Wi-Fi Password Two Factor Authentication for Home users (W2FA)

W.M.G. Kanishka, R. Suresh, M.F.A.E. De Silva, Thennakoon T.B.S.P, Amarasinghe G.C.J, D.B.D.R.B Ehelepola, Dhishan Dhammearatchi

Sri Lanka Institute of Information Technology Computing (PVT) Ltd.

Abstract- In the past decades Wireless Fidelity, wireless internet(Wi-Fi) networks have enhanced its features and got closer to the home users. Back in the day home users used wired internet connections in their homes. Due to the technical revolution and the vast use of mobile devices it became a must to have a Wi-Fi network in a regular home. There is a down side in every technology, the major down side in Wi-Fi is the integrity of the network password. This research paper is focuses on “How to improve the integrity of the Wi-Fi network password”. There are various security mechanisms currently used to protect the integrity of the Wi-Fi passphrase from intruders, such as Wireless Equivalent Privacy(WEP)/ Wi-Fi Protected Access (WPA)/ Wi-Fi Protected Access 2 Pre shared key (WPA2-PSK)/Wi-Fi Protected Setup(WPS). This research is mainly focusing on WPA2 as the base technology and build a solution on top of it. WPA2-PSK stands for “Wi-Fi protected access 2 pre shared key” it is the predecessor of WPA. When a user provides a Plain-English text as the password for the Wi-Fi network, the Temporal Key Integrity Protocol(TKIP) technology uses the password and the Service set Identifier(SSID) to generate a unique encryption keys. One disadvantage in WPS2 is that it does not provide a second level of a security to the password. Think of a scenario where the intruder somehow gets to know the Wi-Fi network password, the intruder will freely gain access to the network because the password is correct. To address this vulnerability, in this research paper the team has used two factor authentication. Once the correct password is entered then the user will be asked to enter the 6-digit authentication key. If the 6-digt key is correct then the user will be granted the access to the network. Mac-address filtering is used to provide a 6-digit key and identify the device uniquely. This research paper does not stop from two factor authentication; it will use Multi factor authentication to provide security to the network. After 01 hour of time if a connected device dose not communicate with the network then the device will be removed from the access granted list of the router. The outcome of this research paper is providing the home Wi-Fi network users with highly secure Wi-Fi network password authentication mechanism.

Index Terms- WPA2-PSK, mac address filtering, encryption, two factor authentication, RSA.

I. Introduction

With the Vast use of Wi-Fi networks in home environment, it has raised number of issues and vulnerabilities. Mainly the security threats of the network have risen. There are currently various standards to make the Wi-Fi networks more secure and constant. Every Wi-Fi network is protected with a password, in order to protect the network from outside parties. Basically the passphrase of the network is encrypted using an encryption standard such as: WEP, WPA, WPA2. To authenticate a user into the network there are other mechanisms such as: WPS and Rivest-Shamir-Adleman (RSA). Even though there are such standards the intruders find their way into the network [7] [2]. In the co-operate world there are mechanisms to block intruders and secure the network. The issue with those mechanisms are that they are very costly and because of the cost, it’s harder to the home users to use them in their networks. Routers play main role in networking. Since its play a main role malicious people try to hack routers, securing a router is a crucial matter. There are several methods to secure a router. Mac address filtering, password encryption and using firewall are some solutions. When mac address filtering once can control number of people who can access a local area network(LAN). That avoid unauthorized people to assign network applying password and encrypting avoid hackers to accessing and configuring router by third party. By introducing the W2FA standard for the users the research team is trying to implement a more secure Wi-Fi authentication standard with a low cost approach. For the succeed the proposed research there need to be done some modifications to router firmware and the operating system of the end device. The main base standard for the W2FA is two factor authentication mechanism [1].

