Security Enhancement & Solution for WPA 2 (Wi-Fi Protected Access 2)

A.K.M. NAZMUS SAKIB
B.Sc Engr. dept. of C.S.E, Chittagong University of Engineering & Technology
Lecturer of IBAIS University, Dhaka International University
Dhaka, Bangladesh
e-mail: sakib425@gmail.com

***Abstract*— WPA and WPA2 (Wi-Fi Protected Access) is a certification program developed by the Wi-Fi Alliance to indicate compliance with the security protocol created by the WiFi Alliance to secure wireless networks. The Alliance defined the protocol in response to several weaknesses researchers had found in the previous system: Wired Equivalent Privacy (WEP). Many sophisticated authentication and encryption techniques have been embedded into WPA2 but it still facing a lot of challenging situations. In this paper we discuss the benefit of WPA2, its vulnerability & weakness .This paper also present solutions or suggestions which will improve Wi-Fi Protected Access 2 (WPA2) protocol.**

Keywords- WPA2, Key, Authentication, Hash Function, DH Algorithm, PRNG

I. Introduction

Wireless network has been an excellent invantion at the end of 20th century in inter-network communication. WiFi (wireless fidelity) is one of today's leading wireless technologies [1][4]. WiFi networks based on IEEE 802.11 standard are being widely deployed in different environment due to standardization and ease to use. It allows an Internet connection to be broadcast through radio waves. The waves can be picked up by WiFi receivers which is attached to computers, personal digital assistants or cell phones. As the businesses expanded wireless demands increased and have become necessity as the day passed. The networking world suffers from many problems with networks the wireless too are also more prone to problems. Though the problems related to wireless networks is been on constant track to be removed but the solutions are not always perfect. The main two problems that have been faced by the wireless network are security and signal interference. The problem with security can never be solved fully but it can be minimized. Since 1990, many wireless security protocols have been designed and implemented, but none proved to be convincing with the security threats that come every day with new dangers to our systems and information. So, depending on the business needs and requirements it is very much important to address wireless network security more efficiently. Through the last two decades wireless network researchers have come with 3 main Security protocols: WEP, WPA and WPA2 [1]. Wireless Equivalent Privacy) (WEP) was the first default encryption protocol introduced in the first IEEE 802.11 standard, received a great deal of coverage due to various technical failures in the protocol. WiFi protected access (WPA) came with the purpose of solving the problems in the WEP cryptography method. First WEP, then WPA are used to secure wireless communications were found inadequate due to many proven vulnerabilities so a new protocol was implemented, WiFi protected access 2 (WPA2) protocol [1][3]. WPA2 also known as IEEE 802.11i standard is an amendment to the 802.11 standard which specifying security mechanisms for wireless networks.

II. WPA2

The WiFi security protocol (WPA2) has not yet addressed many security vulnerabilities in its process of authentication. The 4 process that the WPA2 has at present are given below

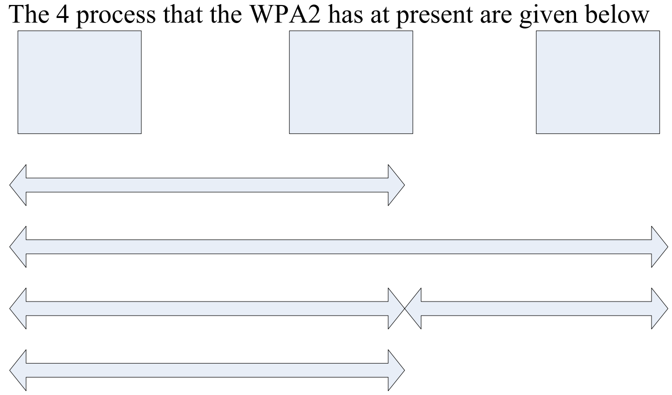

Fig.1. WPA2 or 802.11i operational phases

From the above picture, it is clear that the confidentiality and integrity are only defined in the 4th step where the 1st 3 steps are not secured. So at those three steps the station (client, supplicant) or AP (the authenticator) can be compromised [1][8].

For station

- When a station sends security policy a rouge AP can collect them and extract information based on the information on probe and beacons.
- When 802.1 x authentications takes place the PSK is transmitted on air in plain text, so any attacker through any software can capture what a station is sending through signals in air.

