Physical Threat Description of Smart Card Protection Profile in Security Level 1st

Sang-Soo Yeo[1], Sang-Jo Youk[2], Gil-cheol Park[2], Seok-soo Kim[2], Tai-hoon Kim[2]
[1]*Dept. of Electrical Engineering and Computer Science, Kyushu University, Japan*
ssyeo@msn.com
[2]*Dept. of Multimedia Engineering, Hannam University, Daejeon, Korea*
{ youksj, gcpark, sskim, taihoonn }@hannam.ac.kr

Abstract

Security is concerned with the protection of assets from threats, where threats are categorised as the potential for abuse of protected assets. All categories of threats should be considered, but in the domain of security greater attention is given to those threats that are related to malicious or other human activities. 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 threats about the TOE security environment or the intended usage of the TOE. This paper presents a specific physical threats should be considered in the smart card PP which developers of smart card PP must consider in Security Level 1st.

1. Introduction

Many assets are in the form of information that is stored, processed and transmitted by IT products or systems to meet requirements laid down by owners of the information. Information owners may require that dissemination and modification of any such information representations (data) be strictly controlled. They may demand that the IT product or system implement IT specific security controls as part of the overall set of security countermeasures put in place to counteract the threats to the data.

IT systems are procured and constructed to meet specific requirements and may, for economic reasons, make maximum use of existing commodity IT products such as operating systems, general purpose application components, and hardware platforms. IT security countermeasures implemented by a system may use functions of the underlying IT products and depend upon the correct operation of IT product security functions. The IT products may, therefore, be subject to evaluation as part of the IT system security evaluation.

Where an IT product, such as smart card, is incorporated or being considered for incorporation in multiple IT systems, there are cost advantages in evaluating the security aspects of such a product independently and building a catalogue of evaluated products. The results of such an evaluation should be expressed in a manner that supports incorporation of the product in multiple IT systems without unnecessary repetition of work required to examine the security of products.

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.

This paper presents a specific physical threats should be considered in the smart card PP which developers 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.

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.

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 Threats

ISO/IEC 15408 requires that the PP or ST contains a description of any threats to the assets against which protection will be required ([15408-1], subclause B.2.4, page 39). However, ISO/IEC 15408 goes on to say that the statement of threats may be omitted if the security objectives are derived solely from the organisational security policies (OSPs) and assumptions: in other words, where the security concerns are defined in full by the OSPs and assumptions. This might be the case, for example, where an ST is being written in response to an RFP which defines those OSPs.

In practice, it is recommended that a statement of threats be included in the PP or ST as these generally provide a better understanding of the security concerns than a corresponding set of OSPs. Moreover, there is a danger in relying on the OSPs alone, since they may not be

up-to-date and accurately reflect the current threat. If you already have a comprehensive set of OSPs you are nonetheless encouraged to extrapolate the threats that they address in order to facilitate maximum reuse of the PP, as well as to convey a more thorough understanding of the security concerns.

The importance of risk analysis, to correctly identify the assets and the threats to those assets, should not be underestimated since if it is not done properly

a) the TOE may provide inadequate protection, as a result of which the organisation's assets may be exposed to an unacceptable level of risk;
b) the threats may be over estimated, raising the cost of implementation and the assurance required in the implementation, and limiting potential solutions.

It should, however, be noted that ISO/IEC 15408 does not provide a framework for risk analysis or the specification of threats at an organisational level. Similarly, a detailed discussion of the process by which the threats to the assets are identified (which is one of the hardest parts of an organisation s risk analysis) is outside the scope of this Guide. However, for completeness, the general principles involved are stated below; see also [15408-1] clause 4. The reader is referred to standards such as [GMITS] for more detailed guidance on this topic.

2.4 Completing the statement of threats

ISO/IEC 15408 requires the TOE Security Environment section to include all threats to the assets that are relevant for secure TOE operation. The threats that are of principal interest are those that will be countered by the TOE (which will often be in association with procedural or other non-technical countermeasures). However, for completeness, the PP or ST may need to include some threats that are not at all addressed by the TOE, for example because of attack methods or threat agents against which the TOE offers no protection.

Examples of threats that are relevant to secure operation of the TOE, but which might not be addressed by the TOE, might include:

a) physical attack against the TOE;
b) abuse of trust by highly privileged users;
c) improper administration and operation of the TOE by careless or improperly trained administrators.

The decision as to which threats are to be addressed by the TOE, and which (if any) are only addressed by the environment, will not (of course) be made until the security objectives are finalised.

It should be noted that the identified environmental assumptions may preclude certain threats that would otherwise have been considered relevant to the secure operation of the TOE. It follows from this that the PP or ST author has a certain amount of freedom in deciding whether such aspects are dealt with in the environmental assumptions or in the statement of threats to be countered by the operating environment. Either approach is acceptable since both assumptions and threats have to be mapped onto the security objectives which uphold or address them. The choice between these two alternatives should therefore be made on the basis of which approach best helps the reader to understand the security concerns. As a general rule, specific attacks should be handled as threats, whilst more general forms of attack may be best handled as assumptions. Whichever approach is adopted, however, it is important that the issue is only stated once.

2.5 Attacker’s capability

Attackers are assumed to have various levels of expertise, resources, and motivation. Relevant expertise may be in general semiconductor technology, software engineering, hacking techniques, or in the specific TOE. Resources may be software routines, some of which are readily available on the Internet. Hardware resources may range from personal computers and inexpensive card reading devices to integrated circuit test and measurement devices. It should be noted that some of the most sophisticated capabilities required to attack the TOE are derived from integrated circuit fault analysis and reverse engineering techniques developed for integrated circuit manufacturing. As such, not only are these techniques published, but supporting test equipment is also widespread and commercially available. Motivation may include economic reward or the satisfaction and notoriety of defeating expert security. It is assumed that given sufficient time and expertise, any smart card can be compromised.

