

The difficulty of standardising Smart Card Security Evaluation*

Audun Josang
Norwegian Institute of Technology
Trondheim

September 1994

Abstract

There is a need for assessing the security of smart cards by an independent third party, specially if multi-application smart cards become reality. Intuitively, the methods to obtain this could be derived from the computer industry where security evaluation already is commonplace, but because of the special properties of smart cards, this seems very difficult. The article discusses the problems related to this topic, and makes suggestions on how security evaluation of smart cards can be achieved.

Introduction

Key words:

security evaluation	smart cards
security validation	assurance
ITSEC	security through obscurity
standards	illegal cloning

Subject classification: Security Verification and Evaluation.

Smart cards form an important new class of computer systems which are highly suitable for security applications. In order to show the need to have better security assurance in smart card systems, the first section illustrates that there is a lack of justification for the

*Appears in Computer Standards and Interfaces Journal, 17, September 1995, pp.333-341.

inherent security of smart cards, then gives as example a smart card system which recently was successfully attacked, and defines the kind of security assurance which is needed. Section 2 makes predictions about the evolution of smart cards and discusses three different methods of approach for obtaining security assurance. One of the methods, which then is further discussed in section 3, and which is the main topic of this article, is security evaluation of smart cards. Section 3.1 discusses validation v. evaluation, section 3.2 comes down to details about smart card properties which clearly illustrates the differences between smart cards and ordinary computer systems, section 3.3 gives suggestions on how the evaluation should be conducted, and section 3.4 finally evokes confidentiality as a fundamental problem for the evaluation. This article is based on: [Jøs93].

1 The need for better Security Assurance in Smart Card Systems

1.1 The lack of justification for smart card security

Smart cards are exposed to particular risks because they can not be physically isolated from the malicious user. One attack which can be imagined is the removal of the protecting layers of the chip to allow inspection with microscope and the interception of electrical signals while the chip is operating. For such attacks to succeed, it is necessary to know or understand the chip architecture. A popular technique to prevent optical inspection consists of trying to fool or confuse the attacker by using a chip mask layout which deviates from the standard. Publication of too many details about the chip would then undermine the security. This is clearly expressed in [Kru91]:

“Normal” ICs are designed to facilitate testing during the manufacturing phase with probes and test tools. This approach is reversed for chip card ICs, i.e. they must be very difficult to test, and the entire layout of the mask must be as obscure as possible. Just how much this complicates IC analysis is obvious in the light of the difficulties semiconductor specialists have in analysing normal ICs. Moreover, for security reasons, all design data are kept secret.

The conclusion which can be drawn from this is that confidentiality of the details and principles of design is a fundamental factor in the security of smart cards. This creates a dilemma for the smart card manufacturers when they make claims about the security of their products: In order to justify the claims one should think it was necessary to explain the techniques and publish results of security assessments, but this would at the same time undermine the security. As a consequence, one often hears from the manufacturers: *Our products are secure, and any justification should be unnecessary.*

In order to convince the public that smart cards are secure, manufacturers talk about special hardware techniques such as fuses, transport codes, application codes, security detectors and operation modes, and describe secure procedures for manufacturing and delivery of the products. All these measures are without any doubt contributing to the security, but we can never be sure that they are sufficient or even correctly implemented. In fact there are already examples of irregular cloning of smart cards used for encrypted TV signals (see below). How do we know that other types of smart cards can not be cloned ?

1.2 A case study: Pay-TV and the Eurocrypt clone

Said briefly, Pay-TV systems ensure that only paid up subscribers can view their Pay-TV channels by encrypting the TV signals and selling smart cards containing the key and perhaps the algorithm for decryption. The three most widespread encryption techniques in Europe are Eurocrypt, Videocrypt and Nagravision. The combination of Eurocrypt and the signal format D2-Mac provides program providers with powerful features and is considered to be state of the art: all pay modes are available, security management has been especially developed, and system features comply with the criteria and desires of program providers. Nevertheless the security seems to be insufficient because exactly this combination has been the target of recent successful attacks by pirate companies.

