Improvement on WPA with RSA

Sonika Mittal , Bhupesh Thakur ,Puneet Mangla
(Dept. of CSE, Lovely Professional University, Phagwara, India)
(Dept. of CSE, Lovely Professional University, Phagwara, India)
(Dept. of CSE, Lovely Professional University, Phagwara, India)

ABSTRACT

Wireless networks require very tight security so that the unauthorized users cannot exploit the information. As it is convenient for the hackers to catch wireless signals which spread in the air. Security protocols must be building in order to secure the wireless signals like WPA. The paper discusses the security weakness of Wired Equivalent Privacy (WEP) and provides with the interim and ultimate solutions: Wi-Fi Protected Access (WPA) and 802.11i standards. The paper begins with an introduction of WEP's well-known vulnerability. Many sophisticated authentication and encryption techniques have been embedded into WPA but it is still facing a lot of challenging situations. In this paper we discuss the vulnerability & weakness of WPA. This paper also present solutions or suggestions which will improve Wi-Fi Protected Access (WPA) protocol.

Keywords- **Wireless Security, WEP, WPA, RSA, encryption**.

1. INTRODUCTION

Wired Equivalent Privacy (WEP) was an encryption algorithm designed to provide wireless security for users implementing 802.11 wireless networks.

WEP was developed by a group of volunteer IEEE members. [1]

After the WEP encryption mechanism was released, it was proved (by Nikita Borisov, Ian Goldberg, and David Wagner, in 2001) to be vulnerable to multiple forms of attack. WEP uses the symmetric cryptography system called RC4 with a user-specified key (64 bits and 128 bits) to protect the data. As a result, WEP alone is not enough to protect your data.

The problems we focus on concern how a hacker could attack the network. The attack methodology is as follows:

Footprint the wireless network Locate and understand your target.

Passive attack Analyze the network traffic or break the WEP.

Authentication and authorization Determine what methods are enforced and how they can be circumvented.

Active attack Launch denial of service (DoS) attacks.[7]

2. WEP

WEP has serious flaws that under certain circumstances could permit malicious hackers to penetrate the network defenses. The Wi-Fi Protected Access (WPA) standard and subsequent WPA2 standard overcome these flaws by adding stronger authentication and encryption.

Wired Equivalent Privacy (WEP) was designed to provide the security of a wired LAN by encryption through use of the RC4 algorithm with two side of a data communication. The Research explained about problems and solutions on WEP. Some of the weakness of WEP are:

• WEP does not prevent forgery of packets.

• WEP does not prevent replay attacks. An attacker can simply record and replay packets as desired.

• WEP uses RC4 improperly. The keys used are very weak, and can be brute-forced on standard computers in hours to minutes, using freely available software.

• WEP reuses initialization vectors. A variety of available cryptanalytic methods can decrypt data without knowing the encryption key.

• Key management is lack and updating is poor.

• Problem in the RC-4 algorithm.

2.1 AUTHENTICATION AND AUTHORIZATION

Once the attacker knows information such as the SSID of the network, MAC addresses on the network, and maybe even the WEP key, they can try to establish an association with the AP. There are currently three ways to authenticate users before they can establish an association with the wireless network.

2.2 OPEN AUTHENTICATION

Open authentication usually means you only need to provide the SSID or use the correct WEP key for the AP. It can be used with other authentication methods, for example, using MAC address authentication. The problem with open authentication is that if you don't have other protection or authentication mechanisms in place, then your wireless network is totally open, as the name indicates.

Enhancements over WEP are improved data encryption (TKIP).The WPA came with the purpose of solving the problems in the WEP cryptography method. WPA was generated after WEP as WPA allows a more complex data encryption on the TKIP protocol (Temporal Key Integrity Protocol) and assisted by MIC (Message Integrity Check).[3]

3. WPA

WPA is widely used on today's Wi-Fi networks and is considered a better alternative to the original WEP (Wired Equivalent Privacy) standard. hackers found a way to break its encryption and it is now considered insecure by most security professionals. Store chain T.J. Maxx was in the process of upgrading from WEP to WPA encryption when it experienced one of the most widely publicized data breaches in U.S. history.
Security experts had known that TKIP could be cracked using what's known as a dictionary attack. Using massive computational resources, the attacker essentially cracks the encryption by making an extremely large number of educated guesses as to what key is being used to secure the wireless data.

The work of Tews and Beck does not involve a dictionary attack, however.

To pull off their trick, the researchers first discosvered a way to trick a WPA router into sending them large amounts of data. This makes cracking the key easier, but this technique is also combined with a "mathematical breakthrough," that lets them crack WPA much more quickly than any previous attempt, Ruiu said[4].

