Type based vital memory access in specific shielded mobile agent

V.Arun[1], Dr. K.L. Shunmuganathan[2]

[1]Ph.D Research Scholar,Sathyabama University,Chennai,India
[2]Prof and Head of CSE , R.M.K Engineering College, Thiruvallur, India

Abstract

Mobile computing ensures the portable flexibility for the mobile devices. Various services and application are provided for these devices for entertainment and other aspects. But the targeted devices are subjected to intrusion when the service provider access irrelevant confidential data such as contact details, credit card number etc. Shielded Mobile Agent (SMA) [1] ensures intrusion prevention measure to generic levels. But access to the vital memory by a service provider can access irrelevant data apart from the data requested. We introduce a new mobile agent replacing SMA and new file system for vital memory. We used Tracer and Checker Model [2] to provide intrusion detection in the system along with the SMA.

Keywords: mobile computing, intrusion mechanism, Specific SMA Intrusion model, Shielded mobile agent

1. Introduction

1.1. Tracer and Checker Model

TCM, a model to assist the network against intrusion, is used in this paper to support mobile host [2]. TCM Server uses Tracer Mobile Agent to check any intrusion in host and raise alarm in the system. Checker Mobile Agent prevents intrusion in other host by checking the malicious host .Mobile host is registered with TCM and in addition with unique ids generated in TCM, it carries sandbox UID (Unique Identification) for each host. Service client provides the service necessary for the mobile host and sandbox act as a barrier between the vital memory and service provider. TCM service provider resides in the mobile host and interacts with the TCM server.

1.2. Vital Memory

Mobile host holds vital information which is stored in memory hardware is organized in a safer way known as vital memory. Sandbox can have only access to the vital memory so that any service to interact with the vital memory can interact on the sandbox. Vital memory normally refers to the stored user data in mobile host which are usually credit card information, personal user data such as important contact details etc. Vital memory stores the information in encrypted way so that even hacked hardware information provides no use to the outsiders.

1.3. Sandbox

Sandbox is a platform to run the entrusted programs with restrictions. Usually it is used in development phase of a program since the behavior of developing program may affect the system. In this paper, sandbox refers a region to run the application services that access the vital memory of the system. The service will get mounted in the sandbox and sandbox knows the way to handle the vital memory.

1.4. TCM Service Provider

It interacts with the TCM server [2] to obtain the information required for the sandbox. Sandbox can access the vital memory through the password which keeps on changing by the TCM server. It connects to the TCM server to obtain the information and also to change the password in course of time automatically.

ISBN 978-93-82338-91-8 © 2013 Bonfring

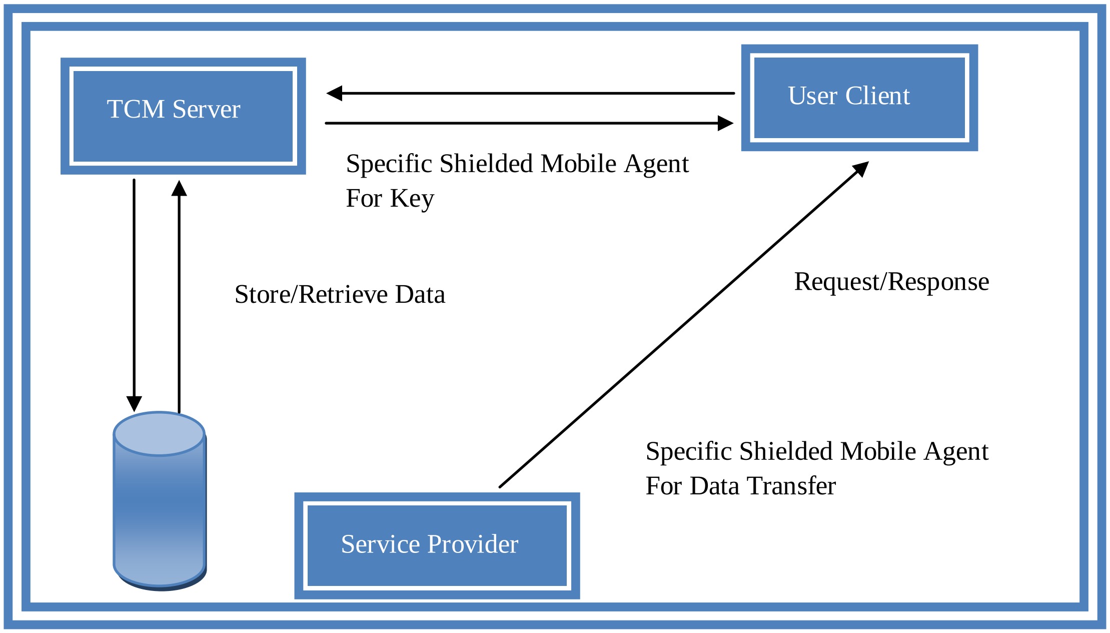

Fig.1. Overall Architecture

2. Vital File System

Vital memory holds credential information in a unique file system as described here. Each file is distinguished with unique ids based on the user defined labels. Since each information is related to some type of genre, user defined types are related to the file in the vital system.