II. BACKGROUND

Wi-Fi technology allows electronic devices connect to a wireless LAN (WLAN), mainly through Ultra high frequency (UHF) 2.4 GHz (12 cm) and 5 GHz (6 cm) radio bands connect Super high frequency (SHF) ISM. A WLAN is a password protected generally, but can be opened, so that each device access at the touch of the resources of the wireless network. The Alliance Wi - Fi Wi - Fi defined as any “wireless local area network “(WLAN) products based on the Institute of Electrical and Electronics Engineers ' (IEEE) 802.11 standards. " Wi - Fi “is a registered trademark of the Alliance Wi - Fi. The “Wi-Fi Certified “trademark of Wi-Fi products that are successfully used a full interoperability certification testing Wi-Fi Grouping. Devices Wi - Fi include personal computer use, video game consoles, smart phones, digital and modern printers. Connecting devices compatible with Wi - Fi using a wireless network anda wireless Internet access. Such access point (or hotspot) has a range of about 20 meters (66 feet) inside and a wider range outdoors. Hotspot analysis can be as small as a single room with walls that block radio signals, or many square kilometers achieved by using multiple access points that overlap. Wi-Fi is less secure than wired connections such as Ethernet, just because an intruder does not need physical connection. Websites that use Transport Layer Security (TLS), are safe, but the access to unencrypted Internet can be easily familiar by intruders. For this reason, Wi - Fi various encryption technologies has made. Early Wired Same Privacy (WEP) encryption was easy to break. The highest quality protocols Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) were added later [11].

The main advantages of using Wi-Fi technology is the lack of wires. This is a wireless connection that can merge together multiple devices. Wi- Fi products are widely used in the market. There are several brands of access points and user network interfaces are able to inter - work with a very simple level of service. Wi-Fi networks can support roaming. With the emergence of public wireless networks, users can access the internet even outside their normal work location. Wireless networking hardware at worst a modest increase from wired counterparts. This potentially increased cost is almost always more than balanced by the savings in cost and labor connected to running physical cables.

The rate in most wireless networks (typically 1-54 Mbps) is much slower than even the slowest common wired networks (100 Mbps to several Gbps). However, in special applications, the performance of a cable network may be required. Wi-Fi has a limited range and is suitable for home networks, which is more dependent on the location. To combat this consideration, wireless networks are available to use some of the different encryption technologies. However, some of the methods most commonly dedicated. Like any radio frequency transmission, wireless networking signals are subject to a wide variety of interference, as well as complex propagation effects that are beyond the control of the network administrator.

III. RELATED WORK

The research team have a done literature review of about eighteen research papers (Refer Table II). All of those papers are related to the area that research team is focusses. This section contains six literature reviews. The included literature reviews are crucial ones for the proposed system.

The patent publication “METHOD AND SYSTEM FOR MAINTAINING A MAC ADDRESS FILTERING TABLE” is invented by Erik J. Johnson. The primary goal ofthe invention is to introduce a method that will efficiently maintain a MAC address filtering table. This research paper will be used in “Wi-Fi password multi factor authentication for home users” to address the issue the research team having with managing a trusted mac address list. What this means is the home admin need to add all of his devices into the routers trusted mac list. If a device tries to connect to the network first of all the router will check weather the device is on the trusted mac list, if not it will not send the 6digit verification key otherwise it will send the verification key to the device. This research paper shows a methodology to manage and maintain a mac address filtering table, the research team will modify its capabilities in order to fit them to the functionality what they are trying to build. Since this is a patent paper the technology is invented already, so there is no future work in this paper. The research term could easily use this method and modify its functionalities without a limitation [8].

Enhanced Security Evaluation and Analysis of Wireless Network based on MAC Protocol.

The purpose of this paper is to educate the public at large and protecting them from several serious attacks. This paper has highlighted WLAN vulnerabilities and concluded that Wireless Security is always the major issue. IEEE 802.11 Standard for wireless network classifies security Pre-RSNA AND RSNA algorithm. This Paper evaluates why pre-RSNA methods fail for providing security to wireless Networks. This analysis is necessary to migrate to RSNA and making more highly secure and reliable RSNA methods. RSNA provides two data confidentiality protocols, called the Temporal Key Integrity Protocol (TKIP) and the Counter-mode/CBC-MAC Protocol (CCMP), and the RSNA establishment procedure, including 802.1X authentication and key management protocols. The IEEE 802.11 standard defines two types of WEP authentication: Open System and Shared Key. There are two other mechanisms: The Service Set Identifier (SSID) and authentication by client Media Access Control (MAC) address are also commonly used in home environment and business environment. Network security is mostly achieved through the use of cryptography. security algorithm or cryptography techniques broadly, classified as symmetric & asymmetric key cryptography algorithms used in classified as stream cipher and block cipher, DES (Data Encryption Standard) and AES (Advanced Encryption Standard). IEEE 802.11i, an IEEE standard and designed to provide enhanced security in the Medium Access Control (MAC) layer for 802.11. Pre-RSNA Methods fail to meet their security goals and are deprecated except for Open System authentication. After going through this research paper research team was able to identify why Pre-RSNA Methods fail? And get know the RSNA new method. Finally, how we used this RSNA method to our security mode Multifactor authentication and apply this secure method to home environments [3].

