Delegated Validation System for Secure Authentication in WLAN Roaming

Yan ADIKUSUMA[†], Takeshi OKUDA[†], and Suguru YAMAGUCHI[†]

[†] Graduate School of Information Science, Nara Institute of Science and Technology
Takayama-cho 8916-5, Ikoma-shi, Nara, 630-0192 Japan
E-mail: {adik-yan,okuda,suguru}@is.aist-nara.ac.jp

Abstract Rapid deployment of wireless technology has led to rapid growth of Wireless LAN (WLAN). Since workforce is becoming increasingly mobile, roaming across WLAN infrastructures, which gives attractive features both for user and service provider, is required. However, some issues are impeding further adoption of the technology, in particular insufficient security protection for authentication data exchange between different domains that vulnerables to attack. Therefore, we propose secure authentication system for WLAN roaming based on digital certificate combined with delegated validation system. In our scheme, a user is authenticated by presenting an X.509 identity certificate. Then service provider will grant or deny the user's access request by delegating the validation process of certificate to specific validation-server. Although our system requires a user to have digital certificate, it can prevent all the security threats listed above. Moreover, it also provides a basis for independent model of WLAN roaming.

Key words Wireless LAN, roaming, authentication, digital certificate, delegated validation

1. Introduction

Mobility and flexibility for wireless network has led to rapid growth of wireless networking including wireless local area network (WLAN). Based on the IEEE 802.11 standard - commonly known as Wi-Fi (short for wireless fidelity), WLAN has proven to be a fast wireless-networking approach that is relatively easy and inexpensive to implement. Wireless LAN such as home wireless, corporate wireless, campus wireless and public WLAN hotspot service is growing fast and becoming available in many areas. It is estimated that it will continue to develop and grow in the near future especially for the hotspots [1] [2].

Moreover, since the workforce has become increasingly mobile, traditional ways of networking by physical cable is inadequate to meet challenges posed by this new lifestyle. As a result, wireless network along with global roaming across WLAN infrastructure is required. Roaming allows user to use any one of multiple domain/entities (e.g. Internet Service Provider(ISP) or Wireless ISP (WISP), corporate) for connectivity and services, while maintaining formal relationship with only one domain/entity. As such, a global access for users can be achieved through inter-domain WLAN roaming. Furthermore, since it is difficult for a single service provider to build an infrastructure that offers access to its user from any location, roaming between service providers is essential for delivering universal user access. Service providers (i.e. ISP or WISP) can enlarge the service area at a minimal cost.

Given the high demand for the mobile workforce especially business travelers, providing secure WLAN roaming is becoming a critical aspect. From the point of view of the network, providing access to roaming users to connect to the Internet through a domain's network is equal to providing access to their resources. Networks in most cases require some form of authentication in order to prevent unauthorized access. Only authenticated and authorized clients are able to attach to an access network for sending and receiving IP packets. On the other hand, because of the nature of wireless network itself, in which no clear physical connection exist, it is also important to ensure that the user is communicating with a legitimate authenticator rather than with rogue access point. At the same time the user may want seamless authentication for roaming that does not require any manual action. In short, security mechanism especially secure authentication in roaming environment is required in order to mutually ensure the identity of both the user and network while also minimizing the user interaction in the authentication process.

In this paper, we will emphasize the security aspect on the authentication mechanism for the WLAN roaming. The rest of this paper is organized as follows. In Section 2 we describe existing problems in the WLAN roaming and current solutions as well as our solution. In section 3 we present the design of our proposed system. In section 4 we discuss the implementation of our proposed system. In section 5 we discuss how the proposed system can eliminate the problems. Finally, section 6 concludes the paper and briefly mentions our future work.

2. Issues in WLAN Roaming

2.1 Existing problems in WLAN Roaming

As previously stated, since mobile user is increasing rapidly, roaming across WLAN infrastructure is required. Roaming technology will also continue to increase in popularity, if people could roam among more WLAN infrastructure. However, some issues are impeding further adoption of the technology to its continued popularity and success, in particular related with security and authentication such as; (1)proxy-based roaming, (2)insufficient password protection, (3)key management for shared secrets as well. In addition, due to general model of roaming, global access for roaming is limited.

