(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 699 29 772 T2** 2006.11.09

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 058 873 B1**
(21) Deutsches Aktenzeichen: **699 29 772.9**
(86) PCT-Aktenzeichen: **PCT/US99/04550**
(96) Europäisches Aktenzeichen: **99 909 745.4**
(87) PCT-Veröffentlichungs-Nr.: **WO 1999/045456**
(86) PCT-Anmeldetag: **02.03.1999**
(87) Veröffentlichungstag der PCT-Anmeldung: **10.09.1999**
(97) Erstveröffentlichung durch das EPA: **13.12.2000**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **08.02.2006**
(47) Veröffentlichungstag im Patentblatt: **09.11.2006**

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

(30) Unionspriorität:
35234 **03.03.1998** **US**

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE

(73) Patentinhaber:
Network Appliance, Inc., Sunnyvale, Calif., US

(74) Vertreter:
Klunker, Schmitt-Nilson, Hirsch, 80797 München

(72) Erfinder:
HITZ, David, Portola Valley, CA 94028, US; BORR, Andrea, Los Gatos, CA 95033, US; HAWLEY, J., Robert, San Jose, CA 95120-4037, US; MUHLESTEIN, Mark, Morgan Hill, CA 95037, US; PEARSON, Joan, Menlo Park, CA 94025, US

(54) Bezeichnung: **DATEIZUGRIFFSTEUERUNG IN EINEM MEHRFACHPROTOKOLL-DATEI-SERVER**

Beschreibung

Hintergrund der Erfindung

1. Gebiet der Erfindung

[0001] Die Erfindung betrifft eine Dateizugriffssteuerung in einem Mehrfachprotokoll-Dateiserver.

2. Stand der Technik

[0002] In einem integrierten Computernetzwerk ist es für vielfältige Client-Einrichtungen wünschenswert, einen Zugriff auf die gleichen Dateien zu teilen. Ein bekanntes Verfahren ist, einen Netzwerkdateiserver zum Speichern von Dateien bereitzustellen, der im Stande ist, Dateiserveranfragen von diesen Client-Einrichtungen zu empfangen und zu beantworten. Diese Dateiserveranfragen werden unter Verwendung eines Dateiserverprotokolls erzeugt, das sowohl von dem Dateiserver als auch von der Client-Einrichtung erkannt und befolgt wird. Weil die Dateien auf dem Dateiserver gespeichert sind, haben vielfältige Client-Einrichtungen die Möglichkeit, einen Zugriff auf die gleichen Dateien zu teilen.

[0003] In einem Dateisystem, das zur Verwendung durch mehr als einen Benutzer vorgesehen ist, ist es wünschenswert, durch Programme einen Zugriff auf Dateien auf dem Dateisystem einzuschränken. Ein eingeschränkter Zugriff umfasst wenigstens den Aspekt der (1) Benutzerauthentisierung – Ermitteln, dass die anfragenden Benutzer wirklich diejenigen sind, die sie vorgeben zu sein, und (2) der Zugriffssteuervalidierung – Ermitteln, dass es einem authentisierten Benutzer erlaubt ist, auf eine bestimmte Datei in einer bestimmten Weise zuzugreifen. Wenn das Dateisystem auf einem Dateiserver geführt wird, der entfernt von dem Benutzer, der die Anfrage durchführt, ist, gibt es einen zusätzlichen Aspekt des Zugriffssteuerprotokolls – welche Anfragen können von dem Benutzer zum Zugriff auf Dateien oder um eine Zugriffssteuerung für Dateien einzustellen gemacht werden.

[0004] Ein Problem im Stand der Technik ist, dass es vielfältige diverse Modelle zur Zugriffssteuervalidierung gibt, wobei jedes typischerweise mit einem bestimmten Dateisystem verknüpft ist, und es gibt vielfältige diverse Zugriffssteuerprotokolle, wobei jedes typischerweise mit einem Modell zur Zugriffssteuervalidierung korrespondiert. Abgesehen von den Unterschieden zwischen diesen Modellen und Protokollen sollte der Dateiserver auf Dateiserveranfragen von jedem Benutzer antworten und ein Zugriffssteuervalidierungsverhalten zeigen, dass mit jedem Modell eines Benutzers konsistent ist und ohne Sicherheitsverletzungen oder Überraschungen für Benutzer ist.

[0005] Zum Beispiel ist ein erstes Zugriffssteuermodell, welches häufig verwendet wird, mit dem Unix-Betriebssystem (oder einer Variante davon) verknüpft. Dieses erste Zugriffssteuermodell verknüpft Berechtigungen mit jeder Datei für einen Dateibesitzer, für eine Gruppe des Besitzers und für alle anderen Benutzer. Diese Berechtigungen erlauben einen Zugriff (für den Besitzer, die Gruppe oder alle anderen Benutzer) zum Lesen, Schreiben oder Ausführen der betreffenden Datei. Dieses erste Zugriffssteuermodell wird typischerweise durch das NFS-Dateiserverprotokoll („Network File System")implementiert, das möglicherweise durch ein zusätzliches Dateisperrprotokoll erweitert ist, NLM („Network Lock Manager"). Ein zweites Zugriffssteuermodell, das häufig verwendet wird, ist mit dem Windows-NT-Betriebssystem verknüpft. Dieses zweite Zugriffssteuermodell verknüpft eine ACL („Access Control List") mit jeder Datei, wobei jeder Eintrag in der ACL einen individuellen Benutzer, eine Gruppe von Benutzern oder alle Benutzer spezifiziert. Jeder Eintrag kann einen Zugriff (für die spezifizierten Benutzer) zum Schreiben, Lesen oder Ausführen der betreffenden Datei erlauben, oder kann einen Zugriff spezifisch versagen. Dieses zweite Zugriffssteuermodell wird typischerweise durch das CIFS-Protokoll („Common Internet File System") implementiert. Jedoch können NT-Einrichtungen mittels der „PC NFS"-Implementierung auch das NFS-Protokoll benutzen und Unix-Einrichtungen können auch POSIX-ACLs manipulieren. Diese beiden Zugriffssteuermodelle, die häufig verwendet werden, unterscheiden sich in wesentlichen Punkten, umfassend, (1) welche Berechtigungen einer Datei zugewiesen werden können, (2) mit welcher Genauigkeitsgranularität Berechtigungen zugewiesen werden können und (3) wie Benutzer identifiziert werden, um sie mit Berechtigungen abzugleichen.

[0006] Ein im Stand der Technik bekanntes Verfahren ist, einen Mehrfachprotokoll-Dateiserver bereitzustellen, der sämtliche Sicherheitssemantik auf diejenige eines einzelnen nativen Betriebssystems für den Dateiserver abbildet und dieses einzelne native Betriebssystem verwendet, um die Dateizugriffssteuerung zu validieren. Dem „Samba"-System und ähnlichen Emulationspaketen wird zugestanden, dieses bekannte Verfahren zu verwenden. Dieses bekannte Verfahren hat den Nachteil, dass es in Sicherheitsfehlern oder Überraschungen für diejenigen Client-Einrichtungen resultieren kann, die eine andere Sicherheitssemantik verwenden, als das native Betriebssystem des Dateiservers.

[0007] Ein weiteres im Stand der Technik bekanntes Verfahren ist, einen Mehrfachprotokoll-Dateiserver bereitzustellen, der unterschiedliche Typen von Sicherheitssemantiken für unterschiedliche Dateien unterstützt, aber versucht, eine Dateizugriffssteuerung für jeden Benutzer unter Verwendung des Zu-

griffssteuermodells des Benutzers zu validieren. Einige „Netware"-Produkte, die von Novell Corporation erhältlich sind, wird zugestanden, dieses bekannte Verfahren zu verwenden. Dieses bekannte Verfahren hat den Nachteil, dass das Zugriffssteuermodell des Benutzers wesentlich von dem Zugriffssteuermodell abweichen kann, das für die Datei eingestellt ist, was in Sicherheitsfehlern oder Überraschungen für diejenigen Client-Einrichtungen resultiert, die andere Sicherheitssemantiken verwenden, als sie mit der Zieldatei verknüpft sind.

[0008] US 5,675,782 offenbart ein Verfahren und ein System zum Steuern von Einheiten auf einem Netzwerk, auf dem eine Vielzahl von Servern installiert sind, die verschiedene Betriebssysteme verwenden. Eine Anfrage wird durch einen Benutzer an einer Workstation auf dem Netzwerk eingegeben, um Zugriffsberechtigungen im Hinblick auf eine vertrauenswürdige Stelle für eine Einheit auf dem Netzwerk einzustellen. In Reaktion auf die Anfrage werden verschiedene Anwendungsprogrammierungsschnittstellen aufgerufen, um die generische Anfrage zum Einstellen von Berechtigungen auf der Einheit in ein Format zu übersetzen, das für das Betriebssystem geeignet ist, das die Einheit steuert. Einheiten sind entweder Software, wie zum Beispiel Verzeichnisse und Dateien, oder Hardware, wie zum Beispiel Drucker.

