International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7017
Issue 01, Volume 6 (January 2019) www.ijiris.com

A MODEL BASED APPROACH FOR IMPLEMENTING WLAN SECURITY

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

Manuscript History
Number: **IJIRIS/RS/Vol.06/Issue01/JAIS10082**
DOI: 10.26562/IJIRAE.2019.JAIS10082
Received: 02, January 2019
Final Correction: 12, January 2019
Final Accepted: 21 January 2019
Published: **January 2019**
Citation: Mwathi (2019). A MODEL BASED APPROACH FOR IMPLEMENTING WLAN SECURITY . IJIRIS:: International Journal of Innovative Research in Information Security, Volume VI, 20-28. **doi://10.26562/IJIRIS.2019.JAIS10082**
Editor: Dr.A.Arul L.S, Chief Editor, IJIRIS, AM Publications, India
Copyright: **©2019 This is an open access article distributed under the terms of the Creative Commons Attribution License, Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited**

Abstract- This paper presents various security features and configurations commonly implemented in WLANs and their aggregated security levels and then proposes a model that enables implementation and evaluation of WLAN security.

Keywords- WLAN Security model; WLAN Security; WLAN attacks & Vulnerabilities; WLAN Security Features Selection; WLAN Security Measurement;

I. INTRODUCTION

In recent years, the proliferation of wireless local area network[WLAN] enabled laptop computers, smart phones and tablets has caused an increase in the range of places people perform computing. As a result, WLANs of various kinds have gained a lot of popularity. But with the added convenience of wireless access come new problems: Security. When transmissions are broadcast over radio waves, interception and masquerading becomes trivial to anyone with WLAN enabled device in the range. WLANs implement IEEE 802.11i and IEEE 802.11w standards whose focus is provision of appropriate integrity and confidentiality levels.

These standards provide a variety of options for various security features.This flexible nature of the provisions of these standards and supporting technologies create potential for selection of vulnerable cipher suite, authentication & access control, end-user and server system security features. This makes selection and configuration of the appropriate security features a challenge to many WLAN security implementers [1]. This issue is a major concern because several software attack tools targeting vulnerabilities in authentication methods, cipher suites and supporting technologies on client devices and server implementations continue to proliferate, effectively empowering attackers.

This research aims to make a contribution by addressing the issue of poor implementation of WLAN security through development of a model that enables design or selection of security features and their configuration for WLAN security.

© 2014- 19, IJIRIS- All Rights Reserved

II. RELATED WORK ON WLAN SECURITY IMPLEMENTATION APPROACHES

Several works propose the following variables for selection of appropriate cipher suite to support WLAN authentication and access control: core cryptographic algorithm, key sizes, per packet key, integrity mechanism, header protection, replay detection, authentication supported and mode of key distribution [2]. Other works focus on selection of extensible authentication protocol [EAP] method for securing WLANs. Some of the variables proposed to influence an implementer into selecting an EAP authentication mechanism in a WLAN include: mutual authentication, identity privacy, dictionary attack resistance, replay attack resistance, derivation of strong session keys, tested implementation, delegation, and fast reconnect.[3]

Mutual authentication requires that an EAP method should enable both client device and authentication server to authenticate each other**.** It has been shown that the absence of mutual authentication in WEP based authentication was responsible of many of its weaknesses [4]. Many network security administrators use their experience of past solutions and documentation to configure security of network equipment [5]. In this case, selection and configuration of security features is mainly guided by following a documented procedure or a wizard for installation which enables network administrators bypass the "hardness" of dependency analysis. 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 follow these instructions without analyzing the cumulative effect of the combination of cipher suite and authentication method selected on overall security [5]. Use of documentation and experience approaches alone is not sufficient because documentation is not always accurate due to errors in the software, human error, time and cost of developing detailed installation/configuration wizards by equipment manufacturers [5].Additionally, documentation does not address all possible platforms because WLANs may comprise equipment/components from various developers and vendors. Even where the equipment have been tested and verified fully by their developers for any platform, it is possible that they can fail to function as specified in a particular platform.Experience on the other hand may also not be always accurate and in a very dynamic environment, it is possible to misconfigure the system by simply relying on experience that may not apply to the system's current state.

