Department of Computer Science and Engineering

CSE 6813 : Network Security

Report on

Security Aspects of Smart Cards in Machine-to-Machine (M2M) Mobile Networks

Report Writer:
Md. Mostafizur Rahman
Roll: 0416052032

Submitted to:
Dr. Mahfuzur Rahman

March 5, 2017

Contents

Abstract

The advantages of utilizing smart card technology, in the machine to machine mobile networks for common usage i.e. health sector, transport industry etc have long been realized. With great potential and advantages also come some security concerns. Since the invention, smart card has come a long way in facilitating easy and fast transaction and authentication processes. Still, security threat remains as a major concern in deploying smart card based system specially in mobile M2M communication. Proper procedure and process must be followed to ensure security in diverse environments.

1 Introduction

Among the main driving factors towards the success of smart card technology are the capabilities of performing security sensitive operations along with maintaining the integrity of the internally stored information in machine to machine communication. These characteristics enable the wide deployment of smart card based services in a variety of applications and sectors. Smart cards are increasingly used as authentication and encryption vehicles in mobile phones, as bankcards, and as the carrying medium for various payment and access control applications.

Due to the sensitive and important role of the smart card device within the overall smart card based system it is evident that the card as well as the infrastructure components be designed to withstand various attacks and attempts of fraud during their lifecycle. This has implications on both physical and logical security levels, which are of vital importance and at the same time act as the driving factor for the adoption of the technology. In mobile networks where the terminals are exposed to vulnerabilities security is a major concern. Without proper security features the whole system will face difficulties in running operations.

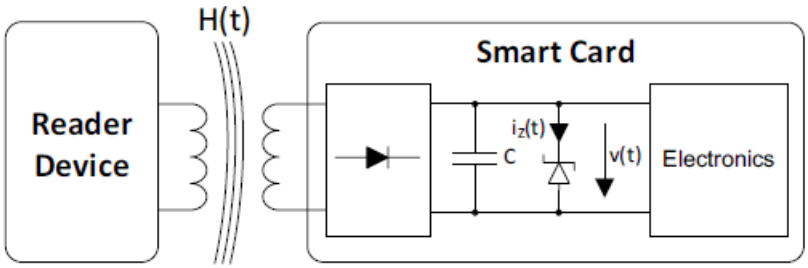

Figure 1: Basic internal structure of smart card

2 Common Terminologies

2.1 Smart Card

Smart card is small embedded computer. More specifically, its a built-in microprocessor, used typically for electronic processes such as financial transactions , personal identification etc. Some of the applications of smart card are:

- Computer Security
- Credit Cards
- Financial transaction
- Health Care(medical)
- Identification

Figure 1 is the smart card that was used for health insurance in France in early 90s.

2.2 Machine to Machine(M2M) Communication

Machine to machine refers to direct communication between devices using any communications channel, including wired and wireless. Machine to machine communication can include industrial instrumentation, enabling a sensor or meter to communicate the data it records (such as temperature, inventory level, etc.) to application software that can use it (for example, adjusting an industrial process based on temperature or placing orders to

replenish inventory). Such communication was originally accomplished by having a remote network of machines relay information back to a central hub for analysis, which would then be rerouted into a system like a personal computer.

2.3 Security of Smart Cards

With great advantages smart cards are forced to face some inevitable security issues. Smart card security is associated with both the physical and logical design of the cards.

3 Challenges of M2M

M2M communication system has some major challenges to deal with. Some of the critical challenges are:

- Terminals may be in hard-to-reach locations (e.g. traffic cameras)
- Terminals may become geographically dispersed over time (e.g. cargo containers)
- Owners of large populations of terminals may want to change the network operator without visiting the terminals (e.g. to change the UICC [1])).
- Terminals need to be protected against unauthorised removal of UICC
- Terminals may require over-network provisioning after sale or installation.

M2M requirements may make the conventional UICC a less advantageous solution for secure authentication. It is necessary to look at the options for a non-personalised security module to which a network operator's Network Access Application (NAA) can be downloaded. This may be accomplished using an embedded Trusted Environment (TRE) in a terminal. The TRE acts as a hardware root of trust for the storage and execution of secure applications and may also have protected software functions. The TRE may host downloaded software NAAs that emulate the behavior of the USIM or ISIM applications.