The attack, which reads encrypted traffic sent between computers and certain types of routers that use the WPA (Wi-Fi Protected Access) encryption system, was devised by Toshihiro Ohigashi of Hiroshima University and Masakatu Morii of Kobe University. Both attacks work only on WPA systemsthat use the Temporal Key Integrity Protocol (TKIP) algorithm.[5]

4. WPA with TKIP

To improve data encryption, WPA utilizes TKIP. TKIP dynamically changes keys as the system is used, and provides a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP. An important part of TKIP is that it changes the key used for each packet. This is the "temporal" part. TKIP is one of the two choices provided by both WAPs and Operating Systems (such as Windows XP) when initializing WPA protection on your wireless network. [6]

5. PROBLEM

Wi-Fi Protected Access (WPA and WPA2) is a standard by WiFi Alliance to indicate

compliance with the security protocol to secure wireless computer networks. WPA is a recommended solution to WEP security problem it runs on the same hardware that WEP does. The protocol implements the majority of the IEEE 802.11i standards, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared.

Specifically, the TKIP (temporal Key Integrity Protocol), was brought into WPA.[2]

5.1 PRE-SHARED KEY MODE

Pre-shared key mode is one of the operation modes of WPA it is also known as Personal mode. It is designed for home and small office networks that don’t require complexity of 802.11i authentication server. Each wireless network device encrypts the network traffic using a 256 bit key. This key may be entered either as a string of 64 hexadecimal digits, or as a passphrases of 8 to 63 printable ASCII characters. Shared-key WPA is vulnerable to password cracking attacks if a weak passphrase is used.

To protect against brute force attack, a 13 character truly random passphrase is sufficient.

5.2 FLAWS IN WPA

WPA had done an excellent job for patching the problems in WEP. But there were some flaws in this which are described as:-

One flaw allowed an attacker to cause a denial-of-service attack, if the attacker could bypass several other layers of protection. [8]

While TKIP & Michael significantly improve WEP security, design limitations result in cryptographic weaknesses[10].

TKIP designers do not expect a potential successful attack on WPA is not expected to be simple or cheap.

Another flaw exists in the method with which WPA initializes its encryption scheme. Consequently, it's actually easier to crack WPA than it is to crack WEP. [9]

Other is it is not secure to use WPA.

6. PROPOSAL

The most recent physical security protocol, Wi-Fi Protected Access (WPA) and the emerging 802.11i standard, both specify 802.1 x securities as a framework for strong wireless security. 802.1x use authentication, it requires user to provide credentials to security server before getting access to the network. The credentials can be in the form of user name and password, certificate, token or biometric. The security server authenticates the user's credentials to verify that the user is who he or she claims to be and is authorized to access the network. The security server also verifies that the access point is a valid part of the network.

This is done to protect the user from connecting to an authorized access point that may have been set ups to fraudulently capture network data.

6.1ASYMMETRIC ENCRYPTION

This method employs a pair of keys, consisting of a public key and a private key. The algorithm used in asymmetric encryption, such as RSA are usually based on solving number theoretical problems. The security of these algorithms is assured by the inherent difficulty of solving such problem. Example is decomposing large amount into their prime factors.

Asymmetric is more acceptable solution for e-commerce, the world is currently promoting encryption as the transaction without the prior requirement to exchange key or secrets. The e-commerce world is currently promoting asymmetric encryption as the solution to all the security need. The advantage of asymmetric is in its functionality. It provides security in awide range of applications that cannot be solved using only symmetric techniques.

However, we pay a price for this in a computational efficiency and increased cost. The following figure shows the typical Asymmetric encryption.

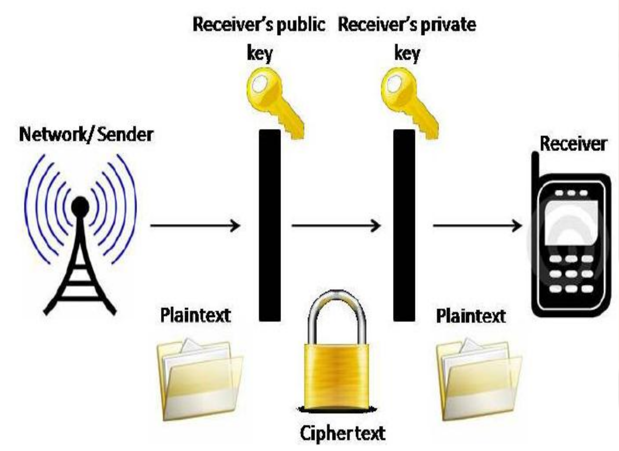

FIG 1:Asymmetric encryption

6.2RSA AS ASYMMETRIC

RSA (Rivest, Shamir and Adleman) is widely used public key stream. It is an asymmetric key system, which uses variable key sizes. 512-bit, 1024-bit and 2048-bit RSA are the most common. Its security lies in the difficulty of factoring large composite integers. Although RSA is the most popular Asymmetric cryptography.[2]

RSA is an advantage that can be gained from smaller parameters included in speed and smaller keys or certificates. These advantages are specifically important in environments where at least one of the following resources is limited:

Power consumption

Processing power

Storage space

Bandwidth

6.3 METHODOLOGY

Theproposedalgorithmwewilluseformakethepasswordbasedauthenticationbetweenthe two wirelessnodesusingthepublickeycryptographictechnique.Inthisalgorithmwefollowthefollowingstepsthathelpsinmakesthepasswordbasedauthenticationbetweentwonodes.

