

# Localized Authentication for Wireless LAN Inter-network Roaming

Men Long , Chwan-Hwa “John” Wu , J. David Irwin  
Department of Electrical and Computer Engineering  
Auburn University  
Auburn, Alabama 36849, USA  
Email: wu@eng.auburn.edu

**Abstract**— Authentication is an essential premise for deploying wireless LAN inter-network roaming in the real world. The technical challenge lies in the fact that a visited network does not initially have the authentication credentials of a roaming user. Existing solutions require that authentication is performed via three-party communications: user to visited network to home network. In this paper, a new concept that mutual authentication between a visited network and a roaming user can be performed locally without the contact with user’s home network is proposed. This new protocol not only satisfies the roaming authentication requirements, but also has efficiency in terms of authentication time delay.

**Keywords**—AAA; authentication; inter-network roaming; SSL; wireless security

## I. INTRODUCTION

With the continuing deployment of wireless LANs, the support of roaming among different wireless Internet service providers (ISP) will become crucial for wireless ISPs to build their subscriber base. A potential scenario may take place as follows. A user subscribes to the network access service from his home network. When the user visits another network, he is capable of employing the same authentication credentials that are used in his home network in order to be authenticated by the visited network. This will provide a tremendous convenience for subscribers who want to access the Internet at any time and anywhere.

At present, the solution for mutual authentication between a roaming user and a visited network has yet to be fully optimized. The technical challenge is that a roaming user and a visited network do not *a priori* share any secret. All the existing solutions require the intervention of the user’s home network for authentication [1], [2].

The state-of-the-art proposals by industry with regard to the inter-network roaming suggest that the authentication, authorization, and accounting (AAA) server [3] of a visited network obtains a roaming user’s credentials, such as his user name, domain name and password, and then sends them to the AAA server of the user’s home network during the authentication process [1], [2]. The home network’s AAA server then authenticates the user’s credentials and sends back the decision (“accept” or “reject”) to the visited network.

We argue that the above approach inherently incurs more time delay for authentication as a result of the extra

communication between the AAA servers of the wireless ISPs. The fact is that the home AAA server may be far away (hundreds of miles) from the visited AAA server while a roaming user and the visited network are geographically close. Furthermore, any possible failure of the home AAA server or any of the networks along the path between the home and visited AAA servers would prevent a roaming user from being authenticated.

In this paper, we propose a new approach in which an initial mutual authentication between a visited network and a roaming user can be performed locally without any intervention by the user’s home network. Two unique advantages are low time delay and robustness. Compared to the existing solutions, the proposed protocol avoids two time-delay factors (the home AAA server processing delay and the transmission delay between the home and visited networks). It is clear that when either the home network is under heavy workload or the home network is far away from the visited network, a noticeable authentication time delay will arise. The proposed protocol is robust because even if the home AAA server is down the roaming user can still be authenticated by the visited network.

The main features of the proposed method can be stated as follows. 1) A simple and flexible public key infrastructure is constructed by wireless ISPs. The wireless ISP’s public key certificates are issued by the ISPs themselves. In addition, a subscriber has a private key as well as the corresponding public key certificate issued by his home ISP. 2) The authentication protocol adapts the SSL v3.0 handshake protocol [4] to provide strong mutual authentication. Our design protects a user’s identity from leaking to irrelevant parties on an open radio interface and prevents a visited network from learning a roaming user’s secret. 3) The protocol is quite efficient, demonstrated by preliminary experimental results.

The remainder of this paper is organized as follows. In Section 2, some basic concepts of wireless roaming are introduced. In Section 3, the proposed public key certificate structure is presented at length. In Section 4, the protocol for the roaming authentication is described in detail. In Section 5, the design rationale is discussed, which provides an explicit understanding of the design process that led to the protocol. In Section 6, a preliminary performance assessment is given. Finally, some concluding remarks are provided in Section 7.

## II. BACKGROUND AND RELATED WORKS

Fig. 1 illustrates two basic settings of wireless roaming. A user has a billing relationship with his home network, i.e. paying a monthly fee. When the user moves into another ISP's domain at cell 1, the inter-network roaming takes place. If the user subsequently moves from cell 1 to cell 2 within the ISP, the intra-network roaming occurs. The authentication for inter-network roaming can establish a shared secret between a roaming user and a visited network, which, in turn, may be used for the intra-network roaming authentication. Thus the difficult part for protocol designers is the inter-network roaming authentication.

