Secure Sandbox for Mobile Computing Host with Shielded Mobile Agent

KEYWORDS: mobile computing, intrusion mechanism, SMA intrusion model, shielded mobile agent

V.Arun
Ph.D Research Scholar, Sathyabama University, Chennai, India

Dr. K.L. Shunmuganathan
Department of CSE, RMK Engineering College, Chennai, India

ABSTRACT *Portability is the major aspect in mobile computing which involves in mobile communication, hardware and software. Software used in mobile host such as Smartphone, laptop, PDA etc.., may lead to malicious intrusion to carry private data from the host. Access of private data from the host memory without user permission creates a dangerous outbreak result in intrusion. Some application requires private data with authorized access but they are likely to attack in network. We use Mobile agent, a piece of code that run parallel in any host, secures the data that migrates among the host. A secure sandbox model is described in this paper that enables a secure transaction for the access of private data. We used Tracer and Checker Model [1] to provide intrusion detection in the system.*

1. Introduction:

1.1. Tracer and Checker Model:

TCM, a model to assist the network against malicious intrusion, is used in this paper to support mobile host [1]. Mobile host are 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.

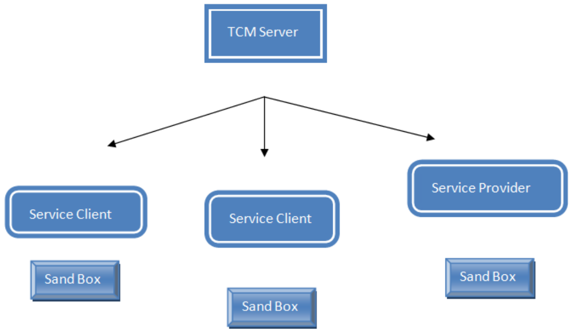

Figure.1. Overall Architecture

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 [1] 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.

2. Vital Information 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
- 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.

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 information 2 holds 32bits.

Information	Memory Address	Unique Memory ID	Key generated from TCM server
Information1	0x9FFF0-0x9FFF8	MID6985455	Key1 (128 bits)
Information2	0x9FFF9-0xA0000	MID6985488	Key2 (128 bits)
Information1	0xA0001-0xA0008	MID6985455	Key1 (128 bits)
Information2	0xA0009-0xA0010	MID6985488	Key2 (128 bits)
Information2	0xA0011-0xA0018	MID6985488	Key2 (128 bits)
Information2	0xA0019-0xA0021	MID6985488	Key2 (128 bits)

Table.1.Memory segment in vital memory

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.

3. Architecture:

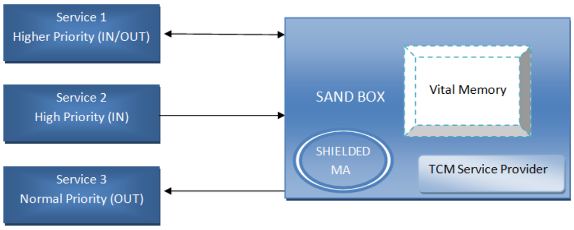

Figure.2. Mobile host architecture

3.1 Shielded Mobile Agent (SMA):

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].

3. 1.1. Pseudocode:

```
/*service = service provider*/
Request_Priority=service.requestPriority
Service_UID=service.uid
Connect to TCM Service provider
Begin
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
Get Host_Memory_Key;
Service_Result=Execute_Service();
End
Update_TCM_Server(Service_Result);
End
```

3.2. Priority:

Service	Priority	Description
IN/OUT	Higher Priority	Service attempt for input and output
IN	High Priority	Service attempt for write operation
OUT	Normal Priority	Service attempt for read only operation

Table.2. Priority pattern

3.3. 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 Shielded Mobile Agent. Mobile host registered with the TCM gets an asymmetric key to access the vital memory by the sandbox [4].

4. Service Client Interaction:

When a service client requests a mobile host, it requests with any three priority. IN/OUT and OUT priority requests the user permission in order to retrieve data from vital memory.

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

1. Sandbox checks the UID of the service client that requests.
2. Sandbox sends the UID to the TCM service provider and it authenticates the service.
3. It packs the following to the SMA and send to the TCM server asynchronously.

- Priority of the service client such as IN/OUT, IN or OUT
- Mobile host UID that receives the service client request
- Vital memory keys

4. TCM server checks the service and authenticates depending upon the service client UID and the priority. For example if user requested not to add any vital information, it blocks the service if priority is not normal (refer table 1).
5. SMA updates the TCM server database with the timestamp, service client UID and the mobile host to track the changes.
6. 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.
7. TCM server generates a unique one-time asymmetric key valid for certain session.
8. SMA gets the key for the vital memory access.
9. SMA clones itself and public key is send to the user and private key is send to the service client with authentication message along with vital memory access key.
10. 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.
11. SMA encrypts the memory with the key received from the TCM server and migrates to the service client.
12. Sandbox in service client receives the SMA with the private key. It receives the information and decrypts the information and uses it.

5. Conclusion:

SMA plays a vital role in performing various tasks in the host. TCM server performs intrusion alert mechanism which can block any service client when a 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.

Future work deals with the inclusion about a mechanism for fixing service client to access certain vital information such as bank client can access bank details from the mobile host persistently.

REFERENCE

1.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 | | 2. David B. Johnson Wireless Networks 1995, Volume 1, Issue 3, pp 311-321 Scalable support for transparent mobile host internetworking. | 3. 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 | 4. 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 |