A.K.M. Nazmus Sakib, Fauzia Yasmeen, Samiur Rahman, Md.Monjurul Islam, Prof. Dr. Md. Matiur Rahaman Mian / International Journal of Engineering Research and Applications (IJERA)
ISSN: 2248-9622 www.ijera.com
Vol. 1, Issue 4, pp. 1448-1452

# Security Thread Analysis & Solution for NGN (Next Generation Network)

A.K.M. Nazmus Sakib[1], Fauzia Yasmeen[2], Samiur Rahman[3], Md.Monjurul Islam[4], Prof. Dr. Md. Matiur Rahaman Mian[5]

[1](Lecturer, Department of CSE, Dhaka International University, IBAIS University, Bangladesh.)
[2](Lecturer, Department of CSE, IBAIS University, Bangladesh.)
[3] (Department of CSE, Chittangong University of Engineering & Technology, Bangladesh.)
[4](Lecturer, Department of CSE, University of Asia Pacific, Bangladesh.)
[5](Dean, Faculty of science & Engineering, IBAIS University, Bangladesh)

## ABSTRACT

**Essential feature of New Generation Networks (NGN) is the availability of many new services offered by several different players. Different applications and services have their own authentication method and use different credentials, more reliable, flexible and easy-to-use methods are needed.**

**In this paper we concern about different security vulnerabilities found in existing system and gives possible solutions to eliminate them. These vulnerabilities are the possibilities to forge key messages, unauthenticated messages and Man In the Middle attack. We proposed a secure key generation process, random number and function generation process to eliminate these vulnerabilities. Also We modify DH key exchange protocol to fit it into NGN network as well as eliminate existing weakness in original DH key exchange protocol.**

*Keywords* - **NGN, IMS, AKA, IKEv-2, Multi-pass Security.**

## I. INTRODUCTION

Next Generation Network (NGN) technology evolved in the past few years. NGN architecture is a Next Generation Network where wired and wireless services are converged and quality of service is guaranteed. One of NGN access networks is the Wireless LANs (WLAN). WLAN systems are more suited for hotspots coverage and offer high data rates

with low investment cost. The multimedia services provided to the users through WLAN depend on the IP multimedia subsystem (IMS), which is based on All-IP architecture. NGN provides many new services through different access networks, which in turn raises security issues. New security architecture is currently under study that aim at protecting the mobile users, the data transferred and the underlying network.

## II. THE EXISTING ARCHITECTURE

NGN security architecture is currently under study [1] [2] that aim at protecting the mobile users, the data transferred and the underlying network. This architecture make the WLAN user have to execute multi-pass Authentication and Key Agreement (AKA) procedure in order to get access to the IMS services. The architecture specifies three authentication steps (see Fig. 1).

**In the first step**, the user executes the (Extensible Authentication Protocol) EAP-AKA protocol [3] to register in WLAN domain.

**In the second step**, the user executes the Internet Key Exchange version 2 (IKEv2) protocol [4] that encapsulates EAP-AKA, which registers him to the 3G public land mobile network (PLMN) domain.

**In the third step,** the user using the Session Initiation Protocol (SIP) [5] [6] executes the IMS-AKA procedure [3] for registration in the IMS domain.

As we can see the EAP-AKA has been repeated and an execution of IMS AKA introduce an authentication overhead [5]. This overhead is related to:

(a) The exchange of messages that cause delays in users' authentication (i.e., especially in cases that the users are located away from their home network) and consumes radio resources and

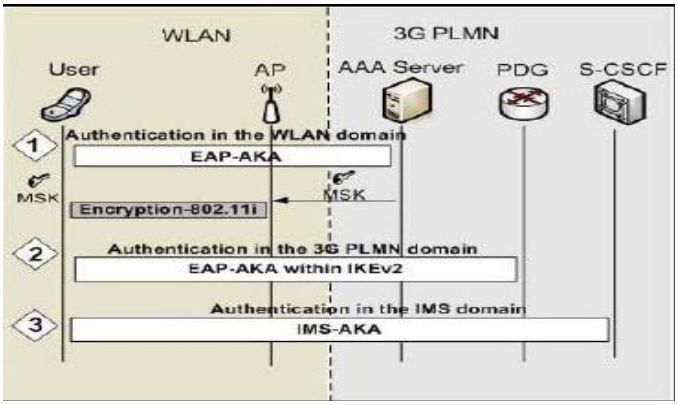


Fig. 1 Multi-pass AKA procedure for IMS service

(b) The computational processing that will consume the limited energy and computational resources at the mobile devices. Therefore, the aforementioned multi-pass AKA procedure deteriorates the overall system performance and may impact negatively on the quality of service offered to the end-users.

