A Comparative Study of Security Protocols of Wireless Networks

Kumar Pal Singh[1], Gaurav Kumar[2], Abhay N Tripathi[3]

[1]Assistant Professor, Dept. of IT, Institute of Technology and Science, Ghaziabad

[2]Assistant Professor, Dept. of IT, Institute of Technology and Science, Ghaziabad

[3]Assistant Professor, Dept. of IT, Institute of Technology and Science, Ghaziabad

Abstract

The Wireless Network has become essential and integral part of our lives. It is being used at extensive level in present scenario and increasing with great speed. Because of its nature and characteristics the wireless networks is more vulnerable in terms of information security. The information in wireless networks is present ubiquitously with lesser security platform [4]. In our previous article we focused the main and important security threats on wireless networks which were termed as CIAAS Pentagon, where CIAAS is expanded as Confidentiality, Integrity, Authentication, Availability, and Secrecy, which was driven from CIA Triad, stands for Confidentiality, Integrity, and Availability.

In this article we are broadening the horizon of various important security protocols for Wireless Networks. These protocols are studied and analyzed with their working and functionality, importance, and demerits. Finally these security protocols are compared with each other based on some important parameters.

Keywords: *Wireless Networks, Security Protocols, CIA Triad, WEP, WPA, WPA2, CIAAS Pentagon, Confidentiality, Authentication, Integrity, Secrecy, Availability, Integrity Threats, Integrity Preventions*

1. Introduction

1.1 CIA Triad

The security threats of wireless networks can impair it in terms of disturbance to a set of three critical components of wireless network that are liable to reliability and robustness of not wireless network but all kinds of computer networks also [2]. We refer it CIA Triad, where CIA is expanded as Confidentiality, Integrity and Availability Fig. 1 [1][3].

1.1.1 Confidentiality

Confidentiality is referred to protecting the information from disclosure to unauthorized user by making computer network secure.

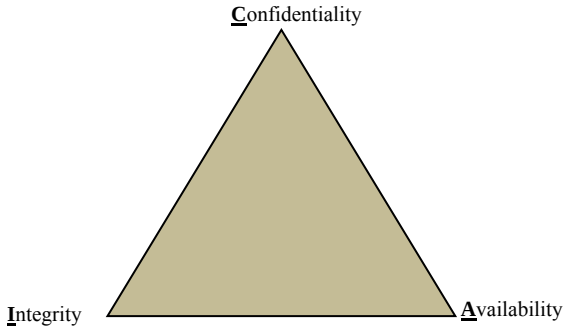

Fig1: Outline of CIA Triad

In present scenario users generally access very critical and vital information on wireless network such as banking details, credit card numbers, personal information, online transactions, trade secrets, government documents and so on. The loss or hacking of such information may lead to financial, social or personal mischief[6].

1.1.2 Integrity

Integrity of information refers to protecting information from being tampered by unauthorized users. For instance any transaction of $100 is tampered to $10,000 it can become very harmful for user.

1.1.3 Availability

Availability of network may lead to misuse of wireless two ways. The network can be accessed firstly by outside users who are not actually authorized to do for instance the network of Wi-Fi can be accessed by outsiders that is not made secure. Secondly the accessibility of network can be protected from access of authorized users if it is controlled by wrong users [8][9]

2. Security Protocols

Wired Equivalent Privacy (WEP): The original encryption protocol developed and designed for wireless networks. As its name implies, WEP was made to furnish the same level of security as wired networks. However, many known drawbacks have been figured out in WEP which is difficult to make consistent.

Wi-Fi Protected Access (WPA): Inducted as an interim security enhancement over WEP while the 802.11i wireless security standard was being developed. Pre-shared key (PSK) is used mainly by WPA which is commonly referred to as WPA Personal, and the Temporal Key Integrity Protocol (TKIP, pronounced tee-kip) for encryption. WPA Enterprise uses an authentication server to generate keys or certificates.

Wi-Fi Protected Access version 2 (WPA2): Based on the 802.11i wireless security standard, which was finalized in 2004. The great achievement and enhancement to WPA2 over WPA is the use of the Advanced Encryption Standard (AES) for encryption. The AES provides sufficient security (and approved) for use by the U.S. government to encrypt information classified as top secret — that is possibly appropriate to protect your secretes!

