USING THE COMMON CRITERIA IN SMART CARD SECURITY

Title of Panel: Using the Common Criteria in Smart Card Security

Panel Chair: Stuart W. Katzke, PhD
Chief Scientist, Information Assurance Solutions Group
National Security Agency
9800 Savage Road, Suite 6713
Fort George G. Meade, MD 20755-6713
phone: +1.410.854.7308
email: swkatzk@missi.ncsc.mil

Panelists:
The panelists are currently engaged in different aspects of smart card security in industry and government. The wide variety of viewpoints offered on the common problem of securing this cutting-edge technology should provide a very useful, stimulating and enlightening discussion.

Kenneth R. Ayer, Ph.D.
Chip Card Security Director
Visa International
PO Box 8999
San Francisco, CA 94128-8999
phone: +1.650.432.3356
email: kayer@visa.com

Eugene F. (Gene) Troy
National Institute of Standards & Technology
100 Bureau Drive, MS:8930
Gaithersburg, MD 20899
phone: +1.301.975.3361
email: eugene.troy@nist.gov
Chair, Smart Card Security Users Group

Gilles Lisimaque
Chief Technology Officer
Gemplus
6701 Democracy Blvd., Suite 505
Bethesda, MD 20817
phone: +1.301.581.1006
email: gilles.lisimaque@gemplus.com

Session Abstract

Smart cards are extremely popular in Europe and elsewhere, and are just beginning to become popular in the U.S. These very flexible tools are, in effect, highly portable and accessible computers that can be used to control very sensitive information, e.g., financial, personal identification, system authentication, and health records. The security of the smart card is rapidly becoming a major issue in securing the information infrastructure. Public confidence in the security of smart cards could be supported through development of industry-standard smart card security requirement sets, along with careful evaluation of smart card products against these requirements, including verification of sound development/construction practices and stringent testing.

The panel members will discuss current trends in smart card security from their perspectives. They will focus on identification and expression of security requirements for smart cards, development of smart card security capabilities, and Common Criteria (ISO 15408) based processes for evaluating smart card security in the international community. In the United States, this process is the National Information Assurance Partnership (NIAP), a joint activity of NIST and NSA. NIAP and the CC have superseded the old "Orange Book" based evaluation processes.

The following key issues will be addressed during the panel:

- Smart cards represent a variety of security challenges not present with more commonplace IT security products. The threat pattern is very different for these small but complex and highly-trusted objects, which typically control or represent assets of considerable value, yet are held and used by untrusted users.

- The security and functional testing of smart cards is now being done in a fragmented way, as may be agreed between a particular manufacturer and a customer (which may be an association of financial card issuers, such as VISA, MasterCard, American Express, etc.). There are no agreed industry standards for the secure development and functioning of smart cards, while basic standards do exist for their physical aspects and electronic interfaces with card readers.

- The IT product security evaluation process (e.g., The National Security Agency's TPEP/TTAP) has been used for about 15 years, first in the U.S., then in Canada, Europe, and now elsewhere. This process was originally based on NSA's "Orange Book", and later in different nations became based on a variety of security criteria.

- Through extensive international cooperation, IT product security evaluation is now increasingly based on ISO International Standard 15408 (the Common Criteria for IT Security Evaluation). ISO 15408 is the underpinning of a widening circle of Mutual Recognition of product evaluations done by member nations. ISO 15408 provides the capability of defining IT security requirements in a very comprehensive yet flexible way.

- The main question to be addressed by the panel is whether this ISO 15408-based process for defining requirements then using them in product evaluations, with the potential for widespread mutually recognized international acceptance of results, can beneficially be applied to smart cards.

The panel participants will represent the following viewpoints in their presentations:

- **Gilles Lisimaque, GemPlus**, will present the viewpoint of smart card vendors, who would like to bring a new product on line as quickly and inexpensively as possible, while meeting contractual commitments to customers.

- **Kenneth Ayer, VISA International**, will present the viewpoint of smart card issuers, who have the potential for extensive liability and operating problems due to security flaws in

smart cards.

- **Gene Troy, NIST**, will present the viewpoint of NIAP, an ISO 15408-based evaluation scheme that can help the industry develop standardized requirement sets (Protection Profiles) and provide for evaluation of smart card products at accredited testing laboratories. He will also discuss the activities of the Smart Card Security Users Group, of which he is chairman.