(1) In order to provide inter-domain roaming services, the concept of proxy chaining [3] is the most widely used, where the authentication requests and responses are forwarded through a series of proxies to the correct destination (i.e. home server). One idea for roaming is to use proxy RADIUS protocol [4] to carry authentication information. It is the most prevalent protocol for roaming including being deployed in the public WLANs [5]. Roaming implementation based on the proxy chaining typically provide only hop-by-hop authentication and integrity protection [Figure 1]. This security weakness make proxy-based roaming vulnerable to attack from external parties as well as susceptible to fraud perpetrated by the roaming partners themselves [3]. Security threats include; rogue proxies message alteration, and theft of password as well as connection hijacking. As a result, proxy chaining based roaming is not suitable for wide-scale use on the Internet [3].

(2) When the user password employed and transmitted using RADIUS, confidentiality protection is considered insufficient, since the user-password hiding mechanism use only modification of one-way MD5 hash [6].

(3) Shared secret scheme used by the RADIUS brings forth key management problems. With RADIUS proxies, each two directly communicating entities have their own shared secret. The difficulties are emphasized with large number of secrets to protect, as there must own secret for each hop in the proxy chain [4]. This result in a large administrative burden, which may create temptation to reuse the shared secrets.

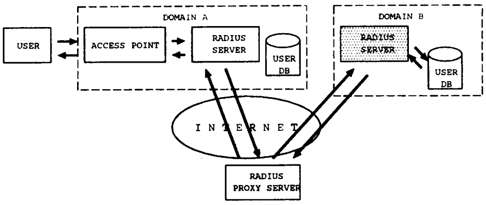


Figure 1 RADIUS proxy chaining

In addition, currently, general model of roaming that applicable to WLAN roaming presumes the prior existence of relationship among domains. There are two models of WLAN roaming; first model, a bilateral relationship between two parties to allow users to access one another's access point. In general, this model does not scale, as a domain need to maintain many bilateral agreements with another domain. Second model, third party relationship through intermediary/roaming consortia that consist of collection of domains. These two models carries-over much of the inherent operation difficulties caused by legacy authentication/authorization system. Moreover, roaming only achievable when relationships exist between domains. Consequently, it makes the user has to maintain multiple identities and credential that may be considered as a burden.

2.2 Current Solution

Several solutions are available in order to mitigate the problems mentioned above. At first, IP Security (IPSec) [7] or other Virtual Private Network (VPN) technology is used to protect the RADIUS messages between RADIUS servers [5]. This solution assures very good security level and it is good for one domain. However, IPSec imposes significant overhead, particularly if EAP authentication also involved and scalability issues for extending VPN amongst many domains. Furthermore, even IPSec or other VPN technology is used, the sending service provider may not be able to assure to their user that all the parties involved along the proxy will similarly protect the RADIUS traffic. Service provider could only be sure that the RADIUS message is protected between the sending provider and the receiving provider [5].

Another solution is to employ web based authentication system. Since this system is simple and easy to be implemented, many WLAN service providers use it in conjunction with IP packet filtering based on the MAC/IP addresses. Generally, HTTPS (HTTP over SSL) is also used in order to protect user's credentials (e.g. username and password). This way risk would harder for rogue access networks to collect user's credential. The main drawback of this system is that IP spoofing is possible. Although this problem can be mitigated as it is explained in [8], however, they do not help to protect the communication between the RADIUS servers. In addition, this system depends heavily upon user control over the login process to make decisions, clicks button, and manually enter credentials. In many situations, this amount of user interaction is undesirable as also previously stated in section 1.

On other hand, Diameter protocol [9] was defined as a successor to RADIUS, removing known RADIUS deficiencies. At the moment, Diameter is still an Internet Draft and subject to changes. In Diameter, IPSec and/or TLS as well as separate end-to-end security framework handle security aspect of protocol. So, basically there is no specific work has been done that relates to the client/server security. Furthermore, full IPSec/TLS implementation gives a very significant cost in bandwidth and communication overhead.

