International Research Journal of Computer Science (IRJCS)
Issue 06, Volume 4 (June 2017)
ISSN: 2393-9842
www.irjcs.com

Vulnerability Analysis of 802.11 Authentications and Encryption Protocols: CVSS Based Approach

David Gitonga Mwathi*
Department of Computer Science,
Chuka University, Kenya.
dgmwathi@chuka.ac.ke

William Okelo-Odongo
School of Computing and informatics,
University of Nairobi, Kenya.
wokelo@uonbi.ac.ke

Elisha Opiyo
School of Computing and informatics,
University of Nairobi, Kenya.
opiyo@uonbi.ac.ke

Manuscript History
Number: IRJCS/RS/Vol.04/Issue06/JNCS10082
Received: 19, May 2017
Final Correction: 24, May 2017
Final Accepted: 26, May 2017
Published: June 2017
Citation: Mwathi, D. G.; Okelo-Odongo, W. & Opiyo, E. (2017), 'Vulnerability Analysis of 802.11 Authentications and Encryption Protocols: CVSS Based Approach', IRJCS:: International Research Journal of Computer Science Volume IV (Issue VI), 16-23.
Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

Abstract - *This paper analysis vulnerability of known attacks on WLAN cipher suite, authentication mechanisms and credentials using common vulnerability scoring system (CVSS).*

Keywords *- WLAN vulnerabilities, Cipher suite, CVSS analysis, attack tree analysis, authentication mechanism*

I. INTRODUCTION

Public wireless local area networks (PWLANs) are today available in many places; University campuses, coffee shops, hotels, airports, homes, fast-food restaurants and municipalities/cities [13], [14]. One of the main reasons for their popularity is provision for the support of a normal local area network while allowing movement of client devices without the added cost and complexity of cabling within the coverage area of that Wireless LAN. However, WLANs presents a set of unique risks [5]. The access point broadcasts its service set identifier (SSID), signal level, MAC address, security features and location to devices within its signal coverage. This allows client devices deployed by attackers within the range to detect it and possibly connect to the institutional network. Also WLAN sniffer tools can be deployed by attackers to capture data frames sent over the air .The captured data is then imported into encryption crackers for decryption. In situations where the captured frames are unencrypted, one can directly extract sensitive security data such as email and website passwords since they will be in clear-text. In addition rogue WLANs masquerading as real access points can establish connections and intercept or inject data into the real WLAN. Since it is inevitable to deploy WLANs because of the benefits they come with, it is crucial that critical vulnerabilities are identified so that appropriate countermeasures can be prioritized.

II. RELATED WORK

A survey carried out by [9] to investigate IEEE 802.11 implementation specific issues that may contribute to poor WLAN authentication and access control security performance in WLANs implemented in Kenyan Universities revealed that University WLANs have implemented cipher suite protocols and authentication mechanisms in ways that expose them to well-known vulnerabilities. Khidir and Ali [6] provide a comparative analysis that reveals strengths and weaknesses of common EAP methods used for authentication namely; MD5, TLS, TTLS, PEAP, LEAP and FAST. The analysis is based on the following 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. In another study [7] compares the same authentication methods based on the same parameters with addition of a new parameter implementation technique.[12] gives a detailed study of some of the commonly used EAP methods; MD5, LEAP, TLS, TTLS and PEAP. The main advantage of these comparative studies is that we can choose between a technique which is more reliable for communication and one which is worse. However, in all these studies, none provides severity levels of the security attacks associated with each method. This information if provided would facilitate decision making on the choice of the appropriate method based on the underlying circumstances.

Many researchers have established that credentials used during authentication can be pilfered in order to gain access to a WLAN with dictionary and brute force attacks being the most common techniques [13].Other known techniques for credential pilfering includes phishing and sniffing. Analysis of various authentication methods show that the most common authentication credentials include; password, secret key, pre shared key, SSID, MAC address, one time password, client and server certificates. Each of these credentials has its own vulnerabilities when used for authentication, most of which are due to misconfigurations. Many hotspots and guest WLANS operate in open mode allowing any station to connect to that network without any credentials while others have been configured with default passwords [10]. Some open WLANs may rely on MAC address as credentials .However, various available open source attack tools e.g. Kismet can sniff MAC addresses of authorized client devices [8].While these vulnerabilities are known, their severity levels have not been studied.