III. METHODOLOGY

Descriptive 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 (nonintrusive) WLAN network search tools. This information was used to verify the questionnaire responses. The data collected led to the discovery of security features and configuration options which were aggregated as: cipher suite, authentication credentials, client driver, client utility, accespoint firmware, authentication and access control mechanism, user database and authentication server. The researcher evaluated the security levels of these security features/configuration options and used the results of evaluation to develop a model that maps these security features/configuration options to security strengths as well as an algorithm that combines and propagates the security strengths of the security features and configurations selected to generate the overall security strength.

IV.RESULTS

This section presents the security features and configurations options available to the security implementer and then proposes a model that maps these security features to security strengths as well as an algorithm that combines and propagates the security strengths of the security features and configurations selected to generate the overall security strength.

A. Model Operation Overview

The model has three steps that define its operation:

(i) Identification of security features and configuration options
(ii) Mapping security features/configurations options to security strengths.
(iii) Combining and propagating the security strengths of the security features and configurations selected to generate the overall security strength

Subsequent sub-sections detail the activities of each step.

© 2014- 19, IJIRIS- All Rights Reserved

B. Identification of Security Features and Configuration Options

This is the set of security features/configurations available to the security implementer for each of the eight key components namely: cipher suite, authentication credentials. Client utility, client driver, access point utility, authentication & access control mechanism, user database and authentication server. All these eight components have been considered equivalent in relative importance in relation to their influence on WLAN security. This means none of them can be considered superior to the other. However, their actual influence values/strength will be determined by the security features selected or configurations on each of the components.

C. Mapping Security Features/Configuration options to Security Strengths

The model maps the security features/configuration option selected to "Very Low", "Low", "Moderate" or "High" security strength based on already predetermined values. Each security feature/configuration is associated with certain characteristics which determine its security strength. The decision on which strength a security feature/configuration is mapped to is based on a value function as indicated in function table 1 to table 8.Looking at each function table, whenever security strength of a security feature/configuration is mapped to level low, moderate or high, it is denoted 1, 2 and 3 respectively.

Whenever security strength of a security feature/configuration is mapped to level very low, it is denoted as 0 which means that if this security feature/configuration is selected and implemented, the WLAN implementation is highly susceptible to attacks. This means that such security feature/configuration should not be implemented in a WLAN.

TABLE 1: VALUE FUNCTION TABLE FOR AUTHENTICATION CREDENTIALS

Security Strength [Weight of influence]	Description of Security Feature/ Configuration
High [3]	Both Client and Server Certificates
Moderate [2]	PAC, One time password OR Server Side certificate only(Tunneled)
Low [1]	Secret Key/password(Mutual or Unilateral)
Very Low [0]	SSID
Very Low [0]	MAC address
Very Low [0]	PIN

TABLE 2: VALUE FUNCTION TABLE FOR CIPHER SUITE

Security Strength [Weight of influence]	Description of the Security feature/Configuration
High [3]	CCMP (WPA2 +AES)
Moderate [2]	TKIP(WPA +AES)
Low [1]	TKIP(WPA +RC4)
Low [1]	TKIP(WPA2 +RC4)
Very Low [0]	WEP

TABLE 3: VALUE FUNCTION TABLE FOR WLAN CLIENT DRIVER

Security Strength Weight of influence	Description of Security Feature/ Configuration
High [3]	• Supports management frame protection (MFP/IEEE 802.11w) and validation. • Supports configurable active scanning approach.
Moderate [2]	• Supports management frame protection(MFP/IEEE 802.11w) and validation • Lacks Support for Configurable active scanning approach
Moderate [2]	• Lacks support for management frame protection (IEEE 802.11w) and validation • Supports IEEE 802.11i. • Supports configurable active scanning approach.
Low [1]	• Lacks support for management frame protection (MFP/IEEE 802.11w) and validation • Lacks support for Configurable active scanning approach. • Supports IEEE 802.11i.
Very Low [0]	Lacks support for IEEE 802.11i.