2.3 Proposed Solution for Secure Authentication in WLAN Roaming

Based on the problems mentioned before, we propose secure authentication system for WLAN roaming, by using digital certificates combined with delegated validation system. First, we assume that Public Key Infrastructure that is the basis for digital certificate exist and will become more widespread in the near future. Thus, we eliminate the use of intermediate proxy and use digital certificates as centerpiece of user identity whether user's request will be granted or denied for access to the Internet. Therefore, it is very important to employ reliable validation mechanism to authenticate a user that present a certificate, requesting to obtain connectivity. Secondly, we assume that the prior existence of relationship between domains may not exist and there may be more than one entity (e.g. WLAN access provider) in a single administrative domain. Hence, it is desirable to provide a mechanism for implementing domain's policies. In this case, policy refers to validation policy, since the validation determines whether or not to accept a certificate. Thus, validation policy becomes the reliance of access permission, which based on digital certificates. For this purpose, we use delegated validation system that enabling a client (e.g. RADIUS server) to offloading the validation process to a specific server. By doing so, we can provide reliable validation mechanism and allow central administration to manage policy on behalf of a domain.

3. System Design

3.1 System Overview

In order to provide secure authentication for wireless LAN roaming, certificate-based authentication is attractive because it enables mutual authentication and ensure that the user is communicating with the legitimate authenticator rather than with rogue access point. As such, it becomes essential, since on the wireless network, clear physical connection do not exist, unlike in wired networks.

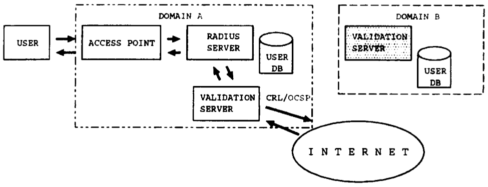


Figure 2 Proposed Authentication Scheme

Thus, the basic idea of our system is to use the digital certificate combined with the delegated validation system. Digital certificates can be used as centerpiece information that conveys identity of a user and attributes. It may be used also for authorizations. In wireless network, it can be achieved by using public key certificate-based authentication protocol running over Extensible Authentication Protocol (EAP) [10]. EAP provides architecture for several authentication mechanisms including the use of digital certificate like EAP-TLS [11]. In EAP, access point act as a "bridge", forwarding EAP packets without understanding the details between the user and local RADIUS server, using the RADIUS extension described in [12].

Users are authenticated by presenting an X.509 identity certificate [13] and proving that they know the associated private key. Through the use of digital certificate for authentication, it is possible for the local domain (i.e. WLAN access provider where the roaming user request for connectivity) to verify the user's identity without the need to proxy the authentication to the home server. This is possible, since the local domain is capable to verify that the user has access to the private key corresponding to the public key included on the user's certificate. Consequently, certificate validation mechanism that determines the acceptance of certificate is becoming critical. The security of the system is compromised by failure to verify certificate properly.

In order to perform reliable validation mechanism, we use delegated validation system where RADIUS server delegates all the validation process to specific validation server [Figure 2]. The use of delegated validation system gives other advantages for the WLAN roaming. It provides domain administrator with convenient central point to manage inter-domain trust relationship and implement domain's policies. It also provides interoperability between different domains. It means though prior relationship do not exist between local domain and the roaming user's domain, the certificate can be accepted as long as certificate it is valid according to the validation policy including certificate status is not revoked.

3.2 Delegated Validation System and Validation Policy

Validation processing determines whether or not the acceptance of a certificate or represent a suitable risk to a relying party. As such, it is a central and necessary basis to support reliance on the PKI-based authentication. The basic idea of delegated validation system is to allow a client to offload certificate validation process to a specific server. All the essential process of validation such as certificate path building, certificate path verification and certificate status checking may be done in specific validation server. The client is basically looking for a boolean response as whether or not it can accept the target certificate. There are several advantages can be achieved, including reduce overhead of validation process in the client side, allow central administration to manage inter-domain trust and policy, provide interoperability between different PKI domains as well. In addition, validation policy can be employed in the specific validation server.

