[NC-Rase 18]
DOI: 10.5281/zenodo.1485478

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

A SYSTEM FOR IMPROVING AUTHENTICATION METHODS FOR IEEE 802.11 WIRELESS LAN

Kshitj R.Mawale[1] & Dhananjay M.Dakhane[2]

[1] Asst. Prof , Department of Computer Science and Engineering, MGI-COET, Shegaon, India
[2] Associate. Prof, Department of Computer Science and Engineering, Sipna COET, Amravati, India

ABSTRACT

Wireless local area network (WLAN'S) has become more prevalent now a days. The IEEE 802.11 is one of the most widely adopted standards for broadband wireless internet access. Also, security issues became more complicated in the wireless network than wired network. The default IEEE 802.11 standard has defined some security mechanism for securing access to its network. But Security is always a major concern for wireless LAN development. This type of development is suffering today from different security problems due to the fact that it is a wireless technology.This concerns the main threats to EAP and some common EAP methods. Specifically EAP-MD5, EAP-LEAP, EAP-TLS, EAP-TTLS and EAP-PEAP.

In our proposed system we are trying to implement advance method for authentication of 802.11 wireless-LAN by overcoming the threats in EAP methods. Like using OAuth protocol in authentication phase, we can offer better security while using third party applications. We also consider roaming situations of mobile nodes.

Keywords: *IEEE 802.11, EAP, EAP-MD5, EAP-TLS, EAP-TTLS, EAP-LEAP,OAUTH.*

I. INTRODUCTION

The original IEEE 802.11 standard [1] has defined the following basic security mechanism for securing access to IEEE 802.11 network:

1) Authentication of entity, which involves open-system authentication.
2) Wired Equivalent Privacy (WEP), which are proved to be having vulnerability.

For enhancing security in IEEE 802.11, IEEE 802.11i has been proposed. It also introduced protocols for key management and establishment and further improvement like encryption and authentication. The IEEE 802.11i does its management of security key by algorithms and protocols.

Mainly IEEE 802.11 divides network environment in 3 parts:

1) Server, which has to perform authentication decisions.
2) An Authenticator, which has to controls access.
3) Supplicate, who wants to be connected to network.

The working of IEEE 802.11 is based on simple concept, it implement access control at connection point between user and network. It provides port security to protect network security. To achieve its goal IEEE 802.11 utilises well known protocol such as Extensible Authentication Protocol and RADIUS. Due to the ranges of different applications for WALNs, a single authentication method is not suitable in all cases, [2]. Currently WIRE1x provides various authentication mechanisms including EAP-MD5 (message digests), EAP-TLS (Transport Layer Security), EAP-PEAP (Protected Extensible Authentication Protocol), [3]. As there are different ranges are available of WLAN's for different application, a single authentication method is not be able to sufficiently overcome all needs of system implementers. The IEEE 802.11 is not able to define the upper layer authentication method; it leaves this choice to system implementers to decide which method to use. As we know that many methods are available for authentication, which are supported by EAP, among this ideally chosen for a specific networking environment.

[NC-Rase 18] ISSN 2348 – 8034
DOI: 10.5281/zenodo.1485478 Impact Factor- 5.070

We know that single authentication is not sufficient overcome all needs of system implementers. The system implementers use combination of more than one protocol for security. If we provide an improved authentication method for authentication of user we can able to minimize the use of more protocol and provide better security. Like we are going to add OAuth in the authentication phase, so that we get the better outputs.

The OAuth 2.0 authorization framework permits a third-party application to get access to an HTTP service but in limited manner, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by permitting the third-party application to get access on its own behalf. This specification replaces and obsoletes the OAuth 1.0 protocol described in RFC 5849.OAuth has taken off as a standard way and a best practice for apps and websites to handle authentication. Social login is currently used by millions of Facebook users to sign in more than one million supporting websites. The protocol behinds this web-based single sign-on (SSO) scheme is OAuth 2.0, which is also adopted by major service providers such as Google and Microsoft. Meant to facilitate personal content sharing across websites in a secure manner, the OAuth 2.0 protocol enables users to grant third-party application access to their web resources without sharing their login credentials or the full extent of their data. OAuth supports a diversity of use cases such as websites, user-agent based applications, and native applications on mobile, desktop or appliance devices. For use case in which user identity information is authorized as an accessible web resource to third-party websites, OAuth can be purposed as a web single sign-on (SSO) scheme.

