5-2009

Token-based Fast Authentication for Wireless Network

Ghassan Kbar
American University in Dubai, gkbar@aud.edu

Wathiq Mansoor
American University in Dubai, wmansoor@aud.edu

32. TOKEN-BASED FAST AUTHENTICATION FOR WIRELESS NETWORK

Ghassan Kbar
American University in Dubai,
gkbar@aud.edu

Wathiq Mansoor
American University in Dubai,
wmansoor@aud.edu

Abstract

Wireless Networks based on WIFI or WIMAX become popular and are used in many places as compliment network to wired LAN to support mobility. The support of mobility of clients, the continuous access anywhere and anytime make WLAN preferable network for many applications. However, there are some issues associated with the usage of WLAN that put some restriction on adapting this technology everywhere. These issues are related to using the best routing algorithm to achieve good performance of throughput and delay, and to securing the open access to avoid attacks at the physical and MAC layer. IEEE 802.1x, suggested a solution to address the security issue at the MAC layer and but there are varieties of implementations address this solution and they differ in performance. IEEE 802.1af tried to address other security issue remained at the MAC layer but it is still at early stage and need verification for easy deployment. In this paper a new technique for securing wireless network using fast token-based authentication has been invented to address the vulnerability inherited by the wireless network at the MAC layer using fast authentication process. This technique is based on an authentication server distributing a security token, public authentication key, and network access key parameter to eligible mobile client MCs during registration. All messages will be encrypted during registration using temporary derived token key, but it will use derived valid token key during authentication. Authenticated MCs will then use derived group temporal key generated from the network access parameter key to encrypt all messages exchanged over the wireless network. The token, the authentication key and the access network parameter key will be only distributed during registration. This makes the security parameters known only to authentication server, authenticator and MC. Hence, this technique will protect the wireless network against attack since attackers are unable to know the token and other security keys. Moreover, it will avoid the exchange of public keys during authentication such as the one used in other existing technologies, and consequently speedup the authentication phase which is very critical to wireless technologies.

1. Introduction

WLANs based on 802.11 standards are vulnerable to attack if no authentication or weak encryption key is used. In addition man-in-the-middle (MiM) attack becomes a great concern for

users and owners in WLAN. Several types of attacks have been reported and been studied extensively by researchers worldwide. Although attempts are continuously being made to address the security issues in the later versions of 802.11 [1], security of WLAN remains challenging. Despite the enhancements provided by WEP for WLANs, the demands for a further secured environment still a high priority issues in wireless network. There was considerable ongoing research to address the security issue in 802.11 WLANs. John Bellardo et al [2] describes the vulnerabilities of the 802.11 management and media access services, and different types of Denial of- Service attacks possible on 802.11 networks. This paper suggests the implementation and evaluation of non-cryptographic counter measures that can be implemented in the firmware of the MAC hardware. Meritt Maxim et al [3] present a review of the threats that are unique to a wireless environment especially the problems that occur due to inter-cell roaming. A detailed description of MiM attack and its ramifications have been discussed in [4]. This paper suggests the usage of a VPN (Virtual Private Network) and the necessity that all the traffic requires to pass through the VPN to a trusted, secure, wired network. Joshua Wright [5] reviews the techniques attackers utilize to disrupt wireless networks through MAC address spoofing. This paper proposes a method of detecting anomalous MAC addresses. Shared key authentication implemented using Wired Equivalent Privacy algorithm (WEP) provides a much higher degree of security than the open system approach. This algorithm performs encryption of messages by generating secret shared encryption keys that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdropping on the network. WEP is easy to administer. Basically the device using the 802.11 NIC is configured with a key, which in practice usually consists of a password or a key derived from a password. The same key is deployed on all devices, including the access points. While increasing the encoding bits does make breaking a WEP communications more difficult, it doesn't fundamentally improve wireless network security. A longer key, even 256-bits, just means that a cracker needs to collect more data. Cisco's LEAP wireless authentication process helps eliminate security vulnerabilities by supporting centralized, user-based authentication and the ability to generate dynamic WEP keys [7]. Cisco LEAP is one of the extensible authentication protocol (EAP) types specified by 802.1X [6]. Using EAP for authentication, the access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the access point can verify the client's identity using an authentication server. Similar to LEAP, Wi-Fi Protected Access (WPA) [8] also securely authenticates wireless users to the network. There are a couple of differences between the two, however. Unlike LEAP which uses EAP for authentication, WPA specifies Temporal Key Integrity Protocol (TKIP) for distributing dynamic encryption keys and then lets the client use the EAP type of their choice. In WPA these two functions are separate from each other. WAP uses 4-way key handshake – advanced four-way key handshake that helps in solving problems in previous key exchange. WPA is a subset of the abilities of 802.11i, including better encryption with Temporal Key Integrity Protocol (TKIP), easier setup using a pre-shared key, and the ability to use RADIUS-based 802.1X authentication

