw of the existing IEEE 802.16 security design is the lack of a BS certificate. The only way to defend the client against forgery or replay attack is to replace the standards authentication scheme with a scheme providing mutual authentication. Mutual authentication is required for any wireless medium to avoid security threats whether it is dynamic or static.

C. PKMv2 Authentication Protocol

The latest standard IEEE 802.16e-2005 proposes PKMv2, in which one additional message is added at the end of the original protocol. The MS initiates the RSA-based mutual authentication process by sending two messages. The first message contains the manufacturer X.509 certificate. The second, authorization request message, contains the MS's X.509 certificate, 64-bit MS random number Ns, list of security capabilities that the MS supports, the SAID and the MS signature. If the MS is authenticated and authorized to join the network, the BS sends an authorization reply message. In the response message, the BS includes the 64-bit MS random number Ns received, its own 64-bit random number Nb, a 256-bit key pre-primary authorization key (pre-PAK) encrypted with the MS's public key, the pre-PAK key lifetime and its sequence number, a list of SAIDs (one or more), the BS's X.509 certificate and BS's signature in the authorization reply. The MS verifies liveness by comparing the Ns it sent with the received Ns in the authorization response message. It then extracts the PAK, because only the authorized MS can extract the PAK. This can be used as a proof of authorization.

Finally, the last message of this authentication is send by the MS to confirm the authentication of the BS. The MS includes the BS random number Nb received in the authorization response message, used to proof liveness, the MS's MAC address and a cryptographic checksum of the message. At the end of the RSA authorization exchange, both MS and BS are authenticated by each other.

D.Analysis of PKMv2 Attacks

Though PKMv2 allows mutual authentication to protect from forgery attacks, but we can find there is no mechanism to ensure integrity and non repudiation in the authorization process. In the Authorization request/reply message, if anyone with a properly positioned radio receiver catches the message, no digest is used to prove that the messages have not been changed by others and nothing is used to make sure the sender cannot repudiate the message. An attacker could forge new frames and capture, modify, and retransmit frames from authorized parties. Without MS signature, the request message is easy to be modified or impersonated. This is similar to what we discussed before on PKMv1 and we refer to it as simple replay attack. Even with the signature from MS served as message authentication, attack still exists. Such attack is similar to the one proposed in [7], A new attack on the original X.509 3- way authentication protocol was found by [8] when one agent is mistaken about the multiplicity of sessions. This attack can be eliminated by adding the BS's identity.

From the above discussion, we can conclude that Basic PKM has many flaws such that it provides almost no guarantees to MS about the AK. PKMv2 adds an additional message at the end of the protocol, intending to assure BS the freshness of the first message. However, this goal fails and interleaving attack still applies. So we can conclude that the MS's signature and the BS's certificate are critical to all versions of authentication protocols.

III. FORMAL ANALYSIS USING SCYTHER TOOL

Scyther is an automated security protocol checking, which has proven to be an effective tool for verification,

falsification, and analysis of security protocols. It can verify protocols with unbounded number of sessions, with guaranteed termination.

As well, it is the only currently existing tool capable of verifying synchronization [9]. Synchronization expresses that the messages are transmitted exactly as prescribed by the protocol description. In other words, whenever an initiator I completes a run of the protocol with responder R, and R has been running the protocol with I. Then, all messages are received exactly as they were sent, in the order as described by the protocol. Synchronization is a strictly stronger property than agreement for the standard intruder model, because it can be used to detect suppress-replay attacks (also known as preplay attacks).

Scyther uses backward symbolic state search technique to analyze security protocols. The backward symbolic state search technique which uses the Arachne engine, based on the Athena method [9]. The Arachne engine finds attacks by searching backwards from the claim that is broken. This technique allows full type flaws and can explore infinite state spaces. Contrary to Athena, Scyther can verify authentication properties such as synchronization as described, and can handle non-atomic keys and multiple key structures. In this section, we formally verify our analysis on different versions of PKM protocols using scyther.

