Secure Hotspot

A Novel Approach to Secure Public Wi-Fi Hotspot

Laiju K Raju
Dept. of Computer Science and Engineering
College of Engineering Trivandrum
Trivandrum, India
Email: lkr.laiju@gmail.com

Reena Nair
Dept. of Computer Science and Engineering
College of Engineering Trivandrum
Trivandrum, India
Email:reenanair@cet.ac.in

Abstract—**Wi-Fi technology has gained its wide popularity in computer networking in the last decade. Today, Wi-Fi is being used as the major networking medium in LAN (WLAN), adhoc networks, house hold networks, VAN etc. Another promising area where Wi-Fi is being used is the public internet Access Points called hotspots. These days internet is made available for free via a Wi-Fi Access Point (Hotspot) in many public places like restaurants, shopping malls etc. Security of confidential information exchanged through these public hotspots should be ensured. None of the existing security measures adopted in a public hotspot ensures secure communication. Behind every such network, waiting like a mugger in a dark corner may be a hacker, intercepting your confidential information such as credit card numbers, name, address and more, before it ever reaches the intended destination.**

A security protocol that ensures secure internet access through public Wi-Fi hotspot is important in this scenario. The existing solutions to this problem are mostly user centric and they are considered as precautions taken from the user side. This paper considers vulnerabilities like open nature of communication channel, lack of confidentiality, weak encryption methods etc. in a public Wi-Fi hotspot and proposes a security protocol that ensures individual confidentiality during the communication. The solution tries to eliminate the dependency on any pre-shared information between the AP (Access Point) and the client device to implement security. Existing WPA2-PSK protocol is modified to generate an Instantaneous Session Key (ISK) between the client and the Access Point through secured Diffie Hellman key exchange thereby eliminating the dependency on a pre-shared key.

The study covers existing security issues in a public hotspot, limitations in the existing security protocols and other precautionary measures, the proposed solution and security analysis of the proposed solution.

KeywordsWi-Fi Hotspot; Wireless Protocol; WPA; Wi-Fi; Wi-Fi Networks

I. Introduction

Wi-Fi, short for Wireless Fidelity is the commercial name for 802.11 standard that has become the preferred technology for wireless local area networking (WLAN) in both business and home environments. Generally, Wi-Fi uses a limited pool of narrow band radio frequencies on unlicensed bands at 2.4 GHz UHF (Ultra High Frequency) and 5 GHz SHF (Super High Frequency). The available power range in Wi-Fi devices allow for cells with an average radius of less than 100 meters [1]. The use of wireless networking has grown rapidly, with organizations and home users extending their wired local area networks (LAN) to include wireless LANs (WLAN). It is easy for an attacker to get access to the wireless medium and this makes the possibilities of attacks against Wi-Fi networks promising.

This study concentrates on the security aspects of a public Wi-Fi hotspot network. The present security means of Wi-Fi technology has limitations that make them unsuitable for a public hotspot network. In a hotspot network that is open to all, the major security requirement is confidentiality to the individual users. The proposed solution aims at providing a new security protocol that can successfully meet various security requirements of a public Wi-Fi hotspot network. The protocol is free from any pre-shared information between the client and the Access Point. This protocol, that meets the security challenges of a public Wi-Fi hotspot can be used in wide range of applications.

II. WI-FI SECURITY PROTOCOLS

A. Evolution

The IEEE 802.11 standard includes the following security features [2].

1) Service Set Identifier (SSID) which is used to control access to an Access Point (AP).
2) The Access Control List (ACL) to prevent unauthorized access.
3) The encryption protocol intended to provide data security.

Since 1997, evolution of Wi-Fi encryption protocol happened in three main stages: the original IEEE 802.11b (WEP) protocol, an intermediate stage with Wi-Fi Protected Access (WPA), and the third stage defining the IEEE 802.11i (WPA2) protocol [3].

WEP was designed to provide an equivalent security to the wireless networks as that of the wired counterpart by providing authentication, encryption, and data integrity. The protocol includes a set of message exchanges and uses RC4 (Rivest Cipher 4) encryption algorithm. Serious vulnerabilities identified in WEP led to an interim security protocol in Wi-Fi domain called WPA. It tried to eliminate the vulnerabilities in WEP by replacing RC4 with TKIP (Temporal Key Integrity Protocol). Soon after WPA, IEEE and Wi-Fi Alliance came up with WPA2, the more stable version that uses stronger AES (Advanced Encryption Standard) algorithm for encryption

978-1-4673-7349-4/15/$31.00 ©2015 IEEE

TABLE I
COMPARISON OF WI-FI SECURITY PROTOCOLS [6]