IEEE 802.11 [2] and [3] defines several cipher suites, authentication and access control methods. Many researchers have revealed vulnerabilities in these security components. However, their severity levels have also not been studied. We therefore argue that a lot can be gained by understanding the severity levels of various attacks targeting various security features.

III. INTRODUCTION TO COMMON VULNERABILITY SCORING SYSTEM (CVSS)

CVSS [4] is an industry open standard designed to convey vulnerability severity and helps determine urgency and priority of response. It solves the problem of multiple, incompatible scoring systems and is easy to understand and use. CVSS was commissioned by the National infrastructure advisory council (NIAC) tasked in support of the global vulnerability disclosure framework. It is currently maintained by forum of incidence response and security teams (FIRST).CVSS is a joint effort involving many groups including CERT/CC, Cisco, DHS/MITRE, eBay, IBM internet security systems, Microsoft, Qualysis, Symantec. Many other groups have assisted in improving CVSS. The CVSS Model is designed to provide the end user with an overall composite score representing the severity and risk of a vulnerability. It is derived from metrics and formulae. CVSS has three main metrics that can be quantitatively and qualitatively measured; temporal metrics, environmental metrics and base metrics. Temporal metrics contain characteristics of vulnerability which evolve over the lifetime of vulnerability while environmental metrics contain those characteristics of vulnerability which are tied to an implementation in a specific environment. Base metrics on the other hand contain characteristics that are intrinsic to any given vulnerability and do not change over time or in different environments. In this research, base metrics were adopted for analysis of vulnerabilities because of their intrinsic and static nature. These metrics include; attack vector (AV), attack complexity (AC), privileges required (PR), user interaction (UI), scope(S), confidentiality impact(C), integrity impact (I) and availability impact (A).Attack Vector (AV) reflects the context in which the vulnerability exploitation occurs. The more remote an attacker can be to the target, the greater the vulnerability score. The rationale is that the number of potential attackers for a remotely exploitable vulnerability would be much larger than that for an attack requiring local access. Attack Complexity (AC) describes the conditions beyond the attacker's control that must occur in order to place the system in a vulnerable state. This metric excludes any user interaction requirements. Privileges Required (PR) describes the privileges an attacker requires before successfully exploiting the vulnerability, and the potential impact they could inflict on a system after exploiting it. User Interaction (UI) captures the requirement for a user (other than the attacker) to participate in the successful exploit of the target system. This metric will determine whether or not the vulnerability can be exploited solely at the will of the attacker, or if a user must participate by taking action.

Metric scope(S) measures whether the authorization scope of the vulnerable component is the same or different from the authorization scope of the component impacted by the vulnerability. If the vulnerable component is in the same authorization scope as the component impacted by the vulnerability, then the scope of impact is unchanged. However if the vulnerable component is in a different authorization scope from the component impacted by the vulnerability then the scope is changed. Confidentiality Impact (C) measures the impact to confidentiality of a successfully exploited vulnerability. Increased confidentiality impact increases the vulnerability score. Integrity Impact (I) measures the impact to integrity of a successfully exploited vulnerability. Increased integrity impact increases the vulnerability score. Lastly, Availability Impact (A) measures the impact to the availability of the affected Impact Scope resulting from a successfully exploited vulnerability. While the Confidentiality and Integrity impact metrics apply to the loss of confidentiality or integrity of data (e.g. information, files) used by a affected Impact Scope, this metric refers to the loss of availability of the affected Impact Scope, itself, such as networked service (e.g. web, database, email, etc). Since availability refers to the accessibility of information resources, attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of an affected Impact Scope. Increased availability impact increases the vulnerability score.