Resource hosting site (e.g., Facebook) plays the role of identity provider (IdP) that maintains the identity information of the user and authenticates it, while third-party website acts as a relying party (RP) that relies on the authenticated and authorized identity to authenticate the user and customize the user experience. There are currently over billions of OAuth-based SSO user accounts provided by major service providers such as Facebook, Google and Microsoft.

II. LITERATURE REVIEW AND RELATED WORK

The Extensible Authentication Protocol (EAP) is an authentication framework that is widely used in Wi-Fi 802.11. EAP is a basis to transfer authentication information between a client and a network. It provides a basic request/response protocol framework over which to implement a specific authentication algorithm, so called EAP method. Commonly used EAP methods are EAP-MD5, EAPLEAP, EAP-TLS, EAP-TTLS and EAP-PEAP. Within the EAP framework, three entities are involved in the authentication process Supplicant, Authenticator, and Authentication Server. The supplicant is a user that is trying to access the network. It is also known as the peer. The authenticator is an access point (AP) that is requiring EAP authentication prior to granting access to a network. It provides users a point of entry into the network. The authentication server (AS) is the entity that negotiates the use of a specific EAP method with an EAP supplicant, then validates the supplicant, and authorizes access to the network. Typically, the supplicant is a mobile station (MS) and the authentication server is a Remote Authentication Dial-In User Service (RADIUS) server.

The EAP authentication protocol is based on a challenge-response scheme. Four types of messages are used: REQUEST, RESPONSE, SUCCESS and FAILURE. Firstly, a supplicant sends a connection request to a wireless network through the authenticator. Then a series of REQUEST and RESPONSE messages are exchanged. The length and details of the authentication conversation depend on the underlying authentication method. The AS uses the SUCCESS or FAILURE message to notify the AP whether the supplicant authentication was successful or not, and the supplicant will be connected to the network as requested in a successful case. The AP is unaware of any details of the authentication process. It only cares about the AS's final decision, and forwards packets back and forth between the supplicant and the AS. At the same time, the AP listens for the SUCCESS or FAILURE message from the AS and ends the authentication conversation by passing by the SUCCESS/FAILURE message to the supplicant. EAP runs over data link layers without requiring an Internet Protocol (IP) and itselfeliminate duplicate and re-transmission also.

The EAP mechanism makes the authentication process flexible by using a backend authentication server, which may implement some or all authentication methods. EAP methods can be extended by plugging-in at both the supplicant and authentication server ends of a connection. This capability provides the flexibility to allow for several authentication methods. Although EAP provides authentication flexibility through the use of EAP types, the entire EAP conversation might be sent as clear text. This is problematic in WLAN, in which the attacker can be located outside of your business.

EAP is widely used today and attacks have been found from industry. Possible attacks are denial of service (DoS), dictionary attack, man-in-the-middle attack, impersonation of authenticator, impersonation of user, and weaken authentication method.

III. ANALYSIS OF PROBLEM

3.1 Security attacks to EAP and EAP methods

Wireless networks are inherently vulnerable to several network attacks due to the broadcast nature of the wireless radio signals. Malicious users are able to passively eavesdrop on the EAP packets and could potentially access information from the packets. It is also possible to actively transmit EAP packets that can attack the network. EAP methods are developed to mitigate those attacks but each single method has its own flaws based on the properties it has. Main threats to EAP methods can be grouped into three categories: Secret-key methods, Public-key methods, and Tunnelled methods.

3.2 Overview of security attacks to EAP

In wireless networks, since EAP authentication data packets are being transmitted via radio waves rather than over a wire, EAP methods are vulnerable to the following attacks:

1. **Impersonation of a user**: an attacker may discover user identities by snooping authentication traffic.
2. **Impersonation of an authenticator**: an attacker may act as an authenticator and provide incorrect information to supplicants.
3. **Data alteration**: an attacker may try to modify and spoof EAP packets.
4. **DoS**(Denial of Service): an attacker may spoof Success/Failure packets or replay EAP packets or generate packets with overlapping identifiers to carry out this attack.
5. **Dictionary attack**: an attacker my mount an offline dictionary attack by discovering user's password
6. **MITM** (Man-In-The-Middle): an attacker can pass through the entire authentication conversation, then hijack the session and act as the user.