of users [9]. WPA comes in two flavors, one that's easier for home users, and one for enterprises (the latter incorporates 802.1X). Official 802.11i (IEEE 802.11 Working Group) [10] is the long-awaited security standard for Wi-Fi networks that upgrades the former "official" wireless security standard, has all the abilities of WPA and adds the requirement to use Advanced Encryption Standard (AES) for encryption of data. AES provides enough security to meet the needs for the Federal Information Processing Standard (FIPS) 140-2 specification. Another attack facing wireless network is rogue access point. In this case, the motivation of the attack is to trick wandering wireless users into attempting to associate with the rogue access point instead of the intended, authorized one. After the user has inadvertently connected to a rogue AP, the rogue operator may attempt to collect login credentials or perform a man-in-the-middle attack where all of the traffic traversing the unauthorized device is received, captured, and passed on to the intended destination. The IEEE 802.1af [11] is an amendment to the IEEE 802.1x, which identifies and specifies protocols that establish security association for IEEE 802.1ae, and facilitates additional use of industry standard authentication, authorization, and key management protocols. A proposed Intelligent Policy Management System IPMS architecture model [14] enhances the current security practices for WiMAX and can be applied to other wireless technologies. IPMS along with the IEEE 802.1ar [13], IEEE 802.1af [12], and IEEE 802.1ae [11] resolve key security vulnerabilities for open access networks and reduce the risk of having rogue devices introduced into the network. Wireless security will continue to be a concern for the foreseeable future. Although a single overall solution has yet to be perfected, the best protection is always prevention [16]. WLAN clients and enterprise infrastructure can still be vulnerable to a variety of threats that are unique to WLANs. These threats cannot be mitigated by traditional firewall technologies and virtual private networks (VPNs), nor eliminated through encryption and authentication mechanisms used in conventional enterprise network security systems. Conventional enterprise network security systems are not designed to detect and prevent threats from MAC spoofing, honeypots, DoS, and ad hoc wireless networks. However, An IDS/IPS specifically designed for WLANs addresses the risks associated with this networking technology [17]. Five fundamental areas which must be considered when securing the enterprise against wireless threats as described in [18]. These are: Creating a wireless security policy, Securing the enterprise wireless LAN, Securing the enterprise wireLine (Ethernet) network, Securing corporate laptops from wireless threats when outside the enterprise, Educate employees regarding the wireless policy. Other security techniques for addressing the wireless security at different layers have been covered in next section. These techniques explain the different way used for Wireless network authentications. However to address the issues of flexibility and high speed authentication technique, a new novel approach using Token-based fast Authentication method for Wireless network is covered in section III. In addition implementation of this technique is presented in section IV, and conclusion is done in section V.

2. Wireless Security at Different Layers

Wireless access points are just another entry point to the network which can lead to easily reaching the more sensitive information on the wired side. There are different attacks facing

wireless devices such as attacks on integrity, and attacks on availability that are designed to prevent legitimate users from using a resource. Example of availability attack is the Denial of Service (DoS) attack that uses crafted packets which might cause a networking device to crash or freeze. It is well known that the open system authentication in WLAN is mainly done in one direction for Mobile client MC to prove its credentials to an access point (AP) but the AP is not required to authenticate itself to the MC. This basic deficiency leads to several potential security attacks on WLAN which can be exploited by the MiM attack.

