MultiCraft

International Journal of Engineering, Science and Technology
Vol. 5, No. 4, 2013, pp. 37-42

INTERNATIONAL JOURNAL OF ENGINEERING, SCIENCE AND TECHNOLOGY

www.ijest-ng.com
www.ajol.info/index.php/ijest

Improving the security of the Hwang-Su protocol for mobile networks

Miloud Ait Hemad, My Ahmed El-Kiram, Azzeddine Lazrek

Cadi Ayyad University, Faculty of Sciences, Department of Computer Science, Marrakech, MOROCCO
Corresponding Author: e-mail: m.aithemad@ucam.ac.ma, Tel +212-667660340, Fax.+212-524437407

Abstract

The mobile networks are experiencing a growing success. This success is mainly due to the fact that these networks providing the mobility of users, the transmission of data through open air and the requirement of low power. But, it is threatened by weak security, especially at the level of authentication. Hwang and Su have proposed an efficient authentication protocol for mobile networks. This protocol, called Hwang-Su here, is based on the use of one-way hash function, symmetric key cryptosystem and nonce. Hwang-Su protocol consists of two sub-protocols, named intra-domain authentication and inter-domain authentication. If the user and the service provider registered in the same domain, we would use intra-domain authentication protocol. Otherwise, we would initiate inter-domain authentication protocol. In this article, we show that both sub-protocols are not secured. Indeed, any legitimate user can abuse of these rights to attack them. We also propose improvements to increase its security.

Keywords: Authentication, Mobile communication, Cryptography, Security.

DOI: http://dx.doi.org/10.4314/ijest.v5i4.4

1. Introduction

Wireless networks (IEEE standard 802.11 1996, Gast 2005) have allowed computer systems to exchange data without cable connections. The development of these networks and associated communication protocols, such as Mobile-IP (Perkons 1996, 1997), and the increased need of communicating without space and time constraints, made mobile units (PDAs, laptops, smart phones,…) more and more used. Many service providers offer services to mobile users. Each one must be able to reject any non legitimate user to access these services. Consequently, mobile users must prove their identity to the service provider in order to be authorized according to rules defined by an authentication protocol. Mobile units are mainly characterized by their small size and their weak computing power. Furthermore, the wireless data channel is low data rate. These restrictions have an effect while designing the authentication protocol for mobile networks. Therefore, the number of encryption and decryption operations should be low. The size and the number of exchanged messages have to be small. In addition, the authentication inter-domain must be supported.

Many authentication protocols have been proposed (Neuman *et al.* 2004, Molva *et al*. 1992, Tardo *et al.* 1991, Shieh *et al.* 1999, Chien *et al.* 2003, Hwang *et al.* 2005) and many efforts have been devoted to improve their security (Fox *et al.* 1996, Tang *et al.* 2006, Chan *et al.* 2007, Wu *et al.* 2010, Xua *et al.* 2011). Among these proposed authentication protocols, Kerberos (Neuman *et al.* 2004), which was developed by Project Athena at MIT (Champine *et al.* 1990) is one of the most widely deployed protocols. Unfortunately, it is not only vulnerable to password guessing attacks but also very inefficient when inter-domain authentications are required. So, it is less suitable for mobile environments. Among the efficient protocols which is designed for mobile networks, the one proposed by Hwang and Su. Hwang-Su protocol is based on symmetric cryptosystem, challenge-response and hash chaining. This protocol has several merits including providing inter-domain authentication, low computational costs and low communication capacity.

2. Review of the Hwang-Su authentication protocol

In this section, we are going to review Hwang-Su authentication protocol. There are three principals: the mobile user (*M*), the service provider (*S*) and the key distribution center (*KDC* for short). Each entity (mobile user and service provider) share a secret key with the *KDC* of its own domain. The mobile user, the service provider and the *KDC* store secretly and respectively the different keys K_{MC}, K_{SC} and K_C.. By using a secret one-way hash function f and the key K_C, the *KDC* can compute K_{MC} and K_{SC} as follows: $K_{MC} = f(K_C, M)$ and $K_{SC} = f(K_C, S)$. In this way, the *KDC* doesn't need store all the secret keys of the entities which it controls. The Hwang-Su protocol (Hwang *et al.* 2005) offers the intra-domain authentication and the inter-domain authentication.

2.1 Intra-domain authentication protocol

The intra-domain authentication is used when the mobile users and the service provider registered in the same KDC. This authentication consists of two parts: the initial authentication and the subsequent authentication.