- At the 3rd step also the various keys like PTK,GTK,KEK,KCK are transmitted in plain text that can be captured and used by the attacker [1][6].

For AP

- When an attacker sends security policies that have 1 in 100 of chances to match with security policy of AP can compromise the AP itself.
- When an attacker also sends identity or PSK by a dictionary tool and a spoofed MAC, the AP is forced to send the authentication request to RADIUS server [1][4].

From above, both station and AP can be compromised. In that case some mechanism should be introduced to include some level of security to the existing WPA2 system.

A. WPA2 Weakness

When a number of minor weaknesses have been discovered in WPA/ WPA2 since their release, none of them are too dangerous provided simple security recommendations are followed. The most practical vulnerability is the attack against WPA and WPA2's PSK key .As already mentioned, the PSK provides an alternative to 802.1 x PMK generations using an authentication server. It is a string of 256 bits or a passphrase of 8 to 63 characters used to generate such a string using a known algorithm: PSK = PMK = PBKDF2 (password, SSID, SSID length, 4096, 256) where PBKDF2 is a method used in PKCS#5, 4096 is the number of hashes and 256 is the length of the output[4][5]. The PTK is derived from the PMK, using the 4-Way Handshake and all information used to calculate its value is transmitted in plain text. Strength of PTK therefore relies only on the PMK value, which for PSK effectively means the strength of the passphrase. As indicated by Robert Moskowitz, second message of the 4-Way handshake [1] could be subjected to both dictionary and brute force offline attacks.

B. WPA2 Authentication

One of the major changes introduced with the WPA2 standard is the separation of user authentication from the enforcement of message privacy and integrity, thereby providing a more scalable and robust security architecture suitable to home networks or corporate networks with equal prowess.

1) Personal mode

Authentication in the WPA2 Personal mode, which does not require an authentication server and is performed between the client and the AP generating a 256-bit PSK from a plain-text pass phrase (from 8 to 63 characters) [1]. The PSK in conjunction with the Service Set Identifier and SSID length form the mathematical basis for the Pair-wise Master Key (PMK) to be used later in key generation.

2) Enterprise mode

Authentication in Enterprise mode relies on the IEEE 802.1X authentication standard. The major components are the supplicant (client) joining the network, the authenticator (the AP serves) providing access control and the authentication server (RADIUS) making authorization decisions [1]. The authenticator (AP) divides each virtual port into two logical ports: one for service and the other for authentication, making up the PAE (Port Access Entity). The authentication PAE always open to allow authentication frames through, while the service PAE is only open upon successful authentication by the RADIUS server. The supplicant and the authenticator communicate using Layer 2 EAPoL (EAP over LAN) [8] [6]. Authenticator converts EAPoL messages to RADIUS messages and then forwards them to the RADIUS server. Authentication server (RADIUS), which must be compatible with the supplicant's EAP types, receives and processes the authentication request [1][3]. Once the authentication process is complete the supplicant and authenticator have a secret Master Key (MK) as shown in Figure 2.

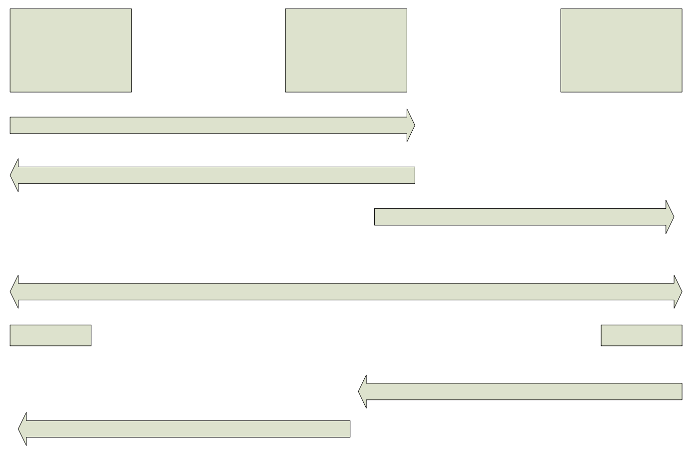

Fig. 2. 802.1x authentication [6]

C. Secure Authentication process by using Hash function

The security steps are as follows:

Step1: Client request for communication & send out a string as a challenge to A.P.

