(19) österreichisches patentamt

(10) **AT 504 214 B1 2008-04-15**

(12) **Patentschrift**

(21) Anmeldenummer: A 6/2007

(22) Anmeldetag: 2007-01-03

(43) Veröffentlicht am: 2008-04-15

(51) Int. Cl.[8]: ***G06F 21/00*** (2006.01)

(56) Entgegenhaltungen:
US 6038563A DE 102004047146A1
WO 2005/091106A DE 10038779A1
EP 1282432A1 WO 2004/010271A2
WO 2001/67705A2

(73) Patentanmelder:
BERNHARD HANS-PETER DIPL.ING. DR.
A-4300 ST. VALENTIN (AT)

(54) VERFAHREN ZUR DYNAMISCHEN, DATENABHÄNGIGEN BESTIMMUNG UND ANWENDUNG VON BERECHTIGUNGEN IN HIERARCHISCHEN UND RELATIONALEN UMGEBUNGEN

(57) Der Zugriff auf Informationen, Baugruppen, o.ä. wird durch eine Berechtigungsstruktur gelöst, die Benutzern Zugriff auf Objektgruppen erlaubt oder verweigert. Die Gruppen können Gruppen in einer hierarchischen Struktur sein oder auf Grund ihrer Eigenschaft ermittelt werden. Alle Objekte sollen in einer linearen Anordnung (Tabelle, Liste) vorhanden sein um zu vermeiden, dass Redundanzen oder Doubletten zu einer nicht eindeutigen Situation (Entity Anomalie) führen. Die Objekte verschiedener eindeutiger Listen werden variabel kombiniert, um Gesamtgeräte unterschiedlicher Funktionalität oder unterschiedliche Informationsdarstellungen zu erzeugen. Abhängig von Gerät oder Informationsdarstellung und Benutzer ergeben sich unterschiedliche Berechtigungen.

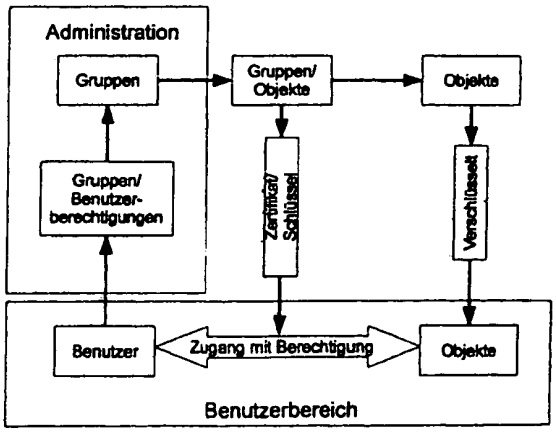

Abbildung 1: Berechtigungssystem

AT 504 214 B1 2008-04-15

Gegenstand der Erfindung ist ein Verfahren zur dynamischen und datenabhängigen Bestimmung und Anwendung von Berechtigungen in hierarchischen und relationalen Umgebungen, bestehend aus einer geeigneten Zusammenschaltung von elektronischen oder informationstechnischen Authentifizierungssystemen, einem Kryptographie- oder Kodiersystem und einem hierarichisch organisierten relationalen System (beispielsweise elektronisches Schließsystem, Multiuserdatenbanken oder Schalt- und Baugruppenpläne etc.).

Es sind verschiedene Verfahren zur Bestimmung und Anwendung von Berechtigungen bekannt: Eintragen der Berechtigungen in eine Zugriffsliste (ACL Access Control List) pro Objekt. Vererben von Berechtigungen eines übergeordneten Objektes an untergeordnete Objekte (IACL Inherited Access Control List). Gesteuerte Berechtigungen (SACL Scripted Access Control List), bei denen über ein Regelsystem (Script, Programm, Verdrahtung) für jedes Objekt die speziellen Berechtigungen bestimmt werden und einige mehr. Auf diese Verfahren wird nicht näher eingegangen, da sie als allgemein bekannt vorausgesetzt werden können.

Dem Erfinder ist das Patent US 6 038 563 A (Bapat et al.) bekannt, in dem die Objekte einer Datenbank über Zertifikatstabellen verwaltet werden. Die Tabellen entsprechen nicht dem dynamischen Zugriff, der in Anspruch 1 beschrieben ist.

Dem Erfinder ist das Patent DE 10 2004 047 146 A1 (Bayer Business Services GmbH) bekannt, das sich im Gegensatz zu Anspruch 1, auf das Verfahren zur Rechteverwaltung bezieht.

Dem Erfinder ist das Patent WO 2005/091106 A1 (Siemens Aktiengesellschaft) bekannt, das ein Programm beschreibt, mit dem Berechtigungen geprüft und gesetzt werden und nicht, wie in Anspruch 1, die Objekte selbst mit einer Verschlüsselung ausgestattet sind.