Authentication is the gateway to a secure system. Along with the integrity, confidentiality and authorize it helps avoid any interference in the system. Until a few years ago was based authentication password again is the most common form of authentication for each network secure. However, with the advent of more sophisticated technologies that form of authentication, although not yet become widespread unsafe. Moreover, with the increase of the "Internet of things" in which the number of devices grow collector, it would not be feasible to remember countless passwords for users It is therefore important to resolve this concern by drawing paths, where multiple forms of authentication are required to access all intelligent devices and also the ability to use would be high. This article, a methodology, discussed what type of authentication mechanisms internet of things (IOT) could be used [5].

In recent years, service providers of wireless Internet (WISP) access points Wi established - to increase Fi in numbers to the public Type access, the local coverage for users who travel and offer the possibility of e-mail, Web and other Internet applications emotional. In this paper, it is observed that while the mobile computing landscape has changed in terms of the number and type of access point both Places there remain several technical and implementation challenges before access points can be a common setup. These challenges include authentication, security, coverage, management, location-based services, billing and discuss existing interoperability. We Research, the work of standardization bodies and the experience of commercial hotspots providers in these fields, and then define believably open research questions that remain [12].

In current world wireless networking provides many advantages for personal and organizational level. But it's coupled with new threats, unauthorized access and intrusions. So overall databases and information are in very high risk stage. Although implementation of technological solutions is a very usual thing wireless security in current world. And researchers discuss what are the solutions for countering a number of threats. And main target of these researches mitigates these identified threats and vulnerabilities. Network configuration is very faster, easier and it is less expensive. Although wireless technologies create new threats day by day. As an example wireless communication takes place using (through the air) using radio frequencies the risk of unauthorized accesses is greater than wired networks. In this research paper, researchers provide basic understanding of the nature of the various threats associated with wireless networking. Some of wireless network attacks are accidental association, Malicious association, Ad-hoc networks, nontraditional networks, Identity theft (MAC spoofing), Man-in-the-middle attacks and etc. Use of encryption and turn off identifier broadcasting possible to securing wireless networking. Although it is impossible to eliminate all the risks associated with wireless networking [15].

Most computer systems today use identification and authentication through username and password as the first line defense. An easy way to protect confidential informationis the use of passwords, however this solution often involves a compromise between security and convenience. This risk of an attacker guessing a valid password cannot be eliminated however you can try to lower probability of such an event. Therefore, two factor authentication has been introduced. Two-factor authentication uses two factors for identity verification. Two-factor authentication (2FA) schemes aim at strengthening the security of login password-based authentication by deploying secondary authentication tokens [10].

IV. METHODOLOGY

In this section the research team specify the mechanism and the technology that is been used in W2FA standard.

A. Research question

The main research question that the team tries to address with this methodology is, the home users' vulnerability in Wi-Fi password authentication. Which occurs when an intruder discovers the Wi-Fi password of the network. Using the proposed implementation, the home users will be able to experience a secure WI-FI network in their homes.

B. Objectives

With the successful implementation of this research the Wi-Fi network home users will be facilitated with more secure work environment. Research functions are listed in the Appendix.

- Second level of security for the Wi-Fi home network authentication engine.
- Blocks Malicious network attacks from the outsiders.
- To kick out the connected device from the connected list after an hour of inactivity.