The high profits to be made from Pay-TV seem to be the reason why certain organisations have invested in developing cloned decryption smart cards which are sold at a cheaper price than the official. It has been known for some time that this is a problem, and advertisements in magazines like *What Satellite TV* give irrefutable

evidence that it really has happened.

A clone is a smart card that is functionally equivalent to the original. It is not necessarily a copy, and does not have to be based on the original chip. As long as the card behaves like the original and uses the same interface, the decoder is not able to distinguish the original from the clone. When all cards are identical, the cloning of one card is enough to undermine the whole system. It is here interesting to notice that prEN 726-2 [CEN94] contains a security requirement which, if followed, would have prevented this:

The manufacturing of the IC and the IC card, shall be performed in such a way, that compromising one IC card implementation shall not compromise any other IC card implementation.

1.3 Definition of Security Assurance

The above example merely illustrates that smart card based security is vulnerable to attacks and that there is a need for establishing security assurance. The assurance shall reflect how well security has been taken care of and the correctness of hardware and software. In other words it allows the service providers and service users to be reasonably sure that they will not suffer as a result of security breaches.

In principle, the assurance does not tell anything about the absolute level of protection, e.g. the strength of enciphering algorithm or the key length used. The same level of protection can be adequate for one application but insufficient for another if the risk of the second is much higher. Similarly, a high protection level can be useless if the implementation contains severe bugs. The assurance must therefore certify that the protection is appropriate for the risk of the application and that the implementation is correct.

2 How to obtain Security Assurance

2.1 Directions of smart card evolution

Multi-application smart cards do not exist yet, but have become a common theme in emerging standards like prEN726-1,2,3 [CEN94]

and CD-IS7816-4 [ISO93] in addition to articles and seminar papers. It can be discussed in which degree multi-application cards really are needed, and one should realise the difficulties involved with it. Approximately 500 million mono-application smart card chips will be manufactured in 1994 and the growth rate is about 45% per year. Mono-application cards definitely have a future and will constitute the main volume for many years, and the role of future multi-application cards should not be exaggerated in spite of the ongoing research and standardisation activities. Two directions of evolution can be expected for the multi-application cards. Firstly, because of the considerable difficulties related to a totally open multi-application architecture, we will see systems with limited openness which combine more or less related applications or applications from the same provider. Secondly, an evolution towards total openness where the hardware constitutes a standardised platform which can support independent applications.

2.2 The methods to obtain security assurance

This section will provide some suggestions on how security assurance can be achieved. Three methods can be envisaged, and they can be applied either separately or in combination. Firstly, there can be a standardised set of test procedures which can be applied in-house by the manufacturer or developer with no or little involvement from external parties. Secondly, companies can be certified to follow certain standards for development and manufacturing of secure smart card products, very much in line with the ISO 9000 quality certification. Finally, a scheme can be set up to assess and subsequently validate smart card products by external independent parties.

2.2.1 Method 1: Standardised test procedures

There are clear signs showing that initiatives are being taken to establish standardised test procedures for smart cards. ETSI STC TE9 is in the process of writing a document for test methods and necessary conformance testing for the series of standards on IC cards for telecommunication purposes. The work is still at a very early stage, and only when the documents pass the stage of working documents they will be circulated within CEN TC224 for comments

before they will be sent out for public inquiry as prENs. It was impossible to obtain any information from ETSI at this stage, and even a request to see the suggested scope of the standard was refused.

In Germany, smart cards are presently tested by the Fernmeldezeugamt (FZA) in Malsh which is a semi-government institution. They were similarly reluctant to give away any information about their activities.

In France as well, there already exists, or there are plans to set up test facilities for smart cards, although information about it is difficult to obtain.

This short survey shows that the activities are surrounded by confidentiality. This will sooner or later create a dilemma for ETSI because standards per definition are public. It will therefore not be surprising if the ETSI activities are halted or moved to other institutions which are not obliged to publish their work. Presently there is no other international body which could lead such activities. Unless the status of ETSI or some other standardisation organisation can be changed to permit non-public standards, the activities will have to stay at national levels.