## III. SECURITY THREAD OF EXISTING SYSTEM

The main drawback of this authentication procedure is that it is vulnerable to Denial of Service attacks & Man-In-The-Middle attack. An adversary could simply send false authentication messages that the WLAN has to forward to the 3G PLMN causing overflow. To remove this vulnerability requires a secure authentication process between user and PDG (Hashed based or etc).

## IV. SOLUTION

### Shared Key Generation Process:

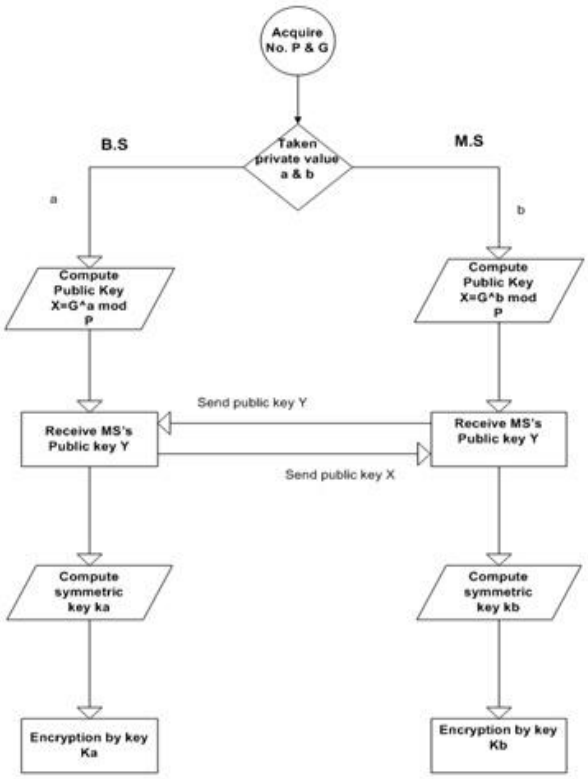


Fig. 2 Generation of symmetric key to Encrypt Management message

### For Secure Key Generation (MK, MSK):

DH key agreement [4] 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 MS, and 'b' is the private key of BS.

SS's public key is *PKMS* = G^a mod P, and

BS's public key is *PKBS* = *G^b* mod P.

The DH key exchange protocol is described as follows where both BS and MS exchange keys.

### Man-in-the-middle Vulnerabilities:

A man-in-the-middle [8] attack is one in which the attacker intercepts messages during the process of communication establishment or a public key exchange and then retransmits them, tampering the information [9] contained in the messages, so that the two original parties still appear to be communicating with each other.

In Diffie-Hellman key exchange process, it is possible to man-in-the-middle attack. Figure 3 illustrated this type of vulnerability in DH key exchange protocol.

In man-in-the-middle attack, a legitimate SS sends its public key to an adversary. This adversary acts as a PDG to a legitimate SS. It also acts as a SS to a legitimate PDG. This way, it can exchange its public key to both SS and PDG. A legitimate SS and adversary exchange keys and both generate the same symmetric key for encryption and evil SS uses this key to communicate with the SS but it also generate another symmetric key to communicate with legitimate PDG. When traffic received from legitimate SS, the evil SS just decrypt the message by the symmetric key generated by DH key exchange protocol and listen the message and finally, again encrypt the message by the symmetric key generated by DH key exchange protocol [7] between legitimate BS and evil SS and send to the legitimate BS.

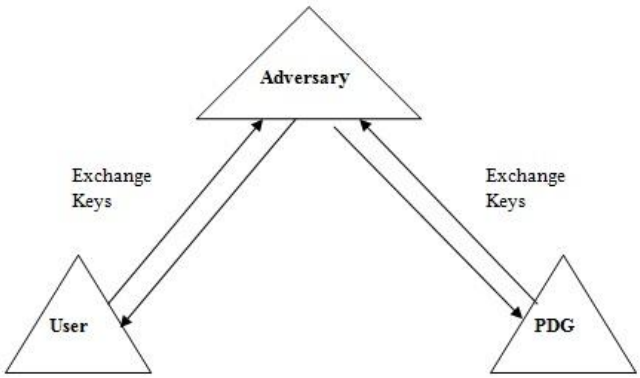


Fig. 3 Man-In-The-Middle Attack

## Improvement of DH Protocol

It is possible to overcome the man-in-the-middle vulnerability by using cryptographic solution.