[0009] Dementsprechend wäre es wünschenswert, ein Verfahren und ein System zum Durchsetzen einer Dateisicherheitssemantik zwischen Client-Einrichtungen bereitzustellen, die vielfältige, diverse Zugriffssteuermodelle und vielfältige diverse Dateiserverprotokolle verwenden. Dieser Vorteil wird in einer Ausführungsform der Erfindung erreicht, in welcher ein Mehrfachprotokoll-Dateiserver jede Datei mit einem bestimmten Zugriffssteuermodell aus einer Vielzahl von möglichen Zugriffssteuermodellen identifiziert und dieses bestimmte Zugriffssteuermodell für alle Zugriffe auf diese Datei durchsetzt. Wenn der Dateiserver eine Dateiserveranfrage für diese Datei unter Verwendung eines Dateiserverprotokolls mit einem unterschiedlichen Zugriffssteuermodell empfängt, übersetzt der Dateiserver die Zugriffssteuereinschränkungen, die durch das Zugriffssteuermodell der Datei gegeben sind, in nicht weniger restriktive Zugriffssteuereinschränkungen in dem unterschiedlichen Zugriffssteuermodell. Der Dateiserver beschränkt einen Zugriff auf die Datei unter Verwendung der übersetzten Zugriffssteuereinschränkungen.

Zusammenfassung der Erfindung

[0010] Gemäß eines Aspekts der Erfindung wird ein Verfahren zum Betreiben eines Dateiservers bereitgestellt, gekennzeichnet durch die Schritte:
Identifizieren einer ersten Datei auf dem Dateiserver mit einem ersten Zugriffssteuermodell, das aus einer Vielzahl von Zugriffssteuermodellen ausgewählt wird, die auf dem Dateiserver implementiert sind, wobei der Dateiserver eine Vielzahl von Dateien beinhaltet, von welchen wenigstens einige mit verschiedenen Zugriffssteuermodellen verknüpft sind;
Identifizieren der ersten Datei mit einem zweiten Zugriffssteuermodell in Reaktion auf eine Dateiserveranfrage; und
Durchsetzen des ersten Zugriffssteuermodells für alle Zugriffe auf die erste Datei, wobei ein Zugriff auf die erste Datei nur in Reaktion auf eine Anfrage erlaubt wird, welche Berechtigungen in dem ersten Zugriffssteuermodell genügt.

[0011] Ein weiterer Aspekt der Erfindung ist ein Dateiserver, wie er in Anspruch 20 definiert ist. Weitere Ausführungsformen der Erfindung sind in den entsprechenden abhängigen Ansprüchen spezifiziert.

[0012] Wenn der Dateiserver eine Dateiserveranfrage für diese Datei unter Verwendung eines verschiedenen Zugriffssteuermodells empfängt, übersetzt der Dateiserver die Zugriffssteuereinschränkungen für diese Datei in nicht weniger restriktive Einschränkungen in dem verschiedenen Modell.

[0013] Der Dateiserver schränkt einen Zugriff durch die Client-Einrichtung unter Verwendung der übersetzten Zugriffssteuereinschränkungen ein.

[0014] In einer bevorzugten Ausführungsform wird jeder Datei das Zugriffssteuermodell des Benutzers zugeordnet, der die Datei erzeugt hat oder der als letztes Zugriffssteuereinschränkungen für die Datei eingestellt hatte. Wenn ein Benutzer mit einem unterschiedlichen Zugriffssteuermodell Zugriffssteuereinschränkungen einstellt, wird das Zugriffssteuermodell für die Datei in das neuen Modell geändert. Dateien sind in einer Baumhierarchie organisiert, in der jeder Baum auf eins oder mehrere Zugriffssteuermodelle eingeschränkt ist (was die Fähigkeit von Benutzer einschränken kann, Zugriffssteuereinschränkungen für Dateien in dem Baum einzustellen). Jeder Baum kann auf ein Nur-NT-Modell-Format, ein Nur-Unix-Modell-Format oder ein gemischtes NT-oder-Unix-Modell-Format eingeschränkt werden.

Kurze Beschreibung der Zeichnungen

[0015] Die Zeichnung zeigt ein Blockdiagramm eines Systems zum Durchsetzen diverser Zugriffssteuermodelle unter Client-Einrichtungen.

Detaillierte Beschreibung der bevorzugten Ausführungsform

[0016] In der folgenden Beschreibung wird eine bevorzugte Ausführungsform der Erfindung im Hinblick auf bevorzugte Prozessschritte und Datenstrukturen beschrieben. Jedoch erkennt der Fachmann nach ei-

ner Prüfung dieser Anmeldung, dass Ausführungsformen der Erfindung unter Verwendung eines oder mehrerer Allzweckprozessoren (oder Spezialprozessoren, die auf die bestimmten Prozessschritte und Datenstrukturen angepasst sind), die unter einer Programmsteuerung betrieben werden, implementiert werden können, und dass eine hier beschriebene Implementierung der bevorzugten Prozessschritte und Datenstrukturen, die eine solche Ausrüstung verwendet, keine übermäßigen Experimente oder eine weitere Erfindung erfordert.

Systemelemente

[0017] Die Figur zeigt ein Blockdiagramm eines Systems zum Durchsetzen diverser Zugriffssteuermodelle unter Client-Einrichtungen.

[0018] Ein System **100** umfasst einen Dateiserver **110** und eine Menge von Client-Einrichtungen **120**.

[0019] Der Dateiserver **110** hält ein Dateisystem **111**, welches eine Menge von Dateien **112** umfasst.

[0020] Der Dateiserver **110** ist eingerichtet, Dateiserveranfragen **121** von den Client-Einrichtungen **120** zu empfangen. Der Dateiserver **110** analysiert die Syntax (engl.: to parse) jeder Anfrage **121**, ermittelt, ob die in der Anfrage **121** angefragte Operation erlaubt ist (für die Client-Einrichtung **120**, die die Anfrage **121** gesendet hat, und für die eine oder die mehreren Zieldateien **112**, die in der Anfrage **121** spezifiziert sind). Falls sie erlaubt ist, führt der Dateiserver **110** diese Operation auf der einen oder den mehreren Zieldateien **112** durch.

[0021] Der Dateiserver **110** ist auch eingerichtet, um Dateiserverantworten **122** an die Client-Einrichtungen **120** zu übertragen. Der Dateiserver **110** ermittelt die Antwort auf jede Anfrage **121** (möglicherweise umfassend eine Antwort, die anzeigt, dass die angefragte Operation nicht erlaubt war), erzeugt diese Antwort **122** und überträgt die Antwort **122** an die Client-Einrichtung **120**, die die Anfrage **121** gesendet hatte.

[0022] Jede Client-Einrichtung **120** ist eingerichtet, Dateiserveranfragen **121** an den Dateiserver **110** zu übertragen und Dateiserverantworten **122** von dem Dateiserver **110** zu empfangen.

Zugriffssteuermodelle

[0023] In einer bevorzugten Ausführungsform kann jede Client-Einrichtung **120** entweder eine Unix-Client-Einrichtung **120** oder eine Windows-NT-Client-Einrichtung **120** sein. Jede Client-Einrichtung **120** kann entweder das NFS-Dateiserverprotokoll verwenden, um Anfragen **121** zu machen, oder das CIFS-Dateiserverprotokoll verwenden, um Anfragen **121** zu machen. (Obwohl typischerweise Unix-Client-Einrichtungen **120** das NFS-Dateiserverprotokoll verwenden und NT-Client-Einrichtungen **120** das CIFS-Dateiserverprotokoll verwenden, ist es für NT-Client-Einrichtungen **120** möglich, das NFS-Dateiserverprotokoll unter Verwendung der PC-NFS-Implementierung dieses Dateiserverprotokolls zu verwenden.) Der Dateiserver **110** empfängt jede Anfrage **121** und führt (falls erlaubt) die angefragte Operation auf den Zieldateien **112** durch, die durch die Anfrage **121** spezifiziert werden.

[0024] Der Dateiserver **110** unterstützt mehr als ein Zugriffssteuermodell, umfassend ein „Unix Perms"-Zugriffssteuermodell (hier „Unix-Sicherheitsausführung") und ein „NT-ACL"-Zugriffssteuermodell (hier „NT-Sicherheitsausführung").

[0025] Die Unix-Sicherheitsausführung verwendet Benutzer-IDs (UIDs), um Benutzer zu identifizieren, und Gruppen-IDs (GIDs), um Gruppen zu identifizieren, zu denen diese Benutzer gehören. Die Unix-Sicherheitsausführung verknüpft die folgenden Zugriffssteuereinschränkungen mit jeder Datei:

- eine UID für den Besitzer;
- eine GID für den Besitzer;
- eine Menge von „Benutzer"-Berechtigungen – die dem Benutzer, dem die Datei gehört, eine Berechtigung zum Lesen, Schreiben oder Ausführen der Datei erteilen;
- eine Menge von „Gruppen"-Berechtigungen – die der Gruppe des Benutzers, dem die Datei gehört, Berechtigungen zum Lesen, Schreiben oder Ausführen der Datei erteilen; und
- eine Menge von „anderen" Berechtigungen – die allen anderen Benutzern eine Berechtigung zum Lesen, Schreiben oder Ausführen der Datei erteilen.