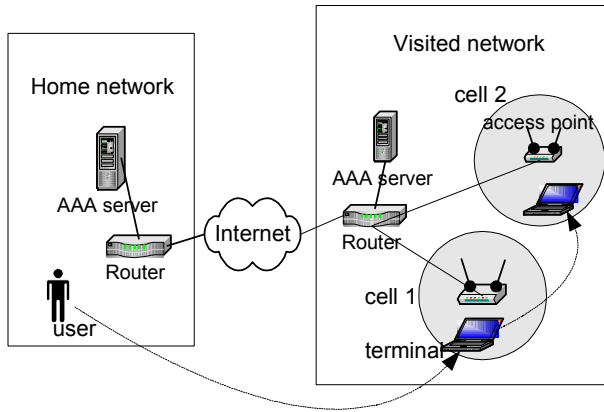


Figure 1. A simple wireless LAN roaming illustration

Under the solution proposed by the Wi-Fi Alliance [1], an SSL encrypted channel will be set up after a visited network receives a roaming user's authentication request and sends its public key certificate to the user's mobile terminal. Then the user is expected to enter his credentials, such as name@domain and password, into the authentication portal of the visited network. The SSL channel protects the user's password. Next, the visited network sends the user's credentials to his home network through a pre-established secure channel between ISPs. Only the home network is capable of verifying the user's credentials and thus sends the decision ("accept" or "reject") back to the visited network. If the decision is "accept", the visited network will authorize access service to the user.

It is worthy pointing out there are some other authentication solutions proposed for roaming [5], [6], [7]. However all of them require the intervention of a roaming user's home network for authentication between a visited network and a roaming user.

## III. A PRACTICAL CERTIFICATE STRUCTURE

In this paper, we argue that the general-purpose X.509 certificate structure [8] may not be the best solution for the wireless roaming authentication. If X.509 is used, different ISPs may use different certification authorities (CA). The ramifications of this arrangement are that the system participants, i.e. roaming users and ISPs, must trust the root CAs as well as the intermediate CAs. In reality, it is not easy to establish the required trust relationship of a hierarchy in the civilian world. Additionally, if the certificates are issued by

commercial CAs, the users and ISPs must share the financial costs associated with the certificates.

Our observation is that there is a closed system with respect to ISPs and their subscribers. The ISPs directly manage their own user's account. In addition, a roaming agreement has to be established *a priori* by the participant ISPs in order to provide roaming service. Thus we propose that the certificates should be issued by the ISPs themselves, not by the commercial CAs.

To simplify the presentation, we assume there are two ISPs, ISP 1 and ISP 2, and a user Bob is a subscriber of ISP 2. ISP 1 and ISP 2 have a roaming agreement. The ISP 1 has its own private key  $SK_1$ , the corresponding public key certificate (including the public key  $PK_1$  and the signature on  $PK_1$  made by ISP 2's private key  $SK_2$ ), and the public key  $PK_2$  of ISP 2. In generalization, if an ISP has a relationship with other  $n-1$  ISPs, the ISP stores one private key of its own,  $n-1$  public key certificates of its own public key and  $n-1$  public keys of the other ISPs. The user Bob has his private key  $S_{Bob}$  and public key  $P_{Bob}$ , generated by the ISP 2, and ISP 2's public key  $PK_2$ .

## IV. PROPOSED AUTHENTICATION PROTOCOL

The primary focus of this paper is the initial authentication between a visited network and a roaming user (inter-network roaming authentication). The proposed approach for authentication adapts the SSL v3.0 handshake protocol.

The major modification made by our approach is to efficiently encrypt a user's certificate and then have the user explicitly sign the challenge posed by an AAA server.

### A. Authentication Handshake Messages

We present the proposed protocol in its most basic form in Fig. 2, showing its cryptographic core. The details on the packet format are similar to those in the SSL protocol specification. The well known mathematical details of some cryptographic algorithms can be found in [9].

- flow (1)** roaming user's terminal → visited network  
 $N_U, D$
- flow (2)** visited network → roaming user's terminal  
 $N_S, Cert_S$
- flow (3)** roaming user's terminal → visited network  
 $Enc_{PK_S}(k), E_{k_1}(Cert_U), Sign_{S_U}(N_S || N_U || S || U)$

Figure 2. Basic form of the proposed authentication protocol

**Flows (1) and (2).** These two flows perform the same function as the "ClientHello" and "ServerHello" in the SSL protocol.  $N_U$  is a random number employed as the user's nonce, which prevents a replay attack.  $D$  is the domain name of the roaming user, and thus the visited network is able to determine the user's originating domain. Upon receiving the domain name in flow 1, the AAA server of the visited network will attempt to find its public key certificate  $Cert_S$  signed by that domain  $D$ . If no such certificate exists, which implies no roaming agreement, the protocol aborts at this stage.

