제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

WLAN에서 Kerberos v5를 이용하여 안전성을 강화한 DIAMETER의 확장

위룬 씨버리락*, 김태윤*
*고려대학교 컴퓨터학과
e-mail: wiroon@netlab.korea.ac.kr

DIAMETER Strong Security Extension using Kerberos v5 in WLAN

Sriborrirux Wiroon*, Tai-Yun Kim*
*Dept. of Computer Science and Engineering, Korea University

Abstract

The demand for Wireless LAN (WLAN) access to use their network and the Internet is surged dramatically over the past year. Since WLAN provides users' access from anywhere in the workplace without having to plug in, it therefore leads the WLAN market to grow steadily. Unfortunately, the first WLAN implementation designed primarily for home networking did little to address these security issues. Moreover, although the 802.11b standard published by IEEE in 1999 improved WLAN connections LAN-equivalent speed and security from the 802.11 standard. However, there still are several flaws such as the weaknesses in the Authentication and WEP encryption schemes in the IEEE 802.11 WLAN standard. In this paper, we propose WLAN architecture for providing the strong centralized authentication, encryption, and dynamic key distribution on a WLAN. Additionally, this proposed architecture is able to support roaming users and is flexible and extensible to future developments in the network security.

1. Introduction

Currently, the security issue is one of the most significant in WLAN that is becoming one of the most interesting targets for hackers today as well. A WLAN, using radio frequency technology (e.g. 2.4 GHz for 802.11b or 5 GHz for 802.11a) to transmit and receive data over the air, still cannot safeguard information traveling on it well. The 802.11 security features alone do not provide a complete wireless security solution because of many vulnerabilities such as *MAC Address Authentication* – This type of authentication does not consider the identify of the user because open and shared key authentication involves the station that authenticates to an Access Point (AP) using the station's MAC address. Thus, anyone stealing a laptop or NIC configured with the WEP keys can obtain network access, *One-way Authentication* – WEP authentication is one-way only. So the AP does not need to authenticate to the mobile station. This may allow a rouge AP to hijack that station's data, *WEP key/RC4 Vulnerability* – Recently, papers described successful attacks on the WEP algorithm. This new report shows that WEP, which is based on the well known and widely implemented RSA RC4 algorithm, can be easily cracked in both 40- and 128-bit variants in less than 15 and 45 minutes in order by using off-the-shelf tools readily available on the Internet. In the presence, there are varieties of security extensions or proprietary techniques having been implemented in order to provide the requirements of WLAN security. The technologies approached are such as a network layer encryption approach based on IPSec, a mutual authentication-based, key distribution method using 802.1X, and some proprietary improvements to WEP recently implemented by Cisco. Additionally, IEEE 802.11 Task Group "i" (TGi) is working on standardizing WLAN encryption improvements.

The best of the core security issues thus is standards-based approach being extensibility and compatibility with future WLAN products and standards. To point out the main key elements for WLAN security, its requirements should be provided as below:

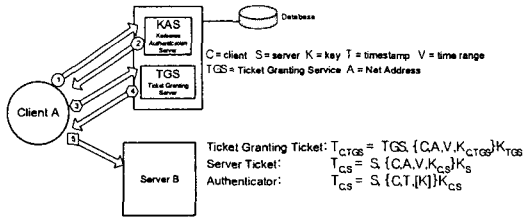
Table 1: WLAN security requirements

Requirement	*Details*
Mutual authentication	both the client and server must authenticate with each other.
End-to-end encryption	user data must never be allowed to appear in the clear on the network except at authorized and points.
Per-client keys	keys must be unique for each authorized user. This prevents the compromising of security keys due to theft or otherwise unauthorized access.
Key distribution	a technique for the central management of security keys
Full support for mobility	finally, any security implementation must take into account the fundamental nature of wireless LANs that users can move from AP to AP as they roam throughout a given facility, and even between facilities.

We start analyzing the current approaches that are Kerberos and RADIUS approach in Section 2 and 3. Then in Section 4, we discuss the related works, which proposed several techniques to enhance security issues in WLAN. In next section 5, we also discuss some drawbacks occurring in the current approaches and present the requirement-matched framework (architecture) that provides the stronger security in WLAN by using "DIAMETER security extensions using Kerberos v5". Finally, we give some conclusions in Section 6.