[1] Universal integrated circuit card. For example SIM card

4 Challenges of Mobile Networks

The challenges of M2M intensifies when considered in mobile networks. Mobile networks changes over time and places. The topology changes are too frequent. Data delivery,throughput, bandwidth etc are major concerns in this type of networks.

5 Smart Card Security in Mobile Networks

Current implementation of smart card manufacture has some positive security aspects that plays a great role in using smart card in M2M mobile networks.

5.1 Physical Tamper-Resistance

An ISO-7816 smart card has, in practice, a single-chip architecture with little possibility of monitoring communications between different chips on the card. Smart card ICs are designed and implemented to prevent probing and reverse-engineering. They are fabricated on a dedicated production line in a secure facility. Measures include scrambling of busses and of memory addresses, bonded passivation layers, permanently disabled test points, self-generated programming voltage.

5.2 Proprietary, Secure O/S

The Smart card's standardised API, e.g. [4], consists of a restricted command set that has no hidden commands or access methods. It is trusted because of its own built-in security mechanisms and because of those of the underlying hardware platform. It is non-updateable.
For applications such as USIM, the Ki and OTA keys are stored and accessed by the O/S in proprietary ways. The O/S cannot be made to reveal the values or memory locations of those data. Conventional GSM SIM cards did not allow adding applications to a live card. The advent of the Javacard now allows applications on a multi-application UICC platform to be updated, deleted or added to an issued card, either remotely or locally. The potential of Javacard for Network Operators is currently restricted by:

- Implementation by Network Operators of only SMS as the bearer (for OTA messages to the UICC), which has a very limited bandwidth
- OTA security standards [11] are not profiled for IP bearers
- Lack of a sufficiently rich terminal/UICC interface on nearly all MEs [2]
- General concerns about the security of multi-application Javacards.

In the world of telecoms, it is generally up to the buyer to perform a due diligence test on the smart card vendor to ensure that the O/S has been properly developed and evaluated.

5.3 Other Measures

Smart cards include proprietary measures to prevent attacks such as slowing down the external clock and measures against power analysis attacks by the use of noise-free computational algorithms and/or injection of artificial noise and/or damping of noise on the power rail. There are also said to be a large number of detailed precautionary measures taken, some of which are described in the public domain.

5.3.1 Design and Development Process

Security is designed into a smart card IC in the secure facilities of a semiconductor manufacturer. The computers that are used for this are isolated from the rest of the world. Undocumented counter-measures in the IC are supported by corresponding design criteria. Once the O/S development is finished, the entire source code may be checked by an independent evaluation.

5.3.2 Supply Chain

There are only a handful of world-class vendors of smart cards, so it is feasible for Network Operators to perform the necessary security audits. There will be an agreed arrangement for transferring the Ki objects between network operators and UICC vendors. Ki values cannot be retained in the vendors' personalisation systems or be discovered by system operatives.

[2] A few terminals have implemented the JSR177 terminal/UICC interface, but it's usually only the SIM toolkit part and not the general APDU API. A few Windows Mobile MEs have allowed an open APDU API to the UICC, using the terminal's RIL (Radio Interface Layer) but it is not clear if those are still in production

5.3.3 Security Evaluations

Card vendors have their O/S independently evaluated and MNOs perform security evaluations of their card vendors' products and facilities. GSMA [15] provides non-public guidance to its members on how to do that. Common Criteria Protection Profiles have been published for smart cards. One of these [16] is aimed at the underlying IC platform but some are aimed at payment cards issued by financial institutions such as Visa and Mastercard. Cost can be an issue for wider adoption of these evaluation regimes. There are no standard specifications or protection profiles for the security evaluation of telecoms smart cards such as UICCs.

5.3.4 Terminal Interface Security

The UICC employs some security measures in the interface with the terminal:

- User Authentication: PINs (called CHV1 and CHV2 in a SIM card), provide some level of protection with user authorisation on the interface. CHV1 can be disabled by the user, in which case there is no PIN-protection for making calls. The use of CHV1 and CHV2 poses a security vulnerability since the passwords get transported across the UICC-ME interface in clear. The UICC does not authenticate itself to the user, although 3G authentication provides mutual authentication of the card and the network. In M2M, a remote user could rely on two possible methods of assuring himself of the authenticity of a UICC, i.e. (a) using a remote access protocol that exploits a pre-shared or private key on the UICC and/or (b) using e.g. Liberty Alliance protocols to trigger the UICC issuer to perform an authentication of the UICC and possibly binding that to the remote access session.