To prevent the wireless network from being discovered, a proper *secure authentication* before allowing anyone to associate with the access point should be used, and the *best available encryption* to protect the data in transit should also be considered. Different authentication mechanisms can be used in wireless network to allow only eligible MC to associate with AP. Once authentication phase is complete, encryption key such as WEP key can be used to encrypt all messages exchanged over wireless network. *Shared keys* (or *private keys*) can be used to encrypt data such as WEP encryption used in 802.11b. However, if an access point is set up for WEP with shared keys, it will require that a key be entered on both the client and the access point. Using WEP encryption makes eavesdropping more difficult, but not impossible. WEP encryption is known to have several weaknesses that can be exploited by attackers with moderate resources. To address the issue of strong wireless authentication and key management IEEE 802.1x has been developed. This mechanism provides a facility for port-based authentication and key distribution via an external authentication server, such as RADIUS or Kerberos. IEEE 802.1x can provide layer 2 authentication for wired devices connected to a switch. In these environments, only pre-specified MAC addresses are allowed to have network connectivity. Implementing 802.1x requires an authentication server that supports Extensible Authentication Protocol EAP. There are already a handful of commercially available servers exist that do have that support including Microsoft IAS, Cisco Secure ACS Server, and Steel-Belted Radius from Funk Software. Unfortunately, support for EAP in open-source RADIUS servers still a challenge. EAP provides a mechanism to enable per-user, per-session keys (EAP-TLS) instead of authenticating MC based on its MAC or shared-key. EAP requires users to enter a username and password that is unique to the wireless network or that is part of an existing authentication mechanism such as LDAP or Microsoft Windows. Wireless EAP has also been enhanced to include transport layer encryption and key management. This addition tried to eliminate the risks and burden of traditional WEP with static keys. EAP uses a RADIUS server for centralized credential management and accounting to dynamically distribute encryption key to authenticated user, and therefore eliminate the need for administrators to manually update static WEP keys. There are several types of EAP; the types that are relevant to wireless include the following:

- **EAP-MD5** provides a strong authentication mechanism using MD5 hashes instead of plain text passwords.
- **EAP-TLS** provides the key management for transport layer encryption.
- **EAP-TTLS** is similar to EAP-TLS but uses server certificates.
- EAP-enabled access points act as RADIUS clients in WLANs.
- LEAP (also known as EAP-Cisco Wireless) uses dynamically generated WEP keys, 802.1x port access controls, and mutual authentication between the MS and the RADIUS server [20].

A technical comparison between TTLS and PEAP has been done in [15]. TTLS has a number of slight advantages over PEAP and offer a slight degree of flexibility at the protocol level. Other comparison between different EAP products has been presented in [19]. The use of mutual authentication would secure the wireless network during the phase of authentication between the AP and the Mobile clients. There is still need to provide secure wireless communication channel over the Internet using secure SSL according to G. Kbar [21], which uses the double key encryption decryption during SSL authentication. To augment WLAN security an IPSEC VPN client can be added to each of the mobile users. This solution requires the client to establish a VPN connection after associating with an AP. One of the primary advantages of using a VPN client with the WLAN adapter is the additional authentication option that most VPN clients offer which make it stronger. Most VPN clients can handle multiple types of authentication including RSA SecureID, Crypto Card, and RADIUS, any of which would be considerably stronger than a simple username and password.

3. Token based hashed MC ID for securing wireless network

As described in section II, strong authentication mechanisms suggested by IEEE 802.1x has improved the wireless security since it goes beyond shared key authentication to use authentication server AS that applies security at transport layer to validates Supplicants/MCs. This is done using EAP protocol that allow AS to request login name, password and hashing or public/private key to authenticate MCs as well its users . However, exchanging the public key and digital signature used in EAP-TLS is need for every authentication session. This will slow down the authentication process and forces MC to wait for long authentication phase before it gets fully associated with AP as shown in Figure 1. In EAP authentication phase, the public key and digital signature used for authentication will be exchanged between supplicant (MC) and Authenticator Server AS in order to complete this mutual authentication. This adds lots of overhead which makes this process slow and MC has to wait for long period of time during this phase. Following this authentication phase, authenticated MC will get Pairwise Master Key (PMK) from AS, which is used to generate Pairwise transient key (PTK). This PTK is used to install a key at the MC and AS, and is also used to generate the Group Temporal Key (GTK). The GTK will be used by both supplicant (MC) and Authenticator (AP) to encrypt all messages exchanged between each other or between other MCs.

