International Journal of Basic Sciences & Applied Research. Vol., 3 (SP), 167-169, 2014
Available online at http://www.isicenter.org
ISSN 2147-3749 ©2014

The Study of Wpa and Wpa2 Algorithms in Wifi Technology

Mehdi Nasiri Noroozani[1*] and Hamid Reza Ebrahimi[2]

Department of Computer Science and Engineering, FiruzAbad Branch, Farashband Center, Islamic Azad University, Farashband, Fars, Iran

[*]***Corresponding Author Email:*** Nasiri@Farashband-iau.ac.ir

Abstract

Today's electronic devices such as mobile phones, laptops and other technology for communication and information sharing are relatively new WIFI. Security in data exchange is one of the main concerns of users. Companies to standardize their protocols and upgrades have been trying to solve this problem. The main research question to investigate this problem to examine the strengths and weaknesses of cryptographic protocols known as wpa and wpa2 encryption algorithms are known, respectively. Descriptive research method because of its theoretical approach - the library was determined and the results showed that the enhanced algorithm compared to their older wpa wpa2 security weaknesses more and wpa2 are also common in data exchange with wifi is a serious weakness.

Keywords: Wifi, Encryption algorithm, Wpa, Wpa2 encryption algorithm.

Introduction

Today the electronics that allow the exchange of information with other electronic devices or the Internet wirelessly, and are exposed to security threats most hackers to penetrate and Communications and different goals on their own. The electronics companies are always looking for ways to secure information and in this regard to the standardization of products in terms of encryption algorithms and security protocols have been presented. The main thing to keep updated algorithm against a variety of attacks and enhance the level of performance and the introduction of more efficient algorithm is the end users. The main objective of this study was to examine two common algorithms wpa1 and wpa2 on wireless communication technology which has been used wifi2 where we try to identify the strengths and weaknesses any users in the use of communication devices that benefit from these algorithms guide. This case it is important to know and understand algorithms no algorithm is not safe in any vehicle are one of t that kind of information sharing between other devices.

Review of literature

Bahrami and Nasr Abadi (Bahrami, 2012) in his description of the article "Security in wireless networks with protocols wpe and wpa» introduced two security protocols and describe the strengths and weaknesses of each type have been more appropriate to introduce it. Mehdi Eskandari (Eskandari, 2011) in a research paper entitled "Review and enhance the security of wireless local area networks." while introducing the local network wlan security solutions in the form of lattice and in between the two protocols wpa wpe and evaluate data.

Methodology

Because of the theoretical approach as well as the purpose of the research, descriptive research method - was selected library. First collected by major research papers have been published in recent years by studying the literature on the theoretical analysis algorithm was discussed.

Conclusion

Wifi technology is and how it works? At the airport, hotel, restaurant, library or office, you may be able to imagine today, wherever you connect to the Internet. In future wireless communication networks such extended at any time or place we'll be offering wireless internet services. Using Wi-Fi network such as a bedroom or office computers will be able to easily connect to each other.

Wireless networks use radio waves constantly. This is a piece of computer networks; the data is converted to radio waves and sends them via an antenna. On the other hand, a wireless router, the received signals and convert them to raw data, data will be understandable to computers. Very simply, the Wi-Fi system such as a pair Waki -Taki a vine you talk with your friends using the metaphor you. These appliances, small radios are able to transmit and receive radio signals.

When you talk with them, the microphone, your voice is received and combining it with radio waves, the antenna sends them. On the other hand, the target device, the signal received by the antenna is sent from your hand, reveal them, and through the speaker system, your sound will play. The transmitter output power or the power of these tools is often about a quarter watt However, their range is about 50 to 100 meters. Suppose we want to form a network between two computers that are wirelessly (like Waki -Taki) you communicate. The fundamental problem in the way the parts of it were built for voice transmission, the low rate of speed and can transfer large quantities of data in a short time. Wi-Fi radios that are used in the system, as in the previous example, the ability to write and have the receipt but the main difference is that these radios are capable in the three big differences between Wi-Fi radios and radio systems Waki -Taki typical kiwi are as follows:

- Radio System with Wi-Fi 802.11b and 802.11g standards work and practice sending and receiving on frequencies in the 2.4 GHz or 5 GHz doing. But Waki -Taki on frequencies above 49 MHz work.
- Wi-Fi radios systems will benefit from a variety of encryption techniques thereby increasing the rate of data transfer speed. The methods for 802.11a and 802.11g standards, including 802.11b standard techniques for OFDM and CCK is included.
- Wi-Fi radio that is used in the system, they have the ability to change frequencies. The benefit of this feature is that it prevents interference from nearby Wi-Fi system will also be different.