Although some authentication protocols for wireless LANs are suggested earlier, but they either put a lot of workload on the wireless station, or they do not consider the roaming situation of wireless sensor networks, or they conflict with certain upper layer protocols. Some others target are specific domains in wireless communication, such as Public WLANs. IEEE 802.11i is an improved version of the original IEEE 802.11 standard, which was shown to be vulnerable due to too short key, short Initialization Vector (IV), and weak authentication based on RC4. Based on IEEE 802.1X, IEEE 802.11i is developed to provide port-based access control and to overcome the security vulnerabilities of the original 802.11a/b. According to this standard, three types of entities are involved in the authentication process in a wireless network: wireless stations, 802.11i-enabled access points, and an authentication server hidden behind access points.

Consider the following scenario in which an access point in a wireless LAN is compromised. A compromised access point pretends to be legitimate and obtains the Pair wise Master Key (PMK) s of all the wireless stations that have ever connected to it. Normally a wireless station and an access point have the option to cache the PMK for a period of time. With this information, the access point can dupe the wireless stations and get authenticated using the stored PMK. The compromised access point can thus gain control over this wireless station by connecting it to an adversary network. This attack can be even worse if the compromised access point has mobility.

[NC-Rase 18] ISSN 2348 – 8034
DOI: 10.5281/zenodo.1485478 Impact Factor- 5.070

To summarize, there is weakness in the new IEEE 802.11i standard about the authentication of access point and the update of MAC during roaming situation. Therefore, a new method, which can provide authentication for both wireless stations and access points during both the initial connection stage and the roaming situation, is needed.

IV. PROPOSED WORK

4.1 Overview of OAuth

OAuth stands for Open Authorization. It's a free and open protocol, built on IETF standards and is the right solution for securing open platforms. The developers of OAuth set out to solve the problem that services and passwords don't mix well as you start to combine apps and mash them up. Imagine, in today's environment of web APIs and mobile apps, if every web site that used an API from another web site had to share and store that web site password. Soon you'd have the proliferation of your passwords all over the Internet with every service you've used from Facebook, to Twitter, to Skype, to your bank account. OAuth is another way to authenticate to a service;it is a security protocol that allows users to allow third-party access to credentials without sharing their passwords. The heart of OAuth is an authorization token with limited rights, which the user can revoke at any time should they become suspicious or dissatisfied with the app they're using to access your business.

In previous client-server authentication model, the client requests a protected resource on the server by authenticating with the server using the resource owner's credentials. In order to provide third-party applications access to restricted resources, the resource owner shares its credentials with the third party. This creates several problems and limitations:

1. Third-party applications are required to save the resource owner's credentials for using in future if required, basically a password in clear-text.
2. Servers are required to support password authentication, despite the security weaknesses inherent in passwords. Third-party applications gain overly broad access to the resource owner's protected resources, leaving resource owners without any ability to restrict duration or access to a limited subset of resources.
3. Resource owners does not abolish access to an individual third party without revoking access to all third parties, and must achieve it by changing the third party's password.
4. Compromise of any third-party application results in compromise of the end-user's password and all of the data protected by that password.

These problems are solved by introducing an authorization layer and separating the role of the client from, that of the resource owner, in OAuth. In OAuth, the client requests access to resources controlled by the resource owner and hosted by the resource server, and is issued a different set of credentials than those of the resource owner. Instead of using the credentials of resource owner's to access protected resources, the client is given an access token i.e. a string denoting a specific scope, lifetime, and other access attributes. These tokens are given to third-party clients by an authorization server with the permissionof the resource owner. The client uses the access token to access the protected resources hosted by the resource server.

V. SYSTEM MODULE'S

5.1 Using OAuth in Wireless Sensor Network

In our proposed system we are trying to implement OAuth 2.0 protocol in WSN nodes which cannot be done previously. Our proposed system consisting of following modules

1. Development of network with nodes.
2. Node registration based on name and password.
3. Development of OAuth 2.0 protocol.
4. Communication of nodes which are authenticated.

5.1.1 Development of network with nodes

First we are going to develop a network with certain nodes which are having a unique MAC addresses, not going to change in any situation, for wireless sensor network. A wireless sensor network is a collection of nodes organized

[NC-Rase 18] ISSN 2348 – 8034
DOI: 10.5281/zenodo.1485478 Impact Factor- 5.070
into a cooperative network [10]. Each node consists of processing capability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single omni- directional antenna), have a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators.

5.1.2Node registration based on name and password

In this phase we have to register the nodes based on their name and password. Also the MAC address is also registered in this authentication phase.

