International Research Journal of Computer Science (IRJCS)
Issue 01, Volume 6 (January 2019)
ISSN: 2393-9842
www.irjcs.com

WLAN SECURITY: A TRUSTED COMPUTING BASE APPROACH

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

Manuscript History
Number: **IRJCS/RS/Vol.06/Issue01/JACS10084**
Received: 02, January 2019
Final Correction: 17, January 2019
Final Accepted: 23, January 2019
Published: January 2018
Citation: Mwathi (2019). WLAN SECURITY: A TRUSTED COMPUTING BASE APPROACH. IRJCS:: International Research Journal of Computer Science, Volume VI, 15-20. **doi://10.26562/IRJCS.2019.JACS10084**
Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

Abstract- This paper identifies the gaps in IEEE 802.11 standards and supporting technologies and then proposes a conceptual architecture that can be used to develop a model for analyzing and predicting the security performance of selected WLAN security features and configurations.
Key Words- Trusted computing base; WLAN Security; WLAN Authentication; WLAN attacks; vulnerabilities;

I. INTRODUCTION

A Wireless Local Area Networks (WLAN) is a communication network that relies on radio frequencies for data transmission. Devices participating in this local area network broadcast data frames over a radio frequency interface. Consequently, any WLAN enabled device in the range will receive the data frames. Such networks are readily available in coffee shops, hotels, fast food restaurants and many other public places such as Universities, airports and urban areas [1], [2]. WLANs are popular because they provide all services that a wired local area network can with added advantages of client device mobility and avoiding costs associated with cabling within the WLAN coverage area. Developments in the use of portable devices such as laptops, mobile phones and tablets have also made WLANs popular. WLANs implement IEEE 802.11i and IEEE 802.11w security standards whose focus is provision of appropriate integrity and confidentiality levels. This they achieve by implementing WLAN users' access control and encrypting all the data exchanged in the WLAN. However, the flexibility of the provisions of these security standards and supporting technologies create potential for selection and configuration of vulnerable security features for various components that are key to security consequently exposing WLANs to attacks. When poorly implemented, these standards fail to achieve appropriate levels of confidentiality and integrity consequently subjecting the WLAN to unwanted access by hackers/intruders.

Once inside, the hackers make all information susceptible to sniffing and manipulation by exploiting the vulnerabilities in the implementation of the standard [3]. Current approaches to WLAN security implementation focus on few security components and therefore not comprehensive enough to address many security issues. Many network security administrators use their experience of past solutions and documentation to configure security of network equipment [4]. Once they establish that it is proper to use past experience or documentation in the environment at hand, they repeat those routine actions or follow instructions of the documentation (documented procedure or a wizard for installation) without doing dependency analysis [4]. Selection and configuration of security features in such a case is therefore guided by documented procedure or a wizard for installation. For example, suppose a network administrator needs to configure a new access point's security settings. The installation guide may instruct one to select the cipher suite first, then authentication method. The network administrator may just follow these instructions without bothering to analyze the effect of the cipher suite-authentication method security features selected on overall WLAN security. There is therefore a need to develop a comprehensive model for analyzing and predicting the overall security strength provided by selected WLAN security features and configurations.

II. RELATED WORK ON WLAN SECURITY IMPLEMENTATION APPROACHES

A. Pre-Robust security Network (Pre-RSN) Approach

Pre-RSN approach focuses on two components: client device and accesspoint.It is characterized by use of wired equivalent privacy (WEP) protocol to provide confidentiality and integrity. WEP was designed to provide reasonable strength, self-synchronization and processing efficiency that could leverage the security of a wired network against external attacks[5].While initially WEP appeared to have met this goal, it has since been established to be very weak[6], [7]. Despite its weaknesses, WEP is still widely deployed in WLANs like those of universities to allow students to connect to university's hot spots [8], [9].

