International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Comparative Study between WEP, WPA and WPA2 Security Algorithms

Tagwa Ahmed Bakri Gali[1], Amin Babiker A/Nabi Mustafa[2]

Department of Communication Al–Neelain University

Abstract: ***This paper is a review study of the different security techniques that used to protect wireless networks from hackers. The main goal of this is to understand the concept of security techniques in the network and knowledge of the strengths and weakness points of these techniques in this field.***

Keywords: Wireless LAN, security technique, Wired Equivalent Privacy, Wi-Fi Protected Access, Wi-Fi Protected Access 2.

1. Introduction

A wireless network is a type of computer networks that uses wireless data connections for connecting nodes. Wireless networking is a method used by homes, telecommunications networks and enterprise (business) to ward off the pricey procedure of introducing cables into a building, or to a connection between various equipment locations [1]. Wireless telecommunications networks are broadly put through and administered using radio communication. This implementation takes place in the physical layer (layer) of the OSI model network structure [2].

2. Methodology

Wireless Security

Wireless security is the prevention of unauthorized access or damage to information processing systems using wireless networks.

2.1 WEP (Wired Equivalent Privacy)

It is the first encryption algorithms employed in wireless networks [3]. It fundamentals: plain text-RC4-X OR ED - Key stream.
Where the WEP Providing: Authentication-Confidentiality - Integrity -Control Access, which offers security through encryption keys. [4]

2.2 WPA (Wi-Fi Protected Access)

Because of the porosity of the WEP, the scientists had to be discovered another way. (WPA) is similar to the WEP, but the difference in encryption [5]. Where operations consist of two options:

1) AES (Advanced Encryption Standards) it is more potent than the RC4.
2) TKIP (Temporal Key Integrity Protocol) it is compatible with WEP devices, and providing security through a password.

There are two versions of WPA. Personal mode WPA has PSK authentication and TKIP/MIC encryption. Enterprise mode WPA has EAP authentication and TKIP/MIC encryption.

2.3WPA2 (Wi-Fi Protected Access 2)

The recommended solution to WEP security problems is to switch to WPA2. The WPA was an intermediate solution for hardware that could not support WPA2. Both WPA and WPA2 are much more secure than WEP. [6] To add support for WPA or WPA2, some old Wi-Fi access points might need to be replaced or have their firmware upgraded [7]. WPA was designed as an interim software-implementable solution for WEP that could forestall immediate deployment of new hardware. There are two versions of WPA2. Personal mode WPA has PSK authentication and AES/CCMP encryption. Enterprise mode WPA2 has EAP authentication and AES/CCMP encryption.

3. Results and Discussion

Comparison table between the three algorithms and the difference between them. WPA Contains message integrity verification to prevent the attacker from modifying or getting messages and make sure it is right. But the fault was identified in the WPA is the use of Short- packed for spoofing and re-injection, for that has been replaced WPA to WPA2, which uses CCMP instead of TKIP and The encryption system AES instead of RC4 with a very strong security, It is approaching that recommended security in wireless networks today [8].

WPA2 is a Wi-Fi Alliance branded version of the last 802.11i standard. The main enhancement over WPA is the inclusion of the AES-CCMP algorithm as a compulsory feature. Both WPA and WPA2 support EAP authentication methods using RADIUS servers and pre shared key (PSK) [9]. The number of WPA2 and WPA networks is increasing, while the number of WEP networks is falling because of the security vulnerabilities in WEP.

	WPA	WPA2	WEP
Stands For	Wi-Fi Protected Access.	Wi-Fi Protected Access 2.	Wired Equivalent Privacy.
What Is It?	A security protocol developed by the Wi-Fi Alliance in 2003 for use in securing Wireless networks.	A security protocol developed by the Wi-Fi Alliance in 2004 for use in securing wireless networks; designed to replace the WEP and WPA protocols.	A security protocol for wireless networks introduced in 1999 to provide data confidentiality comparable to a traditional wired network.
Methods	As a temporary solution to WEP's problems, WPA still uses WEP's insecure RC4 stream cipher, but provides extra security through TKIP.	WPA2 uses the AES standard instead of the RC4 stream cipher. CCMP replaces WPA's TKIP.	Through the use of a security algorithm for IEEE 802.11 wireless networks, it operates to create a wireless network that is as strong as a wired net.
Keys	Unique encryption Key. Uses the temporary key – TKIP.	You set up your unique encryption key.	It applies a static key.
Speed	A little processing power.	Requires greater processing power.	Not much processing power.

Figure 1: Summary comparison of protection algorithms.

4. Conclusion

These comparisons made between security techniques have sacrificed our basic concept of Wireless Networks and the strengths and weaknesses of security techniques. Where can the WEP making to give the confidentiality and dependability of the information in the same confidentiality of wired networks, but with over time we have found out some of the gaps that it was necessary to get a solution for it. This is the WPA Use the same technique in WEP, but added some secrecy like TKIP. As the WPA2 is the best in terms of their confidential and reliability attributed to the difficulty of a break and has a unique encryption key, so it needs a bit of time. This makes it a better standard to be applied in wireless LAN. It is hoped that in the continuing paper, we will suggest the solution addressing WPA2 shortcomings.

References

[1] "Overview of Wireless Communications". Cambridge.org. Retrieved 8 February2008.
[2] "Getting to Know Wireless Networks and Technology". Informit.com. Retrieved 8 February 2008.
[3] Andrea Bittau, Mark Handley, Joshua Lackey. "The Final Nail in WEP's Coffin". Retrieved 2008-03-16
[4] "An Inductive Chosen Plaintext Attack against WEP/WEP2". cs.umd.edu. Retrieved 2008-03-16.
[5] "Understanding WEP Weaknesses". Wiley Publishing. Retrieved.
[6] Jonsson, Jakob. "On the Security of CTR + CBC-MAC". NIST."Wi-Fi Protected Access White Paper". Wi-Fi Alliance. WPA is both backward-compatible and is designed to run on existing Wi-Fi devices as a software download
[7] "Wi-Fi Protected Access White Paper". Wi-Fi Alliance. WPA is both backward-compatible and is designed to run on existing Wi-Fi devices as a software download. 12. https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access.
[8] Meyers, Mike (2004). Managing and Troubleshooting Networks. McGraw Hill. ISBN 978-0-07-225665-9.
[9] https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access