To address the issue of fast authentication at WLAN, a new novel technique has been suggested in this paper to exchange a valid token VT during registration phase between AS and MC. This token will be used during authentication phase to generate a valid token key to encrypt all messages during this authentication phase. The supplicant will get a new use name, password and temporary token TT by the administrator to register in the WLAN. As shown in figure 2, step 1 to 6 used to allow MC discovers AP which is similar to IEEE 802.1x standard shown in figure 1. After a supplicant/MC detects and get associated with the authenticator/AP, it generates a temporary token key TTK from the MC's MAC and TT. Then it uses this TTK to encrypt the user credentials (name, and password) and send it along with the TT given by administrator and MC's MAC to Authenticator in step7. The Authenticator will forward this request to AS. The AS will check if MC is not registered before, by evaluating the received TT, and generate a TTK based on the received MAC, and TT. Then AS will decrypt the request to extract the login name

and password and validate them against its stored database. If all validations pass, AS would authenticate MC and pass another valid token VT to this MC along with its authentication token key ATK, encrypted by TTK as shown in step8. The MC will then decrypt the response, extract the valid token VT to store it for future authentication. It will also extract the ATK to send encrypted acknowledgment to the AS. Following the successful authentication, AS will send a PMK to MC which can be used to drive other GTK that would be used for encrypting all messages. If supplicant/MC was registered before, or hacked, the AS will challenge the MC to authenticate itself as described in figure 3. In the above mechanism described in figure 2, a temporary token will only be used during registration to generate a TTK which is used to encrypt all MC messages during authentication. The Valid token VT is encrypted and sent only by the AS MC during registration phase. This will avoid hacker from getting this VT during authentication phase. This VT will be stored permanently on the MC and will be used to generate a VTK key that can be used during the authentication phase as shown in figure3. Since the VT will never be transmitted after registration, it would be extremely hard for hacker to know the key associated with this VT, and consequently would be unable to hack this key if relevant long VTK key is used. The steps of authentication are described in the authentication phase figure3. In this figure, once MC and authenticator/AP discover each other at step 1, and 2, MC would generate a valid token key VTK using the stored VT, MC's MAC address and current date. Then at step 3, Authentication request would be sent to AP and forward it to the AS at step 4. In this request, user credentials (user name and password) would be encrypted by VTK, then by ATK. In addition, MC's MAC and current date used to generate the VTK would be encrypted by ATK which is known to MC during registration phase. AS would decrypt the request using its ATK key and extract the MAC and date. It then checks its database to identify the Valid Token VT linked to this MAC address. If MC is registered before, its MAC address would be found, as well as the VT associated with this MAC. The AS then would generate a VTK key to decrypt the request and extract the user credential (login name and password). Date has been used during authentication to detect replay attack. If user credential is valid, and accept authentication message including a PMK would be send to authenticator/AP at step5. The AP would update its own database and send authentication success at step6. This will follow up by success association as shown in step 7 and 8. Once MC and AP pass the association phase, both will derive GTK as shown in encryption phase on figure3. This encryption phase is the same as the one used in standard IEEE 802.1x shown in figure1.

4. Implementation result

A complete program using C++ has been developed. Following is the algorithm for the program is as follows:

a. User generates the TTK from TT and MAC of the user machine.

   1. Convert TT for 128 bits representation.

   2. MAC is a 128 bits representation.

   3. Concatenates TT with MAC to produce the TTK for symmetric encryption of size 256 bits.

b. Encrypt the pair of UserID and Pwd using the TTK.

    1. Convert UserID to 128 bits representation.

    2. Convert Pwd to 128 bits representation.

    3. Concatenates UserID and Pwd, then apply the TTK for encryption using XOR.

c. The user sends the encrypted UserID and Pwd pair and TT, and MAC as a plain text.

d. Server generates TTK from the received TT and MAC pair. Same as step (a) above.

e. Server decrypts the encrypted UserID and Pwd pair using TTK using XOR.

f. Server generates VT and mapped to MAC value.

g. Server generates asymmetric encryption key ATK using RSA method.

h. Server sends VT and the public part of ATK encrypted by TTK to the user.

i. The private key of ATK is always kept in the server and never sent to any user.

j. User decrypts the encrypted VT and the public key of ATK using TTK.

k. User generates VTK from VT, date and MAC for future authentication and association.

l. User sends the messages using ATK for encryption.

m. For future authentication with the server; user encrypts UserID and Pwd using VTK and then encrypts it with ATK. Send the MAC and Date pair encrypted with ATK only.

n. Server uses the table to retrieve the VT associated with MAC then it uses the VT along with MAC and date to generate the VTK. This VTK will be used to decrypt the association information to extract the UserID and Pwd. If UserID and Pwd can be verified, the client would pass the authentication phase and send signal to AP to allow client association. Note that valid token VT will only be sent in encrypted format during registration.

