IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-I, Issue-3 E-ISSN: 2347-2693

# Wireless Network Security: Susceptibilities, Extortion and kiosk

Mohd. Amjad*

*Deptt. Of Computer Engineering, F/o Engg. & Technology, Jamia Millia Islamia, New Delhi*
*E-mail: amjad2k8@gmail.com*

www.ijcaonline.org

Received: 07 Nov 2013 Revised: 14 Nov 13 Accepted: 26 Nov 13 Published: 30 Nov 2013

***Abstract—***Wireless networking brings a whole new meaning to network security risk analysis and mitigation. With readily available equipment, attacks on wireless networks are very easy. The wireless security mechanism is not same as in wired networks. Because there is no user controlling for each individual node, wireless environment, and more importantly, scarce energy resources. The wireless security mechanism is not same as in wired networks. Because there is no user-controlling for each individual node, wireless environment, and more importantly, scarce energy resources. This paper looks at the basic risks inherent in wireless networking security protects a wireless network by denying access to the network itself before a user is successfully authenticated. This paper proposed a new security model which addresses three important types of active attacks like Rushing attack, Black hole and Replay attack. By using 3-roundof well known AES algorithm we implement this model. Thus it is easy for the administrator to identify these attacks using WPA. Different types of attack there related information, different cryptographic strength and performance of the proposed model get analyzed in this system. One particularly important improvement over the WPA standards is the inclusion of the Advanced Encryption Standard (AES) which could be used in many rounds to protect the overall network from the external attacks.

***Index Term***— Wireless Network, Wireless Security, Wireless Threats, WEP, RC4, AES, IEEE 802.11, WPA

## I. Introduction

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Wireless networks have properties that imply different security solutions for wired and wireless networks [1][5][6]. They use the same networking protocols but use specialized physical and data link protocols. It

- Connect to existing networks via access points which provide a bridging function
- Let you stay connected when roaming from one coverage area to another
- Have unique security considerations
- Have specific interoperability requirements
- Require different hardware
- Offer performance that differs from wired LANs

Some basic measures securing the wireless network against casual access by intruders attacks such as changing both the access points (AP), factory default administration key and service set identifier (SSID), updating the APs to support Wi-Fi protected access (WPA) or Wi-Fi protected access 2 (WPA2) security, disabling the SSID broadcast to prevent connecting non-authorized users, filtering the media access control address to allow known station only connection and adjusting transmitting power to restrict coverage to that which is strictly required. Truly effective measures for protecting a wireless network must include encryption and authentication [2][3]. Regarding encryption, WLAN hardware options are (in order of security encryption strength) wired equivalent privacy (WEP), WPA and WPA2. WEP is considered unsafe whilst WPA and WPA2 provide suitable security levels. The main difference between WPA and WPA2 is that the former supports encryption using temporal key integrity protocol (TKIP) whilst the latter supports encryption using advanced encryption standard (AES). Both WPA and WEP use the Rivest Cipher 4 algorithm but WPA outperforms WEP because the encryption key changes dynamically for WPA. WEP is an optional security mechanism for protecting wireless. WEP was included in clause 802 of the first version of 802.11 IEEE and has remained unchanged in newer versions of IEEE 802.11 b, 802.11g, 802.11a for ensuring compatibility amongst different versions. WEP is a standard encryption system implemented at the MAC level and is supported by most wireless solutions. WEP establishes a similar level of security to that of wired networks using encryption of the data being transported by the radio signals [4]. WEP uses the RC4 algorithm developed by RSA Data Security. WEP is also used for preventing unauthorized users from gaining access to WLANs i.e., provides authentication; such purpose is not explicitly set out in 802.11 but is considered an important feature of WEP.

Corresponding Author: *Mohd. Amjad**

Specific threats and vulnerabilities to wireless networks include the following [9][10]:

- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- Malicious entities may gain unauthorized access to an agency's computer network through wireless connections, bypassing any firewall protections.
- Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed.
- DoS attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade as them on internal or external corporate networks.
- Sensitive data may be corrupted during improper synchronization.
- Malicious entities may be able to violate the privacy of legitimate users and be able to track their movements.
- Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) to surreptitiously gain access to sensitive information.
- Handheld devices are easily stolen and can reveal sensitive information.
- Data may be extracted without detection from improperly configured devices.
- Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.

