2003년도 대한전기학회 하계학술대회 논문집 2003.7.21-23

스마트 카드 평가를 위한 보호프로파일의 가정요소 분석

김태훈, 김민철, 노병규
한국정보보호진흥원

Analysis of Assumption Part of Protection Profile for Evaluation of Smart Card

Tai-hoon Kim, Min-chul kim, Byung-gyu No
Korea Information Security Agency

Abstract - ISO/IEC 15408 requires the TOE(Target of Evaluation) Security Environment section of a Protection Profile(PP) or Security Target(ST) to contain a list of assumptions about the TOE security environment or the intended usage of the TOE. This paper presents a specific conditions should be assumed to exist in the smart card environment and the analysis of those conditions developer of smart card PP must consider.

1. Introduction

The credit-card-sized smart card uses an embedded chip that, unlike a credit card, can be programmed to accept, store and send data. Most smart cards manage binary text and numeric data. Smart cards can store a dollar value, and the user can buy items at convenience stores or other retailers that accept the cards. The cards can store medical records or can be used to swipe through a card reader on a PC to purchase goods over the Internet. Another use is to pay for boarding trains and buses.

The number of smart cards in use worldwide will more than double to 2.3 billion by the year 2000, according to a new survey. About 1.1 billion smart cards are in use today, according to the Global Smart Card Advisory Service, a cooperative venture by The Tower Group and The Centum Consultancy, which is owned by VeriFone, Inc. Companies will spend $1.9 billion on smart cards this year, the report said. The market will take off when processors are built into the cards, allowing multiple uses. Among the functions would be credit cards, debit cards and storage of identification information storage, such a person's medical history, we thought.

This paper presents a specific conditions should be assumed to exist in the smart card environment and the analysis of those conditions developer of smart card PP must consider.

2. Protection Profile

2.1 Overview of Protection Profile

A PP defines an implementation-independent set of IT security requirements for a category of TOEs. Such TOEs are intended to meet common consumer needs for IT security. Consumers can therefore construct or cite a PP to express their IT security needs without reference to any specific TOE[1-3].

The purpose of a PP is to state a security problem rigorously for a given collection of systems or products (known as the TOE) and to specify security requirements to address that problem without dictating how these requirements will be implemented. For this reason, a PP is said to provide an implementation-independent security description. A PP thus includes several related kinds of security information (See the Fig. 1).

A description of the TOE security environment which refines the statement of need with respect to the intended environment of use, producing the threats to be countered and the organisational security policies to be met in light of specific assumptions.

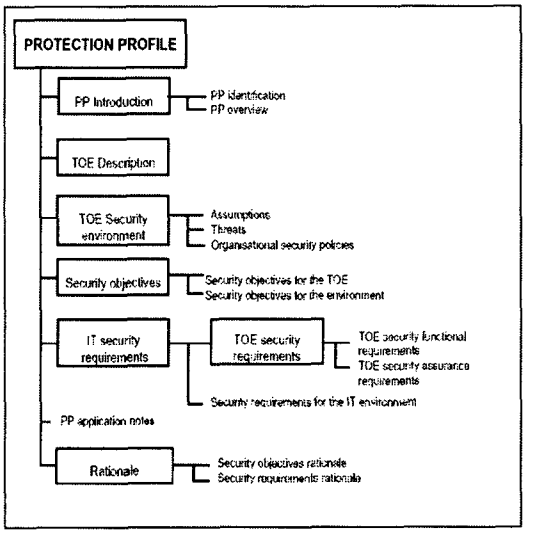

Fig. 1. Protection Profile content

2.2 TOE Security Environment

ISO/IEC 15408 defines the requirements for the content of this part of a PP in [15408-1], subclauses B.2.4 and C.2.4. The wording of these two sections is identical, which can be taken as an indication that the expected

content of the TOE Security Environment section does not differ greatly between a PP and an ST[4-6].
The purpose of the TOE Security Environment section is to define the nature and scope of the definition of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed, i.e. the security concerns, to be addressed by the TOE.
TOE security environment will therefore involve a discussion of:

a)assumptions made regarding the TOE security environment, thereby defining the scope of the security concerns;
b)the assets requiring protection (typically information or resources within the IT environment or the TOE itself), the identified threat agents, and the threats they pose to the assets;
c)any organisational security policies or rules with which the TOE must comply in addressing the security concerns.

Subsequent sections of the PP show how the security concerns will be addressed by the TOE, in combination with its operating environment. It is therefore important to ensure that the security concerns are clearly and concisely defined - otherwise you may end up with a PP that addresses the wrong concerns.

2.3 How to Identify and Specify the Assumptions

ISO/IEC 15408 requires the TOE Security Environment section of a PP to contain a list of assumptions about the TOE security environment or the intended usage of the TOE. To compile such a list, we first need to ask the following question:

"What assumptions are we making about the TOE security environment and the scope of the security concerns?"

For example, it may be necessary to make some assumptions in order to ensure that a potential threat to an asset is not, in practice, relevant in the TOE security environment. The following types of assumption should be included:

a)aspects relating to the intended usage of the TOE;
b)environmental protection of any part of the TOE;
c)connectivity aspects;
d)personnel aspects.

