Vol. 7, No. 6, June 2016 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences

http://www.cisjournal.org

Algorithm for Selection of EAP Authentication Method for Use In A Public WLAN

David Gitonga Mwathi[1], William Okello-Odongo[2], Elisha Opiyo[3]
[1]Department of Computer Science and ICT, Chuka University, Kenya
[2,3]School of Computing and informatics, University of Nairobi, Kenya
dgmwathi@chuka.ac.ke

ABSTRACT

Several recent studies indicate that many implementations of authentication and access control in public WLANs are compromisable. This is because IEEE 802.11 standard leaves the choice of EAP method to use to the discretion of WLAN system implementers due to the fact that IEEE 802.11 standard cannot and does not define the upper layer authentication. Therefore, this paper presents IEEE 802.11 implementation specific issues that may contribute to poor security performance of WLAN authentication and access control implementation. It also analyses various EAP methods and presents an algorithm for selection of an Extensible authentication protocol (EAP) method for a Public WLAN.

Keywords: *Extensible authentication protocol, wireless LAN, attacks.*

1. INTRODUCTION

Since its inception, the IEEE 802.11 Wireless Local Area Network (WLAN) has become one of the most popular means of setting up networking technology. It has been deployed in almost every possible sector of networking due to the rapid proliferation of mobile devices. Whereas wireless networking is emerging as a significant aspect of internetworking, it presents a set of unique issues based on the fact that the only limit to a wireless network is the radio signal strength. There is no wiring to define membership in a network. There is no physical method to restrict a system in radio range to be a member of a wireless network. Hackers and intruders can therefore exploit the loopholes of the wireless communication. As a result, there are many security threats associated with Wireless Local Area Network (WLAN) due the following inherent security issues found in all WLANs.

- The WLAN broadcasts the access point name and location beyond the boundaries of the institution they are deployed. This allows external malicious users to see and recognize the institutional network.
- WLAN is vulnerable to spoofing i.e. rogue networks mimicking a real access point and establishing connections to intercept data and files.
- Data transmitted via WLAN can be vulnerable to interception and monitoring, creating risks for the user.

Controlling user access and possible WLAN security attacks in a public WLAN can be achieved through authentication and access control. While attempts to enhance security of IEEE 802.11 standard have been made [1] & [2], design or selection of security features and how to configure them is a challenge to many WLAN security implementers

BASIC Operation of Wireless Local Area Network (WLAN) Technology

The general architecture used by WLAN, whether they are using the 802.11a, b, g or n technology, is to allow client devices e.g. laptops, tablets, smartphones and workstations to establish a connection with the WLAN through a wireless access point. Each IEEE 802.11 a/b/g/n device can operate in one of four possible modes; master mode, managed mode, adhoc mode or monitor mode. When operating in master mode, the device is a service provider operating with a specific SSID and channel. When in managed mode, the device is a client and joins a network created by a master and will change the channel to match that of the master. When in adhoc mode, the device creates peer to peer connections with other devices creating a multipoint to multipoint network. When in monitor mode, the device does not transmit any data but passively listens to all radio traffic on a given channel. Association is the name given to the process of connecting a station (laptop, tablet, smartphone or workstation) to the WLAN. The station must have a wireless network interface card (NIC) installed and have its wireless protocols running. The station will periodically scan the environment looking for an access point. The station will use either active scanning or passive scanning. If the station is using active scanning, it will transmit a probe frame on all available frequency channels. When an access point receives the probe frame, it will respond with a probe response. The probe response contains all the information needed by the station to associate itself with the access point. If the station then agrees to associate with the given access point, communication has been established. In passive scanning, the station listens on all available channels for a beacon frame from the access point. The beacon frame, like the probe response, contains all the information needed by the station to associate itself with the access point. Once the station detects a beacon frame, it may choose to associate itself with the access point that transmitted the beacon frame. The type of information required to associate a station with an access point includes the Service Set Identifier (SSID) and the wireless network's transmission rate.