Validation Policy may consist of a set of rules against which validation of the certificate is performed. To validate the user certificate in the context of WLAN roaming environment, validation policy is needed and may consist of following components as described below.

- *Define Certificate Authority (CA) as a trust point*

A domain can include one or more CA's certificate trusted by domain. For example, if WLAN domains have their own CA, CA's certificate can be inserted in the policy for all domains included in the roaming relationship. And for the user of a domain, which there is no prior relationship, we can check the validity of that CA's certificate if it is included in the user certificate or retrieve it from the directory pointed out in the certificate.

- *Define acceptable method for revocation checking*

For the purpose of revocation checking mechanism, requirements for the end user certificate can be defined. For example, for the user including in the domain roaming relationship, we can use loose method for revocation such as Certificate Revocation List (CRL). Then, for the user, which no prior roaming relationship, more strict revocation method can be employed such as Online Certificate Status Protocol (OCSP). As a result, the CRL distribution point or OCSP responder location must be included in the user certificate.

- *Define specific requirement for user certificate*

Validation policy might require user's certificate to contain specific extension with specific types or values. For example, user's certificate must include specific key usage only for TLS client authentication and it has to mention the domain organization's name for billing purposes or others instead of just mentioning certificate issuer.

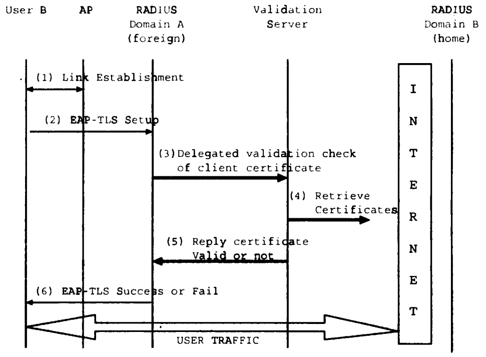

User B
AP
RADIUS Domain A (foreign)
Validation Server
RADIUS Domain B (home)
(1) Link Establishment
(2) EAP-TLS Setup
(3)Delegated validation check of client certificate
(4) Retrieve Certificates
(5) Reply certificate Valid or not
(6) EAP-TLS Success or Fail
USER TRAFFIC
INTERNET

Figure 3 Authentication Flow

3.3 Authentication Conversation

As previously mentioned, this proposed system use EAP-TLS for the authentication between user terminal and RADIUS server through access point. As it shown in Fig. 3, when the user requests to obtain an access, the process will begin with the user terminal first associates with the access point for the link establishment (event-1). Then the process will be proceed to set up EAP-TLS conversation by a handshake process between the user terminal and RADIUS server through the access point-AP (event-2). A conversation in EAP-TLS initially begins with EAP negotiation between the access point-AP and user terminal. Then it continues to the rest of handshake processes in EAP-TLS including *client_hello* and *server_hello* handshake messages as noted in [11]. But when it comes to the process of verifying user certificate, RADIUS will delegate the process of certificate verification to a specific validation server to ask whether the certificate can be accepted or not (event-3). Then the validation server will check the validity of the certificate based on the validation policy including basic verification process of a certificate such as verifying signatures, verifying valid date and so on. Validation server also need to retrieve the necessary certificates to verify the user certificate including for checking the revocation status according to defined method such as CRL or OCSP (event-4). Later, the result of validation process will be replied to the RADIUS server (event-5). If the verification succeeds, RADIUS server will return authentication response as access-accept and access-reject if the verification failed (event-6).

4. Implementation of prototype system

We have implemented the proposed solution as a prototype system. The main parts of our prototype system are process between RADIUS server and validation server including ceritificate validation mechanism. We use open source FreeRADIUS snapshot version for RADIUS server [15] and OpenSSL

0.9.7c [16] for the validation server in Redhat Linux 9. For the EAP-TLS conversation, the packets are conveyed using IEEE 802.1X standard [14] that defines an architectural framework for WLAN security between communicating entities. The 802.1X framework allows the use of TLS handshake in the context of EAP as a transport, with the final aim of achieving key agreement between the end-user with the RADIUS as an authentication server, which then delivers the shared key to access point (AP). For this purpose, we also use access point with 801.1X capability and user terminal with 802.1X support.