2.2.2 Method 2: Company certification

A scheme for security certification of companies can be organised in the same way as for quality certification according to ISO 9000. Typical requirements will include a proper security management and the installation of security controls. For the product development, a strict methodology to safeguard security must be adhered to. The existing draft standards prEN726-1&2 provide a good basis for this. To have a set of standardised test procedures alone as described above, without any way of encouraging or enforcing their use has limited value. It is therefore assumed that it will be linked to company certification.

This method may be the cheapest and the most practical solution. New developments and new releases of a product will immediately be available for the public.

2.2.3 Method 3: Independent evaluation

In 1985, the US government institution NCSC published a set of criteria for security evaluation of computer equipment, called TC-

SEC [USD85] (also called the *Orange Book*) which was the first of its kind. This was done because the US DoD and other US state agencies were paying more and more attention to information security and therefore saw the need to have computer systems evaluated before they were purchased.

When similar schemes later were set up by other countries, like the ITSEC [EC92] in Europe, they were more oriented towards the civil market, and this led to a fundamental problem regarding the responsibility for the evaluation. In the case of TCSEC, the government is responsible for the evaluation, and if the systems still contain flaws, it is the governments own fault. In the case of an independent evaluation of computer equipment for the civil market, the evaluator can not take the responsibility of damage caused by undiscovered security flaws. What an evaluation really is worth can therefore be questioned. For most companies which consider having their products evaluated, marketing pressure seem to be the most important reason. This creates a market for an evaluation which in it self has questionable value. This would also be a problem in a scheme for evaluation of smart card products.

In 1992, the European Commission set up an action plan, called the INFOSEC Initiative, in order to co-ordinate the activities in the area of information security in Europe. ITSEC goes under the INFOSEC umbrella and one of the 1993 investigations, called *Security Project for Evaluating Smart Cards* [EC94a] (project S2108), had as goal to see how the evaluation of smart cards can be included in ITSEC and to gain some experience in evaluating smart cards. The report was released in September 1994, and one the results is the definition of two *Security Targets*, based respectively on the draft standard prEN726 and on CEN's working draft for Intersector Electronic Purse [CEN93]. In ITSEC terminology, the Security Target is a specification of the security required of the *Target of Evaluation*, i.e. the product to be evaluated. It is therefore surprising to note that two draft standards were used as target of evaluation instead of a specific product, and the report explains this by saying that the problems with confidentiality of e.g. security enforcing functions of real products forced them to go away from the normal approach and instead choose an "abstract" Target of Evaluation. This again illustrates to what extent the manufacturers fear the leak of details about the security mechanisms, and the report also mentions the

confidentiality of information and the trust in the evaluators as a problem to be solved before a real smart card can be evaluated. Although the report is modest when it says that “*we are at the beginning of the relationship between smart cards and ITSEC*”, the overall conclusion is positive.

In this context, it is interesting to touch another 1993 INFOSEC investigation (project S2109) entitled *Security Evaluation and Communications Systems* [EC94b] where the report also was released in September 1994. One part of the project is an assessment of the feasibility of performing an evaluation on CERDIAL, a Trusted Third Party service supplied by the French data carrier TRANSPAC. Since CERDIAL is based on the use of smart cards, the feasibility of evaluating smart cards is also a part of the study, but in this regard the conclusion of S2109 is more negative than that of S2108.

2.3 Suggestions for using the assurance methods

2.3.1 In a mono-application environment:

Mono-application cards will constitute the vast majority of smart cards for many years. These cards are developed with only one application in mind, and although there is no strict need to comply with standards, it will often be an advantage. It will for example provide reusability of modules and test equipment, and probably a better acceptance of the systems in the market. The security requirements can be adapted to each particular system. Confidentiality of the specifications will typically be an important security factor, and independent third party evaluation of the products will therefore not be realistic. This is very much like the present situation where the service provider is totally responsible for the whole system. To increase the public trust in the system, adherence to standardised test procedures and company certification is the best solution.

2.3.2 In a closed multi-application environment:

An evolution towards closed multi-applications systems will be initiated by associated service providers who see the advantage of combining their respective applications on one card. Service providers which set up several services will also try to integrate all its services

on one card. A typical example will be a student card where access to the library, payment for meals and photocopying, etc. will be put on a single card. Because applications coexist on one card and often will be using the same terminals, they must comply to the same specifications.