Only the implementation of the token based registration and authentication has been implemented which is the contribution of this paper. Whereas the second part of encrypting data is based on the standard IEEE 802.x. The implementation proved the transfer of valid token VT along with server public key in encrypted format during registration only. This will minimize the chance for hacker to sniff packets to determine these parameters and used for future authentication.

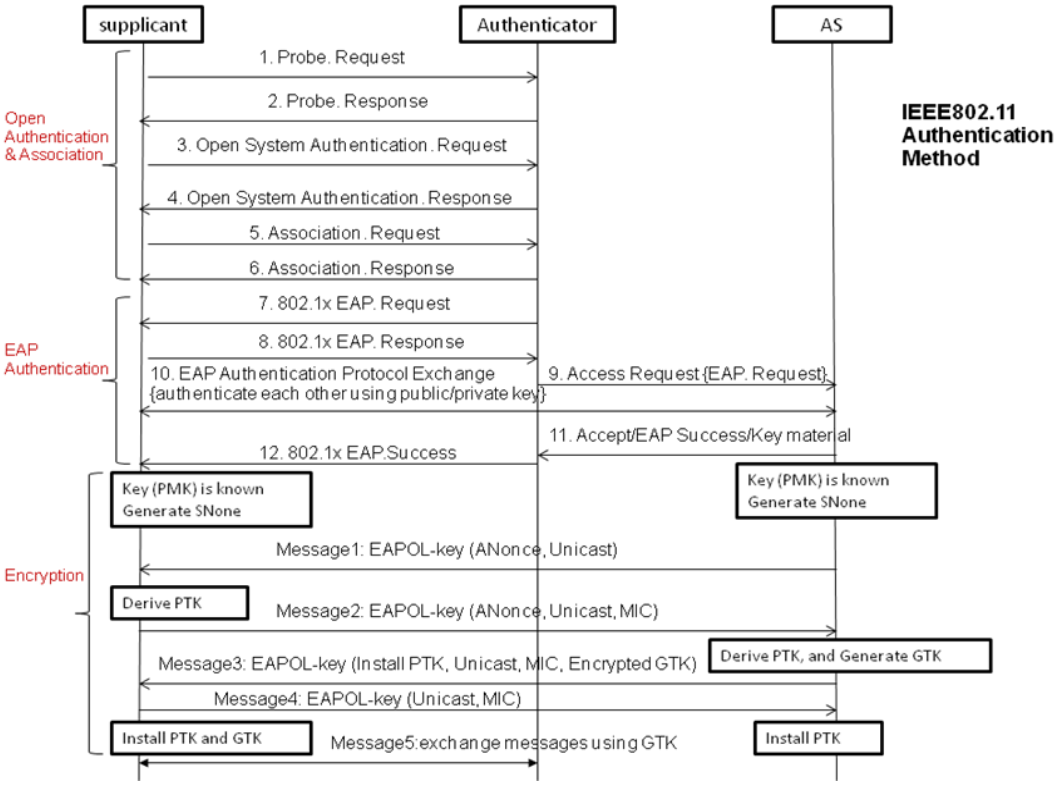

Figure 1, IEEE 802.1x EAP authentication

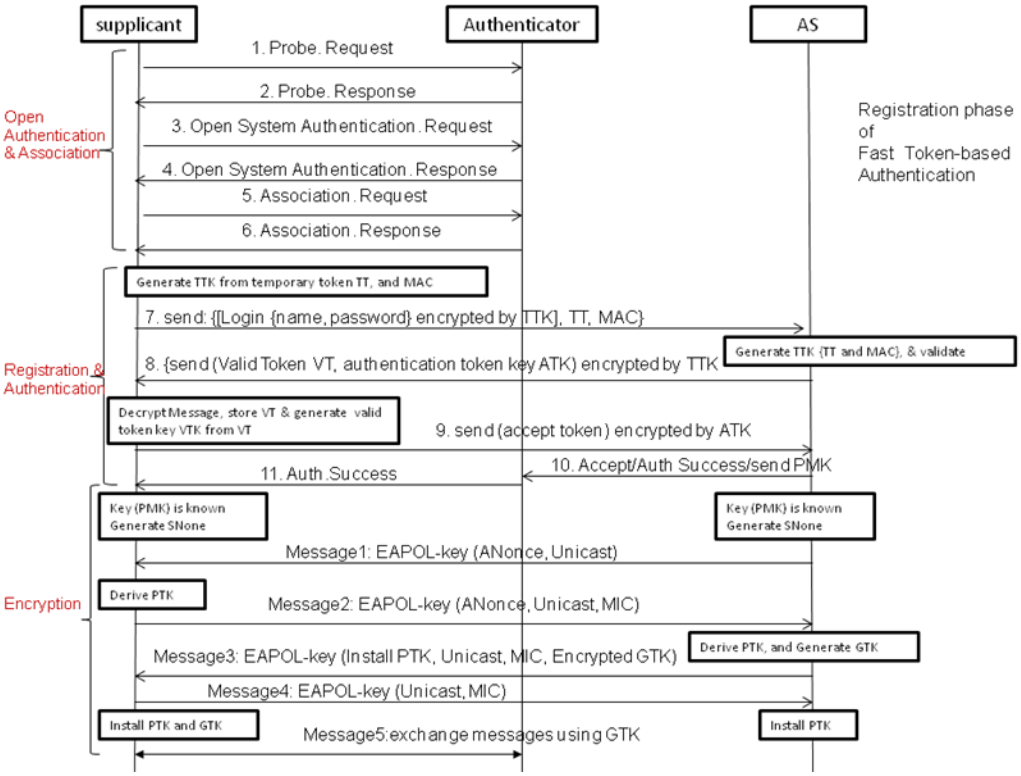

Figure 2, Token-based Fast Authentication Registration phase in WLAN

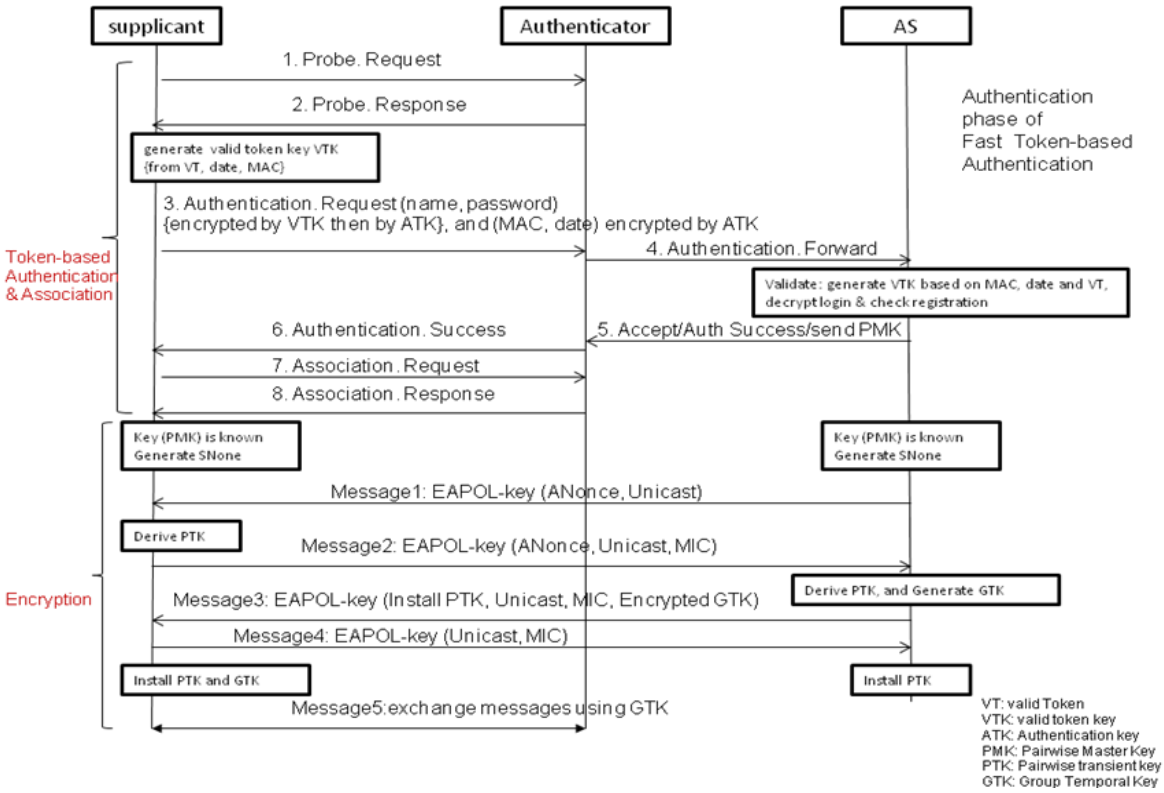

Figure 3, Token-based Fast Authentication phase in WLAN

5. Conclusion

In this paper a new technique "token-based fast authentication" for authenticating wireless client has been presented. In this technique a temporary token will be issued to MC by the AS which will be used during registration. A token key will be generated from the temporary token to encrypt message between authentication server and MC. During registration, the AS will issue another permanent token and send it to the MC. This permanent token will be used by the MC to generate a token key which is used to encrypt the user credentials during the authentication phase. Since only the AS and MC would know the permanent token key which will never be transmitted after registration, hackers would be unable to know this key and therefore is unable to decrypt the message used for authentication. Similar to IEEE 802,1x, another