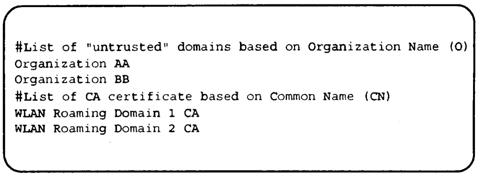
In order to realize delegated validation system, our proposal need to modify the verification process of certificate in RADIUS server. Instead of using original verification routine, user's certificate is delegated to specific validation server using request and response communication. We decided to implement the communication by secure communication such as Secure Socket Layer (SSL) to provide better protection of data transmitted. The RADIUS server simply ask to the validation server for response about status of certificate whether valid or not. Then, it will continue to the normal handshake process of EAP-TLS.

In the validation server, the real process of verification of certificate will be conducted. After receiving a user certificate from RADIUS server, the verification process will make two main checks:

- User certificate is checked according the validation policy
- User certificate is checked according the verification process of a certificate

Firstly, certificate is checked based on the validation policy. In this prototype, to avoid unintended use of general certificate purpose for WLAN roaming, we define the policy that each of user certificates must specify the certificate with the purpose only for TLS client authentication by using "Extended Key Usage" in the X.509 certificate's extension field. Then domain of the user will be checked whether it is trusted or not by using policy description. In this case, policy description is defined using file contains the lines of of "untrusted" domain [Figure 4]. The name of the domain is defined by using "Issuer Name" specifically at the Organization Name (O) in the field of X.509 certificate. For the revocation status check of user certificate, current prototype only considers to use CRL for simplicity. Since the prototype does not manage collection of CRLs certificate, user certificate must specify "CRL Distribution Point" in the X.509 certificate's extension field for the revocation checking.

Secondly, verification process of user's certificate. To verify a user's certificate, all the necessary certificates such as CA's certificates and CRL is needed. CA's certificate of a user certificate need to be retrieved if it is not available in our CA list. In our implementation, we consider that CA's certificate is included in CA list if the user's domain is part of roaming relationship. If there is no prior relationship with local domain, CA's certificate will be retrieved from the directory defined at "Authority Information Access" in the X.509 certificate's extension field. Therefore, we need to manage list of domains, which has roaming relationship by specifying the Common Name (CN) of CA's certificates by using file containing the lines of CA's list [Figure 4].



```
#List of "untrusted" domains based on Organization Name (O)
Organization AA
Organization BB
#List of CA certificate based on Common Name (CN)
WLAN Roaming Domain 1 CA
WLAN Roaming Domain 2 CA
```

Figure 4 Example of Policy File

5. Discussion

In this section, we give an analysis how the proposed system that use digital certificate combined with the delegated validation system can deal with existing problems mentioned in section 2.1

Firstly, regarding to the security threats in proxy chaining for roaming implementation.

- *Rogue proxies and message alteration*

Through the use of shared secrets it is possible for proxies operating in different domains to establish a trust relationship. However, since only hop-by-hop security is available in the proxy chaining, then untrusted proxies are capable to penetrate with a number of attacks include modification of messages. For example, an Access-Accept could be substituted for an Access-Reject, and without end-to-end integrity protection, there is no way to detect this. In our proposed system, this kind of attack does not work, because authentication process terminates at the local domain RADIUS server. Hence, the risk of rogue proxies is eliminated.

- *Theft of passwords*

It is obvious that theft of password can be prevented in our system, because our system only supports certificate-based authentication without proxies. Consequently, there is no circumstance either for local domain or proxy domain to have access to passwords.

- *Connection hijacking*

In this form of attack, the attacker attempts to inject packets into the conversation between local domain and home server. RADIUS does not support encryption, and as described in [4], only Access Reply and Access Challenge packets are authenticated. Again, since certificate-based roaming avoids proxying of authentication, the risk of connection hijacking is reduced.