2.1 WEP Encryption

For WEP encryption two processes are applied to the plaintext data. One encrypts the plaintext while the other protects the data from being modified by unauthorized personnel. The 40-bit secret key is connected with a 24-bit Initialization Vector (IV) as a result 64-bit total key size. The resulting key is input into the Pseudo-random Number Generator (PRNG). The PRNG (RC4) gives an output a pseudorandom key sequence based on the input key. The resulting sequence is used to encrypt the data by doing a bitwise XOR. The result is encrypted bytes equal in length to the number of data bytes that are to be transmitted in the expanded data plus four bytes. This is because the key sequence is used to protect the 32-bit Integrity Check Value(ICV) as well as the data. The picture below describes how the WEP is encrypted.

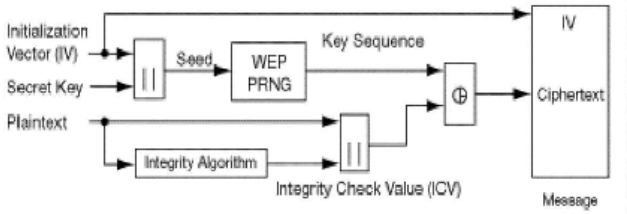

Fig 1 WEP Encryption

2.2 WEP Decryption

An integrity algorithm CRC-32 is used to prevent unauthorized data modification by operating on the plaintext to produce the ICV. The cipher text is obtained by computing the ICV using CRC-32 over the message plaintext connecting the ICV to the plaintext choosing a random initialization vector (IV) and connecting this to the secret key inputting the secret key + IV into the RC4 algorithm to produce pseudorandom key sequence encrypting the plaintext + ICV by doing a bitwise XOR with the pseudorandom key sequence under RC4 to produce the cipher text communicating the IV to the peer by placing it in front of the ciphertext. The IV, plaintext, and ICV triplet forms the actual data sent in the data frame.

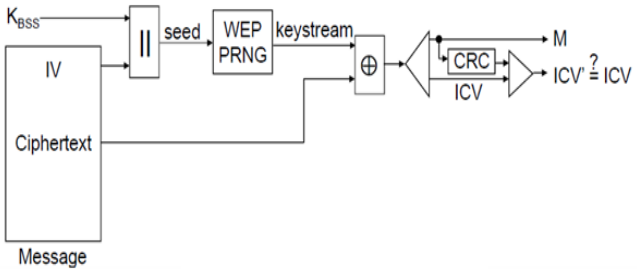

Fig 2: WEP Decryption

3. Short-comings of Security Protocols

3.1 Short-comings of WEP

3.1.1 Key Management and Key Size

The salient management features are not specified in the WEP standard, and therefore is one of its weaknesses, because without interoperable key management, keys will tend to be long-lived and of poor quality. Most wireless networks that use WEP have one single WEP key shared between every node on the network. Access Points (APs) and client stations must be programmed

with the same WEP key. Since synchronizing the change of keys is tedious and difficult, keys are seldom changed. In addition, the size of the key---40 bits---has been cited as a weakness of WEP. When the standard was written in 1997, 40 bit keys were considered reasonable for some applications. Since the objective was to protect against "casual eavesdropping" it appeared sufficient at the time. The US did not tightly control exports of 40-bit encryption, and the IEEE wanted to ensure exportability of wireless devices. The 802.11 standard does not specify any WEP key sizes other than 40 bits[22].

3.1.2 The Initialization Vector (IV) is Too Small

WEP's IV size of 24 bits provides for 16,777,216 different RC4 cipher streams for a given WEP key, for any key size. Remember that the RC4 cipher stream is XOR-ed with the original packet to give the encrypted packet which is transmitted, and the IV is sent in the clear with each packet. The problem is IV reuse. If the RC4 cipher stream for a given IV is found, an attacker can decrypt subsequent packets that were encrypted with the same IV, or, can forge packets. This means that you don't need to know the WEP key to decrypt packets if you know what the key stream was used to encrypt that packet. They sound like similar problems, but it's actually much easier to discover the key stream than it is to discover the WEP key[[22].