A. Properties Specifications

Pseudonymity, information confidentiality, no theft of service possible [5] and secrecy and uniqueness of the session keys are selected for formal verification. The goals of the authentication protocol should be:

1) Pseudonymity: This claim is fulfilled if an outsider, who keeps track of the communication, cannot relate the traffic to a specific MS. In order to fulfill pseudonymity the MAC address of the MS which identifies it must remain secret. The MAC address is included in the MS's certificate (MsCert). The formal definition of pseudonymity is given below.

Property 1: *{claim (MS, Secret, BsCert)}*

2) Information confidentiality: This claim is fulfilled if the MS has the guarantee that all exchanged user data is secret. The exchanged user data messages between the MS and the BS is called Msg. Every information (α) in Message should remain secret. The formalization of information confidentiality is given below.

Property 2: ∀α∈Msg (claim (MS, Secret, α))

3) No theft of Service possible: This claim is fulfilled if the BS has the guarantee that neither an unauthenticated user should gain access to the services provided, nor should an unauthenticated user be able to impersonate another user. A service should always be bound to an authenticated user. This claim is similar to information confidentiality. Its formal definition is given as follows:

Property 3: *∀α∈Msg (claim (BS, Secret, α))*

4) Secrecy and uniqueness of the session keys: This claim is fulfilled if the BS and the MS have the guarantee that all exchanged keys (described as key) are secret and unique. We have included an additional restriction that only claims concerning sessions between trusted agents are evaluated. Its formal definition is shown as follows:

Property 4*:∀key (claim (BS|MS, Secret, key))*

Formal Verification

1) PKMv1 Authentication Protocol: The formal definition of the authentication scenario of PKMv1 described above is shown as follows:

MS⟶ BS: Mancert (MS);

MS⟶BS: MsCert, Capabilities, SAID;

BS⟶MS :{ AK}pk(Ms), SAIDlist, AKSeqno;

This model is going to be challenged with the following requirements using the Scyther tool:

1. *Property 1:* Scyther detected a possible attack, as an intruder eavesdrops the second message and obtains the MS's certificate (MsCert) [5].

2. Property 2: Scyther identified problems in the authentication protocol, as the MS does not authenticate the BS and so the MS has no way of knowing whether the entity sending the AK is a legitimate BS or not. This design lack opens the protocol to forgery attacks, where an unauthorized

BS can communicate with a MS (MS thinks it is communicating with the trusted BS). The result is that the intruder can decrypt the information needed.

3. Property 3: It is proved that unauthenticated user cannot access the services provided, and cannot impersonate another user. The BS uses the certificate of the MS to determine if the MS is authorized, then sends the AK encrypted with the public key of the MS. This guarantees that only the specific MS can decrypt the AK.

4. Property 4: It is proved that an adversary cannot obtain the unique AK as it is encrypted with the public key of the MS. AK is proved to be unique using synchronization claim and the fact that AK is a constant in one of the roles appearing only in one send event.

2) PKMv2 Authentication Protocol: The formal definition of the PKMv2 authentication protocol is shown as follows:

MS⟶BS: Mancert (MS);

MS⟶BS {MsCert,Capabilities,SAID,Ns}sk(MS)

BS⟶MS:{{prePAK}pk(MS),SAIDlist,Ns,Nb, prePAKSeq prePAKlifetime,BsCert}sk(BS);

MS ⟶BS :{Nb}sk(MS);

This model is going to be challenged with the following requirements using the Scyther tool, as in PKMv1:

1. Property 1: A possible attack is detected as in PKMv1, as an intruder eavesdrops the second message and obtains the MS certificate (MsCert).

2. Property 2: it is proved that the authorization key exchanged in the authentication protocol is secret and not broken if the backward compatibility to PKMv1 is disabled [5].

3. Property 3: It is proved that unauthenticated user cannot access the services provided, and cannot impersonate another user. Also, it is not possible to modify the data by an unauthorized individual.