	Protocol Name		
Properties	WEP	WPA	WPA2
Cipher	RC4	RC4	AES
Key Size	40/104 bits	128 bits (encryption) 64 bits (authentication)	128 Bits
Key Life	24-bit IV Concatenate IV to base key	48/128-bit IV TKIP mixing function	48/128-bit IV TKIP mixing function
Packet Key	Concatenated	Mixing function	Not needed
Data Integrity	CRC-32	MIC (Michael)	CCM
Replay Detection	None	Enforce IV sequencing	Enforce IV sequencing
Header Integrity	None	MIC (Michael)	CCM
Key Management	None	EAP-based (802.1X)	EAP-based (802.1X)

[4][5]. Today WPA2 is the most widely used security protocol in Wi-Fi networks. It has 2 modes of operation,

- WPA2 - PSK(Pre Shared Key) : Based on a pre-shared key between the client and Access Point
- WPA2 - Enterprise : Based on a dedicated Remote Authentication Dial-In Service(RADIUS) server.

B. Security Issues of Public Wi-Fi Hotspot

A public Wi-Fi hotspot is set up mainly to provide broadband internet connection through wireless medium to the users. Since it is meant for the public, anybody can connect to the hotspot and use internet through the Access Point provided. This utility scenario posts many security challenges in front of a user who access critical information through the hotspot. Encryption methods used to protect private wireless networks such as WEP and WPA2, are not suitable for public networks due to the complexities in supporting the users[7]. Furthermore, using WEP or WPA2 impels us to advertise the secret password used to generate private encryption key(s). This destroys the effect of encryption since wireless eavesdroppers can easily decode the encrypted hotspot traffic. None of the existing security measures are sufficient for a public hotspot since all of them depends on a pre-shared secret information between the client and the Access Point, which is practically impossible in case of a public hotspot. Some of the security vulnerabilities in an open hotspot are discussed below.

Unlike public wired internet connections, the use of hotspots impose the risk of people capturing real-time traffic over the wireless connections[8]. People can easily capture the packets of unsecured hotspot connections from the air and decrypt them. Eavesdroppers can get private information such as web sites visited by a user, login credentials of the user for unsecured web pages and web services, even the web page content, using tools which are freely available[9].

The device used to connect to the network can get exposed to an attacker. Access may be open to any shared files on your mobile device which can become a back door for an attacker.

'Evil-Twin Hotspots'- Access Point (AP) posing as a legitimate hotspot, may create serious information thefts from the users.

C. Existing Solutions and Limitations

No effective solutions exist to secure the communication from the hotspot perspective. The available solutions require the client to take a set of precautions. Whenever a user connects to the public hotspot, he has to adopt these precautions which keeps him safe to a better extent than taking none. Few of them are

- Activate the device firewall
- Use a VPN tunnel for communication with the Access Point
- Use open DNS to guard against DNS poisoning
- Access only https enabled web sites

These precautions have to be intentionally adopted by the user and it may not be easy for a common man who is not a computer or communication expert to configure them. For a normal user these precautions may not be user friendly and moreover they cannot assure a reasonable level of security for the user.

III. SECURED HOTSPOT

Public hotspots demand a security mechanism that does not depends on any pre-shared information. The mechanism should be computationally light weight as well to be affordable by all kinds of ubiquitous communication devices. Considering these constraints, we propose a new protocol which aims at ensuring the necessary security properties such as confidentiality and privacy in a public Wi-Fi hotspot network. The protocol is developed as an extension to WPA2 which inherits all security features of WPA2 mechanism. It tries to eliminate the dependency on a pre-shared key in WPA2 - PSK.

A. WPA2 - PSK

Wi-Fi Protected Access 2 - Pre-Shared Key (WPA2-PSK), popularly known as WPA2 Personal, was designed for home users who doesn't have a dedicated enterprise authentication server. It uses WPA2 along with an optional Pre-Shared Key (PSK) for authentication.

To encrypt a network with WPA2-PSK, the Access Point router is provided with a plain English passphrase, 8 to 63 characters wide. The passphrase, along with the network SSID, is used to generate a Master Session Key (MSK)from which the encryption keys are derived using a 4-way handshake

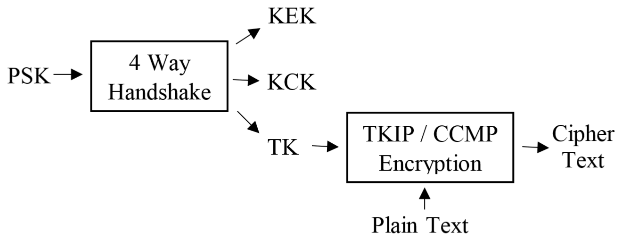

Fig. 1. Key Generation in WPA2

process. PSK mode is one of two available authentication methods used for WPA and WPA2 encryption.

