A.K.M.Nazmus Sakib, Rezaul Karim, Md. Moshiur Rahman, Abdullah Al Azad, Rasidul Islam, Md. Monowarul Haque / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue5, September- October 2012, pp.450-453

Euclid's & RSA Algorithm For 802.11 (Wifi) Security Protocol

A.K.M.NAZMUS SAKIB[*], REZAUL KARIM[**], MD. MOSHIUR RAHMAN[***], ABDULLAH AL AZAD[****], RASIDUL ISLAM[*****], MD. MONOWARUL HAQUE[******]

*(Faculty Member, Department of CSE, Dhaka International University, Bangladesh
(B.Sc in CSE, Dhaka International University, Bangladesh)

ABSTRACT

Technology making rapid progress & is making many things easier. As the innovative thinking of persons is increasing day-by-day new methods for wireless networking have been evolved of which our present topic WiFi is the most accepted technology. WiFi (Wireless-Fidelity), which is the wireless way to handle networking. This paper introduces WiFi technology & various Security Vulnerabilities. Also we present solutions for some of these security vulnerabilities. Our solution is based on Random number generation process & several encryption & decryption Algorithm.

Keywords – WiFI, RNG, Euclid's Algorithm, Key Generation, RSA

I. INTRODUCTION

Wi-Fi, is a set of product compatibility standards for Wireless Local Area Networks (WLAN) based on IEEE 802.11. Wi-Fi is intended to be used for mobile devices and LANs, but is now often used for Internet access [2]. It enables a person with a wireless-enabled computer or personal digital assistant to connect to the Internet when in proximity of an access point. WiFi is the wireless way to handle networking [2]. It is known as 802.11 networking and wireless networking. And using this technology we can connect computers anywhere in a office or home without the need of any wires [2]. Computers connect to the network using radio signals and they can be up to 100 feet or so apart. It allow to connect to the internet from virtually anywhere at speeds of up to 55 Mbps. Computers or handsets enabled with this technology use radio technologies based on the IEEE 802.11 standard to send and receive data anywhere within the range of a base station [2]. WiFi goes beyond wirelessly connecting computers, it also connects people.

1.1 What is Wi-Fi?

Wi-Fi refers to wireless networking technology that allows computers & other devices to communicate over a wireless media. It describes all network components that are based on one of [2] the 802.11 standards, including 802.11a, 802.11b, 802.11g, & 802.11n. These standards are developed by the IEEE & adopted by the Wi-Fi Alliance [2].

1.3 Objective:

1. Identify security vulnerability in WiFi System
2. Produce a secure Authentication process by using Random Number Generator.
3. Provide a secure Encryption / Decryption Algorithm

2. Different Security Vulnerabilities

2.1. Authentication Vulnerability

We can describe the Attacks on authentication by the way the privacy of the users be compromised & a network can be intruded. Secure access of network services is becoming an important issue for the present communication system [2]. Any attempts of an intruder to create a chaos or to get registered with the network illegitimately in it, is possible; if the user authorization and authentication is compromised [2]. Way to breach the authentication frameworks are termed as attacks on privacy and key management protocols [2].

2.2 Interleaving

Sub-class of Man-in-the-Middle attacks & it is aimed for PKM v2. In this attack, an adversary interleaves a communication session by maintaining connections with the BS (Base station) & SS (Subscriber Station), pertaining as SS to BS and vice versa [2]. All the information on route passes to the adversary node & an information leakage point built [2]. The interleaving attack is the re-transmission of a set of messages from the same session. The HA model proposed an way to cater the interleaving attack by introducing storage and transmission overheads in the network [2].

