A Pauper's Callback Scheme

Matt Bishop
Research Institute for Advanced Computer Science, NASA Ames
Research Center, Moffett Field, CA 94035, U.S.A.

This paper discusses the implementation of callback schema in software, including a protocol for having one computer call another, and describes two methods to authenticate users without sending passwords over a telephone line. This decreases the probability of a wiretapper obtaining a valid user password.

Keywords: Challenge protocol, pass-algorithm, callback

1. Introduction

People and computers often communicate with one another over a telephone line. This leads to a problem of authentication: there is simply no way to verify the identity of the calling party. Moreover, if the caller is unauthorized, no information is available on the called system that can be used to identify the caller.

One method of authenticating callers is to use a device called a callback modem. This device has a list of users authorized to dial into the computer. When someone calls the computer, the callback modem answers; the user types an authorization code, and hangs up. The callback modem breaks the connection, looks up the telephone number corresponding to the authorization code, and calls it. When the telephone is answered, the computer begins an ordinary user session (usually, by prompting for the user's name and password).

There are a few problems with this scheme. First, callback cannot be used between two computers lest they be deadlocked in a cycle of calling each other. Second, each user is restricted to calling from a known (or list of known) telephone numbers associated with that user. This is a problem when a user cannot use a prearranged telephone, for example, when he is at a conference. Finally, callback schemes dependent on a callback modem will not work when media other than the telephone system (such as a network using dedicated communication lines) are used.

2. Another Callback Mechanism

Assuming a computer has both dial-out and dial-in telephone lines, it is possible to implement a callback scheme in software without using a callback modem. When a user wishes to log in over a telephone line, he calls the computer. Rather than beginning a login session, however, the computer executes a simple program which asks the
user for his name, his password (or some other authorization code), and the telephone number from which the user wishes to work. The user then hangs up; the computer calls the user back at the indicated number and then begins the session.

In more detail, suppose the user mab wishes to log into the computer daedalus. The procedure is:

1. Mab calls daedalus
2. Daedalus requests the user identification and password, and a telephone number to call back.
3. Both mab and daedalus hang up.
4. Assuming the password corresponds to the user identification, daedalus calls the number supplied and begins an ordinary session with mab.
   If the password does not correspond to the user identification (or there is no such user) daedalus notifies the system administrator.

Notice the advantages of this method. No new equipment must be purchased. Users are no longer restricted to calling in from a telephone number on a preset list. By recording all numbers called on hardcopy, the computer can provide an audit trail of numbers and users called. Should a penetration occur, this information will provide a starting point for any investigation into the identity of the attacker.

Preventing deadlock is not much more difficult provided the calling computer uses a unique, or set of unique, identifications. The protocol above is modified slightly; the following step is added between Steps 3 and 4.
3.5 The program that called daedalus from the computer mab creates a file with the name daedalus and an appropriate time range; then, if a call from daedalus is received within that time, a computer session begins (rather than the callback procedure outlines above).

Of course, all this should be noted in the audit trail, and once the user has successfully logged in, the file granting permission should be deleted.

3. Passwords and Eavesdropping

A related problem is that of an attacker tapping the telephone line. Since a user must send an authorization code and/or password in the clear under the callback scheme, a wiretapper would be able to eavesdrop on the line, interpret the electronic signals corresponding to the information the user sends to the computer, and be able to spoof the computer later. (Callback modems also suffer from this defect.) There are two rather elegant ways to prevent this. Both depend on a password, and an algorithm for changing the password after each use, being agreed upon by all parties involved before any communication occurs over a telephone line.

The first method is suitable when one computer calls another. It is called the challenge protocol and was devised by Sytek, Inc. Immediately after the calling computer supplies a name, the called computer sends a message to the caller. Both computer encrypt this message locally using the password; the calling computer then transmits the encrypted message to the called computer, which then compares it to the results of its encryption. If the two are the same, the authentication succeeds; otherwise it fails. After each encryption, passwords are altered according to a prearranged scheme, so an eavesdropper will not only have to find a password, but also the algorithm used to update the password.