© 2014- 19, IJIRIS- All Rights Reserved

TABLE 4: VALUE FUNCTION TABLE FOR WLAN CLIENT UTILITY

Security Strength Weight of influence	Description of Security Feature/ Configuration
High [3]	• Configured to support both client and server side Certificate based mutual Authentication. • Supports Management frame protection. • Configured to enforce validation of server certificates and server name. • Configured not to allow Self signed certificates.
Moderate [2]	• Configured to support server side only Certificate based mutual Authentication. • Supports Management frame protection (IEEE 802.11w). • Configured to enforce validation of server certificates and server name. • Configured not to allow Self signed certificates.
Low [1]	• Configured to support Password, pre-shared key or MAC address based mutual Authentication mechanism. • Supports Management frame protection (IEEE 802.11w)
Low [1]	• Configured to support server side only or both client and server side Certificate based mutual Authentication • Lacks Support for Management frame protection (IEEE 802.11w) and validation. • Supports IEEE 802.11i.
Low [1]	• Configured to support Password, pre-shared key or MAC address based mutual Authentication mechanism. • Lacks Support for Management frame protection (IEEE 802.11w) and validation. • Supports IEEE 802.11i.
Very Low [0]	Lacks support for IEEE 802.11i.
Very Low [0]	Configured to support server side only or both client and server side certificate but Validation of server certificates and/or server name not enforced.
Very Low [0]	Configured to support server side only or both client and server side certificate but allows Self signed certificates.
Very Low [0]	Mutual authentication not supported.

TABLE 5: VALUE FUNCTION TABLE FOR ACCESS POINT UTILITY

Security Strength Weight of influence	Description of Security Feature/ Configuration
High [3]	• Firmware configured to support management frame protection (MFP/IEEE 802.11w) and validation and is set to required. • Firmware configured to Support only RSNA connections(RSNA enabled)
Moderate [2]	• Firmware configured to support optional management frame protection (MFP/IEEE 802.11w) and validation. • Firmware configured to Support only RSNA connections(RSNA enabled)
Low [1]	• Firmware does not support MFP/IEEE 802.11w and validation • Firmware configured to Support only RSNA connections(RSNA enabled)
Very Low [0]	Firmware not configured to Support only RSNA connections(Pre-RSNA enabled)

TABLE 6: VALUE FUNCTION TABLE FOR AUTHENTICATION AND ACCESS CONTROL MECHANISM

Security Strength Weight of influence	Description of Security Feature/ Configuration
High [3]	IEEE 802.1x With EAP method
High [3]	Captive portal and IEEE 802.1x With EAP Method
Moderate [2]	Captive Portal and Pre-shared Key
Low [1]	Captive Portal Only
Low [1]	Pre-shared Key Only
Very Low [0]	MAC address filtering

© 2014- 19, IJIRIS- All Rights Reserved

Very Low [0]	Open SSID
Very Low [0]	PIN based authentication(WPS)
Very Low [0]	Button press based authentication(WPS)

D. Combining and Propagating the Security levels of the Security Features/Configurations in the Model

The model determines the overall security level of an implementation by aggregating security levels of individual components based on security features and configurations set in them. The components whose security levels are aggregated are: client utility, client driver, access point utility, authentication server, authentication & access control mechanism, user database, cipher suite and authentication credentials. Fig. 1 shows the structure of hierarchy and direction of propagation of security levels. The aggregation of security levels is hierarchical (parent-child structure) and is done bottom up.

.