Wireless technologies generally come with some embedded security features, although frequently many of the features are disabled by default. As with many newer technologies, the security features available may not be as comprehensive or robust as necessary. Because the security features provided in some wireless products may be weak, to attain the highest levels of integrity, authentication, and confidentiality, agencies should carefully consider the deployment of robust, proven, and well-developed and implemented cryptography. NIST strongly recommends that the built-in security features of 802.11in data link level encryption and authentication protocols be used as part of an overall defense-in-depth strategy. Although these protection mechanisms have weaknesses described in this publication, they can provide a degree of protection against unauthorized disclosure, unauthorized network access, and other active probing attacks.

## II. ENCRYPTION IN WEP

WEP uses a secret key shared between a wireless station and an access point. All data sent and received between station and access point can be encrypted by using the "shared key." 802.11 do not specify how the shared key should be established but allows for a table associating a unique key with each station [6][7]. However, the same key is usually shared in practice amongst all stations and access points within a given WLAN system. WEP applies a cyclic redundancy check (CRC-32) to plaintext to protect cipher text against unauthorized modifications while it is in transit, producing an integrity check value (ICV). ICV is a type of fingerprint for plaintext; it is added to plaintext and the result is encrypted with a "key stream" and sent to the recipient along with the initialization vector in plaintext

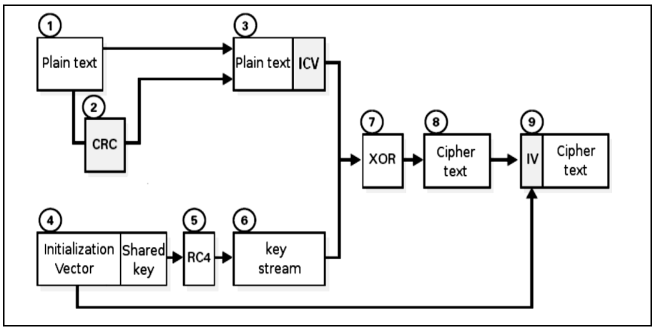

Fig.1. WEP Encryption.

The receiver combines the cipher text with the key stream to retrieve both the plaintext and the ICV [5][6]. It is possible to verify that the decryption process has been correct and that the data has not been altered by applying the integrity check to the plaintext and comparing the output with the ICV value received; if the two ICV values are identical (i.e., matching fingerprints) the message is authenticated .

### II.I WEP Encryption Algorithm using RC4 cryptography

RC4 (or ARC4) is the most frequently used stream cipher in cryptography; it is used in some of the most popular protocols such as transport layer security (TLS) or secure socket layer (SSL) to protect Internet traffic and wired equivalent privacy (WEP) to add wireless network security. Using WEP is not recommended in modern systems; however, some RC4 based systems are safe enough for common use. The RC4 cryptography algorithm was designed by Ron Rivest of RSA Security in 1987; its full name is Rivest Cipher 4, taking the alternative acronym RC for "Ron's Code" which is used by RC2, RC5 and RC 6 encryption algorithms. RC4 is part of the most commonly used encryption methods such as WEP, TKIP (WPA) for wireless cards and TLS [6][7][8]. RC4's substantial speed and simplicity are among the main factors that have helped it to be used in such a wide range of applications. RC4 generates a pseudo-random stream of bytes (key stream) which is XOR added to the plain text for encryption. Deciphering the message is done in the same way. To generate the key stream, the encryption algorithm has an internal secret state consisting of the following:

