US006119230A

United States Patent [19]

Carter

[11] Patent Number: 6,119,230

[45] Date of Patent: Sep. 12, 2000

[54] **DISTRIBUTED DYNAMIC SECURITY CAPABILITIES**

[75] Inventor: **Stephen R. Carter**, Spanish Fork, Utah

[73] Assignee: **Novell, Inc.**, Provo, Utah

[21] Appl. No.: **08/943,537**

[22] Filed: **Oct. 1, 1997**

[51] **Int. Cl.**[7] **G06F 12/14**

[52] **U.S. Cl.** **713/200**

[58] **Field of Search** 713/200, 201, 713/202, 161; 709/229; 380/3, 229, 4, 232, 25, 30

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,558,176	12/1985	Arnold et al.	380/4
4,599,509	7/1986	Silverman et al.	235/382
5,196,840	3/1993	Leith et al.	340/825.3
5,204,961	4/1993	Barlow	395/725
5,263,165	11/1993	Janis	395/725
5,315,657	5/1994	Abadi et al.	380/25
5,349,642	9/1994	Kingdon	380/25
5,481,715	1/1996	Hamilton et al.	395/700
5,604,490	2/1997	Blakley, III et al.	340/825.31
5,649,194	7/1997	Miller et al.	395/616
5,818,936	10/1998	Mashayekhi	380/25
5,913,025	6/1999	Higley et al.	713/201

FOREIGN PATENT DOCUMENTS

0 695 985 A1	2/1996	European Pat. Off. .

OTHER PUBLICATIONS

Lampson et al., Abstract—"Authentication in distributed systems:theory and practice" , *ACM Transaction on Computer Systems,*vol. 10, No. 4 (Nov. 1992), pp. 265–310.

Jurec et al., Abstract—"Exchange of patient records–prototype implementation of a security attributes service in X.500", *Proceedings of the 2ACM Conference on Computer and Communications Security,*pp. 30–38.

Chaum, Abstract—"Security without identification:transaction systems to make big brother obsolete", *Communications of the ACM,*vol. 28, No. (Oct. 1985) pp. 1030–1044.

Särs, "The SSH Transport Layer Protocol", *Dr. Dobb's Journal,*(Oct. 1997), pp. 38–43.

Tanenbaum, Distributed Operating Systems, Prentice Hall, Inc. (1995), pp. 544–63.

"Dover AFB employs Vigilant Networks with NDS™", *Electronic Government;Special Novell®Issue,*pp. 12–13.

Dalton et al., Windows NT Server 4: Security, Troubleshooting, and Optimization, New Riders Publishing (1996), pp. 92–93, 371–75.

Tanenbaum, Computer Networks, Third Edition, Prentice Hall, Inc. (1996), pp. 577–630.

Grimes, Professional DCOM Programming, Wrox Press (1997), Ch. 7 pp. 319–389.

Lampson et al., "Authentication in Distributed Systems: Theory and Practice", *ACM Transaction on Computer Systems,*vol. 10, No. 4 (Nov. 1992), pp. 265–310.

"DCE web and Security Domains", no later than May 16, 1997.

Steve Lewontin, "The DCE–Web: Securing the Enterprises Web", Nov. 1995.

"Secure Web–Architecture", no later than May 16, 1997.

"Secure Web Architecture–Scalability", no later than May 16, 1997.

"DCE Web Security", no later than May 16, 1997.

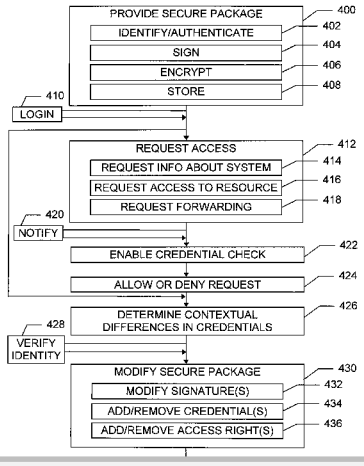
Rich Salz, "Re: [Q]DCE RPC Encription", Jul. 21, 1995.

Primary Examiner—Robert W. Beausoliel, Jr.
Assistant Examiner—Pierre Eddy Elisca
Attorney, Agent, or Firm—Computer Law++

[57] **ABSTRACT**

Methods and systems are provided for managing security credentials in a distributed computer system. Multiple security contexts may be defined for a given principal in the system without requiring the use of multiple accounts. A secure package is provided to allow the principal to roam. Methods are provided for identifying differences in the principal's access rights in different contexts and for updating the secure package as needed.

