US005740361A

United States Patent [19]

Brown

[11] Patent Number: 5,740,361

[45] Date of Patent: Apr. 14, 1998

[54] **SYSTEM FOR REMOTE PASS-PHRASE AUTHENTICATION**

[75] Inventor: **Gary S. Brown**, Columbus, Ohio

[73] Assignee: **CompuServe Incorporated**, Columbus, Ohio

[21] Appl. No.: **656,936**

[22] Filed: **Jun. 3, 1996**

[51] **Int. Cl.**[6] **G06F 12/14**

[52] **U.S. Cl.** **395/187.01**

[58] **Field of Search** ..... 364/DIG. 1 MS File, 364/DIG. 2 MS File; 380/4, 21, 23, 46, 49; 395/601, 609, 761, 762, 186, 187.01, 188.01, 200.3, 200.33

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,535,276	7/1996	Ganesan	380/25
5,550,984	8/1996	Gells	395/200.75
5,604,803	2/1997	Aziz	380/25
5,638,448	6/1997	Nguyen	380/29

OTHER PUBLICATIONS

Dave Raggett, Internet Draft, *Mediated Digest Authentication*, Mar. 1995, pp. 1–12.

Bird, et al., *A Modular Family of Secure Protocols for Authentication and Key Distribution*, Nov. 1992, pp. 1–15.

Bird, et al., *Systematic Design of a Family of Attack–Resistant Authentication Protocols*, Sep. 1992, pp. 1–26.

Molva, et al., *KryptoKnight Authentication and Key Distribution System*, 20 pages.

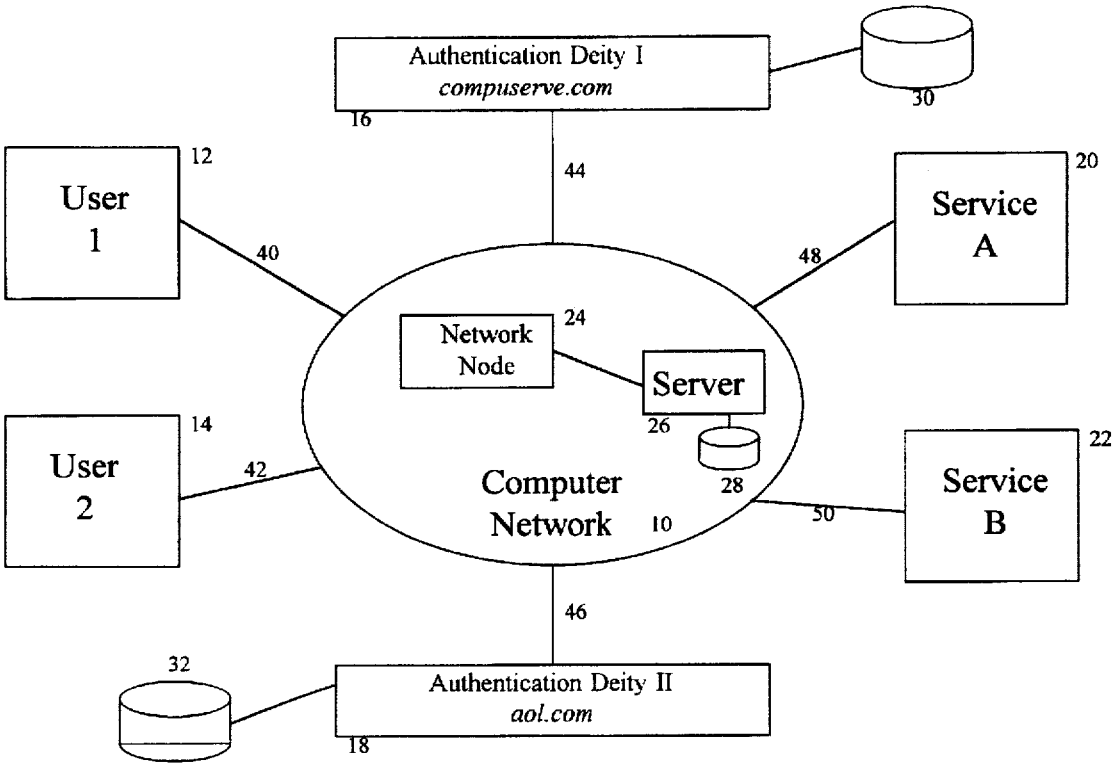
Primary Examiner—Robert B. Harrell

Attorney, Agent, or Firm—Standley & Gilcrest

[57] **ABSTRACT**

A system and method are disclosed for authenticating users and services communicating over an insecure network. Each user and service has a pass-phrase used for authentication. However, the pass-phrases are not revealed during the authentication process as challenge-response techniques are used to keep the pass-phrase secret. In addition, the users and services do not need to know nor do they learn each other's pass-phrases making the process useful in a distributed environment. Pass-phrases are known by an authentication entity with which the service communicates to authenticate both users and services. Users may have identities in and services may support a number of realms, each of which may be viewed as large collection of users (e.g., CompuServe.com). Users choose the realm in which they would like to be authenticated. In one embodiment of the present invention, the system and method are adapted for use with the HyperText Transfer Protocol of the World Wide Web so that secure transactions may be accomplished between users and services communicating via the Internet.