Dem Erfinder ist das Patent DE 100 38 779 A1 (Schneider Automation GmbH) bekannt, das nur die Übertragung von oder zu einem Steuergerät betrachtet.

Dem Erfinder ist das Patent EP 1 282 432 A1 (Swisscom AG) bekannt, das ein Zertifikats-Auskunftssystem darstellt und nicht wie in Anspruch 1 niedergelegt, die Verwendung der Zertifikate zur Indizierung.

Dem Erfinder ist das Patent WO 2004/010271 A2 (Eoriginal Inc.) bekannt, das sich auf ein Dokumentenmanagement-System bezieht, mit dem die Dokumente signiert werden und man so deren Gültigkeit feststellen kann.

Dem Erfinder ist das Patent WO 2001/67705 A2 (Herbert Street Technologies Ltd.) bekannt, das lediglich ein Datentransfer- und Managementsystem darstellt. Dieses System hat mit dem vom Erfinder beschriebenen System nichts zu tun, weil es sich nicht auf die Berechtigungsverwaltung, sondern auf den Datentransfer bezieht.

Die gegenständliche Erfindung vermeidet, im Gegensatz zu den bekannten Verfahren, dass ein Objekt im Gesamtsystem mit nur einem bestimmten Satz von Berechtigungen pro Teilnehmer ausgestattet werden kann. Weiters ist es möglich, die Vorteile von hierarchischen und relationalen Systemen zu verbinden.

Der Erfindung liegt die Aufgabe zugrunde, in systematischer Art und Weise Zugriff auf Informationen, Baugruppen o.ä., im weiteren als Objekte bezeichnet, zu ermöglichen. Alle Objekte sollen in einer linearen Anordnung (Tabelle, Liste) vorhanden sein um zu vermeiden, dass Redundanzen oder Doubletten zu einer nicht eindeutigen Situation (Entity Anomalie) führen. Die Objekte verschiedener eindeutiger Listen werden variabel kombiniert, um Gesamtgeräte unterschiedlicher Funktionalität oder unterschiedliche Informationsdarstellungen zu erzeugen. Abhängig vom Gerät oder von Informationsdarstellung und Benutzer ergeben sich unterschiedliche Berechtigungen. Diese Zusammenstellungen muss man in einem hierarchischen System

abbilden.

Der Erfindung liegt die Aufgabe zugrunde, in ein und der selben Liste befindliche Objekte von verschiedenen Benutzern verwendbar zu machen. In dieser Tabelle werden die Berechtigungen disjunkt vergeben. Ein Benutzer darf bestimmte Objekte lesen und bestimmte verändern. Für einen anderen Benutzer muss eine andere Konfiguration der Berechtigungen möglich sein.

Der Erfindung liegt die Aufgabe zugrunde, eine leicht zu modifizierende Rechtestruktur zu ermöglichen, die z.B. ein und die selbe Baugruppe im Entwurfsfall eines elektronischen Regelsystems für den Entwickler in seinen Eigenschaften veränderbar macht und im Falle des Produktivgerätes nur mehr einen lesenden Zugriff erlaubt.

Vorteilhaft gegenüber allen anderen bekannten Verfahren ist hier, dass die Informationen über Berechtigungen abseits der Liste oder Tabelle definiert sind, sodass bezüglich des Objekteinsatzes völlige Freiheit besteht. Die Berechtigungen werden nicht wie bei z.B. herkömmlichen relationalen Datenbanken als Berechtigung für Tabellen gespeichert, wobei nur die Attribute der Objekte der gesamten Tabelle lesbar oder schreibbar sein können. Die Berechtigungen werden nicht wie bei hierarchischen Systemen in einem Hierarchieknoten gespeichert und die Objekte in diese Hierarchiestufe kopiert, woraus die Gefahr von Ambiguitäten resultiert, wie in EDV-Verzeichnissystemen üblich. In bekannten Verfahren werden Objekte von einem in den anderen Kontext transferiert, um unterschiedliche Zugriffsberechtigungen zu erzielen, dadurch ergibt sich, dass in dem einen Kontext das Objekt verschwindet, um im anderen Kontext vorhanden zu sein. Vorteilhaft gegenüber diesem Verfahren ist, dass die Objekte nicht von einem Kontext in den anderen Kontext transportiert werden, wodurch ein gleichzeitiges Darstellen unter unterschiedlichen Voraussetzungen möglich ist.

Nach einem vorteilhaften Merkmal der Erfindung ist vorgesehen, dass die Information über die Berechtigungen nicht beim Objekt abgespeichert werden, sondern in der Beziehung zwischen Objekt und Betrachter oder einem obergeordneten Hierarchieelement. Dadurch wird eine Trennung in Objektdaten und Berechtigungsdaten möglich. Dabei ist es unerheblich, ob dies in Zusammenhang mit einer Datenbank, einem elektronischen System oder einer organisatorischen Einheit steht.