WPA2-PSK mode works on the pre-shared passphrase. This passphrase will be shared to all users in the network, assuming that nobody from outside knows it. Passphrase is used to generate MSK at both client and AP. MSK is used as input to the 4-way handshake that generates PTK (Pairwise Transient Key)and the 3 significant keys used in WPA2 encryption.

Conventional four way handshake includes a series of steps performed by the client and the Access Point to exchange a set of keys. The major goals of the 4 - way handshake are

- To derive PTK from MSK
- Verify the agreed cypher suit
- Communicate the group key

The 3 significant keys derived during the handshake are:-

- Temporal Key (TK) - Used for Encryption and integrity protection for the data packet
- Key Confirmation Key (KCK) - For integrity protection of messages passed in 4 - way handshake
- Key Encryption Key (KEK) - To encrypt the message used for distribution of the group Key

B. Secure Hotspot Protocol

The proposed solution executes 4 - way handshake with a minor but important change. This protocol has an additional step before the handshake in which it establishes an instantaneously generated session key that can be used instead of pre-shared key. Thus the protocol no more depends on a pre-shard key between the client and AP. The Instantaneous Session Key (ISK) is generated through a strongly protected Diffie Hellman (DH) algorithm. The protocol assumes that the Access Point has a valid PKE certificate. This is necessary to mitigate Man in the Middle(MIM) attack during DH Key exchange.

The protocol starts with a session key establishment phase which generates an ISK (Instantaneous Session Key). This key is used instead of a pre-shared key in the subsequent phases. The protocol uses a suitable variation of the Diffie Hellman key exchange method to exchange the session key. The steps are shown in Fig.2.

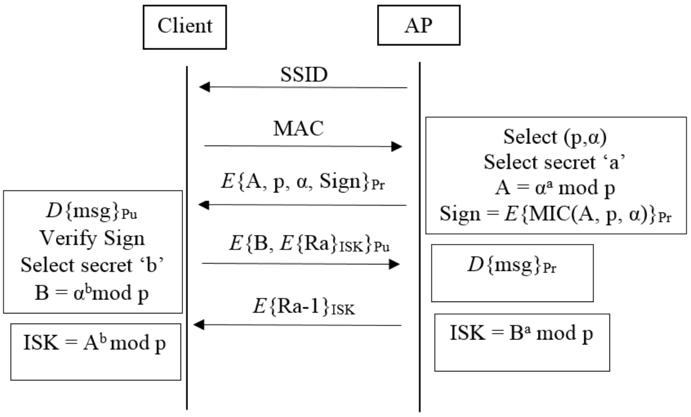

Fig. 2. Secured Hotspot Protocol

- Step 1: Access Point broadcasts the beacon signal which contains the SSID.
- Step 2: Client receives the SSID and sends its MAC address to the AP
- Step 3: Access Point selects the Diffie Hellman parameters, a reasonably large prime number p, and the secret value a. Calculate α, which is the primitive root of p. These values are used to calculate A using the formula $A = \alpha^a modp$. A MIC (Message Integrity Code) value is calculated from (A, p, α) and is encrypted using the private key of the AP. This encrypted MIC value is used as a signature of the AP to mitigate 'Man In The Middle(MIM)'attack. The third message from AP to the client consists of $(A, p, \alpha, Sign)$ and will be encrypted with private key of the AP.
- Step 4: The client, upon receiving the message decrypts the packet using public key of the AP and verifies the AP certificate and signature. Then select its secret value b and calculates the value B using the formula $B = \alpha^b modp$. Now client will be ready to calculate the new Instantaneous Session Key (ISK), K as $K = A^b modp$. Then it sends B along with an encrypted nonce value Ra together encrypted with public key of the AP.
- Step 5: AP decrypts the fourth message using its private key. Then it calculates the ISK as $K = B^a modp$. The nonce value Ra is decrypted, decremented and sent back to the client encrypted by the session key K. This proves that both agree upon the same session key.

The DH parameters are selected in such a way that the generated ISK will be 256 bits wide. After the key exchange, both AP and the client share an instantaneous session key (ISK). This key is passed to the WPA2 4-way handshake instead of the PSK to proceed with the WPA2-PSK protocol.

When there are more than one client connecting to the AP, the corresponding ISKs will be stored in a database maintained at the AP. When the connection with a client device is terminated, the ISK entry is removed from the database after making an entry in a connection history log file. At any instant of an active connection, ISK will not be known to intruders, keeping the communication strictly confidential.