2.3 Water-Torture

It is aimed to perturb the network's operation by causing flooding. Some messages are used to initiate cyclic processes when received on any node [2]. In the admission control process, at the reception end, this message at Base Station initiates the cyclic authentication procedure [2].These triggering messages are captured & are transmitted in

a loop to cause trigger flooding and employ one-way authentication [2]. The PKM v1 model and Time Stamping model are vulnerable to this type of infringement attempt [2]. This is why it is called one-way authentication i.e., Base Station (BS) authenticates Subscriber Station (SS) but vice versa does not occur. This attack can compromise the security of the users and produce severe threats to the Employment of BWA infrastructure in security & defense installations [2].

2. 4 Suppress Replay

The perfect synchronization must be maintained to protect the authentication session from intruder [2]. Due to the loss of synchronization in the clocks of the entities the intruder can gain control on the authentication framework by capturing the messages and transmitting them with added delays, this will cause forward message replay [2]. This class of attack is difficult to counter & it is also vulnerable for the Timestamp Authentication model [2]. This attack is also manipulated the Hybrid Authentication model.

2. 5 Interception

Is a passive attack on confidentiality where an intruding entity is able to read the information that is sent from the source entity to the destination entity [2]. The perfect example of interception attack is eavesdropping and sniffing in which; gathering information about the network (the SSID, information about whether WEP is enabled & the MAC address of the Access Point (AP)) is getting easier with the release of several products [2]. By using high gain antennas the Interception can occur far outside the user's working range (many standard offerings from some vendors) [2].

2.6 Fabrication

Another active attack on authentication, where an intruder pretends to be the source entity. Examples of fabrication attack are Fake e-mails & Spoofed packets. Man-in-the-Middle Attacks is an example of fabrication, in order to execute a man-in-the-middle attack [2], two hosts must have to convince that the computer in the middle is the other host [2]. Some other example of fabrication attack is Spoofing, Brute-Force Password Attacks and Insertion Attacks [2].

2.7 Modification, Replay and Reaction Attacks

The insertion of a Trojan horse program or virus is a perfect example of a modification attack [2]. It is an active attack on integrity, where an intruding entity can able to changes the information that is sent from the source entity to the destination entity [2]. Another issue is virus infection that affects both wireless and wired networks. Two of these are VBS/Timo-A and the LoveBug [2]. Replay is another type os active attack on integrity where an intruding party resends information that is sent from the source entity to the destination entity [2]. Examples of Replay attacks are Traffic Redirection, Resource Stealing and Invasion. In Reaction attack the packets are sent by an intruder to the destination and the intruder monitors the reaction [2].

2.8 Man In The Middle Attack

A simple man-in-the-middle attack is described in following Figure:

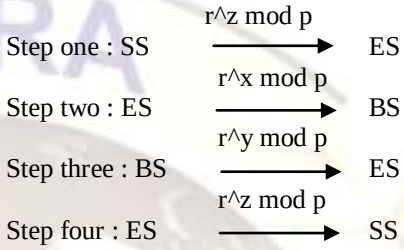

Figure 1: Man-In-the-Middle attack

Evil Station (ES) captured Victim SS's public key *PKss* . The ES (Evil Station) camouflages as SS (Subscriber Station) & Sends its own public key *PKES* to BS (Base Station), then the severing BS (Base Station) sends back its public key *PKBS*, at this time, the ES (Evil Station) could establish a shared key with BS [7]. Finally, ES (Evil Station) sends its own public key *PKES* to victim SS (Subscriber Station), and establishes a shared key with SSe [7]. Consequently, all the messages that the victim SS (Subscriber Station) sends to BS (Base Station) are relayed by ES (Evil Station) and the encryption keys are known by ES (Evil Station). Thus, ES could eavesdrop and tamper all these messages [7]. A secure authentication process can resist man-in-the-middle attacks in this procedure.