2. Kerberos

Kerberos [4] is an authentication service developed at MIT in the 1980s. It provides all the tools for maximum security and protection of our network. Two versions of Kerberos are in common use. First Kerberos v4 is still widely used but there are some of the security deficiencies. Thus, next version 5 of Kerberos was proposed to address the limitations of version 4 [6] in two areas: "*environmental shortcomings*" and "*technical deficiencies*"[4]. Since Kerberos v4 was insecure because it used a nonstandard mode. So Kerberos v5 uses CBC mode for encryption. Kerberos provides a mutual authentication between client and server and between servers before a network connection is opened. Note that Kerberos is independent of the security features defined in 802.11 standard. This is particularly important since changes to 802.11 securities will be made as part of TGi group. Moreover, Kerberos v5 have exceptionally low overhead, making it well-suited for WLAN applications.



1. Client _ TGS: $\{C, TGS\}K_C$
2. KAS _ Client: $\{K_{C,TGS}\}K_C$, $T_{C,TGS}$
3. Client _ TGS: $\{A_{C,TGS}\}T_{C,TGS}$
4. TGS _ Client: $\{K_{C,S}\}K_{C,TGS}, T_{C,S}$
5. Client _ Server: $A_{C,S}, T_{C,S}$

Ticket: {identities, IP addresses, timestamp, lifetime, session key} encrypted with the server's key
Authenticator: {identity, IP address, timestamp} encrypted with the session key

Figure 1: The Kerberos version 5 layout

3. RADIUS (Remote Access Dial-In User Service)

RADIUS [2] is today the most widely used AAA protocol in the world, in competition with TACACS+[5] and Kerberos. Requests and Responses, carried by the RADIUS protocol between a Network Access Server (NAS) and a RADIUS authentication server, provide the information needed by a RADIUS server to authenticate and to establish authorized network service for users.

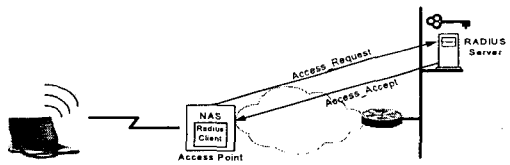


Figure 2: RADIUS function

The RADIUS client on the NAS forwards the end user's credentials in an Access-Request message to the RADIUS server. After validating the end user's credentials, the RADIUS server returns an Access-Accept message to the client as shown in Figure 2. The market has overwhelmingly adopted RADIUS as the preferred authentication process on WLANs for several compelling reasons such as

authentication is user-based rather than device-based for example; if a laptop is stolen, it is not necessarily imply a serious security breach. Moreover, RADIUS eliminates the need to store and manage authentication data on every AP on the WLAN, making security considerably easier to manage and scale.

4. Related Works

Currently, there are varieties of security extensions presented. For instance, one of the most obvious is service, which operate at network layer or above. One popular technique is the use of a VPN solution for wireless access being currently the most suitable alternative WLAN security approach to WEP and MAC address filtering. In addition, an alternative WLAN security approach focuses on developing a framework for providing centralized authentication and dynamic key distribution. A proposal jointly suited to the IEEE by Cisco Systems, Microsoft, and other organizations introduced an end-to-end framework using 802.1X and the Extensible Authentication Protocol (EAP), allowing wireless client adapters that may support different authentication types to communicate with different back-end servers such as RADIUS, to provide this enhanced functionality. Furthermore, standardizing WLAN encryption improvements IEEE 802.11 TGi working on, are that *WEP key Hashing* to prevent the weak IVs from being used to derive the base WEP key and *Message Integrity Check* to protect WEP frames from tampering.

5. Proposed Architecture

People have been reluctant to embrace WLAN development because of the inherent security issues. Most of the available solutions involve the use of VPN technology or similar, to circumvent the problem than solve it. Moreover, use of VPNs have not been standardized and may have implementation dependencies that can make them complex in operation.

However, Kerberos v5 gets to the core of the problem and ensure end-to-end network security. It is entirely based on open standards with a well-tested and widely understood reference implementation and is a mature standard, which have been scrutinized cryptologists and security experts. In addition, Kerberos v5 can be easily implemented on an embedded device with small code size requirement and is flexible and extensible for future developments in network security.

With a RADIUS used in WLAN applications, the problem is that its heritage as a dial-up remote access product is visible there is currently on support for mobility, no key distribution or support for key exchange, no inherent security features, and fundamental issues with latency that can interfere with roaming. Therefore, in order to support Mobile IP security and roaming and overcome limitations of RADIUS, the DIAMETER protocol was proposed as a new framework for the next-generation AAA server. The DIAMETER [3] defines message integrity and Attribute-Value-Pair (AVP) encryption using symmetric transforms to secure the communication between two DIAMETER nodes and to prevent the authentication replay attack while RADIUS not.