Step2: A.P also sends out a string as a challenge to Client.

Step3: Client calculates the message digest of the string by applying hash algorithm and sends the challenging string value and its ISSI number to A.P.

Step4: A.P also calculates the message digest for the corresponding string & send to the Client. Only the legitimate A.P & Client knows the hash algorithm. But the evil M.S is not able to produce correct value for the given string.

A.P & Client compare the corresponding message digest value. If it matches then continue further communication, otherwise, ceases the communication immediately.

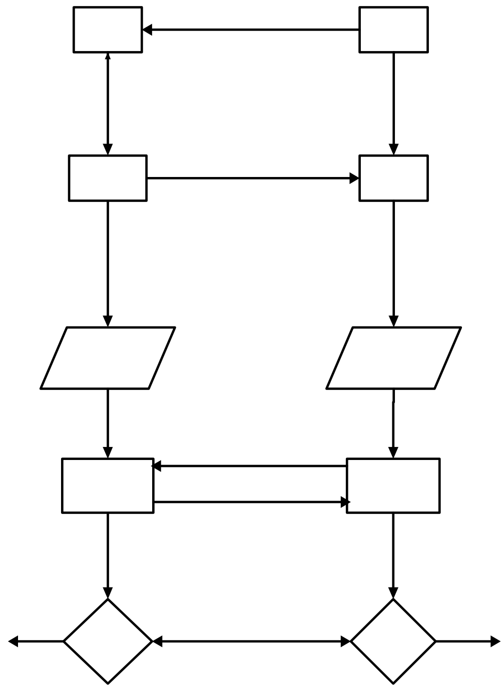

Fig. 3.Authentication in secure way

D. WPA2 key generation

Key generation is accomplished by means of two handshakes: a 4-Way Handshake for PTK (Pair wise Transient Key) and GTK (Group Transient Key) derivation and a Group Key Handshake for GTK renewal. The 4-Way Handshake is accomplished by four EAPoL-Key messages between the client and the AP, is initiated by the access point and performs the following tasks:

- Confirm the client's knowledge of the PMK. The PMK derivation, required to generate the PTK, is rely on the authentication method used. In WPA2 Personal mode the PMK is derived from the authentication PSK and for WPA2 Enterprise mode the PMK is derived from the authentication MK[1] (key hierarchy in Fig. 6).
- Derive a fresh PTK, which is comprised of three types of keys: KCK (Key Confirmation Key – 128 bits) used to check the integrity of EAPoL-Key frames, Key Encryption Key(KEK – 128 bits) used to encrypt the GTK and the Temporal Keys(TK – 128 bits) used to secure data traffic[1].
- Install encryption and integrity keys.
- Encrypt transport of the GTK which is calculated by the AP from a random Group Master Key (GMK).
- Confirm the cipher suite selection.

E. Key generation in a secure way

Symmetric key generation by DH algorithm

DH key agreement is a key management method to share an encryption key with global variables known as prime number 'P' and 'G', 'G' is a primitive root of P. 'a' is the private key of Client, and 'b' is the private key of A.P. Client's public key is $PK_{Client} = G^{a}$ mod P and A.P's public key is $PK_{AP} = G^{b}$

The DH key exchange protocol is described as follows where both A.P and Client exchange keys.

