International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 2– No.1, May 2012 – www.ijais.org

Technologies to Overcome from Intimidation of Wireless Network Security

Kuljeet Kaur
Lovely Professional University
School of Computer Applications
Systems and Architecture Domain

ABSTRACT
Inbuilt physical security in wireless networks is not obtainable and unfortunately these are more prone to attacks from intruders. Resources are easily accessible, once an unauthorized access is gained. Paper elucidates numerous attacks which an intruder could use to detect and connect to the wireless network. Focus of the paper is on two technologies Wired Equivalent Privacy (WEP) and IEEE 802.1X Authentication which would secure wireless network from unauthorized access or intimidation. Complete process and authentication components used by WEP and IEEE 802.1X are elaborated in the paper. Detailed understanding for the client is generated in the paper for planning the wireless security. Paper analyzes the pros and cons of WEP and IEEE 802.1X and suggests the best practices for securing wireless networks. I have tried to generate an idea that how wireless security could be enhanced through this paper and best practices are also suggested by me.

General Terms
Wireless Networks, Unauthorized Access

Keywords
Wired Equivalent Privacy, Wireless Network Security

1. INTRODUCTION
Intruders can easily access resources from wireless network when unauthorized authentication is successfully done. Attacks like eavesdropping, masquerading, denial of service attack and man in the middle attacks, are performed by the intruders on the wireless networks. Because of the attacks performed by the intruders requirement of the security originates in the wireless network. Certain technologies like WEP, IEEE 802.1 Authentication are used by intruders after detecting and connecting the wireless network for security. Paper elaborates upon the process and authentication components which are used by these technologies for securing wireless networks. These technologies have various pros and cons which affects the security of the wireless networks so the focus of the paper is on those technologies and tools along with their pros and cons.

As there are numerous technologies which assure the security of the wireless network so it becomes difficult for client to establish the trust relationship. Paper suggests the best practices to the clients for securing wireless networks.

Remaining sections of the paper are Section II talks about attacks used by intruders to detect and connect to wireless network, Section III elucidates the WEP and IEEE 802.1X technologies for securing wireless network Section IV states the process and authentication components used by WEP and IEEE 802.1X, Section V elucidates that how to plan for wireless network security, Section VI elaborates the pros and cons of WEP and IEEE 802.1X, Section VII concludes the paper in which I have stated the best practices for securing wireless networks and Section VIII specifies the references of the paper.

2. ATTACKS USED BY INTRUDERS TO DETECT AND CONNECT TO WIRELESS NETWORK
There are various attacks to detect and connect to the wireless networks. Paper focuses on the following attacks which are used by most of the intruders to hamper the security of the wireless networks:

- Eavesdropping (unauthorized access is done when message transfer from wireless computer to wireless access point (WAP) [1].
- Masquerading (impersonation is done by the intruder as an authorized wireless user) [2].
- Denial of Service Attack (to deny legitimate users access to particular resources. False verification information of the legal user can be updated by the attacker for the next login phase. Later on the legal user would not be able to login successfully. A malicious user intentionally disrupts service to a computer or network resource) [3].
- Man in the Middle Attack (An attacker intercepts (views or modifies) sensitive data sent to or received by a user from the router in an untrusted public network, by deploying injections, key manipulations and filtering etc. This attack is possible when different clients share the same secret or the intruder could generate fake security certificate or the attacker is able to modify the payload of the packets by recalculating the checksum etc) [4].

Attacker starts the attack through the actual wireless computer; this computer is connected to a wireless network which is untrusted. To secure wireless networks and its connections, all wireless communication has to be authentic and encrypted, and administrators are responsible for authenticity.