The set of security requirements should be more or less the same for all the applications, and is therefore less flexible. The assurance level for all applications must be determined by the application with the highest risk. As for mono-application systems, adherence to standardised tests and company certification are the most appropriate methods of providing the assurance.

2.3.3 In an open multi-application environment:

A totally open architecture must be orchestrated by national or international bodies. It will open up for multi-purpose terminals from which access to the information infrastructure of the modern society can be made. It will be possible to accommodate totally independent applications on the same smart card, and the loading, modification and removal of applications on a card must be possible either at a multi-purpose terminal, from home or by a simple visit to the service provider.

The security requirements for a totally open system would need to be more strict than the two previous cases because of higher complexity and additional threats. Company certification may be sufficient to provide a certain level of assurance, but because all applications should have the same assurance level, independent third party validation of products will probably be needed. This will necessarily include a strong scheme for evaluation and validation of hardware and the application software.

3 Independent Third Party Evaluation of Smart Cards

3.1 Validation v. Evaluation

The previous paragraphs defined security evaluation as one of three possible security assurance methods, in particular the best solution for open multi-application smart cards, and this method will be dis-

cussed in more detail below. Said very simply, evaluation according to TCSEC or ITSEC results in a level of assurance in a scale from 1 to 6 which reflects in which degree the security features implemented in the system are correctly implemented and adequate. This scheme would not be acceptable for smart cards intended for an open multi-application environment and the mass consumer market:

- The scheme is not well adapted to the mass consumer market.
- Administration and control would be unmanageable.
- It would have limited practical and legal implications anyway.

A scheme similar to the BSI approval of for example electrical equipment is certainly a better idea. Instead of evaluation, *validation* is maybe a more appropriate term. According to this scheme, only validated smart cards and validated applications would be certified for the consumer market.

Most of the principles already established for evaluation are nevertheless applicable to validation, the main difference being that instead of a scale of assurance levels, there must be a *minimum* level. There are two types of assurance according to ITSEC which both should be considered for validation. A product will pass only when both assurance levels are above the minimum:

- **Assurance of effectiveness:** This tells whether the implemented security features are adequate and strong enough to cover the security requirements and to counter the expected threats.
- **Assurance of correctness:** This tells whether a correct methodology has been used during the development process and whether the development and manufacturing environment is sufficiently protected.

When the application is not a pure security product, which is the general case, having different security functionality classes is irrelevant. The assurance of effectiveness will reflect whether the security functionality is adequate and appropriate for the security requirements and the given application.

It is assumed that the validation method to provide assurance will only be used for products intended for open multi-application

systems. This will require that both the chip hardware and the application software comply to international standards. The hardware must provide a standardised set of features and the application software must be written according to certain rules.

3.2 Properties of smart cards

The chip of a smart card is a complete computer system integrated into a single piece of silicon, and is commonly referred to as an MCU (Single-chip Microcomputer Unit). The CPU corresponds to the processor in a normal computer. The operating system and application programs are stored as ROM mask and can not be altered after manufacturing. Data and sometimes additional program code is stored in the *non volatile memory* (NVM) which physically is made of EPROM or EEPROM. The RAM is only used to store intermediate data during execution and not, as in a normal computer, to load executable code. An MCU is self programmable. That means that the ROM contains functions which make it possible to write to the NVM.

In present implementations, there is no real separation between operating system and application program. All the functions are implemented as one module which provides a set of commands at the interface. This type of MCU configuration would be unacceptable in a multi-application environment.

The only possible approach to a multi-application MCU is to have a clear logical separation between the operating system and the application programs. Applications can be stored as ROM mask together with the operating system or separately in NVM. The last alternative is the more flexible because it allows applications to be loaded, modified or deleted during the user phase of the smart card, but has the disadvantage that it requires from 3 to 6 times more space on the MCU than an equivalent ROM implementation. This is not only a limitation in today's mono-application cards, but will be the factor which determines the possible size and complexity of future multi-application cards

Most modern microprocessors are designed to function in a number of different operating modes which can be selected by the user. In the user-mode, which is the normal mode of operation in most applications, the CPU runs under the complete control of the user

software. Other modes allow access to internal data and address buses and are used for testing and initialisation purposes.