WPA protocol

Optimized version is based on WEP. All devices that are compatible with WEP can also support the upgrading of WPA. There are several ways that will support the WPA. One of these methods is that, like WEP uses a PreShare Key. With the difference the stronger the encryption algorithm is used. In this method, Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) is called. 8 to 63 characters use a key. Today there are many tools by which the EP / WPA crack at it. Another method that can be used to secure wireless networks that use WPA IEEE 802.1 xs is a plus. In this method, only computers that can connect to the Access Point are authorized to use. Then the connection is encrypted with WPA. WEP data encryption technology to make his transition in wireless networks, early in the 40-bit key used for encrypting data that is later upgraded to 128 bits however, this improvement is still easily hacked and even free software to hack WEP ready for production. You can easily search on Google to find and download software to hack WEP. WEP security is too low and should be used better technology. Why or Wi-Fi Protected Access WPA technology came into being. The improved version of WEP WPA TKIP was also used. In such a way that every time the TKIP key encryption uses a higher and it is safe. WPA also uses EAP technology. Extensible Authentication Protocol, or EAP, means "extensible authentication protocol". EAP is based on Public Key Encryption that this is a very safe way to transfer data is WPA.

WPA2 protocol

WPA2 is a security technology that is used in Wi-Fi wireless networks. Stands for Wireless Protected Access 2 WPA2 protected wireless access means. It is from 2006, replacing the previous generation WPA (Surbhi, 2013).

WPA and WEP to WPA2

WPA to replace old technology with a degree of security than WEP poorly designed. WEP stands for Wireless Protected Protocol. The home wireless network wherever possible to replace WEP to WPA2. WPA2 as the security situation improves Wi-Fi connectivity to WPA is a stronger encryption system uses. Especially in WPA2 security system will not allow the use of algorithms. These algorithms were known as WPA security holes (Pacheco, 2013).

Featuring WPA2

The study can be downloaded wpa2 technology that is based on four factors:

- Or mutual authentication (mutual authentication)
- Strong encryption (strong encryption) or
- Interoperability (Interoperability)
- Ease of Use, or (Ease of use)

Wpa2 in both corporate and household has been proposed (Chhillar, 2012).

Security researchers from different angles algorithms wpa and wpa2 the wpa2 papers had been published to the conclusion that if a strong password is used better performance as well as the encryption method is presented in two versions of home and corporate users certainly the type of company that will provide extra security. The internal structure of this cipher is described briefly and process it in the way of home and corporate procedure described Wpa2 encryption and security components listed above is also how important centers wpa2 encryption method used and noted that two of America is one of the most important centers of the University of Texas at Dallas the encryption method used to teach and engage.

References

Bahrami P, Nasrabadi M, 2012. "Security in wireless networking by wpe and wpa protocols", First National Conference on Science and Computer Engineering, Islamic Azad University of Najaf Abad, Iran.

Chhillar RS, 2012. WI-FI Security by using Proxy server. International Journal Of Computational Engineering Research. 2(5): 1408-1411.

Eskandari M, 2011. Reviewing and enhancing the security of wireless local area networks. Second National Conference on Information and Communications Technology Of Iran.

Pacheco de Carvalhoa JAR, 2013. Performance evaluation of laboratory wi-fi ieee 802.11a wpa point-to-multipoint links. International Conference on Project MANagement / HCIST.

Surbhi Gubta, 2013. Securing Wifi Network Via Proxy Server. Research Inventy: International Journal Of Engineering And Science. 3(7): 1-5.