AUTHENTICATION AND SIGNATURES IN COMMERCE AND BANKING

D.W. Davies

Rapporteurs: D.H. Mundy
R.J. Stroud

Abstract:

Authentication

Authentication of a message has two aspects: preserving the integrity of the message content during transmission and verifying the origin of the message. The 'origin' may refer to the organisation from which it came, the terminal, the identity of the person who originated it or simply that that person was authorised to send such a message.

Integrity and origin must be related and one is worthless without the other. A message from an intruder that has not been altered in transit is no more to be trusted than a message from the true originator which could have been altered by a crook.

Established techniques for authentication employ a secret key known to the sender and receiver of the message and a number calculated from the whole of the message using the secret key. This number is called an authenticator with the alternative names "message authentication code" or MAC or, in some banking applications "test key". The properties required of an authenticator function were described. Many authenticator functions are available for practical use, some are on the point of becoming international standards at ISO.

Authentication is widely used in banking and examples were given from the international SWIFT network and the British CHAPS system.

The problem of disputes

Authentication, which uses a secret key known to sender and receiver, protects them against third parties interfering with their messages or falsifying the message origin. It does not protect the sender and receiver against each other's misdeeds. Thus, the forgery of the message by the receiver or an assertion by the sender that it was forged by the receiver can result in disputes which cannot be solved by any objective evidence. This difficulty is overcome in the "digital signature" which is formed by public key cryptographic methods using a secret key for generating the signature at the point of origin and a public key for verifying it at the receiving point. The principal of the digital signature was described, together with the characteristics which are needed for its safe operation. With the aid of the public key, any number of people can verify their

signature whereas authentication, since it depends on a secret key, would be weakened, if large numbers of people were involved. With digital signatures, everything depends on the authenticity of the public key and this can be related, by means of certificates with digital signatures, to one authentic public key, the key of a key registry.

The RSA public key cypher and signature

The number of proposals that have been made since public key cryptography and digital signature were first suggested, the cyper and signature devised by Rivest, Shamir and Adleman (the RSA system) has been most generally accepted and remains secure, given the difficulty of the factorisation problem. The principal of the RSA system was described. Its practical application depends on fast implementation of a modular expotential calculation with a large modulus, for example 512 bits. To give an idea of the problem, the exponential can be calculated in the BBC Micro in four and a half minutes or, using the Texas Instruments TMS 320 signal processor, in ten seconds. (More recent information indicates that three seconds may be possible with the TMS 320.) Special chips are being designed for exponential, with times less than one second and at least one development at Sandia Corporation indicated the possibility of moderate communications speed with RSA encryption. For signature purposes, however, the calculation in less than one second will be satisfactory.

A number of alternative public key encryption and signature methods have been devised. One developed by C.P. Schnorr in conjuction with Ong and Shamir (the OSS signature) uses only a few multiplications and divisions but in its earlier forms was broken by John Pollard. Since Pollard used the Euclidean Algorithm for his method, Schnorr proposes to make it secure by using algebraic numbers. Unfortunately this increases the size of the signature to four numbers of whatever size the modulus determines. When RSA chips of reasonable speed are available it seems likely that the RSA signature will become adopted.

Digital Signatures in Banking

Because of the properties of digital signatures in enabling disputes to be resolved, contracts can be entered into using digital messages in such a way that their validity could be tested in front of a third party, such as a judge. In particular, payments can be made by a digital cheque, and the form of such a cheque was described, together with a hierarchical mechanism for verifying the signature using only the public key of a central bank. With the aid of the digital cheque, payments systems can be devised for many types of electronic funds transfer which are being developed in banking.

The use of smart cards as developed in France employs, at the present time, an authenticator based on a key contained in the card and known to the card issuer. This has enabled an off line point of sale payment system to be operated, subject to a number of the risks which are inherent to off line systems but enabling the issuing bank to verify that a good card was used and that the correct password or

PIN was entered at the time of use. Unfortunately, there are a number of fraud mechanisms possible for the French system and these can be overcome by employment of a digital signature. In order to avoid some of the shopkeeper fraud mechanisms which remain, it seems desirable to include on a card a keyboard for entering the PIN and a display for showing the payment being made (and other purposes). The technology for this development exists with the possible exception of the RSA signature function. Physical security of the secret data on the chip in the card is another unknown, at present. The resulting device can be called a "signature token" and need not, in the long run, be compatible with the thin plastic card. It is technically possible for a single token to function for a number of accounts held with different organisations so that one token replaces a large number of plastic cards.

Negotiable Documents

Writing on paper has three characteristics which we would like to imitate in electronic systems. The first of these is the handling of information, which is more efficiently stored and transmitted electronically. The second of these is entering into contractual agreement which can now be achieved with digital signatures. The third characteristic of paper is more difficult to obtain since it gives the paper document itself a value as a "negotiable document". Essentially such documents must not only be signed but also be unforgeable, that is to say a copy cannot be made. Such documents in practice range from theatre tickets to valuable instruments such as negotiable bonds and bills of lading.

