TWOBESMART:

MULTI-FUNCTIONAL SMARTCARDS FOR ACCESS CONTROL

V.W. STINESEN

ptt research

A WAY OF IMPROVING ACCESS CONTROL AT ROYAL PTT NEDERLAND NV HAS BEEN IDENTIFIED BY THE INFORMATION MANAGEMENT AND CORPORATE SECURITY DEPARTMENTS. AN EXAMINATION BY PTT RESEARCH REVEALED THAT THE PRESENT MEANS OF ACCESS CONTROL, I.E. A MAGNETIC-STRIPE CARD AND THE USER ID/PASSWORD COMBINATION, DO NOT SATISFY SECURITY CRITERIA. THE MAGNETIC-STRIPE CARD IS VERY EASY TO COPY, WHILE PEOPLE WITH USER ID/PASSWORD COMBINATIONS TEND TO BE FAR TOO LAX WITH THEIR PASSWORDS. THEY OFTEN CHOOSE SIMPLE PASSWORDS AND SOME PEOPLE EVEN WRITE THEM DOWN.

As these shortcomings can be eliminated by the smart card, the departments mentioned above asked PTT Research to improve logical and physical access control and at the same time to pinpoint any weaknesses in the smartcard concept.

smartcards

A smartcard is basically a small computer surrounded by plastic about the size and thickness of a credit card. It has the following features:

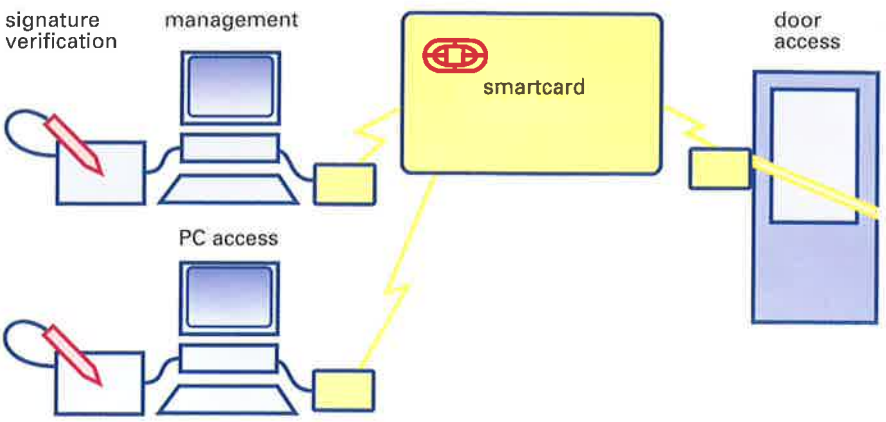
- a secure memory which, unlike the magnetic-stripe card, cannot be copied.
- a processor which can perform various tasks. Mutual identification is possible between a smartcard and other systems. The smartcard can encrypt communication with other systems and eliminates the security threat posed by tapping.
- multi-functionality which enables various security and other applications to be implemented on the smartcard.

The Twobesmart project

The Twobesmart project team was commissioned to implement physical and logical access control by means of smartcards. The examination concentrated on use of a single smartcard for physical access to rooms and logical access to workstations. It resulted in the development by the Twobesmart project team of a prototype access control system.

Prototype

The prototype has four independent elements: smartcard, door access, PC access and management (see Figure).



smartcard

At the heart of the system is the smartcard. It contains the authorizations to open doors and get into personal computers. The card also contains a PIN and signature characteristics which identify the holder as the real owner. A card which communicates by means of a contactless interface was chosen because it does not have contacts sensitive to abrasion.

Door access

Door access has been created using an interface with the existing access control system called Tobias. The old magnetic-stripe card readers have been replaced by a smart-card reader and specially developed software.

To open the door the user must place the smartcard against the reader for approximately half a second. This is the time it takes for the Tobias information to be read from the card and checked for authorization. If the information is correct the door is opened.

PC access

Before a user can work at a PC he must place his smartcard on the reader. The smartcard checks whether the holder is authorized to work on this particular PC. This is followed by a check on the user's identity for which purpose he has to give his PIN or signature. If both the authorization and identity of the user are correct he will be allowed to work at the PC.

