SIM Applet Security

Secure communication between application & server

Sonal Rohilla

Reaserch & Development, Syscom Corporation ltd., Morpho, Safran

Abstract — This paper delineate the most imperative feature of SIM industry; rather all communication industries i.e. SECURE COMMUNICATION. The research done herein is primarilary focused on secure commuicatons between a SIM application often called SIM Applet and the supporting/controlling server. The work done here will assist a SIM applet architect, developer, business solution designer to know how to ensure secure communication between applet & server.

Index Terms — SIM (Subscriber Identity Module), OS(Operating System), OTA (Over the Air), Security Domain (SD), ISD (Issure Security domain), SSD (Suplematary security domain), APSD (Application security domain), MNO (Mobile Network Operator), RAM (Random access memory)

1 INTRODUCTION

Applications; a word which is becoming much common in todays technological world and when this word is connected with mobile or SIM industry it becomes even more common. There were days when every user service was embedded as a feature in operating system. With more and more people joining the mobile phone ecosystem, these features kept on growing exponentially & became more and more diverse. As a result the operating system's size grew exponentially. Eventually, the memory size of operating sytem became a decisive concern. Talking about SIM card, keeping the size of silicon (microcontroller chip over which lots of things exists: chip OS + SIM OS + File system of OS + user space) constant; the more the size of OS, the less is the space available for user. So now the world was ready for facing the new challenge to minimize the size of operaing system as low as possible. To meet these requirements the services were pulled from OS and build as stand alone java applets. Now the final SIM card could be easily made customizable as per user's diverse needs. Some one needs more user space and fewer applications, while the other group of users desires to have bunch of applications and considerable user space. The SIM world has a solution to all such needs.

On the contrary; Mobile apps are also growing with equal pace. They offer a cut throat competition to SIM java applets. SIM applets over mobile apps offer an inherited advantage of being more secure and when the word secure comes it becomes an indespensible aspect for; be it a SIM applet or mobile app.

All in all, there are three primary requirements for a SIM applet:

- Applet size
- Security
- Performance

All the requirements are contrary to each other i.e. the more security you code into your application the more heavy it becomes. Performance depends on usage of RAM area by OS/application. Hence somehow a tradeoff needs to be made between all primary artifacts to make the SIM applet acceptable to the end user.

Our current telecommuinication market is stuffed with numerous SIM applets where interaction with server is required. This server is often established and owned by service provider, in many cases network provider also.

The scope of this paper is confined to security attributes; to be more specific secure communication between administrative Server and SIM applet.

2 RESEARCH ELABORATION

Before going into the details of SIM applet security it is mandatory to know about Security Domains (SD).

A SIM operating system existing on a java card often has one or more security domain (specification provided by Global platform GP). Security domain is the on card representative of an offcard entity. GP specifies three types of security domains:

- ISD: Issuer Security domain
- SSD: Supplementary security domain
- CASD: Controlling Authority security domain

Key points for security domains:

- ✓ Security Domains support security services such as key handling, encryption, decryption, digital signature generation and verification for their providers.
- ✓ ISD is a mandatory security domain for card issuer.
- ✓ SSD is an optional security domain for application provider or card issuer
- ✓ CASD is a special type of SSD who mainly enforces security policy for all applications loaded on the card. There can be multiple CASD in one card.
- ✓ Each security domain has their own isolated keys which can be used for securely wrapping the data.

In context to this paper the main area of concern will be first and last point.

Now, SIM applets involving interaction with a server can secure the communication with the server in several ways:

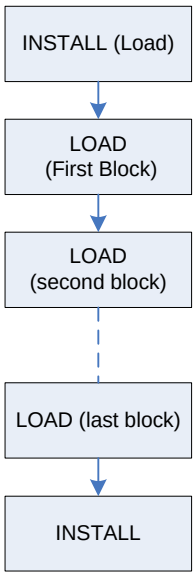
1. **APPLET DEPLOYED ON SIM SECURITY DOMAIN**
2. **APPLET USING ITS OWN APPLICATIVE SECURITY**
3. **APPLET USING SD SECURITY + APPLICATIVE SECURITY**

An applet can be directly made to use the security domain keys owned by MNO.

How to deploy applet on security domain?

