Information integrity protection and authentication in a banking environment

Bart Preneel\textsuperscript{1}, René Govaerts and Joos Vandewalle

Katholieke Universiteit Leuven, Laboratorium ESAT
Kardinaal Mercierlaan, 94, B–3030 Heverlee, Belgium

Abstract

Cryptographic techniques for integrity protection and authentication in a banking environment are discussed. A first solution is to add controlled redundancy with or without encryption. A more secure alternative, the digital signature is explained and compared to the other techniques. As an example, TRASEC, the Belgian standard security system for electronic funds transfer is treated. Finally we present our conclusions.

1 Introduction

In former days, the protection of information and transactions in the banking environment was mainly an issue of physical security and selection and motivation of people. To keep information confidential, it was carefully locked in a vault and the discretion of the personnel prevented data from being disclosed. The protection of authenticity relied exclusively on the impossibility of forging certain documents (as is now still the case for e.g. banknotes) and of manual signatures. The identification of people relied on eye-to-eye contact and transfer of information and of securities was done by a courier.

The first evolution was the processing of information stored on punch cards or tapes with digital computers. The processing capabilities of the computers increased and large amounts of data are now stored on magnetic or optical carriers. Transfer of information and financial transfers are realised through both local and worldwide telecommunication networks. Think of the S.W.I.F.T. banking network that has over 3000 nodes in 71 countries all over the world [VAus89].

As a consequence of these evolutions new threats emerge. Obtaining confidential information e.g. the status of accounts is still possible with the aid of dishonest employers, but an alternative is to eavesdrop communication lines or to enter the bank computer and to browse through available data. Active attacks are even more dangerous: information in

\textsuperscript{1}NFWO aspirant navorser, sponsored by the National Fund for Scientific Research (Belgium).

transfer on a communication line or stored in computers could be modified or deleted without leaving any trace. Computers are vulnerable to more specific threats [VG88]: computer viruses, Trojan Horses, worms, and logic bombs can cause considerable damage. Apart from outsiders, breaking into the computer systems, the people operating the computer also can be malicious. Copying or changing electronic data is much easier for them than modifying data stored on paper.

A special problem is disputes between sender and receiver. Suppose someone gives instructions to a stockbroker. If some days later the transaction turns out badly, the sender could deny his order. On the other hand the receiver of a customer order could increase the ordered volume. From these simple examples it is clear that for some applications an electronic equivalent of an ordinary signature is necessary.

The objective of this paper is not to enumerate all threats but to discuss solutions. A very important observation is that cryptographic techniques are essential for obtaining information security in individual computer systems and in computer networks. Of course, other aspects e.g. management and selection of personnel are also very important. We can use here the old cliché saying that a chain is as strong as its weakest link. Moreover existing solutions will never be 100% sufficient and therefore audit trails and arbitration procedures are necessary.

Protection of confidentiality will not be treated, but we draw the attention of the reader to a blockcipher that is widely used in the financial world. It was designed by IBM in the early seventies and became in 1977 widely known as the Data Encryption Standard (DES) [Fips46]. It was also standardized within ANSI as ANSI X3.92-1981 [ANSI81] and was approved by US government (NBS) in 1987 for another five years for financial applications [SmBr88]. In the rest of this paper cryptographic techniques for information authentication and for digital signatures will be treated. Finally a practical example, TRASEC [Vanb87], the Belgian standard security system for electronic funds transfer will be described and our conclusions will be presented.

We conclude our introduction with a short note on the terminology: in cryptographic literature and in the standards developed within the ISO Technical Comittee 68 on Banking Procedures, the term message authentication is commonly used. It corresponds in CCITT/ISO terminology for Open Systems Interconnection (OSI) [ISO88b, MWR89] to protection of both content integrity and message origin authentication. Of course, it makes no sense to protect the integrity if nothing is known about the origin of a message. A digital signature scheme is being standardized in [ISO90]. The service corresponding to this mechanism is called non-repudiation of origin.

2 Information authentication

For a long time, there was a wide misunderstanding that encrypted data was also protected against modifications or active attacks. Two objections can be made against this. At first, the security level against active attacks is totally dependent on the way the enciphering algorithm is used (e.g. the mode of use of a blockcipher [Fips81]) and on the internal
redundancy of the information. If the information consists of natural language and is verified by a person, active attacks are difficult. However, if one of those conditions is not met, e.g. if numerical data are encrypted, the information is vulnerable to an active attack. A second objection is that it might be necessary that information is readable to everyone, but nevertheless it has to be protected against active attacks.

The best definition, in our opinion, of information authentication was given by G. Simmons [Sim88]: “information authentication is concerned with establishing the integrity of information purely on the basis of the internal structure of the information itself, irrespective of the source of that information”. To protect the integrity of information, controlled redundancy has to be added to the information. The message will be extended with a special field of fixed length. This field is a complex function of the information that has to be protected. If the evaluation of the function depends on a secret key, the special field is called a “Message Authentication Code” (MAC). If no secret quantity is involved in the computation of the special field, it is called a “Manipulation Detection Code” (MDC).