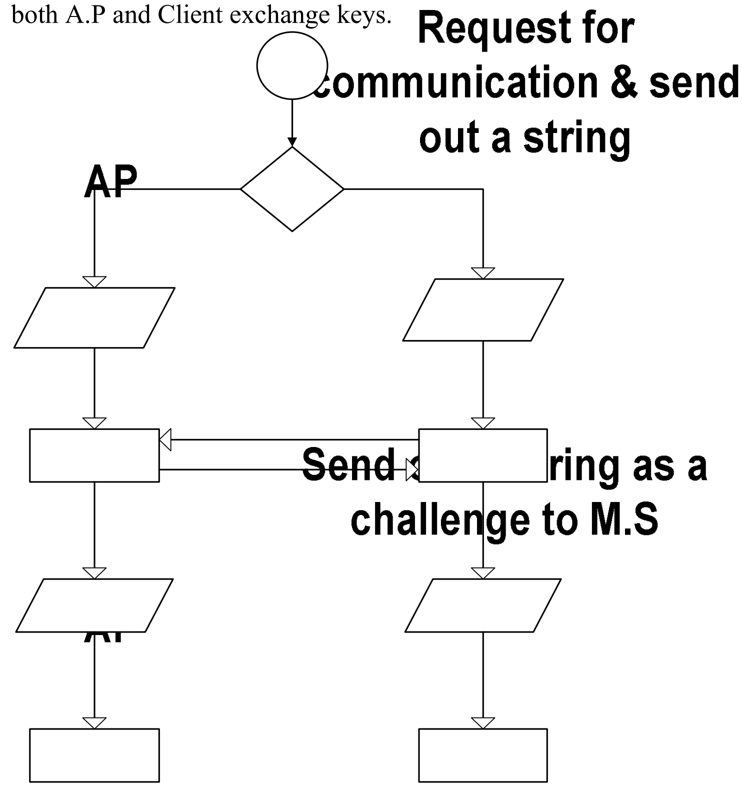

Fig: 4. Symmetric Key generation

F. Pseudo Random Number Generation

A pseudorandom number generator (PRNG) is an algorithm for generating a sequence of numbers that approximates the properties of random numbers. The sequence is not truly random in that it is completely determine by a relatively small set of initial values, called the PRNG's state. Although sequences that are closer to truly random can be generated using hardware random number generators, pseudorandom numbers are important in practice for simulation (e.g., physical system with Monte Carlo Method) and are central in the practice of cryptography and procedural generation. Common classes of these algorithms are linear congruential generators, Lagged Fibonacci generators, linear feedback shift registers, feedback with carry shift registers and generalized feedback shift registers. Recent instances of pseudorandom algorithm include Blum Blum Shub, Fortuna and Mersenne twister.

1) Blum Blum Shub (B.B.S.)

2) is a pseudorandom number generator proposed in 1986 by Lenore Blum, Manuel Blum and Michael Shub (Blum et al., 1986).

Blum Blum Shub takes the form:

$$x_{n+1} = x_n^2 \bmod M$$

where M=pq is the product of two large primes p and q. At each step of the algorithm, some output is derived from x_{n+1}; the output is commonly either the bit parity of x_{n+1} or one or more of the least significant bits of x_{n+1}.

The seed x_0 should be an integer that's not 1 or co-prime to M (ie. p and q are not factors of x_0).

The two primes, p and q, should both be congruent to 3 (mod 4) (this guarantees that each quadratic residue has one square root which is also a quadratic residue) and gcd(φ(p-1), φ(q-1)) should be small (this makes the cycle length large).

An interesting characteristic of the Blum Blum Shub generator is the possibility to calculate any x_i value directly (via Euler's Theorem):

$$x_i = \left(x_0^{2^i \bmod \lambda(M)}\right) \bmod M$$

where λ is the Carmichael function. (Here we have $\lambda(M) = \lambda(p \cdot q) = \operatorname{lcm}(p-1, q-1)$).

2) Mersenne Twister

The Mersenne twister is a pseudorandom number generator developed in 1997 by Makoto Matsumoto and Takuji Nishimura that is based on a matrix linear recurrence over a finite binary field F_2. It provides for fast generation of very high-quality pseudorandom numbers, having been designed specifically to rectify many of the flaws found in older algorithms.

Its name derives from the fact that period length is chosen to be a Mersenne prime. There are at least two common variants of the algorithm, differing only in the size of the Mersenne primes used. The newer and more commonly used one is the Mersenne Twister MT19937, with 32-bit word length. There is also a variant with 64-bit word length, MT19937-64, which generates a different sequence.

For a k-bit word length, the Mersenne Twister generates numbers with an almost uniform distribution in the range $[0, 2^k - 1]$.