The IEEE 802.11 media access control (MAC) protocol supplies the functionality in WLANs that is required to provide reliable delivery of user data over the potentially noisy unreliable wireless media [3].After association to the accesspoint,the station must be authenticated into the WLAN.Two authentication approaches defined by IEEE 802.11 are use of pre-shared key and IEEE 802.1x[2][1]. Pre-shared key authentication is based on a secret cryptographic key which is shared by legitimate STAs and APs.It uses a simple challenge–response scheme based on whether the STA seeking WLAN access knows the secret key.The STA initiates an authentication request with AP. The AP generates a random 128 –bit challenge and sends it to the STA.Using the key, STA encrypts the challenge and returns the result to the AP.The AP decrypts the result using the same key and allows STA access only if the decrypted value is the same as the challenge.

IEEE 802.1x authentication enables the station, upon accessing the network, to communicate to the authenticator via EAPOL packets. Those packets are then forwarded to the authentication server, commonly RADIUS Server. Integrated authenticator/authentication server softwares are available e.g. hostapd. As at this early stage none of those packets are encrypted at the 802.11 MAC layer and therefore a secure authentication must be guaranteed by the EAP authentication method itself.

2. RELATED WORK

Khidir and Owens[4] proposes algorithms to guide selection of EAP authentication methods based on four major parameters; degree/level of protection provided by an authentication method, the vulnerability of a WLAN in a specific environment, supportive network infrastructure and cost of implementing a particular authentication method. According to [4], the level of protection provided by a certain authentication method depends on authentication method’s implementation technique and authentication attribute whether mutual or unilateral.

Vulnerability of a WLAN in a specific environment refers to the security threats and possible attacks in that environment. Khidir and Owens [4] propose a selection algorithm for EAP authentication method based on possible attacks and threats in that environment. The researchers consider two categories of attacks; man in the middle and dictionary attacks. This analysis is not comprehensive as other attacks such as denial of service, confidentiality or integrity related attacks that could be as a result of cipher suite, system software or authentication server systems are very common in many implementations. Support network infrastructure includes all the hardware, software and firmware components required by a certain authentication method. The authentication method’s implementation cost always includes the cost of any infrastructure upgrade required to implement the method as well as the cost associated with upgrading the knowledge and skills of the users of the WLAN clients to a level that enables them to use the newly implemented authentication method without difficulties[4]).Though all parameters are desirable, they point out the degree/level of protection as the most important parameter to be considered in the selection of EAP methods.Khidir & Owen’s algorithm fails to incorporate EAP-FAST which was developed as an improvement on LEAP. Some comparative studies on EAP authentication methods namely; MD5, TLS, TTLS, PEAP, LEAP and FAST have been carried based on the fact that EAP supports a variety of upper layer authentication protocols each having its own strengths and weaknesses [5] and [6]. However, the studies differ in the parameters because one study is based on the parameters authentication attributes, deployment difficulties, dynamic re-keying, requirement for server Certificate, requirement for client certificate, tunneled, WPA compatibility, level of WLAN security and Security risks (attacks) associated with a method[5]while a similar study compares the same authentication methods based on the following; implementation technique, authentication attributes, deployment difficulties, dynamic key delivery, server certificate requirement, supplicant certificate, tunneled, WPA compatibility, WLAN security level and vulnerabilities (attacks) associated with a method[6]. Another study [7] gives a detailed analysis of the following EAP methods; MD5, LEAP, TLS, TTLS and PEAP.The main advantage of these analysis is that by help of these comparative studies, we can choose between a technique which is more reliable for communication and one which is worse. Additionally, the detailed explanation of these methods makes it easy for implementers to understand these methods.

3. IEEE 802.11 IMPLEMENTATION SPECIFIC ISSUES THAT MAY CONTRIBUTE TO POOR WLAN AUTHENTICATION AND ACCESS CONTROL SECURITY PERFORMANCE IN A PUBLIC/OPEN WLAN

3.1 Methodology

Survey of 31 WLAN networks of public and private Universities in Kenya was made. Questionnaires were sent to network administrators of these wireless networks to collect hard facts related to their network. Observation of the configuration information on sampled networks was also made on the user devices and access point using passive (non-intrusive) WLAN network search tools. This information was used to verify the questionnaire responses.

