Enhancement WPA2 protocol with WTLS to certify security in large scale organizations inner access layer Wi-Fi media associated devices

V.A.A.S.Perera, E.A.M.K.B.Ekanayake, S.S. Shurane, P.A.Isuru Udayanga, J.P.Maharajage, R.M.C.Bandara, Dhishan Dhammearatchi

Sri Lanka Institute of Information Technology Computing (Pvt) Ltd

Abstract- Now a days Wireless networks are very famous the reason is user friendliness of Wi-Fi, within 20 meters any one can connect any Wi-Fi device to network without any wire. Wi-Fi use 2.4gigahertz UHF and 5gighertz range. Mainly devices connect through wireless access points. This is the main entrance of network attackers to large scale organizations. Network security is very important in large scale organizations. Wireless security is help to prevent unauthorized access to the network via wireless access points. Increment of thousands of Wi-Fi users, need to improve wireless security. This Wi-Fi network attacks always focus on large organizations, now organizations consider about their wireless network security. The research explain how increase Wi-Fi security in large scale company networks using WPA2, WTLS, AES Encryption, IP-VPN and HTTP Proxy Servers. Research paper explain things that need to include in new protocol and discussion about the most efficient and fast way to transfer data through the wireless network in a large scale organization has been discussed.

Index Terms- wireless, network, security, organization

I. Introduction

Wireless technology is the best dynamic, high mobility GO-TO connectivity in the rapidly changing Technological world. Increasing bandwidth, freedom and flexibility of the communication method is making it the best communication infrastructure by choice. The wireless technology provides the capability to conduct commerce at any place and with any individual, where communication mechanism is established. As the popularity of the connectivity medium it has been adopted to small, medium and large sized organization. IN Network Engineers perspective regardless of the organization size, Figure 1 shows the diagrammatic view of pyramid architecture of the network. The network is falling under to a pyramid top to bottom (Core layer, Distribution layer and Access Layer), which is further illustrated in the **Appendix [A]**.

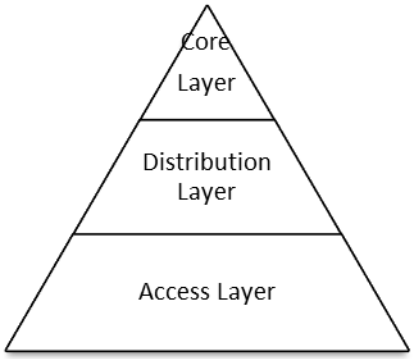

Figure 1: Pyramid architecture of a network

The client's connectivity to the network is done through the access layer and Wireless connectivity devices also falls under to this category. Large scale organizations secure that the pyramid architecture is properly established and always maintain the architecture because of the complexity will increase of the network. The core layers are tightly coupled with security countermeasures such as perimeter firewalls, intruder prevention systems which is further described in **Appendix [B]**. Even though the counter measures can avoid attackers who are trying to penetrate the large scale organization structure from other internet connectivity methods such as wired, in Wi-Fi connectivity clients can be a threat as the clients are dynamically changing with increasing number of established connections in the networks' inner access layer devices are not which is static. Which make this connectivity method more vulnerable that is a main drawback to this high scale organization and considering about networking whole as a theory. WPA/WPA2 are the most commonly used Wi-Fi Connection protocols and most of the industrial routers which supports Wi-Fi, follow these connection establishment protocols to establish a connection. Popularity of the connection protocols have made attackers to eavesdrop to these networks and now it has been proven that these protocols are not 100% bullet proof. How to secure a large scale organization from attackers? How to make a secured connection to a user with proper security counter measures by Through this research paper authors consider existing WPA or WPA2 connections are not further reliable connection protocols and will suffer exploitation. Therefore, authors suggest an updated WPA2 protocol a better replacement in encryption method and adding a Transport Layer security to the Protocol, and a networking concepts all together to make sure the security of the High scale

organization is protected in a user's and organization's perspectives.

II. Network Security Encryption Mechanism.

What is encryption?