IV. DATA COLLECTION AND ANALYSIS PROCEDURE

This involved identification and analyzing the WLAN vulnerabilities exploited by known attacks on cipher suite, authentication credentials and authentication mechanisms. The attacks directly target the authentication mechanism itself, authentication credentials or confidentiality and integrity cryptographic algorithms in use during and after successful authentication and access control. Attack tree methodology was used to model the attacks which were analyzed using common vulnerability scoring system (CVSS). Articles from peer reviewed journals, white papers, conference papers, technical reports or part of the standards literature that is emerging in the area addressing known WLAN authentication and access control attacks on WEP, WPA and WPA2 was used. Exhaustive search was employed i.e. articles were searched and picked from various sources and databases matching the inclusion criteria above. The scope of the literature analysis extended from most current to 2001 when the first serious paper on WEP insecurity was presented [1] and the limiting factor was the natural limit to the effort the author spent on collection. Work that clearly diverged from operational WLAN security was not taken into account as well as papers that offered highly specific analysis not related to computing and information security in operational settings. Redundant articles were discarded e.g. where the same or very similar attacks appear in more than one publication, often by the same (or common subsets of) authors that have gradually extended a concept. This procedure is summarized as follows;

(a). From the literature sources:

(i) Identify known attacks targeting authentication and access control mechanisms (open, pre-shared key, MAC address filtering, captive portal, IEEE 802.1x EAP methods),authentication credentials(password, secret key, pre shared key ,SSID,MAC address, one time password, client and server certificates) and Cipher suites negotiated during Authentication and Access Control(WEP,TKIP,CCMP)

(ii) Establish the set of tools that can be used to launch each of the attacks and the availability of the tools.

(iii) Establish the security features and configurations that contribute to each of the identified attacks.

(iv) Establish the vulnerabilities in the identified security feature or configuration that lead to realization of the attack.

(b). Model the attacks on an attack tree using attack tree methodology.

(c). Based on CVSSv3 model base metrics, analyze the severity of the vulnerabilities.

A. Attack Tree

Attack trees are formal methods of modeling attacks by systematically characterizing system security based on varying attacks [11]. Based on [11], the following procedure was used to create attack trees for this research;

(i) Cipher suite, authentication credentials and authentication mechanism formed the goals with each goal forming a separate tree.

(ii) All attacks against each goal were identified and added to the respective tree with the vulnerabilities for each attack forming the tree branch nodes (sub tree)

(iii) This process was repeated for all the three goals.

B. Analysis Based On CVSS Base Metrics

Figure 1shows the online calculator used to compute CVSS scores for all the vulnerabilities

