Detection of Intruder in Secure Roaming Service

[1]S.Sangeetha, [1]D.Jebakumar Immanuel
[1]P.G.Scholar, [1]Assistant Professor (SG)
Department of Computer Science and Engineering
SNS College of Engineering, Coimbatore, India.

Abstract-- Mobile computing plays a vital role in today environment. Now a day it act as a pervasive computing that is any time any where computing. In that roaming service enables the wireless device to be kept connected with the network without breaking the network connections. During the roaming service data to be maintain integrity, and also to have strong anonymous authentication group signature algorithm is used. In order to detect internal attacker root canal algorithm is used. Root canal algorithm is used to detect the host attacker. It also helps to protect the program code.

Index Terms-- Pervasive Computing, Roaming Services, Group Signature, Internal Attacker, Root Canal Algorithm.

I. INTRODUCTION

Roaming service will be takes place in anywhere at any time. It is important to secure ones data. Attacker will have many possible ways to attack our data. Protecting our valuable data is must. Today we have more software to protect our data but in olden days data protection is not easy. For robbery in those days they will keep single guard for night will be provided to control the robberies. Another option is to keep their valuable asset in safer place in bank. But earlier they came to understand that also is not an effective one because the one who protect the asset may also be another attacker which is known as internal attacker that is attacker within the organization.

Today[1] assert protection is an easier one. There are many factors came to fight against attacker. Some of them were used to have voice, signature etc. Even though there are much software was build to protect the data attackers is attacking the data is also common. So still we are fighting with the attacker to protect our data.

Whenever we are talking about security there are three important aspect to address it they are

1. Confidentiality

2. Integrity

3. Availability

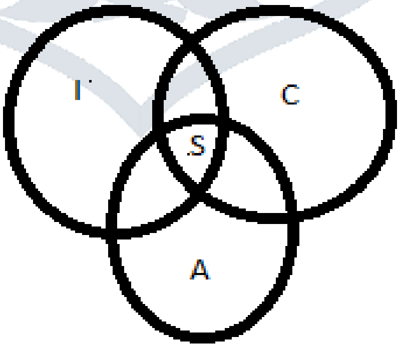

Fig 1.1 Relationships between Security versus Confidentiality, Integrity, and Availability.

II. BACKGROUND

Consider[1] the following procedure to know how the intruder will attack or block the data. A will be sender and B will be the receiver. A will be sending data to B using transmission medium. This transmission medium is consider as T. Where O is an outside attacker which attacks the data sending from sender A to receiver B. Any time after A transmit the data via T then O might try to access the message in any of the following ways:

1. **BLOCK**

Block prevents the data moving from sender A, thereby affecting the availability of the messages.

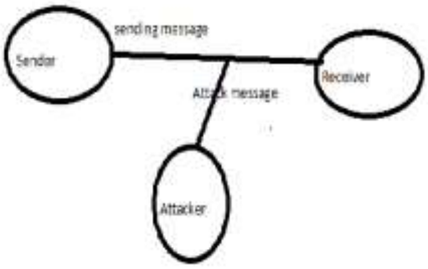

Fig 2.1 blocking the message

2. **INTERCEPT**
It refers to reading the message or listening the message will cause affecting the confidentiality of the data.

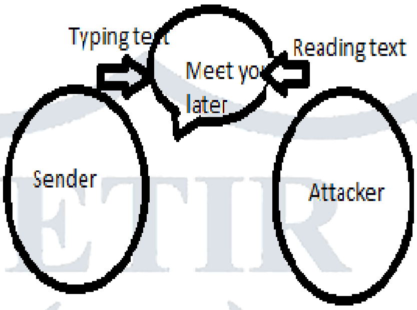

Fig 2.2 Affecting Confidentiality

3. **MODIFY**
Modify ensures the data to be losing its integrity of the original content that is making some changes to the original message by inserting unwanted data or by deleting the original data etc.