4. *Property 4:* It is proved that an adversary cannot obtain

the unique pre-PAK, which will be used to extract the PAK, as it is encrypted with the public key of the MS. Also pre-PAK is proved to be unique because of synchronization and the fact that pre-PAK is a constant in one of the roles appearing only in one send event, accompanied within a signature by the recipient's nonce.

As seen in the formal analysis, the secrecy and uniqueness of the keying material distributed and the no theft of service possible claims are valid in both PKMv1 and PKMv2. However, pseudonymity and information confidentiality are broken in both versions of PKM.

IV. THE PROPOSED REVISED AUTHENTICATION PROTOCOL

As discussed in the previous section, the existing protocol does not fulfill the claims pseudonymity and information confidentiality because it still vulnerable to replay, DoS and Man-in-the-middle. Some solutions are introduced to solve those problems in our new revised protocol. To prevent replay and man-in-the-middle attacks we add timestamp. The problem with timestamp is that it requires time synchronization between MS and BS. In the wireless scenario, time synchronization is considered to be difficult (particularly under mobility). But In IEEE 802.16(e), it is assumed that time synchronization is done between MS and BS.

Nonce is a possible alternative to timestamps for use in the authentication protocols. Nonce shows that the request queued were not used before. Timestamp identifies which request are the newer one and also the time sent by the MS and BS.

Nonce will not give any information about the time that was sent. Nonce is also not sufficient to tell the BS that it is the current message received from the MS. There are two problems with the protocol that has timestamps only. An adversary can easily capture the timestamp of MS by listening to message 2. The time adjustment can be done by the adversary accordingly. Hence the scope of man in middle attack is persists with timestamp added protocol. To prevent security threats like replay attacks, DoS attack and Man-in-the-middle attack, both nonce and time stamp are needed. So the revised protocol has the timestamp attached with the MS message to the BS along with the nonce. *The protocol is shown as follows:*

MS sends a message to BS, which contains an X.509 certificate identifying MS's manufacturer. BS is using this message in order to decide if the particular MS is a trusted device or not. MS sends a second message without waiting for an answer from the BS. This second message contains the MS certificate (MsCert) and a nonce (Ns1) used for identification, both are encrypted with the public key of the BS pk(Bs), it also contains the timestamp of MS and generated nonce of MS along with SAID and its security capabilities. MS signs the message ensuring the BS that he/she is not an adversary with her private key sk(MS), the time stamp addition could bring an extra layer of security since the BS could identify the message as current one. The time stamp could avoid the intruders who are trying to synchronize time with either BS or MS. If BS determines that the MS is authorized it replies with a message. BS sends a generated nonce along with nonce which was sent by the MS. That could ensure MS that message3 is the reply of the request send by MS itself. BS Nonce ensures the MS about the authentication of BS. This mutual authentication gives extra layer of security. BS sends a pre-AK encrypted with the secret key of BS sk(Bs), The AK is derived from Pre-AK. Use of Pre-AK gives the opportunity to avoid AK sending in raw format (though encrypted with the public key). From pre-PAK, the MS generates AK. If AK is used correctly, then MS gains the authorization to access the WMAN channel. The Lifetime of Pre-AK and Sequence no of pre-AK are sent in message3. This protocol using the public key of MS in message3 ensures MS that the message received is from a legitimate BS. As this message sends the BS certificate, the MS is now sure that the message is not copied by the adversaries.MS sends its Timestamp and the nonce of BS previously received to confirm authorization access.

MS signs the message with its private key.

Formal analysis of the revised authentication protocol

The formal definition of the revised authentication protocol is shown as follows:

MS⟶BS:Mancert(MS);

MS⟶BS:{{MSsCert,Ns1}pk(BS),Capabilities, SAID,Tms,Ns}sk(MS);

BS⟶MS:{{prePAK}sk(Bs),SAIDlist,Tms,Tbs, Ns,Nb,prePAKSeq,prePAKlifetime,BsCert}pk(MS);

MS⟶BS:{Nb,Tms }sk(MS);

In this section, we formally verify the correctness of our reversion. We model the revised authentication protocol in Scyther tool and we verify if the four properties (claim events) are respected.