Algorithm Details:

The Mersenne Twister algorithm is a twisted generalised feedback shift register (twisted GFSR, or TGFSR) of rational normal form (TGFSR(R)), with state bit reflection and tempering. It is characterized by the following quantities:

- w: word size (in number of bits)
- n: degree of recurrence
- m: middle word, or the number of parallel sequences, $1 \le m \le n$
- r: separation point of one word, or the number of bits of the lower bitmask, $0 \le r \le w - 1$
- a: coefficients of the rational normal form twist matrix
- b, c: TGFSR(R) tempering bitmasks
- s, t: TGFSR(R) tempering bit shifts
- u, l: additional Mersenne Twister tempering bit shifts with the restriction that $2^{nw-r} - 1$ is a Mersenne prime. This choice simplifies the primitivity test and k-distribution test that are needed in the parameter search.

For a word x with w bit width, it is expressed as the recurrence relation

$$x_{k+n} := x_{k+m} \oplus ({x_k}^u \mid {x_{k+1}}^l)A \qquad k = 0, 1, \ldots$$

with | as the bitwise or and $\oplus$ as the bitwise exclusive or (XOR), x^u, x^l being x with upper and lower bitmasks applied. The twist transformation A is defined in rational normal form

$$A = R = \begin{pmatrix} 0 & I_{w-1} \\ a_{w-1} & (a_{w-2}, \ldots, a_0) \end{pmatrix}$$

with I_{n-1} as the $(n-1) \times (n-1)$ identity matrix (and in contrast to normal matrix multiplication, bitwise XOR replaces addition). The rational normal form has the benefit that it can be efficiently expressed as

$$\boldsymbol{x}A = \begin{cases} \boldsymbol{x} \gg 1 & x_0 = 0 \\ (\boldsymbol{x} \gg 1) \oplus \boldsymbol{a} & x_0 = 1 \end{cases}$$

Where

$$\boldsymbol{x} := ({x_k}^u \mid {x_{k+1}}^l) \qquad k = 0, 1, \ldots$$

In order to achieve the $2^{nw-r} - 1$ theoretical upper limit of the period in a TGFSR, $\varphi_B(t)$ must be a primitive polynomial, $\varphi_B(t)$ being the characteristic polynomial of

$$B = \begin{pmatrix} 0 & I_w & \cdots & 0 & 0 \\ \vdots & & & & \\ I_w & \vdots & \ddots & \vdots & \vdots \\ \vdots & & & & \\ 0 & 0 & \cdots & I_w & 0 \\ 0 & 0 & \cdots & 0 & I_{w-r} \\ S & 0 & \cdots & 0 & 0 \end{pmatrix} \leftarrow m\text{-th row}$$

$$S = \begin{pmatrix} 0 & I_r \\ I_{w-r} & 0 \end{pmatrix} A$$

The twist transformation improves the classical GFSR with the following key properties:

- Period reaches the theoretical upper limit $2^{nw-r} - 1$ (except if initialized with 0)
- Equidistribution in n dimensions (e.g. linear congruential generators can at best manage reasonable distribution in 5 dimensions)

As like TGFSR(R), the Mersenne Twister is cascaded with a tempering transform to compensate for the reduced dimensionality of equidistribution (because of the choice of A being in the rational normal form), which is equivalent to the transformation $A = R \rightarrow A = T^{-1}RT$, T invertible. The tempering is defined in the case of Mersenne Twister as

y := x ⊕ (x >> u)

y := :y ⊕ ((y << s) & b)

y := :y ⊕ ((y << t) & c)

z := y ⊕ (y >> l)

with <<, >> as the bitwise left and right shifts, and & as the bitwise and. The first and last transforms are added in order to improve lower bit equidistribution. From the property of TGFSR, $s + t \geq \lfloor w/2 \rfloor - 1$ is required to reach the upper bound of equidistribution for the upper bits.

The coefficients for MT19937 are:

- (w, n, m, r) = (32, 624, 397, 31)
- a = $9908B0DF_{16}$
- u = 11
- (s, b) = (7, $9D2C5680_{16}$)
- (t, c) = (15, $EFC60000_{16}$)
- l = 18

3) *Lagged Fibonacci generator (LFG)*

A Lagged Fibonacci generator (LFG) is an example of a pseudorandom number generator. This class of random number generator is aimed at being an improvement on the 'standard' linear congruential generator. These are based on a generalization of the Fibonacci sequence.