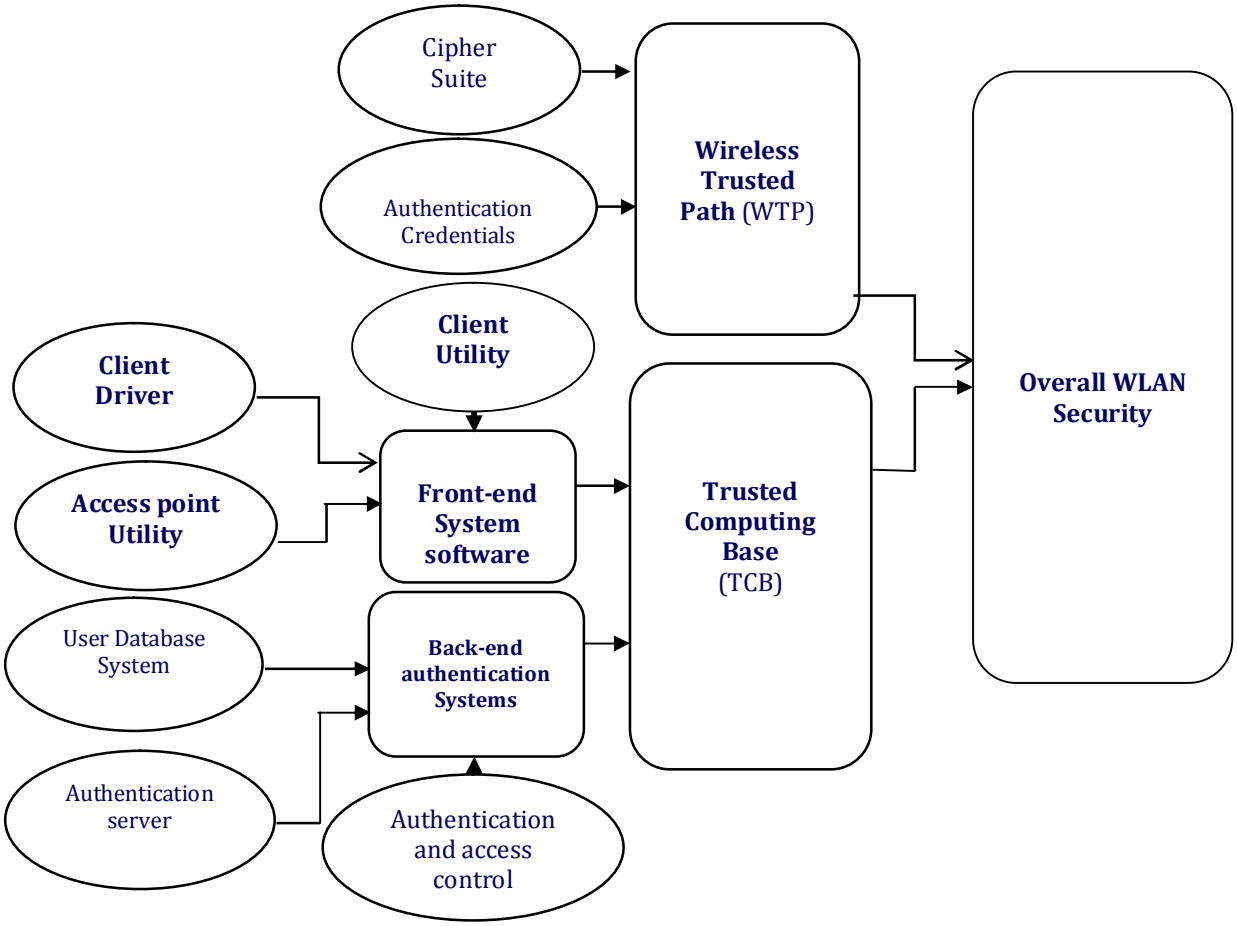

Fig 1: Structure of Hierarchy and Direction of Propagation of Security levels

TABLE 7: VALUE FUNCTION TABLE FOR AUTHENTICATION SERVER

Security Strength Weight of influence	Description of Security Feature/ Configuration
High [3]	DIAMETER. Configured to Support mutual authentication
Moderate [2]	RADIUS. Configured to Support mutual authentication
Low [1]	DIAMETER. Not Configured to Support mutual authentication
Low [1]	RADIUS. Not Configured to Support mutual authentication
Low [1]	KERBEROS
Very Low [0]	None/Independent on each Access point