derived group temporal key GTK would be used by MC and AP/authenticator to encrypt all messages exchanged between each other. However, unlike IEEE802.1x at the authentication phase a token is used to authenticate MC instead of digital certificate which makes it faster but achieving the same purpose of high secure authentication technique.

References

[1] Jim Geier, "802.1X Offers Authentication and Key Management" *http://www.wifiplanet.com/tutorials/article.php/1041171*, May 2002

[2] Bellardo, J. and S. Savage, "802.11 Denial-Of-Service Attacks: Real Vulnerabilities and Practical Solutions," *Proceedings of the USENIX Security Symposium*, Washington D.C., August 2003, 15 – 28.

[3] Chapter 2, Maxim, M. and D. Pollino, Wireless Threats, in *Wireless Security*, (McGraw-Hill Companies, 2002), 48 – 63.

[4] Godber, A. and Partha Dasgupta, "Countering Rogues in Wireless Networks", *First International Workshop on Wireless Security and Privacy in conjunction with ICPP 2003*, Taiwan, October, 2003 425 – 431.

[5] Wright, J., "Detecting Wireless LAN MAC Address Spoofing", *www.polarcove.com/whitepapers/*, accessed on 3rd November 2003.

[6] IEEE 802.1x

[7] Jim Geier, "LEAPing Over Wireless LANs"**,** http://www.wifiplanet.com/tutorials/article.php/3070071, August 2003

[8] Jim Geier, **"**Wi-Fi Protected Access (WPA)", *http://www.wifiplanet.com/tutorials/article.php/2148721* **,** March 2003

[9] *http://grouper.ieee.org/groups/802/11/* , July 18 2004

[10] Whitepaper, *http://www.wirelesssecuritycorp.com/wsc/public/Witepapers.do*

[11] Mick Seaman, IEEE 802.1af draft 1.2 (PAR), "Media Access Control (MAC) Key Security".

