REASONABLE AUTHENTICATION IN DISTRIBUTED SYSTEMS

Jim Alves-Foss
Department of Computer Science
University of Idaho

Munna
Department of Computer Science
University of Idaho

Abstract – One major concern of such computer systems is the authentication of users who are accessing the host computer from a remote site. In such cases, the communication lines are open to intrusion where the information transferred can be captured or replayed by an intruder. Not only is the information transferred from one place to the other unprotected, but so are the machines themselves. Because, as in most cases, the identification tokens such as passwords are transferred through communication lines in plain text and any intruder who captures this can use it later to get access to the computer. Thus, reliable authentication becomes a crucial factor for security of distributed systems.

1 Introduction

In the technologically advanced world of today, computers are used to aid in a variety of ways. Often, the computers we interact with are connected to a large distributed system of computers, all working cooperatively. The proliferation and interconnection of these distributed computer systems are essential to the success of most businesses and government agencies. On the other hand, this interconnection poses a serious threat to the safety of the computers and the systems they are dealing with, such as automatic teller machines, flight control systems of advanced aerospace systems, control systems at government installations, etc. The interconnection makes the system vulnerable to outside penetration by malicious software or by unauthorized users and this can greatly affect the correct performance of these systems and have substantial economic and safety consequences.

One major concern of such computer systems is the authentication of users who are accessing the host computer from a remote site. In such cases, the communication lines are open to intrusion where the information transferred can be captured or replayed by an intruder. Not only is the information transferred from one place to the other unprotected, but so are the machines themselves. Because, as in most cases, the identification tokens such as passwords are transferred through communication lines in plain text and any intruder who captures this can use it later to get access to the computer. Thus, reliable authentication becomes a crucial factor for security of distributed systems.

2 Authentication

In the context of secure computer communication, authentication means verifying the identity of the communicating principals to one another. It is fundamental to access control, accounting and secure communication. Authentication consists of *identification* and *verification* (i.e., an entity claims a certain identity and the claim is checked by a specific process). For identification, an entity has to present some form of key to the verifying entity. Such a key can be a password, physical or electronic item, unique biological feature, etc.

In a distributed system, in which a large number of computers communicate, there may be no central machine or system that contains authoritative descriptions of the connected computers, of the purposes for which they are used, or the individuals who use them [Nee78]. Thus, authentication becomes a more serious issue when distributed systems are dealt with.

In a distributed system, the authentication can be classified [Lie93] into three types:

- *message content authentication.* This involves the verification of the content of a message to ensure that it is the same as the message that was sent.
- *origin authentication.* This involves the verification of the origin of the message, to ensure that the actual source of the message is as it appears to be.
- *general identity authentication.* This involves verifying that a principal's identity is as claimed. Our focus in this paper is on this area.

The two kinds of threats that one has to consider, in the case of networked or distributed systems are: *host*

compromise and *communication compromise*. In host compromise, the host is under the control of an intruder who can then have access to information maintained by the computer. In communication compromise, the communication lines are under the control of an intruder, who can then eavesdrop; modify, insert and delete messages; or replay old messages. In this paper, our concern is mostly with communication compromise, we address host compromise only in how an intruder can compromise the host once they have compromised communication.

3 Authentication Mechanisms

Researchers have developed several authentication mechanisms addressing these different authentication problems (eavesdropping, modification and replay). These mechanisms can be classified according to two categories, *presentation types* and *key management*.

3.1 Presentation Type

A mechanism's *presentation type* determines how the user presents themselves to the system for authentication. The authentication mechanism can either require that the user present information in a *disclosing* manner such that an "eavesdropper" can obtain that information and use it later to spoof the system, or in a *non-disclosing* manner that makes that information useless to the eavesdropper.

The most common form of authentication is a simple password checking mechanism. Different kinds of password checks exist, in which the key may be a password memorized by the user, a physical or electronic item possessed by the user or a unique biological feature [Hal93]. These are called disclosing passwords because, if the password is transmitted over a network, it is disclosed to eavesdroppers. If the access keys are stored in the target system to verify the incoming passwords, a single breach in the system security may give access to all passwords. To avoid this, in most of the simple password systems, the passwords are not stored, but only the information sufficient to verify passwords and not the data for generating them [Hal93]. Disclosing passwords were developed for single-host computer systems, where the likelihood of communication compromise was very small.