3. Algorithm for Solution

3.1 Euclid's algorithm

Euclid's algorithm appears as Proposition II in Book VII (Elementary Number Theory) of his Elements [4]. Euclid poses the problem: "Given two numbers not prime to one another, to find their greatest common measure". He defines "A number a multitude composed of units": a counting number, a positive integer not including 0 [4]. And to "measure" is to place a shorter measuring length *s* successively (*q* times) along longer length *l* until the remaining portion *r* is less than the shorter length *s* in modern words [4], remainder $r = l - q*s$, *q* being the quotient, or remainder *r* is the "modulus", the integer-fractional part left over after the division [4]. For Euclid's method to succeed, the starting lengths must satisfy two requirements: (i) the lengths must not be 0, AND (ii) the subtraction must be "proper" [4], a test must guarantee that the smaller of the two

numbers is subtracted from the larger (alternately, the two can be equal so their subtraction yields 0) [4].
Example of 1599 and 650:

Step 1: 1599 = 650*2 + 299
Step 2: 650 = 299*2 + 52
Step 3: 299 = 52*5 + 39
Step 4: 52 = 39*1 + 13
Step 5: 39 = 13*3 + 0

3.2 An inelegant program for Euclid's algorithm

The following algorithm is framed as Knuth's 4-step version of Euclid's and Nichomachus' [4], but rather than using division to find the remainder it uses successive subtractions of the shorter length *s* from the remaining length *r* until *r* is less than *s [4]*. The high-level description, shown in boldface, is adapted from Knuth 1973:2–4 [4]:

INPUT:

Step: 1 [Into two locations L and S put the numbers *l* & *s* that represent the two lengths]: INPUT L, S

Step: 2 [Initialize R: make the remaining length *r* equal to the starting/initial/input length *l*] R ← L

E0: [Insure $r \geq s$.]

Step: 3 [Insure the smaller of the two numbers is in S & the larger in R]: IF R > S THEN the contents of L is the larger number so skip over the exchange-steps 4, 5 and 6: GOTO step 6 ELSE swap the contents of R and S.] 4 L ← R (this first step is redundant, but will be useful for later discussion) [4].

Step: 5 R ← S

Step: 6 S ← L

E1:[Find remainder]: Until the remaining length *r* in R is less than the shorter length *s* in S, repeatedly subtract the measuring number *s* in S from the remaining length *r* in R [4].

Step: 7 IF S > R THEN done measuring so GOTO 10 ELSE measure again,

Step: 8 R ← R − S

Step: 9 [Remainder-loop]: GOTO 7.

E2: [Is the remainder 0?]: EITHER (i) the last measure was exact & the remainder in R is 0 program can halt [4], OR (ii) the algorithm must continue: the last measure left a remainder in R less than measuring number in S. 10 IF R = 0 then done so GOTO step 15 ELSE continue to step 11 [4],

E3: [Interchange *s* and *r*]: The nut of Euclid's algorithm. Use remainder *r* to measure which was previously smaller number *s*:; L serves as a temporary location [4].

Step: 11 L ← R

Step: 12 R ← S

Step: 13 S ← L

Step: 14 [Repeat the measuring process]: GOTO 7

OUTPUT:

Step: 15 [Done. S contains the greatest common divisor]: PRINT S

DONE:

Step: 16 HALT, END, STOP.

3.3 RSA (Rivest Shamir Adleman) Encryption Algorithm

RSA is an algorithm for public key cryptography which is based on the presumed difficulty of factoring large integers [6]. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978 [6]. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key [6]. The prime factors need to be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods [6], when the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.[6] Whether breaking RSA encryption is as hard as factoring is an open question known as the RSA problem [6].

Operation

The RSA algorithm involves three steps: 1. key generation 2.Encryption, 3. Decryption.