C. Solution brief introduction

To address the above mentioned vulnerability the research team will implement a two factor authentication mechanism in a WI-FI network. Solution brief introduction will briefly explain the steps on how this will be archived. In the upcoming chapters the methodology will be deeply described. Mainly the Wi-Fi router firmware need to be modified to support this new standard, after wards there will be newly implemented mac address filtering tables in the routers memory. Filtering table will keep track of all the trusted device macs in its memory. The home admin will have to manually add trusted devices to the router beforehand. To add a device to the router, the admin must access the routers control panel and add the macs to the filtering table (Table I). This is only a onetime process. Once the above process is done when a device tries to connect with the correct network password the router will cross check device mac address with the filtering list's macs. If the device mac is not found in the trusted list, the request will be rejected. Ifit is found, then the router will generate the 6-digit verification key and it will be sent to the requested device. The key generation and distribution will be done in a secure manner, which will be explained in the next few chapters. Once the user's device receives the verification key the devices authentication engine will decrypted the received key. Then it will check the device mac address with the decrypted key. If the two verification keys are a match, the user will be granted access to the network (refer figure. 1), else the user will not be granted access to the network (refer figure. 2). The second part of the research is to kick out a user from the router after a certain amount of inactive time in the network. If the device and the router does not communicate for about 1 hour, then the device record will be removed from the access granted list of the router. To archive these suggested mechanisms there should be modifications done to the router and the end-device software as well. The proposed system is not for the cooperate world, because there are other mechanics for the cooperate world to archive the above security measures [4] [6].

D. Mac address table technique

Media Access(MAC) Filtering technique is a crucial component in this research, because basically it controls the whole work flow of the methodology. In order to make the research a success the research team have focused deeply on this component. To implement a mac address filtering table in a router the router firmware needs to be modified. Once this is implemented in the router there will be a table called "MAC Address trusted List" this table will keep track of all the devices of the home user. In order to trust a device, the user will need to add the device into the router [8]. MAC address trusted table contains three columns. Entry number, Mac address and Status. To add a device into the router there need to be a special user interface inside the router's control panel firmware. Once the home user Admin gets into the above interface he or she will need to try to connect their device by entering the network password into their device. While this is happening, the router interface will be listening to incoming request traffic. Once the device with a correct network password sends the request to the router it will capture the device mac address. The captured mac will be added to the trusted list table.

E. Generating authentication key and distribution

Generating the 6-digit authentication key is done from the router side. Once the correct Wi-Fi network password is provided to the router, the router will cross check the trusted list table for the requested device mac. Once the device mac is found, router will start generating the 6-digit authentication key. To generate the 6-digit authentication key, the Algorithm needs to request the device Mac address as the parameter. Then the RSA algorithm will generate the authentication key. The RSA algorithm that is being used in W2FA is a customized algorithm. The customized algorithm will decrypt the 12-character mac address into a 6-digit key [14] [9]. The generated key will be sent to the user device. Distribution of the generated key is done through the opened path between the router and the user device. The above mentioned path is opened when the user enter the correct WI-FI network password. This path is opened until the device is connected to the network or until the router close the path. Closing the path occurs when the device mac address is not found on the trusted list table.

F. Authentication keys validation

Authentication key validation is done in the user's device. To perform the authentication process, the device operating system authentication engine needs to be modified. The client authentication engine will decrypt the received encryption key using RSA algorithm. It will compare the decrypted key with MAC Address of the end device. If the both keys are matching, the user device will send a packet with the flag (Authentication success) to the router. If the key does not match with end device MAC address it will send a packet with the flag (Authentication failed). The router will check the received packets, if the flag of the packets is "successful" the device will be connected to the network. Otherwise the device will be kicked out [13].

G. Kicking out a connected user from the network

When a connected user is inactive for about one hour of time, the connected user will be kicked out of the network. This is done using the connected list table. If a connected device does not communicate with the router for about one hour the entry of the connected user will be removed from the table. Afterwards that user will need to re-authenticate.

APPENDIX

V. CONCLUSION

Wi-Fi has a notoriously weak security standard. The password it uses can often be cracked within a few minutes with a basic laptop computer and widely available software tools. Wireless networks are an important evolving marketplace for the telecom industry to distribute a variety of applications and facilities to both mobile and fixed users. It is possible to implement this concept the firmware of the router and the authentication engine in the client operating system. There is a minor issue in the performance of the router, even if the firmware is changed, the router hardware and processing power may not be sufficient to support the firmware upgrade. In reality it is impossible to totally eliminate all risks associated with wireless networking. The outcome of this research paper is providing the home Wi-Fi network users with highly secure Wi-Fi network password authentication mechanism. It is impossible to totally eliminate all risks associated with wireless networking. After this research, the team can give a highly secured Wi-Fi network. Some of these methodologies, mechanisms, and theories practically does cause a minor delay but since it is for home network security, delay in establishing connection to the Wi-Fi network is tolerable.