© 2014- 19, IJIRIS- All Rights Reserved

TABLE 8: VALUE FUNCTION TABLE FOR USER DATABASE SYSTEM

Security Strength Weight of influence	Description of Security Feature/Configuration
High [3]	Distributed Database Servers with an Intrusion Detection System(IDS)
Moderate [2]	Distributed Database Servers without an Intrusion Detection System(IDS)
Moderate [2]	Centralized Database Server with an Intrusion Detection System(IDS)
Low [1]	Centralized Database Server without an Intrusion Detection System(IDS)
Very Low [0]	None/Independent on each Access point

The combination and propagation algorithm used to aggregate security levels is illustrated below:

(a) Starting with terminal/leaf nodes, every subtree has a parent node **R** and a set of child nodes **C**. The child nodes may have a negative or positive type of influence on **R.** A positive influence of child $\mathbf{C_i}$ on **R** means that when security level of $\mathbf{C_i}$ is high, that of **R** is influenced to move upwards too. On the other hand, a negative influence of child $\mathbf{C_i}$ on **R** means that when security level of $\mathbf{C_i}$ is high, that of **R** is influenced to move downwards.

(b) If a parent node **R** has at least one child with **very low** security level, the model gives a notification that the security feature or configuration is not recommended. This is because this feature renders the security of the entire WLAN very weak.

(c) If a parent node **R** has ***k*** child nodes with combination of positive and negative influences and of strength S_i (High, Moderate, and Low) and values of security level for all child nodes are known, the value of the parent node, V_R is computed based on the following weighted average.

$$V_R = \frac{\sum_{i=1}^{k} (S_i * V_i)}{\sum_{i=1}^{k} (S_i)}$$

Where: S_i refers to the strength of the security influence of a child C_i on parent **R** which is equal to 1, 2, or 3 if the influence of the child is low, moderate, and high respectively. V_i refers to the value of child $\mathbf{C_i}$ and is dependent on S_i and type of influence of child C_i on parent node **R**. If the child node C_i has a positive influence on Parent node **R** and the strength of influence (S_i) of node C_i is low, moderate, or high then V_i is equal to 1, 2, and 3 respectively. On the other hand, if the child node C_i has a negative influence on parent node **R** and strength of influence (S_i) of node C_i is low, moderate or high then V_i is equal to 3, 2 or 1 respectively

(d) Once a value V_R is determined, thresholds have been set to decide the values of V_R as follows:

(i) If $1 <= V_R < 1.5$, then the value of R is **low**
(ii) If $1.5 <= V_R <= 2.5$, then the value of R is **moderate**
(iii) If $2.5 < V_R <= 3$, then the value of R is **High.**

(e)The process is repeated recursively up the hierarchy until a value for the root node is established.

Based on the algorithm described above the security levels of the eight model components are propagated as follows:

(i) Security level of **client utility**, **client driver** and **access point utility** are aggregated to derive a composite security levels for front-end system software subtree.
(ii) Security levels of **authentication server**, **authentication & access control mechanism** and **user database** are aggregated to derive a composite security levels for back-end authentication systems subtree.
(iii) The derived security levels for **front-end system software** is aggregated with that of **back-end authentication systems** to derive a composite security levels for trusted computing base (TCB).
(iv) Security levels of **cipher suite** and **authentication credentials** are aggregated to derive a composite security levels for wireless path subtree.
(v) Finally, the security levels of **trusted computing base (TCB)** and that of **wireless path** are aggregated to form an **overall** security levels of the implementation.

The model therefore provides a what-if simulation of the security level expected from a combination of the influences of the selected security features and/or configurations.