It is important to note that information authentication can not be provided ‘out of the blue’. One has to rely on the secrecy or integrity of something else. Compare this to encryption, where the secrecy of large data amounts depends on the secrecy of a small key. In a similar way, the secret key involved in the computation of a MAC can protect the integrity of the data. In case of an MDC, where no secret quantity comes into play, two options exist: encrypt subsequently the MDC and the information or protect the integrity of the MDC. In a computer, this can be done by printing it on paper and storing it in a vault while in a telecommunication environment an integrity channel has to be established. This could be a telephone line when the two people know each other’s voice.

For technical requirements to be imposed on a MAC or an MDC, we refer the reader to [PGV89]. To obtain a sufficient security level against exhaustive and random attacks, the key, the MAC and the MDC may not be too short (64-128 bits dependent on the application).

We will briefly compare the two approaches. In case of a MAC the protection of the authenticity is independent of the protection of the secrecy in the sense that:

- protection of the authenticity without confidentiality is possible.
- even when the encryption scheme is broken, the authenticity of the information can still be verified.

The disadvantage is the complexity of the key management (two independent keys are necessary) in case of additional confidentiality protection.

The advantages of an MDC are:

- The computation requires only publicly known quantities. This results in a simplified key management.
- The separation of the function of authentication from encryption. This implies that the authentication is independent of the encryption algorithm or the mode of operation. In the context of the ISO Open System Interconnect Reference Model integrity and confidentiality can be protected at different layers.

The disadvantage of this approach is that in case of a compromise of the security of the encryption algorithm, the integrity protection is also jeopardized.

The ISO technical committee 68 on Banking Procedures has produced standards on message authentication. The general requirements for message authentication for wholesale banking are described in ISO 8730 [ISO89] (based on ANSI X9.9). Three algorithms for computation of a MAC are described in ISO8731/1 and in ISO 8731/2 [ISO88], namely the CBC and CFB mode of the DES algorithm (see figure 1) and the Message Authentication Algorithm (MAA) of D. Davies [Dav84]. This last algorithm is software oriented and has a 32-bit result, which makes it unsuitable for certain applications. The CBC mode of the DES is widely used and can be recommended if all 64 bits of the result are used and if a different key is used for data encryption. Similar standards are being developed for retail banking (DIS 9807, corresponding to ANSI X9.19). The standardization of an MDC is still under study in ISO/IEC/JTC1. A variety of schemes have been proposed and were subsequently broken [PGV89, ISO89b]. The conclusion is that one has to be very careful with new proposals.

The addition of redundancy is certainly not sufficient. Even if the information has not been changed, a replay of a financial transaction is a serious threat. Also the timeliness and the order of messages can be important. To protect against these threats, a time stamp or a serial number can be added to the information. In case of stored information, a restore can be avoided through the use of version numbers and the order of the blocks can be protected through adding the memory address to the information before the computation of the redundancy.

\[ \begin{align*}
X & \rightarrow \text{DES} \\
K & \rightarrow \text{DES} \\
Y & \rightarrow \\
\end{align*} \]

\[ \begin{align*}
X & \rightarrow + \\
64-k & \rightarrow k \\
\end{align*} \]

\[ \begin{align*}
K & \rightarrow \text{DES} \\
K & \rightarrow 64-k \\
k & \rightarrow \text{DES} \\
\end{align*} \]

\[ \begin{align*}
X & \rightarrow + \\
Y & \rightarrow \\
\end{align*} \]

Figure 1: Cipher Block Chaining (CBC) and Cipher Feedback (CFB with \( k \)-bit feedback) modes of operation of the DES.

3 Digital Signatures

As indicated in the introduction, the use of a MAC or an MDC can not solve disputes
between sender and receiver, because they share the same secret information. If one of
the parties claims that the information was changed by the other party, a judge can not
make a distinction between them, even if they disclose their common secret key. To get an
equivalent of a manual signature, an asymmetry has to exist. Hence the sender must be
able to carry out some operations that the receiver cannot perform.

The problem has been solved by W. Diffie and M.E. Hellman in the mid seventies
[DH76]. They invented the concept of trapdoor one-way functions. These functions are
easy to compute in one direction and difficult to compute in the other direction, except for
someone who knows the ‘trapdoor’ information. Information can then be digitally signed
if the sender transforms the information with his secret key (the trapdoor information).
The receiver can then verify the digital signature by applying the transformation in the
‘easy direction’. The signature is unique to the sender because he is the only one that has
the secret information.

The same trapdoor one-way functions can also be used for public-key encryption sys-
tems, where the receiver can make his key public through an integrity protected channel.
The encryption operation is then the transformation with the public key, and the decryption
the inverse transformation (using the secret key or trapdoor). Note that some digital
signature schemes based on conventional cryptosystems have been proposed. However,
they are very impractical because of the large size of signatures and keys together with the
fact that the keys can be used only once.

