International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume- 2 Number-1 Issue-3 March-2012

Secure Handshake in Wi-Fi Connection (A Secure and Enhanced Communication Protocol)

Ranbir Sinha[1], Nishant Behar[2], Devendra Singh[3]
IT-GGV, Bilaspur[1], IT-GGV, Bilaspur[2], IT-GGV, Bilaspur[3]

Abstract

This paper presents a concept of enhancing the security in wireless communication. A Computer Network is an interconnected group of autonomous computing nodes, which use a well-defined, mutually agreed set of rules and conventions known as protocols, interact with one-another meaningfully and allow resource sharing preferably in a predictable and controllable manner. Communication has a major impact on today's business. It is desired to communicate data with high security. These days wireless communication has become an essential form of communication in all aspects of daily life. The main reason for this popularity among other things like the speed of communication and low cost is the convenience of managing and handling data transfer. However this communication is diminished by the insecurity of communication and unidentified intrusion into the network. This paper deals with a communication protocol that can be used in any wireless network for enhancing the security and preventing any unwanted intruders in penetrating the network.

Keywords

Security, wireless communication, intrusion, network, protocol

1. Introduction

Wi-Fi or wireless fidelity refers to a wireless LAN technology that is developed based on IEEE 802.11a/b/g or the recently ratified IEEE 802.11n. Wi-Fi is commonly used in a star configuration with a wireless access point or wireless router as a central connection point that connects all computers (palmtop, laptop, desktop) or other Wi-Fi enabled devices together, connects the wireless network to a wired network, and connects the wireless network to the Internet. A wireless network that connects via a wireless access point or a wireless router works in infrastructure mode [1].

On the other hand, a wireless network in which computers link directly to one another without an access point works in ad hoc mode. A Wi-Fi ad hoc network typically consists of two Wi-Fi-enabled computers. However, some Wi-Fi network adapters allow more than two computers to be connected in an ad hoc network.

A Wi-Fi ad hoc network functions just like Wi-Fi network in infrastructure mode. It can be used to share files, folders, drives, printer, etc. It can also be used for sharing an Internet connection or play a networked game.

Wi-Fi is a mechanism for wirelessly connecting electronic devices. A device enabled with Wi-Fi, such as a personal computer, video game console, Smartphone, tablet, or digital audio player, can connect to the Internet via a wireless network access point. An access point (or hotspot) has a range of about 20 meters (65 ft.) indoors and a greater range outdoors. Multiple overlapping access points can cover large areas.

A Wi-Fi enabled device such as a PC, Smartphone, tablet or games console can connect to the Internet when within range of a hotspot. Hotspot coverage can comprise an area as small as a single room with wireless-opaque walls or as large as many square miles covered by overlapping access points. "Wi-Fi" is a trademark of the Wi-Fi Alliance and the brand name for products using the IEEE 802.11 family of standards. Wi-Fi products that complete Wi-Fi Alliance interoperability certification testing successfully may use the "Wi-Fi CERTIFIED" designation and trademark [2].

2. Problem Domain

Unsecured Wi-Fi network (genetically known as Wireless Local Area Network or WLAN) has become a national celebrity in vamp category due to its misuse by terrorists, in the recent past.

Even Otherwise, any open and unsecured node, especially wireless, is an extremely serious security hazard for any network, whether it is corporate, personal, home or small office user. The hacker (unauthorized user or intruder or perpetrator or

criminal or terrorists breaking in any network) get access not only to your internet bandwidth, but he can send e-mails, download classified and/or confidential data/information, upload obscene material, hack into networks, initiate attack on other computers in the network or connected to internet, send malicious code to others, install a Trojan or Botnet on the victim's computer to get long term control of it through internet, etc. And this is not an exhaustive list but just a tip of the proverbial iceberg [3].

Wi-Fi networks are in the news in the recent past due to effective misuse of these by terror organizations. They have been misused as these wireless (Wi-Fi) networks have been installed unsecured. With the misuse by terrorists, unsecured Wi-Fi misuse has become national celebrity in villain and vamp categories.

In the recent past, we saw a high drama about unsecured Wi-Fi connection subscribed at his residency by an American IT Trainer Mr. Ken Haywood in Navi Mumbai. Terrorists used the internet connection, to send e-mail to authorities and news channel about the serial bomb blasts in Ahmedabad, just 5 minutes before the blasts. This strengthen the hypothesis that some members of terrorist organization were located near the unsecured Wi-Fi network connection, at least till 5 minutes before the bomb blasts at Ahmedabad.