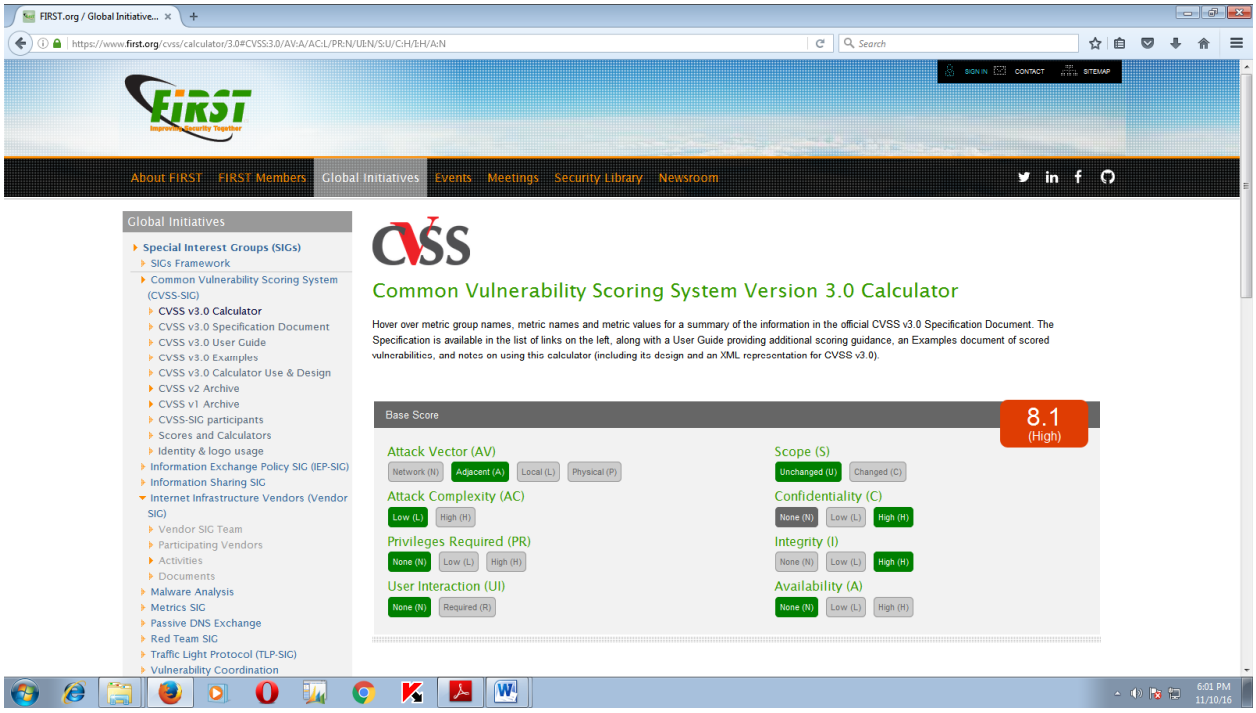

Figure 1: Common vulnerability scoring system version 3.0 calculator (FIRST, 2014)

V. RESULTS

A. Authentication and Access Control Mechanisms Attacks

Table I, II and III shows vulnerability scores of attacks on authentication mechanisms. From the CVSS scores, captive portal has highly vulnerable attacks when used as an authentication mechanism especially if not SSL encrypted. Captive portals provide no encryption for wireless users; instead they rely on the MAC and IP address of the client as a unique identifier which can be spoofed easily. They therefore do not provide protection against eavesdropping and so are vulnerable to session hijacking (man in the middle attack)/captive portal evil twin. Pre-shared key authentication exposes a WLAN to access point impersonation attacks as well as Pre-shared key recovery attacks both with high attack susceptibility. Lack of mutual authentication (access point is not authenticated to a client station) is a major contributor to access point impersonation/rogue access points. Also Password recovery, cracker and sniffer tools such as Cain and Abel, which are freely available, can easily recover weak pre-shared keys. The difficulty of managing security of manually distributed pre-shared keys (PSKs) on numerous devices makes pre-shared key authentication not suitable for use in large enterprise public WLAN deployments such as universities. The challenge handshake protocol (CHAP) used in this scheme has vulnerabilities that are easily broken. This indicates that pre-shared key is a weak authentication mechanism. Combining pre-shared key and captive portal authentication provides improved security.MAC address filtering access control mechanism leads to highly vulnerable impersonation attacks and so needs to be avoided. Though 802.1x authentication and access control has many attacks, attack susceptibility of these attacks is on average low. This makes it stronger than both captive portal and pre-shared key.

TABLE I: CVSS VULNERABILITY SCORES OF ATTACKS ON AUTHENTICATION AND ACCESS CONTROL MECHANISMS

S/N	Attack	Configuration issue/Vulnerable feature	AV	AC	PR	UI	S	C	I	A	CVSS Score
1	STA Impersonation attacks	-Use of MAC address filtering access control mechanism^ -Lack of Management frame protection^ -MAC address spoofing^ -Open/Null Authentication^ -No Mutual Authentication	A	L	N	N	U	H	H	N	8.1 [Very High]
2	Captive Portal circumvention (Evil Twin)	-Use of captive portal authentication that is not SSL encrypted.	A	L	N	N	U	H	H	L	8.3 [Very High]
		Allowing SSL Self signed certificates from the captive portal Lack of Validation of SSL server certificate Lack of validation of captive portal server name.	A	H	N	N	U	H	H	L	7.1 [High]

3	Pre-shared key recovery attacks	Use of Pre-shared key authentication mechanism^ Weak Pre-shared key ^ Use of challenge handshake authentication protocol.	A	L	N	N	U	H	L	N	7.1 [High]
4	802.1x Identity theft	-Use of 802.1x with EAP TLS ^ -Capturing user identities from clear text 802.1x Identity response packets.	A	H	N	N	U	L	N	N	3.1 [Low]
5	802.1x password guessing	Capturing identity and then repeatedly attempting 802.1 x authentications to guess the user's password.	A	H	N	N	U	L	N	N	3.1 [Low]