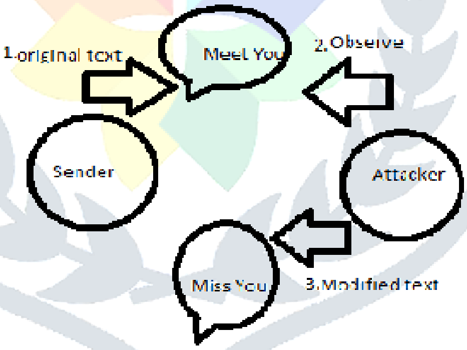

Fig 2.3 Modification of the original content by adding or deleting.

4. **FABRICATE**
When transferring huge data from sender A to receiver B data arranged by the sender will be rearranged when it receives to receiver also affect data integrity.

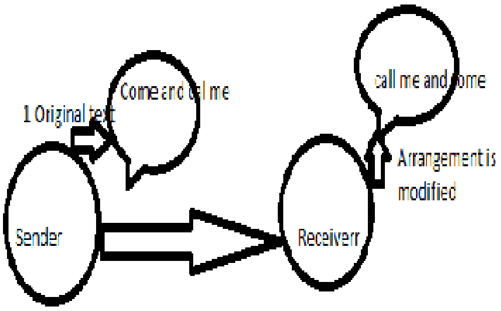

Fig 2.4 Modification in arrangement of the message

In this paper [4] we had a discuss about various kinds of security issues that are used for securing the data when communicating between them.

.

III. INTRUSION DETECTION SYSTEM (IDS)

Intrusion detection is used to find the internal attacker [2][3] who are revealing details about the organization to easily gain the details about the organization. Internal attacker are the one who are depending within the organization. This can be identified by two techniques: protection and detection. Protection used to protect the data from attacker for e.g., masquerade attackers. This mechanism states that when any two people were sharing data between themselves an attacker will be occurred to attack the data before data receiving to another person. These types of attacker will be attack the data and modifies them and transform to another person by acting as original person sending the data. Detection were used to identify who is the attacker and what technique he/she used to attack the data.

These intrusions can be identified by monitoring following process of mobile user. First mobile originating and termination calls should be monitored and details should be collected. Handovers also should be monitored when moving from one network service to another network service. Location updating also be tracked when moving devices to home location to any visiting location and their accessing details will be mentioned in clear manner.

We have defined three levels of intrusion detection can be performed. The levels are: level 1, level 2, level 3[7].

Level 1: It is used to have fast identification of intruder based on velocity and clone verification of data transmitted. Clone states that same person ID hass been established on different network.

Level 2: This will be enhancing the subscriber moving to different networking and the frequency variations which cause the attacker to attack the data.

Level 3: This will be helps to identify the internal attacker with the help of subscriber details that is profile details. If any irrelevant activities found from subscriber than their usual activities then service provider can easily found that some internal attacker has been found.

Whenever these attacker found then there will be raising of alarem will be placed inorder to altert them that something unusual things were happening on network[8].

IV. EXSISTING TECHNIQUES

1. WORMHOLE ATTACK

Wormhole attack[4] used to attack the routing path of the data. Routing path will be tunneled into another route. This happens by the attacker will be monitoring the route and tunnel them into another networking path. By disrupting the routing control message threats will be occurring.

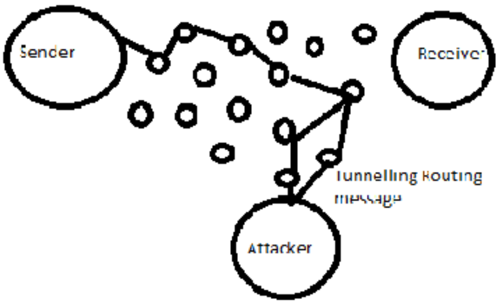

Fig 4.1 Tunneling Routing Message

2. UNSECURED WIRELESS CHANNEL

Whenever[4] data is sending from the sender to receiver they transfer the data through transmission medium. This transmission medium will be always in opened manner which will leads to attacker to attack the data. To avoid this situation regular monitoring is needed. Attacker will be monitoring the transmission channel once they attack the medium then malicious activity will be done.