Sealing functions. In this process every SS has an International Subscriber Station Identity (ISSI) [10] and a cryptographic function as a seal of legitimate SS. The security process is as follows:

**Step1:** SS alleges that it is a legitimate subscriber.

**Step2:** PDG sends a random number, $R_{BS}$ as a challenge to SS.

**Step3:** SS calculates the value of the function for this random number and sends the value and its ISSI number to PDG.

**Step4:** SS sends a random number, $R_{SS}$ as a challenge to PDG that it is a legitimate PDG.

**Step5:** PDG calculates the value of the function by this random number for the corresponding ISSI and sends to PDG.

**Step6:** Only the legitimate PDG knows the function which is used by the given ISSI but not the adversary.

So the adversary is not able to produce correct value for the given random number. Then SS checks adversary identity using the response that it receives, if the PDG is legitimate, the shared key is established and SS continues to communicate with PDG; otherwise, SS ceases the communication.

Suppose a SS's ISSI number is: 0346AE2D and it consists the cryptographic function:

$f(x)= x^3 + x - 5$

Now, the initial communication will be as follows:

**Step1:** SS says that: "I am a legitimate subscriber".

**Step2:** Suppose, PDG sends a random number $R_{PDG} = 3$ to SS as challenge to SS.

**Step3:** SS calculate the value of f(x) =25, and send the value as well as the ISSI number.

**Step4:** PDG also calculates the value of f(x) for the given ISSI number and finds that it is a legitimate SS.

**Step5:** Suppose, SS also sends a random number $R_{MS}$ =5 to PDG as a challenge to PDG.

**Step6:** PDG calculates the value of f(x) =125, send to PDG.

**Step7:** SS verify the value and continue to communicate with PDG if the value of the cryptographic function matches with SS's calculated value. Otherwise SS ceases the communication.

Afterward, both SS and PDG exchange their public key and generate a common key by DH algorithm for exchanging management information and other messages which verify the message authenticity and enhance system reliability that gives no information to attackers.

**Random Number Generation Process:**

Random number for both SS and PDG can be generated by using the system date of the SS and PDG. Although it is not difficult to generate random numbers for a PDG because there are a lot of numbers and keys have to process by the PDG, but very little scope for SS to generate random numbers. Initially, vendors have to define some of the random numbers for a SS and as well as a private number for key generation. Then random numbers will be generated by using the system date or using the given numbers.

**Process1:** Multiplication of the two numbers taken randomly from the given numbers.

**Process2:** Using system date where the random number will be the result of subtraction of the multiplication of current date and month from the year.

**Process3:** It is also possible to generate random numbers by multiplication the current hour, minutes and then subtracts from the result of process2 to generate unique random number every times.

**Function Generation Process:**

To use function as a seal or mark of an authenticate SS [4]; a process must be needed to generate unique functions for a large numbers of SS under each vendor. Although, there are infinite numbers of functions but it must be assigned in a systematic way to ensure that each SS gets a unique function. A systematic way of generating functions for 10,000 SSs is described as follows:

Suppose a vendor wants to assign such functions to 10,000 SSs. For that the vendor makes a table for functions which consists C =5 columns and each column has R =100 functions of same characteristics.

TABLE I

| Polynomial Function | Log Function | Trigonometric Function | Exponential Function |
|---|---|---|---|
| $X^{12}+3X$ | Log2X-33X | Cos5X/2 | $e^{5X+44}$ |
| 190X +1/X | $2X^{11}$ + LogX | Sin2X -21X | $e^{X}+e^{1/X}$ |
| $X^3/5X$ | $X^3/123Log2$ | Tan33X- $X^2$ | $e^{44X+177}$ |
| $44/X^{12}$ | Log4X-230 | 2SinX +33TanX | $1/e^{x}$ |
| $X^2$ - 1X+55X | 3+ Log$X^2$ | CotX –Sec2X | $e^{\sqrt{X}}$ |

So there are total (C×R) =50 functions in the table. Now, the vendor will assign a function to a SS by combining two functions of two columns. So, there are total $R^2 \times \{C (C-1)\}/ 2$ =100,000 numbers of possible functions are available to use. This process is explained in the following example:

Here we see that, there are C =4 columns and R =5 rows in the table created by a vendor. Now the vendor can assign a sealing function to a SS by combining any of two columns. So the first sealing function will be $F(X) = X^{12}+3X$ + Log2X-33X and the second sealing function will be $F(X) = X^{12}+3X +2X^{11}$ + LogX.