B. Robust Security Network (RSN) Approach

Robust security network approach focuses on three components: client device, accesspoint and authentication server to provide security to a WLAN.It is a product of IEEE 802.11 amendment. The client device identifies an accesspoint for a WLAN and both negotiate and agree on a common security policy which specifies key security parameters such as cipher suite protocols (TKIP or CCMP), authentication mechanism and a key distribution approach. The two devices finally associate based on agreed security policy. The client station and authentication server authenticate each other via the access point. When authentication is successful, the accesspoint and the client device perform a four way handshaking operations that cause cryptographic keys to be generated and placed on the accesspoint and the client device. The four way key handshake mechanism validates that both accesspoint and client device share a pair-wise master key(PMK),synchronizes the installation of temporal keys and confirms the selection and configuration of data confidentiality and integrity protocols When this is done, all communications between the client device and access point are encrypted[10]. While this architecture is designed to provide a high level of security in a WLAN, it requires implementers to be cautions with accesspoint configurations such that they only allow RSN associations. Any combination of pre-RSN and RSN associations will lead to a vulnerable implementation because attackers will exploit pre-RSN vulnerabilities to launch attacks [11].

C. Wireless Group Network Policies Approach

Consists of two subsystems; wireless MMC snap-in which operates on the server side and used to make wireless group policy settings. The other subsystem is wireless client side extension (CSE) which operates on the client side and pulls settings made on the server side to the client's registry. This approach focuses on five components which it considers key to WLAN security: Wireless client, wireless accesspoint, Authentication server, authentication and access control mechanism and user database. Wireless network group policy architecture covers salient components of WLAN security and has the ability to enforce uniform security features on all client devices on the WLAN.On the other hand, besides being a proprietary design; implementers do not have a way of visualizing the level of security expected from the wireless group security policies set.

III. METHODOLOGY

Informed by survey and observation of 31 WLAN networks and related works on WLAN security, provisions of IEEE 802.11 standards and protocols, known attacks and vulnerabilities to WLAN security and attack tools, the researcher developed a conceptual architecture for implementing WLAN security. Twenty experts (researchers and consultants) in the area of network security with high level of competence in WLAN security were used to validate the suitability of the conceptual architecture for its intended purpose within the domain of its intended applicability. These experts were drawn from universities and industry.

IV. PROPOSED APPROACH

The architecture is based on trusted computing base concept. Trusted computing base is a small amount of software and hardware components that security depends on and that we distinguish from a much larger amount that can misbehave without affecting security [12]. The orange book regards TCB of a computer system as totality of protection mechanisms within it, including hardware, firmware, software and controls the combination of which are responsible for enforcing a computer security policy [13]. This fundamentally means that a TCB is a set of all hardware, firmware and software components of a computer system that are critical to its security such that any vulnerabilities occurring inside a TCB negatively influences the security level of the entire system. WLAN security which is a measure of the overall security strength provided by a WLAN implementation is therefore influenced by eight components which comprise its trusted computing base; Cipher suite, Authentication credentials, Client driver, Client utility, Access point utility, Authentication server, Authentication & access control Mechanism and User database system. The eight components are the key sources of vulnerabilities which may lead to security attacks in a WLAN. Client utility, Client driver and access point utility constitute the client side of security components(Front-End system software) while Authentication server, Authentication & access control Mechanism and User database system constitute the server side of security components(Back-End authentication systems). Cipher suite and authentication credentials constitute the security of the wireless path linking client device and access point. The wireless path between client device and access point is a key security element because it is prone to major security threats.While the trusted computing base concept was originally used in design of operating systems security [14], the researcher has adopted the concept for use in WLAN security. Fig 1 shows the proposed conceptual architecture for WLAN security implementation followed by a detailed description of the components.