3. WEP AND IEEE 802.1X FOR SECURING WIRELESS NETWORK
Two technologies Wired Equivalent Privacy (WEP) and IEEE 802.1X Authentication for the security of the wireless network are discussed in this section. A comparative analysis is done in Table 1 so that user can generate an idea that which of the technology could be used to enhance wireless security. Overall analysis of Table 1 states that with the use of IEEE 802.1X Authentication the encryption of WEP becomes

stronger and it is more intricate for an intruder to break this WEP encryption.But if WEP alone is used then there are many tools available in the market which could be used to decipher WEP encryption so that wireless traffic could be captured and analyzed.

One of the major attacks performed by the intruder in wireless network is eavesdropping. In order to provide protection from this casual eavesdropping WEP has various options [5]:

- 64-bit encryption (Length of the encryption key defines the degree of encryption which is provided to the secure transmissions)
- 128-bit encryption (It provides more security than 64-bit encryption)
- No encryption (All transmissions are performed in the clear text)

But the components used in IEEE 802.1X Authentication are [6]:

- EAP-TLS Authentication (Public key certificates are used to authenticate the RADIUS)
- Protected EAP (PEAP) Authentication (username and password is used to authenticate clients)
- RADIUS Service (used to authenticate dial up users and wireless users when they attempt to connect to the network)

Both of these technologies are used in the wireless network for strengthening security.

Table 1: Comparative Analysis of WEP and IEEE 802.1X Authentication

Parameters of Comparison	**WEP**	**IEEE 802.1X**
Authentication	Uses shared key for encryption of the messages. It has stream ciphering	Protects from casual eavesdropping.
Shared Key	Shared key in WEP enables wireless communication to be easily encrypted and decrypted [5]	Used to address the weaknesses of WEP [6].
Security and Privacy	Clarifies that WEP was designed for providing the data privacy.	Uses EAP to provide fully authenticated communication between WAP and RADIUS.
Secrecy of the Key	Does not work well when high level of security is required because secret key of WEP could be easily discovered by minutely analyzing the wireless traffic.	Encryption keys could be regularly changed in WEP if IEEE 802.1X is used because EAP regularly produces new encryption keys.
Encryption and Decryption	Moreover tools are also available in the market which can be used to decipher WEP encryption.	With the use of it the encryption of WEP becomes stronger and it is more intricate for an intruder to break it.

This comparative analysis of WEP and IEEE 802.1X Authentication in Table 1 has proved that complete security of the wireless network could be there if IEEE 802.1X Authentication is used. Because with the use of IEEE 802.1X Authentication, the data encrypted by using WEP becomes stronger.

4. PROCESS AND AUTHENTICATION COMPONENTS USED BY WEP AND IEEE 802.1X

Process followed by WEP for securing the transmissions is [7]:

i. Plain text message is passed through CRC-32 integrity check algorithm to generate integrity check value (ICV) (Fig 1)
ii. ICV is appended to the end of plaintext message (Fig 1)
iii. Random 24-bit initialization vector (IV) is produced (Fig 1)
iv. IV is added to the beginning of secret key
v. IV is used to create value for WEP pseudorandom number generator (PRNG)
vi. WEP PRNG produces encrypting cipher stream (ECS) (Fig 1)
vii. ECS is XOR'ed with message to create WEP ciphertext (Fig 1)
viii. WEP ciphertext is added with IV and then sent
ix. Each frame uses new IV which means each key has different value

