



US005911143A

United States Patent [19]

[11] Patent Number: **5,911,143**

Deinhart et al.

[45] Date of Patent: ***Jun. 8, 1999**

[54] **METHOD AND SYSTEM FOR ADVANCED ROLE-BASED ACCESS CONTROL IN DISTRIBUTED AND CENTRALIZED COMPUTER SYSTEMS**

5,475,839	12/1995	Watson et al.	395/650
5,539,906	7/1996	Abraham et al.	395/600
5,564,016	10/1996	Korenshtien	395/186

OTHER PUBLICATIONS

[75] Inventors: **Klaus Deinhart**, Renningen, Germany; **Virgil Gligor**, Chevy Chase, Md.; **Christoph Lingenfelder**, Walldorf; **Sven Lorenz**, Stuttgart, both of Germany

Hartig et al., "Mechanisms for persistence and security in birlix", IEEE/INSPEC, pp. 309-318. May, 1990.

Born et al., "Discretionary access control by means of usage conditions", IEEE/INSPEC, pp. 437-450, vol.: 13, No. 5, Jan. 1994.

[73] Assignee: **International Business Machines Corporation**, Armonk, N.Y.

Hu et al., "User-role based security profiles for an object-oriented design model", IEEE/INSPEC, pp. 333-348, vol. A-21, Aug. 1992.

[*] Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

Hu et al., "User-role based security profiles for an object-oriented design model", Compendex Plus, issue: N. A-21, pp. 333-348, Aug. 1993.

(List continued on next page.)

[21] Appl. No.: **08/514,710**

Primary Examiner—Paul V. Kulik
Assistant Examiner—Jean M. Corrielus
Attorney, Agent, or Firm—Edward H. Duffield

[22] Filed: **Aug. 14, 1995**

[30] Foreign Application Priority Data

Aug. 15, 1994 [DE] Germany 94 112 649

[57] ABSTRACT

[51] **Int. Cl.⁶** **G06F 17/30**

A method and system for registration, authorization, and control of access rights in a computer system. Access rights of subjects on objects in a computer system are controlled using parameterized role types that can be instantiated into role instances equivalent to roles or groups. The required parameters are provided by the subject of the computer system, e.g. by a person, a job position, or an organization unit. Furthermore, relative resource sets are instantiated into concrete resource sets and individual resources by using the same parameter values as for instantiating the role types. Authorization and control of access rights include capability lists providing the access rights of the subjects on the objects of a computer system on a per subject basis. Furthermore, access control lists are derived from capability lists, so that access rights of the subjects on the respective objects are provided.

[52] **U.S. Cl.** **707/103; 707/104; 707/10; 707/9; 395/728; 395/800**

[58] **Field of Search** 395/614, 650, 395/728, 800, 700; 707/103, 104, 9, 10

[56] References Cited

U.S. PATENT DOCUMENTS

4,941,175	7/1990	Enescu et al.	380/23
5,113,442	5/1992	Moir	380/25
5,191,522	3/1993	Bosco et al.	364/401
5,315,657	5/1994	Adabi et al.	380/25
5,321,841	6/1994	East et al.	395/725
5,414,844	5/1995	Wang	395/650
5,414,852	5/1995	Kramer et al.	395/700
5,446,903	8/1995	Abraham et al.	395/725
5,450,593	9/1995	Howell et al.	395/650
5,469,556	11/1995	Clifton	395/490

11 Claims, 10 Drawing Sheets