The first trapdoor one-way function was proposed by Rivest, Shamir and Adleman in
1977 [RSA78]. The RSA-public key cryptosystem is based on modular exponentiation and
its security relies on the difficulty of factoring big integers that are the product of two
primes. It is widely used and became a ‘de facto’ public-key algorithm standard. The only
disadvantage of the system is the performance: even with fast dedicated hardware, the
encryption speed never exceeds 50 kbit/sec (see e.g. [HVG88]). A software implementation
will be much slower (16 MHz 80386: ± 500 bit/s).

To overcome the speed problems, one can compress the information before the signing
operation to a fixed length of 128 bits. This is done with a cryptographically secure and
fast hash function. The requirements to be imposed on a hash function are similar to
those for an MDC, but are more stringent. Apart from speeding up the computation and
decreasing the size of the signature, the hash function increases the security level. From
the fact that almost all proposals have been broken, one may conclude that the design of
a both efficient and secure hash function is not a trivial task. Within ISO two schemes
are selected [ISO89b]: one based on blockcipher algorithms and one based on modular
squaring.

A recent evolution is that the concept of digital signature becomes more independent of
public-key cryptosystems. New signature schemes have been proposed making use of zero-
knowledge proofs. Moreover the concept has been extended to arbitrated signatures [DP89]
and undeniable signatures [ChVA89]. This last category are signatures that can not be

verified without the cooperation of the signer. An important technological breakthrough is the announcement of an inexpensive RSA-smart card with an 8-bit processor for the Fall of 1990 [Quis90]. This opens the possibility to compute secure and efficient digital signatures in a smart card.

In a practical system, many problems have to be addressed: what if someone has lost its secret key, or what if he claims he has lost its secret key. In both cases he will try to revoke his digital signatures. It is certainly true that some problems exist, but this is no reason to throw out the baby with the bathwater. Someone can indeed revoke his signature, but if this happens repeatedly, people will lose confidence in this person. Secondly, it is possible to store the secret key in a secure device (e.g. a smart card) such that even the owner does not know it. This makes fraudulent revocations very difficult. An important problem however are the legal aspects of digital signatures [ABEP89]. Manual signatures are also not unforgeable, but it remains an open problem whether at present a judge will accept a digital signature. Legal support of digital signatures is certainly necessary to get a wide acceptance and will be a big step forward for the automation of financial transactions.

4 TRASEC: the Belgian Security system for Electronic Funds Transfer

The TRASEC (TRAnsmission SECurity) system is a standard security system designed by the Belgian Banking community for Electronic Funds Transfer between corporate customers and all financial institutions. It became operational by the end of 1987.

The objectives of the system are:

- put forward a standard system, to avoid that the customers become dependent on one bank.
- to provide information integrity and authentication (no confidentiality protection has been provided).
- applicable to financial applications and transparent to any transfer medium and computer configuration.
- automatic, user-friendly and easy to integrate in the existing computer systems of both banks and customers.
- feasible at a reasonable cost.

The customer has two modules: the condensing module and the authentication module. The first is a specially developed hash function called the “Binary Condensing Algorithm” (BCA). It is based on a combination of permutations, translations and rolling exclusive ors. Its function is to compress the transaction file to an 8 byte result. This hash function is implemented in the computer system of the customer.

The authentication module is implemented in a smart card. The CBC mode of DES is applied to the result of the BCA concatenated with a sequence number to generate a MAC. The secret key for the MAC computation is a function of the secret card key and of a password. This means that if technology would allow for inspection of the card, the card key is not sufficient to obtain the secret key for the MAC. Every user has one smart card per financial institution he communicates with to increase the security level.

A specially designed terminal provides for communication between user and smart card. This terminal contains no critical data or procedures, hence it can be very simple and cheap. The user identifies himself to the terminal with a password. The result of the BCA is entered on the keyboard of the terminal and the MAC appears on a display. It is also possible to connect the terminal directly to a computer.

The management facility in the financial institution consists of a PC with a plugged-in security board. Access control to the PC is based on a smart card. The functions provided are the application of the BCA, the verification of a MAC and the initialization of new smart cards.

The disadvantage of this system is that it does not provide a digital signature: the management facility has access to the secret key to compute the MAC. Hence it has to be carefully protected to avoid anyone from modifying or inserting a transaction and calculating the corresponding MAC. This fact could be used by the customer to deny messages that were authenticated before. However, because the transactions are carried out between corporate customers and their banks, one can assume a certain level of trust. The advantage of the system is the use of smart cards. For the time being, information can not be read from smart cards and only password encrypting keys are stored on the card. Hence the customer can not claim that his secret key was stolen, unless he has lost his card and his password was disclosed at the same time. If smart cards with RSA operations become available at a reasonable price, the MAC could be replaced with a digital signature resulting in an increased security level.

5 Conclusions

For protecting information authentication, several cryptographic techniques are available: MAC, MDC, digital signature. For a MAC, efficient standards exist that are widely accepted. The design of MDC’s and hash functions for digital signatures is apparently more complicated, and new proposals that are both efficient and secure are still under study. The concept of digital signatures is very promising. At present, first standards on the subject are emerging and commercial applications become feasible. Smart card implementations are announced for the near future. Further theoretical developments together with legal support will make digital signatures widely accepted and used in the nineties.

References


