



US006023765A

United States Patent [19]

[11] Patent Number: **6,023,765**

Kuhn

[45] Date of Patent: **Feb. 8, 2000**

[54] **IMPLEMENTATION OF ROLE-BASED ACCESS CONTROL IN MULTI-LEVEL SECURE SYSTEMS**

5,881,225 3/1999 Worth 395/186
5,898,781 4/1999 Shanton 380/25
5,911,143 6/1999 Deinhart et al. 707/103

[75] Inventor: **D. Richard Kuhn**, Columbia, Md.

FOREIGN PATENT DOCUMENTS

94112649 8/1994 European Pat. Off. .

[73] Assignee: **The United States of America as represented by the Secretary of Commerce**, Washington, D.C.

OTHER PUBLICATIONS

Ferraiolo and Kuhn, "Role-Based Access Controls" Proc. 15th NIST-NSA National Computer Security Conference (1992).

[21] Appl. No.: **08/975,159**

Primary Examiner—Robert W. Beausoliel, Jr.
Assistant Examiner—Nadeem Iqbal
Attorney, Agent, or Firm—Michael De Angeli P.C.

[22] Filed: **Nov. 20, 1997**

Related U.S. Application Data

[60] Provisional application No. 60/032,531, Dec. 6, 1996.

[51] **Int. Cl.**⁷ **G06F 13/00**; H04L 9/00

[52] **U.S. Cl.** **713/200**; 380/25

[58] **Field of Search** 713/200, 201, 713/202; 380/3, 4, 23, 25, 29; 707/104, 514, 103; 711/163; 395/728, 700, 800

[57] ABSTRACT

Role-based access control (RBAC) is implemented on a multi-level secure (MLS) system by establishing a relationship between privileges within the RBAC system and pairs of levels and compartments within the MLS system. The advantages provided by RBAC, that is, reducing the overall number of connections that must be maintained, and, for example, greatly simplifying the process required in response to a change of job status of individuals within an organization, are then realized without loss of the security provided by MLS.

[56] References Cited

U.S. PATENT DOCUMENTS

5,265,221	11/1993	Miller	395/725
5,347,578	9/1994	Duxbury	380/4
5,481,700	1/1996	Thurailingham	395/600
5,535,383	7/1996	Gower	395/600
5,577,209	11/1996	Boyle et al.	395/200.06
5,680,452	10/1997	Shanton	380/4
5,692,124	11/1997	Holden et al.	395/187.01
5,717,755	2/1998	Shanton	380/25
5,724,426	3/1998	Rosenow et al.	380/25
5,828,832	10/1998	Holden et al.	395/187.01
5,832,228	11/1998	Holden et al.	395/200.55
5,836,011	11/1998	Hambrick et al.	395/208
5,848,232	12/1998	Lermuzeaux et al.	395/187.01
5,859,966	1/1999	Hayman et al.	395/186

A trusted interface function is developed to ensure that the RBAC rules permitting individuals access to objects are followed rigorously, and provides a proper mapping of the roles to corresponding pairs of levels and compartments. No other modifications are necessary. Access requests from subjects are mapped by the interface function to pairs of levels and compartments, after which access is controlled entirely by the rules of the MLS system.

6 Claims, 4 Drawing Sheets