3.2 Results and Discussion

The analysis was done using descriptive statistics and the following issues were observed and are discussed.

Issue1-Cipher Suite

77.4 % of the WLANS (35.5% WEP,41.9 % TKIP) use confidentiality and integrity protocols that are vulnerable. Special concern is on 35.5 % of WLANs using WEP that has been proven very trivial to crack and many tools targeting it are available. Additionally 16.1% equivalent to five university WLANS use combinations

(CCMP and TKIP(1),WEP and TKIP(1),WEP,TKIP and CCMP (2) and WEP,TKIP(1).Only 6.5% of the networks(i.e those implementing CCMP) have ability to support RSN associations. This means therefore that many WLANs are vulnerable to pre-RSN related attacks.

Issue 2-Authentication Mechanism

The primary methods of authentication used by universities are; Pre-shared key only authentication(32.3 %), EAP method with 802.1x RADIUS Server(32.3 %).35.5 % use combined methods as follows;Pre-shared and EAP method with IEEE 802.1x(19.35%), Pre-shared key and captive portal(6.45%)Captive portal and EAP method with IEEE 802.1x(6.45 %),MAC address and Pre-shared key (3.23%).Similarly MAC address authentication though rarely in use(3.23%) is prone to MAC address spoofing.

Issue 3: Authentication Server Protocol

58.1 % WLANs corresponding to 18 Universities use RADIUS server for authentication while 41.9% do not.

Issue 4: Authentication Credentials

Among the 18 University WLANs using RADIUS server for authentication, 11.2% of them use password based extensible authentication protocol(EAP) methods i.e LEAP and MD5.LEAP and MD5 has known vulnerabilities.However,88.8% use client side certificate based EAP methods (61.1 % PEAP,27.7 % EAP TTLS).However, client ,configurations have been implemented in such a way to ignore validation of server certificates. PEAP and TTLS though are known to suffer from known MITM attack are moderately secure. No University WLAN among those sampled uses Both client and server side certificate (TLS) .TLS is known to be the most secure EAP method but the most complex to implement because of complexities associated with Public key infrastructure(PKI).38.7% of the university WLAN administrators never change the pre-shared key while 9.7% change them yearly.

Issue 5: Unchanged RADIUS Server-AP Passphrase

45% of the WLANs implementing IEEE 802.1x with EAP do not change RADIUS server-AP passphrase.Another 22% change it yearly. This indicates that these WLANs suffer the risk of RADIUS Server-AP passphrase being revealed which can lead to man in the middle attacks.

Issue 6-Lack of Digital Certificate Infrastructure

Only 6.4 % of Universities have a system where students can register for digital certificates. This indicates that very few WLANs are ready to deploy the most secure authentication methods such as TLS.

Issue 7-Attacks on WLANS

A significant percentage of WLAN implementers (38.7 %) reported having experienced WLAN attacks in one form or another. The most common attack at 75% was denial of service and man in the middle at 8%.

Some of the causes of attack or vulnerabilities exploited were provided and include;

(i)Lack of proper setup/configuration of authentication scheme in use
(ii)Cracking the authentication credentials(pre-shared key) and consequently broadcasting packets
(iii)Network device failure due to old age
(iv)Students setting their own accesspoints on their laptops. 45.2% indicated that their WLAN supports configuration of Virtual WiFi Soft Access points by WLAN devices
(v)Weak pre-shared key
(vi)Lack of network segmentation to separate WLAN traffic from wired traffic.
(vii)Weak/poor authentication methods
(viii)Vulnerable student devices e.g Lack of configuration of server name and other security details on user devices.
(ix)Overwhelming the RADIUS server.
(x)Unauthenticated server
(vi)Lack of updating the Operating system

4. IMPLEMENTATION OF EAP METHODS IN IEEE 802.1X AUTHENTICATION

The research findings from the survey indicate that various University WLANs have implemented some form of EAP method in their authentication. However, some of the implementations are very vulnerable to attacks .This is a reflection of operational security in many other open/public WLANS.This section therefore attempts to analyze some of the features of five selected EAP methods that can be adopted for use in a open/public WLAN.The EAP methods are compared and an algorithm for selection of an EAP method is proposed.