C. Security and Performance Analysis

Communication secrecy is the prime security requirement in a public hotspot network. The proposed solution provides strict confidentiality to the communication in such networks.

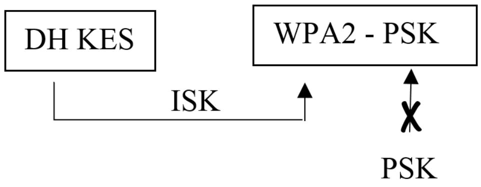

Fig. 3. Secure Hot Spot Solution

1) Formal Security Analysis using CASPER/FDR : Formal security analysis of the project was performed using FDR (Failures Divergences Refinement) - a model checker for the process algebra CSP (Communicating Sequential Processes)[10]. The CSP descriptions of the protocol was prepared using Casper [11], a compiler that produces the CSP from a more concise description. The analysis tested the protocol against various threats to ensure the secrecy of the packets exchanged between the AP and the client. FDR reported no attacks for the secrecy specification of the exchanged messages. The CASPER script used to describe the protocol is given in APPENDIX A.

- Man in the Middle (MIM) attack/Impersonation attack - MIM is handled using digital signature technology by providing a PKE (Public Key Encryption) certificate to the Access Point. Adding digital signature to the DH based key exchange protocol has been a common solution to the MIM attack. No external intruder can send spoofed messages to the client since the DH parameter exchange messages are signed by the Access Point. Messages sent from the client are also encrypted using the public key of the Access Point.
- The scheme is still vulnerable to DoS attack where an intruder(s) can continuously send connection request messages keeping the Access Point busy with the key exchange phase. Key exchange phase has some computational overhead that can be exploited to plan a DoS attack against this scheme.

The public hotspot scenario does not require authentication since it is open to all users. The protocol ensures necessary confidentiality in a hotspot.

- Storage Requirement - To store the ISKs for multiple client devices the AP requires some additional storage space. Each client stores a 32 byte ISK. For N users connected simultaneuosly, the AP requires $(32 \times N)$ bytes of additional memmory to store all the ISKs. AP maintains a log file to store the details of completed sessions. When a client is disconected, corresponding ISK will be deleted from the AP and log file is updated with the completed session details. Log file is archived periodically. Size of the file can be decided according to the period of archival.
- Computational Complexity - Time complexity of the Diffie Hellman key exchange algorithm depends on the number of bits selected for the associated values. Since the Key exchange is a one time effort it will not add much to the computational complexity. Diffie Hellman Key Exchange can be realised using various mathematical domains like modulo prime and elliptical curve system. This also affects the time complexity. There are modifications of Diffie Hellman algorithm which improves the performance considerably. In [12], Nan Li has proposed a similar key exchange mechanism using hash functions that has improved computational efficiency. In [13] ‘Uma and Azman’describe a new Diffie Hellman Key Exchange primitive based upon ‘Binary Field’. This considerably reduces the computation time. They have stated that a 1024 bit key exchange can be completed in 44.14 milliseconds, and for 512 bits it is just less than 21 milliseconds. This is a reasonable time when it is considered that the key exchange in our protocol is a one time effort per session.

IV. Future Work

Several key exchange algorithms have been proposed with improved features. Efficiency of the discussed protocol can be improved by replacing the conventional key exchange mechanism by a better approach. DoS attack is still a major threat to the proposed solution. This can be another vital area for improvement. For extended security, multiple keys can be used for extended sessions as explained by Nistala and Vankamamidi in [14] where the session key changes periodically. This can be explored for multiple keys in single session.

V. Conclusion

It is evident that the security mechanism offered by the industry for public Wi-Fi hotspot networks are not enough to provide the required protection against various attacks in different circumstances. Though WPA2 can protect a private network, it cannot be used for a public hotspot network because of the dependency on a pre-shared key (PSK). It is not possible to set a password for security in public networks where anyone can come, join and leave the network any time. Even if it is decided to set a password, that should be made available to everybody which destroys the very purpose of secrecy. This makes the network highly vulnerable to attacks. Addressing this problem, it is clear that a protocol that can meet all the security requirements of a public hotspot satisfying the limitations of such a network will be beneficial. The proposed solution tries to eliminate the dependency on a pre-shared key in such a network. When the client tries to connect to the network, the protocol generates an ISK (Instant Session Key) between the client and AP without using any pre-shared information. The established ISK is used instead of the pre-shared key in the legacy WPA2 PSK mode. The protocol derives all the security properties of WPA2 system. In addition, it provides the most necessary requirement of the hotspot network, which is network confidentiality. The proposed security protocol will have applications in various scenarios where public Wi-Fi hotspot is provided to share internet connection. The analysis of the security properties and performance of the protocol are also covered in the study.