Ein Ausführungsbeispiel des Verfahrens ist in Zeichnung 1 und der folgenden Beschreibung dargestellt. Es zeigt:

In Zeichnung 1 ist beispielhaft eine Anwendung auf ein Berechtigungsystem eines RDBMS (Relationalen Datenbank Management Systems) dargestellt. Dabei handelt es sich um den Zugriff eines beliebigen Benutzers auf eine Tabelle mit Objekten. Der Benutzer hat nur Zugang zum Benutzerbereich und so auch nur zu den verschlüsselten Objektdaten, die er mit Hilfe des für ihn erzeugten Zertifikates entschlüsseln kann.

Die Administration erfolgt im Administrationsbereich, in dem Benutzerberechtigungen beliebiger Art bestimmten Gruppen zugeordnet werden. Unter Gruppen versteht man in diesem Zusammenhang Gruppen von Objekten der betrachteten Tabelle, beispielsweise alle rechteckigen Objekte.

Das RDBMS erstellt nun ein Benutzerzertifikat und eine passende Verschlüsselung für die Objektgruppe aus der Tabelle mit Objekten und wendet die Verschlüsselung auf diese Objekte an. Die so erzeugten Daten werden dem Benutzer zugänglich gemacht.

Für die Verschlüsselung können beliebig komplizierte oder einfache unsymmetrische Schlüssel (RSA, MD5, ...) verwendet werden, es muss nur sicher gestellt sein, dass diese den Geschwindigkeits- und Sicherheitsanforderungen genügen.

Bei einer neuerlichen Abfrage werden alle Zertifikate und Schlüssel neu erzeugt, sodass die erhaltenen Daten nur im Moment des Abfragens uneingeschränkte Gültigkeit haben. Wenn sich die Berechtigungen ändern, werden im Moment des Änderns alle weiteren Abfragen mit den richtigen Berechtigungen abgearbeitet.

Patentanspruch:

Verfahren zur dynamischen datenabhängigen Bestimmung und Anwendung von Berechtigungen in hierarchischen und relationalen Umgebungen, *dadurch gekennzeichnet*, dass die Berechtigung Objekte zu lesen oder zu modifizieren über ein Zugangszertifikat gesteuert wird, wobei der Zugriff mit Hilfe des Zertifikates transparent für den Benutzer erfolgt mit einem Zertifikat, das datenabhängig erstellt wird, sodass der Benutzer nur die für ihn erlaubten Aktionen, lesen, schreiben, modifizieren, löschen, auf erlaubten Objekten anwenden kann, mit der wesentlichen Eigenschaft, dass die Berechtigungen in einer Berechtigungsreferenz niedergelegt werden, die dem Benutzer nicht zugänglich ist und die Selektion der Objekte mit dem zur Verfügung gestellten Schlüssel erfolgt.

Hiezu 1 Blatt Zeichnungen

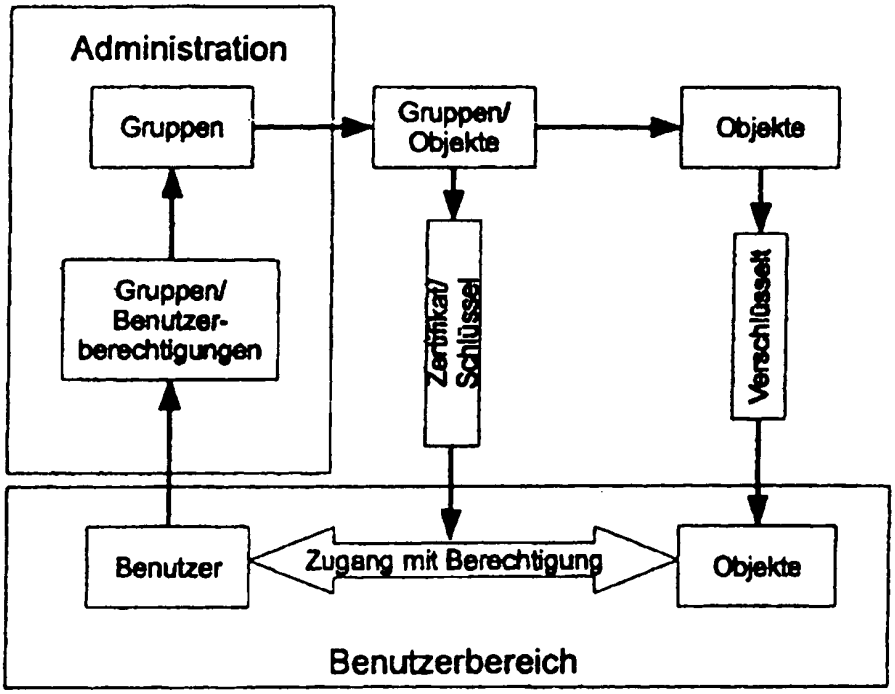

Abbildung 1: Berechtigungssystem