Other assumptions may be included where these have had a material effect on the PP content, for example assumptions which led to the choice of the assurance requirement. However, it must be remembered that ISO/IEC 15408 requires that the formally identified assumptions have to be shown to be upheld by the security objectives. General assumptions which cannot be traced to security objectives may nonetheless be usefully included within the descriptive (informative)
text in the PP.
It is unlikely that we will be able to completely identify all the assumptions we are making in a single attempt. Rather, we should expect to be identifying additional assumptions throughout the development of the PP. In particular, when constructing the PP rationale, we should consider whether we are making any assumptions that have not been stated in the PP.
When adopting this iterative approach to identifying assumptions, it is important to avoid the inclusion of any assumptions relating to the effective use of specific TOE security functions that we identify in the process of constructing the rationale. Such detail would be more appropriately included as security requirements for the non-IT environment.
It is, however, reasonable to state as a personnel assumption that the TOE has one or more administrators who are assigned responsibility for ensuring the TOE security functions are configured and used appropriately.
For ease of reference, it is recommended that each assumption is numbered or otherwise uniquely labelled.

3. Assumptions for Smart Card PP

There may be very many assumptions for the smart card PP, and next are some of them.

1. A CAD to which the TOE establishes a secure link is assumed to be secure : The CAD may have the capability to establish a secure communication channel with the TOE. This is typically accomplished through shared secret keys, public/private key pairs, and/or generation of session keys derived from other stored keys. It is assumed that when such a secure link is established, the TOE may consider the CAD to be adequately secure for trusted communications. Threats resulting from any failure of security in the CAD are beyond the scope of this PP and are assumed to be addressed in the CAD.

2. Management of TOE data off of the TOE is assumed to be performed in a secure manner : Significant information regarding TOE profile, personalization, ownership, etc. may be held by issuers or others in data bases not associated with the TOE. This information, if revealed in an unauthorized manner, could compromise all of the major security objectives. It is therefore important that the security of such data be adequately maintained.

3. All imported cryptographic keys are assumed

to be supported off-card in a secure manner : A variety of keys may be imported for use by, and in conjunction with, the TOE. These may include shared secret keys, public/private key pairs, etc. These keys will be supplied from the various bodies controlling the operations of the system in which the TOE is functioning. It is assumed that the generation, distribution, maintenance, and destruction of these keys is adequately secure.

4. Power and clock come from the CAD : The TOE is internally unpowered, so support must be delivered to the TOE from the card acceptor device or through an alternate connection to the TOE terminals. Both power and clock may be interrupted or reset in the normal course of business.

5. Management of roles for the TOE is performed in a secure manner off-card : The various roles involved in working with the TOE are established in the development and user community through the TOE manufacturers, card issuing bodies, etc. These roles will be managed off-card by these or other appropriate bodies.

6. Attacker Capability : Attackers are assumed to have various levels of expertise, resources and motivation. Relevant expertise may be in general semi-conductor technology, software engineering, hacking techniques, or the specific TOE. Resources may range from personal computers and inexpensive card reading devices to very expensive and sophisticated engineering test and measurement devices. They may also include software routines, some of which are readily available on the internet. Motivation may include economic reward or the satisfaction and notoriety of defeating expert security.

7. User Privilege : Users of the TOE are assumed to possess the necessary privileges to access the information managed by the TOE.

8. Administrator Competence : It is assumed that one or more authorized administrators are assigned who are competent to manage the security features of the TOE competently and in an on-going basis.

9. Card Protection during Packaging, Finishing and Personalisation : It is assumed that security procedures are used after delivery of the TOE by the IC Manufacturer up to delivery to the end-user to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that the Phases after TOE Delivery are assumed to be protected appropriately.

10. Plat-Appl Usage of Hardware Platform : The Smart card Embedded Software is designed so that the requirements from the following documents are met: (i) guidance documents (refer to the Common Criteria assurance class AGD) as the hardware data sheet, and the hardware application notes, and (ii) major findings of the hardware evaluation reports relevant for the Smart card Embedded Software. Note that particular requirements for the Smar tcard Embedded Software are often not clear before considering a specific attack scenario during vulnerability analysis of the smart card integrated circuit(AVA_VLA).
Therefore, such results from the evaluation of the smart card integrated circuit (as contained in the Evaluation Technical Report (ETR)) must be given to the developer of the Smart card Embedded Software in an appropriate and authorised form and be taken into account during the evaluation of the software. This may also hold for additional tests being required for the combination of hardware and software. The hardware evaluation shall be conducted before software evaluation can be completed. The hardware evaluation can be conducted before and independent from the evaluation of the Smart card Embedded Software.

3. Conclusion

For the Evaluation of IT products or systems, ISO/IEC 15408 (Common Criteria) requires PP or ST, and the TOE Security Environment section of a PP or ST contains a list of assumptions about the TOE security environment or the intended usage of the TOE. In this paper, we presented a specific conditions should be assumed to exist in the smart card environment and the meaning of those conditions.

Refernces

[1] ISO. ISO/IEC 15408-1:1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model
[2] ISO. ISO/IEC 15408-2:1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements
[3] ISO. ISO/IEC 15408-3:1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements
[4] KISA. Information Security Systems & Certification Guide, 2002
[5] ISO. ISO/IEC 15292:2001 Information technology - Security techniques - Protection Profile registration procedures
[6] ISO. ISO/IEC PDTR 15446 Guide for the Production of PPs and STs, Version 0.92
[7] Smart Card Security User Group Smart Card Protection Profile, Version 3.0, 9 September 2001
[8] Visa Smart Card Protection Profile, Draft Version 1.6, May 4, 1999