A Method of Software Protection Based on the Use of Smart Cards and Cryptographic Techniques

by

Ingrid Schaumueller-Bichl
VOEST ALPINE AG
P.O. Box 2
A-4010 Linz/Austria

Ernst Piller
HONEYWELL BULL AG
Linke Wienzeile 236
A-1150 Vienna/Austria

Abstract

The paper presents a software protection system that prevents "software piracy" reliably while allowing to produce an unlimited number of program copies.

Based on a combination of smart card technology and cryptographic techniques the system provides not only a high level of security, but also enhanced ease-of-use for the software manufacturer as well as for the user.

T. Beth, N. Cot, and I. Ingemarsson (Eds.): Advances in Cryptology - EUROCRYPT '84, LNCS 209, pp. 446-454, 1985.

I) Introduction

According to estimates made in 1983 software manufacturers loose at least 50% of their turnover due to "illegal copying" or - to be more accurate - to "unauthorized execution" of programs. The problem is especially serious in the field of mini- and microcomputers and is growing steadily.

Presently the way to compensate the losses caused by software piracy is to raise software prices accordingly. Thus there is an urgent need for software protection systems from the manufacturers as well as the users point of view.

In particular there are two up-to-date methods that seem specially suited to solve problems like these - smart card technology and cryptographic techniques.

Smart cards, plastic cards equipped with a microprocessor to execute special security algorithms and a protected memory to store even highly confidential data, present a mean to realize security systems of various kinds, that are not only highly secure, but also provide a plain and clear user interface. So it is possible for the first time to make high level security systems available in everyday life, thus meeting the strongly rising security demands the new technologies bring with them.

The software protection system described below is based on CP8-cards - smart cards developed by BULL France - and card readers.

The cards are used in their standard form and linked with the system via special software, the card reader is connected to the computer via a V.24-interface (RS 232).

The cryptographic techniques used for protection comprise standard methods provided by CP8-cards as well as specially developed algorithms. Encipherment and decipherment of data is accomplished by the algorithm "C80".

II) Design Criteria / Requirements

The central goal of a software protection system is to protect software against "piracy".

A detailed analysis of the problem shows that this does not necessarily mean to prevent the production of program copies, but rather their illegal use.

So the first and central goal of a software protection system has to be:

to prevent unauthorized execution of programs.

Copying is allowed unlimitedly.

In addition to the security demands, an up-to-date software protection system has to fulfill strong requirements with regard to its ease-of-use, applicability and flexibility.

The software manufacturer needs a system that is

- of reasonably low cost, relative to the losses caused by software piracy
- independent of storage media
- applicable independently of the computer manufacturer

For the software user the most attractive feature of the system is that protected software can be sold at a greatly reduced price.

In order to raise acceptance levels, two additional criteria have been demanded for the software protection system presented below:

- greater ease-of-use of the protected software
- additional protection of user software and data against unauthorized access

III) The Method of Protection

Basic Idea

The software to be protected is connected with a proper, specially issued smart card, so that the execution of programs is possible if and only if the card is inserted in the card reader.

As it is impossible to copy smart cards, the software can only be executed by users who legally bought a licence and got a card then.

Copying of programs can be performed unrestrictedly.

If wanted, several different programs can be associated with a single smart card.

Protection Mechanisms

The connection between the software to be protected and the proper smart card is established in three different ways:

1) Repeated inquiries if the card is inserted in the card reader:

At certain stages the protected software calls the "TELEPASS function" that is inherently integrated in every CP8-card. Certain data, in our case pseudo random numbers, are transmitted to the card, where they are enciphered by a certain algorithm under a secret key that is stored in the card, and retransmitted.

The calling program enciphers the PRN too and compares the results. If they are equal the authenticity of the card can be taken for granted.

The use of a new PRN whenever the TELEPASS function is called ensures that the transfer of data between smart card and card reader is unpredictable and irreproducable.

So an "active" wiretaper can not break the system by intercepting data, storing them and recording them later.

2) Storing selected enciphered program data on the card.

The following rules are to be observed:

- Only those data may be stored that will certainly never be changed in subsequent program releases. Else for every new program version new cards would have to be distributed.