Table.1. Sample data and Type relationship

Data	Type	Unique ID	Unique Key
Data1	Type1	UID1239546	128bit Key1
Data2	Type2	UID6623345	128biy Key2
Data3	Type 1	UID1239546	128bit Key1
Data4	Type 1	UID1239546	128bit Key1
Data5	Type2	UID6623345	128biy Key2

Each file in the vital memory is organized with a type described by the user. Each type possess unique id generated by the TCM server and a key is generated for each unique ID. When a service requires a resource to access the vital memory, the priority attaches the type of resource required by the service provider.

3. Storage Mechanism

User may store vital information to the mobile host through sandbox. Sandbox receives the information and follows the following steps.

- Sandbox generates a unique id for the information entered by the user
- Search Type for the information. If not exists, SSMA registers the new type to the TCM server.
- Encrypt with the Type Key (128 bit) using RSA Algorithm.
- Queries TCM service provider for the 128 bits key.

- Perform encryption process and store in the memory location along with the table entry about memory address and unique id.
- Double encryption is performed on the data to ensure type and data based encryption.

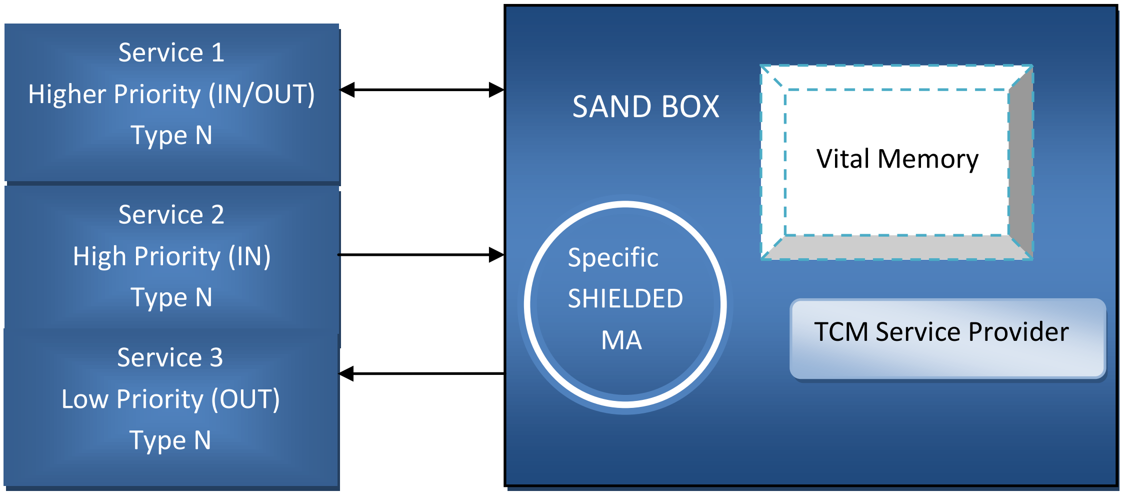

Fig.2.Mobile Host Architecture

Sample memory processed by sandbox and unique id allocation. Consider a word holds 8 bits and user stores two vital memories. Information A holds 16bits and 3 Data holds 32bits.

Data1 -> Type1 Data2 -> Type1 Data3 -> Type2

Table.2.Memory Segment in Vital memory with File System

Data	Memory Address	Unique Memory ID	Generated Key	Type Key
Data1	0x9FFF0-0x9FFF8	MID6985455	Key1(128 bits)	Type1 Key1
Data2	0x9FFF9-0xA0000	MID6985488	Key2(128 bits)	Type1 Key1
Data1	0xA0001-0xA0008	MID6985455	Key1(128 bits)	Type1 Key1
Data3	0xA0009-0xA0010	MID6985488	Key2(128 bits)	Type2 Key1
Data2	0xA0011-0xA0018	MID6985488	Key2(128 bits)	Type1 Key1
Data3	0xA0019-0xA0021	MID6985488	Key2(128 bits)	Type2 Key1

4. Memory Encryption

128 bit key is used to encrypt the memory block using Advanced Encryption Standard algorithm. Intrusion in the vital memory result in no loss of any information since encryption is information dependent and not memory depended since TCM server only knows the key for it. Type key are unique for data that belongs to same type. So double encryption is performed rather than a single, thus ensure a most reliable model than SMA.