To overcome the problems associated with disclosing passwords, researchers have developed several schemes for *nondisclosing passwords*. This class of passwords was developed to prevent replay attacks. Replay attack is the kind of attack on an authentication system that works by recording and replaying previously sent valid messages, or parts of messages. Any constant authentication information can be recorded and used later to forge messages that appear to be authentic [Hal93]. The disclosing password mechanism fails when there is a replay attack, as the passwords used are constant. Nondisclosing password generating systems were developed to overcome this flaw. The systems developed include ID cards which generate a visual display to prove the authenticity. The owner of the card will be considered as a valid user by the authentication system.

3.2 Key Management

Key management is the most important part of a secure cryptosystem used for authentication. Unless the keys are given the same level of protection as the data itself, they will be the weak link. The entire system can be vulnerable if the keys are not adequately protected, even if the encryption algorithm is computationally infeasible to break [Denn82]. Typically the key system can be classified as one of two types: *symmetric* or *asymmetric*.

Cryptographic systems with the same key for encryption and decryption are called *symmetric cryptographic systems*. They are also known as private key or secret key cryptographic systems. This method is excellent for private encryption and decryption. It is also good for protecting information transmitted over computer networks. Unfortunately, because only one key exists for each communication link, management and distribution of this key becomes very difficult.

In an *asymmetric cryptographic system*, different keys are used for encryption and decryption. They differ in such a way that at least one key is computationally infeasible to determine from the other [Denn82]. Secrecy and authenticity are provided by protecting the separate transformations - deciphering transformation for secrecy and enciphering transformation for authenticity. This simplifies the key distribution problem of the symmetric cryptography method.

4 Authentication in Distributed Systems

Current distributed system architectures have often taken the approach that a remote connection is similar to a directly connected terminal. This permits the use of the same protocols and interface mechanisms by abstracting away the physical location of the remote connection. Unfortunately this abstraction fails for normal single-host authentication mechanisms. On a single host there is high assurance that the user is sitting at a terminal where the physical connection between the terminal and host computer is secure. In a networked situation this is unrealistic.

While in the single-host system a user can type in a password (which is not echoed to the screen) and feel secure in the transfer of this information, on a networked system that same typed password is often passed over the network in plain text. This grants any computer attached to the same network the ability to view the password, thus possibly allowing an eavesdropper to gain access to the system. Recent attacks on computer systems, where intruders have placed network "sniffers" on systems to pick up these passwords, have shown how vulnerable we can be.

Although several proposals have been made to remedy this situation, they all require either a "trusted" third-party computer or an elaborate public-key encryption scheme. The protocol we propose requires neither,

but rather uses a version of the Diffie-Hellman [Dif76] key-exchange algorithm to ensure authentication while not compromising the user's password. Our algorithm does not defend against all attacks, nor is it meant to. Rather we are trying to dramatically increase the difficulty of compromise and render useless the current "sniffer" attacks.

The process behind this algorithm is very straight forward. It will work for any existing internet protocol that grants a remote user access to a host via a password mechanisms (e.g., telnet, ftp). After the user has sent a request for access to the host, the host responds with a challenge. The remote user then sends an authentication response that is validated by the host. The important idea here is the contents of the challenge and the response.

- *Challenge.* The challenge consists of a partial session key such as that defined by the Diffie-Hellman protocol. This partial key will be used to establish a private authentication key for the remote user's response. This partial key is randomly generated for each session.
- *Response.* The user's response consists of a new partial session key as well as the password encrypted by the full session key. The host will decrypt this password and use it to validate the remote user.

In this protocol, passwords are no longer sent across the network in plain text, but are encrypted. To break this scheme an intruder must either be able to masquerade as the host, or be able to compute the discrete logarithm of very large numbers (currently computationally intractable). Although these attacks are plausible they are not nearly as likely to occur as the current "sniffer" attacks. This protocol can be rapidly employed as an extension of existing internet protocols without requiring special purpose hardware, or trusted third-party authentication servers.

References

[Denn82] D.E.Denning. Cryptography and Data Security. Addison-Wesley 1982

[Dif76] W.Diffie & M.Hellman New Directions in Cryptography. *IEEE Transactions on Information Theory.* V22, N6, pp. 74–84, November 1976

[Hal93] N.Haller & R.Atkinson. Internet Authentication Guidelines. *Internet draft* October 1993

[Lie93] A.Liebl. Authentication in Distributed Systems: A Bibliography. *Operating Systems Review* V27 N4, pp. 31–41, October 1993

[Nee78] R.M.Needham & M.D.Schroeder. Using Encryption for Authentication in Large Networks of Computers. *Communications of the ACM* V21, N12, pp. 993–999, December 1978