- The Fibonacci sequence may be described by the recurrence relation:
- $S_n = S_{n-1} + S_{n-2}$
- Hence, the new term is the sum of the last two terms in the sequence. This can be generalized to the sequence:
- $S_n \equiv S_{n-j} \star S_{n-k} \pmod{m}, 0 < j < k$
- In which case, the new term is some combination of any two previous terms. m is usually a power of 2 ($m = 2^M$), often 2^{32} or 2^{64}. The $\star$ operator denotes a general binary operation. This may be either addition, subtraction, multiplication, or the bitwise arithmetic exclusive-or operator (XOR). The theory of this type of generator is rather complex, and it may not be sufficient simply to choose random values for j and k. These generators also tend to be very sensitive to initialization.
- Generators of this type employ k words of state (they 'remember' the last k values).
- If the operation used is addition, then the generator is described as an *Additive Lagged Fibonacci Generator* or ALFG, if multiplication is used, it is a *Multiplicative Lagged Fibonacci Generator* or MLFG, and if the XOR operation is used, it is called a *Two-tap generalized feedback shift register* or GFSR. The Mersenne twister algorithm is a variation on a GFSR. The GFSR is also related to the *Linear Feedback Shift Register*, or LFSR.

a) Properties of lagged Fibonacci generators

- Lagged Fibonacci generators have a maximum period of $(2^k - 1)*2^{M-1}$ if addition or subtraction is used, and $(2^k-1)*k$ if exclusive-or operations are used to combine the previous values. If, on the other hand, multiplication is used, the maximum period is $(2^k - 1)*2^{M-3}$, or 1/4 of period of the additive case.

- For the generator to achieve this maximum period, the polynomial:

- $y = x^k + x^j + 1$

- must be primitive over the integers mod 2. Values of j and k satisfying this constraint have been published in the literature. Popular pairs are:

- {j = 7, k = 10}, {j = 5, k = 17}, {j = 24, k = 55}, {j = 65, k = 71}, {j = 128, k = 159} [1], {j = 6, k = 31}, {j = 31, k = 63}, {j = 97, k = 127}, {j = 353, k = 521}, {j = 168, k = 521}, {j = 334, k = 607}, {j = 273, k = 607}, {j = 418, k = 1279} [2]

- Another list of possible values for *j* and *k* is on page 29 of volume 2 of *The Art of Computer Programming*:

- (24,55), (38,89), (37,100), (30,127), (83,258), (107,378), (273,607), (1029,2281), (576,3217), (4187,9689), (7083,19937), (9739,23209)

- Note that the smaller numbers have short periods (only a few "random" numbers are generated before the first "random" number is repeated and the sequence restarts).

- It is required that at least one of the first k values chosen to initialize the generator be odd.

- It has been suggested that good ratios between j and k are approximately the golden ratio

III. CONCLUCION

In this paper, an overview of security scheme in WiFi is presented. Attacks on authentication can be described as the ways by which a network can be intruded and the privacy of the users is compromised; if the user authentication and authorization stage is compromised. Therefore, the ways to breach the authentication frameworks are termed as attacks on privacy and key management protocols. But the hash based authentication protocol will protect this type of interception. We also proposed secure symmetric key generation process by using DH algorithm & also PRNG. This will prevent a key misuse & save band width in the multi- and broadcast services. We also used DH key exchange protocol to fit it into WiFi network to eliminate existing weakness of unencrypted management communication message.

REFERENCES

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

[2] "IEEE 802.11i." *Wikipedia, The Free Encyclopedia*. 11 Nov 2006, 10:22 UTC. Wikimedia Foundation, Inc. Nov. 25 2006<http://en.wikipedia.org/w/index.php?title=IEEE_802.11i&oldid=87121019>

[3] "Wi-Fi Protected Access 2 Data Encryption and Integrity." Microsoft TechNet. The Cable Guy. July 29 2005.<http://www.microsoft.com/technet/community/columns/cabl eguy/cg0805.mspx>

[4] "Understanding the updated WPA and WPA2 standards".ZDNet Blogs. Posted by George Ou. June 2 2005. <http://blogs.zdnet.com/Ou/?p=67>

[5] "Deploying Wi-Fi Protected Access (WPAtm) and WPA2tm in the Enterprise." Wi-Fi Alliance, Feb. 27 2005<http://www.wifi.org/files/uploaded_files/wp_9_WPAWPA2% 20Implementation_2-27-05.pdf>