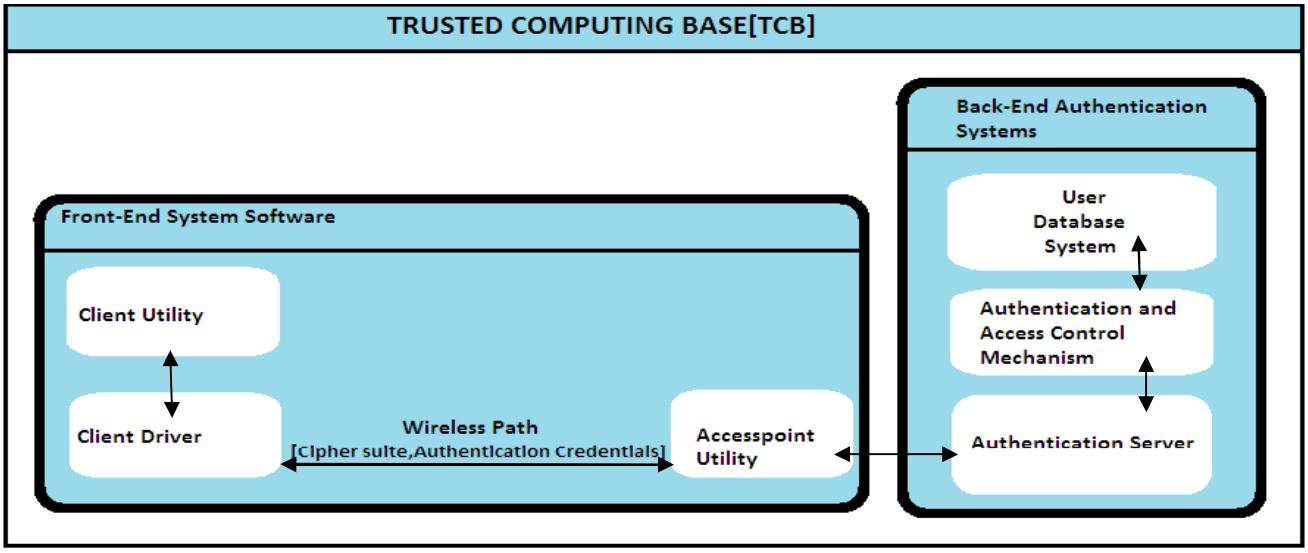

Fig 1: Conceptual Architecture of WLAN Security Implementation

A. Cipher Suite

Refers to cryptographic algorithms used to encrypt messages as well as perform integrity check for possible modification of messages between a wireless client device and access point. The strength of cryptographic algorithms implemented impacts on security of traffic exchanged on the wireless path between a client device and access point. Cipher suites used in WLANs include: CCMP, TKIP (WPA +AES), TKIP (WPA + RC4), TKIP (WPA2 +RC4) and WEP. The type of cipher suites employed in a WLAN impacts on its security because each has varying attack susceptibilities.

B. Authentication Credentials

Refers to the messages delivered to the authentication server or provided by the authentication server and used to verify a claim by an entity (client or server) that it is authorized to act on behalf of a known identity. The nature and type of authentication credentials exchanged between a client device and access point impacts on the security of the wireless path because each has unique attack susceptibilities. Credentials used for authentication in WLANs include: client and/or server certificates, protected access credential (PAC), one time password, secret key, password, SSID, MAC address and PIN.

C. Client Utility

Client utility refers to utility software (also called supplicant) running on the client machine and that communicates with access point firmware/utility. Whenever a client utility is misconfigured e.g. a client device configured not to support management frame protection or where support is optional, then connection by the client device to a WLAN without protection for management frames is possible. This has potential to cause security breaches such as disassociate and de-authentication attacks [15]. Many WLAN users configure their client utility to ignore validation of authentication server certificate and the specific authentication server address (name) verification. Additionally the client utility is also configured in such a way that users can choose the server that is the source of the certificate creating a potential for RADIUS certificate attacks [9].

D. WLAN Client Driver

WLAN Client driver refers to the WLAN device driver implemented on the client Machine. Device drivers are key sources of security vulnerabilities in operating systems [16].Although protected by security mechanisms such as personal firewalls, anti-virus and host intrusion prevention systems, the mechanisms are ineffective in handling WLAN driver attacks. This is because drivers run with kernel privileges and therefore the attacker targeting WLAN drivers is able to run code with kernel privileges [17]. Compared with other kernel code, drivers experience higher error rates making them the most poor quality code in most kernels [18]. The fact that the device driver code is developed by programmars who may not possess deep knowledge of the target operating system kernel is one factor that contributes to the high error rate [19]. Drivers for wireless interface cards, most of which conform to IEEE 802.11 standards are easy to interact with and potentially exploit if the attacker is within the radio range of the client device [20] .Therefore the high availability of IEEE 802.11 devices, the ease of driver interaction and possibility of poor quality driver code creates potential for an attacker to fingerprint a device driver and consequently launch a driver-specific exploit [17]. IEEE 802.11i does not provide an explicit algorithm to be used by client device drivers to scan (probe) for access point. Therefore, developers of device drivers develop and implement their own probing mechanism. Since various WLAN drivers have their specific probing algorithm it is easy to identify a driver based on the unique scanning approach it employs. Once identified its vulnerabilities may then be exploited. Security features and configurations of a WLAN driver implemented on wireless client Machines therefore impact on WLAN security.