© 2014- 19, IJIRIS- All Rights Reserved

E. Theoretical Analysis of the Model Algorithm Using Degenerate and Trace Tests

Degenerate and traces validation was used to perform theoretical validation of the model. Degenerate validation involved analysis of input values to test the corresponding changes in the internal components e.g. does the security level/strength go up when more secure configurations and security features are selected and vice versa? Does the security level/strength go down when highly vulnerable configurations and security features are selected and vice versa?

Validation using traces on the other hand was done to determine whether the mathematical logic of the technique for propagation of values in the model maintains necessary accuracy and consistency. To achieve this, the researcher tracked entities' strength and type of security influence through each sub-model and the overall model and analyzed the results.

Table 9 shows results for a one component sub-model when type of influence is positive and a similar scenario when type of influence is negative**.** The following can be deduced from the table.

i. When the security strength of the child component is low, moderate or high, the security strength of the root/parent component is low, medium and high respectively when the type of influence is positive (+ve).
ii. When the security strength of the child component is low, medium or high, the security strength of the root/parent component is high, medium and low respectively when the type of influence is negative (-ve).

TABLE 9: ONE COMPONENT SUB-MODEL FOR BOTH POSITIVE AND NEGATIVE INFLUENCE

Strength of component	Strength of sub-model Root(P) When Relationship is +ve	Strength of sub-model Root(P) When Relationship is -ve
Low [1]	Low [1]	High [3]
Moderate [2]	Moderate [2]	Moderate [2]
High [3]	High [3]	Low [1]

Table 10 shows a summary of results for a two component sub-model when type of influence is positive and a similar scenario when type of influence is negative**.**

The following can be deduced from the table.

i. When all the two child components have low, moderate or high security strength, the root/overall security strength is also low, moderate and high respectively.
ii. Where one of the components has high security strength, and the other low security strength, the root/overall security strength is moderate.
iii. When the relationship changes to type negative, the results are inverted.

TABLE 10: TWO COMPONENT SUB-MODEL FOR BOTH POSITIVE AND NEGATIVE INFLUENCE.

Strength of component 1(S1)	Strength of component 2(S2)	Strength of sub-model Root(P) when Relationship type +ve	Strength of Sub-model Root(P) when Relationship type -ve
Low [1]	Low [1]	Low [1.00]	High [3.00]
Low [1]	Moderate[2]	Moderate [1.67]	Moderate [2.33]
Low [1]	High [3]	Moderate [2.50]	Moderate [1.50]
Moderate[2]	Low [1]	Moderate [1.67]	Moderate [2.33]
Moderate[2]	Moderate[2]	Moderate [2.00]	Moderate [2.00]
Moderate[2]	High [3]	High [2.60]	Low [1.40]
High [3]	Low [1]	Moderate [2.50]	Moderate [1.50]
High [3]	Moderate[2]	High [2.60]	Low [1.40]
High [3]	High [3]	High [3.00]	Low [1.00]

Table11 shows a summary of results for a three component sub-model when type of influence is positive and a similar scenario when type of influence is negative**.**

The following can be deduced from the table.

© 2014- 19, IJIRIS- All Rights Reserved

i. When all the three components have low, moderate or high security strength, the root/overall security strength is low, moderate and high respectively.
ii. For any given set of component input values, the results of situations where the relationship is of type positive(+ve) are the inversion of the results under the same component values if relationship is of type negative(-ve) as expected.