3.1.3 The Integrity Check Value (ICV) algorithm is not appropriate

The WEP ICV is an algorithm based on CRC-32, which is used for detecting noise and common errors in transmission. CRC-32 is an excellent checksum for finding errors, but an awful choice for a cryptographic hash The encryption systems which are better, use algorithms such as MD5 or SHA-1 for their ICVs. The CRC-32 ICV is a linear function of the message meaning that an attacker can modify an encrypted message and easily fix the ICV so the message appears authentic. The ability of modification gives encrypted packets provides for a nearly limitless number of very simple attacks. For example, an attacker can easily make the victim's wireless AP decrypt packets for him. Simply capture an encrypted packet stream, modify the destination address of each packet to be the attacker's wired IP address, fix up the CRC-32, and retransmit the packets over the air to the AP. The AP will happily decrypt the packets and forward them to the attacker. (The attack is slightly more complex than that, but to keep this paper short, we've skipped some of the details.) The biggest challenge of IV and ICV-based attacks is they are independent in respect of key size, meaning that even huge keys all look the same. The effort taken is same for the attack.[22].

3.1.4 WEP's use of RC4 is weak

RC4 in its implementation in WEP has been found to have weak keys. Having a weak key means that there is more correlation between the key and the output than there should be for good security. Determining which packets were encrypted with weak keys is easy because the first three bytes of the key are taken from the IV that is sent unencrypted in each packet. This weakness can be exploited by a passive attack. All the attacker needs to do is be within a hundred feet or so of the AP. Out of the 16 million IV values available, about 9000 are interesting to the most popular attack tool, meaning they indicate the presence of weak keys. The attacker captures "interesting packets", filtering for IVs that suggest weak keys. After that attacker gathers enough interesting packets, he analyzes them and only has to try a small number of keys to gain access to the network. Because all of the original IP packets start with a known value, it's easy to know when you have the right key. To determine a 104 bit WEP key, you have to capture between 2000 and 4000 interesting packets. On a fairly busy network that generates one million packets per day, a few hundred interesting packets might be captured. That would mean that a week or two of capturing would be required to determine the key[22].

3.1.5 Authentication Messages can be easily forged

802.11 defines two forms of authentication: Open System (no authentication) and Shared Key authentication. These are used to authenticate the client to the access point. The idea was that authentication would be better than no authentication because the user has to prove knowledge of the shared WEP key, in effect, authenticating himself. In fact, the exact opposite is true: if you turn on authentication, you actually reduce the total security of your network and make it easier to guess your WEP key. Shared Key authentication involves demonstrating the knowledge of the shared WEP key by encrypting a challenge. The problem is that a monitoring attacker can observe both the challenge and the encrypted response. From those, he can determine the RC4 stream used to encrypt the response, and use that stream to encrypt any challenge he receives in the future. So by monitoring a successful authentication, the attacker can later forge an authentication[22].

3.2 Short-comings of WPA & WPA2

3.2.1 DoS (Denial of Service)

DOS attacks like RF jamming, data flooding, and Layer 2 session hijacking, are all attacks against availability. None of the Wi-Fi security standards can prevent attacks on the physical layer simply because they operate on Layer 2 an above. Similarly none of the standards can deal with AP failure. Management Frames – report network topology and modify client behavior - are not protected so they provide an attacker the means to discover the layout of the network, pinpoint the location of devices therefore allowing for more successful DoS attacks against a network [18].

3.2.2 Control Frames – are not protected leaving them open to DoS attacks.

3.2.3 De-authentication – The objective is to force the client to re-authenticate, which coupled with the lack of authentication for control frames which are used for authentication and association make it possible for the attacker to spoof MAC addresses (for more details refer to). Mass de-authentication is also possible[18].

3.2.4 Disassociation – the objective is to force an authenticated client with multiple AP's to disassociate from them therefore affecting the forwarding of packets to and from the client [16][18]

4. Comparison of security protocols based on various parameters

Note: Table is given in Annexure-1

5. Conclusion

Wireless Network is one of the premier and fast growing technology of today's life. Due to its technological nature such as mobility, ubiquity a vast number of users, it becomes vulnerable in terms of security. The wireless network becomes an easy target for intruders. Keeping this most important aspect of wireless network security in our mind we put our efforts to study and analyze various security factors of wireless network. After putting focus on security factors we have studied and analyzed security protocols as well. In this paper the most important security protocols (WEP, WPA and WPA2) have been analyzed with their limitations and vulnerabilities. Finally a comparative study is done on all these security protocols based on some important parameters.