Encryption is a mechanism that encode message or information in a way that unauthorized parties can't intercept. Encryption does not of itself prevent interception. Its rejects the message content to the interceptor. In encryption process intended data packet to communicate is referred as plaintext. It use encrypting algorithm for encryption. That algorithm generates cypher text could read by decrypting the message. An encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. Only the authorized receivers can decrypt the message with the key provided by the originator, but not to unauthorized interceptors.

Computer network encryption.

Computer network encryption could be known as the process of encrypting or encoding packed transmitted or communicated over a computer network. The primary purpose of network encryption is to protect the secrecy of digital data stored on computer systems or transmitted through the Internet or other computer networks.

It is a broad process that includes various tools and techniques to ensure that the messages are unreadable when in transition between two or more network nodes.

Network transfer layers are in OSI model layer 3 and 4. These two layers responsible for connectivity and routing between sender and receiver. Using the existing network services and security application soft wares, network encryption is invisible to the end user and operates without depending on any other encryption processes used. Data is encrypted only while in transmission as plaintext on the originating and receiving hosts. Plaintext is in cryptography is ordinary readable text before being encrypted in to or cypher text or after being encrypted. Network encryption is implemented based on a set of open standards that given by IETF. Network encryption products and services are offered by companies such as Cisco, Motorola, and Oracle.

Following are the vital elements that provided by the modern encryption algorithms to security assurance of IT systems and communication.

- **Authentication**: the origin of a message can be verified.
- **Integrity**: proof of the message contents have not been changed since it was sent.
- **Non-repudiation**: the sender of a message cannot deny sending the message.

Plaintext is encrypted using an encryption algorithm and an encryption key. Today's encryption algorithms are divided into two categories.

1. Symmetric.
2. Asymmetric.

Symmetric-key ciphers use same key to encrypt and decrypt a message or file. The most widely used symmetric-key cipher is Advanced Encryption Standard (AES). This is mainly created for the government classified information. Symmetric-key is much faster than asymmetric encryption. In this algorithm sender must send back the key used to encrypt the data with the receiver before he or she can decrypt it. According to this requirement to securely distribute large number of data needs large number of keys. That means most cryptographic processes load happen in symmetric algorithm.

Asymmetric cryptography (public-key cryptography), This uses two different but mathematically linked keys. One is public and other is private. The public key can be shared with everyone. RSA is the most widely used asymmetric algorithm. The reason is in RSA both the both keys can encrypt a message. The opposite key that used to encrypt a message is used to decrypt it. Confidentiality, integrity, authenticity and non-reputability of electronic communications assures by this method.

WEP and WPA encryption.

WEP (Wireless Encryption Protocol) and WPA (Wireless Protected Access) are the encryption protocols that used for wireless networks. WEP is much older and much less secure than WPA. Therefore WPA is relatively easy to crack. But WEP is the most commonly used wireless security algorithm in the world. The keys used by WEP is implemented correspondingly are 64-bit, 128-bit, and 256-bit. The Wi-Fi Alliance officially retired WEP in 2004.

WPA is the direct replacement for the WEP. Same wireless network is possible to run only one protocol. These two protocols cannot run on same network same time. Same many protocol versions can run. There are wireless routers that supports the hybrid WPA with WPA2. The keys used by WPA and WPA2 change dynamically. In order to that it is impossible to intercept. WPA (IEEE 802.11i standard) consists with message integrity checks a technique that can determine if the intruder captured or altered the packets passed between the access point and client. TKIP (Temporal Key Integrity Protocol) employs key for per packet system that is more secure key system than WEP. In 2006 WPA outdated by WPA2. In WPA2 came up with compulsory use of AES (Advance Encryption Standards) algorithms and the introduction of CCMP. CCMP mechanism came as a replacement for TKIP. Security vulnerability in WPA2 is limited than WPA. WPA2 security vulnerabilities are limited among almost business level networks. Regarding the home networks it's more than secure to implement. But intrude through Wireless Protected Setup (WPS) is possible.

Background and Related Works

With the day by day expansion of technology and the economy strength of many countries, so many huge firms created in all over the world. As well as in past decade, number of users in internet had been increased rapidly. Big organizations communicate and exchange their information and personal detail with other related firms throughout the world by using internet. For this they create intranet among them. When doing this, the biggest problem those firms faced is securing their network from intruders and hackers. As an answer for that question plenty of intruder prevention systems and methods had been introduced.