Otherwise, the server sends the certificate  $Cert_S$  and server's nonce  $N_S$  to the user.

**Flow (3).** Upon receiving the visited network's certificate, the user employs its home network's public key to verify the  $Cert_S$ . If the certificate is valid, the user chooses a random number  $k$  as the pre-master secret and then encrypts it by  $Enc_{PK_S}(k)$  using the visited network's public key  $PK_S$  in  $Cert_S$ . Also, the user's terminal applies a pseudo random function to the pre-master secret to derive a key  $k_I$ . Then  $k_I$  encrypts the user's certificate  $Cert_U$  by  $E_{k_I}(Cert_U)$  via a symmetric cipher such as the AES-128 with an appropriate mode. In addition, the user signs the message  $N_S || N_U || S || U$  using his private key  $S_U$ , where  $S$  and  $U$  denote the identities of the visited network and the roaming user, respectively, and "||" denotes concatenation. Note that the signature, rather than message, is transmitted in flow 3.

### B. Visited Network Verification

On obtaining flow 3, the visited network will first decrypt to obtain the pre-master secret  $k$  using its own private key  $SK_S$ . It then applies the publicly known pseudorandom function to the pre-master secret to derive  $k_I$  and subsequently use it to decrypt to obtain the user's certificate. Since the visited network has the authentic copy of the user's home domain public key, it can verify the authenticity of the user's public key certificate and then the validity of the user's signature.

### C. Authentication Key Establishment

If all the verifications are valid, the visited network and the roaming user can derive a shared secret based on the pre-master secret and two nonces. Also, following the "Finished" procedures in SSL/TLS handshake protocol, each side will explicitly convince the other side that it already possesses the shared secret, which on the other hand concludes the mutual authentication.

When the roaming user subsequently moves within the boundary of the visited network, the shared secret can be utilized for an authentication using the symmetric key cryptographic techniques, which are faster and of less power consumption.

## V. PROTOCOL DESIGN RATIONALES

We give the design rationale for the flow 3 of the protocol, since it is a major component of the proposed protocol.

### A. Seal Roaming User's Identity

The confidentiality requirement of wireless security demands user's identity should be encrypted. One straightforward approach is to encrypt the certificate (with the pre-master secret) by the server's public key. However this approach will increase the client's computational cost and significantly augment the workload of the server. Consider that the certificate length is usually about 900 bytes. Assume the

RSA 1024-bit encryption is employed (a typical setting of the SSL protocol). Thus the client has to perform 8 RSA encryption operations ( $\approx 900 \times 8 / 1024$ ) instead of the original one operation, while the server has to perform 8 RSA decryption operations instead of the original one operation.

Under our approach, the certificate is encrypted by a symmetric cipher and its key can be derived only by the pre-master secret through a fast pseudo random function. Since the server and the client know the pre-master secret, only they two can correctly decrypt the encrypted certificate. The certificate encryption can be performed very fast because of the symmetric cipher.

The key derivation function (pseudo random function) for flow 3 can be implemented using the standard HMAC-SHA-1 [10],

$$k_I = \text{HMAC}(k, \text{Flow1}, \text{Flow2}), \quad (1)$$

Where  $k$  is the pre-master secret described in Section 4.

### B. Roaming User's Signature

A user's signature can be implemented by the standard algorithm such as the DSA [11] or the RSA methods [12]. The message to be signed includes flow 1, flow 2 and the certificate. The signature and its associated message provide the evidence that the user has been provided network access service. A visited network can use the roaming user's signature and the documented service usage to request payments from the user's home network. The signature is capable of connecting three important pieces of information: the authentication time, the identities of a user and a visited network, which provides a possible way to a *posteriori* payment settlement.

### C. Security Feature Comparison

Table 1 summarizes a security feature comparison between the proposed protocol and previous proposals. The proposed protocol has the advantages over the protocols from Wi-Fi Alliance and GSM Association [1], [2].

TABLE I. SECURITY FEATURE COMPARISON

	Previous proposals [1], [2]	Proposed protocol
Time overhead due to communication between home and visited networks	Yes	No
Impact resulting from home network failure	Maximum	Minimum
Visited network learns a roaming user's secret	Yes	No
Strong authentication against cryptanalysis	No	Yes

## VI. PRELIMINARY PERFORMANCE ANALYSIS

Efficiency is an important aspect in protocol design. We assume that the 1024-bit RSA signature and encryption (a common practice) are employed for the performance evaluation.