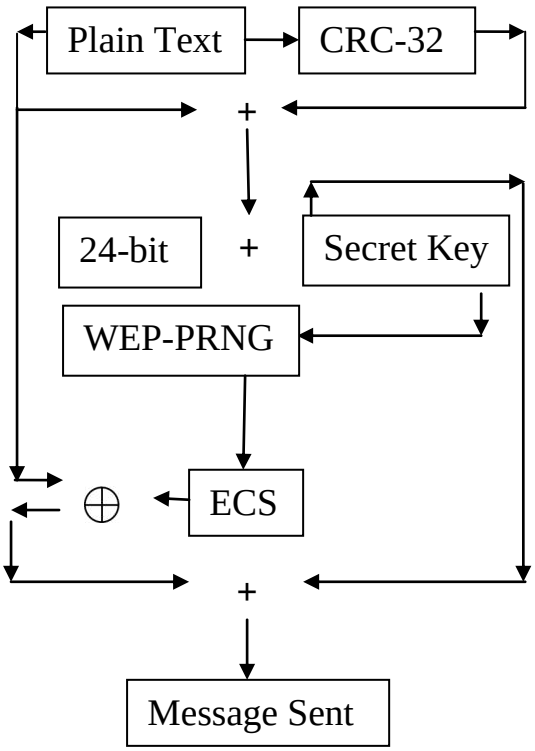

Fig 1: Process of WEP for securing the transactions

When IEEE 802.1X Authentication is used then WEP has open and shared key authentication for this process [8]. Fig 1 shows the complete process followed by WEP for securing transactions. Components used in IEEE 802.1X Authentication are EAP-TLS, PEAP and RADIUS.

Process that is followed by IEEE 802.1X Authentication is [9] [10]:

i. Clients attempts to connect to WAP through network key for proving authenticity to the network
ii. WAP creates channel to enable the client to communicate with RADIUS
iii. For checking RADIUS authenticity the client verifies public key certificate of RADIUS
iv. For client side authenticity public key certificate of client is verified for using EAP-TLS
v. If PEAP authentication is to be used the TLS is established between client and RADIUS
vi. Security credentials are sent by client to RADIUS once TLS is established
vii. RADIUS verifies these credentials and if authenticity is proven access is granted
viii. Information of access granted is sent by RADIUS to WAP
ix. Secret key is used to encrypt and decrypt communication between client and WAPAbove stated is the process and authentication components used by WEP and IEEE 802.1X Authentication.

5. SUGGESTIONS OF THE PAPER: HOW TO PLAN FOR WIRELESS NETWORK SECURITY

There are various technologies which could be followed for securing wireless network. So proper planning is required before the administrator starts the task of securing wireless networks [7]. Few issues which need clarification when planning of wireless security is done are [8] [9] [10]:

i. Which protocol to be used, either Wi-Fi Protected Access (WPA) or Wired Equivalent Privacy (WEP)
ii. Hardware needs if WPA is selected and type of encryption (64-bit or 128-bit) if WEP is selected
iii. Whether IEEE 802.1X Authentication would be used or not
iv. Whether Media Access Control (MAC) address filtering would be used to limit wireless access based on MAC addresses
v. Whether group policy would be used to configure wireless client security settings or would be manually configured
vi. Whether monitoring of wireless network security strategies is required or not

If above stated issues are handled well then it becomes easy for administrator to plan wireless network security.

6. PROS AND CONS OF WEP AND IEEE 802.1x DERIVED IN THE PAPER FROM LITERATURE REVIEW

In Section III the technologies which could be used for securing wireless network are mentioned. But there are certain pros and cons which are associated with the use of these technologies. Whenever administrator uses these technologies following pros are there [7] [8] [9] [10]:

i. WEP provides basic security for applications and IEEE 802.1X Authentication is there for high level security
ii. Shared key is used in both the technologies so transmission privacy is ensured
iii. Only XOR gate is used for ECS and plain text and this addition is sent as message.
iv. Transmission integrity is ensured by CRC-32 checksum

Table 2: Comparison between WEP and IEEE 802.1X Authentication on the basis of their advantages and disadvantages

Comparison	WEP	IEEE 802.1X Authentication
Implementation	Easy to implement	Easy to implement
Time	Too time consuming	It is less time consuming
Security Applications	WEP provides basic security for applications	IEEE 802.1X Authentication is there for high level security
Shared Key	Shared key is used in this technology so that transmission privacy is ensured	Shared key is used in this technology so that transmission privacy is ensured
Gate Applications	Only XOR gate is used for ECS and plain text and this addition is sent as message.	Clients attempts to connect to WAP through network key for proving authenticity to the network
Cryptography	Weak cryptography in WEP as secret key could be easily discovered by analyzing captured traffic	WEP is inadequate for WLAN security; it has to be used together with IEEE 802.1X Authentication
Implementation of technologies	Implementation of technologies on all access points and on all clients for its smooth operation	Implementation of technologies on all access points and on all clients for its smooth operation
Change in Secret Key	WEP provides no mechanism to change secret key	IEEE 802.1X Authentication provides mechanism to change secret key
Implementation after change in the Secret Key	No provision of any change in the secret key	If secret key is changed it has to be implemented on all access points and clients simultaneously