In this paper, we thus take the advantages of DIAMETER and Kerberos v5 to work together in order to provide very strong security issues in WLAN as proposed in [1]. In [1], they proposed how strong authentication and encryption can be provided in the DIAMETER protocol, by employing security services provided by Kerberos v5. Kerberos v5 security contexts setup across DIAMETER peers using DIAMETER protocol to carry Kerberos v5 messages for context establishment. Also all Kerberos v5 security contexts can be created and saved for the length of a DIAMETER session.

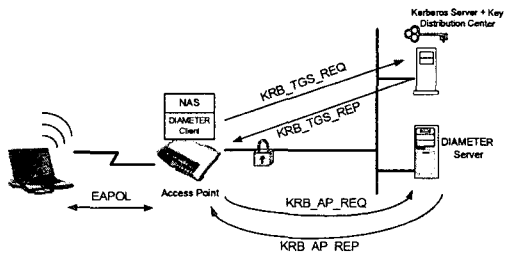


Figure 3: Combination of DIAMETER and Kerberos v5 in WLAN

The architecture we propose as shown in figure 3, firstly use the adaptation of 802.1X by using the EAPOL-Key frame to rotate WEP Keys to update themselves at the station in order to mitigate the static WEP keys security risks. Then, the DIAMETER client uses the Kerberos service principal for service discovery i.e. to discovery the capacity of a DIAMETER server to support Kerberos. After that, in order to get the service principal ticket for the DIAMETER server, the DIAMETER client will send a KRB_TGS_REQ to the TGS. The TGS will reply with a KRB_TGS_REP that contains a session key and Kerberos ticket to the

DIAMETER service. Between NAS and DIAMETER server the KRB_AP_REQ/KRB_AP_REP message are carried in order to turn on mutual authentication mode and specify to DIAMETER server to use its secret key to decrypt the Kerberos ticket. The symmetric keys that are negotiated would be used to provide integrity protection and privacy protection for the DIAMTER AVPs. This can provide all WLAN security requirements and improve security issues of the end-to-end connection in WLAN i.e. "*the end-to-end Integrity Checksum*" in case of preventing a downgrade attack by generating a KRB_SAFE message, and making "*the end-to-end confidentiality protection*" for the DIAMETER AVPs via encryption by generating a KRB_PRIV message into the Kerberos-Data AVP as described in [1].

Moreover, in case of heavy processing cost characteristic, use of DIAMETER that has a 32-bit alignment requirement can be handled efficiently by most processors but RADIUS does not impose any alignment requirements, which adds an unnecessary burden on most processors. Additionally, use of Kerberized DIAMETER can scale to support potentially very large networks, and the their severs can be located anywhere in the network. The evaluation of the our solution shown in the table below;

Table 2: Solution Comparisons

Requirement	Another Approaches (RADIUS, VPN etc.)	Proposed Solution
Compatibility	👍👍	👍👍👍
Mutual Authentication	👍	👍👍👍
Encryption	👍👍👍	👍👍👍
End-to-End Integrity	👍👍	👍👍👍
Confidentiality	👍👍	👍👍👍
Manageability	👍👍	👍👍👍
Scalability	👍	👍👍👍
Key Distribution	👍👍	👍👍👍
Full Support Mobility	-	👍👍👍
Unique Key per Client	👍	👍👍👍
Implementation	👍👍	👍👍
Performance	👍👍	👍👍👍

👍👍👍 = Excellent, 👍👍 = Good, 👍 = OK, - = Does not fulfill

6. Conclusions

In this paper, we focus on developing a framework for providing the strong centralized authentication, encryption, and dynamic key distribution on a WLAN. This also proposed architecture is able to support roaming users and is flexible and extensible to future developments in the network security. As the three key services i.e. authentication, privacy (encryption), and access control (authorization), they are needed for a comprehensive WLAN security implementation. The architecture that we presented by combining DIAMETER with Kerberos v5 for strong security in a WLAN, is believed that can enhance the current drawbacks and be flexible and extensible for the future developments in the network security.

References

[1] Narayan Kaushik, "DIAMETER Strong Security Extension using Kerberos v5", draft-kaushik-diameter-strong-sec.00.txt, February 2001.

[2] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service ", RFC 2865, June 2000.

[3] P. Calhoun, A. Rubens, H. Akhtar, E. Guttman, "DIAMETER Base Protocol", draft-calhoun-diameter-17.txt, IETF work in progress, September 2000.

[4] Stallings William, "Cryptography and network security – Principles and Practice 2nd Ed", Prentice Hall, 1998 Edition.

[5] D. Carrel, Lol. Grant, "The TACACS+ Protocol Version 1.78", draft-grant-tacacs-02.txt, January 1997.

[6] J. Kohl, C. Neumsn, "The Kerberos Network Authentication Service (V5)", RFC1510, September 1993.