- Among others, initial values of variables and data, that are needed at highly important program stages, are well suited for storage in the card.

- The data are stored and transmitted in enciphered form. Transmission of data between card and program is again protected by the use of encryption and pseudo random numbers. Deciphering is done either immediately or a while before the data are needed.

3) Enciphering highly valuable programs, storing them on the card and executing them in the card reader / card:

Parts of the software to be protected, that are of particularly high value or central importance, are enciphered and stored in the card.
Together with that card the card reader forms an external computer that in the present version executes the programs.

As soon as freely programmable smart cards are available, the execution can be performed by the card.

The communication between the calling program and the external computer is again protected by cryptographic methods and the use of pseudo random numbers.

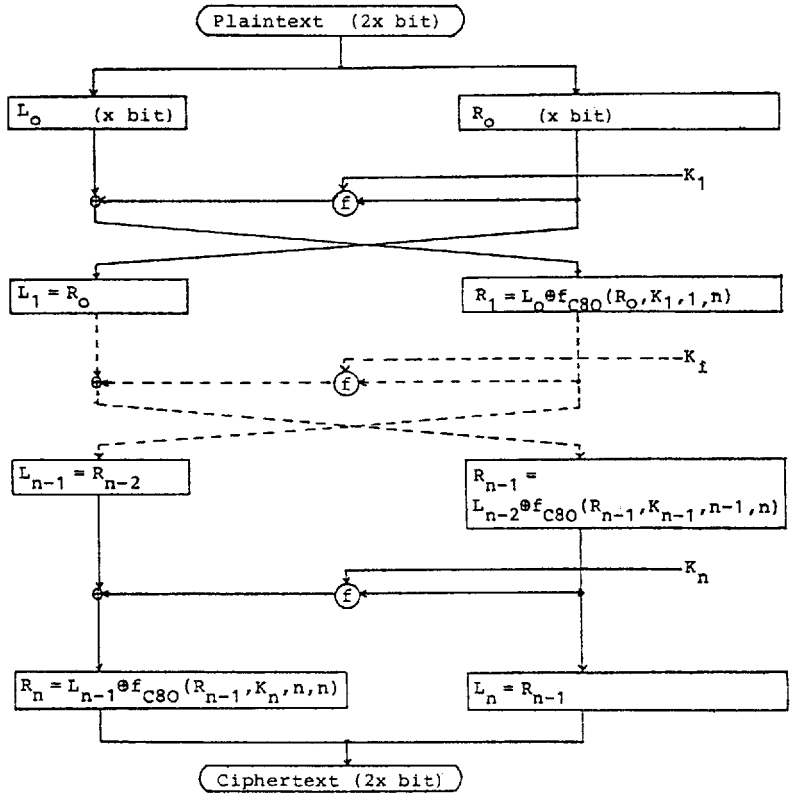
The Cryptographic Background

At the heart of the cryptographic algorithms applied in the software protection system is the cipher algorithm C80.

It is used

- to encipher and decipher the program data stored in the card
- to protect the communication between the card, the card reader and the calling programs against passive and active wiretapping
- to encipher and decipher the programs stored in the card
- to produce pseudo random numbers

C80 is a block cipher algorithm that is similar to the DES in its basic structure. The left and the right halves of a text are interchanged repeatedly and one half is XOR-ed with a binary vector depending on the text and the key. A sketch of the algorithm is given in the following:



In contrast to the DES C80 does not use S-boxes, permutations or any other tables of fixed sizes.
For this reason it is highly flexible - it employes variable numbers of rounds, variable block- and key-lengths - and can be well adapted to the special problems.

A detailed description of C80 and a security analysis are given in "Zur Analyse des DES und Synthese verwandter Chiffriersysteme", Thesis, I. Schaumueller-Bichl, Linz/Austria, May 1981.

For the software protection system the freely selectable parameters for the C80 were chosen to decrease computation time and still provide a degree of security that is essentially higher than that of the DES.

As the C80 has approximately the same good error propagation and statistical properties as the DES, it can be used also for the generation of pseudo random numbers.

In a very complex way it generates the 48-bit-numbers needed by the TELEPASS-function.

