

*NDB*

*ISI Research Report*

*ISI/RS-94-399*

*September 1994*

*70-62-CR*

*6619*

# **Kerberos: An Authentication Service for Computer Networks**

**B. Clifford Neuman and Theodore Ts'o**

**ISI/RS-94-399**

**September 1994**

*University of Southern California*

*Information Science Institute*

*4676 Admiralty Way, Marina del Rey, CA 90292-6695*

*310-822-1511*

The major sponsors of Project Athena were Digital Equipment Corporation and IBM. Neuman's security efforts are funded in part by the Advance Research Projects Agency under NASA Cooperative Agreement NCC-2-539 and other awards, and by CyberSAFE Corporation (formerly Open Computing Security Group). The views and conclusions contained in this paper are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of any of the funding organizations. Figures and descriptions in this paper were provided by the authors and are used with permission.

© 1994 Institute of Electrical and Electronics Engineers. Reprinted, with permission, from IEEE Communications Magazine, Volume 32, Number 9, pages 33-38, September 1994.

---

# Kerberos: An Authentication Service for Computer Networks

When using authentication based on cryptography, an attacker listening to the network gains no information that would enable it to falsely claim another's identity. Kerberos is the most commonly used example of this type of authentication technology.

---

*B. Clifford Neuman and Theodore Ts'o*



Modern computer systems provide service to multiple users and require the ability to accurately identify the user making a request. In traditional systems, the user's identity is verified by checking a password typed during login; the system records the identity and uses it to determine what operations may be performed. The process of verifying the user's identity is called authentication. Password-based authentication is not suitable for use on computer networks. Passwords sent across the network can be intercepted and subsequently used by eavesdroppers to impersonate the user. While this vulnerability has been long known, it was recently demonstrated on a major scale with the discovery of planted password collecting programs at critical points on the Internet [4].

## Authentication, Integrity, Confidentiality, and Authorization

Authentication is the verification of the identity of a party who generated some data, and of the integrity of the data. A principal is the party whose identity is verified. The verifier is the party who demands assurance of the principal's identity. Data integrity is the assurance that the data received is the same as generated. Authentication mechanisms differ in the assurances they provide: some indicate that data was generated by the principal at some point in the past, a few indicate that the principal was present when the data was sent, and others indicate that the data received was freshly generated by the principal. Mechanisms also differ in the number of verifiers: some support a single verifier per message, while others support multiple verifiers. A third difference is whether the mechanism supports non-repudiation, the ability of the verifier to prove to a third party that the message originated with the principal.

Because these differences affect performance, it is important to understand the requirements of an application when choosing a method.

For example, authentication for electronic mail may require support for multiple recipients and non-repudiation, but can tolerate greater latency. In contrast, poor performance would cause problems for authentication to a server responding to frequent queries.

Other security services include confidentiality and authorization. Confidentiality is the protection of information from disclosure to those not intended to receive it. Most strong authentication methods optionally provide confidentiality. Authorization is the process by which one determines whether a principal is allowed to perform an operation. Authorization is usually performed after the principal has been authenticated, and may be based on information local to the verifier, or based on authenticated statements by others.

The remainder of this article will concentrate on authentication for real-time, interactive services that are offered on computer networks. We use the term real-time loosely to mean that a client process is waiting for a response to a query or command so that it can display the results to the user, or otherwise continue performing its intended function. This class of services includes remote login, file system reads and writes, and information retrieval for applications like Mosaic.

## Why Kerberos

The introduction discussed the problems associated with password-based authentication and, in particular, how passwords can be collected by eavesdropping. In addition to the security concern, password based authentication is inconvenient; users do not want to enter a password each time they access a network service. This has led to the use of even weaker authentication on computer networks: authentication by assertion.

While more convenient for the user, authentication by assertion hardly qualifies as authentication at all. Examples include the Berkeley R-command suite and the IDENT protocol. With authentication by assertion, applications assert the identity of the user and the server believes it. Such authentication is easily thwarted by modifying the applica-

---

*CLIFFORD NEUMAN is a scientist at the Information Sciences Institute of the University of Southern California.*

*THEODORE TS'O leads the Kerberos V5 development effort at the Massachusetts Institute of Technology.*

---

*The Kerberos Authentication System uses a series of encrypted messages to prove to a verifier that a client is running on behalf of a particular user.*

tion. This may require privileged access to the system, which is easily obtained on PCs and personal workstations. While most uses of authentication by assertion require that a connection originate from a "trusted" network address, on many networks, addresses are themselves simply assertions.

Stronger authentication methods based on cryptography are required. When using authentication based on cryptography, an attacker listening to the network gains no information that would enable it to falsely claim another's identity. Kerberos is the most commonly used example of this type of authentication technology. Unfortunately, strong authentication technologies are not used as often as they should be, although the situation is gradually improving.