TABLE II: CVSS VULNERABILITY SCORES OF ATTACKS ON AUTHENTICATION AND ACCESS CONTROL MECHANISMS

6	AP impersonation attack	Use of Pre-shared key authentication mechanism ^ Lack of support for mutual authentication(Access point not authenticate) ^ -SSID Unencrypted	A	H	N	N	U	H	H	L	7.1 [High]
		802.1x with EAP based authentication Weak AP-AS passphrase Not regularly changing AP-AS passphrase	A	H	N	N	U	L	N	N	3.1 [Low]
7	802.1x LEAP cracking	Use of light weight EAP method.	A	H	N	N	U	H	N	N	5.3 [Medium]
8	802.1x EAP downgrade attack	802.1x AS forced to offer weak type of authentication using forged EAP-response/Nak packets	A	H	N	N	U	N	L	N	3.1 [Low]
9	802.1x EAP length attacks	AP or RADIUS server crashes after receiving EAP-type-specific messages with bad length fields	A	H	N	N	U	N	N	L	3.1 [Low]
10	802.1x EAP of death	AP crash after receiving malformed 802.1x EAP identity response	A	H	N	N	U	N	N	L	3.1 [Low]

TABLE III: CVSS VULNERABILITY SCORES OF ATTACKS ON AUTHENTICATION AND ACCESS CONTROL MECHANISMS

11	802.1x EAP Start Flood	Flooding an AP with EA Pol –Start messages-AP CRASHES	A	H	N	N	U	N	N	L	3.1 [Low]
12	802.1x EAP Replay	Lack of a nonce or timestamp ^ an eavesdropper records EAP authentication process of a legitimate client and replays it to gain the access to the network	A	H	N	N	U	N	L	N	3.1 [Low]
13	802.1x EAP – failure	Lack of a nonce or timestamp ^ an eavesdropper records a valid 802.1x EAP exchange and then sends a station a forged EAP failure message	A	H	N	N	U	N	L	L	4.2 [Medium]
14	Brute force attacks	Use of PIN based WIFI protected setup for authentication	A	L	N	N	U	H	H	N	8.1 [Very High]

B. Authentication Credentials Attacks

Various Credentials used to authenticate an identity in a WLAN include; passwords/secret key, SSID, PIN, MAC address, session key and certificates. These credentials are attributed to attacks as shown in the tables IV and V. The attacks exploit vulnerabilities that are intrinsic to the credentials or those that are as a result of the way the authentication credentials are implemented e.g. use of MAC address is easily spoof able, wireless protected setup (WPS)-PIN is a weak credential, weak passwords, dictionary based passphrases, not regularly changing authentication server –access point passphrase, use of certificates signed by public CAs, self- signed certificates, allowing a client to choose the CA, etc. Password recovery, cracker and sniffer tools such as Cain and Abel, which are freely available, can easily recover weak pre-shared keys. These attacks can be avoided by using strong passwords, use of certificate signed by an internal trusted CA, not allowing self signed certificates. Implementers should also avoid use of MAC address only for authentication as well as wireless protected setup (WPS) that uses PIN for authentication.

TABLE IV: CVSS VULNERABILITY SCORES FOR AUTHENTICATION CREDENTIALS BASED ATTACKS

S/N	Attack	Configuration issue/Vulnerable feature	AV	AC	PR	UI	S	C	I	A	CVSS Score
1	EAP Dictionary Attacks	Use of weak Ms-CHAP-password	A	L	N	N	U	H	H	N	8.1 [Very High]
2	WPA-PSK Dictionary/ PSK Cracking	-Weak pre-shared key - Use of dictionary based passphrases.	A	H	N	N	U	H	H	N	6.8 [Medium]
3	Password based MITM attack	Use of Password/secret key as authentication credentials for an EAP method	A	H	N	N	U	H	H	N	6.8 [Medium]
4	STA Impersonation attacks	Use of MAC address as only authentication credential.	A	L	N	N	U	H	H	N	8.1 [Very High]
5	802.1x password guessing	-Clear text 802.1x identity -Weak session key/password	A	H	N	N	U	H	H	N	6.8 [Medium]

TABLE V: CVSS VULNERABILITY SCORES FOR AUTHENTICATION CREDENTIALS BASED ATTACKS

6	Brute force attacks	-Use of PIN as authentication credential -Weak pre-shared key - Use of dictionary based passphrases.	A	L	N	N	U	H	H	N	8.1 [Very High]
7	802.1x RADIUS Cracking	Weak AP-AS passphrase AS-AP passphrase that is never changed.	A	H	N	N	U	L	L	N	4.2 [Medium]
8	RADIUS certificate MITM attacks	Self signed certificates.	A	L	N	N	U	H	H	N	8.1 [Very High]
		Certificate signed by a public CA	A	L	N	N	U	H	H	N	8.1[Very High]

C. Cipher Suite Attacks

This consists of attacks emanating from various cipher suites used in combination with authentication mechanisms.