26 Claims, 3 Drawing Sheets



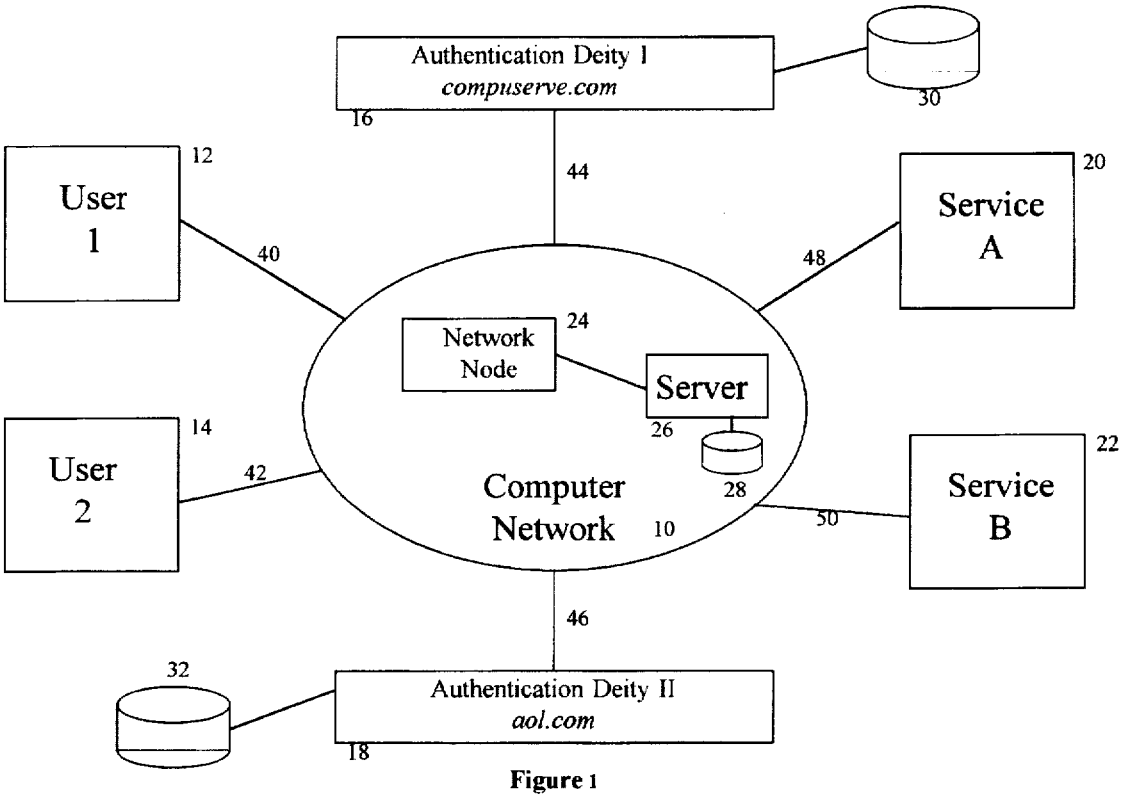


Figure 1

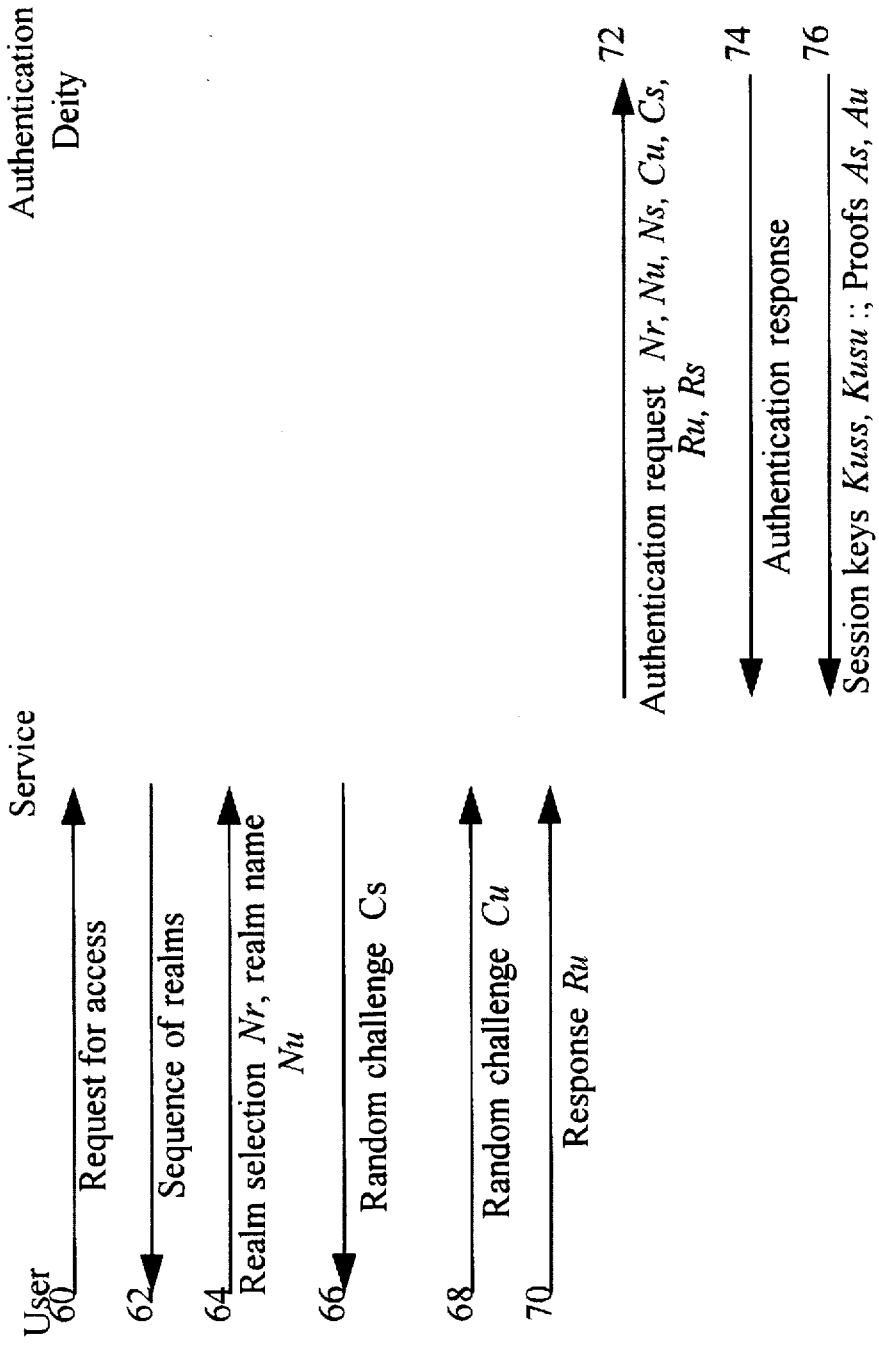


Figure 2

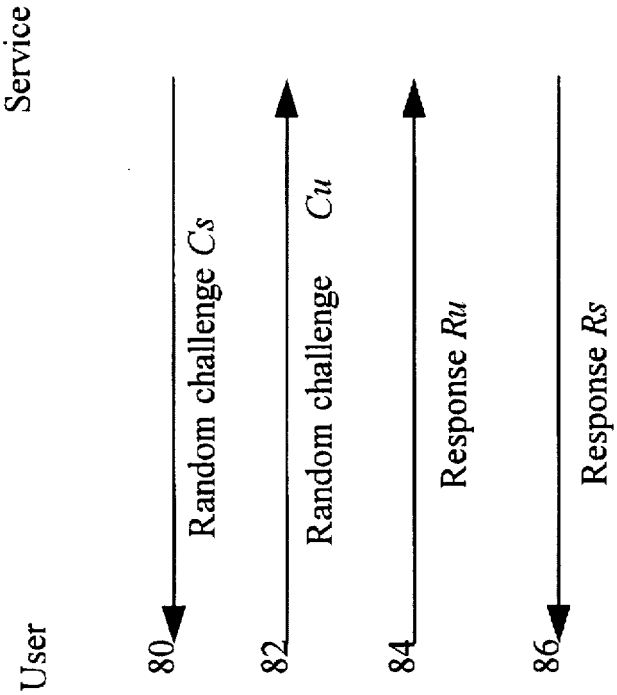


Figure 3

SYSTEM FOR REMOTE PASS-PHRASE AUTHENTICATION

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to authentication of computer users and services in distributed environments. Particularly, the present invention relates to a Remote Pass-phrase Authentication scheme that provides a way to authenticate users and services using a pass-phrase over a computer network without revealing the pass-phrase.