If a signature token is technically possible and if this device is unforgeable then a mechanism exists for generating a negotiable document. A token might be made unforgeable by the difficulty of opening it and reading its secret contents rather than by the difficulty of manufacturing a copy.

The mechanism for generating a negotiable document in this way was described. The information content and its signature can be carried and stored in any way and the text of the document contains a statement that it is owned by whoever possesses a signature token relating to a stated public key. In this way the signature token becomes the symbol of ownership. An interesting bonus is that the value of the token can be locked up by means of a password. This reduces the need to protect the negotiable part of the document in a strong safe.

The need for negotiable documents may in the future be reduced by on-line registry of ownership, so that there is a possibility for their electronic realisation.

DISCUSSION

(The following took place during Mr. Davies' presentation)

During his discussion on Ong, Schnorr and Shamir's digital signature, Mr. Davies explained that Pollard had been able to break both the original quadratic algorithm, and a refinement which was cubic, using Euclidean techniques. In an attempt to prevent such attacks the algorithm was now expressed in terms of algebraic numbers of the form 'a + b$\sqrt{x}$' which made it essentially quartic. So far this form had not been broken.

Professor Churchhouse pointed out that in order to prevent Euclidean attacks on this form of the algorithm the radix 'x' must be chosen carefully. For example, -5 was a good choice since 6 could be expressed in two ways as such an algebraic number, namely

$$6 = 2 * 3 = (1 + i\sqrt{5}) * (1 - i\sqrt{5})$$

and this ambiguity would thwart such an attack.

(Report of the discussion session)

Dr. Andrews remarked that a conventional handwritten signature is mechanical and therefore difficult to forge. In addition it is unlikely that anyone would forget their own signature. On the other hand, a Personal Identification Number (PIN) is easily copied and easily forgotten.

Mr. Davies agreed at present PIN's are only a partial solution although the banks seem quite satisfied with them. It is technically feasible to put a dynamic signature recognition mechanism on the card. However, although the techniques are well understood, at present the error rate is too high. Some of the banks using PIN's in Automated Teller Machines (ATM) have expressed an interest in signature recognition because it should give a reduction in the number of fraudulent claims from customers alleging malfunctioning of the ATM's. Of course, there are better recognition methods, such as the pattern of blood vessels on the retina. However these methods are too good and therefore too difficult to implement practically. It is likely that PIN's will be around for a long time to come!

Professor Randell stated that it is often suggested that the fraudulent use of cheque cards could be prevented by attaching a photograph of the card holder to the card itself. However Charles Read tells of an experiment in the central London area which showed that this does not work. A number of people were sent out with such cheque cards, each bearing an identical picture of the same gorilla! On average each card was used successfully twelve times.

Mr Davies stated that Shopkeepers are not primarily interested in safeguarding the customers' interests; they just want to get their money! Any system which relies on the shopkeepers for its enforcement is bound to fail. To counter the shopkeeper faud by means of a false terminal, one method would be for the card to reply with the holder's name when presented for a transaction, although something known only to the card holder, and thus less obvious, could be used.

Professor Randell suggested that a system of '20 questions could be used.

Mr. Davies replied that they had tried this as an experiment, but that it is very difficult for people to come up with 20 questions which identify themselves uniquely and yet which avoid stereotypes. Choosing questions involves too much creative thought. They tend to dismiss the silly questions, yet these are the most secure.

Professor Beth suggested questions like 'What is your mother's maiden name?' or 'What is your last girl-friend's name?'

Professor Randell remarked that the first is a stereotype; the second may change in time!

Mr. Voysey suggested that a Prestel service giving mothers' maiden names would be very popular.

(General laughter and suggestions such as 'Grandmother's maiden name')

Professor Beth asked Mr. Davies to expand on the distinction between on-line and off-line systems? The banks are interested in off-line systems, but British Telecom wants on-line systems. What is the state-of-the-art?

Mr. Davies replied that an off-line system requires a verification key inside the device itself. This is all right for an ATM which is physically secure, but is not practical for a Point of Sale terminal. There will be too many terminals around, and sooner or later a gang of crooks will steal one and break in, thereby compromising the entire system.

The French system has the customer's own key on the card itself which partly overcomes this particular problem. However, with an off-line system it is not possible to tell whether the card has been stolen or whether it is in credit. Thus, although the bank will save on communication costs, they are undoubtedly running a risk. A compromise would be a semi-online system where the bank periodically down-line loaded a black-list into the POS terminal.

The communication costs are becoming cheaper especially for large organisations such as supermarkets which can multiplex their transactions. However there is still a significant cost for the small corner shop.