• A permutation of 256 bytes called S vector or simply “S”;
• Two 8-bit index pointers: *i* and *j*; and
• The permutation is initialized with a variable-length key, usually 40-256 bits, using a key scheduling algorithm (KSA). Once key scheduling is done, the ciphering “key stream” is produced by means of a pseudo-random generation algorithm (PRGA). RC4 uses two blocks for encryption: KSA and PRGA. The following is RC4’s pseudo-code:

```
/ * $S$ = S VECTOR with fixed 256 bytes * /size
/ * $K$ = VECTOR which contains the seed ,$L$ = length of seed (IV length plus SK length) , $N$ = 256, S vector size * /
KSA ($K$, $S$)
FOR ($i = 0$ to $N - 1$)
$S[i]= i$ (1)
$j = 0$
FOR (i = 0 to $N - 1$) (2)
$j = (j + S[i] + K[i \bmod L]) \bmod N$ SWAP($S[i]$, $S[j]$)
PRGA($S$)
$i = 0$ ,j=0 (3)
Frame production loop
$i = (i + 1) \bmod N$ (4)
$j = (j + S[i]) \bmod N$
SWAP($S[i]$, $S[j]$)
OUTPUT = $S [(S[i] + S[j]) \bmod N]$
```

The previous pseudo-code assumed that the seed vector $K[i]$ contained values [4, 5, 6, 7,8, 9, C, Z] at the respective positions for $i$ from zero to seven. A 256 position memory block is allocated for the S vector for KSA. The two pointers to the S vector, $i$ and $j$ are initialized to zero. Then $j$ is relocated into a pseudo-random position depending on seed vector $K$ content.

$j = j + S[0] + K[0] = 0 + 0 + 4 = 4$

Then there is a swapping of the values in the S pointed by $I$ and $j$. This is done 256 times for each frame which must be encrypted. As a result, if the value of the seed vector $K$ is not known, it is not possible to know the final contents of the $S$ vector in advance.

## III. WPA (WI-FI PROTECTED ACCESS)

WPA encryption and integrity verification (Wi-Fi protected access) is based on the temporary key integrity protocol (TKIP) defined in clause 8.3.2 of the original IEEE 802.11i (IEEE Computer Society LAN MAN Standards Committee) and added later to current IEEE 802.11 standard. While the new IEEE 802.11i standard is being ratified, wireless vendors have agreed on an interoperable interim standard known as WiFi Protected Access (WPA).

### III.I WPA KEY MANAGEMENT

Rekeying of unicast encryption keys is optional with 802.1x. Additionally, 802.11 and 802.1x provide no mechanism to change the global encryption key that is used for multicast and broadcast traffic. With WPA, rekeying of both unicast and global encryption keys is required. The Temporal Key Integrity Protocol (TKIP) changes the unicast encryption key for every frame and each change is synchronized between the wireless client and the wireless AP. For the global encryption key, WPA includes a facility for the wireless AP to advertise changes to the connected wireless clients.

### *TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)*

WEP encryption is optional for 802.11. For WPA, encryption using TKIP is required. TKIP replaces WEP with a new encryption algorithm that is stronger than the WEP algorithm, yet can be performed using the calculation facilities present on existing wireless hardware. TKIP also provides for:

- The verification of the security configuration after the encryption keys are determined.
- The synchronized changing of the unicast encryption key for each frame. The determination of a unique starting unicast encryption key for each pre-shared key authentication.

### *WI-FI PROTECTED ACCESS 2 (WPA-2)*

WPA-2 introduced by the Wi-Fi Alliance was ratified in IEEE 802.11i clause. The WPA2 protocol includes the following features :

- IEEE 802.1X authentication;
- Extensible authentication protocol (EAP); and
- Encryption using advanced encryption standard (AES) (NIST, 2001).
- WPA2 is used in CCMP (counter with CBC MAC protocol) mode for implementing AES in 802.11i, including:
- 128-bit keys;
- Using AES in CBC-MAC mode for calculating MIC and AES in counter mode for data encryption; and
- Guaranteeing 48 bit initialization vector.
- WPA-2 improves WEP shortcomings but, unlike WPA, incorporates AES encryption mechanisms to reduce vulnerabilities which could introduce hash functions with WPA TKIP. WPA- 2 uses a TK and a packet

number (PN) field to prevent attacks by repeating frames. The authentication phase and pair master key (PMK) derivation are performed according to IEEE 802.1X.