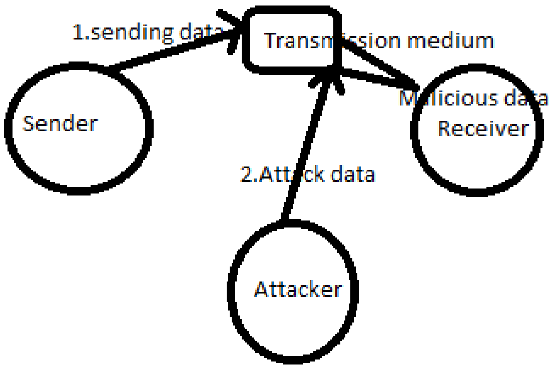

Fig 4.2 Attack on Transmission Medium

3. STATE POLLUTION ATTACK

State[5] pollution attack enables corrupting the parameters. This will lead to packet forwarding into malicious destination. It is one type of internal attacks. By corrupting the parameter data will be moving to destination of attacker.

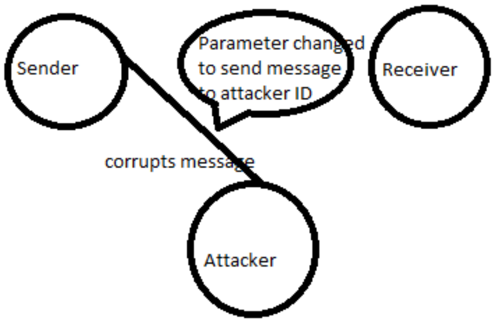

Fig 4.3 Attack on parameter

4. **RUSHING ATTACK**

As[5] the name suggest rushing attack defines that when the data is sending through the node duplicate node is created. When the original node flood the data to nearest node duplicate node also will get the data. Immediately the duplicate node will flood the data to the same nodes. These nodes will take that data is repeated so they will drop the data without forwarding to near nodes. This also an attack which lead to loss of data.

5. **BLACKHOLE ATTACK**

This[5] type of attack will mainly attack the shortest path or stable path. The black hole attack will be disrupting the path moves from source to destination and hide the path without forwarding the data to destination.

V. PROPOSED WORK

1. GROUP SIGNATURE ALGORITHM

In CPAL [6] accessing data in a secure manner made a tedious process. In order to achieve data integrity while sharing in roaming service we propose two main algorithm known to be group signature and diffie-hellman key exchange. These two algorithm is used to hide the MS-ID to FN and get authentication from HN.HN only knows the MS-ID. Group signature allows the FN to show some one has been entered to get service but they don’t know their ID. By getting authority from HN the services from VH will be provided to MS. It mainly focus on achieving two factors that are universal secure roaming service and multilevel access link ability. This done on heterogeneous networking. It also supports revocation function when any unusual messages from endowers try to jam the data sharing. Existing secure roaming does not support revocation function and it is implemented only in homogeneous networking. Existing work mainly done based on three algorithm they are Symmetric Cryptography based scheme Asymmetric Cryptography based scheme and Hybrid scheme (i.e. combination of both algorithm).To overcome the drawbacks of existing work CPAL has been emerged. Main contribution of CPAL is to provide the following functions:

1. **Strong Anonymous Authentication**

Whenever there occurs an interaction between the MS and VH the data sharing should not reveal to the third party i.e unauthorized person, strong anonymous authentication should be maintained.

2. **Session Key Agreement**

Both the MS1 and MS2 should agree on key agreement to protect data while in roaming service to share data.

3. **User Tracking**

When the user moving from one networking to another networking service provider should keep tracking of the current use of the user.

4. **Anonymous User Linking**

Link ability should be maintained when the user moving on to have different service offering in different networking.

Along with this as already stated internal attackers were in many types. Some of them are mobile IP attacker, DNS attacker, host attacker, etc. To overcome disadvantage of internal attacker stated in CPAL root canal algorithm[7] is used .