[12] Allyn Romanow, IEEE 802.1ae, "Media Access Control (MAC) Security", June 8, 2006.

[13] Mike Borza, Max Pritikin, IEEE 802.1ar draft 0.7 (PAR), "Secure Device Identity".

[14] H. Chamas, K. Shuaib, "**Securing Open Access Networks Using Intelligent Policy Management System**", The fourth International Conference on Innovations in Information Technology IIT'08**,** Al Ain-UAE November 2008

[15] Gast, Matthew. "A Technical Comparison of TTLS and PEAP." www.oreillynet.com/pub/a/wireless/2002/10/17/peap.html?page=last&x-maxdepth=0 . This on-line article spells out the most important differences among EAP-TLS, PEAP and EAP-TTLS.

[16] SECURITY FOR THE WIRELESS NETWORK 2006-2007 WatchGuard Technologies, Inc

[17] **Why Your Firewall, VPN, and IEEE 802.11i Aren't Enough to Protect Your Network. ProCurve Networking by HP. developed and sold by Colubris Networks Inc, which was acquired by HP ProCurve in 2008.**

[18] Best Practices for Securing Your Enterprise Wireless Perimeter, 339 N. Bernardo Avenue, Suite 200 • Mountain View, CA 94043 www.airtightnetworks.net

[19] IEEE 802.11 Wireless LAN Security with Microsoft Windows ***Microsoft Corporation Published: January 2007 Updated: January 2008***

[20] Jim Geier, "LEAPing Over Wireless LANs"**,** http://www.wifiplanet.com/tutorials/article.php/3070071, August 2003

[21] G. Kbar "Improved SSL Application using Session Key based Double Key Encryption/Decryption (SDKED) " *Proceedings of the IASTED International Conference, Parallel and Distributed Computing and Networks*, February 17-19, 2004, 294-300.