Table.3.Priority Pattern

Service	Priority	Description
IN/OUT	Higher	128bit Key1
IN	High	128biy Key2
OUT	Normal	128bit Key1

4.1. Combination with Priority and Type

Let P1, P2, P3 be the priority. Let T1,T2,T3 be the types for data D1,D2,D3,D4,D5,D6,D7,D8,D9, D10. Relation between data and type be - D1, D2, D3 belongs to T1 type; D4, D5, D6 belongs to T2 type; D7, D8, D9, D10 belongs to T3 type. Possible combination request by the service provider will be

(P1, T1) (P1, T2) (P1, T3) (P2, T1) (P2, T2) (P2, T3)

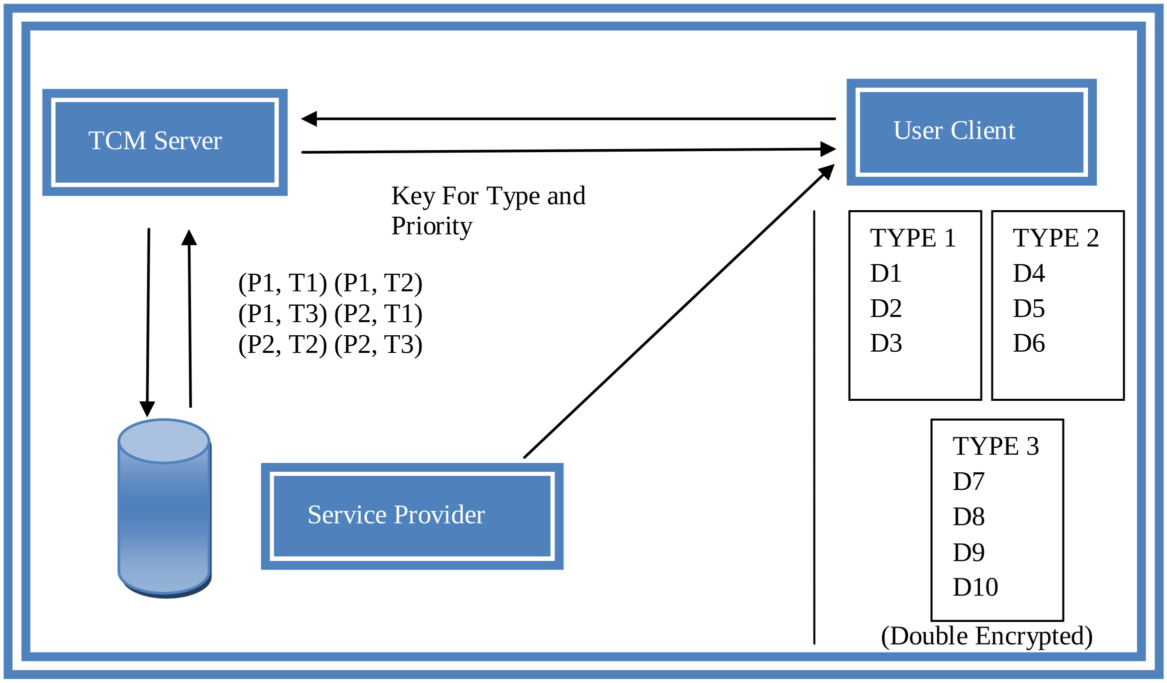

Fig.3.Possible Workflow

5. Specific Shielded Mobile Agent (SSMA)

Mobile Agent, a piece of code that runs parallel in the system [2], is used to handle the vital memory migration from client to the service system [3]. Server controls the service client over a registration process and the unique key generated for specific client is used by SSMA to identify client.

5.1. Initial Setup

Service provider should be a registered user to the TCM server which possesses UID from the TCM. TCM generates asymmetric keys for each host it registered in timeline and updates the host in course of time through Specific Shielded Mobile Agent [6]. Mobile host registered with the TCM gets an asymmetric key to access the vital memory through the sandbox [4].

5.2. Service Client Interaction

Service provider can request three possible priority values such as IN/OUT, IN. OUT with the combination of type it required.

The following steps are carried out when a service client requests the mobile host.

- Sandbox checks the UID of the service client that requests.
- Sandbox sends the UID to the TCM service provider and it authenticates the service.