2.1.1 Initial authentication

The initial authentication proceeds as shown in "Figure 1".

1.	$M \rightarrow S$	:	$M, N_M, h(N_M, K_{MC})$
2.	$S \rightarrow KDC$	:	$M, N_M, h(N_M, K_{MC}), S, N_S, h(N_S, K_{SC})$
3.	$KDC \rightarrow S$	:	$\{N_S, h^n(a), n, \{N_M, a, n\}K_{MC}\}K_{SC}$
4.	$S \rightarrow M$	:	$\{N_M, a, n\}K_{MC}, \{N_M\}K_n$

Figure 1. Initial authentication of Hwang-Su intra-domain protocol

First, the mobile user asks for an authentication from *S* by sending a message (step 1). This message consists of his identity, a nonce N_M and the hash value $h(N_M, K_{MC})$. *h* denotes a one-way hash function. Then, the provider service *S* sends the received message with his own identity, a nonce N_S and the hash value $h(N_S, K_{SC})$ to *KDC* (step 2).

The *KDC* checks $h(N_M, K_{MC})$ and $h(N_S, K_{SC})$. Then, he generates a random number *a* and sends the message $\{N_S, h^n(a), n, \{N_M, a, n\}K_{MC}\}K_{SC}$ to *S* (step 3), where *n* denotes the maximum number of times that the mobile user allowed to access *S*.

S decrypts the received message using his secret key K_{SC}. Then, he checks that the N_S value corresponds well to that of the nonce which he had generated before. If such is the case, he computes $K_n = h(n, h^n(a))$ as the session key and keeps *M*, $h^n(a)$ and *n*. After, he sends $\{N_M, a, n\}K_{MC}, \{N_M\}K_n$ to *M* (step 4). The mobile user *M* decrypts $\{N_M, a, n\}K_{MC}$ and $\{N_M\}K_n$. Then, he checks that the values of both recovered nonces N_M are equal and they correspond to that of the nonce which *M* had sent before. If successful, *M* secretly keeps *a*, *n* and K_n.

2.1.1 Subsequent authentication

After initial authentication, the mobile user can request services from service provider *n* times without involving the *KDC*. The *i*th subsequent authentication ($1 \leq i \leq n$) proceeds as shown in "Figure 2".

1.	$M \rightarrow S$	:	$M, \{h^{n-i}(a)\}K_{n-i+1}$
2.	$S \rightarrow M$	:	$\{h^{n-i}(a)\}K_{n-i}$

Figure 2. Subsequent authentication of Hwang-Su intra-domain protocol

M computes $h^{n-i}(a)$ and sends the message $\{h^{n-i}(a)\}K_{n-i+1}$, along with his identity, to *S* (step 1). Next, *S* computes the current session key $K_{n-i+1} = h(n-i+1, h^{n-i+1}(a))$ from the current hash value $h^{n-i+1}(a)$, that it stocked in *(i-1)*th connection. Then, he decrypts the received message using this key. Thus, he recovers $h^{n-i}(a)$. After, he checks that the hash value $h(h^{n-i}(a))$ equals to that of the stored $h^{n-i+1}(a)$. If such is the case, *S* sends $\{h^{n-i}(a)\}K_{n-i}$ to *M* (step 2). Finally, he updates $h^{n-i+1}(a)$ with $h^{n-i}(a)$ and keeps *i*.

M computes the new session key K_{n-1} and checks the presence of $h^{n-i}(a)$. Then, he keeps *i*.

2.2 Inter-domain authentication protocol

Suppose the mobile user *M* registered in the domain *H* (home domain), the service provider *S* registered in another domain *V* (visited domain) and *P* was the parent domain of *H* and *V*, where the *KDC* of *P* (KDC_P) shares the secret keys K_{HP} and K_{VP} with the *KDC* of *H* (KDC_H) and the *KDC* of *V* (KDC_V) respectively. The following procedures would be performed so that the mobile user could request a service that is provided by the visited service provider.

2.2.1 Initial authentication

The initial authentication proceeds as shown in "Figure 3".