### **The Kerberos Authentication Service**

**K**erberos is a distributed authentication service that allows a process (a client), running on behalf of a principal (a user), to prove its identity to a verifier (an application server, or just server) without sending data across the network that might allow an attacker or the verifier to subsequently impersonate the principal. Kerberos optionally provides integrity and confidentiality for data sent between the client and server. Kerberos was developed in the mid-'80s as part of MIT's Project Athena [2]. As use of Kerberos spread to other environments, changes were needed to support new policies and patterns of use. To address these needs, design of Version 5 of Kerberos (V5) began in 1989 [11]. Though V4 still runs at many sites, V5 is considered to be standard Kerberos [10].

### **Limitations of Kerberos**

Limitations of Kerberos have been described in the literature [1]. Though most are a matter of preference or apply to V4 and early drafts of V5, a few are fundamental and are discussed here. In particular, Kerberos is not effective against password guessing attacks; if a user chooses a poor password, then an attacker guessing that password can impersonate the user. Similarly, Kerberos requires a trusted path through which passwords are entered. If the user enters a password to a program that has already been modified by an attacker (a Trojan horse), or if the path between the user and the initial authentication program can be monitored, then an attacker may obtain sufficient information to impersonate the user. Kerberos can be combined with other techniques, as described later, to address these limitations.

To be useful, Kerberos must be integrated with other parts of the system. It does not protect all messages sent between two computers; it only protects the messages from software that has been written or modified to use it. While it may be used to exchange encryption keys when establishing link encryption and network level security services, this would require changes to the network software of the hosts involved.

Kerberos does not itself provide authorization, but V5 Kerberos passes authorization information generated by other services. In this manner, Kerberos can be used as a base for building separate distributed authorization services [14].

### **How Kerberos Works**

The Kerberos Authentication System [18] uses a series of encrypted messages to prove to a verifier that a client is running on behalf of a particular user. The Kerberos protocol is based in part on the Needham and Schroeder authentication protocol [13], but with changes to support the needs of the environment for which it was developed. Among these changes are the use of timestamps to reduce the number of messages needed for basic authentication [6], the addition of a "ticket-granting" service to support subsequent authentication without re-entry of a principal's password, and a different approach to cross-realm authentication (authentication of a principal registered with a different authentication server than the verifier).

The remainder of this section describes the Kerberos protocol. The description is simplified for clarity; additional fields are present in the actual protocol. Readers should consult RFC 1510 [10] for a more thorough description of the Kerberos protocol.

**Kerberos Encryption** — Though conceptually, Kerberos authentication proves that a client is running on behalf of a particular user, a more precise statement is that the client has knowledge of an encryption key that is known by only the user and the authentication server. In Kerberos, the user's encryption key is derived from and should be thought of as a password; we will refer to it as such in this article. Similarly, each application server shares an encryption key with the authentication server; we will call this key the server key.

Encryption in the present implementation of Kerberos uses the data encryption standard (DES). It is a property of DES that if ciphertext (encrypted data) is decrypted with the same key used to encrypt it, the plaintext (original data) appears. If different encryption keys are used for encryption and decryption, or if the ciphertext is modified, the result will be unintelligible, and the checksum in the Kerberos message will not match the data. This combination of encryption and the checksum provides integrity and confidentiality for encrypted Kerberos messages.

**The Kerberos Ticket** — The client and server do not initially share an encryption key. Whenever a client authenticates itself to a new verifier it relies on the authentication server to generate a new encryption key and distribute it securely to both parties. This new encryption key is called a session key and the Kerberos ticket is used to distribute it to the verifier.

The Kerberos ticket is a certificate issued by an authentication server, encrypted using the server key. Among other information, the ticket contains the random session key that will be used for authentication of the principal to the verifier, the name of the principal to whom the session key was issued, and an expiration time after which the session key is no longer valid. The ticket is not sent directly to the verifier, but is instead sent to the client who forwards it to the verifier as part of the application request. Because the ticket is encrypted in the server key, known only by the authentication server and intended verifier, it

is not possible for the client to modify the ticket without detection.