Then on 23rd August 2008 evening, the above was re-enacted at the prestigious "Khalsa College" in Matunga, Mumbai. In this incident too, the terrorists used the unsecured Wi-Fi connection of Computer Centre of the college, to connect to their laptop or similar device; then created a Gmail account used to send a 7 pages long email with an attachment, all in a span of 6-7 minutes.

Again the same story was repeated, just 5 minutes before Delhi Blasts on 13th September 2008 when the terrorists used an unsecured Wi-Fi connection of a company at Chembur in Mumbai.

3. Proposed Work

Alfred Loo in his paper titled "The Myths and Truths of Wireless Security" wrote that "SECURITY WILL NEVER BE PERFECT as hackers can always find new methods to crack systems."

But "Nothing is impossible because Impossible itself says that I M Possible". So we should never compromise with the security of any network.

First of all, the question arises that what a person must do in order to secure his Wi-Fi. Chanakya said that "Never share your secrets with anybody otherwise it will destroy you". This mantra applies the safest security in protecting any network. Here we describe some new techniques that will enhance the security of any Wi-Fi network. We also take as an example the Wi-Fi network of our university and we will apply the proposed methods to fit the Wi-Fi security needs of our university.

Chanakya said that "Even if a snake is not poisonous, it should pretend to be venomous." The Wi-Fi networks what we use today do apply a lot of features to protect it from any type of intrusion. All the available techniques must be deployed in order to protect a Wi-Fi network. We describe below the techniques which one should follow to protect the Wi-Fi. They are as follows: -

- **Special Registration**

First, the organization which is launching Wi-Fi should register each before the user can actually use the Wi-Fi. The user should register by filling a form which will contain the basic details of the user.

The User should be asked to show any National ID and the details should be entered in the database after examining the ID. The photocopy of the ID along with the contact number of the person should be entered in the database. Also, the product ID of the system which the person will be using on the network and his thumb print should be registered and entered in the database.

After the registration is over, the user should be given an IP Address through which the user will connect to the network.

This Registration will ensure that the person using the network is an authorized citizen of our country and not a terrorist. Furthermore, the person must have his registered contact number with him when his is going to use the Wi-Fi.

- **Use of Static IP Address instead of Dynamic IP Address**

Most of the devices use dynamic IP Addresses to get connected. Devices are always identified by their IP Addresses on the network. It is very convenient to

define dynamic address assignment in any network. At the same time this will also work to the advantage of the hacker. The hacker's device will also be assigned a dynamic IP Address and get connected.

The organization must turn off Dynamic IP Address or "Obtain IP Address Automatically" or DHCP in the configuration. They must define the private IP address for each device which is given to the user during the registration process. These private IP Addresses must be provided in the configuration of the wireless router. The main goal of using this method is to block any undefined IP Address which may belong to terrorists.

- **Key Entry through Mobile Phones**

When a user wants to connect to the Wi-Fi, he is prompted a window where he enters his name, registered contact number and IP Address. After entering the Wireless router checks for the correctness of the data entered by the user. If the data is not correct, the connection to that computer is blocked. Otherwise, the router sends a code to the registered contact number of the user. The user will have to read the message and enter the passkey (code) to the window appearing on the screen. On entering the correct passkey (code), he/she is granted access to use the Wi-Fi.
The purpose of this method is to ensure that the authentic user is working on the network and not any unauthorized person.

- **Matching Product ID and Thumb Print**

The system just before granting the access, checks the product ID of the system which the person is using. The access is granted only if the product ID of the System matches with the registered product ID. In case of an unmatched product ID the system that the person is using will be blocked.
Then a window appears where it demands the person to put his thumb print. The device used for reading the thumb print must be either present in the computer which the person is using or the organization can give that device which the user must return after swapping his thumb. This thumb print will be compared with the thumb print in the database to confirm that the person is an authentic user and not an unregistered user.
So after all these formalities are done, it is confirm that the person is a valid person with all the details matched correctly.