5.1.3 Development of OAuth 2.0 protocol

In phase we are trying to develop the OAuth 2.0 protocol for the Wireless Sensor Network. Where it is used for the authentication of the mobile nodes and also provides better security.

5.1.4 Communication of nodes which are authenticated

After the authentication did by the OAuth protocol in previous phase the communication can be takes place of the networks mobile nodes. The user provided by maximum security using OAuth protocol. Also if the node is in roaming condition the user is alert by the changed security key for avoiding the threats, as MAC address remains same in any condition.

VI. RESULT AND DISCUSSION

The authentication for nodes using OAuth in the experiments is simulation based. Table Ilists the specifications of the experiment setup. We have evaluate the process in the following configuration.

Table I System Specification

CPU	Intel core i5 2.6 GHz
RAM	4GB DDR 3
HDD	500GB
OS	Windows 7, fedora20.01 (for NS allinone)
Software	VMware work station , Ns allinone

We can evaluate the experiments on lower specification also but it will increase the Burdon on the system. So we use the above system for evaluation. We use the Eclipse VMware workstation to use NS2 on window based OS and NS allinone for creating the simulation environment.

The communication between preregister nodes are carried out with and without using OAuth protocol and by using graph we can see the efficiency of OAuth protocol.

The X graph show the comparison of authentication using OAuth and without OAuthon three parameters as delay in authentication, energy consumed by nodes in authentication and total throughput required.

The energy graph shown in the figure 1 show when we apply OAuth protocol in authentication process reduce the energy consume by nodes than other mechanism used in authentication.

ISSN 2348 – 8034
Impact Factor- 5.070

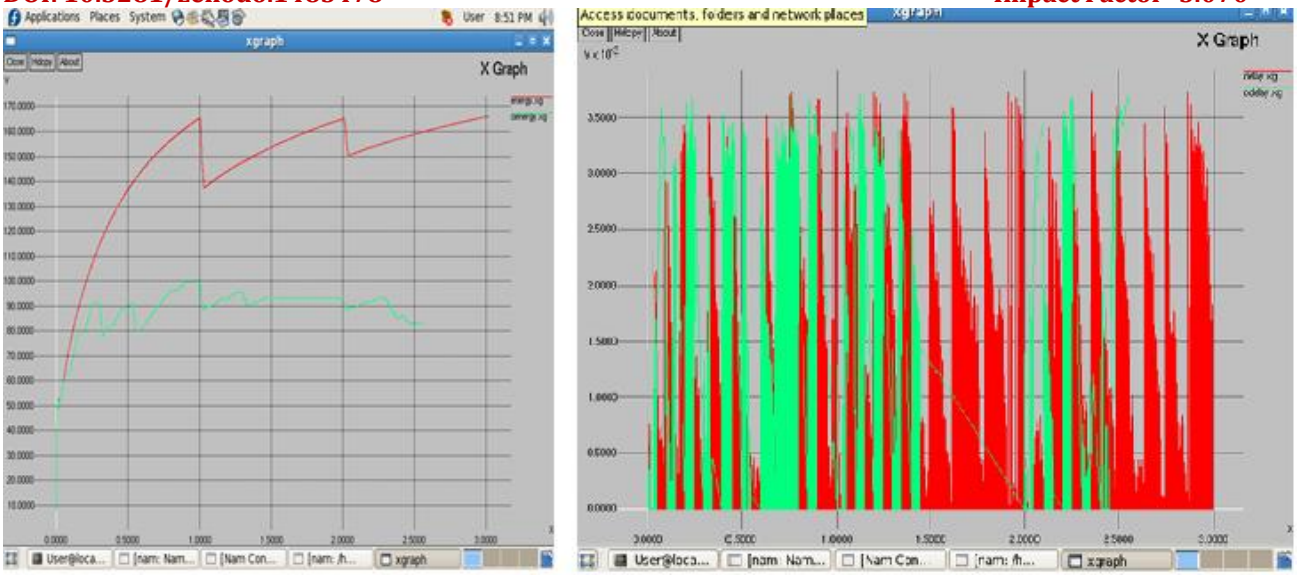

Figure 1: Energy and Delay graph in OAuth protocol implementation.