[6] Lehembre, Guillaume. "Wi-Fi security –WEP, WPA and WPA2". Article published in number 1/2006 (14) of hakin9, Jan.2006. Publication on www.hsc.fr on Dec. 28 2005.<http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_EN.pdf>

[7] Ou, George. "Wireless LAN security guide".www.lanarchitect.net. Revision 2.0 Jan 3 2005.<http://www .lanarchitect.net/Articles/Wireless/SecurityRating>

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

[9] "Extensible Authentication Protocol." Wikipedia, Free Encyclopedia. Nov. 26 2006, 15:39 UTC. Wikimedia Foundation,Inc. Nov27 2006 <http://en.wikipedia.org/w/index.php?title=Extensible_Authentication_Protocol&oldid=90231401>.

[10] Gupta Ashok and Buthmann, Theresa. "The Bell Labs Security Framework: Making the case for End-to-End Wi-Fi Security". LucentTechnologies Sep. 11 2006 (15). <http://www.lucent.com/livelink/09009403800aa8c9_White_paper.pdf>

[11] Epstein Joe. "802.11w fills wireless security holes". Network World Apr. 3 2006 <http://www.networkworld.com/news/tech/2006/040306-80211w-wireless-security.html>

[12] Wright Joshua. "How 802.11w will improve wireless security". Network World May 29 2006 <http://www.net workworldcom/columnists/2006/052906-wireless-security.html>

[13] Wright Joshua. "802.11w security won't block DoS attacks". Tech World Jun. 14 2006 <http://www.techworld.com/security/features/index.cfm?featureID=2599&pagetype=samecatsamchan>

[14] Sood Kapil and Eszenyi Mathew. "Secure Management of IEEE 802.11 Wireless LANs". Intel Software Network <http://www3.intel.com/cd/ids/developer/asmo-na/eng/dc/mobile/287462.htm>

[15] Strand Lars. "802.1X Port-Based Authentication HOWTO". The Linux Documentation Project Oct. 18 2004.<http://tldp.org/HOWTO/html_single/8021X-HOWTO>

[16] Bellardo John and Savage Stefan. "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions" USENIX 2003 Nov. 7

[17] "IEEE 802.16e Security Vulnerability: Analysis & Solution",A.K.M. Nazmus Sakib, Dr. Muhammad Ibrahim Khan, Mir Md. Saki Kowsar, GJCST, October 2010, Volume 10, Issue 13, Version 1

[18] "Security Enhancement & Solution for Authentication Frame work in IEEE 802.16"- A.K.M. NAZMUS SAKIB[1], Academic & Industrial Colleboration Centre [International Journal of Computer Science & Information Technology] Vol2, No 6, 2010.

[19] "Security Improvement of IEEE 802.11i (Wi-Fi Protected Access 2)"- A.K.M. NAZMUS SAKIB[1], Fariha Tasmin Jaigirdar, Muntasim Munim, Armin Akter, International Journal of Engineering Science & Technology.

[20] "Secure Key Exchange & Authentication Protocol For Multicast & Broad cast Service in IEEE 802.16e"- A.K.M. NAZMUS SAKIB[1], Mir Md Saki Kawsor, AP Journal Special Issue

[21] "Security Improvement of Multi & Broadcast services in IEEE 802.16e by removing Forward Secrecy"- A.K.M. NAZMUS SAKIB[1] , Global Journal of Computer Science & Technology, Volume 11 Issue 16 Version 1.0 August/September 2011.

[22] "Secure Authentication & Key Exchange Technique for IEEE 802.16e by using Cryptographic Properties", A.K.M. Nazmus Sakib[1], International Journal of Engineering Research and Applications, Vol 1 Issue 3, 2011

AUTHORS PROFILE

A.K.M. NAZMUS SAKIB, complete his B.Sc Engineering from Chittagong University of Engineering & Technology. Currently acting as a senior lecturer of IBAIS University, Dhaka International university. Also he perform as a Editor Board Member & Reviewer Member of several International Journal & Research org..

Research Area: Information security & Cryptography

Email: sakib425@gmail.com, +01730079790, +01917884634