4.1 Comparison Of EAP Methods

Five EAP methods are discussed and compared.

TLS

EAP with Transport Layer Security (EAP-TLS) by[8] uses TLS[9] a successor of secure Socket Layer version 3 (SSLv3), and requires both the client-side and server-side to have Public Key Infrastructure (PKI) digital certificates in order to provide secure mutual authentication. Both the client and the server are able to validate the certificate chain where the server can additionally match the common name or other attributes of the client certificate. This method is considered as the strongest (security wise) EAP method [4].However, implementation of EAP-TLS is complicated as each client has to be supplied with a certificate.

TTLS

EAP with Tunneled TLS (EAP-TTLS) by [10] requires server-side certificate while user-side can use an extensible set of user authentication such as Windows login, password and legacy user authentication methods. EAP-TTLS uses secure TLS record layer channel to set up tunnel to exchange information between client and server. EAP-TTLS offers strong security while avoiding the complexities of PKI implementation on client’s side.

PEAP

Protected EAP (PEAP) by [11]is similar to EAP-TTLS in that it only requires server-side certificate and uses other ways to authenticate client, uses TLS tunnel, and offers strong security. The main difference is in compatibility with legacy (older) methods and platforms which PEAP is less compatible compared to EAP-TTLS. It was jointly developed by Microsoft, Cisco, and RSA Security.EAP-TTLS and EAP-PEAP are similar to TLS except for a lack of a client certificate. A secure TLS tunnel is established and allows another authentication method be used inside. While TTLS traditionally only supported the transmission of RADIUS-like attribute-value pairs, today TTLS and PEAP are implemented allowing all other EAP authentication methods inside the tunnel. The authenticity of the authentication server (and therefore the whole tunnel) is optionally ensured by verifying the CA certicate. Some supplicants also allow for additional certificate attributes to be checked (e.g. WPA supplicant directive subject match).

LEAP

Lightweight EAP (LEAP) [12] is a proprietary EAP method developed by Cisco Systems for their wireless LAN devices. LEAP supports mutual authentication and dynamic security keys changes in every (re)authentication to improve security