45 Claims, 3 Drawing Sheets



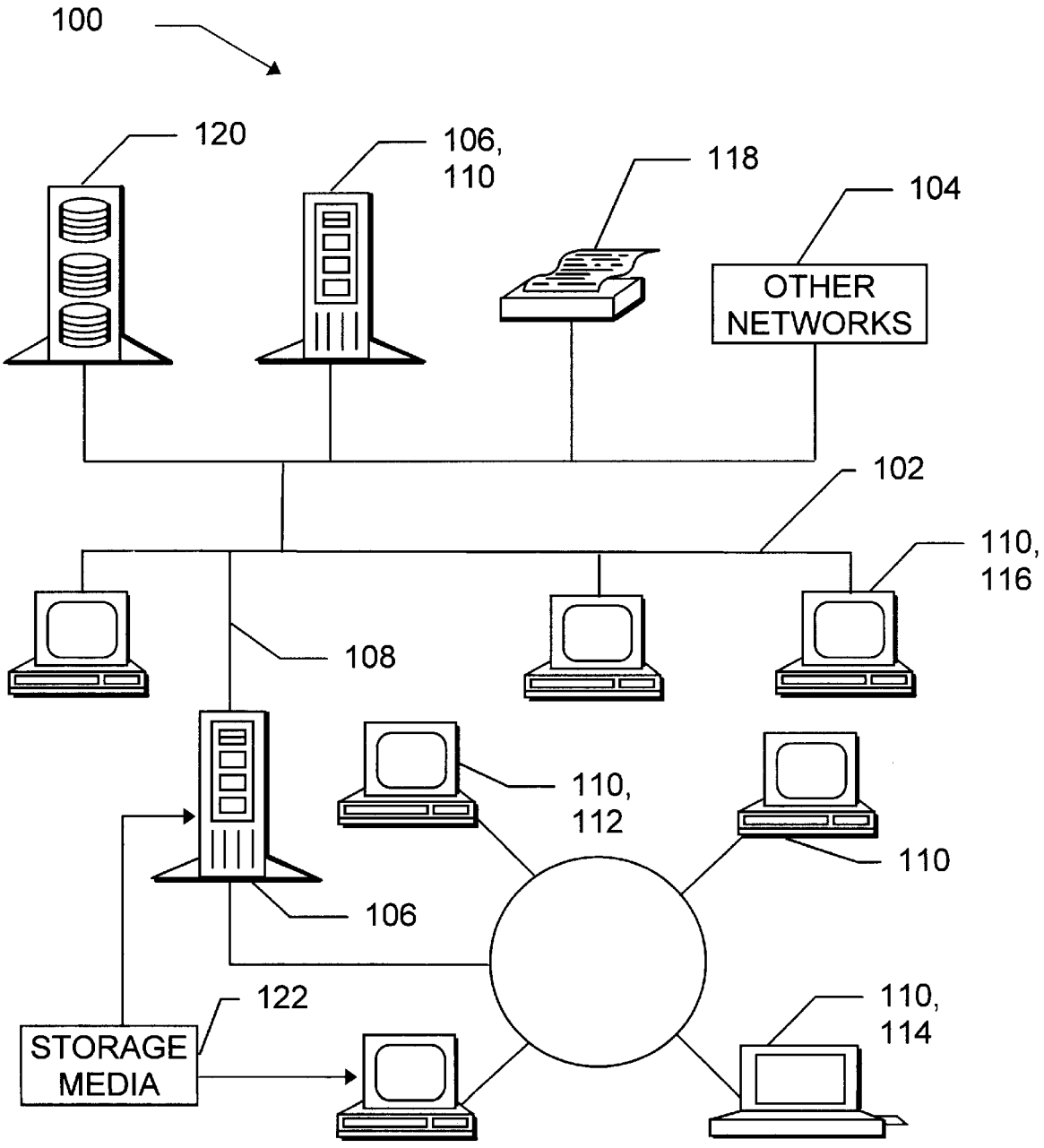


FIG. 1

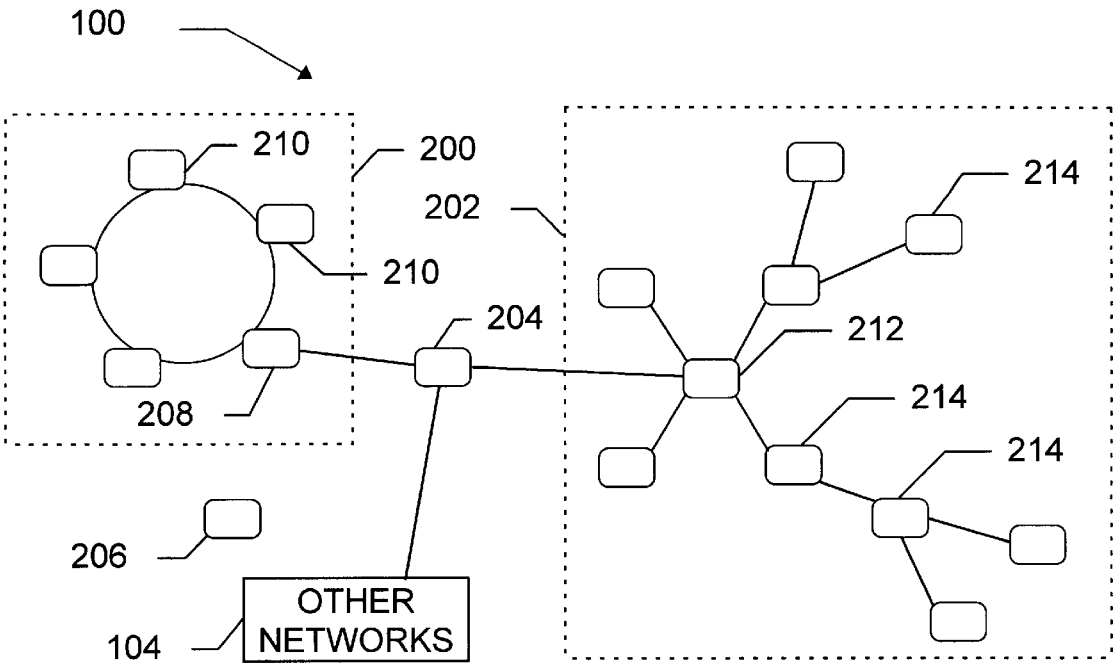


FIG. 2

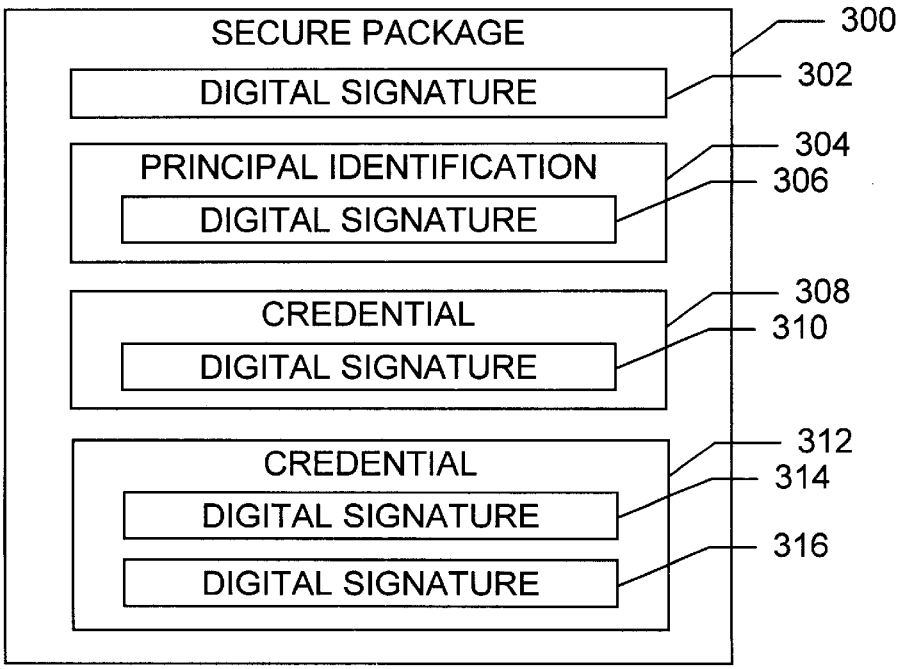


FIG. 3

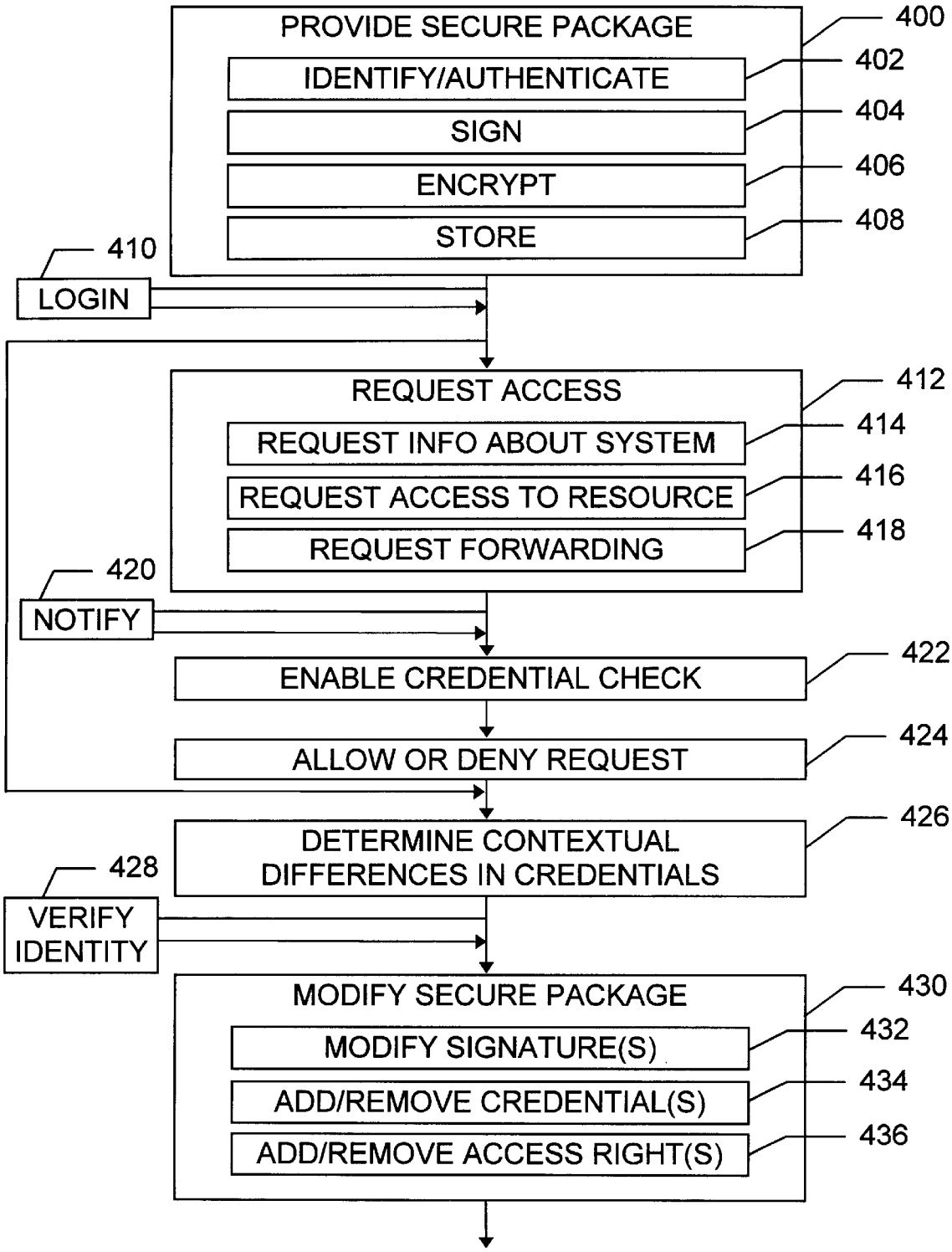


FIG. 4

DISTRIBUTED DYNAMIC SECURITY CAPABILITIES

FIELD OF THE INVENTION

The present invention relates to security in computer systems, and more particularly to a system and method for issuing a secure package of credentials to a user or agent, providing different access capabilities at different system locations based in part on the secure package, and modifying the secure package to reflect local information about the access capabilities of the user or agent.