1) Key generation

RSA involves a public key & a private key [6]. The public key is one which is known to everyone & is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key [6]. The keys for the RSA algorithm are generated the following way:

1. Take two distinct prime numbers *p* & *q*. For security purposes, the integer's *p* and *q* should be chosen at random, & should be of similar bit-length. Prime integers can be efficiently found using a primarily test [6].
2. Compute $n = pq$. *n* is used as the modulus for both the public & private keys [6]
3. Compute $\varphi(n) = (p-1)(q-1)$, where φ is Euler's totient function [6].
4. Choose an integer *e* such that $1 < e < \varphi(n)$ & greatest common divisor of $(e, \varphi(n)) = 1$; i.e., *e* & $\varphi(n)$ are coprime [6]. *e* is released as the public key exponent.*e* having a short bit-length & small Hamming weight results in more efficient encryption - most commonly 0x10001 = 65,537. However, small values of *e* (such as 3) have been shown to be less secure in some settings.[6]
5. Determine *d* as:

   i.e., *d* is the multiplicative inverse of *e* mod $\varphi(n)$ [6].

- This is more clearly stated as solve for d given (de) mod φ(*n*) = 1
- This is often computed using the extended Euclidean algorithm.
- d is kept as the private key exponent.

so, d*e= 1 mod φ(*n*) The public key consists of the modulus *n* & the public (or encryption) exponent *e [6]*. The private key consists of the modulus *n* & the private (or decryption) exponent *d* which must be kept secret [6]. (*p*, *q*, and φ(*n*) must also be kept secret because they can be used to calculate *d*.)

Notes: An alternative, used by PKCS#1, is to choose *d* matching $de \equiv 1 \bmod \lambda$ with $\lambda = \operatorname{lcm}(p-1, q-1)$, where lcm is the least common multiple [6]. Using λ instead of φ(*n*) allows more choices for *d*. λ can also be defined using the Carmichael function, λ(*n*) [6].

- The ANSI X9.31 standard prescribes, IEEE 1363 describes, and PKCS#1 allows, that *p* & *q* match additional requirements: be strong primes, & be different enough that Fermat factorization fails [6].

2) Encryption

Alice transmits her public key (n, e) to Bob and keeps the private key secret. Bob then wishes to send message M to Alice [6].

He first turns M into an integer m, such that $0 < m < n$ by using an agreed-upon reversible protocol known as a padding scheme [6]e. He then computes the ciphertext c corresponding to

$$c = m^e \pmod{n}.$$

This can be done quickly using the method of exponentiation by squaring [6]. Bob then transmits c to Alice.

Note that, at least nine values of m could yield a cipher text c equal to m,[6] but this is very unlikely to occur in practice [6].

3) Decryption

$$d \equiv e^{-1} \pmod{\varphi(n)}$$

Alice can recover m from c by using her private key exponent d via computing

$$m = c^d \pmod{n}.$$

Given m, she can recover the original message M by reversing the padding scheme [6].

(In practice, there are more efficient methods of calculating c^d using the pre computed values below.[6])

Conclusions

As WiFi is now shipped in millions of products & deployed in millions of homes, business & hotspots worldwide, the technology has moved beyond the realm of a computer feature. Wi-Fi has fast become a cultural phenomenon. In our future work we will try to include the complexity analysis of our proposed solution.

REFERENCES

[1] Basic Theory of Wi-Fi: http://www.techterms.com/definition/wifi
[2] Wireless Fidelity: http://www.scribd.com/doc/77023471/Wireless-Fidelity
[3] Cisco Spectrum Expert Wi-Fi Data Sheet: http://www.cisco.com/en/US/prod/collateral/wireless/ps9391/ps9393/product_data_sheet0900aecd807033c3.html
[4] Algorithm: http://en.wikipedia.org/wiki/Algorithm
[5] "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
[6] RSA Algorithm: http://en.wikipedia.org/wiki/RSA_%28algorithm%29
[7] "Security Enhancement & Solution for Authentication Frame work in IEEE 802.16"- A.K.M. Nazmus Sakib, Academic & Industrial Colleboration Centre [International Journal of Computer Science & Information Technology] Vol2, No 6, 2010.
[8] "Security Improvement of IEEE 802.11i (Wi-Fi Protected Access 2)"- A.K.M. Nazmus Sakib, Fariha Tasmin Jaigirdar, Muntasim Munim, Armin Akter, International Journal of Engineering Science & Technology.