Secondly, regarding to the insufficient password protection and key management problems. In the proposed system, it is quite clear that there is no password used and transmitted in the local domain or even proxy domain, because certificate-based authentication is employed. Therefore, eavesdroppers cannot learn anything useful and password protection issue can be eliminated. Moreover, key management problems to distribute shared secrets especially in large scale also can be reduced. Shared secrets basically uses the concept of symmetric encryption technique, which has one secrets used by both entities. While certificate based authentication uses the concept of asymmetric encrypting techniques, which has different key pairs that are private and public key for encryption and decryption. Public key usually is made available to be accessed. Therefore, by using digital certificates, the management problem can be minimized.

Finally, since delegated validation system enables interoperability between domains, access request from roaming user is not limited only when user's domain has agreement with the local domain (i.e. the place where user ask for an access). However, from the point of technical view, though there is no prior relationship between local domain and roaming user's domain, user's access request still can be processed. Because the acceptance of the request depends on the certificate validation process and validation policy as well in order to verify user's certificate correctly. As a result, user could have better roaming access across more WLAN infrastructures without the need to maintain multiple identities and credentials.

6. Conclusion and Future Work

With the increasing number of mobile workers, security in particular seamless authentication in WLAN roaming access is becoming critical. We proposed authentication scheme by using digital certificate in conjunction with delegated validation system that can prevent security threats in proxy chain roaming while also minimized user interaction in the authentication process. Digital certificate enables the system to eliminate the use of proxy chaining in WLAN roaming and makes key management problem smaller in scale. While, delegated validation system supports inter-domain roaming by emphasizing on the reliable validation mechanism as well as its policy as a reliance of access permission, which based on the digital certificate. Although this system requires a user to have digital certificate, by doing so, we believe that the approach can provide as basis for independent model of WLAN roaming which may provide better scalability.

A prototype system is developed to evaluate our authentication scheme. With several modifications in a RADIUS server and newly developed validation server, it is confirmed that our scheme works with standard wireless access point and can provide better security protection for WLAN roaming system.

We are currently working on the building testbed environment to evaluate the performance of the system through our prototype. For the future work, we consider to develop the system for handling other aspects in WLAN roaming scheme such as authorizations and accounting.

References

[1] Gartner Inc, http://www.gartner.com

[2] Pyramid Research, http://www.pyramidresearch.com

[3] B. Aboba, J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming",Internet RFC-2607, June 1999.

[4] C. Rigney, S. Williams, A. Rubens, W. Simpson, "Remote Authentication Dial in User Service (RADIUS)", Internet RFC-2865, June 2002.

[5] Wi-Fi Alliance, "Best Current Practices for Wireless Internet Service Provider (WISP) Roaming", version 1.0, February 2003.

[6] Dobertin, H, "The Status of MD5 After a Recent Attack", CryptoBytes Vol.2 No.2, Summer 1996.

[7] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", Internet RFC-2401, November 1998.

[8] Yasuhiko Matsunaga, Ana Sanz Merino, Takashi Suzuki, Randy H. Katz, "Secure Authentication System for Public WLAN Roaming", WMASH '03, September 2003.

[9] Pat R. Calhoun, John Loughney, Erik Guttman, Glen Zorn, Jari Arkko, "Diameter Base Protocol", Internet draft-aaa-diameter-17, December 2002.

[10] L.Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", Internet RFC-2284, March 1998.

[11] B.Aboba, D.Simon, "PPP EAP TLS Authentication Protocol", Internet RFC-2716, October 1999.

[12] C. Rigney, W. Willats, P. Calhoun, "Radius Extensions", Internet RFC-2869, June 2000.

[13] R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", Internet RFC-3280, April 2002.

[14] IEEE Std 802.1X-2001, "Port Based Network Access Control", June 2001.

[15] FreeRADIUS server project, http://www.freeradius.org

[16] OpenSSL Project, http://www.openssl.org