E. Access Point Utility

Refers to the security features and configurations of system software running on the access point and/or WLAN controller. Access point is a device that authenticates client devices or may be configured to act as an authenticator passing authentication information to a separate authentication server. Access point broadcasts its security capabilities using two approaches. The first approach is through beacon frames sent from access point's specific channel and the other one is through a probe response frame. Security capabilities of beacon or probe response frames are contained in robust security network information element. Client devices configured to managed mode can therefore discover available access points and their corresponding security capabilities by actively probing every channel while those in monitor mode will passively monitor the beacon frames from the access point. Many access point utility/firmware are configured not to support management frame protection such as authentication requests [21].An adversary can install his/her own access point with a spoofed MAC address, spoofed SSID, configured with appropriate freeware e.g. HostAP and with a strong signal to fool a client device into associating with it and leaking credentials or private data [22].

F. Authentication Server

Refers to the protocol employed by the server application (IEEE 802.1x enabled or non-IEEE 802.1x) that processes authentication requests from the client utility [23]. While there are many authentication servers, different authentication servers support varying authentication and access control methods. The two main protocols standardized by internet engineering task force (IETF) and used for WLAN authentication are RADIUS and DIAMETER. While DIAMETER provides end to end authentication, RADIUS authentication of the entity is hop by hop and not end to end. DIAMETER'S end-to-end security framework provides message origin authenticity even when there are relays or proxies present[24].On the other hand, because of the RADIUS hop-per-hop shared secrets and changing identifiers, all proxies must be able to read and modify any message. Proxies also may or may not send proxy-state attributes from the client side to the remote server, and they may need to modify other attributes to enforce a local policy. Thus the messages may change when travelling through the proxies. This makes the entire data authentication, integrity and confidentiality support difficult [23]. While both protocols offer some protection against replay attacks ,DIAMETER is more secure than RADIUS because it uses some kind of transport layer security scheme, such as IP Security or TLS which guarantees replay protection[24].On the other hand, IP security support for RADIUS is optional. Whereas DIAMETER server is allowed to initialize messages e.g server re-authentication, RADIUS server cannot initiate messages. Only its client can do so.In RADIUS, all user passwords are always sent encrypted. However, password is the only part of the packet that is encrypted and that neither the RADIUS specification nor the RADIUS extensions provide support for whole packet confidentiality [23].While RADIUS uses unreliable, best effort delivery UDP for transport, DIAMETER uses TCP or SCTP at transport layer which are reliable [25].Use of a reliable transport protocol enables DIAMETER to have an error reporting mechanism such that its messages are only discarded when there is no other suitable way to solve the problem. This is unlike RADIUS which stops any further processing and discards/drops packets whenever any fault occurs causing denial of service. Other AAA protocols that may be used for authentication include; Terminal access controller access control system (TACACS), Enhanced Terminal access controller access control system (TACACS+) and Kerberos. Each has its own unique weakneses that influence WLAN security if implemented.

G. Authentication and Access Control Mechanism

Refers to the specific approaches used to verify the claim that an entity is allowed to act on behalf of a given known identity in order to access wireless LAN. The approaches also restrict the right of an entity to accessing a WLAN until the entity is verified and cryptographic keys established.Authentication and access control mechanisms range from open SSID authentication,MAC address filtering, PIN based authentication(WPS), Button press based authentication(WPS),pre-shared key authentication, IEEE 802.1x Port based access control with EAP authentication and captive portals. The type of authentication and access control mechanism employed in a WLAN impacts on its security because each has unique attack susceptibilities.

