VOL. 12, NO. 22, NOVEMBER 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

MAN-IN-THE-MIDDLE-ATTACK PREVENTION USING INTERLOCK PROTOCOL METHOD

Robbi Rahim
Akademi Perekam Medik dan Infokes Imelda, Jl. Bilal, Kota Medan, Sumatera Utara, Indonesia
E-Mail: usurobbi85@zoho.com

ABSTRACT

In the process of data communications, although data has been encrypted, there is the possibility of such data can be known by others. One possibility is that the person intercepts the communication medium used by the two individuals who are communicating. This technique called man-in-the-middle-attack. This research provides a step-by-step procedure for securing messages from man-in-the-middle-attack attacks with interlock protocols where the process of sending messages is encrypted using the RSA algorithm, and test results show that the use of interlock protocols can overcome man-in-the-middle-attack.

Keywords: man-in-the-middle-attack, interlock protocol, intercept communication, prevention attack.

INTRODUCTION

In the process of data communications, although data has been encrypted, there is the possibility of such data can be known by others [1] [2] [3]. One possibility is that the person intercepts the communication medium used by the two people who are communicating [1]. This technique is called man-in-the-middle-attack. In this circumstance, the person who tapped is between the two people who are communicating. The data transmitted by people who are communicating with each other is always through the individual who tapped them so that the wiretapped person can know all the information sent to each other [1]. This state of affairs arises because the two communicating persons are unable to verify the status of the person communicating with them [1] [4], taking the assumption that the interception process does not cause interference in the network.

This man-in-the-middle-attack problem can illustrate as follows, suppose Alice and Bob are communicating, and Mallory wants to tap into it. When Alice sends her public key to Bob, Mallory can grab this key and send Bob's public key. Then, when Bob sends his public key to Alice, Mallory can also catch the key and send Alice her public key. When Alice sends a message to Bob who is encrypted using Bob's public key, Mallory can catch it. Since the message is encrypted using Mallory's public key, Mallory can decrypt the message using its private key and then re-encrypted using the public key from Bob and send it to Bob. The same thing happened when Bob sent Alice a message. Mallory can find out all the messages sent by Bob and Alice. This man-in-the-middle-attack problem can prevented by using an interlock protocol. The interlock protocol created by Ron Rivest and Adi Shamir. The core algorithm of this protocol is that this protocol sends two parts of encrypted message [5]. The first part can be the result of the one-way hash function of the message and the second part is the encrypted message itself. This procedure will cause the wiretapped person to be unable to decrypt the first message by using its private key. It can only create a new message and send it to the person who will receive the message.

THEORY

Cryptography is a science that studies mathematical techniques related to aspects of information security such as confidentiality, data integrity, sender/data receiving authentication, and data authentication [2] [5] [3] [6].

Cryptography aims to maintain the confidentiality of the information contained in the data so that the information cannot be known by unauthorized parties [5] [7], there are several demands related to data security issues, such as:

1. Confidentiality. Ensure that these data can only be accessed by certain parties only.
2. Authentication. Whether sending or receiving information, both parties need to know that the sender of the message is the actual person as claimed.
3. Integrity. This demand relates to the guarantee that each message sent must be received by the recipient without any portion of the message being replaced, duplicated, defaced, altered, and added.
4. Nonrepudiation. Prevent senders and beneficiaries from denying that they have sent or received a message/information. If a message is sent, the recipient can prove that the message was indeed sent by the sender listed. Conversely, if a message is received, the sender can prove that the intended party has been given the message.
5. Access Control. Limit data sources only to specific people.
6. Availability. If required at any time all information on a computer system must be available to all parties entitled to such information.

Six aspects of data security, four of them can be overcome by using cryptography that is confidentiality, integrity, authentication, and nonrepudiation.

Rivest-Shamir-Adleman (RSA) algorithm

RSA is one of the techniques of encryption and decryption using two keys. The keys are obtained from the calculation of exponential, multiplication, division, sum

and subtraction. The calculation is performed on two prime numbers [2].

Types of attack patterns

Data and information protection in computer communications is necessary because of the value of information itself and the increasing use of computers in various sectors. Seeing the fact that more data is processed by computers and sent through electronic communication devices then the threat to data security will increase [2]. Some threat patterns or attacks on computer data communications can explain as follows:

1. Interruption

Interruption occurs when data sent from A does not reach the proper person (B). Interruption is the pattern of attack on the nature of availability.