- Commands to the UICC are not secured unless they are inside a 3GPP OTA envelope . That is why ETSI and 3GPP have recently specified secure channels and their key establishment methods across the terminal-UICC interface. ISO 7816 and EN726 define secure messaging between a terminal and a smart card but key distribution was not defined (it being assumed that it would be based on pre-installed keys). ISO7816 also defines a set of security-related commands. Neither the ISO nor CEN techniques are included in UICC specifications such as ETSI and 3GPP secure channel specs and compliment the ISO and

CEN standards by defining methods for key distribution between the terminal and UICC. There does not seem to be any reason to believe that normal terminals can be trusted to store the distributed key. Protocols such as Global Platform, ETSI RAM/RFM and 3GPP OTA provide end-to-end security from server to card for the purpose of loading and managing files and applications on the UICC. They do not require a secure ME/UICC interface[3].

- Protection of data across the interface: All standardised command-sets of a UICC are designed to be sent in the clear across the terminal/UICC interface. Protocols that may be subject to replay attacks must have counter-measures built in, e.g. the sequence numbers used in 3G authentication. In future, the Smart Card Web Server (SCWS), could use HTTPS/TLS to establish a secure tunnel from card to server (or to terminal) via which usernames and passwords could be sent.

- Access control: In general, access control lists (ACLs) are not used in today's UICC O/Ss. Access to file operations relies on the principle that if the entity accessing the file can satisfy the access policy (embodied in the File Control Parameters), then it must be an authorised entity.

6 Meeting M2M Requirements with Smart Cards

Followings are the features of smart card that make it a suitable candidate to use in M2M mobile networks.

[3]Remote Application Management can theoretically be used to download any Javacard application to a UICC and to store it in a security domain. It does not currently apply to the U(I)SIM applications, as there is no standardised mechanism for the UICC to extract and store the Ki and algorithm customisation parameters. For the case of updating existing files either locally or remotely, this is possible only where the access conditions in the File Control Parameters can be satisfied. Remote (OTA) file update is possible on files in any application on the UICC, but only if the files were OTA-enabled at the time the file was created on the UICC

6.1 Advent of the "Big SIM" UICC

Recent innovations in smart card technology could go a long way to enabling the UICC to fulfill the M2M requirements. The new features described below, plus the ability to store downloaded applications and multimedia files, would need the large memory of "Big SIM".

6.2 Large Memory

Recently, Smart cards with flash memory of up to 2Gbytes have become available.

6.3 High-Speed I/O

The conventional I/O speed of the UICC or terminal interface is only a half-duplex 9.6Kbit. In order to be able to move data on and off the Big SIM in a meaningful timeframe is required. Modern smart cards can be equipped with this speed.

6.4 Smart Card Web Server (SCWS)

The advent of Mega SIM with USB I/O enables the UICC to support an IP stack and web server. There are a number of advantages to this, e.g. use of (X)HTML to communicate with the UICC. UICCs could even have their own IP addresses, which could introduce a whole set of security issues. ETSI SCP has standardised SCWS and IP on a UICC. Use of SMS for application download is limited in practice to about a 1kByte payload, i.e. 7 concatenated SMSs. Even then, this requires a dedicated SMS-C to achieve an effective success-rate. With ordinary SMS-Cs whose resources are shared with mainstream SMS, the practical limit may be as little as 2 concatenated SMSs, i.e. about 300 bytes. The size of a download using an IP bearer does not suffer from such limitations.

6.5 Internal Security Domains

Global Platform has specifications [10] that define security domains on a Javacard smart card. ETSI SCP are now expanding upon these in their specifications for "Confidential Applications." This allows the card issuer to

set up domains for the use of third parties to load applets onto the card. The issuer cannot examine those applets. The UICC provides a sandbox environment in which the domains are isolated from each other – a feature that has been somewhat limited in Javacard implementations up to now.

7 Some Example of usages of Smart card in M2M mobile networks

8 Enhancements Required for M2M Mass Market

A Smart card to be used in mass-market M2M applications would have to support the requirements of long life-time with long maintenance intervals, non-removability, remote download of operator's authentication application and remote change of operator. Some very significant enhancements need to be considered as follows:

8.1 Security Domains

Support is required for security domains for the card issuer and for third parties, e.g. as per the SCP specifications "Confidential Applications" concept. But in the M2M scenario, network operators would be classed as third parties. In order for the card issuer to allow the M2M equipment owner to change to a new network operator, the card issuer (who is therefore not a network operator) assigns a domain to a new network operator and closes the domain of the old network operator.

