Security, the Smart Card and Cryptography

Guest Commentary of Jay Wack as seen on Telekom.net

How far can today's security technology take us in complex and mobile situations? An industry leader surveys a range of problems and solutions. (Complete Story)

Smart Cards and Cryptographic Software

By C. Jay Wack President, TECSEC, Inc.

August 14, 2000

The idea of access control has historically been defined as a physical property: guards, gates and guns are the operative metaphors. As our storage mediums became electronic in structure, we could still think in terms of limiting physical access to a terminal, a server, a computer.

Early connectivity between computers allowed us to continue to think in physical terms - a modem, a router, a gateway, a switch. But I believe that we have now reached such a stage of complexity that physical definitions of access control are inadequate by themselves. It is time to think of protecting the information object itself. If the object itself is provided some level of protection, then the method of transmission and storage of that object can be wide and varied, and supportive.

In the past, cryptography has been the exclusive province of hardware and has focused on communication links. It must now move to recognize a proportional response to risk, and mix software and hardware elements where appropriate.

This need can be met by a system that recognizes the differing levels of information that we want to create and the data separation that we want to enforce. The definition of hardware must also take into consideration the mobility of the user. Many of us have laptops, a desktop computer at work and a computer at home. Some of us have several points of entry into diverse networks and have multiple networks and multiple computers in our offices. We may also carry cell phones, pagers, digital assistants, and even computer-linkable watches.

The problems are apparent to all of us. The answer to these mobility problems is a system that will allow us to conduct our jobs and provide to us the information access that makes complex decisions possible. This Information Security problem of mobility, coupled with multiple applications, under differing levels of access, on a common platform with recognition of mixed ownership, mitigated liability, and tiered services, and at the same time remaining user-friendly, is also the current problem of commercial credit card issuers.

The Smart Card As Foundation Hardware

One of the enabling technologies being offered to accomplish this mobility is the smart card. The smart card of today is not the simple memory card, historically built for the telephone industry in Europe. Here in the US we have a weak business case for a single-application card.

Our telecom infrastructure has supported a magnetic stripe, online process very well. The movement to smart cards only becomes cost effective when we discuss multiple applications, under different ownership, and the support of complex functions and the storage of information.

Because of semiconductor industry efforts to make ever smaller dies for faster chips to enable faster and more capable applications, and efforts to continue to raise the level of complexity of the circuitry to continue to provide more capacity, which is the backbone for speed and capability, we now can put more computing power inside a 25mm square chip than was available on a small mainframe 15 years ago, and we can put that chip inside a robust smart card.

This is the foundation hardware to address mobility and multiple applications. No other product delivers this much at such a low price.

Today we are producing a smart card which contains an 8-bit processor, with 32k bytes of EPROM and a math co-processor for the public key generation, which by the way is done on card, with the participation of the owner of the card. By December, a card with 64k bytes of EPROM should cost less than $10. Within a year, a 32-bit processor fronting 256k bytes of storage should be available at under $20.

Adding Cryptography

To these high-end smart cards, TECSEC adds cryptography. The efforts to provide strong I & A with public key must be augmented by the use of supportive cryptographic key management extensions (such as ANSI Std X9.69, recently adopted by the American Banking Association for financial transactions) to provide for a manageable process to support data separation at the object level.

These same key management processes support multiple algorithms for compartmentalization and, by mirroring the logical existing lexicon of the organization, the ability to control who talks to whom, about what information, on what device. What we have designed and built is a Component Management System.

The modular approach offered here provides a proportional response to risk. The system can enable an all-software user, with limited access, to communicate with a smart card-enabled software user package providing more access control, to communicate with another user who has been augmented with hardware accelerators and alarms for special circumstances. All have the proportional ability to communicate privately with each other.

The Task Force on Security of Electronic Money was established by the Committee on Payment and Settlement Systems of the G10 Central Banks. The task force, in its report "Security of Electronic Money," found that a variety of security measures have been adopted to protect the integrity, authenticity and confidentiality of data and processes of smart cards. One critical feature of the card is the degree of tamper-resistance of the embedded microchip. Cryptography is the other critical safeguard identified by the task force, used to authenticate devices and messages and to protect data from unauthorized observation and alteration.

The issue of liability

We have found that putting multiple applications on a single card raises several issues. The largest of these issues is liability. The idea of a single authority for a card is easy if all of the applications are owned by that authority. Multiple ownership of applications demands keeping the access to the individual applications under the control of the owner of that application.

This control has been achieved by the use of the high-end card and its companion cryptographic controls, and most importantly, this approach has been accepted by the legal side of the banking industry. In addition, it has been pointed out that our approach does not require the organizations to change their current relationships or way of doing business.

An example: A document is generated for corporate discussion, by a program manager for, let's say, project Alpha. He knows the overall document is financial in nature, about budgets, concerning project Alpha. The overall document is labeled "company confidential," representing the first restriction to be enforced. He also embeds within the document several other subdocuments; each of these has further restrictions.

The enclosed spreadsheet is divided to reflect increasing detail, and each sheet is encrypted using names as part of the cryptographically enforced restricted access; "managerial" for one sheet, and "executive" for the final profit analysis.

The program manager does not know everyone in the company who may have this specific level of access. Nor does he need to know. His software application, combined with his smart card, which holds his particular cryptographic permission set, describing his roles within the company, affords him the ability to encrypt the information and use email to forward the document to his office server for later review, by him and by his appropriate co-workers.

This is a product developed by TECSEC, for the Windows environment, called Constructive Key Management, and licensed by Lockheed Martin in a product called Minotaur.

Isn't this the same application of the process needed for the analyst who edits collateral from a sensor, and encrypts the image of the airfield, with "coalition force access", the enlargement with the term, "US-Only" and his own annotations with the term "Eyes only"? This has been developed as a product called View from Northrop Grumman, designed for multi-level access to photographic images.

The process offered here can also be considered an extension to the X.509 Attribute model, which is used to convey a set of attributes along with a Public Key Certificate identifier or entity name.

The use of the attribute as an index function to a split key value, which when combined with the collective intent of an object produces a unique key, which in turn is used to restrict access to that object.

COMMERCIAL APPLICATIONS

This same solution might be applied commercially for the posting of a price list on a web site. The price list to the casual consumer shows retail in the first column, and first level quantity discount in the second. The authorized distributor, accessing the same website and the same object, would be provided columns 1&2, but also column 3, which shows his discount. The master distributor, with his permission set, sees column 4, cost. One posted object, with multi-level access, cryptographically assured.

Another commercial application: A telephone, the use of which is determined by the presence of a smart card. The first user can only make local calls, the next user local and long distance, the third, local/long-distance and network access.

The cryptographic link is also established to offer privacy and security to whatever call is made, at the level commensurate with the role-based permission set of the users.

Or equipment that, with the presentation of the proper smart card (and with the individual's cryptographically protected permissions on board) allows the equipment to turn on for the first soldier, and act as a simple receiver, while for the next soldier the same equipment is a transmitter/receiver.

The applications for this smart card-enabled cryptographically enforced technique will help all of us achieve the goal of using the networks all around us, in a controlled manner, to share appropriately the knowledge we have, and to execute the decisions we must make.

http://www.telekomnet.com/news/8-14-00_smartcards_cryptographic.asp