THE SMART DISKETTE

A UNIVERSAL USER TOKEN AND PERSONAL CRYPTO-ENGINE

- Paul Barrett and Raymund Eisele -

1. Security and Personal Computers

It is becoming increasingly common for large, distributed systems to utilise personal computers (PC's) for the purpose of user access, and hence the security arrangements for such an access point have become a focus of attention in systems security design. Generally speaking the functional requirements of a PC security sub-system are as follows:-

(i) Identity verification of the user, for controlling access both to resources within the local PC workstation and to remote teleprocessing services on other machines.

(ii) File encryption at the PC for secure storage.

(iii) Message encryption and message authentication for secure communications.

(iv) Digital signatures for proof of origin of communications and for data and software certification.

2. A Token-based Solution

In general the solution to this set of requirements must include a user token of some description [1] to provide a method for verifying the personal identity of the user. For identity verification the user must be in possession of the token and be able to supply the password which is verified on the token. There are several good examples of how this has been achieved on stand-alone tokens [2] [3]. To prevent "Trojan Horse" software on the PC from capturing passwords, the token should have its own keypad and display for direct password entry.

G. Brassard (Ed.): Advances in Cryptology - CRYPTO '89, LNCS 435, pp. 74-79, 1990.

Once the token has authenticated its user it may then act as the agent of that user, performing encryption, decryption and key management as required to achieve file security, message security and digital signatures [4]. In this case it therefore needs a machine-readable interface with the PC, preferably one which is widely available as a standard feature without the addition of expensive, extra equipment.

The ideal token must also be user-friendly, highly reliable, portable and secure, as well as being a low-cost component that can easily be supplied to each user on a personal basis. This implies a small size, a method for self-powering, programmability for multiple applications, fast RSA [5] [6] processing to implement digital signatures and crypto-key management, tamper-resistance [7] to protect stored cryptographic keys and high-performance in its data-transfer and processing to provide acceptable response times.

These requirements are to some extent met by the "super smart card" [8], i.e. a smart card with an added keypad and display; although the size restrictions imposed by copying the form of the ISO standard magnetic card cause problems with processing power, reliability and user friendliness. The "intelligent token" developed by the National Physical Laboratory (NPL) in the UK comes closer to meeting the ideal specification but falls short in two critical areas, namely connectivity and data throughput.

In fact, with all tokens currently available there exist serious deficiences in respect of a low-cost, universally available, machine-readable interface, and in respect of a self-powered device with the sort of processing power that can deliver a 512-bit RSA decryption in less than one second. If the solution does not at present exist among the multitude of smart cards available on the market, what might it look like? The answer is - a SMART DISKETTE!

3. The Smart Diskette Solution

Consider the following:-

(i) The smart diskette is identical in size to the industry standard 3.5 inch diskette. Hence it plugs directly into all PC's that have a diskette drive of that size.

(ii) It isn't really a diskette at all, but a solid state device with a set of coils and magnets which emulate the magnetic field of a rotating diskette. Hence the reading and writing of data is carried out by the PC exactly as if it were a normal diskette.

(iii) The smart diskette is physically large enough to embed a considerable number of powerful IC's, thus overcoming the memory and processing restrictions imposed by conventional smart card packages. Also there is plenty of space for a usable key-pad and display. Furthermore, reliability issues are considerably easier to resolve within a diskette sized package than with a smart card sized one.

(iv) As well as fulfilling the role of an identity verification token which can be carried in a shirt pocket, the smart diskette is powerful enough to provide all of the encryption functions normally put into a PC on an add-on circuit board, including the provision of high-performance RSA public key cryptography.