References

[1] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. IEEE Computer Society, 2013.

[2] Stephane, "Wireless security and the ieee 802.11 standards," in *SANS Conference - London*, London, Jun. 2004.

[3] "The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards," *SANS Institute InfoSec Reading Room*, 2003.

[4] "An Overview of 802.11 Wireless Network Security Standards and Mechanisms," *SANS Institute InfoSec Reading Room*, 2003.

[5] G. Lehembre, "Wi-Fi security WEP, WPA and WPA2," *https: www.hakin9.org*, 2007.

[6] M. Mathews and R. Hunt, "Evolution of wireless lan security architecture to ieee 802.11i (wpa2)," Department of Computer Science and Software Engineering, University of Canterbury, New Zealand.

[7] B. Nada and Hossam, "Performance evaluation of the security in wireless local area networks (wifi)," Departement of computer and communication, Lebanese University, Lebanon and Departement of networks and communication services, National Instituteof Telecommunication, France.

[8] "Dependability in Wireless Networks - Can We Rely on WiFi?" *The IEEE Computer Society*, 2007.

[9] H. Peng, "Wifi network information security analysis research," Chongqing College of Electronic Engineering, Chongqing, China, Apr. 2012, pp. 2243 – 2245.

[10] A. W. Roscoe, *The Theory and Practice of Concurrency*. Prentice Hall, 1997.

[11] G. Lowe, "Casper : A compiler for the analysis of security protocols," in *10th IEEE Computer Security Foundations Workshop (CSFW'97).*

[12] N. Li, "Research on diffiehellman key exchange protocol," Information Engineering Teaching and research section, People's Armed Police Force Academy of China, Langfang, China, Apr. 2010, pp. V4–634 – V4–637.

[13] U. S. Kanniah and A. Samsudin, "New diffie hellman key exchange primitive based upon binary field," School of Computer Sciences, Universiti Sains Malaysia, 11800, Pulau Pinang, Malaysia.

[14] N. V. Murthy and V. S. Naresh, "Extended diffie-hellman technique to generate multiple shared keys at a time with reduced keos and its polynomial time complexity," Department of Computer Science, Andhra University and Department of Computer Science, S.V.K.P. and Dr. K.S.R. Arts and Science College, India.

VI. Appendix

A. CASPER script to generate CSP

#Free variables

datatype Field = Gen|Exp(Field, Num) unwinding 2

A, B : Agent

pk : Agent − > PublicKey

sk : Agent − > SecretKey

ktk : SessionKey

na, nb : Nonce

x, y : Num

expx, expy, isk : Field

text,ack,macA,macB : TEXT

InverseKeys = (isk,isk), (Exp,Exp), (Gen,Gen), (pk, sk), (ktk,ktk),(fwh,fwh)

fwh:Field X Nonce X Nonce X TEXT X TEXT − > SessionKey

#Processes

INITIATOR(A, x, na, text,macA) knows pk, sk(A)

RESPONDER(B, y, nb, ack,macB) knows pk, sk(B)

#Protocol description

$0. - > A : B$

$[A! = B]$

$1.A- > B : \{Exp(Gen, x)\}\{sk(A)\}\%expx, na, macA$

$[A! = B \ and \ expx! = Gen]$

$< isk : \ = Exp(expx, y); ktk : \ = fwh(isk, na, nb, macB, macA) >$

$2.B- > A : \{Exp(Gen, y)\}\{pk(A)\}\%expy, nb, macB$

$< isk : \ = Exp(expy, x); ktk : \ = fwh(isk, nb, na, macA, macB) >$

$3.A- > B : \{text\}\{ktk\}$

#Specification

Secret(A, text, [B])

Secret(B, text, [A])

#Actual variables

AccessPoint, Client, Mallory : Agent

X, Y, Z : Num

Text1, ACK, MACa, MACb : TEXT

Na, Nb : Nonce

#Inline functions

symbolic pk,sk,fwh

#Equivalences

forall x, y : Num . Exp (Exp(Gen,x), y) = Exp(Exp(Gen,y), x)

#System

INITIATOR(AccessPoint, X, Na, Text1, MACa)

RESPONDER(Client, Y, Nb,ACK,MACb)

#Intruder Information

Intruder = Mallory

IntruderKnowledge = {AccessPoint, Client, Mallory, Z,fwh,pk}