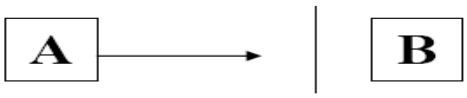

Figure-1. Interruption.

2. Interception

This attack occurs when a third party C manages to read the data sent. Interception is an attack pattern on the nature of confidentiality.

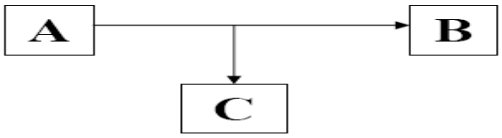

Figure-2. Interception.

3. Modification

In this attack, the third party C managed to change the message sent. The modification is an attack pattern on the nature of integrity.

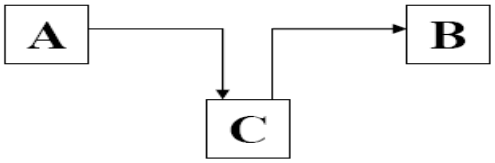

Figure-3. Modification.

4. Fabrication

In this attack, the attacker successfully sends data to the destination by exploiting the identity of others. Fabrication is the pattern of attack against the nature of authenticity.

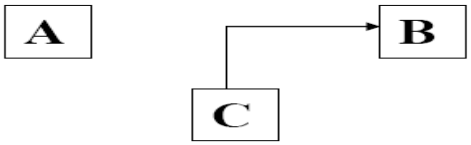

Figure-4. Fabrication.

Man-in-the-middle attack

In the process of data communications, although data has encrypted, there is the possibility of such data can be known by others [8]. One possibility is that the person intercepts the communication medium used by the two people who are communicating. This technique is called man-in-the-middle-attack [8].

This situation arises because the two persons who are communicating are unable to verify the status of the person communicating with them, taking the assumption that the interception process does not cause interference in the network [8] [9]. To be clearer, see the following image:

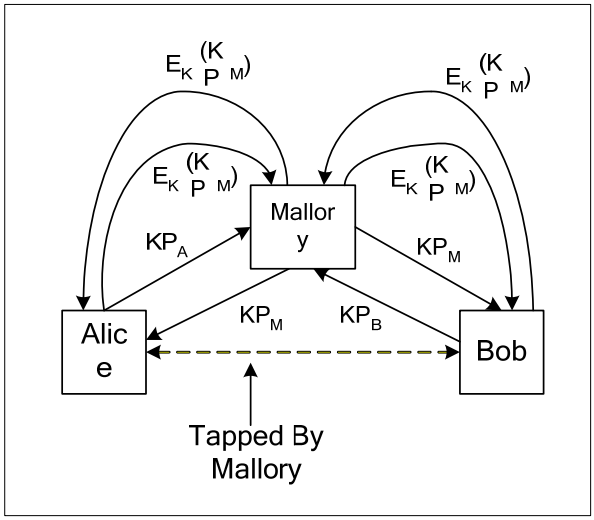

Figure-5. Man-in-the-middle attack procedure.

Interlock protocol

This man-in-the-middle-attack problem can be overcome by using an interlock protocol. The interlock protocol was created by Ron Rivest and Adi Shamir. The core algorithm of this protocol is that this protocol sends two parts of encrypted message [1].

The first part can be the result of the one-way hash function of the message and the second part is the encrypted message itself [1] [9].

This causes the wiretapped person to be unable to decrypt the first message by using its private key. It can only create a new message and send it to the person who will receive the message [9]. In short, the workings of the interlock protocol are as follows:

1. Alice sends her public key to Bob.
2. Bob sends his public key to Alice.
3. Alice encrypts the message by using Bob's public key. Then, send part of the encrypted message to Bob.
4. Bob encrypts his message using Alice's public key. Then, send a partially encrypted message to Alice.
5. Alice sends another part to Bob.
6. Bob combined both Alice messages and decrypted using his private key.
7. Bob sends the other piece to Alice.
8. Alice combined both Bob's messages and decrypted using her private key.

