1979

Handshakes Are Shaky

Giovanni Maria Sacco

Dorothy E. Denning

Report Number:
79-322

HANDSHAKES ARE SHAKY[1]

Giovanni Maria Sacco
and
Dorothy E. Denning[2]

Purdue University

CSD TR 322

November 1979

Abstract

The distribution of secret communication keys in a computer network using single-key encryption is discussed. It is shown that simple handshakes cannot prevent impersonation. A solution based on time-stamps is proposed.

1. This research was supported in part by NSF Grant MCS77-04835.

2. Authors' present address: Computer Sciences Dept., Purdue Univ., W. Lafayette, IN 47907.

Introduction

Secret communication between two users on a computer network is possible using either single-key (conventional) encryption or public-key encryption [DIFF76]. With single-key encryption, the communicants share a secret communication key that is used both to encipher and decipher messages transmitted between them. With public-key encryption, each user has both a public key and secret key, and two users can communicate secretly simply by employing each other's public keys. (The sender transmits a message enciphered under the receiver's public key, which the receiver then deciphers using his secret key.) In this note we consider the problem of establishing secret communication in a single-key system.

Key Distribution

Needham and Schroeder propose protocols for obtaining communication keys from an Authentication Server (AS) [NEED78]. They assume that each user A has a private (secret) key KA which is known only to A and AS. If two users wish to secretly communicate, one of them obtains a secret communication key from AS and distributes it to the other. If a new key is obtained for each interaction, then a user need not keep a list of secret communication keys for all of his correspondents.

The key distribution protocol is as follows. Let x^K denote the message x enciphered under key K. For a user A to acquire a

key CK to share with another user B, these steps are taken:

$$A \rightarrow AS: (A, B, I_{A1}) \qquad (1)$$

where I_{A1} is an identifier chosen by A and used only once. Since I_{A1} is returned by the server, enciphered with A's secret key, A can be sure that the response (2) is not a replay of a previous response.

$$AS \rightarrow A: (I_{A1}, B, CK, Y)^{KA} \qquad (2)$$

where

$$Y = (CK, A)^{KB}$$

Note that since Y is enciphered with B's secret key, it cannot be deciphered by A. A distributes the message Y containing CK to B:

$$A \rightarrow B: Y \qquad (3)$$

At this point A can be sure that the key CK is safe to use, but B cannot be sure that the enciphered message Y is not a replay of a previous message sent from A. To protect against this problem, a handshake between B and A follows:

$$B \rightarrow A: (I_{B1})^{CK} \qquad (4)$$

$$A \rightarrow B: (f(I_{B1}))^{CK} \qquad (5)$$

where I_{B1} is an identifier chosen by B. A returns an agreed function f of I_{B1} in order to signal his acceptance of CK. The function f could be something simple like f(I) = I - 1. Needham

and Schroeder maintain that the complete sequence (1) - (5) will establish a secure channel between A and B (assuming neither of the private keys KA or KB has been compromised).

Analysis of the Handshake

As described, the handshake is inadequate. We will argue first that, if any previous communication keys has been compromised, the handshake does not provide an acceptable level of security. We will argue second that, if no keys are ever compromised, the handshake does not prevent message blocking.

First we suppose that a previous communication key CK' used by A and B has been compromised. If the intruder also intercepted the previous message Y' sent from A to B (step 3) as well as the previous handshake (steps 4 and 5), then he can impersonate A unless the function f used in the handshake is a non-trivial secret function known only to A and B. In particular, the intruder can replay the message Y' to B, and then apply the same function f used in the previous handshake to impersonate A in the next handshake. If the same function f is used by all users, then the intruder need only have intercepted the message Y' (he needs at least Y' since he does not know B's secret key KB). After successfully tricking B into accepting the known key CK', the intruder can decipher any messages transmitted from B to A.

Now, the problem of securing secret handshake functions is as difficult as the problem of securing communication keys.

Users must either privately exchange and remember permanent handshake functions, or they must obtain them from the authentication server. If the former approach is taken, then users may as well exchange directly their communication keys and dispense with the handshake functions. If the latter approach is taken, the problem of distributing handshake functions is identical to the problem of distributing keys.

Next, suppose that keys are never compromised. In this case the handshake does guard against replay: an intruder who has intercepted a previous exchange (1) - (5) between A and B of a key CK' will be unable to impersonate A and trick B into using CK'. However, consider the motives of the intruder attempting to trick B into using CK'. Since he will be unable to decipher any messages enciphered under CK', his motive must be either simply to block the communication path from B to A, or to block the path and trick B into accepting previous (replayed) messages from A. Blocking the communication path from B to A could be achieved in many other ways (e.g., by interjecting noise onto the channel); successful completion of a handshake does not guarantee that subsequent transmissions are not blocked. If B wishes to be sure that messages sent to A are not blocked, then he should add sequence numbers and time-stamps to his messages and request a reply from A to each message. If messages and replies have sequence numbers and time-stamps, this will also prevent the intruder from tricking B into accepting previous messages from A. The use of time-stamps to protect against message replay was also

noted by Needham and Schroeder and by Kent [KENT78].

Solution

We believe that any key distribution system should be based on the premise that communication keys may be compromised, and that recovery from compromise must be possible. Operating from this premise, secure distribution of secret communication keys on a computer network requires more than a handshake. We propose a simple solution which eliminates steps (4) and (5) of the distribution protocol, but adds a time-stamp T to steps (2) and (3). The complete protocol is thus:

$$A \rightarrow AS: (A, B) \qquad (1)$$

$$AS \rightarrow A: (B, CK, T, (A, T, CK)^{KB})^{KA} \qquad (2)$$

$$A \rightarrow B: (A, T, CK)^{KB} \qquad (3)$$

A and B can verify that their messages are not replays by checking that:

$$|Clock - T| < \Delta t1 + \Delta t2$$

where Clock gives the local time, $\Delta t1$ is an interval representing the normal discrepancy between the server's clock and the local clock, and $\Delta t2$ is an interval representing the expected network delay time. If each node sets its clock manually by reference to a standard source, such as the NBS broadcast time on WWV, $\Delta t1$ on the order of one or two minutes would suffice. As long as $\Delta t1$ +

$\Delta t2$ is less than the interval since the last use of the protocol, this method of time-stamping will protect against replays. Since the time-stamp T is enciphered under the secret keys KA and KB, impersonation of AS is not possible.

Needham and Schroeder rejected the use of time-stamps in their key distribution protocol on the grounds that there might not be a network-wide reliable source of time. As we have argued, time-stamps can be used reliably even if the settings of local clocks are not completely reliable.

Acknowledgements

We wish to thank P. J. Denning for critically reading this note.

References

DIFF76 Diffie, W. and Hellman, M., "New Directions in Cryptography," IEEE Trans. on Info. Theory, IT-22, 6 (Nov. 1976), 644-654.

KENT78 Kent, S. B., "Protocol Design Considerations for Network Security," Interlinking of Computer Networks; Proc. of the NATO Adv. Stud. Inst., D. Reidel Pub., Sonas, France, Aug. 1978, 239-259.

NEED78 Needham, R. M. and Schroeder, M. D., "Using Encryption for Authentication in Large Networks of Computers," Comm. ACM 21, 12 (Dec. 1978), 993-999.