Table VI, VII and VIII shows vulnerability scores of attacks on confidentiality and integrity cryptographic algorithms (cipher suite) negotiated during authentication and access control. From the table, wired equivalent privacy (WEP) is highly susceptible / vulnerable because of weak confidentiality (RC4) and integrity (CRC-32) algorithms. The researcher therefore recommends that this cipher suite is not used at all in any implementation because it will expose the WLAN to highly vulnerable attacks. While TKIP/WPA is also prone to attacks due to weak encryption algorithm (RC4), the vulnerability susceptibility is moderate because the integrity algorithm is moderately strong.WPA2/CCMP is strongest cipher suite with known vulnerabilities whose susceptibility is low. Some of the attack tools include Air Snort for cracking WEP key and Air Crack for attacking WPA.

TABLE VI: CVSS VULNERABILITY SCORES OF ATTACKS ON CONFIDENTIALITY AND INTEGRITY PROTOCOLS

S/N	Attack	Configuration issue/Vulnerable feature	AV	AC	PR	UI	S	C	I	A	CVSS Score
1	FMS	WEP with Weak encryption algorithm (RC4^ Use of static encryption key.	A	L	N	N	U	H	H	N	8.1 [Very High]
2	KoreK	WEP with Weak encryption algorithm(RC4)	A	L	N	N	U	H	H	N	8.1 [Very High]
3	PTW	WEP with Weak encryption algorithm(RC4)	A	L	N	N	U	H	H	N	8.1 [Very High]
4	ChopChop	WEP with Weak encryption algorithm(RC4)	A	L	N	N	U	H	H	N	8.1 [Very High]
5	Bit flipping attacks	WEP with Weak integrity protection CRC-32^Weak encryption algorithm(RC4)	A	L	N	N	U	H	H	N	8.1 [Very High]

TABLE VII: CVSS VULNERABILITY SCORES OF ATTACKS ON CONFIDENTIALITY AND INTEGRITY PROTOCOLS

6	Iterative key guessing attacks	WEP with static encryption key^ Weak encryption algorithm(RC4)	A	L	N	N	U	H	H	N	8.1 [Very High]
7	STA Impersonation attacks	WEP with Weak integrity algorithm allowing spoofing of the source address WEP with Weak confidentiality protection algorithm (RC4) allowing spoofing of the source address.	A	L	N	N	U	H	H	N	8.1 [Very High]
8	WPA/TKIP Decryption attack.	WPA with Weak encryption algorithm(RC4)	A	H	N	N	U	H	H	N	6.8 [Medium]
9	WPA-PSK Dictionary/ PSK Cracking	WPA with short, dictionary based passphrases ^ -Weak encryption algorithm(RC4)	A	H	N	N	U	H	H	N	6.8 [Medium]
10	WPA-PSK Dictionary/ PSK Cracking	WPA2 with Short, dictionary based passphrases.	A	H	N	N	U	L	L	N	4.2 [Medium]

TABLE VIII: CVSS VULNERABILITY SCORES OF ATTACKS ON CONFIDENTIALITY AND INTEGRITY PROTOCOLS

11	TKIP Countermeasures	WPA/TKIP^ TKIP Countermeasure	A	H	N	N	U	H	H	L	7.1 [High]
12	WPA Hole 196 Denial of service	Implementing both WPA and WPA2 cipher suites in a WLAN -Virtual WLANs	A	H	L	N	U	L	L	N	3.7 [Low]
13	802.11 Management frame Replay attacks	WEP with Weak integrity protection CRC-32	A	L	N	N	U	H	H	N	8.1 [Very High]
14	Brute force attacks	WEP with Weak pre-shared key	A	L	N	N	U	H	H	N	8.1 [Very High]
		WPA with Weak pre-shared key	A	L	N	N	U	H	H	N	6.8 [Medium]
		WPA2 with Weak pre-shared key	A	H	N	N	U	L	L	N	4.2 [Medium]
15	ARP Poisoning	Implementing both WPA and WPA2 cipher suites in a WLAN	A	H	L	N	U	N	L	L	3.7 [Low]