VI. FUTURE WORK

User authentication is a balance of security and user experience. This Research paper presents the possibility of creating a simple, secure and low-cost two-factor authentication mechanism. The solution proposed also presents a possibility of introducing an additional authentication. The most common type of two-factor authentication involves sending a temporary key. This is still not bulletproof, and it definitely increases the possibility of people being locked out of their accounts if they do not receive the temporary key. Some people are already saying that two-factor authentication has passed its prime, as the research team already seeing it being breached. This proposed method might help to solve this problem. The changes in router firmware and changes in Authentication Technology will be investigated in future work. To support the proposed W2FA standard, the operating system authentication engines will also need to be modified in the future. Modifying the router performance need to be done in the future. Basically an improvement in the processing power is needed. A research team could look into these suggestions and do their research.

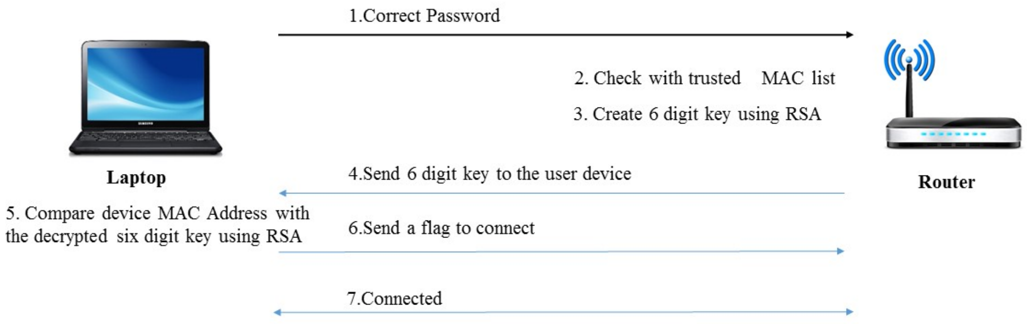
1.Correct Password
2. Check with trusted MAC list
3. Create 6 digit key using RSA
Laptop
Router
4.Send 6 digit key to the user device
5. Compare device MAC Address with the decrypted six digit key using RSA
6.Send a flag to connect
7.Connected

Figure 1: Methodology Overview Diagram (Success login)

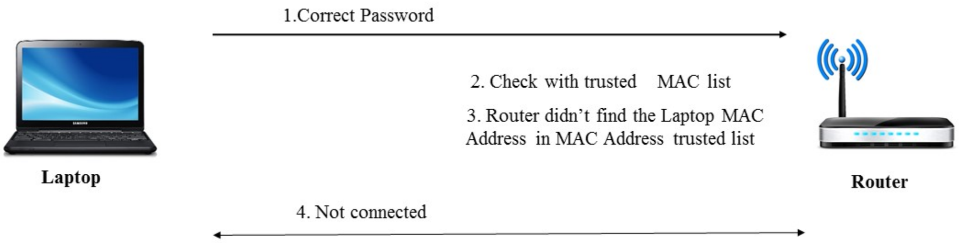
1.Correct Password
2. Check with trusted MAC list
3. Router didn't find the Laptop MAC Address in MAC Address trusted list
Laptop
Router
4. Not connected

Figure 2: Methodology Overview Diagram (Failed login)

TABLE I: MAC Address Trusted List Table

Entry No	**MAC Address**	**Log Time**	**Status**
01	0000 0000 1111	01 : 30	Connected
02	00E0.F921.410C	07 : 30	Connected
03	0002.17E6.B7DC	05 : 30	Connected
04	00E0.8F54.A63B	00:00	Not Connected
05	00A2.1UE6.B77C	00 : 15	Kick out

Research Functionalities List

Function 1 – Two Factor Authentication.
Function 2 – Six digit encrypted key generation.
Function 3 – Mac-Address Filtering
Function 4 – Real Time Computing
Function 5 – Time Base Connection Termination
Function 6 – Anti Hacking Technique

TABLE II: Research Function Table

Research Papers	**Function 1**	**Function 2**	**Function 3**	**Function 4**	**Function 5**	**Function 6**
Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)	x	✓	x	✓	x	✓
METHOD AND SYSTEM FOR MAINTAINING A MAC ADDRESS FILTERING TABLE	x	x	✓	x	x	✓
METHOD AND ARCHITECTURE FOR SECURITY KEY GENERATION AND DISTRIBUTION WITHIN OPTICAL SWITCHED NETWORKS	x	✓	x	✓	x	x
WIRELESS HOME SECURITY SYSTEM WITH MOBILE	✓	x	x	x	x	x
Wireless Network Security: Vulnerabilities, Threats and Countermeasures	✓	✓	✓	x	x	✓
Wireless Visual Visitor Verifier for Home Security Using Smart Phone	✓	✓	x	x	x	x