1. *Property 1:* In the formal analysis it is proved that an intruder cannot obtain the MS certificate (MsCert).

2. Property 2: In the formal analysis it is proved that the authorization key exchanged in the authentication protocol is secret and not broken

3. Property 3: It is proved that unauthenticated user cannot access the services provided, and cannot impersonate another user. Also, it is not possible to modify the data by an unauthorized individual.

4. *Property 4:* It is proved that an adversary cannot obtain the unique pre-PAK.

In our version it is also proved that an adversary cannot obtain the unique pre-PAK. Timestamp and nonce are used in the revised protocol to prevent replay and man-in-the-middle attack. The MS appends the time stamp and nonce. This helps the BS to identify the request as a newer one. The nonce will wipe out the possibility of replay attack.

The nonce helps the BS to identify successive requests and it enhances the BS capacity to reject those requests which was sent by the intruders or adversaries so to prevent DOS attack. BS, thus, can identify the latest requests and it is able to filter out samples of replay attacks. In stapes authorization reply message, the BS sends the timestamp and nonce of MS. That helps in preventing an adversary from forging a BS. This

protocol also provides mutual authentication. The nonce value sent by the BS helps in preventing the man-in-the middle attack.

The timestamp helps the BS in identifying the latest requests, which prevents reply attacks. It also helps the MS to identify the recent messages, and hence it can identify the AK used by the MS as new or not. The addition of nonce from the BS helps the MS to identify whether the message which he received with pre-AK is a newer one or not. It is better to add more buffers to carry the used nonce values in the previous sessions. This gives more security to the BS and user MS.

V.CONCLUSION

The paper analyzes the vulnerabilities in the both versions of authentication protocol PKMv1 and PKMv2. As seen in the formal analysis, the secrecy and uniqueness of the keying material distributed and the no theft of service possible claims are valid in both PKMv1 and PKMv2. However, pseudonymity and information confidentiality are broken in both versions of PKM.

A revised authentication protocol is proposed by using nonce and timestamp together. The new solution is efficient to tackling the various security threats such as replay, man in the middle and DOS attacks.

The revised authentication protocol is expected to provide better secure platform for IEEE 802.16(e).

REFERENCES

[1] G IEEE Std. 802.16-2001, IEEE Standard for Local and Metropolitan Area Networks Part16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE, 2002.

[2] IEEE Std. 802.16-2004: IEEE Standard for Local and Metropolitan Area Networks Part16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE, 2004.

[3] IEEE Std. 802.16e-2005: IEEE Standard for Local and Metropolitan Area Networks Part16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, IEEE, 2006.

[4] Michel Barbeau, "Wimax/802.16 threat analysis", Q2SWinet05, Montreal, Quebec, Canada, ACM proceedings, 294: 456 -475, October 2005.

[5] E. Kaasenbrood, "WiMAX Security - A Formal and Informal Analysis," Master's thesis, Eindhoven University of Technology, Department of Mathematics and Computer Science, Groningen, Netherlands, August 2006.

[6] C. Cremers,"The Scyther tool: Automatic verification of security protocols, http://people.inf.ethz.ch/cremersc/scyther/index.html, 2009.

[7] M. Burrows, M. Abadi, and R. Needham, "A Logic of Authentication", Proceedings of the Royal Society of London, vol. 426, pp. 233-271, 1989.

[8] G. Lowe, "A Family of Attacks upon Authentication Protocols," Technical Report 1997/5, University of Leicester, UK, 1997.

[9] D. Song, "Athena: A new efficient automatic checker for security protocol analysis," In PCSFW: Proceedings of the Computer Security Foundations Workshop, IEEE Computer Society Press, pp.192, 1999.