[0026] Die Unix-Sicherheitsausführung wird von dem NFS-Dateiserverprotokoll („Network File System") unterstützt, welches möglicherweise durch das zusätzliche NLM-Dateisperrprotokoll („Network Lock Manager") erweitert ist.

[0027] NFS ist ein zustandsloses Protokoll, so dass jede NFS-Dateiserveranfrage **121** die UIDs und GIDs des Benutzers umfasst, der die Anfrage macht. Die Unix-Client-Einrichtung **120** ermittelt zur Login-Zeit für den Benutzer die UIDs und GIDs des Benutzers durch Bezugnahme auf die Passwortdatei (/etc/passwd) und die Gruppendatei (/etc/groups) des Systems.

[0028] Um eine Dateizugriffssteuerung durchzusetzen, die eine Unix-Sicherheitsausführung verwendet, ermittelt der Dateiserver **110**, ob die Anfrage **121** von dem besitzenden Benutzer, von einem Benutzer in der Gruppe des besitzenden Benutzers oder von einem anderen Benutzer stammt. In Reaktion auf diese

Ermittlung verwendet der Dateiserver **110** eine der Benutzerberechtigungen, der Gruppenberechtigungen oder der anderen Berechtigungen, um zu ermitteln, ob die Anfrage erlaubt wird.

[0029] Die NT-Sicherheitsausführung verwendet Sicherheits-IDs (SIDs), um sowohl Benutzer und als auch Gruppen zu identifizieren. Die NT-Sicherheitsausführung verknüpft die folgenden Zugriffssteuereinschränkungen mit jeder Datei:

– eine SID für den Besitzer;
– eine SID für die Gruppe des Besitzers;
– eine ACL (Zugriffssteuerliste).

[0030] Die NT-ACL umfasst einen oder mehrere ACEs (Zugriffssteuereinträge), von denen jeder eine SID umfasst, die den Benutzer oder die Gruppe angibt, zu welcher sie gehört, und eine Menge von Berechtigungen. Die NT-Sicherheitsausführung sieht die drei Unix-Berechtigungen (Lesen, Schreiben oder Ausführen) sowie eine „ÄNDERE-BERECHTIGUNGEN"-Berechtigung, eine „ÜBERNEHME-BESITZ"-Berechtigung, eine „LÖSCHE"-Berechtigung, eine „LÖSCHE NACHFOLGER"-Berechtigung und andere Berechtigungen vor.

[0031] Die NT-Sicherheitsausführung wird von dem CIFS-Protokoll („Common Internet File System") unterstützt. Die NT-Sicherheitsausführung wird in den folgenden Artikeln weiter beschrieben: R. Reichel, „Inside Windows NT Security", Windows/DOS Developers' Journal (April und Mai 1993), und in Stephen Sutton, „Windows NT Security Guide" (ISBN 0201419696).

[0032] CIFS ist ein Session-basiertes Protokoll, so dass die NT-Client-Einrichtung **120** zur Session-Verbindungszeit den NT-Benutzernamen und das Passwort an den Dateiserver **110** überträgt, anhand derer die SIDs für den Benutzer und die Gruppen des Benutzers ermittelt werden. Der Dateiserver **110** kann versuchen, den Benutzer selbst zu authentisieren oder (vorzugsweise) den NT-Benutzernamen und das Passwort an einen NT-Primär-Domain-Controller weiterzuleiten.

[0033] Um eine Dateizugriffssteuerung unter Verwendung der NT-Sicherheitsausführung durchzusetzen, ermittelt der Dateiserver **110** für den Benutzer, der die Anfrage **121** macht, die SID für den Benutzer und die Gruppe des Benutzers. Der Dateiserver **110** sammelt Berechtigungen, die diesen von betreffenden ACEs erteilt werden, wobei dann die Berechtigungen subtrahiert werden, die diesem Benutzer spezifisch verweigert wurden. In Reaktion auf diese Sammlung und Subtraktion, ermittelt der Dateiserver **110**, ob die Anfrage **121** erlaubt ist.

[0034] Obwohl eine bevorzugte Ausführungsform der Erfindung im Hinblick auf die Unix-Sicherheitsausführung und die NT-Sicherheitsausführung beschrieben ist, kann die Erfindung leicht mit anderen Zugriffssteuermodellen verwendet werden, wie zum Beispiel dem „POSIX-ACL"-Zugriffssteuermodell, das von einigen Unix-Einrichtungen und von einigen anderen Betriebssystemen unterstützt wird. Die Konzepte und Merkmale der hierin beschriebenen Erfindung können leicht in einem Dateiserver **110** verwende werden, der das „POSIX-ACL"-Zugriffssteuermodell zusätzlich zu oder anstelle der hier im Detail beschriebenen Steuermodelle verwendet, ohne dass eine weitere Erfindung oder übermäßige Experimente durchgeführt werden.

[0035] Der Dateiserver **110** bestimmt, dass jede Datei **112**, die in seinem Dateisystem **111** gehalten wird, ein spezifisches Zugriffssteuermodell aus der Vielzahl von Zugriffssteuermodellen hat, die er unterstützt. In einer bevorzugten Ausführungsform ist jede Datei **112** bestimmt, entweder die Unix-Sicherheitsausführung oder die NT-Sicherheitsausführung zu verwenden. Der Dateiserver **110** setzt die bestimmte Sicherheitsausführung für jede Datei **112** für alle Versuche durch, auf diese Datei **112** zuzugreifen. Somit setzt der Dateiserver **110** die bestimmte Sicherheitsausführung für alle Anfragen **121** durch, die für diese Zieldatei **112** gemacht werden, ob diese Anfragen **121** von Unix-Einrichtungen oder NT-Einrichtungen kommen und ob diese Anfragen **121** das NFS-Dateiserverprotokoll oder das CIFS-Dateiserverprotokoll verwenden.

Durchsetzung der Zugriffssteuerung

[0036] Falls der Dateiserver **110** eine Anfrage **121** für eine Zieldatei **112** erhält und die Anfrage **121** mit der Sicherheitsausführungszieldatei **112** übereinstimmt, validiert der Dateiserver **110** die Anfrage **121** gegenüber Zugriffssteuereinschränkungen für diese Datei **112**, die von dieser Sicherheitsausführung auferlegt sind.

[0037] Der Dateiserver **110** erkennt somit und setzt wenigstens die folgenden Umstände durch:

– NT-Sicherheitsausführung. Die Datei **112** hat eine NT-Sicherheitsausführung und hat eine zugehörige Menge von Zugriffssteuereinschränkungen (eine NT-ACL), die durch eine Client-Einrichtung **120** unter Verwendung des CIFS-Dateiserverprotokolls eingestellt wurden.

[0038] Falls eine Client-Einrichtung **120** eine Anfrage **121** macht, um auf die Datei **112** unter Verwendung des CIFS-Dateiserverprotokolls zuzugreifen, setzt der Dateiserver **110** die NT-ACL unter Verwendung der NT-Sicherheitsausführung durch, falls er dazu im Stande ist.

[0039] Falls der Dateiserver **110** im Stande ist, den NT-Benutzer entweder durch eine Kommunikation

mit einem NT-Domain-Controller oder durch Bezugnahme auf eine NT-Benutzer-SID-Datenbank (Sicherheits-ID) zu ermitteln, ist der Dateiserver **110** im Stande, die NT-ACL unter Verwendung der NT-Sicherheitsausführung durchzusetzen.

[0040] Falls der Dateiserver **110** nicht im Stande ist, den NT-Benutzer zu ermitteln, ermittelt er den äquivalenten Unix-Benutzer unter Verwendung einer UID für einen Unix-Benutzer, der für die CIFS-Dateiserverprotokoll-Session aufgezeichnet ist, und setzt die NT-ACL durch, so als ob die Anfrage **121** von diesem Unix-Benutzer kommt.

– Unix-Sicherheitsausführung. Die Datei **112** hat eine Unix-Sicherheitsausführung und hat eine entsprechende Menge von Zugriffssteuereinschränkungen (Unix-Perms), die durch eine Client-Einrichtung **120** unter Verwendung des NFS-Dateiserverprotokolls eingestellt wurden.

[0041] Falls eine Client-Einrichtung **120** eine Anfrage **121** macht, um auf die Datei **112** unter Verwendung des NFS-Dateiserverprotokolls zuzugreifen, setzt der Dateiserver **110** die Unix-Perms unter Verwendung der Unix-Sicherheitsausführung durch.