VII. APPLICATIONS

1. Using OAuth in the mobile nodes for authentication, by considering the roaming situation we can provide better security.
2. As MAC address remains same in roaming situation we can use this type of authentication in Wireless Sensor Network (WSN).
3. Also by using user's phone number, we can provide user update of security key changed in roaming situation time to time.
4. A trust worthy network can be used for communication of network node

VIII. CONCLUSION

We have identified the need to adopt the new authentication policy in WLAN other than traditional ones. We proposed this model based on OAuth authentication protocol to address the problems in previous authentication scheme. OAuth typically uses the base authorization server which has preregistered resource owner. Whenever the third party wants to access the protected resource on behalf of resource owner authentication server grants token by validating client and third party and upon success protected resource is allowed to use.

We validate our model by presenting OAuth authorization scheme for nodes in wireless environment. The simulation result for Delay, Energy and Throughput shows the efficiency of this model.

IX. ACKNOWLEDGEMENTS

A moment of pause, to express a deep gratitude to several individuals without whom this project could not have been completed.

I am grateful to Principal Dr. S. A. Ladhake sir for their co-operation. I express my sincere thanks to Dr. A. D. Gawande, Head of Department, Computer Science and Engineering & the other staff of the department for their kind co-operation.

I feel immense pleasure to express my gratitude & indebtedness to my guide Dr. D. M. Dakhane for constant encouragement and noble guidance. I shall ever be grateful to him for encouragement and suggestion from time to

time that boosted my morals. I must say, he is enduring source of inspiration & I consider myself lucky for his guidance.

Last but not least, I am thankful to my friend and library staff members whose encouragement and suggestion helped me to complete my seminar. I am also thankful to my parents whose best wishes are always with me

REFERENCES

1. *Cisco Systems, (2002) _A Comprehensive Review of 802.11 WLAN Security and the Cisco wireless Security Suite, Cisco Systems Inc, New York, USA.*
2. *Cisco Systems, (2004) _Cisco Response to Dictionary Attacks, Cisco Systems, Inc, New York, USA.*
3. *Cisco Systems, (2003) _Cisco SAFE: WLAN Security in Depth', Cisco Systems, Inc, New York, USA.*
4. *Edney, J. and Arbaugh, W., (2004) _Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison-Wesley, Boston, USA*
5. *Khidir M. Ali and Thomas J. Owens, (2010) _Access Control Mechanisms in Wi-Fi Networks, State of Art: Flaws & Proposed Solutions', IEEE Proceedings of 2010 International conference on Telecommunications, 3-7 April, Pages 280-287.*
6. *Khidir M. Ali and Thomas J. Owens, (2007), _Selection of EAP-Authentication Methods for a WLAN'. Int. J. Information and Computer Security, Vol. 1, No. 1/2, 2007, pp 210-233.*
7. *Gast M, (2005) _802.11 Wireless Networks; The Definitive Guide, 2nd Edition' O'reilly, USA*
8. *Ma. Y. and Cao, X., (2003), _How to use EAP-TLS Authentication in PWLAN Environment', IEEE, Proceedings of the 2003 International conference on neural networks and signal processing, Volume 2, 14-17 Dec, Pages 1677-1680.*
9. *Mishra, A. and Ho, M., (2004) _Proactive Key Distribution Using Neighbor Graphs', IEEE wirelesscommunication, Volume 11, Pages 26-36.*
10. *Shumman W. and Ran T., (2003), _WLAN and its Security problems', IEEE, Proceedings of the 2003 International conference on Parallel and Distributed Computing, Applications and Technologies, Pages 241- 245.*
11. *http://people.scs.carleton.ca/~barbeau/Honours/Lei_Han.pdf*
12. *http://info.apigee.com/Portals/62317/docs/OAuth_big_picture.pdf*
13. *RFC 6749*
14. *ShakeraShaikh&VeenaGulhane User Authentication Techniques for Wireless Sensor Networks : A Survey, International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) ISSN No. 2248-9738 Volume-1, Issue-4, 2012,Pages 82-85.*
15. *Ismail Butun and Ravi Sankar Advanced Two Tier User Authentication Scheme For Heterogeneous Wireless Sensor Networks, 2nd IEEE CCNC Research Student Workshop, Pages 169-171.*
16. *Al-Sakib Khan Pathan, Hyung-Woo Lee, ChoongSeon Hong Security in Wireless Sensor Networks: Issues and Challenges ISBN 89-5519-129-4 - 1043 - Feb. 20-22, 2006 ICACT2006*
17. *Manjula M. Ramannavar, Monica M. Jagtap Authentication in Wireless Sensor Networks Using Virtual Certificate Authorities International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 11, November 2012)*