8.2 Removable UICC vs. Downloadable UICC

Unauthorised removal of a traditional "removable" UICC must be made very difficult, while its replacement must be easy. A better alternative to this is to fix the UICC in the terminal and for it to support the ability to download MIDs. Such a UICC must be able to extract Ki objects and similarly sensitive data from messages from a remote server and lock them away in secure memory so that they cannot be revealed to entities outside the UICC. Net-

work operators will demand that there be no reduction of security in UICCs that support these features.

8.3 Secure Download Protocols

Support is required for secure download protocols other than standardised OTA, i.e. M2M requires protocols which do not require pre-shared keys and which can be used over IP bearers. (In this respect, support for SCWS and IP stack could be an advantage).

8.3.1 Options for Secure Downloadable Identity

Option for client-side authentication technologies for M2M could include:

- UICC with download capability
- An embedded TRE in the terminal, to provide a secure execution and storage environment. Authentication applications (Managed Identities or "MIDs") would be downloaded to the TRE over public IP networks.
- Smart token such as the new multimedia card with on-card UICC (or SMC)

A framework of standardised specifications is needed for the above solutions. The discussion within standardization about the (dis-)advantages of the various candidate solutions is lively and far from concluded.

Table 1 shows the comparison between different options. No solution comes out as perfect, but the TRE shows promise if it can be standardised. The UICC shows promise if its current limitations (including that of lack of implementation of already-standardised features in cards and terminals) can be overcome

8.4 Secure Interface to Terminal

Support for a secure terminal-UICC interface may be a requirement, as discussed above.

Required Feature	**UICC**	**TRE**	**SMC**
Currently standardised	good	medium (it could be based partly on TCG specs)	medium
Currently available	good	medium (some limited versions available)	poor
Protection against unauthorised removal	poor (good, if M2M form factor UICC is soldered in)	good	poor
Provides secure API	good	good	not known
Does not require connector and interface chips	poor	good	poor
MIDs can be downloaded	poor. Can't download NAAs	good	poor. Can't download NAAs
Key management suits M2M model	poor (pre-shared keys for authentication and download)	good (can use PKI)	poor
Predictable costs	poor (for full-function, big memory, downloadable UICC)	Good (part of chipset)	poor
Secure channel to terminal	poor (standardised but usually not implemented)	good	not known
Remote change of operator	poor	good	poor
Open API for download	poor	good	poor

Table 1: Comparison of Solutions for Secure Downloadable Identity

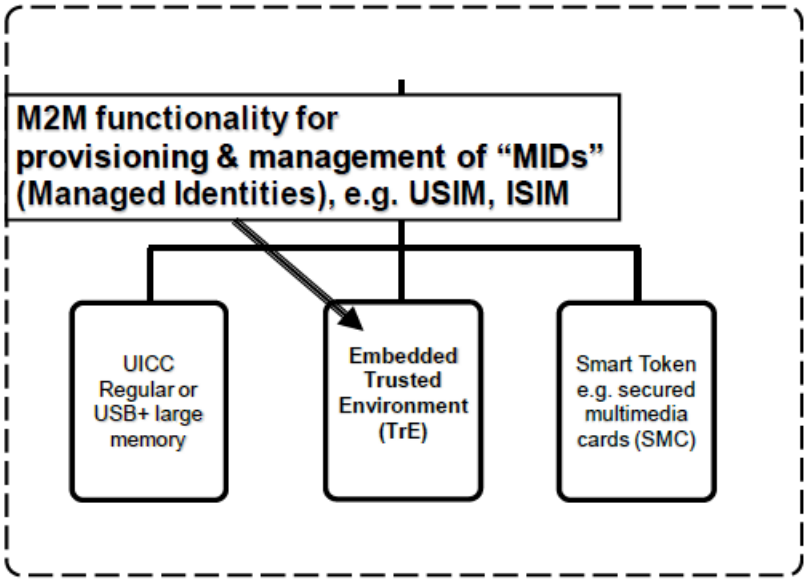

Figure 2: Options for Secure Environments for Downloaded Identity Credentials

References

[1] E. Bonabeau, M. Dorigo, and G. Theraulaz. Swarm intelligence: from natural to artificial intelligence. Oxford University Press, 1999. ISBN 0-19-513158-4.