4. Results

The following snapshots convey the results: -

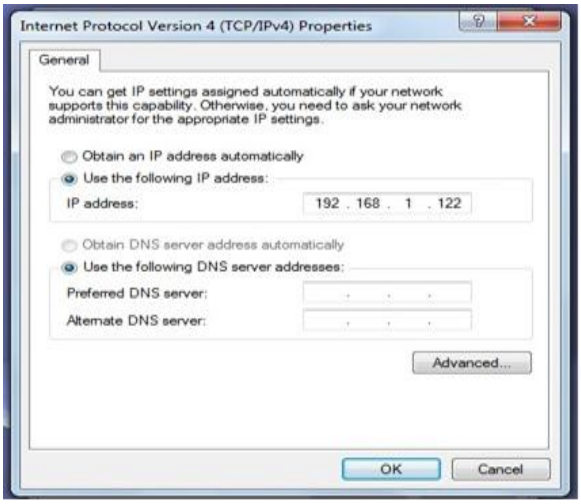

Figure 1: Static IP Address

Figure 2: Key Entry

Figure 3: Wrong Key Entry

Figure 4: Product ID Entry

Figure 5: Product ID Verification

Figure 6: Thumb Print Verification

5. Conclusion

Even all the techniques available today such as Encryption, SSL, etc. must be applied with these methods in order to secure a Wi-Fi network. We know that the hackers try hard to break any system. So timely monitoring must also be done to check the security of the system over a period of time. With timely monitoring and the proposed approaches we can have a better and secure Wi-Fi network. As discussed above, security is not a one-time job. Security is constant vigilance against threats and attacks. We need to create mechanisms in cyber systems, which will constantly monitor the weaknesses, intrusions and breaches in cyber system and take corrective action.

References

[1] For Information about Wi-Fi networks http://www.conniq.com/WinXPNetworking_wifi_direct_connection.htm.
[2] Wikipedia Website for information about Wi-Fi: http://en.wikipedia.org/wiki/Wi-Fi.
[3] R.M.Goyal & A.Goyal "Securing WI-FI Network", Centre for Research and Prevention of Computer Crimes, 2008.
[4] Nasre, Sara. "IT 6823 Information Security Instructor: Dr. Andy Ju An Wang Spring 2004." (2004).
[5] Hassinen, Timo. "Overview of WLAN security." In Proceeding of seminar on network security, TKK T-110.5290. 2006.
[6] Peter Rysavy, "Secure Wireless Networking using SSL VPNs". http://www.rysavy.com/articles/2005_aventail_wireless.pdf
[7] Lehr, William, and Lee W. McKnight. "Wireless internet access: 3G vs. WiFi?." Telecommunications Policy 27, no. 5 (2003): 351-370.
[8] Alfred Loo, "The Myths and Truths of Wireless Security", February 2008/Volume 51 No. 2 Communications of the ACM.
[9] Maxim, Merrit and Daivd Pollino. Wireless Security. McGraw-Hill/Osborne, 2002.
[10] Barken, Lee. How Secure Is Your Wireless Network? Saddle River, NJ: Prentice Hall PTR, 2004.
[11] Dubendorf, Vern A. Wireless Data Technologies. West Sussex, England: John Wiley & Sons Ltd, 2003.
[12] Nichols, Randall K. and Panos C. Lekkas. Wireless Security: Models, Threats, and Solutions. McGraw-Hill, 2002.
[13] Mallick, Martyn. Mobile & Wireless Design Essentials. Wiley Publishing, Inc: Indianapolis,

Indiana, 2003.
[14] IEEE 802.11i Working Group, WEP2 Enhancements,2001. http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/1-572.zip.
[15] Anton T. Rager. WEPCrackhomepage, 2001. http://wepcrack.sourceforge.net.

Ranbir Sinha is B.Tech Scholar in the Department of Computer Science & Engineering, Institute of Technology, Guru Ghasidas Vishwavidyalaya, Bilaspur. He is the Topper of the CSE Department with current CGPA (till 4th Semester) of 9.153. He has published papers in National as well as International Conferences in India & Abroad. His research interests lie in Computer Networks, Network Security & Cryptography. He is a Lifetime Member of International Association of Computer Science & Information Technology (IACSIT). He is a Merit Certificate Holder in Computer Science from Central Board of Secondary Education, Delhi. He is a Gold Medallist in National Cyber Olympiad 2006 and International Mathematics Olympiad 2008 conducted in INDIA.

Nishant Behar (Assistant Professor - Department of Computer Science & Engineering, Institute of Technology, Guru Ghasidas Vishwavidyalaya, Bilaspur) obtained his B.E. Degree from LNCT Bhopal (M.P.) in 1999 and M.Tech. Degree from SATI Vidisha (M.P.) in 2005. He has about 9 years of teaching experience for UG and more than 3 years for PG; he has a number of papers in various national and international journals to his credit. His field of interest is Network Security, Computing, Parallel Computing & Digital Evidence. He is a lifetime member of Indian Society for Technical Education (ISTE – Member No. LM 40800).

Devendra Singh (Assistant Professor - Department of Computer Science & Engineering, Institute of Technology, Guru Ghasidas Vishwavidyalaya, Bilaspur) obtained his B.E. Degree from LNCT Bhopal (M.P.) in 2000 and M.Tech. Degree from AAI-DU Allahabad (U.P.) in 2006. He has about 6 years of teaching experience for UG and 3 years for PG; he has a number of papers in various national and international journals to his credit. His field of interest is System Security, Sensor Networks and Cloud Computing.