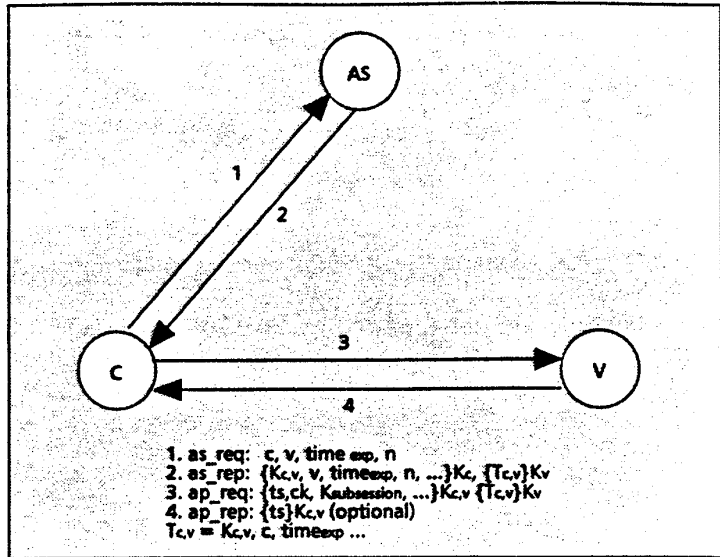
**Application Request and Response** — Messages 3 and 4 in Fig. 1 show the application request and response, the most basic exchange in the Kerberos protocol.<sup>1</sup> It is through this exchange that a client proves to a verifier that it knows the session key embedded in a Kerberos ticket. There are two parts to the application request, a ticket (described above) and an authenticator. The authenticator includes, among other fields: the current time, a checksum, and an optional encryption key, all encrypted with the session key from the accompanying ticket.

Upon receipt of the application request, the verifier decrypts the ticket, extracts the session key, and uses the session key to decrypt the authenticator. If the same key was used to encrypt the authenticator as used to decrypt it, the checksum will match and the verifier can assume the authenticator was generated by the principal named in the ticket and to whom the session key was issued. This is not by itself sufficient for authentication since an attacker can intercept an authenticator and replay it later to impersonate the user. For this reason the verifier additionally checks the timestamp to make sure that the authenticator is fresh. If the timestamp is within a specified window (typically five minutes) centered around the current time on the verifier, and if the timestamp has not been seen on other requests within that window, the verifier accepts the request as authentic. A discussion of the benefits and drawbacks to the use of timestamps in authentication protocols can be found in [15].

At this point the identity of the client has been verified by the server. For some applications the client also wants to be sure of the server's identity. If such mutual authentication is required, the server generates an application response by extracting the client's time from the authenticator, and returns it to the client together with other information, all encrypted using the session key.

**Authentication Request and Response** — The client requires a separate ticket and session key for each verifier with which it communicates. When a client wishes to create an association with a particular verifier, the client uses the authentication request and response, messages 1 and 2 from Fig. 1, to obtain a ticket and session key from the authentication server. In the request, the client sends the authentication server its claimed identity, the name of the verifier, a requested expiration time for the ticket, and a random number that will be used to match the authentication response with the request.

In its response, the authentication server returns the session key, the assigned expiration time, the random number from the request, the name of the verifier, and other information from the ticket, all encrypted with the user's password registered with the authentication server, together with a ticket containing similar information, and which is to be forwarded to the verifier as part of the application request. Together, the authentication request and response and the application request and response comprise the basic Kerberos authentication protocol.



■ Figure 1. Basic Kerberos authentication protocol (simplified).

**Obtaining Additional Tickets** — The basic Kerberos authentication protocol allows a client with knowledge of the user's password to obtain a ticket and session key for and to prove its identity to any verifier registered with the authentication server. The user's password must be presented each time the user performs authentication with a new verifier. This can be cumbersome; instead, a system should support single sign-on, where the user logs in to the system once, providing the password at that time, and with subsequent authentication occurring automatically. The obvious way to support this, caching the user's password on the workstation, is dangerous. Though a Kerberos ticket and the key associated with it are valid for only a short time, the user's password can be used to obtain tickets, and to impersonate the user until the password is changed. A better approach, and that used by Kerberos, is to cache only tickets and encryption keys (collectively called credentials) that will work for a limited period.

The ticket granting exchange of the Kerberos protocol allows a user to obtain tickets and encryption keys using such short-lived credentials, without re-entry of the user's password. When the user first logs in, an authentication request is issued and a ticket and session key for the ticket granting service is returned by the authentication server. This ticket, called a ticket granting ticket, has a relatively short life (typically on the order of eight hours). The response is decrypted, the ticket and session key saved, and the user's password forgotten.

Subsequently, when the user wishes to prove its identity to a new verifier, a new ticket is requested from the authentication server using the ticket granting exchange. The ticket granting exchange is identical to the authentication exchange except that the ticket granting request has embedded within it an application request, authenticating the client to the authentication server, and the ticket granting response is encrypted using the session key from the ticket granting ticket, rather than the user's password.

<sup>1</sup>Messages 1 and 2 are described in the section on authentication request and response.