RESULTS AND DISCUSSIONS

Testing Man-in-the-middle-attack using RSA cryptographic algorithms, so the first step is to generate the keys Alice, Bob and Mallory have, and the process can see below:

Alice Key Calculation
---

1. p = 7639, q = 773
2. n = p * q
   n = 7639 * 773

   n = 5904947

3. e = 865, GCD(e,(p-1)(q-1)) = 1.
4. d = e^(-1) mod ((p-1)(q-1)). (Extended Euclidean)
   d = 2651737

5. Public key alice:
   e = 865

   n = 5904947

6. Private key alice:
   d = 2651737

Bob Key Calculation
---

1. p =991, q = 9059
2. n = p * q
   n = 991 * 9059

   n = 8977469

3. e = 6271, GCD(e,(p-1)(q-1)) = 1.
4. d = e^(-1) mod ((p-1)(q-1)). (Extended Euclidean)
   d = 8885911

5. Public key bob:
   e = 6271

   n = 8977469

6. Private key bob:
   d = 8885911

Mallory Key Calculation
---

1. p = 31319, q = 191
2. n = p * q
   n = 31319 * 191

   n = 5981929

3. e = 558, GCD(e,(p-1)(q-1)) = 1.
4. d = e^(-1) mod ((p-1)(q-1)). (Extended Euclidean)
   d = 1623813

5. Public key mallory:
   e = 558

   n = 5981929

6. Private key mallory:
   d = 1623813

The man-in-the-middle-attack attack process performs during communication between Alice and Bob, and Mallory already knows the public Alice and Bob keys, the process of interlock protocol step by step to overcome man-in-the-middle-attack.

ALICE sends a message to the BOB by using an interlock protocol - message sharing
---

Message = 'password'
Change message to binary
01110000011000010111001101110011011101110110111
10111001001100100

Change every three binary bits into decimal shapes:
3406056334673557344620

Input any 4-digit decimal (m) to the encryption function: c = (m ^ e) mod n
(Use Mallory public key)
c = (3406 ^ 557) mod 5981929 = 169237
c = (0563 ^ 557) mod 5981929 = 1518521
c = (3467 ^ 557) mod 5981929 = 4320844
c = (3557 ^ 557) mod 5981929 = 803784
c = (3446 ^ 557) mod 5981929 = 3924592
c = (2000 ^ 557) mod 5981929 = 4282610

Encryption results:
169237 1518521 4320844 803784 3924592 4282610

The results of encryption are divided into two parts, such as:

Part-1 = 193 582 304 07432524860
Part-2 = 62711514284838 949 221

Mallory decrypts ALICE's message using its public key

CipherText = '193 582 304 07432524860'

Input the cipher text (c) into the decryption function: m = (c ^ d) mod n (use private key mallory)

m = (193 ^ 1623813) mod 5981929 = 3109040
m = (582 ^ 1623813) mod 5981929 = 947053
m = (304 ^ 1623813) mod 5981929 = 1832855
m = (07432524860 ^ 1623813) mod 5981929 = 408785

Decryption Results:
310904094705318328554085785

Change message to biner:
011001000000100000100111000101011001011010101101100000111101

Change every 8 bit binary to ASCII form:
d'–-*f*
(The message cannot be read, Mallory failed to tap and read messages from ALICE)

Mallory changed the message and encrypted the alias using the BOB public key, and send to Bob
---
Message = 'pin-atm'

Convert message to binary:
011100000110100101101110001011010110000101110100011011101

Change every three binary bits to decimal form:
3406455613260564332

Input any 4-digit decimal (m) to the encryption function: c = (m ^ e) mod n
(user Mallory public key)
c = (3406 ^ 6271) mod 8977469 = 8842881
c = (4556 ^ 6271) mod 8977469 = 4287565
c = (1326 ^ 6271) mod 8977469 = 7436799
c = (0564 ^ 6271) mod 8977469 = 7805235
c = (3320 ^ 6271) mod 8977469 = 2087393

Ciphertext Results:
8842881 4287565 7436799 7805235 2087393

Alice send Part-2 Message, Mallory decrypts ALICE's message using its public key
---

Cipher Text = '62711514284838 949 221'

Input the cipher text (c) into the decryption function: m = (c ^ d) mod n
(use Mallory private key)
m = (62711514284838 ^ 1623813) mod 5981929 = 1041165
m = (949 ^ 1623813) mod 5981929 = 4539008
m = (221 ^ 1623813) mod 5981929 = 3131290