1.	$M \rightarrow S$	:	$KDC_H, M, N_M, h(N_M, K_{MH})$
2.	$S \rightarrow KDC_V$	:	$KDC_H, M, N_M, h(N_M, K_{MH}), S, N_S, h(N_S, K_{SV})$
3.	$KDC_V \rightarrow KDC_P$	:	$KDC_H, M, N_M, h(N_M, K_{MH}), S, KDC_V, N_V, h(N_V, K_{VP})$
4.	$KDC_P \rightarrow KDC_H$	:	$\{N_V, h^n(a), n\}K_{VP}$, $\{M, N_M, h(N_M, K_{MH}), S, KDC_V, a, n\}K_{HP}$
5.	$KDC_H \rightarrow KDC_V$	:	$\{N_V, h^n(a), n\}K_{VP}, S, M, \{N_M, a, n\}K_{MH}$
6.	$KDC_V \rightarrow S$	:	$\{N_S, h^n(a), n, \{N_M, a, n\}K_{MH}\}K_{SV}$
7.	$S \rightarrow M$	:	$\{N_M, a, n\}K_{MH}, \{M_T, N_M\}K_n$

Figure 3. Initial authentication of Hwang-Su inter-domain protocol

First, the mobile user sends a message includes his identity, the identity of KDC_H, N_M and $h(N_M, K_{MH})$ to S (step 1). K_{MH} denotes the secret key of M. Next, the provider service S sends the received message with his identity, N_S and $h(N_S, K_{SV})$ to KDC_V (step 2). K_{SV} denotes the secret key of S.

KDC_V authenticates S by checking $h(N_S, K_{SV})$. Then, he sends the message $KDC_H, M, N_M, h(N_M, K_{MH}), S, KDC_V, N_V, h(N_V, K_{VP})$ to KDC_P (step 3). N_V denotes a nonce randomly selected by KDC_V.

KDC_P authenticates KDC_V by checking $h(N_V, K_{VP})$. After, he generates a random number a and sends the message $\{N_V, h^n(a), n\}K_{VP}, \{M, N_M, h(N_M, K_{MH}), S, KDC_V, a, n\}K_{HP}$ to KDC_H (step 4).

KDC_H authenticates M and KDC_P by checking $h(N_M, K_{MH})$. Then, he sends the message $\{N_V, h^n(a), n\}K_{VP}, S, M, \{N_M, a, n\}K_{MH}$ to KDC_V (step 5). Next, KDC_V authenticates M by checking N_V. After, he sends the message $\{N_S, h^n(a), n, \{N_M, a, n\}K_{MH}\}K_{SV}$ to S (step 6).

S checks N_S. After verifying it, he assigns a temporary name M_T to mobile user. This temporary name will permit the mobile user to perform the subsequent authentication without involving the KDC. Then, S computes the session key $K_n = h(n, h^n(a))$, which will be attributed to M_T. After, he keeps M_T, $h^n(a)$ and n. Afterward, he sends the message $\{N_M, a, n\}K_{MC}, \{M_T, N_M\}K_n$ to M (step 7).

2.2.1 Subsequent authentication

The subsequent authentication is similar to that of the intra-domain protocol except the mobile user's identity which is replaced by his temporary name.

3. Vulnerabilities and proposed improvement of the Hwang-Su authentication protocol

In this section, we both show the security problems of Hwang-Su intra-domain and inter-domain authentication protocol, and also we present our proposed improvement.

3.1 Vulnerability and proposed improvement of Hwang-Su intra-domain authentication protocol

3.1.1 Vulnerability of Hwang-Su intra-domain authentication protocol

The initial authentication of Hwan-Su intra-domain protocol presents a major security flaw. This latter can be exploited by a malicious but legitimate user A, to impersonate another user M. The impersonation attack operates as shown in "Figure 4".

1.	$A(M) \rightarrow S$	:	$M, N_A, h(N_A, K_{AC})$
2.1	$S \rightarrow A(KDC)$	:	$M, N_A, h(N_A, K_{AC}), S, N_S, h(N_S, K_{SC})$
2.2	$A(S) \rightarrow KDC$	:	$A, N_A, h(N_A, K_{AC}), S, N_S, h(N_S, K_{SC})$
3.	$KDC \rightarrow S$	:	$\{N_S, h^n(a), n, \{N_A, a, n\}K_{AC}\}K_{SC}$
4.	$S \rightarrow A(M)$	:	$\{N_A, a, n\}K_{AC}, \{N_A\}K_n$

Figure 4. Proposed attack against Hwang-Su intra-domain protocol

First, the intruder A, pretending to be M, sends a message consisting of the identity M, a nonce N_A and $h(N_A, K_{AC})$ (step 1). K_{AC} denotes secret key of the intruder, who is the legal user.

Next, the intruder impersonates KDC identity to intercept the message sent from S to KDC (step 2.1).

