available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

Smart card security evaluation: Community solutions to intractable problems

Tony Boswell

SiVenture, Unit 6, Cordwallis Park, Clivemont Road, Maidenhead, Berkshire SL6 7BU, United Kingdom

ABSTRACT

Evaluation of smart card security faced seemingly intractable problems of consistency and repeatability in its early days. The deeply specialised technologies, large parameter spaces for attacks, and the evolving attack types and countermeasures mean that the scope for variation in evaluation practice, and hence in evaluation conclusions, is potentially huge. The situation is further complicated by the fact that countermeasures against some types of attacks depend on both hardware and software, but there is also a need to evaluate hardware without specific software present at the time of evaluation. Stakeholders in the smart card world have formed a Community that has successfully created and applied interpretation of Common Criteria (ISO 15408) to deal with this problem and to achieve international mutual recognition of evaluation results. This paper discusses examples of the smart card security problem in order to illustrate some of the difficulties, and describes some of the interpretation that has been defined for rating the difficulty of an attack via calculation of an attack potential. It also considers the nature of the Community that has enabled the interpretation to be both defined and put into practice successfully.

In this paper we consider the assessment and certification of smart card security, and the ways in which solutions to the problems of assessment and understanding the meaning of security certification have been produced by forming a 'Community' of stakeholders. The paper takes on the dual goals of providing some background in the type and technology of smart card security assessment, and also of trying to describe and explain the importance of the Community in overcoming huge difficulties in standardisation and international recognition of security certification. Because many of the problems arise from the deeply technical nature of carrying out attacks on a smart card (and, especially, on the underlying integrated circuit), the Community goes beyond the notion of a standards committee or working group. It provides a forum for current issues to be discussed (thus helping to ensure that the relevance of security evaluation remains fresh), and for competitors to work together.

The members of the smart card Community that are actively engaged in Common Criteria certifications are currently represented by the JIL Hardware Attacks Subgroup (JHAS) and the International Security Certification Initiative Working Group 1 (ISCI-WG1). It is therefore mainly these groups that the term 'Community' refers to when it is used in this paper. Originally formed out of working groups based around the smart card industry body Eurosmart, these groups have evolved and extended their membership over a number of years to include IC and software developers, card manufacturers, card issuers, evaluators, and Common Criteria certification bodies (which are government bodies established in each country that issues Common Criteria certificates). The Community, principally through the Certification Bodies, has established strong relationships with the bodies that manage and maintain the Common Criteria, and this provides the path for making interpretation documents 'official', in the sense

E-mail address: tony.boswell@siventure.com

1363-4127/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.istr.2009.06.002

that it becomes mandatory to use them in evaluations of smart card products.

This Community has established a regular meeting schedule, with work items that have resulted in Protection Profiles[1] for smart card hardware and software as well as numerous documents that record interpretations of Common Criteria requirements. All of these documents are intended to make clear (and therefore repeatable and hence internationally recognisable) how smart card evaluations need to be carried out.[2] Probably the most widely used of these is the document defining interpretation of attack potentials (SmC AP), which includes the definition of attack parameters described later. But the benefits extend beyond the formal documentation, and the whole Community benefits from a shared understanding of smart card security evaluation, and from the trust relationships that are formed while defining the problems and creating solutions.

The early work on evaluation of smart cards was mainly concerned with their suitability for financial applications, but increasingly we see other significant application domains such as transport ticketing applications (which often also act as electronic purses) and ePassports (or, more generally, Machine-Readable Travel Documents), not to mention the other traditional roles as authentication tokens or signature devices. Recent product developments have seen the smart card move from its origins in the use of a contact interface, through increasing use of contactless and dual-interface cards, and into the 'larger chip' domain: here the IC is no longer constrained to the relatively small dimensions needed for a smart card, but is placed into a portable device (such as a phone handset) to serve a traditional smart card role, not just in terms of the communications network (as with a SIM card) but by enabling the portable device to act as a security token for authentication, payment and ticketing applications.

The Community-based approach to smart cards arises largely because of the complexity of the security problem and the links between the various actors involved. Whilst the problems and issues are not completely resolved – indeed the evolution of some aspects of the attacks and countermeasures is itself one of the problems that need solving – remarkable progress has been made. Smart cards are not unique in having complex security problems and relationships between actors, but the Community solution in this domain has perhaps proceeded along an unusually collaborative path. Part of the purpose of this paper is to try to describe the reasons why the Community approach emerged, and therefore why it may apply to other security fields with similar issues.

In the remainder of this paper we therefore proceed as follows:

- The security problem is discussed: we start from a position in which highly specialised attacks have to be applied, and in which complete coverage of testable attack spaces is unlikely to be achieved in any reasonable time. When potential vulnerabilities are found, we often then face difficulties in relating the results of closely controlled experiments to real-world attacks.
- The problems of composition are discussed: smart card products combine at least a hardware product – the chip – with a software product – the application. In many cases there is more than one piece of software: an operating system and one or more applications, for example. This raises a number of problems concerning what vulnerabilities can be recognised at what stage, how to manage risks between the hardware and software developers (and indeed the users or card issuers), and how to use results from one stage of evaluation to ensure that other stages have suitable information.
- The security evaluation background is discussed: in this paper we will be mainly concerned with Common Criteria (ISO 15408) evaluation and certification, but the relationship to other evaluation approaches is also discussed.
- The nature of the Community is analysed, and some reasons and requirements for its success are discussed.

1. The smart card security problem

Smart cards are often introduced as a security *solution*. They provide a portable, flexible computing platform that is somehow taken to be intrinsically secure. They solve the problems of widely distributing complex cryptographic capabilities to vast numbers of individuals, and of secure key storage to use with that cryptographic capability. This is, of course, not the complete story. Smart cards may seem intrinsically secure because they have such a limited interface: unlike a PC they do not even have direct means to communicate with a user, relying on some sort of interface device (IFD) and an understanding of protocols, file structures, and APIs. They have no apparent peripherals or other removable parts that might be straightforwardly attacked, and their interface can be tightly constrained by the developer to limit the scope for an attacker to interact with the card.

So far this leads us to what we might think of as a traditional software security problem. We have concerns over things such as:

- Protocol errors (e.g. allowing man-in-the-middle attacks; allowing replay attacks; or not protecting the integrity of parameters in critical messages).
- Abuse of the interface to provide unintended functions (e.g. low-level access to a confidential data file; transmitting an unencrypted PIN value for verification over a contactless interface, or returning old data in a communications buffer).
- Internal errors such as buffer overflows.
- Failures in implementation of logic (e.g. conflicts in access control rules; or incorrect state machine transitions).

All of these are relevant when writing and evaluating smart card software. Indeed, as we shall see, there are additional ways in which we may look to the software to address actual or potential vulnerabilities in hardware. However, apart from these areas in which the software may reflect hardware

[1] A Protection Profile is essentially an implementation-independent statement of Common Criteria security and assurance requirements for a certain type of product (such as a smart card IC or smart card operating system).

[2] These documents can be found on the Common Criteria website at www.commoncriteriaportal.org.