An applet is simply a java code written using standard javacard libraries (Reference to java card library). On compilation this javacode gives an output file as .cap. This cap file is loaded & installed on card using three commands specified by Global platform card specification [1]:

a. Load (Install)
b. Load (Load)
c. Install



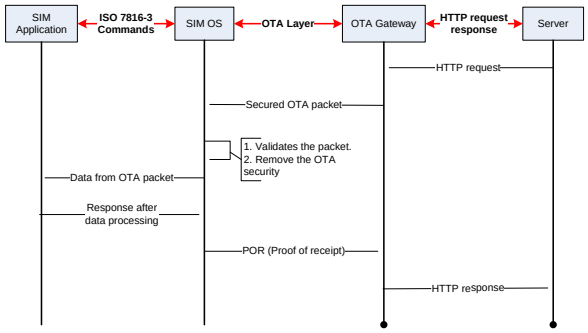
In these command a parameter is given by which an applet can specify its associated security domain. For command details refer [1]. With this parameter set and defined, an applet gets associated with the security domain and thus can use its security features.

The basic working is:

1. Server communicates in the form of HTTP requests response pair while SIM OS communicates as per ISO commands.
2. Since the mode of communication is different so a gateway is required which accept one form of communication from one entity and convert it into a form acceptable for the other entity.
3. Server sends a HTTP request to the gateway.
4. Gateway converts the request into an OTA requests often called OTA packet. Since it is coming from server so it is called incoming packet. OTA is over the air, standards defined in [2]. Just to brief; via OTA, a SIM card can be accessed remotely by an authorized entity. After converting into OTA packet; the gateway wraps the OTA security over the packet and forward it to SIM OS.

5. SIM OS have an inbuilt OTA interpreter which validates the packet i.e. decrypts the data, checks the security of packet, verifies the checksum for authenticity etc. Once the packet is fully verified the OS accepts the packet. OS removes the OTA security from the packet and forward the plain data to intended application. *Please note that there can be multiple applications residing on same SIM OS. So the question is how do the OS find out to which application the packet is intended to? The answer is TAR (Toolkit application reference). Each application has its defined address known as TAR. For details of TAR refer [2]*
6. Application executes its code, prepares response data and send to SIM OS.
7. SIM OS adds the desired security in response and send to server in the form of transport carrier called proof of receipt (POR).
8. Any OTA packet intended to SIM can define whether it requires POR or not, POR only on error or POR on error/success both. Also it can define whether POR should be plain or secured. It can even define which security to be applied to POR. SIM OS takes this information from incoming packet and adds the desired security in POR i.e. response packet.
9. Secured POR is send to server via gateway.
10. Gateway validates the security of POR and after interpretation forward the desired information to server.
11. With this; the communication between application and server becomes secured **without explicitly writing any code for security inside applet thereby reducing the applet size and complexity**.

Below mentioned is the pictorial representation for the above explanation:



There are cases where the SD's security cannot be used by application and/or an additional security specially needs to be built inside the applet. The cases include:

1. Service provider needs applet developer to explicitly build an additional security inside applet i.e. service provider needs double security; SD security + applet additional security.

2. The applet functionality is such that it requires some input from end user. For eg: case where an applet takes few details like name, gender, area of interest etc. from user; passes the entered info to server. Depending on this the server sends the next request accordingly.

The formal is simply a requirement which needs to be fulfilled in order to be complaint to requester needs. But the latter is more a **Limitation**.

Limitation in context to TS 43.019 [3] a SIM API standard to which a java card is complaint for interoperable reasons.

As specified in standard,

"The EnvelopeResponseHandler content must be posted before the first invocation of a ProactiveHandler.send method or before the termination of the processToolkit, so that the GSM applet can offer these data to the ME (eg 9Fxx/9Exx/91xx). After the first invocation of the Proactiv Handler.send method theEnvelopeResponseHandler is no more available"

To explain the above statement:

- EnvelopeResponseHandler – Via this handler the SIM applet provide the response for the received OTA envelope.
- Proactiv Handler - Via this handler the SIM applet issues a proactive SIM commands; defined in [4].

A brief for proactive commands: This is a way by which a SIM can interact with ME and via ME to the end user, to network

or any other involved entity.

If an application code is such that it does not involve any interaction with end user/network i.e. does not involve the issuing of proactive SIM commands then the response can simply be given in POR thereby SD security can be used **BUT** if to send response to server, the SIM has to interact with user or issue proactive command then SD security cannot be used. In such a case the application should have its own security called applicative security.

Let's try to make the point clearer by taking an example applet Suppose an applet is designed to accept two commands coming from server:

1. Cmd1: Server will send some data to be stored in applet internal buffers for future use.
2. Cmd2: Server want to know the gender of the applet user + current location of the applet user.

For both cmd1 and cmd2 server needs the response back in case of success/error. Both incoming (cmd1 envelopes) and outgoing (response) should be secured.