[0042] Jedoch kann der Dateiserver **110** auch eine Anfrage **121** empfangen, die nicht mit der Sicherheitsausführung für die Zieldatei **112** übereinstimmt. Der Dateiserver **110** kann die Sicherheitsausführung für die Zieldatei **112** gegenüber einer nichtübereinstimmenden Client-Einrichtung **120** durchsetzen, durch Validieren von entweder (1) einer übersetzten Unix-ID für die Client-Einrichtung **120** oder (2) einer übersetzten Menge von Zugriffssteuereinrichtungen für diese Datei **112**. Wie hier beschrieben, validiert der Dateiserver **110** übersetzte Benutzer-IDs für alle Unix-Sicherheitsausführungsdateien **112** und validiert vorzugsweise übersetzte Benutzer-IDs für NT-Sicherheitsausführungsdateien **112** (wenn möglich).

[0043] Darüber hinaus werden die übersetzten Zugriffssteuereinschränkungen nicht für jede Anfrage **121** neu berechnet, sondern mit der Datei **112** zur Wiederverwendung in einem Cache-Speicher gespeichert, wenn der Dateiserver **110** übersetzte Zugriffssteuereinschränkungen für die Datei **112** validiert.

[0044] Der Dateiserver **110** erkennt und setzt somit auch wenigstens die folgenden Umstände durch:

– NT-Sicherheitsausführung. Die Datei **112** hat eine NT-Sicherheitsausführung und hat eine entsprechende Menge von Zugriffssteuereinschränkungen (eine NT-ACL), die durch eine Client-Einrichtung **120** unter Verwendung des CIFS-Dateiserverprotokolls eingestellt wurden.

[0045] Falls eine Client-Einrichtung **120** eine Anfrage **121** macht, um auf die Datei **112** unter Verwendung des NFS-Dateiserverprotokolls zuzugreifen, ermittelt der Dateiserver **110** den Unix-Benutzer, der mit der Client-Einrichtung **120** verknüpft ist, die die Anfrage **121** macht. Der Unix-Benutzer hat eine UID (Benutzer-ID).

[0046] In einer bevorzugten Ausführungsform bildet der Dateiserver **110** den Unix-Benutzer auf einen äquivalenten NT-Benutzer ab. Der Dateiserver **110** übersetzt die UID in eine SID (Sicherheits-ID), die ein zu dem Unix-Benutzer äquivalenter Benutzer ist. Der Dateiserver **110** setzt die Zugriffssteuereinschränkungen (die NT-ACL) für den äquivalenten NT-Benutzer (die SID) durch.

[0047] Der Dateiserver **110** führt den folgenden Prozess durch, um den Unix-Benutzer auf einen äquivalenten NT-Benutzer abzubilden.

– Die Client-Einrichtung **120** kontaktiert den Dateiserver **110** unter Verwendung des NFS-Dateiserverprotokolls. Die NFS-Dateiserverprotokollanfrage **121** umfasst eine UID für den Unix-Benutzer, der mit der Client-Einrichtung **120** verknüpft ist.

– Der Dateiserver **110** schaut die UID in der Unix-Passwortdatei (/etc/passwd) nach und identifiziert somit den Unix-Benutzernamen für den Unix-Benutzer. Der Unix-Benutzername ist eine alphanumerische Zeichenkette, die den Unix-Benutzer identifiziert.

– Der Dateiserver **110** übersetzt den Unix-Benutzernamen in einen NT-Benutzernamen unter Verwendung einer ausgewählten Abbildungsdatei. Ähnlich wie der Unix-Benutzername ist der NT-Benutzername eine alphanumerische Zeichenkette, die den NT-Benutzer identifiziert. Falls es für den Unix-Benutzernamen keine derartige Übersetzung gibt, bildet der Dateiserver **110** den Unix-Benutzernamen als den NT-Namen ohne Übersetzung.

In einer bevorzugten Ausführungsform umfasst die Abbildungsdatei eine Menge von Einträgen, die jeweils einen NT-Benutzer durch einen NT-Benutzernamen identifizieren und einen äquivalenten Unix-Benutzernamen mit dem NT-Benutzernamen verknüpfen.

– Der Dateiserver **110** kontaktiert einen NT-Domain-Controller, um eine SID für den NT-Benutzernamen zu ermitteln. Falls es keine solchen NT-Benutzer gibt, verwendet der Dateiserver **110** einen ausgewählten Parameter für nicht abgebildete Unix-Benutzer. In einer bevorzugten Ausführungsform ist dieser ausgewählte Parameter auf den NT-Benutzer „Gast" von vornherein eingestellt.

– Der Dateiserver **110** kontaktiert den NT-Domain-Controller, um die SIDs für alle Gruppen zu erhalten, bei denen der NT-Benutzer Mitglied ist.

[0048] Der Dateiserver **110** fängt UID-auf-SID-Ab-

bildungen für eine Zeitdauer ab, vo zugsweise für ungefähr einige Stunden.

[0049] In einer alternativen bevorzugten Ausführungsform oder falls der Dateiserver **110** nicht im Stande ist, Unix-Benutzer auf NT-Benutzer abzubilden (zum Beispiel falls eine Domain-Authentisierung abgeschaltet wurde), bildet der Dateiserver **110** die NT-ACL in eine nicht weniger restriktive Menge von Unix-Perms ab. Der Dateiserver **110** ermittelt diese Unix-Perms in Reaktion auf die NT-ACL und in Reaktion auf den Unix-Benutzer. Der Dateiserver **110** setzt die abgebildeten Zugriffssteuereinschränkungen (die Unix-Perms) für den tatsächlichen Unix-Benutzer (die UID) durch.

[0050] Der Dateiserver **110** kann eine dynamische Berechtigungsabbildung durchführen, in welcher der Dateiserver **110** die NT-ACL auf eine Menge von Unix-Perms zu dem Zeitpunkt abbildet, zu dem die Abbildung benötigt wird. In einer bevorzugten Ausführungsform fängt der Dateiserver **110** die übersetzten Unix-Perms mit der Datei **110** ab. Dementsprechend führt der Dateiserver **110** eine statische Berechtigungsabbildung zum Validieren von Zugriffssteuereinschränkungen durch, bei der der Dateiserver **110** die NT-ACL auf eine Menge von Unix-Perms zu dem Zeitpunkt abbildet, zu dem die NT-ACL eingestellt werden.

[0051] Der Dateiserver **110** führt den folgenden Prozess durch, um eine statische Berechtigungsabbildung zu erreichen:

– Der Dateiserver **110** ermittelt den NT-Benutzer, der der Besitzer der Datei **112** ist, und bildet den NT-Benutzer auf einen äquivalenten Unix-Benutzer ab (der Dateiserver **110** bildet die SID des NT-Benutzers auf eine UID für einen Unix-Benutzer ab).

– Der Dateiserver **110** untersucht die NT-ACL für die Datei **112** und ermittelt, ob es „Verweigere-Zugriff"-Vorgaben gibt.

– Falls die NT-ACL für die Datei **112** keine „Verweigere-Zugriff"-Vorgaben hat, erzeugt der Dateiserver **110** eine Menge von Unix-Perms mit einem Eintrag für „Benutzer-Berechtigungen", der mit den Dateizugriffseinschränkungen konsistent ist, die durch die NT-ACL bereitgestellt werden. Der Dateiserver **110** stellt die Unix-Perms für „Gruppenberechtigungen" gleich ein, wie die Unix-Perms für „andere Berechtigungen". Der Dateiserver **110** stellt die Unix-Perms für „andere Berechtigungen" gleich ein, wie den NT-ACL-Eintrag für „jedermann", falls einer existiert.

– Falls die NT-ACL für die Datei **112** keine „Verweigere-Zugriff"-Vorgaben hat, weist der Dateiserver **110** die Anfrage **121** zurück.

[0052] Weil eine statische Berechtigungsabbildung nicht in Reaktion auf den bestimmten Benutzer geschieht, der die Anfrage **121** macht, versucht der Dateiserver **110** nicht zu ermitteln, was die Vorgaben für die NT-ACL für diesen bestimmten Benutzer sind.

– Unix-Sicherheitsausführung. Die Datei **112** hat eine Unix-Sicherheitsausführung und hat eine zugehörige Menge von Zugriffssteuereinschränkungen (Unix-Perms), die durch eine Client-Einrichtung **120** unter Verwendung des NFS-Dateiserverprotokolls eingestellt wurden.

[0053] Falls eine Client-Einrichtung **120** eine Anfrage **121** macht, um auf die Datei **112** unter Verwendung des CIFS-Dateiserverprotokolls zuzugreifen, ermittelt der Dateiserver **110** den NT-Benutzer, der mit der Client-Einrichtung **120**, die die Anfrage **121** durchführt, verknüpft ist. Der NT-Benutzer hat eine SID (Session-ID).

[0054] Der Dateiserver **110** bildet den NT-Benutzer auf einen äquivalenten Unix-Benutzer ab. Der Dateiserver **110** übersetzt die SID in eine UID, die ein zu dem NT-Benutzer äquivalenter Benutzer ist. Der Dateiserver **110** setzt die Zugriffssteuereinschränkungen (die Unix-Perms) für den äquivalenten Unix-Benutzer (die UID) durch.