If the user wishes to leave his desk for a moment but does not want to leave his PC unprotected, he simply has to pick up his smartcard and walk away. It renders the PC inaccessible by anyone but himself. The keyboard and mouse are disabled and the screen blanked. All the original user needs to do when he resumes work is to place his smartcard on the reader.

Management

Management consists of three independent applications:

- General management. This records and personalizes the smartcards. The manager records the user details of every smartcard in circulation. Personal data, PIN and signature characteristics are written to the smart card.

- Door access management. An existing application has been adapted and expanded to enable the management of smartcards instead of magnetic-stripe cards.

- PC access management. This records and changes PC authorizations and writes them to the smartcard.

Security and multi-functionality

Security and multi-functionality received special attention during development of the prototype. Together with the obvious question of user-friendliness, these two aspects are crucial to user acceptance of smart-card systems.

Security

Normally a smartcard only has a secure memory, but this alone is not enough to ensure their safe use.

Several security features have therefore been implemented on the smart cards:

- a smartcard does not communicate with another system until mutual identification has taken place;
- the smartcard uses a different key to encrypt communication each time;
- certain data is secured with special keys and only systems that know the key can use that data;
- the smartcard blocks itself permanently or temporarily as soon as it detects unauthorized usage (i.e. too many PIN, signature and key attempts).

Multi-functionality

The smartcard contains only two functionalities in the present system, but more can be added in the future. This modularity is evident from the definition of the management applications. General management controls aspects that do not concern specific applications. It provides the smartcard with the data and functions used by all applications. Each application on the card has its own separate sub-management with its own key-protected memory. Sub-managements do not have access to each other's data.

Smart-card trial

A six-month trial was conducted with the prototype access control system described above at the 'PTT-Borg' building in the city of Groningen. It was used to secure a small number of doors and PCs in the Information Management and Corporate Security departments. While the trial was in progress, PTT Research evaluated practical matters and also the technical and organizational aspects of the system.

One of the problems identified was the management of multi-functional smartcards and its organization. The variety of different applications has increased the complexity of management. Corporate Security and PTT Research are therefore setting up a new management structure which makes allowance for the requirements of all the departments involved.

The trial also revealed a simple way of increasing the security of the existing Tobias access control system by means of smartcards. Users would prefer a hands-free system, with the cards being read from a distance. It would no longer be necessary to place the card in or against a reader. Generally speaking the smartcard used in the trial was considered simple and user-friendly.

Developments

In view of the results obtained, Corporate Security set up a larger trial at the 'Hunzehuys' building in Groningen to test the cards in an operational environment. Initially the cards are being used only for physical access control. Other functionalities will be added as the trial progresses.

In the future the smartcard may replace the cards now in circulation and new functionalities may be added. It will evolve into a multi-functional staff card suitable for all card systems used by Royal PTT Nederland NV.

Summary

The features of the smartcard make it an excellent replacement for the magnetic-stripe card. PTT Research has developed a prototype access control system based on a multi-functional smartcard. The smartcard was successfully added to the existing Tobias access control system and a follow-up trial is now under way. The management of smartcards and the organization of management will require further attention. The smartcard may be introduced in the future as a multi-functional card issued to every employee of Royal PTT Nederland NV.

Addresses PTT Research

Technical scientific research

Dr Neher Laboratories
St. Paulusstraat 4
Leidschendam
P.O. Box 421
2260 AK Leidschendam
The Netherlands

Telephone: +31 70 332 56 02
Telefax: +31 70 332 64 77
Memocom:
Mailbox 27:NPS 1353

Europaviljoen
Winschoterdiep OZ 46
Groningen
P.O. Box 15000
9700 CD Groningen
The Netherlands

Telephone: +31 50 82 10 00
Telefax: +31 50 12 24 15
Memocom:
Mailbox 27:NPS 1126

Social scientific research

Duindoorn 31
Leidschendam
P.O. Box 421
2260 AK Leidschendam
The Netherlands

Telephone: +31 70 332 35 95
Telefax: +31 70 332 95 08

Stationsplein 7
Groningen
P.O. Box 15000
9700 CD Groningen
the Netherlands

Telephone: +31 50 82 25 34
Telefax: +31 50 82 29 80