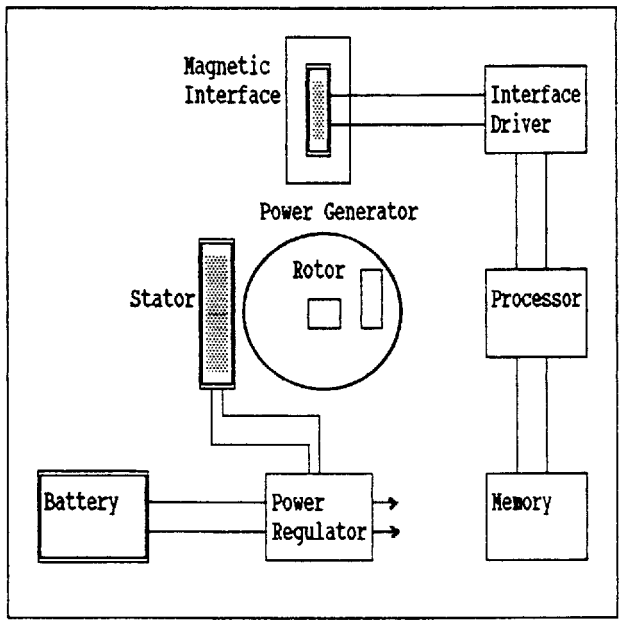
(v) Self-powering is a combination of back-up batteries and an on-board generator driven by the disk-drive rotor. Furthermore the size of the unit allows for the power dissipation required with present-day technologies to support the performance of this device.

(vi) Any PC with a 3.5 inch drive can be "secured" by plugging in an appropriate version of the smart

diskette. Since software can be loaded through the diskette drive for execution on the PC, full control over the PC can be taken by the smart diskette. It has an enormous potential for those who wish to distribute software which is truly copy-protected.

4. Implementing the Smart Diskette

The diagram below shows the schematic block diagram for the circuitry of the smart diskette:



SMART DISKETTE
Functional Schematic

At first sight it may seem that the main area of difficulty in the development of a smart diskette device would be the magnetic interface since most of the other components exist already at least in a form similar to that required. (For example, the processor, memory and other logic components could be produced using standard silicon with hybrid or VLSI manufacturing techniques). However, even the magnetic

interface is nothing more complicated than a disk-drive read/write head albeit in a different shaped and sized form. Likewise, the logic to drive the interface will be very similar, if not identical, to that found in a standard disc-drive controller chip.

On reflection, we may conclude that the biggest challenge facing the implementors of the diskette is the design and development of a device which is suitable for high-volume, low-cost, mass production to meet a quality standard which ensures maximum reliability.

In emphasising the hardware aspects of the device, one is not overlooking the software development requirements. Considerable effort will need to go into the design of a general purpose operating system which includes the basic security functionality. However, with the high level of performance available from the hardware, the software should not present as demanding a challenge as that presented by the present alternative of smart-card, reader and/or PC-crypto-board combination.

5. Conclusions

The original smart card concept was an extension of the ISO mag-stripe banking card; the size was an important consideration when integrating the new device into an existing network of card-readers on cash-machines and point-of-sale terminals and, more importantly, into consumers' wallets. Once we consider a token that is for wide applicability in an existing population of PC's, it is sensible to reconsider the issues of compatibility and integration. Putting smart cards onto PCs is an expensive and awkward business, which fails to give the level of performance that is really needed. The logical solution is the one which we have shown meets a very broad spectrum of requirements - the smart diskette.

References:

[1] Sherwood J. R. and Gallo V. A., "The application of smart cards for RSA digital signatures in a network comprising both interactive and store-and-forward facilities", Proc. of Crypto 88, Springer-Verlag, 1988.

[2] Wong R., Berson T. and Feiertag R., "Polonius: An identity authentication system", Proc. of IEEE symposium on secrecy and privacy, 1985.

[3] Eisele R., "Host access security", presented at Interact 86, Orlando, Florida, 1986.

[4] Sherwood J. R., "Digital signature schemes using smart cards", Proc. of Smart Card 88, London, 1988.

[5] Rivest R., Shamir A. and Adleman L., "A method of obtaining digital signatures and public key cryptosystems", Comm. of ACM, Vol 21, No.2 Feb 1978.

[6] Barrett P. D., "Implementing the RSA public key encryption scheme on a digital signal processor", Proc. of Crypto 86, Springer-Verlag, 1986.

[7] Clark A. J., "Physical protection of cryptographic devices", Eurocrypt 87, Amsterdam, 1987.

[8] Chorley, G.J., & Price W.L. "An intelligent token for secure transactions", Pro IFIP/Sec '86, Monte Carlo December 1986 pp 442-450.