[0055] Der Dateiserver **110** führt den folgenden Prozess durch, um den NT-Benutzer auf einen äquivalenten Unix-Benutzer abzubilden:

– Die Client-Einrichtung **120** startet eine CIFS-Session (die Client-Einrichtung **120** kontaktiert zuerst den Dateiserver **110** unter Verwendung des CIFS-Dateiserverprotokolls). Die Client-Einrichtung **120** übermittelt ihren NT-Benutzernamen an den Dateiserver **110**.

– Der Dateiserver **110** übersetzt den NT-Benutzernamen in einen Unix-Benutzernamen unter Verwendung einer Abbildungsdatei. Falls es keine derartige Übersetzung für den NT-Benutzernamen gibt, verwendet der Dateiserver **110** den NT-Benutzernamen ohne Übersetzung als den Unix-Benutzernamen.

– Der Dateiserver **110** schaut den Unix-Benutzernamen in der Unix-Passwortdatei (/etc/passwd) nach und identifiziert somit den Unix-Benutzer, die UID für den Unix-Benutzer, die primäre Gruppe des Unix-Benutzers und die primäre GID (Gruppen-ID) für den Unix-Benutzer. Falls es keinen derartigen Unix-Benutzernamen in der Unix-Passwortdatei gibt, verwendet der Dateiserver **110** einen ausgewählten Parameter für nicht abgebildete NT-Benutzer. In einer bevorzugten Ausführungsform ist dieser ausgewählte Parameter auf den Unix-Benutzer „Niemand" von vornherein eingestellt.

– Der Dateiserver **110** schaut den Unix-Benutzernamen in der Unix-Gruppendatei (/etc/groups) nach, um alle anderen Gruppen und alle anderen GIDs zu ermitteln, die mit dem Unix-Benutzer verknüpft sind.

Lesen und Modifizieren von Zugriffssteuereinschränkungen

[0056] Jede Datei **112** hat ihre durch den Dateiserver **110** eingestellte Sicherheitsausführung, so dass entweder (a) eine Anfrage **121**, um eine Operation auf der Datei **112** durchzuführen, oder (b) eine Anfrage **121**, um eine Operation durchzuführen, die die Zugriffssteuereinschränkungen für die Datei **112** einstellt, erwartete Ergebnisse erzeugt.

[0057] Wenn die Datei **112** erstmalig erzeugt wird, stellt der Dateiserver **110** die Sicherheitsausführung für die Datei **112** gleich einer Sicherheitsausführung ein, die mit dem Dateiserverprotokoll verknüpft ist, das verwendet wird, um sie zu erzeugen. (Dies wird durch Einschränkungen eingeschränkt, die durch Zugriffssteuerbäume vorgegeben werden, die hierin beschrieben werden.) Somit wird die Sicherheitsausführung für die Datei **112** auf die Unix-Sicherheitsausführung eingestellt, falls die Datei **112** unter Verwendung des NFS-Dateiserverprotokolls erzeugt wird. In ähnlicher Weise wird die Sicherheitsausführung für die Datei **112** auf eine NT-Sicherheitsausführung eingestellt, falls die Datei **112** unter Verwendung des CIFS-Dateiserverprotokolls erzeugt wird.

[0058] Wenn die Zugriffssteuereinschränkungen der Datei **112** modifiziert werden, stellt der Dateiserver **110** die Sicherheitsausführung für die Datei **112** gleich einer Sicherheitsausführung ein, die mit den neuen Zugriffssteuereinschränkungen verknüpft ist. (Dies wird durch Einschränkungen eingeschränkt, die durch Zugriffssteuerbäume vorgeben werden, die hierin beschrieben werden.) Somit wird die Sicherheitsausführung für die Datei **112** auf eine Unix-Sicherheitsausführung eingestellt, falls eine Client-Einrichtung **120** eine Menge von Unix-Perms für die Datei **112** einstellt. In ähnlicher Weise wird die Sicherheitsausführung für die Datei **112** auf eine NT-Sicherheitsausführung eingestellt, falls eine Client-Einrichtung **120** ein NT-ACL für die Datei **112** einstellt.

[0059] Der Dateiserver **110** kann eine Anfrage **121** zum Lesen oder Betrachten der Zugriffssteuereinschränkungen für eine Datei **112** empfangen. Wenn der Dateiserver **110** eine Anfrage **121** zum Durchführen einer inkrementellen Veränderung der Zugriffssteuereinschränkungen für eine Datei **112** empfängt, ermittelt er auch die gegenwärtigen Zugriffssteuereinschränkungen für die Datei **112**, bevor die inkrementelle Veränderung durchgeführt wird.

[0060] Der Dateiserver **110** erkennt somit und setzt wenigstens die folgenden Umstände durch:

– NT-Sicherheitsausführung. Die Datei **112** hat eine NT-Sicherheitsausführung und hat eine entsprechende Menge von Zugriffssteuereinschränkungen (eine NT-ACL), die von einer Client-Einrichtung **120** unter Verwendung des CIFS-Dateiserverprotokolls eingestellt wurde.

[0061] Falls eine Client-Einrichtung **120** eine Anfrage **121** zum Lesen oder Modifizieren der Zugriffssteuereinschränkungen für die Datei **112** unter Verwendung des NFS-Dateiserverprotokolls durchführt, ermittelt der Dateiserver **110** den Unix-Benutzer, der mit der Client-Einrichtung **120** verknüpft ist, der die Anfrage **121** durchführt.

[0062] Der Dateiserver **110** führt den gleichen Prozess zum Abbilden einer NT-ACL auf eine Menge von Unix-Perms durch, wie er oben zur Validierung einer Dateizugriffssteuerung beschrieben wurde, mit den folgenden Ausnahmen:
Anders als bei einer Validierung von Zugriffssteuereinschränkungen behandelt der Dateiserver **110** eine Übersetzung von Zugriffssteuereinschränkungen für Anfragen **121** zum Lesen oder Modifizieren der Zugriffssteuereinschränkungen für die Datei **112** anders.

[0063] Vorzugsweise führt der Dateiserver **110** eine dynamische Berechtigungsabbildung durch, bei welcher der Dateiserver **110** die NT-ACL auf eine Menge von Unix-Perms zu dem Zeitpunkt abbildet, zu dem die Abbildung benötigt wird. Eine NT-Sicherheitsausführung ist reicher als eine Unix-Sicherheitsausführung – zum Beispiel hat eine Unix-Sicherheitsausführung keine „Verweigere-Zugriff"-Vorgaben. Somit ist es für den Dateiserver **110** möglich, die NT-ACL auf eine Menge von Unix-Perms abzubilden, die für verschiedene Unix-Benutzer unterschiedlich sind. Falls zum Beispiel die NT-ACL für eine Datei **112**, deren Besitzer Charles ist, einen Lesezugriff für Allen spezifisch bereitstellt, aber einen Lesezugriff für Beth spezifisch verweigert, wird der Dateiserver **110** verschiedene Unix-Perms für jeden der Benutzer Allen und Beth bereitstellen. Eine Menge wird einen Lesezugriff durch Allen's Gruppe erlauben und eine Menge wird einen Lesezugriff durch Beth's Gruppe verweigern, entsprechend dem Zugriff, der durch die gegenwärtige NT-ACL bereitgestellt wird.

[0064] Der Dateiserver **110** führt den folgenden Prozess durch, um eine dynamische Berechtigungsabbildung zu erreichen:

– Der Dateiserver **110** ermittelt den NT-Benutzer, der der Besitzer der Datei **112** ist, und bildet den NT-Benutzer auf einen äquivalenten Unix-Benutzer ab (der Dateiserver **110** bildet die SID des NT-Benutzers auf eine UID für einen Unix-Benutzer ab).

– Der Dateiserver **110** ermittelt den NT-Benutzer, der der Besitzer der Datei **112** ist, und bildet den NT-Benutzer auf einen äquivalenten Unix-Benutzer ab (der Dateiserver **11** bildet die SID für den NT-Benutzer auf eine UID für einen Unix-Benutzers ab).

– Der Dateiserver **110** untersucht die NT-ACL für

die Datei **112** und ermittelt, ob es „Verweigere Zugriff"-Vorgaben gibt.

– Falls die NT-ACL für die Datei **112** kein „Verweigere Zugriff"-Vorgaben hat, erzeugt der Dateiserver **110** eine Menge von Unix-Perms mit Einträgen für „Benutzer-Berechtigungen" und „andere Berechtigungen", die mit den Dateizugriffssteuereinschränkungen konsistent sind, die durch die NT-ACL bereitgestellt werden. Leer Dateiserver **110** stellt die Unix-Perms für „Gruppen-Berechtigungen" gleich den Unix-Perms für „andere Berechtigungen" ein.