2. Description of the Related Art

The importance of secure communication is increasing as world-wide networks such as the Interact and the World Wide Web (WWW) portion of the Internet expand. As global networks expand through the interconnection of existing networks, users may gain access to an unprecedented amber of services. The services, each of which may be maintained by a different provider, give users access to academic, business, consumer, government, etc. information. Service providers are now able to make their services available to an ever-expanding user base.

The ease with which services and users are able to find each other and the convenience associated with on-line transactions is leading to an increase in the number of remote business and related transactions. However, users and services are not always certain who or what is at the other end of a transaction. Therefore, before they engage in business and other transactions, users and services want and need reassurance that each entity with whom they communicate is who or what it purports to be. For example, users will not be willing to make on-line purchases that require them to reveal their credit card numbers unless they are confident that the service with which they are communicating is in fact the service they wanted to access. Commercial and other private entities who provide on-line services may be more reluctant than individuals to conduct business on-line unless they are confident the communication is with the desired individual or service.

Both users and services need reassurance that neither will compromise the integrity of the other nor that confidential information will be revealed unintentionally to third parties while communications are occurring. Security in a global network, however, may be difficult to achieve for several reasons. First, the connections between remote users and services are dynamic. With the use of portable devices, users may change their remote physical locations frequently. The individual networks that comprise the global networks have many entry and exit points. Also, packet switching techniques used in global networks result in numerous dynamic paths that are established between participating entities in order to achieve reliable communication between two parties. Finally, communication is often accomplished via inherently insecure facilities such as the public telephone network and many private communication facilities. Secure communication is difficult to achieve in such distributed environments because security breaches may occur at the remote user's site, at the service computer site, or along the communication link. Consequently, reliable two-way authentication of users and the services is essential for achieving security in a distributed environment.

Two-way authentication schemes generally involve handshaking techniques so that each party may verify he or she is in communication with the desired party regardless of each party's location or the types of devices in use. The problem to be solved is one in which a user communicates

with a service that wishes to learn and authenticate the user's identity and vice versa. To clarify the problem, there are three aspects of network security that may be distinguished:

Identification:	the way in which a user or service is referenced.
Authentication:	the way in which a user may prove his or her identity.
Authorization:	a method for determining what a given user may do. The same aspects apply to services as well as users.

Identification

A user's identity consists of a user name and a realm name. A realm is a universe of identities. CompuServe Information Service (CIS) user IDs and America Online (AOL) screen names are two examples of realms. The combination of user name and realm—typically shown as name@realm—identifies a user. Any given service recognizes some particular set of identities. A realm does not have to be large, though, either in number of users or size of service. For example, a single WWW server may have its own realm of users.

Often, a service recognizes only one realm: CIS recognizes only identities within the CIS realm and AOL recognizes only identities within the AOL realm. But, one can imagine a service that has agreements with both CIS and AOL. The service gives the user a choice of realms—"Please supply a CIS or AOL identity, and prove it"—and the user chooses a realm in which he or she has an identity. Identification, thus, provides the ability to identify, or to refer to, a user.

Authentication

Authentication provides the ability to prove identity. When asking to do something for which a user's identity matters, the user may be asked for his or her identity—a user name and realm—and the service requires the user to prove that he is who he says he is. To accomplish this, most services use a secret called a pass-phrase, although it is not necessarily derived from text. Such a secret is sometimes called a secret key, but it is not necessarily used for encryption. In this context, the fundamental problem to be solved is: How can a user prove his pass-phrase without revealing the pass-phrase in the process?

Authorization

Authorization refers to the process of determining whether a given user is allowed to do something. For example, may he post a message? May he use a surcharged service? It is important to realize that authentication and authorization are distinct processes—one related to proving an identity and the other related to the properties of an identity. The present invention is not related to authorization, but it is designed to co-exist with authorization mechanisms.

Pass-phrase

A service that wishes to authenticate a user requires the user to identify himself or herself and to prove that he or she knows the pass-phrase. Generally, the service prompts the user for the pass-phrase. However, transmitting the plain text pass-phrases through a network comprises security because an eavesdropper may learn the pass-phrase as it travels through the network. X.25 networks have been compromised, and LANs, modem pools, and "The Internet" likewise are not suitable for plain text pass-phrases due to the eavesdropper problem. Prompting for the pass-phrase, while sufficient in the past, no longer works for extensive world-wide networks

DOCKET ALARM

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.