A modifies the intercepted message replacing the identity M by his own. Then, he sends this message to KDC, pretending to be S (step 2.2).

KDC authenticates *S* and *A*, who is the legitimate user, by checking $h(N_S, K_{SC})$ and $h(N_A, K_{AC})$. After, he creates and sends the step *3* message to *S*.

S decrypts the received message with his secret key. Then, he checks that the N_S value corresponds well to that of the nonce which he had sent before. If the check succeeds, he is convinced that *KDC* authenticated *M*, while *KDC* authenticated *A*. Afterward, *S* sends the step *4* message to *A*, believing that he communicates with *M*.

Thus, the intruder deceives the initial authentication, and later, he can access to *S* as being another user *M*. For that, he just needs to perform normally the subsequent authentication as he possesses *a*, *n* and K_n.

It is also possible that the intruder impersonates the service provider. The scenario of masquerading as the service provider is similar.

3.1.2 Proposed improvement of Hwang-Su intra-domain authentication protocol

The vulnerability, shown in section *3.1.1*, is essentially due to the fact that the message sent by *KDC* doesn't mention the identities authenticated by this latter. To correct this vulnerability, we propose adding the identity of mobile user and the service provider, in the step *3* and *4* messages of initial authentication procedure, as follows:

5. $KDC \rightarrow S$: $\{\mathbf{M}, N_S, h^n(a), n, \{\mathbf{S}, N_M, a, n\}K_{MC}\}K_{SC}$
6. $S \rightarrow M$: $\{\mathbf{S}, N_M, a, n\}K_{MC}, \{N_M\}K_n$

So, the proposed improvement of Hwang-Su intra-domain authentication protocol is as shown in "Figure 5".

Initial authentication

1. $M \rightarrow S$: $M, N_M, h(N_M, K_{MC})$
2. $S \rightarrow KDC$: $M, N_M, h(N_M, K_{MC}), S, N_S, h(N_S, K_{SC})$
3. $KDC \rightarrow S$: $\{M, N_S, h^n(a), n, \{S, N_M, a, n\}K_{MC}\}K_{SC}$
4. $S \rightarrow M$: $\{S, N_M, a, n\}K_{MC}, \{N_M\}K_n$

Subsequent authentication

1. $M \rightarrow S$: $M, \{h^{n-i}(a)\}K_{n-i+1}$
2. $S \rightarrow M$: $\{h^{n-i}(a)\}K_{n-i}$

Figure 5. Proposed improvement of Hwang-Su intra-domain protocol

3.2 Vulnerability and proposed improvement of Hwang-Su inter-domain authentication protocol

3.2.1 Vulnerability of Hwang-Su inter-domain authentication protocol

As the inter-domain protocol is an extension of intra-domain protocol, the initial authentication of Hwang-Su inter-domain protocol suffers from the same security flaw mentioned in section *3.1.1*. To repair this security flaw, we propose to modify the step *6* and *7* messages of initial authentication procedure as follows:

6. $KDC_V \rightarrow S$: $\{M, N_S, h^n(a), n, \{S, N_M, a, n\}K_{MH}\}K_{SV}$
7. $S \rightarrow M$: $\{S, N_M, a, n\}K_{MH}, \{M_T, N_M\}K_n$

Even if this flaw is repaired, the inter-domain protocol is still insecure. In fact, the protocol has another critical security flaw which may permit a malicious but legal user *A*, to be authenticated as another user. To exploit this vulnerability, the intruder has to proceed as illustrated in "Figure 6".

1. $A(M) \rightarrow S$: $KDC_H, M, N_A, h(N_A, K_{AH})$
2. $S \rightarrow KDC_V$: $KDC_H, M, N_A, h(N_A, K_{AH}), S, N_S, h(N_S, K_{SV})$

3.1 $KDC_V \rightarrow A(KDC_P)$: $KDC_H, M, N_A, h(N_A, K_{AH}), S, KDC_V, N_V, h(N_V, K_{VP})$

3.2. $A(KDC_V) \rightarrow KDC_P$: $KDC_H, A, N_A, h(N_A, K_{AH}), S, KDC_V, N_V, h(N_V, K_{VP})$

4. $KDC_P \rightarrow KDC_H$: $\{N_V, h^n(a), n\}K_{VP}, \{A, N_A, h(N_A, K_{AH}), S, KDC_V, a, n\}K_{HP}$

5.1. $KDC_H \rightarrow A(KDC_V)$: $\{N_V, h^n(a), n\}K_{VP}, S, A, \{N_A, a, n\}K_{AH}$