6. References

[1] KP Singh, Gaurav Midha, AN Tripathi, "Analytical Study of Security Threats and Security Protocols of Wireless Network" in IJCA Journal, proceedings of

[2] Network Security Fundamentals, By Gert DeLaet, Gert Schauwers, Published Sep 8, 2004 by Cisco Press.

[3] An article on "What constitutes information integrity" by S. Flowerday & R. Von Solms Nelson Mandela Metropolitan University Port Elizabeth South Africa Port Elizabeth South Africa.

[4] Arockiam .L. and Vani .B, ―A Survey of Denial of Service Attacks and its Countermeasures on Wireless Network, International Journal on Computer Science and Engineering, Vol.02, No. 05, pp. 1563-1571, 201

[5] Microsoft Technet Library, How 802.11 Wireless Works, Technical Reference,

[6] Tom Karygiannis, Les Owens, "Wireless Network Security 802.11, Bluetooth and Handheld Devices, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Special Publication 800-48.

[7] Gast, Matthew. 802.11 Wireless Networks: The Definitive Guide, Second Edition. Sebastapol, CA: O'Reilly & Associates, Inc., 2005.

[8] Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, "Wireless Network Security: Vulnerabilities, Threats and Countermeasures", International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No. 3, July, 2008.

[9] http://en.wikipedia.org/wiki/ Wireless_security.

[10] Bellardo, John and Savage, Stefan. "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions" USENIX 2003 Nov. 7 2003 <http://www.cse.ucsd.edu/%7Esavage/papers/UsenixSec03.pdf>

[11] Bulk, Frank. "Learn the basics of WPA2 Wi-Fi security".Network Computing Jan. 27 2006. http://www.informationweek.com/story/showArticle.jhtml?articleID=177105338

[12] http://en.wikipedia.org/wiki/Information_security

[13] http://itlaw.wikia.com/wiki/Information_integrity

[14] http://en.wikipedia.org/wiki/Relevance _%28 information retrieval%29

[15] Research Methods in Politics by Roger Pierce,University of York © 2008, SAGE Publications Ltd ISBN:9781412935517

[16] http://en.wikibooks.org/wiki/Fundamentals_ of_Information_Systems_Security/Information_Security_ and_Risk_Management

[17] http://msdn.microsoft.com/enus/library/ f9ax34y5%28v=vs.110%29.aspx

[18] "Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)" by Paul Arana INFS 612 – Fall 2006

[19] http://searchsecurity.techtarget.com/tip/WEP-vulnerabilities-wired-equivalent-privacy

[20] Mahmudur Rahman, Md. Asif Hassan Riyad, Md. Ibn Sinha, A.K.M Fazlul Haque Security Enhancement of WEP Protocol IEEE802.11b with Dynamic Key Management, Proceedings of the World Congress on Engineering and Computer Science 2011 Vol I WCECS 2011, October 19-21, 2011, San Francisco, USA

[21] Vulnerabilities of Wireless Security protocols (WEP and WPA2) Vishal Kumkar, Akhil Tiwari, Pawan Tiwari, Ashish Gupta, Seema Shrawne

[22] www.opus1.com/www/whitepapers/ whatswrongwithwep.pdf

Kumar Pal Singh is having 12 years of experience, eleven years in academics and one year experience in industry. Mr. Singh did B.Sc (PCM), MCA, and M.Tech (IT) and he is associated with Institute of Technology & Science, Ghaziabad as Assistant Professor (IT). The research area of Mr. Singh is computer networks, wireless networks and network security. He has published many research papers in various conferences and well reputed journals like IEEE, Springer, and IJCA etc.

Guarav Kumar is having 12 years of experience in academics. Mr. Kumar did B.Sc (PCM), M.Sc. (OR), MCA, and M.Tech (IT) and he is associated with Institute of Technology & Science, Ghaziabad as Assistant Professor (IT). The research area of Mr. Kumar is computer networks and network security. He has published many research papers in various conferences.

Abhay N Tripathi is having 12 years of experience in academics. Mr. Tripathi did B.Sc (PCM), LLB, MCA, and M.Tech (IT) and he is associated with Institute of Technology & Science, Ghaziabad as Assistant Professor (IT). The research area of Mr. Tripathi is computer networks and network security. He has published many research papers in various conferences.