Some of those are WPA, WPA2 as an encryption methods and key exchange methods. But these methods or system couldn't prevent each and every cyber-attacks on the internet.

This research paper explain WPA2 problems, versions and enhancements that have done solve the WPA major weakness. Also WEP, WPA as all wireless security protocols. Today most of hackers know how to go through those technology. Disadvantages in this paper it is only concern about WAP and WPA2. In New research, it concern about best way to protect Wi-Fi network using technologies like Digital Signature, Encryption, Key exchange, LAN Security as well as WEP, WAP, WPA2 [1].

This research is very close to new research, this is a military grade research this PKI system is invented to military, security of the systems and the networks that they connect to has very important. In this System use data encryption, and digital signature as well as the WPA and WPA2.this system is very satisfied system but disadvantage in here is it doesn't use WPE, LAN security methods and special case is this is not a home network product this is a large scale government product [2].

Security Improvement of WPA 2: Wi-Fi Protected Access 2, research group has discussed about WPA and WPA2 (Wi-Fi Protected Access) protocols that created to secure wireless networks. Wired Equivalent Privacy (WEP) and many sophisticated authentication and encryption techniques have been discussed in this paper. This paper present benefits of WPA2, its vulnerability & weakness and also present solutions that will improve Wi-Fi Protected Access 2 (WPA2) protocol. Also project group has talked about Hash function, DH algorithms and they have explained how those going to work on a Wi-Fi network [3].

Exploring the Weak Links of Internet Security: A Study of Wi-Fi Security in Hong Kong, research group investigates Wi-Fi usage, Wi-Fi security and the knowledge of it in Hong Kong. Research group has discussed about Internet security Internet access Wi-Fi security and so on. This study found that many home users of Wi-Fi in Hong Kong are oblivious of the importance of Wi-Fi security and there is a significant gender difference in Wi-Fi security perceptions and knowledge among Wi-Fi users in Hong Kong. They have further discussed about Wi-Fi encryption methods and Wi-Fi decryption methods [4].

Issues in Wi-Fi Networks research group has discussed about the mobile application security, Wi-Fi technology and Wi-Fi security protocols such as IEEE 802.11 and its WEP security algorithms. In this project they have focused on security architectures and algorithms such as Encryption and decryption methods. Wi-Fi Authentication Mechanisms, WEP Encryption/Decryption Issues, WEP Authentication are further discussed in this research paper [5].

Wi-Fi security research group has discussed about the security of Wi-Fi networks and Wi-Fi security protocols. As a major security standard IEEE 802.11 and its WEP protocol has deeply discussed through this research paper. Group also discussed about the Protocols such as WPA, WPA2 (Wi-Fi protected access) protocols. Also Encryption methods and decryption methods has been discussed in this research paper [6].

Solution

Wi-Fi Authentication mechanism for large scale organizations have been the main concern of this research paper and the problem have been divided to main areas which security and integrity is highly concerned. Existing WPA2 protocol which is further described in **Appendix [C]** have been updated in order to make a secure connection protocol.

Conceptualized WPA2 Methodology

WPA2 protocols encryption methods have been highly criticized because of the penetrable capability. And research authors have come up with a concept to increase the encryption capabilities and adding highly impenetrable Encryption method such as AES encryption and adopt WTLS Transport layer security to existing WPA2 protocol to make a secure connection protocol.

AES Encryption

AES encryption consist of three unique block ciphers. Which are AES-128, AES-192 and AES-256.which the key length to 128 to 256 is increasing and the bigger the key value the best the encryption will be. As it is a symmetric key cipher which both Sender and the receiver both the parties should know the same key to encrypt as well as to decrypt. As the conceptualized encryption method that will adopt to updated WPA2 protocol method will be using 256-bit key which is the maximum key length which AES supports, it's also proven that it is ideal for software applications and hardware that require either low-latency or higher throughput, it is also inherited in many protocols such as SSL/TLS. The research authors suggest an Encryption of AES-256-bit length key Encryption to WPA2 protocol. Which will secure highly in key exchange and in encryption module in secured connection protocol.