Algo

```
/*SiandDiaretheMobileStationSireferstosourcenode.
Direferstodestinationnode.*/

{
    1.  RequestsendbySitoitsBaseStationB1
    2.  TheBaseStationwilllookthepathfortheDestinationNodeBaseStation.ItwillperformtheRoutingbetweensourceandthedestinationbasestation
    3.  DatawillbetransferredfromtheEfficientShortestpath
    4.  OntheReciverside
Publickey&privatekey

pr=privatekey(Di)

pu=publickey(Di)

    5.  SendpublictoSi
    6.  BaseStationwillperformtheSecureKeyExchangeBetweenNodes
    7.  ThepublickeyarrivedatSourceNodeSi
    8.  Encode thepacketofsourceSibyusingpublickey
    9.  Sendtheencodedpackettothedestinationside.
    10. Onthereceiverside
    11. Decodetheencryptedpacketbyhelpoftheprivatekeyondestinationside.
    12.  Exit
}
```

7. RESULTS

So the result by implementing RSA with WPA is that

- Provides extremely strong wireless security for the 2003 computing environment.
- Adds authentication to WEP's basic encryption
- It increases the performance
- It increases the security
- It increases the complexity due to which it will take more time to crack or it becomes difficult to crack.
- The SSL layer will provide the RSA based Cryptography along with authentication. In this system we have provided 2 level of authentication using public key cryptography for the authentication and then secure communication using SSL Tunnel. The system will minimize the packet loss over the network with authenticity.
- RSA is more secure because of the reason that the assumption that factoring a big number (n into p, and q) is hard. And thus it is difficult to determine ϕ (n). Without the knowledge of ϕ (n), it would be hard to derive d based on the knowledge of e.
- The security is maintained which is the major concern.

8. CONCLUSION

At first, we explain the structure of WEP in sender and receiver side and describe all steps verbally and practically at the same time as a brief of our previous paper on the first generation of wireless security protocols.

Secondly, we discuss about the second generation of wireless security protocol as WPA and try to describe all major Improvements on WPA such as cryptographic message integrity code or MIC, new IV sequencing discipline, per-packet key mixing function and rekeying mechanism. Finally, explain about the major problem on WPA that happed in the PSK part of algorithm and other flaws. Through which I have concluded that WPA needs to be made more secure for the network privacy.

Then we explain the improvement that has done in this protocol for solve the WPA major problem.

ACKNOWLEDGMENTS

I am very thankful to my Dissertation mentor Mr. Puneet Mangla, who guided me time to time in developing my research related work. Because of my mentor kind support and a very good knowledge of the subject, it becomes possible to complete my research. I also want to say thanks to some of my friends who helped me when I was unable to move further in my research topic. And finally God and my parents, due to them I am able to stand at this stage in all respects. Thanks to all of you.

REFERENCES

JOURNALS:

[1] “*The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards*”,Stanley Wong,GSEC Practical *v1.4b.May 20, 2003*

[2] *“Wi Fi Protected Access-Pre-Shared Key Hybrid Algorithm*”, Maricel O. Balitanas, *International Journal of Advanced Science and Technology,Vol. 12, November, 2009.*

Conferences:

[3] “*A Survey on Wireless Security protocols (WEP,WPA and WPA2/802.11i*)”, Arash Habibi Lashkari, Mir Mohammad Seyed Danesh ,Behrang Samadi, iccsit, *pp.48-52, 2009 2nd IEEE International Conference on Computer Science and Information Technology, 2009*.

[4] http://www.pcworld.com/businesscenter/article/153396/once_thought_safe_wpa_wifi_encryption_is_cracked.html

[5] http://www.zdnet.com/blog/btl/researchers-crack-wpa-wi-fi-encryption-in-60-seconds/23384

[6] http://www.dslreports.com/faq/11274

[7] http://technet.microsoft.com/en-s/library/bb457019.aspx

[8] http://support.netgear.com/app/answers/detail/a_d/1105/~/what's-new-in-security%3A-wpa-(wi-fi-protected-access)

[9] http://www.wpacrack.com

[10] “*Weaknesses in the Temporal Key Hash of WPA*”, Vebjørn Moen, Håvard Raddum, and Kjell J. Hole

[11] “*WPA2 and WPA*”, implementation white paper