**Client/server applications must be modified to use Kerberos for authentication; such Kerberos-aware applications are said to be Kerberized.**

Figure 2 shows the complete Kerberos authentication protocol. Messages 1 and 2 are used only when the user first logs in to the system, messages 3 and 4 whenever a user authenticates to a new verifier, and message 5 is used each time the user authenticates itself. Message 6 is optional and used only when the user requires mutual-authentication by the verifier.

**Protecting Application Data** — As described so far, Kerberos provides only authentication: assurance that the authenticated principal is an active participant in an exchange. A by-product of the Kerberos authentication protocol is the exchange of the session key between the client and the server. The session key may subsequently be used by the application to protect the integrity and privacy of communications. The Kerberos system defines two message types, the safe message and the private message to encapsulate data that must be protected, but the application is free to use a method better suited to the particular data that is transmitted.

**Additional Features** — The description of Kerberos just presented was greatly simplified. Additional fields are present in the ticket, authenticator, and messages, to support bookkeeping and additional functionality. Some of the features present in Version 5 include renewable and forwardable tickets, support for higher level authorization mechanisms, and support for multi-hop cross-realm authentication (described in the following section). A more rigorous presentation of the Kerberos protocol, and a description of each field is found in RFC 1510 [10].

### **Kerberos Infrastructure and Cross-Realm Authentication**

In a system that crosses organizational boundaries, it is not appropriate for all users to be registered with a single authentication server. Instead, multiple authentication servers will exist, each responsible for a subset of the users or servers in the system. The subset of the users and servers registered with a particular authentication server is called a realm (if a realm is replicated, users will be registered with more than one authentication server). Cross-realm authentication allows a principal to prove its identity to a server registered in a different realm.

To prove its identity to a server in a remote realm, a Kerberos principal obtains a ticket granting ticket for the remote realm from its local authentication server. This requires the principal's local authentication server to share a cross-realm key with the verifier's authentication server. The principal next uses the ticket granting exchange to request a ticket for the verifier from the verifier's authentication server, which detects that the ticket granting ticket was issued in a foreign realm, looks up the cross-realm key, verifies the validity of ticket granting ticket, and issues a ticket and session key to the client. The name of the client, embedded in the ticket, includes the name of the realm in which the client was registered.

With Version 4, it was necessary for an authentication server to register with every other realm

with which cross-realm authentication was required. This was not scalable; complete interconnection required the exchange of  $n^2$  keys where  $n$  was the number of realms.

In contrast, Version 5 supports multi-hop cross-realm authentication, allowing keys to be shared hierarchically. With V5, each realm shares a key with its children and parent, i.e. the ISI.EDU realm shares a key with the EDU realm, which also shares keys with MIT.EDU, USC.EDU, and WASHINGTON.EDU. If no key is shared directly by ISI.EDU and MIT.EDU, authentication of the client `bcn@ISI.EDU` to a server registered with the MIT.EDU realm proceeds by obtaining a ticket granting ticket for EDU from the ISI.EDU authentication server, using that ticket granting ticket to obtain a ticket granting ticket for the MIT.EDU realm from the EDU authentication server, and finally obtaining a ticket for the verifier from the MIT.EDU authentication server.

The list of realms that are transited during multi-hop cross-realm authentication is recorded in the ticket and the verifier accepting the authentication makes the final determination about whether the path that was followed should be trusted. Shortcuts through the hierarchy are supported and can improve both the trust in and the performance of the authentication process.

This hierarchical organization of realms is similar to the hierarchical organization of certification authorities and certificate servers for public-key cryptography [3]. As with the public key certification hierarchy, the utility of the authentication infrastructure supporting authentication between parties not previously known to one another depends in part on the availability of authentication servers for realms near the top of the hierarchy. Unfortunately, political and legal ambiguity has the potential to slow the establishment of these realms. In the mean time, pairwise relationships between regions of the hierarchy (shortcuts) are important. A discussion of the tradeoffs available when establishing realms for large organizations can be found in [5].

### **Obtaining and Using Kerberos**

Source code releases for V4 and Beta V5 Kerberos are freely available from MIT, however, MIT does not officially support these releases. Several companies have taken reference implementations from MIT and provide commercially supported products. Information on the free releases and the supported versions can be obtained by reading the "Kerberos Frequently Asked Questions" document [8] periodically posted to the Usenet newsgroup `comp.protocols.kerberos`, or by sending a message to `info-kerberos@mit.edu`.

### **Setting up the Authentication Server**

Since the Kerberos authentication server maintains a database of passwords (encryption keys) for all the users at a site, it is extremely important that it be installed on a carefully protected and physically secure machine. If possible, the machine should be dedicated to running the authentication server and the number of users with access should be limited.

Initial passwords for a site's users must be registered with the authentication server. If the number of users is small, initial registration is best achieved in person in front of an accounts administrator who can check a driver's license, passport, or other physical document.

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

## LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

## FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

## E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.