MESSAGE AUTHENTICATION AND DYNAMIC PASSWORDS

Professor H J Beker & Mr G.M Cole
Racal-Guardata Limited, UK

The security of transactions flowing across a communications network is of ever increasing importance. In many such circumstances it is important not only to protect the messages from passive interception but also, and often of greater importance, to be able to detect any active attack against messages. An active attack may take the form of an interceptor tampering with the message: altering it, adding information, removing information and so on. While it is almost impossible to prevent an active attack there are many mechanisms to ensure, with a high probability, that such an attack may be detected and hence rendered harmless. The techniques to allow detection and thus audit take many forms of which the most common are normally cryptographically based and depend upon the generation, before transmission of the message, of a check-sum which is then appended to the message. The theory underlying this approach works on the basis that if a would-be fraudster changes any part of the message in any way then the check-sum will no longer be correct and thus the recipient of such message can compute, for himself, the expected check-sum, compare it with that received in the message and if they disagree will know the message has been altered. If on the other hand the expected and received check-sums agree then he knows with a high probability that the message has not been altered. This probability is dependent upon the amount of information within the check-sum (i.e. the longer it is) the lower the probability of an undetected alteration.

Many such systems exist. Some of these depend only upon an algorithmic check-sum, often called a test-key or authentication parameter. In this case the security level is often relatively low since someone attacking the system with knowledge of this algorithm may be aware of ways in which he can alter the message without affecting the check-sum computation. A trivial example of this is as follows: suppose the check-sum on a numeric message is computed solely

D. Chaum and W.L. Price (Eds.): Advances in Cryptology - EUROCRYPT '87, LNCS 304, pp. 171-175, 1988.

as the modulo-10 sum of all digits in the message. An attack upon the system which simply involves altering the order of the digits in the message would not be detected by the check-sum.

A normally more secure technique involves the use of a cryptographic check-sum, often termed a message authentication code. In this case the check-sum is dependent not only upon the cryptographic algorithm, but also a cryptographic key. An example of this, in common usage, is the system described within the American National Standards Institute (ANSI) standards X9.9 and X9.19. Within these standards the cryptographic algorithm is the Data Encryption Algorithm as described in FIPS 45 and ANSI X3.92. The cryptographic key is a 56-bit DEA key. The check-sum or message authentication code (MAC) is a 32-bit value appended to the message. It is currently generally accepted that provided the cryptographic key is kept secret then any alteration to the message will be detected by the recipient with a probability of 0.9999999998.

Within some communications systems protection of messages in the above manner is considered adequate. However, there do also exist many systems within which it is important not only to detect any alterations to the message, and thus be able to provide alarms and an audit system of these, but also to identify the person or group of persons from which such a message originated. This is in some sense equivalent to requiring a signature on the message. We shall now go on to describe how, by use of another commonly used technique of dynamic passwords, such messages can be signed and thus far greater protection afforded. We begin by describing the technique of dynamic passwords as it is commonly used for access control. We shall then go on to show how the technique can be combined with a check-sum to provide a 'signature'. As we shall see the combination of the two techniques, in the manner described, will provide far greater levels of security.

Computer access control systems often depend upon a static user password. These systems are notorious for their insecurity. Recently, dynamic password systems have become more popular. There are many variations on this particular theme. By way of example we describe one such method.

Having entered his user identity, the user is presented, by the system, with a challenge. The user must then provide the correct response to this challenge in order to be granted access. The theory behind this system is that since the system has control of the challenge and the response will be unique, for that user, to that challenge, the system is running, essentially, a one-time password system. Any unauthorised person will not know how to respond to the challenge in the correct way and will thus be denied access to the system. Similarly anyone recording the challenge and response will be unable to directly use this information since ideally that challenge will never be used for that user again.

There are many techniques possible to allow the user to produce the correct response. These vary from biometric techniques to user tokens. A typical method involves a user token similar to a small calculator which can be correctly activated by the user via entry of a Personal Identification Number (PIN). Once the device has been correctly activated entry of the challenge will result in the correct response being generated by the token. This may be achieved, for instance, via a one-way function of the challenge and a cryptographic key unique to that user and embedded in his token. Thus, loss of the token does not enable an unauthorised user to enter the system since he requires the PIN to correctly activate the system. Indeed, a would-be hacker requires both the PIN and token as well as the user ID or the algorithm and cryptographic key corresponding to a user ID in order to enter the system. In the case of a token being used in this way it may well take the form of a 'smart card'. Biometric means may also be used.

We shall now give an example of how a check-sum can be combined with a dynamic password system in order to provide message and user authentication within a system.

For example we shall consider a user, issued with a dynamic password token, using a terminal which can provide a cryptographic check-sum or message authentication code (MAC). We shall also assume that the recipient of the message is in possession of the appropriate cryptographic keys to check both the MAC and 'response'.

Once the user has compiled his message the terminal will generate an appropriate MAC, or some derivative of it which is presented to the user as his 'challenge'. Once he has produced the correct response to that challenge and appended this response or a function of it to the message the message has been 'signed' by the user. On receiving the message the recipient can not only check the MAC, but may also, via the user ID, check the response to that 'MAC challenge' thus also authenticating the originator of the message.

Such a system may have considerable benefits within a scenario within which a corporation or institution is allowing users to enter messages into its computer network. Typically this might be a corporate banking network where the institution is a bank and is accepting payments, transfers, etc from its customers. This system may be set up as follows:

The institution issues to the user the cryptographic MAC facility in a tamper resistant form. This may constitute the entire terminal or a part of it. The cryptographic key upon which MAC security depends is contained within the tamper resistant enclosure. The corresponding cryptographic key may be held by the institution itself encrypted under a master key which again is contained in a highly tamper resistant enclosure. Similarly, the user is also issued with his dynamic password token itself containing a cryptographic key in a tamper resistant manner while again held by the institution encrypted under a master key. Assuming the tamper resistant enclosure containing the master key can also carry out the appropriate cryptographic functions then the institution can only be compromised while the devices are being set up or through a breach of the tamper resistant module containing the master key.

At the user level, the system can only be compromised via an attack upon both the user's cryptographic facility and his token. Bearing in mind that should he lose his token it will normally be in his interests to report this as soon as possible the system provides a high level of security.

Since this procedure is centred around the concept of using the MAC (or check-sum) as the 'challenge' to the user let us see what extra security benefits are thus achieved.

1. Since the response now depends on the MAC it depends upon those sensitive parts of the message which the MAC was itself protecting and thus is a message dependent response. It is in this way that it provides a similar facility to a signature. In particular this response cannot be removed from this message and appended to another since it will no longer be appropriate and will therefore be detected by the recipient.

2. Even if some unauthorised person were able to discover the cryptographic key associated with the MAC, by breaking into the user's terminal or otherwise, this would not be sufficient to penetrate the system since any alteration of the MAC in turn would mean the response on the message would now be inappropriate and would therefore be detected by the recipient.

3. An implication of the above remark is that theoretically the institution could give all its users the same cryptographic key for the cryptographic MAC facility and still be assured a high level of security through the response confirmation.

4. Clearly if the user's identity was incorporated into the message and the MAC calculation, then only the holder of that corresponding dynamic password token (and corresponding PIN, if used) could 'sign' the message.

We therefore see that the system now has two interrelated security mechanisms: the MAC and the response. As we stated above an attack by an unauthorised user would need to be directed either at the institution's highly tamper resistant facility or at both user's cryptographic facility and that user's token. We believe such an attack to be extremely difficult.