- It packs the following to the SSMA and send to the TCM server asynchronously.
- Type of the service client such as TYPE123,TYPE356
- Priority of the service client such as IN/OUT, IN or OUT
- Mobile host UID that receives the service client request
- TCM server checks the service and authenticates depending upon the service client UID, priority and type. For example if user requested not to add any vital information, it blocks the service if priority is not normal (refer table 2).
- SSMA updates the TCM server database with the timestamp, service client UID and the mobile host to track the changes.
- If authentication fails because of wrong service client or access denied for the resource, it sends the reissue of access for client to the user and notify the service client.
- Else, TCM server generates a unique one-time asymmetric key valid for certain session.
- SSMA gets the key for Type, Data and Memory Access.
- SSMA clones itself and public key is send to the user and private key is send to the service client with authentication message along with Type, Data and Memory Access keys.
- Sandbox in mobile host receives the key and authentication message. It retrieves the vital memory that in which the information resides using the vital memory access key.
- SSMA decrypts data with Data key and Type key and encrypts the memory with the key received from the TCM server and migrates to the service client.
- Sandbox in service client receives the SMA with the private key. It receives the information and decrypts the information and uses it.

5.3. Pseudocode

```
Request_Type=service.requestType;
Request_Priority=service.requestPriority;
Service_UID=service.uid
TCMServiceProvider.Connect();
Boolean service_Available=false;
Foreach service.uid in services
Begin
    If(Service_UID==service.uid)
    Begin
        service_Available=true;
        break;
    End
End
If(service_Available)
    Begin
        Type_Key= TCMServiceProvider.GetTypeKey(keyType);
        Data_Key= TCMServiceProvider.GetDataKey(dataUID);
        Host_Memory_Key= TCMServiceProvider.GetVitalKey();
        GetAuthentication(Host_Memory_Key);
        Data= Decrypt(Data_Key);
        Data =Decrypt(Type_Key);
        Service_Key= TCMServiceProvider.GetServicePublicKey(Service_UID);
        Encrype(Service_Key,Data)
        Service_Result=Execute_Service();
        Update_TCM_Server(Service_Result);
    End
```

6. Conclusion

Vital memory plays a vital role in the model. The normalized assignment of the data to respective type improves the efficiency of the model. SSMA perform task in TCM Server and service client.TCM server performs intrusion alert mechanism which can block any service client when an intrusion is detected with wrong access of the mobile host. Sandbox usually works in the offline mode when interacting with the vital memory and provides core to the overall process. Thus certain service provider can access only certain type of the data from vital memory that stretches the intrusion prevention margin.

Future work refers to the use of SSMA in the TCM server if user uses cloud storage. Thus, TCM server becomes the cloud storage enabling the data encryption in the server.

References

[1] V.Arun and Dr. K.L Shunmuganathan, 2013, Secure Sandbox for Mobile Computing Host with Shielded Mobile Agent, Indian Journal of Applied Research : Information Technology, PP 47-48, Volume 3, Issue 9.

[2]V.Arun, Dr.K.L.Shunmuganathan, The Journal of Emerging Technologies in Image processing and Networking December 2011, Volume 6, Issue 2, pp 23-27

[3] David B. Johnson Wireless Networks 1995, Volume 1, Issue 3, pp 311-321 Scalable support for transparent mobile host internetworking.

[4] Peng De-wei, He Yan-xiang, Wuhan University Journal of Natural Sciences Study of interoperability in mobile agent environment September 2004, Volume 9, Issue 5, pp 623-628

[5] Yingwei Jin, Wenyu Qu, Yong Zhang, Yong Wang, The Journal of Supercomputing February 2013, Volume 63, Issue 2, pp 431-442, A mobile agent-based routing model for grid computing.

[6] Machado, R.B, A Hybrid Artificial Immune and Mobile Agent Intrusion Detection Based Model for Computer Network Operations, Parallel and Distributed Processing Symposium, 2005. Proceedings. 19th IEEE International, April 2005.

[7] William R. Cockayne and Michael Zyda,"Mobile Agents", Prentice Hall PTR,1988.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[8] T. Sander and C. Tschudin, “Protecting Mobile Agents Against Malicious Hosts”, G. Vigna (Ed.): Mobile Agents and Security, Springer-Verlag, 1998, pp. 44-60.

[9] B. Brewington, R. Gray, K. Moizumi, D. Kotz, G. Cybenko, D. Rus: “Mobile agents in distributed information retrieval”, in “Intelligent Information Agents” (1999).