Decryption results:
104116545390083131290

Convert message to binary:
001000100001001110101100101011000000011001011001010000

Change every 8 bit binary to ASCII form:
"¬¬Y(The message cannot read, Mallory failed to tap and read messages from ALICE)

Mallory changed the message and encrypted the alias using the BOB public key and send it to Bob
---

Message = 'idcard'

Convert message to binary:
011010010110010001100011011000010111001001100100

Change every three binary bits to decimal form:
3226214330271144

Input any 4-digit decimal (m) to the encryption function: c = (m ^ e) mod n
(use Mallory public key)
c = (3226 ^ 6271) mod 8977469 = 1710719
c = (2143 ^ 6271) mod 8977469 = 268916
c = (3027 ^ 6271) mod 8977469 = 7360313
c = (1144 ^ 6271) mod 8977469 = 4906594

Encrypt results:
1710719 268916 7360313 4906594

The encryption results combined into:
81874120878119 4226887951665 77346306371939 47980065529345 2087393

CipherText = '81874120878119 4226887951665 77346306371939 47980065529345 2087393'

Input the cipher text (c) into the decryption function: m = (c ^ d) mod n
(use Mallory private key)
m = (81874120878119 ^ 1623813) mod 5981929 = 4846004
m = (4226887951665 ^ 1623813) mod 5981929 = 0183
m = (77346306371939 ^ 1623813) mod 5981929 = 3560196
m = (47980065529345 ^ 1623813) mod 5981929 = 750638
m = (2087393 ^ 1623813) mod 5981929 = 1779483

Decrypt result:
484600401833560196750638177948 3
Convert message to binary:
100100110000000100000000101101110111000000011101 1
110100011001100111111111100011

Change every 8 bit binary to ASCII form:
“nàw£3ü———————————————— (Message Illegible, And Disguises Tapping Procedure Order By Mallory Not Succeed)

The testing process already finish and could be see that the use of interlock protocol in the process of handling man-in-the-middle-attack attacks successfully done and eavesdroppers cannot know the data or messages sent between Alice and Bob

CONCLUSIONS

After completing the use of interlock protocol method to overcome man-in-the-middle-attack, the authors draw conclusions by using interlock protocol, although the receiver and sender's public key is acquired and replaced by eavesdroppers, eavesdroppers cannot run man-in-the-middle-attack to view and change messages. This is because the encrypted message is split into two parts and the delivery is done gradually so that the eavesdroppers cannot know the original message that was sent.

REFERENCES

[1] S. Glass, V. Muthukkumurasamy and M. Portmann. 2009. Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks. in International Conference on Advanced Information Networking and Applications, Bradford, UK.

[2] R. Rahim and A. Ikhwan. 2016. Study of Three-Pass Protocol on Data Security. International Journal of Science and Research (IJSR). 5(11): 102-104.

[3] R. Rahim. 2017. 128 Bit Hash of Variable Length in Short Message Service Security. International Journal of Security and Its Applications. 11(1): 45-58.

[4] G. N. Nayak and S. G. Samaddar. 2010. Different flavors of Man-In-The-Middle attack, consequences and feasible solutions. in 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), Chengdu, China.

[5] R. Rahim and A. Ikhwan. 2016. Cryptography Technique with Modular Multiplication Block Cipher and Playfair Cipher. IJSRST. II(6): 71-78.

[6] S. D. Nasution, G. L. Ginting, M. Syahrizal and R. Rahim. 2017. Data Security Using Vigenere Cipher and Goldbach Codes Algorithm. International Journal of Engineering Research & Technology (IJERT). 6(1): 360-363.

[7] A. P. U. Siahaan and R. Rahim. 2016. Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm. International Journal of Security and its Application. 10(8): 173-180.

[8] T.-H. Cho and G.-M. Jeon. 2016. Dynamic Delay Time Decision Method for Enhancing Security of the Forced Latency Interlock Protocol in Internet of Things. International Journal of Research - GRANTHAALAYAH. 4(2): 151-158.

[9] D. S. R. Murthy, B. Madhuravani, and G. Sumalatha. 2012. A Study on Asymmetric Key Exchange Authentication Protocols. International Journal of Engineering and Innovative Technology (IJEIT). 2(2): 100-104.