H. User Database Architecture

User database refers to the configuration and database architecture (distributed or centralized) used to store information used to verify user identities during authentication. User Databases stores user names and password or MAC addresses [26].Examples of user databases include: Microsoft's active directory/LDAP, access point internal database, local flat text file, relational database file e.g. SQL or MySQL database. The attacks targeting user database are mainly denial of service attacks. These attacks target situations where the database resides in the access point or when MAC address filtering is used for access control. In other cases, the database server may be on a dedicated server but due to centralized architecture, the server's resources are consumed by malicious and sometimes distributed authentication requests. When WLAN user database is implemented on an active directory, it will constantly be inundated with new queries from various applications which will make WLAN DOS attacks successful [26].Examples of known attacks on user database include database server denial of service(DOS), distributed flooding, authentication flooding and injection attacks[27].

V. DETERMINATION OF SECURITY LEVELS OF ARCHITECTURAL COMPONENTS

Three approaches can be employed to determine security levels of architectural components in the conceptual architecture: Weighted average, Bayesian network and Fuzzy logic. The researcher proposes a weighted average approach to determine security levels. In this approach, the attributes (security feature/configuration on each component) will be scored independently, on a common scale of value. This involves transformation from attribute (security feature/configuration) to value (could be a score e.g 3 or a category e.g "High"). This will be done by a **value function** that needs to be developed. The second step is to combine multiple values (results of value function) into a single value using a **combination function** which also needs to be established. Weighted average approach exhibits pragmatism in assigning attributes to values because an attribute (security feature/configuration) is mapped to a specific value/category e.g. WPA2 is mapped to weak, medium or high security categories. This is unlike Bayesian network and fuzzy logic approaches which allow an attribute(in this case a security feature/ configuration) to have multiple categories with varying degrees e.g a security feature WPA2 could have weak, strong and medium categories within it such as weak(60%) ,medium(30%) or strong(10%).

VI. CONCEPTUAL ARCHITECTURE VALIDITY

Twenty experts (researchers and consultants) in the area of network security with high level of competence in WLAN security were used to validate the suitability of the conceptual architecture for its intended purpose within the domain of its intended applicability. The aggregated findings revealed that majority (96.25 %) of the respondents were confident with the conceptual architectural components, 3.125 % were not decided while 0.625 % disagreed with the components without giving reasons. These findings indicate a high level of expert confidence in the proposed conceptual architecture.

VII. CONCLUSION

This paper has brought into perspective the key WLAN computing components (Trusted computing base) that need to be addressed in order to solve the problem of selection, design and configuration of security features for WLAN.This has been achieved through development of a generic conceptual architecture. However, there is a need to develop detailed procedures and algorithms for analyzing and predicting the security performance of selected WLAN security features and configurations. For this to be achieved, the following needs to be done:

i. Discovery of security features and configurations on each conceptual architectural component.
ii. Analysis of security levels/attack susceptibilities of security features and configurations on each conceptual architectural component.
iii. Development of a value function that maps an attribute (security feature/configuration) to value.
iv. Development of combination function/algorithm to combine multiple values (results of value function) into a single value.

The works in this paper imply that identification of trusted computing base (TCB) components is fundamental in the design and implementation of any computing system's security. While TCB concept has typically been employed in the design of security kernel of operating systems, the concept can be applied in all computing systems including WLANs.

REFERENCES

1. Dokurer, S. (2006). Simulation of Black Hole Attack in Wireless Ad-Hoc Networks. Masters thesis .Atılım University.
2. 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 [Accessed 15 Jan, 2019].
3. Daniel, P. and Edward, G. (2010). Weaknesses and Strengths Analysis over Wireless Network Security Standards. International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering.[Online] Vol 4(12).Available at: https://waset.org/journal/Electrical/2010/12?new=1[Accessed 15 Jan.2019]
4. Yizhan, S. (2006). Complexity of System Configuration Management, PhD thesis, Tufts University.
5. IEEE 802.11. (1997) Number Part 11: Wireless LAN Moderate Access Control (MAC) and Physical Layer (PHY) Specifications: Specific Requirements, IEEE Std. 802.11.
6. 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.
7. Gast, M. (2005). 802.11 Wireless Networks: The Definitive Guide.2rd ed. O'Reilly Media, Inc.
8. Alikira, R. (2012).Evaluation of WLAN security and Performance. [Online] Munich: GRIN Verlag. Available at http://www.grin.com/en/e-book/205389 [Accessed 30 Dec.2018].