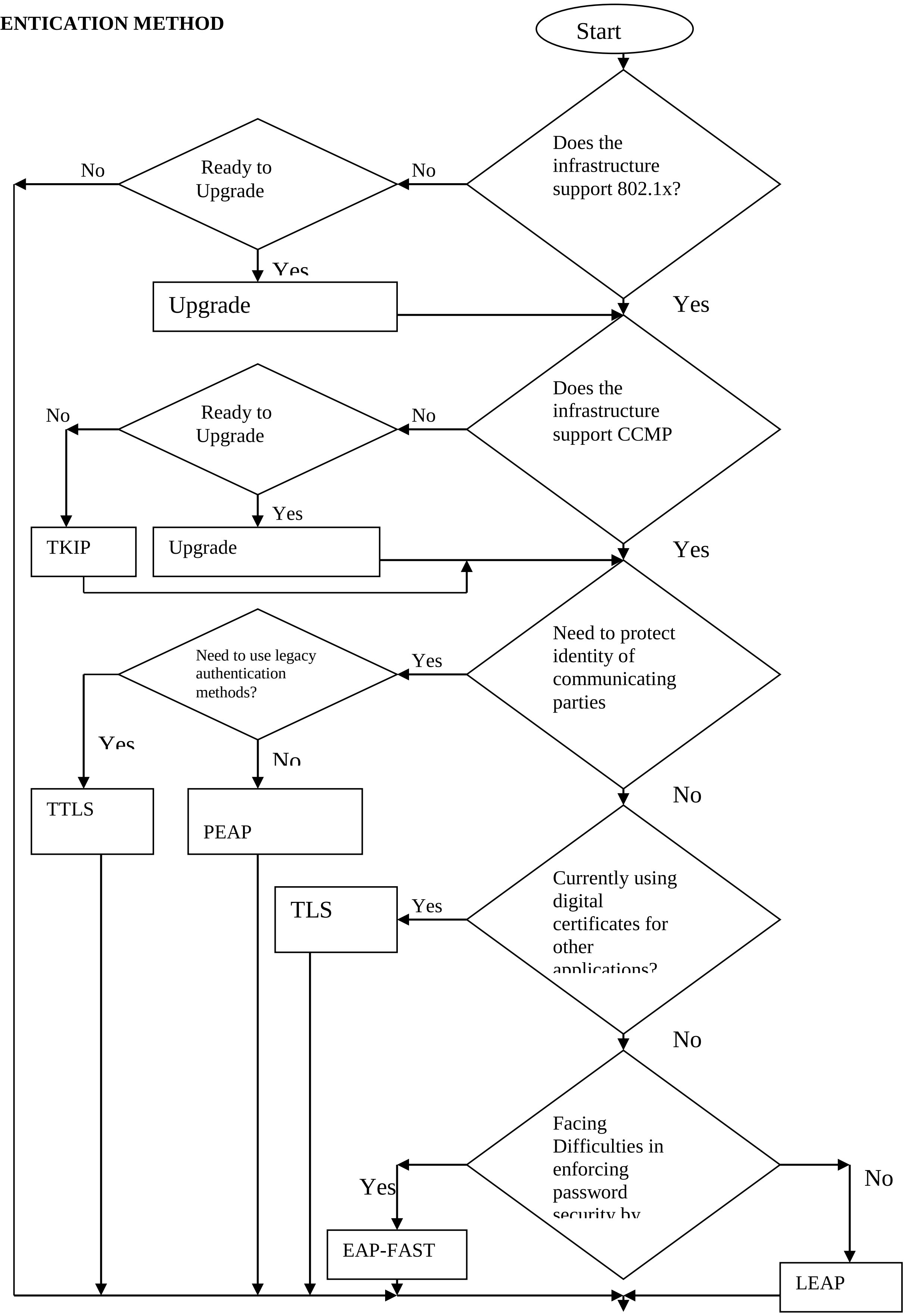
EAP-FAST

EAP-FAST is one type of hybrid method like TTLS and PEAP for authentication. It uses EMP MSCHAPv2 method for credential provisioning and EAP-GTC for authentication. Credential provisioning typically occurs only during the client's initial EAP-FAST authentication. Subsequent authentications rely on the provisioned credential and will usually omit the provisioning step.EAP-FAST is an authentication protocol designed to address the performance shortcomings of prior TLS-based EAP methods while retaining features such as identity privacy and support for password-based protocols. The EAP-FAST credential is known as a Protected Access Credential (PAC) and contains information used to secure the authentication operations. Parts of the PAC are encrypted by the server and are not visible to other entities. Clients are expected to securely store PACs locally for use during authentication. EAP-FAST has two phases. In the first phase a mutually authenticated tunnel is established using a pre-shared key called protected access credential(PAC).Using PAC, the client and the RADIUS server establish a tunnel,. In the second phase, the user information is sent by the client across the established tunnel.EAP-FAST provides security which basically depends on its implementation. If it is poorly implemented, the security level provided by EAP-FAST could be comparable to EAP-LEAP or even MD5.EAP-FAST provides maximum security by using digital certificates at client's machines but the problem will be in the implementation and in this case EAP-FAST will not be easier to use than PEAP, TTLS or even TLS[1].