5.2. $A(KDC_H) \rightarrow KDC_V$: $\{N_V, h^n(a), n\}K_{VP}, S, M, \{N_A, a, n\}K_{AH}$

6. $KDCV \rightarrow S$: $\{NS, h^n(a), n, \{N_A, a, n\} K_{AH}\}K_{SV}$
7. $S \rightarrow A(M)$: $\{N_A, a, n\}K_{AH}, \{M_T, N_A\}K_n$

Figure 6. Proposed attack against Hwang-Su inter-domain protocol

First, the intruder, pretending to be *M*, sends a message consisting of the identity of KDC_H and *M*, a nonce N_A and $h(N_A, K_{AH})$. K_{AH} denotes the secret key of the intruder.

The provider service S sends the received message with his identity, a nonce N_S and $h(N_S, K_{SV})$ to KDC_V.

The intruder impersonates KDC_P identity to intercept the message sent from KDC_V to KDC_P.

The intruder forges a new message form the intercepted message, by replacing the identity *M* with his own.

KDC_P generates a random number *a* and sends the message $\{N_V, h^n(a), n\}K_{VP}, \{A, N_A, h(N_A, K_{AH}), S, KDC_V, a, n\}K_{HP}$ to KDC_H. Then, the intruder impersonates KDC_V identity.

KDC_H authenticates *A*, who is the legitimate user, by checking $h(N_A, K_{AH})$. Then, he sends the message $\{N_V, h^n(a), n\}K_{VP}, S, A, \{N_A, a, n\}K_{AH}$ to *A*, thinking he communicates with KDC_V.

The intruder modifies the received message replacing his identity by *M*. Then, he sends this message to KDC_V, pretending to be KDC_H.

KDC_V authenticates *A* as being *M*, and sends the message $\{N_S, h^n(a), n, \{N_A, a, n\}K_{AH}\}K_{SV}$ to *S*.

By checking N_S, *S* is convinced that KDC_H authenticated *M*, where as KDC_H authenticated *A*. Then, *S* sends the step *7* message to *A*, believing he communicates with *M*.

Thus, the intruder deceives the service provider *S*, by impersonating another user *M*. So making *S* thinks that he communicates with *M*.

3.2.2 Proposed improvement of Hwang-Su inter-domain authentication protocol

To withstand the attack, proposed in section *3.2.1*, we propose adding the identities *M* and *S*, in the step *5*, *6* and *7* messages of initial authentication phase.

So, the proposed improvement of Hwang-Su inter-domain authentication protocol is as shown in "Figure 7".

Initial authentication

1.	$M \rightarrow S$	:	$KDC_H, M, N_M, h(N_M, K_{MH})$
2.	$S \rightarrow KDC_V$	:	$KDC_H, M, N_M, h(N_M, K_{MH}), S, N_S, h(N_S, K_{SV})$
3.	$KDC_V \rightarrow KDC_P$	:	$KDC_H, M, N_M, h(N_M, K_{MH}), S, KDC_V, N_V, h(N_V, K_{VP})$
4.	$KDC_P \rightarrow KDC_H$	:	$\{N_V, h^n(a), n\}K_{VP}, \{M, N_M, h(N_M, K_{MH}), S, KDC_V, a, n\}K_{HP}$
5.	$KDC_H \rightarrow KDC_V$	:	$\{M, N_V, h^n(a), n\}K_{VP}, S, M, \{S, N_M, a, n\}K_{MH}$
6.	$KDC_V \rightarrow S$	:	$\{M, N_S, h^n(a), n, \{S, N_M, a, n\}K_{MH}\}K_{SV}$
7.	$S \rightarrow M$	:	$\{S, N_M, a, n\}K_{MH}, \{M_T, N_M\}K_n$

Subsequent authentication

1.	$M \rightarrow S$	:	$M_T, \{h^{n-i}(a)\}K_{n-i+1}$
2.	$S \rightarrow M$	:	$\{h^{n-i}(a)\}K_{n-i}$

Figure 7. Proposed improvement of Hwang-Su inter-domain protocol

4. Conclusions

Hwang-Su protocol has been proposed to be applied in the mobile networks. In their protocol, Hwang and Su significantly minimized the number and the size of the exchanged messages. They also reduced the number of the keys that should be maintained by *KDCs* to ensure the inter-domain authentication. Despite its merits the protocol, as proposed by its authors, presents security problems. Hwang and Su claim that their protocol is resistant to attacks. However, in this paper we have proposed two attacks: one against the inter-domain authentication and the other against the intra-domain authentication. We have also proposed an improvement of Hwang-Su protocol. Our improvement can withstand the proposed attacks.