WTLS Protocol

WTLS protocol is developed to report problematic concerns in wireless mobile network devices.it is also similar to SSL (secure socket Layer). This protocol has been used in commerce applications in order to provide authentication, integrity and privacy protection which research authors try to adopt to large scale organizations. Wireless oriented Mobile networks which connects through Wi-Fi have a huge drawback that these connections don't provide client to server secured connection and through WTLS optimized dynamic key refreshing and WPA2 updated AES-256-bit key encryption it can be routinely updated during this connection. Which will make this combination impossible to penetrate.

HTTP Proxy Servers

Proxy servers to maintain data traffic between the clients and servers is the next security countermeasure research authors are suggesting to have. This proxy server configuration is done by the ISP (Internet service provider) it will be a dedicated software system which will be running on ISP server to manage large scale organizations data traffic. By using ISP Proxy Server, the users who connect to the network have to undergo another authentication in order to do data transmission using HTTP or HTTPS. Which this countermeasure falls under to HTTP Proxy to make attackers even harder to infiltrate the organizations network.

IP-VPN Protection to the generated traffic

After suggested safeguarded connection establishment the research group advocates to use an IP-VPN. IP-VPN (Internet protocol Virtual Private Network) provides secure communication, increased productivity and most important advantage Tailored to individuals. the research authors are providing the solution to large scale organizations and the authors are suggesting the traffic that organization generates will undergo with the IP-VPN tunnel that organization have to implement for their network. VPN separates organizations data from other traffic over internet which makes outer attackers to really hard to eavesdrop to these data because this data is separated from the outer traffic and which is unique to the organization. VPN tunneling uses three protocols.

1. Carrier protocol - (protocol used by network by the information is travelling over)
2. Encapsulating protocol- (SSL protocol/ IPsec protocol) Encrypting each IP packet of a communication session.
3. Passenger protocol- (IPX protocol) protocol used by the networks that are connected by the tunnel