TABLE 11: THREE COMPONENT SUB-MODEL FOR BOTH POSITIVE AND NEGATIVE INFLUENCE

Strength of Component 1 (S1)	Strength of Component 2(S2)	Strength of Component 3(S3)	Strength of sub model Root (P) when Relationship type +ve	Strength of sub model Root (P) when Relationship type –ve
Low [1]	Low [1]	Low [1]	Low [1.00]	High [3.00]
Low [1]	Low [1]	Moderate[2]	Moderate [1.50]	Moderate [2.50]
Low [1]	Low [1]	High [3]	Moderate [2.20]	Moderate [1.80]
Low [1]	Moderate[2]	Low [1]	Moderate [1.50]	Moderate [2.50]
Low [1]	Moderate[2]	Moderate[2]	Moderate [1.80]	Moderate [2.20]
Low [1]	Moderate[2]	High [3]	Moderate [2.33]	Moderate [1.67]
Low [1]	High [3]	Low [1]	Moderate [2.20]	Moderate [1.80]
Low [1]	High [3]	Moderate[2]	Moderate [2.33]	Moderate [1.67]
Low [1]	High [3]	High [3]	High [2.71]	Low [1.29]
Moderate [2]	Low [1]	Low [1]	Moderate [1.50]	Moderate [2.50]
Moderate [2]	Low [1]	Moderate[2]	Moderate [1.80]	Moderate [2.20]
Moderate [2]	Low [1]	High [3]	Moderate [2.33]	Moderate [1.67]
Moderate [2]	Moderate [2]	Low [1]	Moderate [1.80]	Moderate [2.20]
Moderate [2]	Moderate [2]	Moderate[2]	Moderate [2.00]	Moderate [2.00]
Moderate [2]	Moderate [2]	High [3]	Moderate [2.43]	Moderate [1.57]
Moderate [2]	High [3]	Low [1]	Moderate [2.33]	Moderate [1.67]
Moderate [2]	High [3]	Moderate[2]	Moderate [2.43]	Moderate [1.57]
Moderate [2]	High [3]	High [3]	High [2.75]	Low [1.25]
High [3]	Low [1]	Low [1]	Moderate [2.20]	Moderate [1.80]
High [3]	Low [1]	Moderate [2]	Moderate [2.33]	Moderate [1.67]
High [3]	Low [1]	High [3]	High [2.71]	Low [1.29]
High [3]	Moderate[2]	Low [1]	Moderate [2.33]	Moderate [1.67]
High [3]	Moderate[2]	Moderate [2]	Moderate [2.43]	Moderate [1.57]
High [3]	Moderate[2]	High [3]	High [2.75]	Low [1.25]
High [3]	High [3]	Low [1]	High [2.71]	Low [1.29]
High [3]	High [3]	Moderate[2]	High [2.75]	Low [1.25]
High [3]	High [3]	High [3]	High [3.00]	Low [1.00]

It was also observed that when all the eight components have low, moderate or high security strengths, the overall security strength is low, moderate and high respectively. These observations indicate that the logic of the algorithm for propagation of component values maintains accuracy and consistency as required and that the model results are consistent with the design principles.

V. CONCLUSION

This paper has brought into perspective various security features and configurations commonly implemented in WLANs and their aggregated security levels. It has also proposed a model that enables an implementer to establish the level of security provided by the security features and configurations implemented in a WLAN. The results from the theoretical analysis of the model indicate that the logic of the algorithm for propagation of component values maintains accuracy and consistency as required and that the model results are consistent with the design principles. This model can be used for WLAN security design, implementation and analysis.

© 2014- 19, IJIRIS- All Rights Reserved

Particularly, when implemented in form of a software tool that mines data directly from devices, network administrators can use it to establish highly vulnerable security features and configurations in an implementation, visualize the security implications of selecting certain security features and configurations. Network administrators can also use it as an audit tool for WLAN security and then recommend an appropriate security for an organization's security. Researchers in the area of WLAN security can also use it as a data collection tool.

REFERENCES

1. 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.
2. Sheila, F., Bernard, E., Les, O., Karen, S.(2007). Establishing Wireless Robust security Networks: A Guide to IEEE 802.11i, NIST.US.
3. Kwang-Hyun, B., Sean, W. and David, K. (2004). A Survey of WPA and 802.11i RSN Authentication Protocols. Dartmouth College: Computer Science Technial Report TR2004-524. Available at: www.cs.dartmouth.edu/~dfk/papers/baek-survey-tr.pdf
4. 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.
5. Yizhan, S. (2006). Complexity of System Configuration Management, PhD thesis, Tufts University.

© 2014- 19, IJIRIS- All Rights Reserved