– Falls die NT-ACL für die Datei **112** keine „Verweigere Zugriff"-Vorgaben haben, versucht der Dateiserver **110** zu ermitteln, ob eine auf den bestimmten Unix-Benutzer zutrifft. Falls der Dateiserver dies weiß, erzeugt er eine Menge von Unix-Perms, die die Zugriffssteuereinschränkungen wiedergeben, die gegenwärtig für diese bestimmte Datei **112** und diesen bestimmten Unix-Benutzer erhältlich sind. Falls der Dateiserver **110** dies nicht weiß, weist er die Anfrage **121** zurück. (Alternativ könnte der Dateiserver **110** die Anfrage **121** zurückweisen, falls es „Verweigere Zugriff"-Vorgaben in der NT-ACL gibt.) In alternativen Ausführungsformen kann der Dateiserver **110** für Anfragen **121** zum Lesen oder Modifizieren der Zugriffssteuereinschränkungen für die Datei **112** eine statische Berechtigungsprüfung durchführen, ähnlich einer Validierung von Zugriffssteuereinschränkungen.

[0065] Falls die Anfrage **121** versucht, Attribute der Datei **112** zu modifizieren, die keinen Effekt auf Zugriffssteuereinschränkungen für die Datei **112** haben (wie zum Beispiel Zugriffszeit oder Modifikationszeit), führt der Dateiserver **110** diese Modifikationen ohne eine Änderung der Zugriffssteuereinschränkungen für die Datei **112** durch.

[0066] Falls die Anfrage **121** versucht, einige aber nicht alle Zugriffssteuereinschränkungen für die Datei **112** zu modifizieren, erzeugt der Dateiserver **110**, wie oben beschrieben, eine Menge von Unix-Perms in Reaktion auf die NT-ACL der Datei **112**. Der Dateiserver **110** modifiziert die erzeugten Unix-Perms wie es durch die Anfrage **121** spezifiziert wird. Falls der Dateiserver **110** eine Menge von Unix-Perms in Reaktion auf die NT-ACL für die Datei **112** nicht erzeugen kann, weist der Dateiserver **110** die Anfrage **121** zurück.

[0067] Ein Unterschied beim Einstellen von Zugriffssteuereinschränkungen ist der, dass gemäß der NT-Sicherheitsausführung Dateien **112** spezifisch auf „NUR-LESEN" eingestellt werden können. Gemäß der Unix-Sicherheitsausführung werden Dateien durch Löschen der SCHREIB-Berechtigung für den Besitzer der Datei **112** so eingestellt, dass sie nur gelesen werden können. Wenn eine Client-Einrichtung **120**, die das CIFS-Dateiserverprotokoll verwendet, versucht, das „NUR-LESEN"-Attribut einer Datei **112** mit der Unix-Sicherheitsausführung einzustellen, löscht der Dateiserver **110** die SCHREIB-Berechtigung für den Besitzer der Datei **112** in den Unix-Perms für diese Datei **112**.

– Unix-Sicherheitsausführung. Die Datei **112** hat die Unix-Sicherheitsausführung und hat eine entsprechende Menge von Zugriffssteuereinschränkungen (Unix-Perms), die durch eine Client-Einrichtung **120** unter Verwendung des NFS-Dateiserverprotokolls eingestellt wurden.

[0068] Der Dateiserver **110** führt den folgenden Prozess zum Abbilden einer Menge von Unix-Perms auf eine NT-ACL zum Anzeigen oder zur Modifikation dieser Unix-Perms durch eine CIFS-Client-Einrichtung **120** durch:

– Der Dateiserver **110** erzeugt einen NT-ACL-Eintrag für „Besitzer", der die gleichen Zugriffssteuereinschränkungen bereitstellt, wie der Unix-Perms-Eintrag für „Benutzer-Berechtigungen".

– Der Dateiserver **110** erzeugt einen NT-ACL-Eintrag für „Jedermann", der die gleichen Zugriffssteuereinschränkungen bereitstellt, wie der Unix-Perms-Eintrag für „Andere Berechtigungen".

– Falls möglich, erzeugt der Dateiserver **110** einen NT-ACL-Eintrag für den gegenwärtig anfragenden Benutzer, der die gleichen Zugriffssteuereinschränkungen bereitstellt, wie der Unix-Perms-Eintrag für diesen Benutzer. Dieser Schritt könnte ein Abbilden des Unix-Benutzers auf einen äquivalenten NT-Benutzer unter Verwendung des UID-nach-SID-Cachespeichers erfordern.

[0069] Falls die Anfrage **121** (zur Modifikation von Unix-Perms durch einen NT-Benutzer) versucht, Attribute der Datei **112** zu modifizieren, die keinen Effekt auf Zugriffssteuereinschränkungen der Datei **112** haben, macht der Dateiserver **110**, ähnlich mit der Modifikation eines NT-ACL-Eintrags durch einen Unix-Benutzer, diejenigen Modifikationen ohne eine Veränderung der Zugriffssteuereinschränkungen für die Datei **112**.

[0070] Falls die Anfrage **121** versucht, einige aber nicht alle der Zugriffssteuereinschränkungen für die Datei zu modifizieren, erzeugt der Dateiserver **110** eine NT-ACL in Reaktion auf die Menge von Unix-Perms für die Datei **112**, wie oben beschrieben. Der Dateiserver **110** modifiziert die erzeugte NT-ACL wie es durch die Anfrage **121** spezifiziert wird.

Zugriffssteuerunterbäume

[0071] In einer bevorzugten Ausführungsform sind die Dateien **112** in dem Dateisystem **111** in Bäumen mit einer Menge von Zweigknoten und einer Menge

von Blattknoten organisiert. Ein Zweigknoten des Baums ist ein Wurzelknoten und jeder Zweigknoten des Baums ist ein Wurzelknoten für einen Unterbaum des Baums. In dem Dateisystem **111** ist jeder Zweigknoten ein Verzeichnis und jeder Blattknoten ist eine Datei **112**. Ein Verzeichnis ist eine Art von Datei **112**, die Informationen über diejenigen Zweigknoten und Blattknoten in einem Unterbaum umfasst, für den er der Wurzelknoten ist.

[0072] Der Dateiserver **110** verknüpft eine eingeschränkte Menge von Zugriffssteuermodellen mit jedem Unterbaum. In einer bevorzugten Ausführungsform, in welcher der Dateiserver **110** die Unix-Sicherheitsausführung und die NT-Sicherheitsausführung unterstützt, bestimmt der Dateiserver **110**, dass jeder Unterbaum im Nur-NT-Format, Nur-Unix-Format oder gemischten Format vorliegt.

Nur-NT-Format

[0073] Wenn der Dateiserver **110** einen Unterbaum als Nur-NT-Format bestimmt, schränkt dies eine Erzeugung von Dateien **112** innerhalb dieses Unterbaums auf Dateien **112** mit einer NT-Sicherheitsausführung ein. Der Dateiserver **110** verhindert auch eine Veränderung des Zugriffssteuermodells für Dateien **112** innerhalb dieses Unterbaums auf andere, als die NT-Sicherheitsausführung.

[0074] Gemäß der NT-Sicherheitsausführung erben neue Dateien **112** NT-ACL-Einstellungen von ihren Elternknoten. Falls eine Client-Einrichtung **120**, die das NFS-Dateiserverprotokoll verwendet, versucht, eine Datei **112** in einem Unterbaum im Nur-NT-Format zu erzeugen, kann diese Datei **112** nur durch den Unix-Benutzer erzeugt werden, der zu dem NT-Benutzer äquivalent ist, der der NT-Besitzer des Wurzelknotens des Unterbaums ist. Der Dateiserver **110** ermittelt, ob der Unix-Benutzer, der die Anfrage **121** durchführt, der Äquivalente ist, durch (a) Abbilden der SID für den NT-Benutzer, der der Besitzer ist, auf eine äquivalente UID; (b) Speichern dieser UID in seinem Datensatz für die Datei **112**; und (c) Vergleichen dieser UID mit der UID in der Anfrage **121**.

[0075] Gemäß der NT-Sicherheitsausführung gibt es eine spezielle „LÖSCHEN"-Berechtigung und eine spezielle „LÖSCHE-NACHKOMME"-Berechtigung. Falls der Dateiserver **110** nicht im Stande ist, zu ermitteln, ob ein Unix-Benutzer diese Berechtigungen hat, weist er Anfragen **121** zum Löschen von Dateien **112** in Nur-NT-Format-Unterbäumen zurück, es sei denn, dass die Anfrage **121** von dem Besitzer der Datei **112** (der äquivalente Unix-Benutzer des NT-Benutzers, der der Besitzer ist) oder von dem Unix-Benutzer „root" ist.

[0076] Gemäß der NT-Sicherheitsausführung gibt es eine spezielle „ÄNDERE-BERECHTIGUNG"-Berechtigung und eine spezielle „ÜBERNEHME-BESITZ"-Berechtigung. Falls der Dateiserver **110** nicht im Stande ist, zu ermitteln, ob ein Unix-Benutzer diese Berechtigungen hat, weist er Anfragen **121** zum Einstellen beliebiger Berechtigungen für Dateien **112** in einem Nur-NT-Format-Unterbaum zurück, es sei denn, dass die Anfrage **121** von dem Besitzer der Datei **112** (der äquivalente Unix-Benutzer des NT-Benutzers, der der Besitzer ist) oder von dem Unix-Benutzer „root" ist.