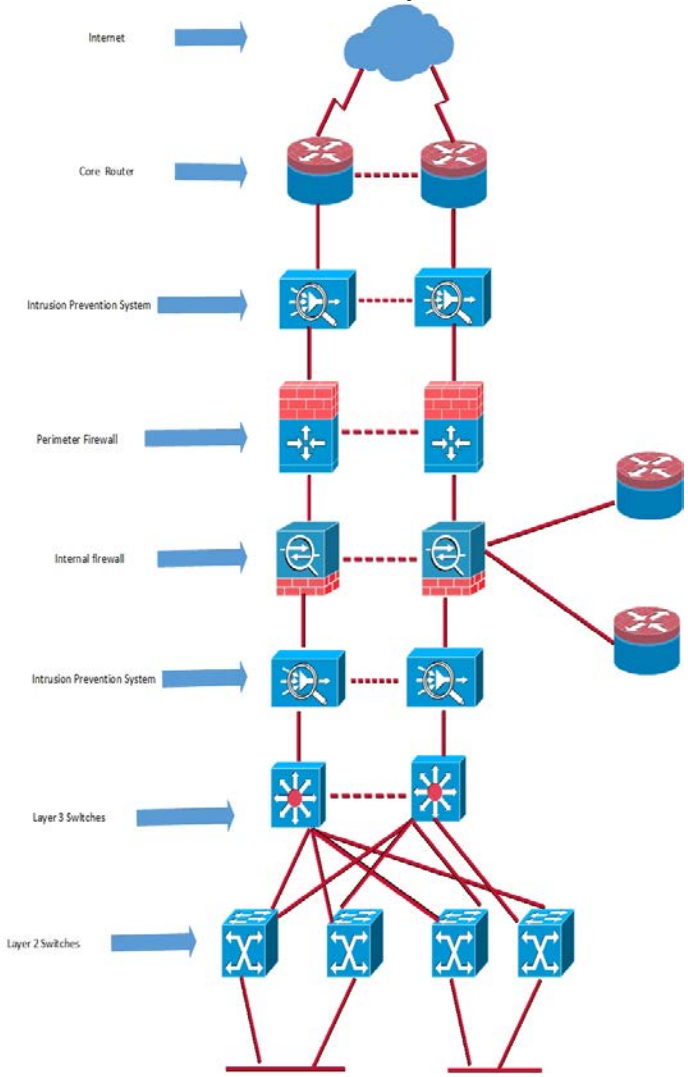

Figure 2: Inside Body of a properly secured High scale organization

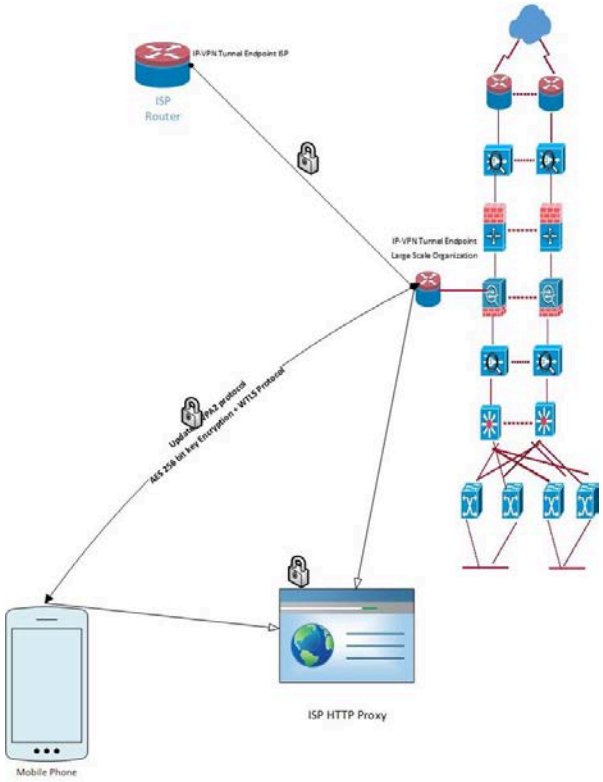

Figure 3: Conceptualized Solution adopted demonstration appearance

Figure 3 illustrates author's suggested solution for the large scale organizations access layer Wi-Fi connection medium security concept Conceptualized WPA2 protocol with AES-256 bit key length encryption and WTLS protocol HTTP Proxy server implementation connecting through high scale organization implemented IP-VPN for high secured connection to stop attackers in eavesdrop.

III. Conclusion

Fast growing of the Information technology field is effects human life style. This increment generate many issues in society specially cyber-crimes. Large scale Organizations are use Wi-Fi Technology. Using this wireless network intruders can access to this large scale organization. This research paper describe about the security in Wi-Fi technology and new technology developed using current technologies. Research paper provide one compact solution for wireless networks in large scale organizations. Solution consider about the all paths that need security in wireless networks and how can give service without any interruption or delay.

IV. Future Work

The projected solution to large scale organizations to secure access layer Wi-Fi connected devices are communicating through the organization IP-VPN and for the research future work the research authors are trying to address the solution in a

manner where the devices which is establishing the connection create a unique VPN to data transactions by client to server end points. HTTP authentication methods and adopting low performance required, high secured, flexible encryption protocols to HTTP authentication are the fields that research authors are trying to discover under future work to make a more secured connection.

ACKNOWLEDGEMENT

It is with excessive will that research team direct deep sense of appreciative and profound feeling of admiration to our Lecturer in charge of Computer Network Designing and Implementation Module and Research supervisor Mr. Dhishan Dhammearatchi for supervisory and instructing through the entire Research project. Without his guidance to the field would have not been potential to be successful in this research. We would like to thank to the members in Sri Lanka Institute of Information Technology for providing adequate resources.

REFERENCES

[1] A. H. Lashkari, M. M. S. Danesh, and B. Samadi, "A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)," IEEE, (2011),[Online:2016-02-09]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5234856&queryText=WPA%20WPA2%20WEP%20Protocols&newsearch=true.

[2] C. K. Williams, "Securing wireless local area networks using smart-card-based digital certificates from the DoD public key infrastructure," IEEE,(2013)[Online:2016-02-09]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4455006&queryText=Network%20Communication%20Protocols%20Wifi%20Security&newsearch=true.