Table 1: Comparison of EAP-TLS, EAP TTLS, EAP-PEAP, EAP-FAST and EAP-LEAP methods

	EAP-TLS	EAP-TTLS	EAP-PEAP	EAP-FAST	EAP-LEAP
Implementation	Certificate Based	Server Certificate	Server Certificate	PAC	Password based
Deployment Difficulties	Hard	Moderate	Moderate	Easy to Moderate depending on security	Easy
Identity protection	No	Yes	Yes	Yes	No
Mutual authentication	Yes	Yes	Yes	Yes	Yes
Ability to enforce password policy	N/A	N/A	N/A	Yes	No
Compatibility with legacy methods	No	Yes	No	No	No
Dynamic Key delivery	Yes	Yes	Yes	Yes	Yes
WPA compatibility	Yes	Yes	Yes	Yes	Yes
Security Strength	Maximum Security	Secure	Secure	Weak to secure depending on implementation	Moderate
Vulnerabilities	Identity exposure	MITM Attack	MITM attack.	MITM attack	-Identity exposed -Dictionary attack

4.2 Algorithm for Selection of A Secure EAP AUTHENTICATION METHOD


Start
Does the infrastructure support 802.1x?
No
Ready to Upgrade
No
Yes
Upgrade
Yes
Does the infrastructure support CCMP
No
Ready to Upgrade
No
Yes
TKIP
Upgrade
Yes
Need to protect identity of communicating parties
Yes
Need to use legacy authentication methods?
Yes
No
TTLS
PEAP
No
Currently using digital certificates for other applications?
Yes
TLS
No
Facing Difficulties in enforcing password security by
Yes
EAP-FAST
No
LEAP

5. CONCLUSION

It is evident that many IEEE 802.11 based networks have various implementation challenges that make them vulnerable to known attacks. While many EAP methods have been developed, each method is prone to its own set of attacks based on its operation mechanism. Network administrators can therefore be guided by the analysis provided for EAP methods and the proposed algorithm in selecting an EAP authentication mechanism for WLAN authentication and access control.

REFERENCES

[1] IEEE Standard 802.11i , IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements, Part 11: Wireless LAN medium access control(MAC)and physical layer (PHY) Specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.

[2] IEEE Standard 802.11w, IEEE standard for information technology -Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements, part 11: Wireless LAN Medium Access Control (MAC) and physical layer (PHY) Specifications. Amendment 4: Protected Management Frames, 2009.

[3] Sheila, F Bernard, E Les, O Karen, S.), Establishing Wireless Robust security Networks: A Guide to IEEE 802.11i (NIST).US, 2007.

[4] Khidir M. Ali and Thomas J. Owens, Selection of EAP-Authentication Methods for a WLAN‘. Int. J.Information and Computer Security, Vol. 1, No. 1/2, 2007, pp 210-233.

[5] Khidir M.Ali and Ali Al-Khalifah, “A Comparative Study of Authentication Methods for Wifi Networks”, Third International Conference on Computational Intelligence, Communication System and Networks, 2011, page 190-194.

[6] Kshitij,R. , Dhananjay, M. & Lavindra,L.,Authentication Methods for WI-Fi Networks, International journal of Applications or innovation in Engineering and Management,Vol 2,no.3 ,March 2013.

[7] Umesh,K. Praveen, K.Sapna, G, Analysis and literature review of IEEE 802.1x(Authentication) protocols,International journal of Engineering and advanced Technology,Vol 3,issue 5,June 2014.

[8] Aboba, B. & Simon, D. RFC 2716, PPP EAP TLS Authentication Protocol. The Internet Society, 1999.

[9] Dierks & Allen, The TLS protocol version 1.0,1999

[10] Funk, P. & Blake-Wilson, S., EAP Tunneled TLS Authentication Protocol Version 0 (EAP-TTLSv0). Internet-Draft. The Internet Trust, 2007.

[11] Kamath, V., Palekar, A. & Wodrich, M.. Microsoft’s PEAP version 0 (Implementation in Windows XP SP1). Internet-Draft. The Internet Society, 2002

[12] Sankar, K., Sundaralingam, S., Miller, D. & Balinsky, A, Cisco Wireless LAN Security. N.York: Cisco Press, 2005.