To give an example, suppose the computer daedalus is attempting to log into the computer icarus, a telephone connection having been made using the steps described in Section 2. The procedure is:

1. Daedalus sends its system identification.
2. Icarus sends a meaningless message (such as “HOWDY-DO!”) to daedalus.
3. Both daedalus and icarus encrypt the meaningless message using the agreed-upon encryption algorithm.
4. Daedalus transmits the encrypted message back to icarus.
5. Icarus compares the encrypted message from daedalus with the results of its encryption. If they are the same, daedalus is allowed to proceed, otherwise, not.
6. Both computers change their password according to an agreed-upon scheme (for example, by moving to the next entry in a table, or performing a mathematical transformation on the current password).

This method can also be used when a person calls a computer. Sytek has devised a scheme in which the user is supplied with a small calculator

---

2 The product name is the PFX Identity Authentication Scheme.
with a function key which performs the encryption and updates the password. An alternative, not involving the use of a special calculator, is the pass-algorithm technique.

The pass-algorithm technique [1] requires the user to supply a different password every time he tries to log on. The user may be cued by a prompt; for example, if the algorithm being used at the time is to type every third character in the prompt, the user would be able to supply the password very quickly. Note the important point is that the user remembers an algorithm rather than a word, just as in the challenge protocol.

As an example, suppose mab wished to log into icarus, which uses a pass-algorithm technique. The procedure is almost the same as for the challenge protocol:

1. Mab sends his user identification.
2. (For this example, suppose the pass-algorithm is to type the letters of the prompt corresponding to a Fibonacci series.) Icarus sends a meaningless message (such as “HELLO, THERE”) to mab.
3. Using the pass-algorithm, mab constructs the appropriate password, and sends it: “HHELOH”.
4. Icarus checks to see the response is what it expects (in this case, the first, first, second, third, fifth, and eighth letters of the prompt it sent). If it is, mab is allowed to proceed, otherwise, not.

In neither of these schemes is a password transmitted over the telephone line; only the output of some prearranged algorithm (possibly involving passwords used locally) is sent. Of course, care must be taken with the passwords and algorithms just as with the keys to any authorization system. In the case of computer-to-computer communications, the password (or the encrypted message the called computer expects) must be stored and if the computer is penetrated, this may result in a compromise. The person may also tell someone else the pass-algorithm’s algorithm. Hence, the passwords and the algorithm should be changed frequently. The encryption scheme used in the challenge protocol should be a one-way function, to make determination of the key by a plaintext-ciphertext attack very difficult; a DES-based scheme would be appropriate (among others). The algorithm for the pass-algorithm technique should also be difficult for someone to guess; this can be done by changing the algorithm frequently and using cues that obscure the algorithm.

4. Conclusion

There are alternatives to using a callback modem, as this article points out. Most of the weaknesses of the scheme described above also exist when callback modems are used. The most dangerous is that calls may be automatically forwarded to another number or extension without the knowledge of the caller. In this case, neither callback modems nor the callback scheme will correctly record the number from which the user worked. However, since a callback modem will use only a predetermined list of telephone numbers, the systems administration can restrict callback to a list of trusted telephone numbers. (Of course, the scheme described in the second section might be modified to work from a list, too. But if someone should penetrate the system, whether or not over a telephone, he could change this list, whereas changing a number on a callback modem usually requires access to a console or the physical callback device.)

With the password scheme described above, either the password must exist in the clear on the computers involved, or a program that has the pass-algorithm’s algorithm must exist on the system. In the first case, the password is vulnerable should an intruder gain access to the system; in the second, a good disassembler and some patience would suffice to determine the algorithm used. Also, because a penetration attempt would result in the passwords becoming out of sync, attempted penetrations become very noticeable.

However, callback modems also suffer from these defects. When one cannot (or does not desire) to use a callback modem, the method described in Section 2 is certainly preferable from the security standpoint to allowing users to dial in directly; and whether or not one uses a callback modem, the methods described in Section 3 are far better than transmitting a password in the clear over a telephone line.

Acknowledgements

Thanks to Peter Denning, George Adams, and Michael Raugh of RIACS, and Dorothy Denning
of SRI International, for helpful discussions and comments on an earlier version of this paper, and Michael Yuen of Sytek, for describing the challenge protocol.

Reference