Our experiments consist of three phases. The first phase implements the cryptographic primitives on a computing platform with a Pentium 4 (2.2 GHz) processor and 512 MB memory. The result shows that the RSA encryption or signature verification time is 0.28 milliseconds while the RSA decryption or signature-signing time is 5.53 milliseconds. The computational time cost of symmetric cryptography is negligible in this case.

The second phase measures the timing of the basic SSL/TLS protocol, where the client does not generate a signature. In our experiment, the client machine is a laptop with a Pentium 4 (1.8 GHz) processor and 256 MB memory and the server is a department email IMAP server employing the SSL/TLS protocol (no client authentication). These two machines are geographically close so that they are used to simulate the roaming user's mobile terminal and the visited network AAA server. The results indicate that the time delay per SSL channel setup averages 24 milliseconds.

At Phase 3, we estimate that the time overhead of the proposed protocol over the basic SSL protocol lies in the operations that a user performs one signing and a server performs two signature verifications (verifying the user's certificate and signature, respectively). According to the data from the phases 1 and 2, the expected time delay for the proposed protocol is about  $30=24+6$  milliseconds.

The time delay of the existing proposals [1], [2] consists of three main factors: 1) a user manually enters his name and password; 2) home AAA server processing delay; 3) transmission delay between the home and visited AAA servers. If the home network is under a heavy load, the roaming user has to compete with many other users, which will deteriorate the time delay. Also, if the home network is far away (hundreds of miles) from the visited network, the time delay will be non-negligible. We estimate that factors 2) and 3) will cause a time delay more than 6 millisecond for today's general wireless ISP networks. In a conclusion, the total authentication delay of the proposed protocol for the inter-network roaming is about 30 milliseconds while the existing solutions, involving 3 parties, cost higher in our experiments.

## VII. CONCLUSION

This paper presents a practical public key certificate structure, in combination with an authentication protocol, for roaming across different wireless ISPs. This new concept employs mutual authentication between a roaming user and a visited network that is performed locally without invoking the user's home ISP. The mutual authentication ensures that the visited network has roaming user authenticity as well as a mechanism for establishing the appropriate revenue stream.

Localized authentication guarantees that the overhead associated with authentication time is significantly reduced, and the impact on its roaming user, caused by the unavailability

of the home network, can be minimized. The special features embedded in this protocol are: 1) a strong mutual authentication between a roaming user and a visited network, 2) the roaming user's identity is encrypted during the handshake protocol, 3) the roaming user's signature can be used *a posteriori* for accounting purposes, 4) the proposed protocol is comparatively efficient in terms of authentication time delay.

## REFERENCES

- [1] B. Anton, B. Bullock, and J. Short, "Best current practices for wireless Internet service provider (WISP) roaming," Wi-Fi Alliance, Feb. 2003, <http://www.weca.net/OpenSection/wispr.asp>.
- [2] GSM Association, "WLAN roaming guidelines," Apr. 2003, <http://www.gsmworld.com/documents/wlan/ir61.pdf>
- [3] C. De Laat, G. Gross, L. Gommans, J. Vollbrecht, and D. Spence, "Generic AAA architecture," Request for Comments (RFC) 2903, Aug. 2000.
- [4] A. Freier, P. Karlton, and P. Kocher, "The SSL protocol version 3.0," Nov. 1996, <http://wp.netscape.com/eng/ssl3/draft302.txt>
- [5] H. Kim and H. Afifi, "Improving mobile authentication with new AAA protocols," Proc. IEEE Int. Conf. on Communications, May 2003, Vol. 1, pp. 497-501.
- [6] S. Suzuki and K. Nakada, "An authentication technique based on distributed security management for the global mobility network," IEEE J. Selected Areas in Communications, vol. 15, no. 8, 1997, pp. 1608-1617.
- [7] K. Hwang and C. Chang, "A self-encryption mechanism for authentication of roaming and teleconference services," IEEE Trans. Wireless Communications, vol. 2, no. 2, 2003, pp. 400-407.
- [8] ITU-T, "Recommendation X.509 (1997 E): information technology-open systems interconnection- the directory: authentication framework," June 1997.
- [9] A. Menezes, P. Van Oorschot, and S. Vanstone, Handbook of applied cryptography, Boca Raton, FL: CRC Press, 1996.
- [10] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: keyed-hashing for message authentication," Request for Comments (RFC) 2104, Feb. 1997.
- [11] FIPS 186-2, Digital Signature Standard (DSS), Feb 2000.
- [12] RSA Laboratories, "PKCS #1 v2.1: RSA cryptography standard", Jun. 2002, <http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html>.