A secure MCU has the built-in capability to prevent, by various means, unauthorised access to the CPU, the memory areas and any data being processed or stored within the device, at any time. After it has been tested and passed as fully functional by the manufacturer, the only possible mode of operation for the chip must be the user mode, i.e. under exclusive control of the operating system and application software in the on-board ROM. The process of making irreversible modifications to the hardware to exclude certain modes of operation can be called sealing the MCU.

Unlike many other high-security systems, which are developed for a special function and used by trained specialists in relatively small numbers, smart cards are intended for large-scale use in a broad range of applications. Whereas the system operator is in control of all the components of a fixed IT system, the smart cards are out of the physical control of the service provider from the moment they have been handed over to the users. This exposes the smart card hardware and software to particular risks.

The most important properties which are unique to smart cards are summarised below. Some properties contribute to the security whereas others are a disadvantage:

- The hardware is physically and literally in the hands of the user. This is a disadvantage because it allows a malicious party to carry out a whole range of subtile attacks.
- The Operating system is stored as ROM mask. This is an advantage and automatically provides integrity and probably confidentiality of the operating system. For an attack to succeed, it must be carried out during the design of the ROM mask, before the manufacturing.
- Application software and data stored in EEPROM or as ROM mask. If access control to files stored in EEPROM can be efficiently enforced, it is an advantage regarding integrity and confidentiality.
- No system booting, only reset of internal state. This is an advantage, because protection mechanisms are active at all times.

- Smart card chips are sealed in order to exclude certain modes of operation. As long as the sealing can not be 100% guaranteed, this is a security risk.
- The present smart card processors lack hardware mechanisms to distinguish between the operating system and application software. This is a disadvantage because it requires that access control and other security functions must be enforced by hardware.
- The application software is split between the smart card and the external world. This is a disadvantage because of increased complexity.

Conceptually and logically, a distinction can be made between the smart card as a hardware platform and the applications which are loaded on top of it, and the validation should reflect this. The microprocessors used in the present smart cards have no hardware mechanism to distinguish between different modes of operation (e.g. privileged and unprivileged) which otherwise would have made possible a hardware enforced differentiation between the functions of the operating system and those of the application software. As long as differentiation can not be achieved, the operating system must be considered as just a special application among all the others. For a smart card to be used in a multi-application environment, it is desirable that the CPU is able to make the distinction, so that the operating system can be considered as part of the hardware platform.

3.3 The validation tasks

The validation of smart cards must have as goal to prove the correctness of the hardware and software, and must be based on the specifications of the required functions and mechanisms. The validation consists of four main tasks:

1. It must be shown that the security requirements are adequate to counter expected threats and sufficient for the level of risk.
2. It must be shown that the specified functions and mechanisms are exactly what is needed to fulfil the requirements.

3. It must be shown that the hardware and software implementation of the specifications is correct.
4. It must be shown that no undesired functions have been implemented.

By “undesired functions” is meant unspecified functions which can be a threat to the overall security of the system. Both the specifications of the cryptographic protocols and algorithms and the hardware/software implementation must be checked for this purpose. Typical examples are weaknesses which only are exposed under certain combinations of functions, weaknesses in the protocols and cryptographic algorithms themselves and Trojan horses in the hardware/software which can be externally activated to leak information or to perform illegal tasks.

The set of security requirements, which constitutes the security policy of the smart card system, must be based on a general risk analysis of the applications. prEN726-2 provides some useful security requirements to start with. The policy must in fact be common for all open multi-application systems, and even if the inherent risk of different applications can vary, a standardised set of security requirements should be used as a basis for the development of all smart card chips and applications of this category. For applications with a higher risk and where additional security requirements are necessary, the open platform can no longer be used.

The task of the developer starts with transforming these requirements into a security model, which for the higher assurance levels must be based on formal or semi formal languages. Examples of requirements which could undergo formalisation can be that certain functions are excluded under a particular mode of operation or that certain areas of the memory must be subject to access control. Any useful security model will necessarily include the definition of subjects and objects as well as access modes which regulate how subjects can access objects.