References

Champine G. A., Geer D. E. Jr., and Ruh W. N. 1990. Project Athena as a distributed computer system. *Computer*, Vol. 23, no. 9, pp. 40-51.

Chan C. W. and Wang R. Y., 2007. Improving the security of the Chien-Jan protocol for large mobile networks, *iih-msp* -Third *International Conference on International Information Hiding and Multimedia Signal Processing-,* Vol. 1, pp. 249-252*, (IIH-MSP 2007*).

Chien H. Y. and Jan J. K., 2003. A hybrid authentication protocol for large mobile network, *Journal of Systems and Software,* Vol. 67, No. 2, pp. 123-130.

Fox A. and Gribble S. D., 1996. Security on the move: indirect authentication using Kerberos, *in Proc. Second Annual International Conference on Mobile Computing and Networking.* ACM Press, pp. 155-164.

Gast M. S., 2005. 802.11 wireless network, O'Reilly.

Hwang R. and Su F., 2005. "A new efficient authentication protocol for mobile networks, *Computer Standards & Interfaces*, vol. 28, No. 2, pp. 241-252, December.

IEEE Standard 802.11, 1996. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, *IEEE Draft Standard*.

Molva R., Tsudik G., Herreweghen E. V. and Zatti S., 1992. KryptoKnight authentication and key distribution system, *in Proc. European Symposium on Research in Computer Security*, pp. 155-174.

Neuman C., Kohl J., Ts'o J., Yu T., Hartman S. and Raeburn K., 2005. The Kerberos network authentication service (v5), September 7 2004, *Internet draft*, expires 7 March.

Perkons C., 1996. IP mobility support, *Internet Request for Comments 2002*.

Perkins C., 1997. Mobile IP, *IEEE Communications Magazine*, Vol. 35, No. 5, pp. 84-99, May.

Shieh S., Ho F. and Huang Y., 1999. An efficient authentication protocol for mobile networks, *Journal of Information Science and Engineering,* Vol. 15, No. 4, pp. 505-520.

Tang Q. and Mitchell C. J., 2006. Cryptanalysis of a hybrid authentication protocol for large mobile networks, *Journal of Systems and Software*, Vol. 79, No. 4, pp. 496-501.

Tardo J. J. and Alagappan K., 1991. SPX: Global authentication using public key certificates, *in Proc. IEEE Symposium on Research in Security and Privacy*.

Wu T. Y. and Tsen Y. M., 2010. An efficient user authentication and key exchange protocol for mobile client–server environment, *Journal of Computer Networks,* Vol. 54, No. 9, pp. 1520-1530.

Xua J., Zhub W. T. and Fenga D. G., 2011. An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks, *Journal of Computer Communications*, Vol. 34, No. 3, pp. 319–325.

Biographical notes

Miloud Ait Hemad received the B. S. in the Cadi Ayyad University in 2001. He has his master in the field of networks and telecommunication at University the Chouaib Doukkali at El Jadida in 2005. He is currently a Ph.D. candidate of the Cadi Ayyad University, Marrakech, Morocco. His main field of research interest is the authentication in wireless networks.

Moulay Ahmed El Kiram is research professor at the Faculty of Science Semlalia, Cadi Ayyad University of Marrakech. He received his DES in Computer Science in 1997 at Mohammed V University of Rabat. El Kiram specializes in Security and network communication. His areas of interest include Authentication, particularly in multicast environment.

Azzeddine Lazrek is full Professor in Computer Science at Cadi Ayyad University in Marrakesh. He holds a Ph.D. in Computer Science from Lorraine Polytechnic National Institute in France, awarded in 1988, and a State Doctorate Morocco awarded in 2002. Prof. Lazrek specializes in communication through multilingual multimedia e-documents. His areas of interest include multimedia information processing and its applications, particularly, to electronic publishing, digital typography, Arabic processing, and history of sciences. He was in charge of the Information Systems and Communication Networks Research Team and the Multilingual Scientific E-Document Processing Research Group. He is an Invited Expert at W3C. He leads a multilingual e-document composition project with some international organizations. He contributes to scientific journals and is a member of several national and international scientific associations. Email: lazrek@ucam.ac.ma

Received May 2012
Accepted May 2013
Final acceptance in revised form June 2013