2. ROOT CANAL ALGORITHM

```
1)Agent at creator S0

i)Hcode= H(Agent Byte Code)

ii.     EHcode = EPR0 (Hcode)

   i.   S0 →Si : Ehcode
   ii.  C=File 1,File 2

2)      Agent at Remote host Si, File 1

i.      RHcode= DPUi-1(EHcode)
ii.     Hcode= H(Agent Byte Code)
iii.    If ( RHcode== Hcode) then
a)      Collect Di
b)       rdi= EPU0 (SigPRi(Di)||Di||Si|| Si+1)
c)       RDi=rdi|| H(rdi)
d)      EHcode = EPRi (Hcode)
e)       Si →Si+1 : EHcode
        Si → S0 : RD
f)                          Else
           Si → S0 : Msg (Error code)

        S0 →Si : msg(Error Data)
3)      Agent at Remote host Sn   , File 2

     i.   RHcode= DPUn-1(EHcode)
     ii.  Hcode= H(Agent Byte Code)
     iii. If ( RHcode== Hcode) then
     a)   Collect Dn

     b)    rdi= EPU0 (SigPRn(Dn)||Dn||Sn|| S0)
     c)    RDn=rdn|| H(rdn)

     d)   EHcode = EPRn (Hcode)

          Sn →S0 : EHcode
     e)
     f)    Sn → S0 : RD
              Else

                 Sn → S0 : Msg (Error code)

4)      Agent at S0
        For each RDi
      i. rdi|| RH(rdi) =RDi
      ii.     if H(rdi) = RH(rdi)) then

 a)     SigPRn(Dn)||Dn||Sn|| S0=DPR0(rdi)

 b) if (DPUi(SigPRn(Dn))==Dn)
C=(File 1||File 2)= Valid
        Process Di
         Else
```

S0 →Si : msg(Error Data)

Root canal algorithm is used to find the internal attacker. It states that attacker will be within the organization. Home sever may also contain attacker. For their well probe they can allow the attacker to enter into their organization and attack the data. For that they use hashing technique. Along with that they use signature for verification. The attacker can extract the original ID of the user and change the programming code. Thus by changing the code tha data send by the ID will be moving to the attacker side. Hence they can easily attack the data. By using root canal algorithm we can easily detect which host ID is being affected. For that continuous monitoring is needed. Whenever there is difference in data transmission then they can identify the attacker has been entered.

VI.CONCLUSION

Above details stated the Universal secure roaming services. It also states some of the functions to be used in secure roaming services to have data sharing should be an authorized one without breaking the network connection. Basic principle behind in roaming service help the user to provide services when the user move out-off coverage area that is from his/her home network. The overall process describe about the outside attacker and the prevention they handled using root canal algorithm.

VII. REFERENCES

[1] Charles P. Pfleeger, Shari Lawrence Pfleeger, Security in computing, Third Edition 2007.

[2] G.B. White, E.A. Fish and U.W. White, «Cooperating Security Managers: A Peer-Based intrusion Detection System», IEEE Network Magazine, January/February 1996.

[3] D. Samfat, V. Devernay, C. Bonnet, «A GSM Simulation Platform for Intrusion Detection», Proceedings of ICC'95, Seattle, June 1995.

[4]Hariom Soni, Preeti Varma, “A survey of performance based secure routing protocol in MANET”,IJARCET, Volume 2, Issue 1, Jan 2013.

[5]Mahendra Kumar, Ajay Bhushan, Amit Kumar,” A Study of wireless Ad-Hoc Network attack and routing protocol attack”, IJARCSSE, Volume 2, Issue 4, Apr 2012.

[6]] J. Y. Hwang, S. Lee, B. Chung, H. S. Cho, and D. Nyang. Group signatures with controllable linkability for dynamic membership. Information Sciences, 222:761-778, 2013.

[7]Geetha .G, Jayakumar .C,” Protection of free roaming mobile agent using root canal algorithm against malicious host attacker”, JTAIT, Vol. 62 No.2.20 April 2014.