Annexure-1

Table 1: Comparison of security protocols based on various parameters

Parameters /Protocol	***WEP***	***WPA***	***WPA2***
Encryption details	WEP uses the stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity. It was deprecated in 2004 and is documented in the current standard	TKIP (Temporal Key Integrity Protocol) The RC4 stream cipher is used with a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet. Used by WPA. CCMP (Counter Cipher Mode with block chaining message authentication code Protocol	WPA2-PSK (Preshared Key) is the strongest and most practical form of WPA for most home users. WPA2 is more secure than WPA because it uses the much stronger AES (Advanced Encryption Standard) protocol for encrypting packets
Authentication	Two methods of authentication can be used with WEP: Open System authentication and Shared Key authentication	IEEE 802.1X standard for network authentication. These authentication methods use the EAP (Extensible Authentication Protocol) framework to enable user authentication to an external RADIUS authentication server or to the XTM device (Firebox-DB.	IEEE 802.1X standard for network authentication. These authentication methods use the EAP (Extensible Authentication Protocol) framework to enable user authentication to an external RADIUS authentication server or to the XTM device (Firebox-DB).
Security Details	Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network	Temporal Key Integrity Protocol (TKIP) is used to wrap WEP in sophisticated cryptographic and security techniques to overcome most of its weaknesses.	Temporal Key Integrity Protocol (TKIP) is used to wrap WEP in sophisticated cryptographic and security techniques to overcome most of its weaknesses.
Data Integrity	Here, a new way to implement the CRC32 checksum algorithm in WEP encryption which will ensure better data integrity has been proposed. The Proposed Scheme is started from the authentication process[20]	TKIP includes a message integrity code (MIC) at the end of each plain text message to ensure messages are not being spoofed	To ensure that data is not changed en-route, a cyclic redundancy check (CRC-32) is created on the original packet and a 4-byte integr ity check value (ICV) is calculated.
Key Management	WEP requires each wireless connection share a secret shared key for encryption. But it does not define any key management technique [7, 8]. So each frame sent through the connection is using the same key, which will ease the task for the hackers to break the WEP encryption [9]. The use of static WEP keys many users in a wireless network potentially sharing the identical key for a long period of time is well known security vulnerability. There is no prescription for the generation and renew of key	With 802.1x, the rekeying of unicast encryption keys is optional. Additionally, 802.11 and 802.1x provide no mechanism to change the global encryption key used for multicast and broadcast traffic. With WPA, rekeying of both unicast and global encryption keys is required. For the unicast encryption key, the Temporal Key Integrity Protocol (TKIP) changes the key for every frame, and the change is synchronized between the wireless client and the wireless access point (AP). For the global encryption key, WPA includes a facility for the wireless AP to advertise the changed key to the connected wireless clients.	With 802.1x, the rekeying of unicast encryption keys is optional. Additionally, 802.11 and 802.1x provide no mechanism to change the global encryption key used for multicast and broadcast traffic. With WPA, rekeying of both unicast and global encryption keys is required. For the unicast encryption key, the Temporal Key Integrity Protocol (TKIP) changes the key for every frame, and the change is synchronized between the wireless client and the wireless access point (AP).
Vulnerability	When it comes to WEP flaws, the problem isn't RC4.	WPA/WPA2 in an attempt to determine the shared	DoS (Denial of Service) attacks like RF jamming,

	The problem is the way that RC4 is implemented. In particular, the implementation of IVs is flawed because it allows IVs to be repeated and hence, violate the No. 1 rule of RC4: Never, ever reuse a key. [a0]	passphrase. That is, because the key is not static, so collecting IVs like when cracking WEP encryption does not speed up the attack. This means that the passphrase must be contained in the dictionary you are using to break WPA/WPA2.	data flooding, and Layer 2 session hijacking, attacks against availability. None of the Wi-Fi security standards can prevent attacks on the physical layer simply because they operate on Layer 2 an above. Similarly none of the standards can deal with AP failure [21].
Infrastructure Compatability	WPA was specifically designed to work with wireless hardware that was produced prior to the introduction of the WPA protocol[8] which had only supported inadequate security through WEP. Some of these devices support the security protocol only after a firmware upgrade. Firmware upgrades are not available for some legacy devices [20]	WPA was specifically designed to work with wireless hardware that was produced prior to the introduction of the WPA protocol[8] which had only supported inadequate security through WEP. Some of these devices support the security protocol only after a firmware upgrade. Firmware upgrades are not available for some legacy devices.[21].	Same as WPA