Nur-Unix-Format

[0077] Wenn der Dateiserver **110** einen Unterbaum im Nur-Unix-Format bestimmt, schränkt dies in ähnlicher Weise eine Erzeugung einer Datei **111** innerhalb dieses Unterbaums auf Dateien **111** mit einer Unix-Sicherheitsausführung ein. Der Dateiserver **110** verhindert auch ein Ändern des Zugriffssteuermodells für Dateien **111** innerhalb dieses Unterbaums auf andere, als die Unix-Sicherheitsausführung. Versuche, eine NT-ACL einzustellen, würden das Zugriffssteuermodell für die Datei **112** auf die NT-Sicherheitsausführung ändern und werden somit in einem Nur-Unix-Format-Unterbaum zurückgewiesen.

[0078] Wenn eine Client-Einrichtung **120**, die das CIFS-Dateiserverprotokoll verwendet, eine Datei **112** in einem Nur-Unix-Format-Unterbaum erzeugt, stellt der Dateiserver **110** den Besitzer der Datei **112** auf den Unix-Benutzer ein, der äquivalent mit dem NT-Benutzer ist, der die Anfrage **121** durchführt. Der Dateiserver **110** bildet die SID für den NT-Benutzer auf eine UID für einen äquivalenten Unix-Benutzer ab und verwendet diese UID, um den Besitzer der Datei **112** einzustellen.

[0079] Gemäß der Unix-Sicherheitsausführung gibt es keine „ÄNDERE-BERECHTIGUNG"-Berechtigung oder „ÜBERNEHME-BESITZ"-Berechtigung. Der Dateiserver **110** weist Anfragen **121** zum Einstellen dieser Berechtigungen für Dateien **112** in einem Nur-Unix-Format-Unterbaum immer zurück.

Gemischtes Format

[0080] Wenn der Dateiserver **110** einen Unterbaum im gemischten Format bestimmt, erlaubt dies eine Erzeugung von Dateien **112** mit entweder der Unix-Sicherheitsausführung oder der NT-Sicherheitsausführung. Der Dateiserver **110** verhindert nicht ein Verändern des Zugriffssteuermodells für Dateien **111** innerhalb dieses Unterbaums in entweder Unix-Sicherheitsausführung oder NT-Sicherheitsausführung.

[0081] Ein Administrator des Dateiservers **110** kann die Bestimmung eines Unterbaums von einem ersten Format in ein zweites Format ändern (zum Beispiel von einem gemischten Format in entweder das Nur-NT-Format oder das Nur-Unix-Format). Wenn

das zweite Format möglicherweise mit dem ersten Format inkompatibel ist (zum Beispiel wenn ein Unterbaum, der in das Nur-NT-Format geändert wird, Knoten umfasst, die die Unix-Sicherheitsausführung haben), konvertiert der Dateiserver **110** diese Dateien **112** mit inkompatiblen Zugriffssteuermodellen, indem er Berechtigungen für diese Dateien **112** einstellt. Anfragen **121** nach einer Datei **112**, die nur Berechtigungen prüft, werden dennoch unter Verwendung des Zugriffssteuermodells anstelle der Datei **112** validiert.

[0082] Obwohl die Erfindung hier im Hinblick auf nur zwei Zugriffssteuermodelle beschrieben wird, kann die Erfindung leicht mit drei oder mehr Zugriffssteuermodellen verwendet werden. In solchen alternativen Ausführungsformen gibt es größere Zahlen von möglichen Unterbaum-Formaten, umfassend Unterbaum-Formate, die die Datei **112** innerhalb dieses Unterbaums auf eines einer Menge einer Vielzahl von Zugriffssteuermodellen einschränkt, die geringer ist, als die Menge aller Zugriffssteuermodelle, die durch den Dateiserver **110** erkannt werden.

[0083] In einer bevorzugten Ausführungsform wird der Wurzelknoten des Dateisystems **111** im gemischten Format bestimmt. Client-Einrichtungen **120**, die Besitzer eines Unterbaums sind, können das Format eines Unterbaums durch Anfrage **121** an den Dateiserver **110** ändern; somit können Client-Einrichtungen **120** Unterbäume modifizieren, um ein Nur-NT-Format, Nur-Unix-Format, gemischtes Form zu haben. Wenn ein neuer Unterbaum erzeugt wird, bestimmt der Dateiserver **110** den neuen Unterbaum in dem gleichen Format wie seine Eltern; somit im gemischten Format, falls er innerhalb eines Unterbaums erzeugt wird, der bereits gemischtes Format (die Voreinstellung) hat, im Nur-NT-Format, falls er innerhalb eines Unterbaums erzeugt wird, der bereits Nur-NT-Format hat, und im Nur-Unix-Format, falls er in einem Unterbaum erzeugt wird, der bereits Nur-Unix-Format hat.

Alternative Ausführungsformen

[0084] Obwohl bevorzugte Ausführungsformen hier offenbart werden, sind viele Variationen möglich, die innerhalb des Schutzbereichs der beanspruchten Erfindung verbleiben, und diese Variationen würden einem Fachmann nach einem Studium dieser Anmeldung deutlich werden.

Patentansprüche

1. Verfahren zum Betreiben eines Dateiservers (**110**), gekennzeichnet durch die Schritte:
Identifizieren einer ersten Datei (**112**) auf dem Dateiserver (**110**) mit einem ersten Zugriffssteuermodell, das aus einer Vielzahl von Zugriffssteuermodellen ausgewählt wird, die auf dem Dateiserver (**110**) implementiert sind, wobei der Dateiserver (**110**) eine Vielzahl von Dateien beinhaltet, von welchen wenigstens einige mit verschiedenen Zugriffssteuermodellen verknüpft sind;
Identifizieren der ersten Datei (**112**) mit einem zweiten Zugriffssteuermodell in Reaktion auf eine Dateiserveranfrage; und
Durchsetzen des ersten Zugriffssteuermodells für alle Zugriffe auf die erste Datei, wobei ein Zugriff auf die erste Datei nur in Reaktion auf eine Anfrage erlaubt wird, welche Berechtigungen in dem ersten Zugriffssteuermodell genügt.

2. Verfahren nach Anspruch 1, wobei der Erlaubnisschritt das Zugriffssteuermodell für alle Zugriffe auf die erste Datei (**112**) durchsetzt, unabhängig von dem Zugriffssteuermodell, das mit der Entität verknüpft ist, welche einen Zugriff auf die erste Datei (**112**) wünscht.

3. Verfahren nach Anspruch 1, umfassend die Schritte:
Verknüpfen der ersten Datei (**112**) mit einer Teilmenge von Dateien in einem Dateisystem (**111**); und
Beschränken der Teilmenge von Dateien auf eine Sicherheitsteilmenge der Vielzahl von Zugriffsteuermodellen;
wobei Versuche, eine Berechtigung in dem Dateisystembaum einzustellen, auf die Sicherheitsteilmenge beschränkt sind.

4. Verfahren nach Anspruch 3, desweiteren umfassend den Schritt des Zwischenspeicherns der Verknüpfung und der Beschränkungen für die Teilmenge von Dateien für eine zukünftige Verwendung.

5. Verfahren nach Anspruch 3, wobei die Schritte des Verknüpfens und Beschränkens dynamisch ausgeführt werden können, wenn sie mit einem spezifischen Versuch verknüpft sind, auf eine Datei (**112**) zuzugreifen, oder statisch, wenn sie nicht mit einem Benutzer oder einem spezifischen Versuch verknüpft sind, auf eine Datei (**112**) zuzugreifen.

6. Verfahren nach Anspruch 1, wobei der Schritt des Erlaubens eines Zugriffs die folgenden Schritte umfasst:
Übersetzen einer ersten Menge von Berechtigungen, die mit der ersten Datei (**112**) in dem ersten Zugriffssteuermodell verknüpfte sind, in eine zweite Menge von Berechtigungen in einem zweiten Zugriffssteuermodell, wobei die zweite Menge von Berechtigungen keinen größeren Zugriff auf die erste Datei (**112**) erlaubt, als die erste Menge von Berechtigungen; und
Durchsetzen einer Dateiserveranfrage in dem zweiten Zugriffssteuermodell unter Verwendung der zweiten Menge von Berechtigungen.

7. Verfahren nach Anspruch 6, desweiteren umfassend Schritte zum Zwischenspeichern der Über-

setzung.

8. Verfahren nach Anspruch 7, wobei die Schritte zum Übersetzen dynamisch ausgeführt werden und auftreten, ungefähr wenn die Schritte des Durchsetzens stattfinden.

9. Verfahren nach Anspruch 7, wobei die Schritte zum Übersetzen statisch ausgeführt werden und auftreten, ungefähr wenn die Zugriffssteuerbeschränkungen eingestellt oder zurückgesetzt werden.

10. Verfahren nach Anspruch 1, wobei die erste Datei (**112**) mit dem zweiten Zugriffssteuermodell verknüpft wird, unabhängig von dem Zugriffssteuermodell, welches vorher mit der ersten Datei (**112**) verknüpft war.