- WPA-2 uses AES in CBC-MAC mode to calculate MIC and AES in counter mode to encrypt the payload. Figure 3 shows these two processes performed in parallel.

*MESSAGE INTEGRITY CHECK (MIC)*
AES uses the data integrity key at this stage:

1. A 128 bit Init Block (starting block), as explained below, and the data integrity key are introduced into AES in CCMP mode producing a 128-bit block.

2. An XOR is applied to the result of the previous step with the first 128 bits of the IEEE 802.11 payload block, producing a 128-bit block.

3. The result from step 2 is introduced into AES in CCMP mode producing a 128-bit block. 4. Steps 2 and 3 are carried out with the remaining 128-bit payload blocks, except for the PN field, used for numbering the frame and already included on the starting block. This is done until the last 128-bit block of the payload field. From the last 128 bits resulting from the AES-CCMP function, the 64 most significant bits are taken and named "R1." R1 corresponds to unencrypted MIC. WPA-2 builds the starting block (used for calculating MIC) using the following information:

- The flag field (8 bits) is set at 01011001. This field contains several flags, including the one that specifies that a 64-bit MIC length is in use;
- The priority field (8 bits) which is fixed at 0 and is reserved for future use;
- The source address field (48 bits) from the IEEE 802.11 frame MAC header;
- The PN field (48 bit); and
- Data length field (16 bits).
- There are two padding fields at the beginning and end of the payload frame used to complete the payload or the header to match 128-bit blocks.

*DATA ENCRYPTION*
AES uses the DEK obtained during the 802.1X authentication process. AES is used in counter mode for payload encryption. An initial 128-bit counter is used with the following fields to start the process:

- Flag field (8 bits) set at 01011001 containing several flags, including the one which specifies that a 64-bit MIC length is in use;
- The priority field (8 bits) which is fixed at 0 and is reserved for future use;
- Source address field (48 bits) from the IEEE 802.11 MAC frame header;

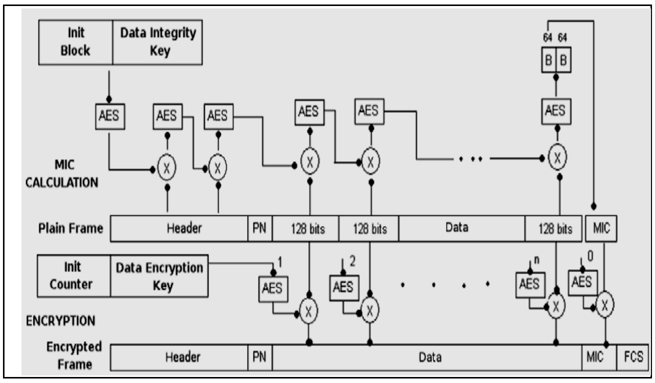

Fig.2. WPA-2 encryption and integrity check.

• PN field (48 bits); and Counter field (16 bits) which is fixed at 1 and is only increased if the 802.11 frame payload is fragmented. It should be noted that this counter is only part of the counter that inputs to the AES function in counter mode, which is actually modified by the package number (field PN) if the payload is not fragmented. The payload is encrypted as follows after this 128-bit initial counter has been built:

1. The initial counter is input into an AES function in counter mode along with the data encryption key producing a 128-bit block;

2. With this result, an XOR is applied to the first 128 payload bits (clear text payload) producing the first 802.11 frame payload 128 ciphered bits; and

3. The initial counter is increased in step 1 and step 2 is repeated with the following 128 bits of clear text payload. This is done until finishing the encryption of the entire frame's payload. The counter is increased and its value is sent to the AES function. The result is XORed with the MIC (and of course with R1) and the most significant 64 ciphered bits are taken and encapsulated along with the frame check sequence (FCS) and IEEE 802.11 header.