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
10. IEEE 802.11i. (2004). ANSI/IEEE 802.11w-2009-IEEE Standard for Information Technology - Telecommunication 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.
11. Sheila, F., Bernard, E., Les, O., Karen, S.(2007). Establishing Wireless Robust security Networks: A Guide to IEEE 802.11i, NIST.US.
12. Lampson, B., Abadi, M., Burrows, M., and Wobber, E. (1992).Authentication in Distributed Systems: Theory and Practice. ACM Transactions on Computer Systems. Vol.10 (4), pp.265-310.
13. Steven, B. (2015).The Birth and Death of the orange book. IEEE annals of the history of computing, Vol.37 (2) pp.19-31.
14. Rushby, J. (1981).Design and verification of secure systems,8th ACM Symposium on operating system principles, Pacific Grove California ,US. pp. 12-21.
15. Scott, A. (2011). Known Wireless Attacks, Loughborough University.
16. Ken, A., Dawson, R. and Engler. (2002). Using Programmer-Written Compiler Extensions to Catch Security Holes. In: Proceedings of IEEE Symposium on Security and Privacy.
17. Laurent, B. and Julien, T. (2007). Discovering and Exploiting 802.11 Wireless Driver Vulnerabilities. Journal in Computer Virology. [Online] Vol 4(1), pp.25-37, Available at: http://link.springer.com/article/10.1007%2Fs11416-007-0065-x#page-1
18. Andy, C., Junfeng, Y., Benjamin, C., Seth, H. and Dawson, R. (2001).An Empirical Study of Operating System Errors. In: Proceedings of Symposium on Operating Systems Principles, Montana: ACM.
19. Tal, G., Ben, P., Jim, C., Mendel, R. and Dan, T. (2003). A Virtual Machine-Based Platform for Trusted Computing. In: Proceedings of Symposium on Operating Systems Principles.
20. Jason, F., Damon, M., Vicenti, N., Jamie, V. and Douglas, S. (2006). Passive data link layer 802.11 wireless device driver fingerprinting. In: Proceedings of the 15th conference on USENIX Security Symposium [Online].Vol 15(12).Available at: https://www.usenix.org/legacy/event/sec06/tech/full_papers/franklin/franklin_html/
21. Eian, M. (2009).Fragility of the Robust Security Network 802.11 Denial of service. In: Applied Cryptography and Network Security: 7th International Conference. Paris: Springer, pp. 400-416.
22. Park, J. and Dicoi, D. (2003).WLAN security: Current and future. IEEE Internet computing, Vol 7(5,) pp. 60-65.
23. Rigney, C., Willens, S., Rubens, A. and Simpson. (2000). Remote Authentication Dial In User Service (RADIUS). RFC 2865, IETF Network Working Group.
24. Pat, R., Calhoun, John, L., Erik, G., Glen, Z. and Jarki, A. (2002). Diameter Base Protocol, IETF AAA Working Group.
25. Li-Chuan, G., Cheng, Z., Shao-Wen, S. and You-hua, Z. (2009).A new network access control Method Based on Diameter Protocol.WRI International Conference on Communications and Mobile Computing [Online] IEEE, Vol 1, pp.600-604. Available at: http://ieeexplore.ieee.org/document/4797323/authors
26. Charlie, O. and Benjamin. (2011).Vulnerabilities of LDAP as an authentication service. Journal of information security.[Online] Vol 2, pp.151-157.Available at: http://www.sciRP.org/journal/jis
27. Bellardo, J. and Savage, S. (2003).802.11 Denial of service attacks: Real vulnerabilities & Practical solutions. In: proceedings of USENIX Security Symposium, pp. 15-28.