TECHNICAL BACKGROUND OF THE INVENTION

Various approaches have been proposed and/or implemented to support roaming users and roaming machines in distributed computer systems. One approach, which is implemented in Novell NetWare 4.1 and later versions and in Novell NDS software, allows users to gain access to multiple servers in a distributed directory tree without logging in and authenticating themselves to each server individually (NOVELL, NETWARE, and NDS are marks of Novell, Inc.). However, a separate account, and separate login and authentication processes, are still required before a user can login to a computer which is not part of the distributed directory tree, even if that computer is in network communication with a computer which is part of the tree.

An other approach, which involves home domains and logon certificates, is described in European Patent Application EP 0 695 985 A1, having priority based on U.S. application Ser. No. 277,144 filed Jul. 18, 1994 ("Logon Certificates Applications"), incorporated herein by reference. Logon certificates support disconnected operation in a distributed system. Each logon certificate is a secure package holding credentials information sufficient to establish the identity and access rights of a principal (a user or a machine) in a domain other than the principal's home domain. Access is enforced through means such as encryption and digital signatures. Logon certificates can be carried by the principal in convenient forms such as on a portable machine or on a floppy disk.

The relationship between a home domain and a distributed directory tree is not clear from the Logon Certificates Applications. The use of logon certificates is presented in the Logon Certificates Applications as an alternative to replicating credentials. Although credentials may be replicated in a distributed directory tree, however, replication is not required. More generally, domains and distributed directory trees differ in the services they provide, the hardware and software they require or allow, and in characteristics such as scalability and fault-tolerance.

However, a home domain and a distributed directory tree each define a context throughout which a given principal has identical access rights. Regardless of the location in the distributed directory tree at which the principal accesses the system, the principal has the same access rights. Similarly, a principal has the same access rights regardless of which location in the home domain is used to access the system. Indeed, if logon certificates are used, the principal will receive the same access rights regardless of whether the access attempt occurs inside the principal's home domain or outside that domain.

Uniformity of access rights simplifies the implementation of authentication methods, but in some situations more flexibility would be beneficial. For instance, a distributed system might contain both a home domain and a directory

tree, with each defining a given principal's access rights differently. It would be useful to provide the principal with a straightforward (from the principal's point of view) way to logon and use machines in the domain, machines in the directory tree, or both. Supporting different access rights for a given principal would also reduce the need to rapidly propagate changes to maintain uniform rights, thereby reducing the burden on domain controllers and directory tree administrators. However, such advances would require a distributed system that functions properly when different parts of the system have different access rights for a given principal, without using separate accounts.

Thus, it would be an advancement in the art to support multiple simultaneous access right contexts for a single principal in a distributed system.

It would be an additional advancement to provide such a method and system which is a compatible extension of known distributed directory tree and logon certificate approaches.

Such a method and system are disclosed and claimed herein.

BRIEF SUMMARY OF THE INVENTION

The present invention provides a method and system for managing security credentials in a distributed system where different locations in the system may contain different information about a principal's access rights. In one embodiment, the system is assumed to have a credential checking facility to authenticate one or more principals. A principal may be a human user. The principal may also be an agent such as a user's avatar or a system maintenance process or an information gathering "spider".

A method of the invention starts by providing the principal with a secure package in a first directory context. The secure package is provided by storing its contents in a buffer. Suitable buffers include RAM, floppy disks, hard disks, portable computers, hard tokens, removable storage media, and combinations of these individual buffers. The secure package contains information identifying the principal and also contains zero or more security credentials of the principal. The package has been at least partially encrypted or digitally signed or otherwise secured to discourage unauthorized disclosure or modification of the package contents. A "directory context" is a portion of the system throughout which the principal has identical access rights. A home domain is one of many possible examples of a directory context.

In a second directory context, the system receives an access request from the principal. The request may seek information about the system, access to information or other resources within the system, or use of the system to forward a message. The credential checking facility checks the access request by accessing the credentials in the secure package and comparing them with the system's internal security records. The system then allows or denies the access request according to the result of the credential check.

The system also determines whether credential information about the principal which is found in the second directory context was not placed in the secure package in the first directory context. If differences exist, the secure package may be modified to reflect the differences. Modification may involve digitally signing at least a portion of the secure package, such as principal identifying information and/or credentials in the secure package. Digital signatures, credentials, access rights, identifying information, and other information may be replaced, removed, or added. One

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.