

All of these arguments are naturally particularly relevant to electronic purses based on Smart Cards. The 'urge' to go online can be triggered by random variables and timing windows that are stored in the Smart Card. An equally effective method is to use a counter in the card that demands an online connection with mutual authentication after a certain number of off-line transactions have taken place, or once a certain off-line transaction level has been achieved. At the end of the session, the background system can reset the counter or modify the values of the parameters that control the on-line behavior of the card.

Protection: black lists

The possibility of counterfeit Smart Cards being used in a system can never be completely excluded, no matter how well they may be protected against attacks. The Smart Card system must also incorporate effective mechanisms for protecting users by blocking stolen cards throughout the entire system. The procedures that are used for this purpose are strongly dependent on the application in question and the design of the system, but they can all be reduced to a few basic techniques.

In order to prevent forged or lost Smart Cards from being used, it is necessary to maintain lists in which either valid cards or invalid cards are noted on the basis of some unique feature. This is usually a number, such as the card number. From the viewpoint of impeccable system design, in which everything that is not explicitly permitted is implicitly prohibited, a list of valid cards would be the best. Such 'white lists' would however be far too large in large systems. This can be easily illustrated by noting that in a system with 10 million Smart Cards and an 8-byte card number, the white list would contain 80 MB of data.

This is why in practice black lists are used, in which only the blocked cards are noted. In the example just mentioned, the size of the list would be reduced to 800 kB if the number of blocked cards were one percent of the total. However, if it were necessary to block significantly more than one percent of the cards in the system due to attacks or loss, the size of the list would quickly become impractical even with this approach.

In order to further reduce number of data transfers and the amount of data that must be transferred between the entity that maintains the list and the entity that tests cards against the list, 'red lists' are sometimes also used. A red list identifies cards that are demonstrably forged, which should either be immediately confiscated or at least blocked for all further transactions. The number of entries in such a list lies in the two or three figures, even with large systems.

Smart Cards can be checked against these lists in real time with systems that work on-line. With systems that work partially or fully offline, updated black lists and red lists must be transferred to the terminals as often as possible. This should occur at least daily, since protective mechanisms that are based on blocking lists are otherwise no longer effective.

Attack and defense: computer viruses and Trojan horses

Until recently, computer viruses were entirely unknown with Smart Cards, since the downloading of program code was not technically feasible in the operational phase. Modern Smart Card operating systems, however, have mechanisms that allows program code to be downloaded to the Smart Card after it has been issued to the cardholder, and that also allows such programs to be executed. This means that, in principle, the necessary conditions for the existence of computer viruses in Smart Cards have been created. By definition, a computer virus is a program that can reproduce itself and thus spread to other computers. If such a program cannot reproduce itself, it is called a Trojan horse. Both types

of program have in common that under certain circumstances they can carry out unauthorized actions in the host computer. With a Smart Card, this could involve reading and sending out the values of secret keys.

In contrast to an ordinary PC, it is not a straightforward task to load a program into the memory of a Smart Card and then execute it. Security mechanisms have been provided to prevent the unauthorized running of programs. For example, it could be necessary to authenticate the terminal, depending on the application in question. In addition, the program code normally must be secured using at least a MAC or a digital signature. Some Smart Card operating systems also mutually isolate the memory regions of the individual applications by means of software or hardware, so that the applications in the Smart Card cannot influence each other. The result of these strong security measures is that quite likely neither computer viruses nor Trojan horses that are unintentionally downloaded when the card is already in use will be able to impair the functions or security of any applications.

Attack and defense: exhaustive key searches

One possible type of attack at the cryptographic level is an exhaustive search for a key. For this, the attacker needs a plaintext–ciphertext pair (or better yet, several pairs) and naturally the cryptographic algorithm that is used. He or she then encrypts the given plaintext with all possible keys in turn, until the given ciphertext is obtained. This key can then be tested with all other plaintext–ciphertext pairs on hand. If the correct encryption can be carried out in each case, then the key that has been identified is very likely the correct key. This procedure is basically suitable for all encryption algorithms, although it is not always the fastest method for determining the value of the secret key.

As early as 1993, Michael Wiener published plans for a special computer that was supposed to cost one million dollars and that could try out all DSS keys for a given plaintext–ciphertext pair within seven hours [Wiener 93]. This would make it possible to determine the value of a 56-bit DES key in 3.5 hours on average. A few years later, in 1997, the DES key for a plaintext–ciphertext pair made available by RSA Inc was determined in 97 days by systematic searching, using something more than 70,000 computers connected via the Internet [RSA 97]. The search rate during the final phase of this experiment amounted to around 0.7 percent of the DES key space every 24 hours.

Several different approaches are taken in practice to counter these attacks. The simplest measure, as is generally known, is to make the key space of the cryptographic algorithm so large that it is not possible to perform a systematic search within an acceptable length of time, even with very high computing power. This is why the DES algorithm is being replaced by the triple DES in more and more applications. The key space of the DES, when compared with currently available computing power, has simply become too small.

Another defense mechanism can be created very easily by constructing the application protocol such that pairs of plaintext and ciphertext do not occur. In most cases involving Smart Card applications, the data is not even encrypted, but simply provided with a MAC. Since the contents of multiple plaintext blocks are not reflected in the MAC in a straightforward manner, a brute force attack with a MAC is a great deal more arduous than the same type of attack on a plaintext–ciphertext pair.

If a random number is placed ahead of the plaintext in the Smart Card (*salted*) before the transferred data are either encrypted or used to calculate a MAC, the data to be encrypted are different every time the function is used. This means that the results are also different each time. This also makes it more difficult to perform an exhaustive search, since in many cases the random number does not have to be public. It could for example be

Smart Card Handbook

Second Edition

W Rankl & W Effing,

Giesecke & Devrient GmbH, Munich, Germany

Translated by Kenneth Cox, Wassenaar,
The Netherlands

First edition translated by Chanterelle Translations,
London, UK

Established as the definitive guide to every aspect of smart card technology, the second edition of the *Smart Card Handbook* is fully revised to incorporate the latest industry developments.

"Indispensable! an invaluable reference to all facets of smart card technology from system architecture to security methods and from manufacturing to testing and quality control."

Hans H. Huber, Editor-in-Chief,
Card-Forum and Card Forum International

"....simple enough for beginners, comprehensive enough for developers...it is THE technical smart card handbook against which all others will be measured."

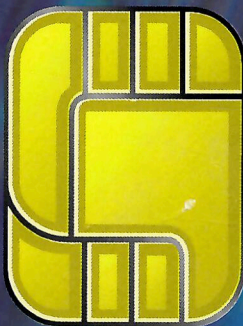
Chris Hills, Hitex, UK

Computer and electronics engineers in security system development, microchip designers and professionals working with smart card products will welcome this timely update of a classic reference.

Featuring:

- Vastly updated coverage of applications design including digital signatures and the new Microsoft PC smart card application interface, *PC/SC*.
- The architecture and development of smart card operating systems, including Java Card.
- New sections on the manufacture and design of smart card components, contactless technology and data encryption techniques, including hacker defence mechanisms.
- Examination of the use of smart cards in e-commerce, the electronic purse, credit and debit cards.
- Comprehensive listing of European and International standards for smart card construction.
- Enlarged Glossary of smart card terms, also available online in HTML and PDF.

Visit the Smart Card Handbook online at www.wiley.co.uk/commstech/



JOHN WILEY & SONS, LTD Chichester · New York · Weinheim · Brisbane · Singapore · Toronto

Exhibit 1017

Page 102 of 102