When a new application is to be loaded into a smart card or an existing application is to be modified, then conclusions of previous validations of the same (version of the) application can be used directly and thereby simplify the 1st, 2nd and 3rd tasks of a validation, i.e. the module specifications do not need to be validated again. For the 4th task on the other hand, which consists of showing that the

implementation of the new application or that combinations with existing applications has not introduced any undesired functions, it will not be possible to take advantage of previous validations unless the application previously has been validated in exactly the same configuration of applications and operating system.

To prove, or at least to show with reasonable confidence, that an application module contains no undesired functions, is a complex task and will for large software modules require a rather large effort. Each reachable state of the finite state machine, including all possible inputs and outputs, must satisfy the security requirements which are assumed to be invariant at the implementation level.

A validator must be independent of both manufacturers and users, and must have access to all documentation and material which are necessary for the validation. Each step of the validation process must be well documented in order to support the conclusions. It must be possible for an expert to go through the resulting documents and verify the correctness of the validation and the soundness of the conclusions. The independent status of the validator will increase the public confidence in the security of a validated application.

3.4 The problem of confidentiality

If independent third party validation should become mandatory, it would require sharing test methods and information about vulnerabilities between private companies and independent institutions. A public acceptance of a validation scheme could even require an open discussion and disclosure of information about risks and vulnerabilities to the public. It is therefore unfortunate if smart card security really depends on confidentiality of MCU design and specifications.

The only way out of this situation seems to make the security totally independent of the semiconductor architecture and ROM mask, and instead to base it on secret keys and algorithms stored in the card. This facilitates the security control by concentrating the trust in a few entities. For this to be possible, it is crucially important that the contents of an EEPROM memory cell cannot be read by physical means and that the access through the specified interface can be strictly controlled.

In this regard it has been claimed that the electrical charges representing information in an EPROM memory cell are so volatile

that approaching probes to the silicon would destroy the memory contents. Nevertheless, irrefutable evidence that no physical method exists to reveal the contents of a memory cell has yet to be found, and new scientific discoveries could change any previous assumptions.

Based on the above, it is very unlikely that test and validation methods will ever be made public through an open standard. Smart card manufacturers who know the vulnerabilities of their products are likely to insist on confidentiality of validation methods. The consequences will be a lack of openness which will jeopardise the introduction of open multi-application smart cards.

Conclusion

Among the three different methods of obtaining security assurance which have been mentioned above, the first two (i.e. standardised test procedures and company certification) were only given little attention although this is a subject which could be explored further.

The third method, i.e. independent third party validation, has been discussed in more detail. This method's major problem, which has been pointed out several places, is the strict confidentiality required for the information needed to perform the evaluation. Smart cards are commonly used as part of computer systems, and if security evaluation of these systems shall be meaningful, smart cards must also be included. It is therefore necessary to find solutions to this problem and to put smart cards on the agenda for security evaluation.

References

- [CEN93] CEN. *WD: Intersector Electronic Purse*. European Committee for Standardisation, TC224/WG10, 1993.
- [CEN94] CEN. *prEN 726-1,2,3: Requirements for IC cards and terminals for telecommunication use*. European Committee for Standardisation / ETSI STC TE9, 1993, 1994.
- [EC92] EC. *Information Technology Security Evaluation Criteria (ITSEC)*. The European Commission, 1992.

- [EC94a] EC. *INFOSEC investigation S2108: Security Project for Evaluating Smart Cards*. The European Commission, September 1994.
- [EC94b] EC. *INFOSEC investigation S2109: Security Evaluation and Communications Systems*. The European Commission, September 1994.
- [ISO93] ISO. *CD 7816-4. Identification cards - Integrated circuit cards with contacts*. ISO/IEC JTC1/SC 17/WG4, 1993.
- [Jøs93] Audun Jøsang. Studies of smart card security in telecommunication systems. Master's thesis, Royal Holloway College, University of London, 1993.
- [Kru91] Dietrich Kruse. The new siemens computer card. In *SMART CARD 2000*. CWI/DigiCash, Amsterdam, 1991.
- [USD85] USDoD. *Trusted Computer System Evaluation Criteria (TCSEC)*. US Department of Defence, 1985.