IV) System Properties

The software protection system we described above meets the requirements and design criteria stated in chapter 2:

- It prevents the unauthorized execution of software:
  Like all practical solutions our system does not provide absolute and unconditional security. But the degree of security was chosen so high that it is considerably easier and cheaper to buy a licence or even to write an equivalent program than to copy protected software.

- It can be applied by software manufacturers without support of hardware manufacturers:
  The method is realized in software, the hardware components required (cards and card readers) can be easily connected with the computer.

- It is independent of specific CPU's:
  The system does not make use of special CPU numbers or similar. Thus protected software can be executed on each suitable computer. This is of special importance in the case of hardware troubles, when a computer is to be replaced.

- It is independent of storage media:
  As the system does not physically prevent copying but execution of programs the software can be protected no matter where and how it is stored.

- Copies can be produced without restrictions:
  The user of a protected program can make as many copies as he wants and use any of them for further work without having to perform additional procedures.

The protection system also provides special advantages for the user as side effects of the methods applied:

- As for the execution of a protected program the smart card is absolutely needed, the system provides additionally some protection of software against unauthorized access. This is of special importance in the case of multiuser systems and computer networks.
  It is possible to additionally provide the system with a Personal Identification Number (PIN) known only by the user and thus making it a real access control system.

- Enhanced ease-of-use:
  A part of the memory implemented in the smart card can be used to store several commands that usually have to be typed by the user. By releasing the user from these routine functions the ease-of-use and consequently the rate of acceptance of a program can be raised considerably.

V) Fields of Application

The software protection system can be used in a variety of cases:

- Protection against multiple use of a single licence:

  Guarantees the observance of software licence contracts

- Protection of software during and after testinstallations:

  If programs are protected in the way described above, the proper card can be returned to the software manufacturer or be destroyed automatically after the end of the testinstallation. From that point on the software cannot be executed by the user.

- Protection of software during transport:

  As the software cannot be executed as long as the proper card is unavailable programs can be sent to a customer e.g. by ordinary mail without any further protection. This is especially valuable for the distribution of new program releases.

Prospects of Application

As stated above the presented software protection system shows several strong points compared to other systems concerning

- security
- universal applicability
- flexibility
- ease of use

Undoubtedly it also shares the weak points inherent to every software protection system, caused by the additionally necessary hard- and software.

For the software manufacturer these disadvantages - having to implement and maintain additional components - are fully compensated by the protection the system provides for his software and consequently by the increase of his turnovers.

For some software user protected software might be unattractive at the first glance as there is no more chance to produce resp. execute unauthorized copies for himself or others. But on the other hand protected software can be sold at a considerably reduced price, a feature that is for the benefit of all users.
The possibilities to enhance the ease-of-use as well as the security against unauthorized access are another crucial reason for a user to buy software protected by the described system.

There is one point left for discussion: the price of the protection system and its relation to the software prices.

The application of the method presupposes the availability of a card reader at every PC resp. terminal.
As smart card technology is very new and card readers are scarcely spread, the card readers usually have to be an integrated component of the protection system.

The full costs of this system - including protection software, card and card reader - have to be taken over by the software manufacturer, the free card reader being another motivation for the software purchaser.

For this reason the system should presently be applied mainly for high-value software.
The threshold for profitableness is in the average at a price of 3000 to 5.000 US$ for the software to be protected, depending on the expected rate of unauthorized to authorized copies.

For the future it is to be expected that card readers - as external devices or integrated in terminals - will be a common device of mini- and microcomputers as floppy disk drives or printers are today. In this case the hardware costs comprise merely the costs for smart cards (estimated less than 5 US$ for mass production), so the protection system can well be applied also for the protection of cheap standard software like textprocessing systems.

In order to be able to apply the system already now for low cost, widely sold software, two ways of proceeding can be conceived:

- construction of card readers dedicated to the specific problem and thus available at a lower price
- an agreement between software companies to share the costs for a card reader, that can be used for different programs of different companies

Summary

The protection system presented secures that software can only be executed in combination with a specially issued, uncopyable smart card. It is realized by software and standard hardware (CP8-cards and card readers).

Its high level of security, flexibility and ease-of-use makes it interesting for manufactures of software as well as for users.