Enhanced Security Evaluation and Analysis of Wireless Network based on MAC Protocol	✓	✓	✓	✓	x	x
Vulnerability of Wireless Network Security due to Parallelized Brute Force Attacks	✓	x	x	x	x	✓
WIRELESS NETWORK SECURITY THREATS	✓	✓	x	x	x	✓
Application of Multi factor authentication in Internet of Things domain	✓	x	x	x	x	x
On the (In)Security of Mobile Two-Factor Authentication	✓	✓	x	x	✓	x
An authentication scheme for fast handover between WiFi access points	x	x	x	✓	x	x
WIFIOTP: PERVASIVE TWO-FACTOR AUTHENTICATION USING WI-FI SSID BROADCASTS	✓	x	✓	x	x	x
oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks	✓	✓	x	✓	x	✓
Authentication Systems in Internet of Things	✓	x	x	x	x	✓
Security in Wireless Local Area Networks	✓	✓	x	✓	x	✓

Wireless Hotspots: Current Challenges and Future Directions	✓	x	✓	x	✓	x
IEEE 802.1X Pre-Authentication	✓	✓	✓	✓	x	x
REFORMED RSA ALGORITHM BASED ON PRIME NUMBER	✓	✓	✓	✓	✓	X
Wi-Fi Password Two Factor Authentication for Home users (W2FA)	✓	✓	✓	✓	✓	X

ACKNOWLEDGEMENT

We would like to thank Mr. Dhishan Dhammearatchi from Sri Lanka Institute of Information Technology Computing (PVT) Ltd, for his feedback and advice on the ideas expressed in this research paper of Wi-Fi Password Two Factor Authentication for Home users (W2FA).

REFERENCES

[1] Kumar, D., Sehgal, U., (January June 2009), “Wireless Network Security Threats”, International Journal of Information Technology and Knowledge Management, Volume 2, [No. 1], pp. 181-183, web [Online]. Available: http://www.csjournals.com/IJITKM/PDF%202-1/38_Umesh_Sehgal_Dinesh_Kr.pdf, [Access Date: 22 /07/2016]

[2] Wolfe, M., (April 25, 2012), “Vulnerability of Wireless Network Security due to Parallelized Brute Force Attacks”, Computer Science Undergraduate Research Symposium, Volume 1, 1 – 4, web [Online]. Available: http://cs.winona.edu/CSConference/2012conference.pdf#page=15, [Access Date: 25/07/2016]

[3] Izhar, M., Shahid, M. And V.R.Singh, (11 November 2013), “Enhanced Security Evaluation and Analysis of Wireless Network based on MAC Protocol”. International Journal of Scientific and Research Publications, Volume 3, 1 – 4, web [Online]. Available: http://www.ijsrp.org/research-paper-1113/ijsrp-p2308.pdf, [Access Date: 18/08/2016]

[4] Bohak, A., Buttyan, L., Dora, L., (October 22-24, 2007), “An authentication Things domain for fast handover between Wi-Fi access points”, Budapest University of Technology and Economics, Hungary, 1 – 9, web [Online]. Available: https://www.crysys.hu/publications/files/BohakBD07wicon.pdf, [Access Date: 21/07/2016]

[5] Gupta, U., (20 Jun 2015),“Application of Multi factor authentication in Internet of Things domain”, Information Networking Institute Carnegie Mellon University, Pittsburgh – Pennsylvania, USA, Volume 2, 1 – 6, web [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1506/1506.03753.pdf, [Access Date: 05/08/2016]

[6] Dmitrienko, A., Liebchen, C., Rossow, C and Sadeghi, A., (April 16, 2014) On the (In)Security of Mobile Two-Factor Authentication, Technische University at Darmstadt Center for Advanced Security Research Darmstadt D-64293 Darmstadt, Germany. 1 – 12, web [Online]. Available: https://www.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_TRUST/PubsPDF/TR-Dmitrienko-2FA-analysis-v2.pdf, [Access Date: 19/07/2016]