The cons which an administrator faces are [8] [9] [10]:

i. Weak cryptography in WEP as secret key could be easily discovered by analyzing captured traffic
ii. WEP is inadequate for WLAN security; it has to be used together with IEEE 802.1X Authentication
iii. Implementation of technologies on all access points and on all clients for its smooth operation
iv. WEP provides no mechanism to change secret key but IEEE 802.1X Authentication provides
v. If secret key is changed it has to be implemented on all access points and clients simultaneously

Table 2 generates a comparison between both the technologies on the basis of their advantages and disadvantages.

Above stated are the pros and cons which WEP and IEEE 802.1X Authentication which are faced by administrators while securing wireless networks.

7. CONCLUSION OF PAPER BY SUGGESTING BEST PRACTICES FOR SECURING WIRELESS NETWORKS

From the discussion of technologies for securing wireless network it is generated that certain practices are to be recommended for strengthening the security of wireless networks. So according to me Intimidation has to be reduced with the use of these technologies, so best practices suggested are:

i. Security features of available wireless devices are to be studied
ii. Any updates if released by the vendors are to be checked regularly and implemented through firmware
iii. Router or firewall has to be in isolated place than complete wireless network
iv. Limit the number of hosts by using extended subnet mask
v. Minimize the wireless zone size by installing more access points
vi. Placement of access points should be in the center of the building rather than near windows
vii. Wireless device should support IEEE 802.1X Authentication which uses EAP
viii. Wireless Access points and adapters should support firmware, MAC filtering and up to 128-bit encryption
ix. Only purchase those devices which support dynamic WEP

x. Change password regularly in order to manage all access points and adapters

xi. Do not use shared key encryption

The paper concludes with the above stated recommended practices which an administrator should follow in order to overcome the intimidation of wireless network security.

8. REFERENCES

[1] Vipul Goyal, Virendra Kumar, Mayank Singh, Ajith Abraham and Sugata Sanyal ," CompChall: Addressing Password Guessing Attacks," http://eprint.iacr.org /2004/136.pdf , 2003

[2] David A. McGrew and Scott R. Fluhrer ,"Multiple forgery attacks against Message Authentication Codes," eprint.iacr.org/2005/161.pdf ,Cisco Systems, Inc., May 31, 2005

[3] Craig A. Huegen, "Network-Based Denial of Service Attacks," www.pentics.net/ denial-of-service/presentations/.../19980209_dos.pp...

[4] Alberto Ornaghi, Marco Valleri ,"Man In the Middle Attacks Demos," in BlackHat Conference, USA 2003

[5] "Wired Equivalent Privacy", http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

[6] "IEEE 802.1X Authentication", http://www.ja.net/documents/publications/factsheets/064-ieee.802.1x.pdf

[7] "Process and Authentication components used by WEP", www.airscanner.com/pubs/**wep**.pdf

[8] Adam Stubblefield, John Ioannidis, Aviel D. Rubin," Using the Fluhrer, Mantin, and Shamir Attack to Break WEP,"AT&T Labs – Research, Florham Park, NJ. www.isoc.org/isoc/ conferences/ndss/02/papers/stubbl.pdf

[9] "Process and Authentication components used by IEEE 802.1X Authentication", www.sans.org/.../authentication/authentication-authoriza... - United StatesSimilar

[10] Configuring IEEE 802.1x Port-Based Authentication," Catalyst 3750 Switch Software Configuration Guide," http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_40_se/configuration/guide/sw8021x.pdf