In this table there are $R^2 \times \{C (C-1)\}/ 2 = 150$ functions available to assign. Now, a vendor just adds one column and one row to this table then there are 360 unique functions will be available to use which is more than the double of the previous value.

## V. CONCLUSION

NGN architecture is in the environment of network convergence, requirements on openness increase network scales, complexity and potential security problems. Focused on architectures of NGN service provision, this paper discusses existing vulnerabilities. We investigate various vulnerabilities in mobile NGN network and give possible solution to eliminate them. We modify DH protocol to fit mobile NGN we propose DH key exchange protocol to enhance the security level by using random number and function generation process.

## REFERENCES

[1] "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.

[2] "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.

[3] "Security Vulnerability in IEEE 802.16 : Analysis & Solution"- A.K.M. NAZMUS SAKIB, Dr Muhammad Ibrahim Khan, Mir Md Saki Kawsor, Global Journal of Computer Science & Technology, Vol 10, Issue 13, Ver 1, 2010.

[4] "Secure Key Exchange & Authentication Protocol For Multicast & Broad cast Service in IEEE802.16e"- A.K.M. NAZMUS SAKIB, Mir Md Saki Kawsor.

[5] A. Kristensen, A. Byttner, R. Kurmanowytsch. Programming SIP Services. 2000. Berlin.

[6] J. Rosenberg, H. Schulzrinne, G. Camarillo et al. IETF RFC 3261 SIP : Session Initiation Protocol. 2002.

[7] "Shared key Vulnerability in IEEE 802.16e: Analysis & Solution"- A.K.M. NAZMUS SAKIB, Mir Md Saki Kawsor, International Conference on Computer & Information Technology 2010 [IEEE].

[8] H. Lu, L. Conroy, S. Bellovin et al. IETF RFC 2458.Towards the PSTN/Internet Inter-Networking-Pre-PINT Implementations. 1998.

[9] IETF RFC 1994. PPP Challenge Handshake Authentication Protocol (CHAP). 1996.

[10] J.R. Dianda, V.K. Gurbani, M.H. Jones. Session Initiation Protocol Service Architecture. Bell Labs Technical Journal, 2002.7(1): p. 3-22.

[11] J. de Keijzer, D. Tait, R. Goedman. JAIN : A New Approach to Services in Communication Networks. IEEE Communication Magazine, 2000(January): p. 94-99.

[12] R. Raj, R. Gupta. JAIN Protocol APIs. IEEE Communication Magazine, 2000(January): p. 100-107.

[13] V. K. Gurbani, X. H. Sun. A Systematic Approach for Closer Integration of Cellular and Internet Services. IEEE Network, 2005(January/February): p. 26-32.

[14] Fanchun Yang. Key technologies towards next generation network. Journal of Beijing University of Posts and Telecommunications, 2003. 26(1): p. 1-8.

[15] R. Stewart, M. Tuexen, G. Camarillo. Internet Draft Stream Control Transmission Protocol (SCTP) Security Threats draft-ietftsvwg- sctpthreat-00.txt. 2006.

[16] T. J. Walsh, D. R. Kuhn. Challenges in Securing Voice over IP. IEEE Security & Privacy, 2005(May/June): p. 44-49.

[17] B. Harris, R. Hunt. TCP/IP security threats and attack methods. Computer Communication, 1999. 22: p. 885-897.

[18] R. H. Glitho, F. Khendek, A. De Marco. Creating Value Added Services in Internet Telephony : An Overview and a Case Study on a High-Level Service Creation Environment. IEEE Transaction on System, Man, and Cybernetics - Part C : Application and Reviews,2003. 33(r).

[19] A. Moerdijk, L. Klostermann. Opening Networks with Parlay / OSA: Standards and Aspects Behind APIs. IEEE Network, 2003(May/June): p. 58-64.

[20] V. Gurbani, A. Brusilovsky, I. Faynberg et al. IETF RFC 3910 The SPIRITS (Services in PSTN requesting Internet Services) Protocol. 2004.

[21] ITU-T Draft Recommendation Y.NGN-overview, General Overview of NGN Functions and Characteristics. 2001.

[22] ETSI ES 202 915. Open Service Access (OSA); Application Programming Interface(API). 2003.

[23] International Organization for Standardization: "ISO/IEC 15693 - Identification cards – Contactless

[24] U.S. General Service Administration: "Government Smart Card Handbook", February 2004.

[26] D. MALTONI, D. MAIO, A.K. JAIN, S. PRABHAKAR: "HANDBOOK OF FINGERPRINT RECOGNITION," SPRINGER, NEW YORK, 2003