CONCLUSION

This paper focused on analysis of vulnerabilities on authentication and cipher suite algorithms when implemented in a Wireless local area network. It brought into light the severity levels of some known attacks on IEEE 802.11 networks. However, we did not suggest any solution to protect the network from the attacks related to these vulnerabilities. As of yet, there is no complete and fully trusted system or protocol developed to provide security as intruders' behaviors are noticeably different from each other . Since technology provides opportunities to find solutions, introducing new technology may provide some sort of support for the time being. However, as time goes on hackers will be able to work on the vulnerabilities and develop tools to exploit them. Protecting WLAN will always pose challenges and therefore implementers need to look at the attack severity levels in this paper and mitigate the risks by introducing countermeasures that particularly target attacks/vulnerabilities with very high to medium severity levels.

REFERENCES

1. Borisov,N., Goldberg, I. and Wagner, D.(2001). Intercepting Mobile Communications: The Insecurity of 802.11. In: *Proceedings of 7th Annual International Conference on Mobile Computing and Networking*, Rome, Italy: ACM Press.
2. EEE Standard 802.11.(1999). Information technology –Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Moderate Access Control and Physical Layer Specifications. IEEE
3. IEEE Standard for Information technology. (2004). Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements, Part 11, Amendment 6: Moderate Access Control (MAC) Security Enhancements. IEEE Standard 802.11i.

4. FIRST.(2014).*Common vulnerability scoring system version 3.0 calculator.*[Online] Available at: https://www.first.org/cvss/calculator/3.0[Accessed 12 July .2016].
5. Joanne, S. (2007*).* Dangerous Mobile Behavior Our Students and University Employees Need To Know About, *CCSC: Southeastern Conference*.
6. Khidir, M. and Ali, A. (2011).A Comparative Study of Authentication Methods for Wi-Fi Networks. In: *Proceedings of International Conference on Computational Intelligence, Communication Systems and Networks*[Online],pp.190-194,Available at: http://www.computer.org/csdl/proceedings/cicsyn/2011/4482/00/4482a190-abs.html[Accesed 10 Jan 2014]
7. Kshitij,R., Dhananjay, M. and Ravindra,L.(2013).Authentication Methods for WI-Fi Networks, *International journal of Applications or innovation in Engineering and Management*[online],Vol 2(3) ,Available at: www.ijaiem.org/volume2issue3/IJAIEM-2013-03-31-123.pdf[Accessed 26.June 2013]
8. Mathews, M., Hunt. (2007).*Evolution of WLAN Architecture IEEE 802.11i.*Newzealand: University of Canterbury.
9. Mwathi, D., Okelo-Odongo., W. and Opiyo., E. (2016).Algorithm Selection of EAP Authentication Method for use in a Public WLAN: Implementation Environment Based Approach. *International Research Journal of Computer Science,* [Online] Vol 3(5), pp.47-52.Available at: http://www.irjcs.com[Accessed 8 June.2016].
10. SANS Institute InfoSec Reading Room.(2003).Wireless LAN: Security issues and solution, US; SANS Institute, Vol 1(4)
11. Schneier.B. (1999).*Attack trees: Modeling security threats.* Dr. Dobb's Journal.
12. Umesh, K., Praveen, K., Sapna, G. (2014).Analysis and literature review of IEEE 802.1x (Authentication) protocols. *International journal of Engineering and advanced Technology* [Online*]*,Vol.3(5),Available at:www.ijeat.org/attachments/file/v315/E3173063514.pdf[Accessed 5 Jan.2015].
13. Waliullah, M., Moniruzzaman, A. and Sadekur, M. (2015). An Experimental Study Analysis of Security Attacks at IEEE 802.11Wireless Local Area Network. *International Journal of Future Generation Communication and Networking* ,Vol. 8(1), pp. 9-18
14. Wei-Lin, C., Quincy, W.(2010).A Proof of MITM Vulnerability in Public WLANs Guarded by Captive Portal. In: *Proceedings of Asian- pacific advanced network 2010* [Online] Vol 30, pp. 66-69, Available at http://dx.doi.org/10.7125/APAN.30.10,Taiwan [Accessed 15 march, 2014]