[7] Arana, P., "Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)", (2006), 1 – 6, web [Online]. Available: http://cs.gmu.edu/~yhwang1/INFS612/Sample_Projects/Fall_06_GPN_6_Final_Report.pdf, [Access Date: 06/8/2016]

[8] Johnson, E., (Jan. 1, 2004), “Method And System For Maintaining A Mac Address Filtering Table", United States Patent Application Publication, no. 041228041254, pp, 1 – 45, web [Online]. Available: https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US20040001492.pdf, [Access Date: 26/7/2016]

[9] Ovadia,S.,(Aug. 11, 2005),"Method And Architecture For Security Key Generation And Distribution Within Optical Switched Networks", United States Patent Application Publication, no. 200501777491, pp,

1 – 36, web [Online]. Available: https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US20050175183.pdf, [Access Date: 20/07/2016]

[10] Huseynov, Emin, Seigneur, Jean-Marc, (04/11/2015), “WifiOTP: Pervasive Two-Factor Authentication Using Wi-Fi SSID Broadcasts”, In: ITU / IEEE. Kaleidoscope International Conference, 1 – 9, web [Online]. Available: http://archive-ouverte.unige.ch/unige:76795, [Access Date: 21/08/2016]

[11] Vishali, R., (April-June 2014), "Security in Wireless Local Area Networks", International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 2, Issue 2, pp: (472-483), 1 – 36, web [Online]. Available: www.researchpublish.com, [Access Date: 19/07/2016]

[12] Balachandran, A., Geoffrey M., Bahl P, (2005), "Wireless Hotspots: Current Challenges and Future Directions", c2005 Springer Science + Business Media, Inc. Manufactured in The Netherlands, Mobile Networks and Applications 10, 265–274,

1 – 10, web [Online]. Available: http://research.microsoft.com/en-us/um/people/bahl/Papers/Pdf/monet05.pdf, [Access Date: 20/08/2016]

[13] Aboba, B., (June 17, 2002) "IEEE 802.1X Pre-Authentication", doc.:IEEE 802.11-02/389r0, 1 – 47, web [Online]. Available: http://www.ieee802.org/1/files/public/docs2002/aboba-pre-authentication.pdf, [Access Date: 22/7/2016]

[14] Jaiswal, J., Soni, R., Mahale, P., (2014), “Reformed RSA algorithm based on Prime Number”, International Journal of Computer Applications (0975 – 8887), 1 – 4, web [Online]. Available: http://research.ijcaonline.org/ncetit/number2/NCETIT3029.pdf, [Access Date: 20/08/2016]

[15] Min-kyu Choi, Rosslin John Robles1, Chang-hwa Hong, Tai-hoon Kim., (July, 2008), “Wireless Network Security: Vulnerabilities, Threats and Countermeasures”, International Journal of Multimedia and Ubiquitous Engineering Vol. 3, [No. 3],), 1 – 10, web [Online]: Available: http://www.sersc.org/journals/IJMUE/vol3_no3_2008/8.pdf , [Access Date: 19/08/2016]

AUTHORS

First Author – W.M.G. Kanishka, Information technology undergraduate student, Sri Lanka Institute of Information TechnologyComputing (PVT) Ltd, gkanishka6@gmail.com.

Second Author – R. Suresh, Information Technology Undergraduate Student, Sri Lanka Institute of Information TechnologyComputing (PVT) Ltd, sureshrajasegaram@gmail.com
Third Author – M.F.A.E. De Silva, Information technology undergraduate student, Sri Lanka Institute of Information TechnologyComputing (PVT) Ltd,silvashani123@gmail.com
Fourth Author – Thennakoon T.B.S.P, Information technology undergraduate student, Sri Lanka Institute of Information TechnologyComputing (PVT) Ltd, poornithennakoon13@gmail.com.
Fifth Author – Amarasinghe G.C.J, Information technology undergraduate student, Sri Lanka Institute of Information TechnologyComputing (PVT) Ltd, amarasinghegcj@gmail.com.
Sixth Author - D.B.D.R.B Ehelepola, Information technology undergraduate student, Sri Lanka Institute of Information TechnologyComputing (PVT) Ltd, dinethehelepola@gmail.com.
Seventh Author - Dhishan Dhammearatchi, Lecturer at Sri Lanka Institute of Information Technology Computing (PVT) Ltd, dhishan.d@sliit.lk

Correspondence Author – W.M.G. Kanishka, gkanishka6@gmail.com, +940770742755.