[3] A.K.M. Nazmus Sakib, Fariha Tasmin Jaigirdar, Muntasim Munim, Armin Akter, (2011), "Security Improvement of WPA 2 (Wi-Fi Protected Access 2)", International Journal of Engineering Science and Technology (IJEST), Volume 3, Issue1 (2011) [Online: 2016-02-09], https://www.researchgate.net/profile/Fariha_Jaigirdar/publication/50392216_Security_Improvement_of_WPA_2_Wi-Fi_Protected_Access_2/links/53f645290cf2fceacc712504.pdf

[4] Ken Kin-Kiu Fong1, Stanley Kam Sing Wong, "Exploring the Weak Links of Internet Security: A Study of Wi-Fi Security in Hong Kong" Network and Communication Technologies, Volume 2, Issue 2, (2013), [Online: 2016-02-09], http://search.proquest.com/openview/7a1805fddadb37ceaee09a232bf0ee42/1?pq-origsite=gscholar

[5] Nicolae TOMAI, Cristian TOMA "ISSUES IN WI-FI NETWORKS", "Journal of Mobile, Embedded and Distributed Systems", Volume. I, Issue 1, (2009), [Online: 2016-02-10], http://jmeds.eu/index.php/jmeds/article/view/Issues-in-WiFi-Networks

[6] M. M. E. Adam and A. G. Elsid Abdallah, "WIFI SECURITY", Volume 2 Issue 2 (2015), [Online2016-02-09].http://www.sustech.edu/staff_publications/20150412092456586.pdf.

AUTHORS

First Author-V.A.A.S.Perera- Sri Lanka Institute of Information Technology Computing (Pvt) Ltd-Email-avishkaperera6@gmail.com
Second Author-E.A.M.K.B.Ekanayake- Sri Lanka Institute of Information Technology Computing (Pvt) Ltd-Email-kanishka.e.bandara@gmail.com
Third Author-S.S. Shurane-s Sri Lanka Institute of Information Technology Computing (Pvt) Ltd-Email-huranesajith@gmail.com
Fourth Author- P.A.Isuru Udayanga- Sri Lanka Institute of Information Technology Computing (Pvt) Ltd-Email-isuru.udayangasliit@gmail.com
Fifth Author- J.P.Maharajage- Sri Lanka Institute of Information Technology Computing (Pvt) Ltd –Email-mjaliya.jay@gmail.com
Sixth Author - R.M.C.Bandara- Sri Lanka Institute of Information Technology Computing (Pvt) Ltd –Email-chamikarabr2014@gmail.com
Seventh Author - Dhishan Dhammearatchi- Sri Lanka Institute of Information Technology Computing (Pvt) Ltd-Lecturer/Network Engineer with 08 years of hand on experience who worked for Millennium Information Technologies, a subsidiary of London Stock exchange as well as a lecturer in SLIIT Computing (Pvt) Ltd. Bachelors and a master degree with a number of professional examinations.(MIEE). Email-dhishan.d@sliit.lk

Appendix

Appendix [A]

Core layer

There are many distribution –layer devices in different areas of network, moving packets between those devices need high-redundant forwarding service core layer provide this service. Most powerful devices are core switches and routers mange to create highest speed connections.

Distribution layer

Purpose of the distribution layer is managing Routing, Filtering and QoS policies. Managing individual WAN branch-office connections also a responsibility of distribution layer. Some call this layer as work group layer.

Access Layer

Connecting client nodes is the main purpose as well as switching platforms and providing or not providing layer 3 switching. In here servers and End-stations connect with enterprise. Connecting with user is the reason that layer got name Desktop layer.

Appendix [B]

Perimeter firewalls

Firewall installed in middle of private and public networks (internet) call perimeter firewalls .those firewalls are the traffic controller between these two networks.

Intrusion prevention systems

Intrusion prevention systems use for monitor system activities for identify malicious activities in networks. In the Intruder prevention systems are doing three task.

- Malicious activity identification

- Log activity information

Block or Stop and report.

WPA2

WPA2 is an upgraded version of WPA. WPA2 is a security protocol developed by the WIFI Alliance to make secure wireless connections and it also a security certification programme.This protocol implements with the IEEE 802.11i standard and also

Appendix [C]

Temporal Key Integrity Protocol (TKIP). WPA2 supports for CCMP, an AES-based encryption modes with very strong security. WPA2 certification is monetary for all new devices which is built after 2006 with the WIFI trademark