## IV. CONCLUSION

In this paper we have discussed some of the key concerns surrounding the security of wireless networks. We have highlighted a number of weaknesses in existing protocols and configurations of wireless networks including how these weaknesses can be exploited. The paper has also considered the legality aspects of accessing information regarding the configuration of a wireless network as well as the accessing of transmitted or stored information on the network by using the WAP.The WEP protocol is vulnerable to attacks; the problem does not lie with the RC4 algorithm used by WEP but the way in which the encryption keys are managed and generated to be used as RC4 algorithm input. Other RC4 algorithm-based security protocols such as transport layer security, secure socket layer and WPA are more secure for practical uses. Due to the weaknesses found in WEP, new alternatives such as WPA have emerged to reduce the lack-of security stigma of wireless networks, ensuring confidence in their use in various premises. These new levels of security are achieved through greater security implementation providing strong encryption and incorporating authentication such as Elliptical curve cryptography.

## REFERENCES

[1]. B. Parno, A. Perrig, and V.D. Gligor, “Distributed Detection of Node Replication Attacks in Sensor B. Parno, A. Perrig, and V.D. Gligor, “Distributed Detection of Node Replication Attacks in Sensor Networks,” Proc. IEEE Symposium. Security and Privacy, **pp. 49-63, May 2005**

[2]. Kai Xing Fang, Liu Xiuzhen, Cheng David, H. C. Du, Real-Time Detection of Clone Attacks in Wireless Sensor Networks Proceedings of the 28th International Conference on Distributed Computing Systems, **2008, Pages 3-10**.

[3]. Klempous R.; Nikodem J.; Radosz, L.; Raus, N. Byzantine Algorithms in Wireless Sensors Network, Wroclaw Univ. of Technology .,Wroclaw; Information and Automation, 2006. ICIA2006.International Conference on, 15-17 **Dec. 2006**, pages :**319-324**

[4]. Mehmet Ulema and Barcin Kozbe, “Management of Next-generation Wireless Networks and Services”, IEEE Communications Managing, **February 2003.**

[5]. B. Parno, A. Perrig, and V.D. Gligor, “Distributed Detection of Node Replication Attacks in Sensor B. Parno, A. Perrig, and V.D. Gligor, “Distributed Detection of Node Replication Attacks in Sensor Networks,” Proc. IEEE Symposium. Security and Privacy, pp**. 49-63, May 2005.**

[6]. Y. Wang, G. Attebury, and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks,” IEEE Communication. Surveys Tutorials, vol. 8**, pp. 2–23, year 2006**

[7]. Security in Mobile Ad Hoc Networks: Challenges and Solutions H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang IEEE Wireless Communications, Vol.11, Issue 1, pp. **38-47, 2004**

[8]. Fluhrer, S., Mantin, I. and Shamir, A. 2001. Weaknesses in the Key Scheduling Algorithm of RC4, Selected Areas in Cryptography 2001, Lecture Notes in Computer Science, Vol. **2259, pp. 1-24**. Springer.

[9]. Mead, N.R. and McGraw, G. **2003**. Wireless Security’s Future, IEEE Security and Privacy, 1 (4), **pp. 68-72.**

[10]. Joseph Binder, Hans Peter Bischof, Zero Knowledge Proofs of Identityfor Ad Hoc Wireless Networks An In-Depth Study Technical Report, **2003**

## AUTHOR’S PROFILE

**Dr. Mohd. Amjad** is currently working as Assistant Professor in the Department of Computer Engineering, F/o Engineering & Technology, Jamia Millia Islamia (Central University), New Delhi. He received B.Tech. degree from A.M.U. Aligarh in computer Engineering, M.Tech. degree in Information Technology from GGSIP University New Delhi and Ph.D. from Jamia Millia Islamia, from the Deptt. Of Computer Engineering New Delhi. Dr. Amjad has more than 11 Years of teaching experience at U.G and P.G. Level. His research interests includes Network Security, Internet and mobile computing, Mobile Ad hoc Networks and wireless sensor networks.