Now coming to working; when cmd1 is received by applet; the applet executes its code; stores the data in its buffers and send secured response via POR using envelopeResponseHandler.

When cmd2 is received by applet, applet has to take input from user and network both. For this applet needs to issue proactive commands ('Get input' for taking input from user and 'Provide location information' for fetching current location form network). The proactive commands will be issued using ProactivHandler. As per [3] once the proactiveHandler is used the envelopeResponseHandler will be lost. So a SIM applet can use either of one handler at a time. The moment the proactivHandler is picked for issuing the proactive command the envlopeResponseHandler is lost and the applet has no access to SD security. Hence the response cannot be wrapped with SD security. Here the applet has to apply applicative security for sending secure response to server.

Working for communication using application security:

1. Server sends a secured HTTP request to the gateway.
2. Gateway converts the request into an OTA requests and forward it to SIM OS.
3. SIM OS removes OTA header and forward the data to intended application.
4. Application validates the security on data. Decrypts the data and executes applet code.
5. Application prepares response data, adds the applicative security and send to SIM OS.
6. SIM OS forward the response POR to gateway.
7. Gateway further forwards the data from POR to server.
8. Server decrypts the data and interprets the response from applet.
9. With this; the communication between application and server becomes secured **using applicative security**.

There are cases where the service provider requires both SD security + applet additional security. Working in such case is:

1. Server sends a secured HTTP request to the gateway.
2. Gateway converts the request into an OTA requests and adds the OTA security then forward it to SIM OS.
3. SIM OS validates the packet, removes the OTA security from the packet and forward the encrypted data to intended application.
4. Application validates the security on data. Decrypts the data and executes applet code.
5. Application prepares response data, adds the applicative security and send to SIM OS.
6. SIM OS adds the OTA security over already secured response data and send to server in the form of POR.
7. Secured POR is send to server via gateway.
8. Gateway validates the security of POR, removes the SD security and forwards the applicative secured data to server.
9. With this; the communication between application and server becomes SD + applicative security secured.

Clearly in such communication using additional applicative

security; the server and applet should be agreed with security + key to be used. The system can work in pre-shared keys i.e. server and applet already holds the keys before initiating the commuicaion session. For pre-shared keys the keys should be included in applet during SIM card manufacturing. Such a system becomes quite rigid i.e. each time an applet is deployed with another server i.e. another MNO the keys needs to be embedded during SIM manufacturing. Thus includes lot of operational cost. To avoid this; the data can be stored in few files defined by applet developer. Data in these files can be updated remotely again using OTA concept. Keeping data in files is somehow considered less secure so there is one more option. The keys can be exchanged between server and applet in run time remotely via OTA.

Thus there are many ways of key handling and sharing between server and applet. Depending on business level agreement between the involved entities an appropriate way is used.

3 ADVANTAGES OF DIFFERENT OPTIONS

Applet deployed on SIM SD

Advantages:

1. Reply on OS inbuild security i.e. standard secure messaging
2. Simple card architecture
3. Minimising applet size as no applicative security

Disadvantages:

1. Agrrement between gateway and server necessarily required.
2. Applet cannot send a secure message to server, response can be secured via POR

Applet using Applicative security

Advantages:

1. No dependency on MNO OTA platform, a simple SMSC will work
2. Applet can send secure message to server
3. Simple card architecture

Disadvantages:

1. Increased applet size due to additional applicative security
2. Incaresed size of message payload
3. Server needs to be designed specially to handle applicative security

4 End Note

Every applet deployment method have its own prones and cones. It is on applet developer, service provider that how they use the different option to earn their maximise business profit together gratifying the users needs and desires.

ACKNOWLEDGEMENT

I would like to acknowledge my co-workers & organization for supporting and encouraging me throughout the course work.

REFERENCES

[1] GlobalPlatform Card Specification Version 2.2.1

[2] ETSI TS 102 223 V5.0.0: Card Application Toolkit (CAT)(Release 5)

[3] 3GPP TS 43.019 version 5.6.0 Release 5: Subscriber Identity Module Application Programming Interface (SIM API) for Java Card

[4] 3GPP TS 11.14 - Specification of the SIM Application Toolkit (SAT) for the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface

AUTHOR

Author Name: Sonal Rohilla

Qualification /Experience: B.Tech .Currently working with Syscom Corporation Ltd, a leading telecom company dealing in SIM and SMART cards. Syscom is a Morpho, Safran organization. Experience is ~ 9 Years.

Email Address: sonal.rohilla@gmail.com