3. Security Level

In general, threat agents' primary goals may fall into three categories: unauthorized access, unauthorized modification or destruction of important information, and denial of authorized access. Security countermeasures are implemented to prevent threat agents from successfully achieving these goals.

Security countermeasures should be considered with consideration of applicable threats and security solutions deployed to support appropriate security services and objectives. Subsequently, proposed security solutions may be evaluated to determine if residual vulnerabilities exist, and a managed approach to mitigating risks may be proposed.

Countermeasures must be considered and designed from the starting point of some DSS design or software development processes. The countermeasure or a group of countermeasures selected by designers or administrators may cover all the possibility of threats. But a problem exits in this situation. How and who can guarantee that the countermeasure is believable?

Security engineering may be used to solve this problem. In fact, the processes for building of security countermeasures may not be fixed because the circumstances of each DSS may be different.

We propose a method for building security countermeasures as below.

3.1. Threats Identification

A 'threat' is an undesirable event, which may be characterized in terms of a threat agent (or attacker), a presumed attack method, a motivation of attack, an identification of the information or systems under attack, and so on.

Threat agents come from various backgrounds and have a wide range of financial resources at their disposal. Typically Threat agents are thought of as having malicious intent. However, in the context of system and information security and protection, it is also important to consider the threat posed by those without malicious intent. Threat agents may be Nation States, Hackers, Terrorists or Cyber terrorists, Organized Crime, Other Criminal Elements, International Press, Industrial Competitors, Disgruntled Employees, and so on.

Most attacks maybe aim at getting inside of information system, and individual motivations of attacks to "get inside" are many and varied. Persons who have malicious

intent and wish to achieve commercial, military, or personal gain are known as hackers (or cracker). At the opposite end of the spectrum are persons who compromise the network accidentally.

3.2. Determination of System Security Level and Robustness Strategy

Robustness strategy should be applied to all components of a solution, both products and systems, to determine the robustness of configured systems and their component parts. It applies to commercial off-the-shelf (COTS), government off-the-shelf (GOTS), and hybrid solutions. The process is to be used by security requirements developers, decision makers, information systems security engineers, customers, and others involved in the solution life cycle. Clearly, if a solution component is modified, or threat levels or the value of information changes, risk must be reassessed with respect to the new configuration [3].

Various risk factors, such as the degree of damage that would be suffered if the security policy were violated, threat environment, and so on, will be used to guide determination of an appropriate strength and an associated level of assurance for each mechanism. Specifically, the value of the information to be protected and the perceived threat environment are used to obtain guidance on the recommended evaluation assurance level (EAL).

Furthermore, to decide systems security level, EAL is not a perfect one. So we should decide TL (Threat Level) and AL (Asset Level) to get more exact SL (Security Level). About the decision of SL, please recommend our report [4].

Table 1. Determination of Security Level by Threat Level and Asset Level

Asset Level	Threat Level					
	TL1	TL2	TL3	TL4	TL5	TL6
AL1	**SL1**	**SL1**	**SL1**	**SL1**	**SL2**	**SL2**
AL2	**SL1**	**SL1**	**SL2**	**SL2**	**SL3**	**SL3**
AL3	**SL1**	**SL2**	**SL2**	**SL3**	**SL3**	**SL4**
AL4	**SL1**	**SL2**	**SL3**	**SL3**	**SL4**	**SL4**

4. Physical Threats for Smart Card PP

There may be some threats for the smart card PP as like those;

1. An attacker may perform physical probing of the TOE to reveal design information and operational contents : Physical probing may entail reading data from the TOE through techniques commonly employed in IC failure analysis and IC reverse engineering efforts. Such probing may include electrical functions but is referred to here as physical since it requires direct physical contact with the chip internals. The goal of the attacker is to identify such design details as hardware security mechanisms, access control mechanisms, authentication systems, data protection systems, memory partitioning, or cryptographic programs. Determination of software design, including initialization data,

personalization data, passwords, or cryptographic keys may also be a goal. The TOE may or may not be powered during probing and may not be operational after such activities.

2. An attacker may perform physical alteration of the TOE in order to reveal operational contents or design information, or to change TSF data or the TOE security functions so that the TOE can be used fraudulently : This modification may be achieved through techniques commonly employed in IC failure analysis and IC reverse engineering efforts. One goal is to identify such design details as hardware security mechanisms, access control mechanisms, authentication systems, data protection systems, memory partitioning, or cryptographic programs. Determination of software design, including initialization data, personalization data, passwords, or cryptographic keys may also be a goal. A further goal is the modification or manipulation of debug lockouts, first use indicators, card use blocking, blocking function configuration, card block indicators, or card disablement indicators so that the TOE could be fraudulently used.

5. 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 threats about the TOE security environment or the intended usage of the TOE.

Security is concerned with the protection of assets from threats, where threats are categorised as the potential for abuse of protected assets. All categories of threats should be considered, but in the domain of security greater attention is given to those threats that are related to malicious or other human activities.

In this paper, we identified a specific physical threats should be considered in the smart card PP which developers of smart card PP must consider in Security Level 1st.

6. References

[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
[9] Tai-hoon Kim and Seung-youn Lee, “Security Evaluation Targets for Enhancement of DSSs Assurance”, ICCSA 2005, LNCS 3481, 491-498
[10] Tai-hoon Kim, “Draft Domestic Standard-Information Systems Security Level Management”, TTA, 2005