Selection of EAP Authentication Method for use in a Public WLAN: Implementation Environment Based Approach

David Gitonga Mwathi*
Department of Computer Science and ICT
Chuka University

William Okello-Odongo
School of Computing and informatics
University of Nairobi

Elisha Opiyo
School of Computing and informatics,
University of Nairobi

Abstract-This paper presents IEEE 802.11 implementation specific issues that may contribute to poor WLAN authentication and access control security performance in a public WLAN. It will also analyse five EAP methods and present a proposed implementation environment based approach for selection of an Extensible Authentication protocol (EAP) method for a Public WLAN authentication.

Keywords- Extensible authentication protocol (EAP), Wireless LAN (WLAN), WLAN Attacks, Cipher suite, IEEE 802.11

1. INTRODUCTION

IEEE 802.11 Wireless Local Area Network (WLAN) has become one of the most popular means of setting up networking technology. However, Information security is a critical issue in the wireless network, because the transmission media is open (no physical control on the air). Any wireless device equipped with wireless interface can use and share the airwave transmission medium with other users. 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) for protection purposes, several security mechanisms have been developed over years to Control user access and possible WLAN security attacks in a public WLAN. While attempts to enhance security of IEEE 802.11 standard have been made [2] & [3], design or selection of security features and how to configure them is a challenge to many WLAN security implementers. WLANs are alternative of conventional LANs that connect nodes in wired environments. WLANs transmit information over wireless medium instead of wire.A Wireless Local Area Networks (WLAN) is a shared medium communication network that broadcast information over wireless links to be received by all stations (e.g. computing devices). 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 [4].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. A public WLAN would be set up to use the infrastructure network where clients are in managed mode and accesspoint is in master mode. Infrastructure network by its very nature allows central management and through it the possibility of enhanced security. Additionally, most public WLANs are connected to a wired LAN of some type. The infrastructure network allows a wireless and wired network to communicate with each other. As part of this architecture, a Dynamic Host Configuration Protocol (DHCP) server is included. The DHCP server provides IP addresses and other required information to allow wireless network workstations and laptops to boot up and communicate on both the WLAN and the attached wired network without any additional attention from network personnel.

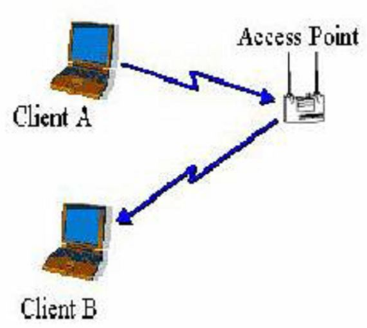

Fig 1: Infrastructure network: Basic service set (BSS)

When in adhoc mode, the device creates peer to peer connections with other devices creating a multipoint to multipoint network. The ad-hoc mode is typically used on very small wireless network, with few nodes. With the ad-hoc mode, wireless stations communicate directly with each other via their wireless NICs.

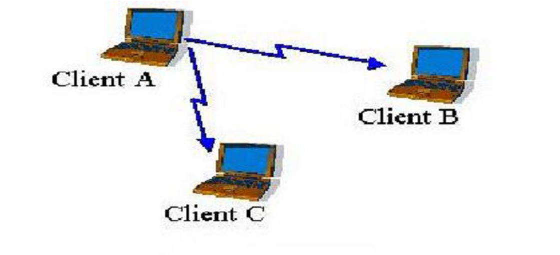

Fig 2: Adhoc mode of WLAN implementation

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. After association to the access point, 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]. 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 software's 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.

II. RELATED WORK

Khidir and Owens[5] 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 [5], 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 [5] 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[5]).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 [1] 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 [1].

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 analyses 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. The detailed explanation of these methods makes it easy for implementers to understand these methods.

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

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.

RESULTS AND DISCUSSION

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

ISSUE 1: 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 2: 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 attacks are moderately secured. 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 3: CIPHER SUITE

77.4 % of the respondents (35.5% WEP, 41.9 % TKIP) use confidentiality and integrity protocols that are vulnerable. Special concern is on 35.5 % who use WEP that has been cracked several times and very trivial to crack and many tools targeting it are available. No organization should be using WEP at all. 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 4: 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 5: 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
(iv) Weak pre-shared key
(v) Lack of network segmentation to separate WLAN traffic from wired traffic.

(vi) Weak/poor authentication methods
(vii) 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

IV. 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 analysed and a mechanism for selection of an EAP method is proposed.

ANALYSIS OF EAP METHODS

Five dominant EAP methods are discussed and analyzed.

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 [5].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: ANALYSIS 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
Known Vulnerabilities	Identity exposure	MITM Attack	MITM attack.	MITM attack	-Identity exposed -Dictionary attack

V. PROPOSED IMPLEMENTATION ENVIRONMENT BASED APPROACH FOR SELECTION OF EAP METHOD

Based on the analysis of the characteristics of various EAP methods as shown in table1, the researcher proposes a method for selection of an EAP method based on six implementation environment parameters; ***Cipher suite supported, Support for IEEE 802.1x , need to protect Identity of Communicating parties, whether the organization is using digital Certificates for other Applications, whether there are challenges in enforcing password security by users and whether there is need to use legacy authentication methods.*** This is shown in table2

TABLE2: IMPLEMENTATION ENVIRONMENT PARAMETERS FOR SELECTION OF AN EAP METHOD

IMPLEMENTATION ENVIRONMENT PARAMETERS						
Cipher suite is CCMP or TKIP	Infrastructure Supports IEEE 802.1x	There is need to protect Identity of Communicating parties	Currently using digital Certificates for other Applications	There are Challenges in Enforcing password security by users	There is Need to use legacy authentication methods	Recommended EAP method
√	√	X	X	X	X	LEAP
√	√	X	X	X	√	LEAP
√	√	X	X	√	X	EAP-FAST
√	√	X	X	√	√	EAP-FAST
√	√	X	√	X	X	TLS
√	√	X	√	√	X	TLS
√	√	√	√	X	X	PEAP
√	√	√	√	X	√	TTLS
√	√	√	√	√	X	PEAP
√	√	√	√	√	√	TTLS

X	X	*	*	*	*	Cipher suite to be upgraded to CCMP or TKIP & Authentication mechanism to IEEE 802.1x
X	√					Cipher suite to be upgraded to TKIP or CCMP.
√	**X**					Authentication mechanism to be upgraded to IEEE 802.1x

Key: √: Yes
X: No
* : Yes/No

VI. CONCLUSION

Based on research carried out in selected public WLANs, it is evident that many IEEE 802.11 WLANs have various implementation issues that may contribute to poor WLAN authentication and access control security performance. Various EAP methods with differing characteristics exist. Each EAP method is suitable for a particular implementation environment characteristics. Network administrators can therefore benefit from the proposed selection mechanism to enable them map an EAP method with the implementation environment.

REFERENCES

[1]. 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.

[2]. 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.

[3]. 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.

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

[5]. 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.

[6]. Kshitij,R. , Dhananjay, M. & Ravindra,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.