11. Verfahren nach Anspruch 1, umfassend Schritte zum Verknüpfen des zweiten Zugriffssteuermodells mit einer Dateiserveranfrage zum Einstellen von Berechtigungen für die erste Datei (**112**), wenn die Dateiserveranfrage erfolgreich ist.

12. Verfahren nach Anspruch 1, wobei die Schritte zum Identifizieren Schritte zum Übersetzen einer ersten Menge von Berechtigungen, die mit der ersten Datei (**112**) in dem ersten Zugriffssteuermodell verknüpft sind, in eine zweite Menge von Berechtigungen in dem zweiten Zugriffssteuermodell umfassen, wobei die zweite Menge von Berechtigungen keinen größeren Zugriff auf die erste Datei (**112**) erlaubt, als die erste Menge von Berechtigungen.

13. Verfahren nach Anspruch 12, wobei die Schritte zum Übersetzen ein Abbilden von NT-Zugriffssteuerbeschränkungen in eine nicht weniger restriktive Menge von Unix-Berechtigungen umfassen.

14. Verfahren nach Anspruch 12, wobei die Schritte zum Übersetzen ein Abbilden einer Menge von Unix-Berechtigungen in eine Menge von nicht weniger restriktiven NT-Zugriffssteuerbeschränkungen umfassen.

15. Verfahren zum Betreiben eines Dateiservers (**110**) gemäß Anspruch 1, wobei der Schritt zum Erlauben eines Zugriffs die folgenden Schritte umfasst:
Erkennen einer ersten Menge von Berechtigungen, die mit der ersten Datei (**112**) in dem ersten Zugriffssteuermodell verknüpft sind;
Definieren eines ersten Benutzertyps, der mit dem ersten Zugriffssteuermodell verknüpft ist;
Übersetzen eines Benutzers von einem zweiten Benutzertyp, der mit einem zweiten Zugriffssteuermodell verknüpft ist, in den ersten Benutzertyp; und
Durchsetzen einer Dateiserveranfrage von dem zweiten Benutzertyp unter Verwendung des ersten Benutzertyps und der ersten Menge von Berechtigungen.

16. Verfahren nach Anspruch 15, desweiteren umfassend den Schritt des Zwischenspeicherns der Übersetzung.

17. Verfahren nach Anspruch 16, wobei die Schritte zum Erkennen, Definieren, Übersetzen und Zwischenspeichern zu einer Zeit statisch ausgeführt werden können, zu welcher die Zugriffssteuerbeschränkungen entweder eingestellt oder zurückgesetzt werden.

18. Verfahren nach Anspruch 6 oder 15, wobei die Schritte zum Übersetzen in Bezug auf Zugriffssteuerbeschränkungen ausgeführt werden, die auf die erste Datei (**112**) anwendbar sind, zu einer Zeit des Schritts zum Durchsetzen.

19. Verfahren nach Anspruch 6 oder 15, wobei die Schritte zum Übersetzen in Bezug auf Zugriffssteuerbeschränkungen ausgeführt werden, die auf die erste Datei (**112**) anwendbar sind, zu einer Zeit, zu der die Zugriffssteuerbeschränkungen eingestellt werden.

20. Dateiserver (**110**), umfassend:
eine Menge von Dateien (**112**), die auf dem Dateiserver (**110**) verfügbar sind, dadurch gekennzeichnet, dass jede Datei ein erstes verknüpftes Zugriffssteuermodell hat, das aus einer Vielzahl von Zugriffssteuermodellen ausgewählt ist, welche auf dem ersten Dateiserver (**110**) implementiert sind, wobei der Dateiserver (**110**) eine Vielzahl von Dateien umfasst, von denen wenigstens einige mit verschiedenen Zugriffssteuermodellen verknüpft sind;
wobei der Dateiserver (**110**) konfiguriert ist, um jede Datei mit einem zweiten Zugriffssteuermodell in Reaktion auf eine Dateiserveranfrage zu verknüpfen; und
wobei der erste Dateiserver (**110**) eingerichtet ist, das verknüpfte Zugriffssteuermodell für alle Zugriffe auf die Datei durchzuführen, indem ein Zugriff auf jede Datei nur in Reaktion auf eine Anfrage erlaubt wird, welche Berechtigungen in dem ersten verknüpften Zugriffssteuermodell genügt.

21. Dateiserver (**110**) nach Anspruch 20, umfassend:
einen Teilbaum von Dateien (**112**) in dem Dateisystem (**111**), welcher mit einer Sicherheitsteilmenge der Vielzahl von Zugriffssteuermodellen verknüpft ist;
wobei der Dateiserver (**110**) Versuche auf den Sicherheitsteilbaum einschränkt, Berechtigungen in dem Teilbaum einzustellen.

22. Dateiserver (**110**) nach Anspruch 20, wobei der Dateiserver (**110**) imstande ist, das Zugriffssteuermodell, das mit der Datei (**112**) verknüpft ist, in Reaktion auf eine Dateiserveranfrage zu ändern.

23. Dateiserver (**110**) nach Anspruch 22, wobei

der Dateiserver (**110**) imstande ist, das Zugriffssteuermodell, das mit der Datei (**112**) verknüpft ist, in Reaktion auf eine Dateiserveranfrage zu ändern, wenn die Dateiserveranfrage erfolgreich ist.

24. Dateiserver (**110**) nach Anspruch 22, wobei der Dateiserver (**110**) imstande ist, eine erste Menge von Berechtigungen, die mit der Datei (**112**) in einem Zugriffssteuermodell verknüpft ist, in eine zweite Menge von Berechtigungen in einem zweiten Zugriffssteuermodell zu übersetzen, wobei die zweite Menge von Berechtigungen keinen größeren Zugriff auf die Datei (**112**) erlaubt, als die erste Menge von Berechtigungen.

Es folgt ein Blatt Zeichnungen

Anhängende Zeichnungen

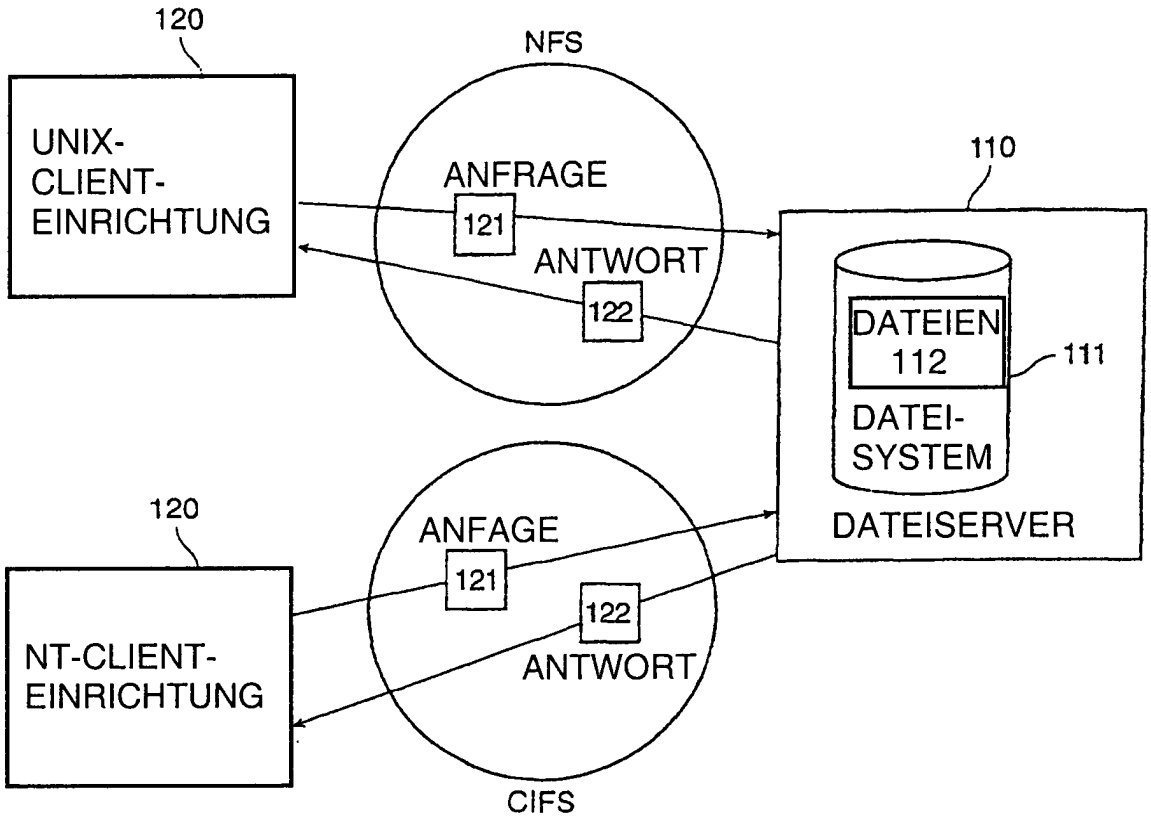

FIG. 1