INTERNET-DRAFT
Expires: January 1999

Lisa Lippert
Microsoft Corporation
August 1998

WebDAV Access Control Goals
draft-ietf-webdav-acl-reqts-00.txt

1. Status of this Memo

This document is an Internet draft. Internet drafts are working documents of the Internet Engineering Task Force (IETF), its areas and its working groups. Note that other groups may also distribute working information as Internet drafts.

Internet Drafts are draft documents valid for a maximum of six months and can be updated, replaced or obsoleted by other documents at any time. It is inappropriate to use Internet drafts as reference material or to cite them as other than as "work in progress".

To view the entire list of current Internet-Drafts, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), ftp.nordu.net (Northern Europe), ftp.nis.garr.it (Southern Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

Distribution of this document is unlimited. Please send comments to the WWW Distributed Authoring and Versioning (WebDAV) mailing list, <w3c-dist-auth@w3.org>, which may be joined by sending a message with subject "subscribe" to <w3c-dist-auth-request@w3.org>. Discussions are archived at URL http://www.w3.org/pub/WWW/Archives/Public/w3c-dist-auth/.

2. Abstract

This document defines goals for an access control system for use with the WebDAV protocol.

Access control systems grant or deny rights (such as "read" or "write") to specified principals for individual resources.

3. Contents

4. Introduction

4.1. Problem to be solved

In distributed authoring scenarios resources may be accessible by multiple principals. To control how these principals can access and alter a resource a system of access controls is needed. These controls define what actions a particular principals is allowed to exercise on a particular resource.

There does not currently exist a mechanism for DAV to be used to grant and deny such access rights. This document outlines the goals for such a method.

5. Definitions

Most terminology in this document is used in the same way as in the WebDAV specification [1].

5.1. Access Control List and Entries

An Access Control List (ACL) usually refers to a collection of Access Control Entries (ACE). Each entry applies to one or more principals and (usually) one object and/or its children. Each entry grants or denies one or more rights to the specified principals on that object. While this is a common model, it is applied differently in various existing stores (see 5.4).

It is not required that the DAV access control draft use the model of ACL as defined by existing stores. This draft refers to ACLs and ACEs because many systems use them, and in order to provide examples for some recommendations and goals.

5.2. Principal

A principal is a user or group of users to whom specific access rights can be granted or denied.

5.3. Scenarios

These are scenarios that SHOULD be accommodated by an access control mechanism for DAV. These are all possible multi-author and distributed-author scenarios. These scenarios were used to build the goals list.

5.3.1. Different authors on each document

Jim owns a directory of documents which must be edited by a variety of different people, in fact a different set of people for each document. He must be able to set access permissions

individually for each document, so that only the correct editors have write access to each document.

5.3.2. Denying to member of a group

Lisa administers a bunch of files which can all be read by members of a group. However, one of them contains details about a surprise party for Josh. Lisa must be able to set the permissions on that document such that even though the group is allowed access to the document, Josh cannot read the document. This scenario is best served if new members can be added to the group and be able to read the document automatically.

5.3.3. Delegation

Jim wishes to delegate some administration of his directory to Rohit. First, Jim must be able to allow Rohit to read ACLs and write resources without being able to write ACLs on those resources. Second, when Rohit is more trusted, Jim must be able to allow Rohit to edit the ACLs on the directory and on all resources in the directory, without giving Rohit the ability to take over entirely from Jim by removing all permissions from Jim.

5.4. Interoperability

DAV implementations will in some cases be built on top of existing access control implementations, e.g. file systems. Many access permission features can be built on top of the underlying store, however DAV access permissions will be more secure if the store's access permission functionality is used.

Some common features of file systems with access control:

- Associate each combination of a resource, a principal and a right with a "yes/no" decision whether the principal gets the right on the resource
- Offer read, write and execute access to files
- Principals include concept of "all users"
- Some have more detailed rights such as "set owner", "set ACL", "synchronize"
- May offer a different set of rights on directories (as opposed to files)
- May allow access to be denied as well as granted
- Groups can be principals as well as users
- May have an "owner" for resources (the owner can have read or write permission removed, but can never be denied permission to take over the resource, set ACLs and restore permissions).
- Has rules for either avoiding conflicting access entries or evaluating access entries in some consistent way to resolve conflict
- May have inheritance rules

6. Goals

6.1. Functionality

Principals with the appropriate rights must be able to read and set access control information.

6.2. Specifying principals

Principals MUST be uniquely identifiable.

It MUST be possible to use a the octet strings which are defined by HTTP 1.1 [2] to identify a principal.

It must also be possible to specify special types of principals, in particular all authorized principals, all anonymous principals, and all principals.

6.3. Rights

It MUST be possible to grant or deny the following rights to any principal

- to alter the body of a resource
- to alter the properties of a resource
- to delete a resource
- to add a child to a collection
- to read the ACL on a resource or collection
- to change the ACL on a resource or collection
- to delete a child from a collection
- to list the contents of a collection

6.4. Granularity of Objects

It must be possible to set ACLs individually on both collections and resources.

6.5. Evaluating rights

The protocol draft must provide an algorithm by which conflicts between rights, both granted and denied, for a particular principal on a particular resource are unambiguously settled.

6.6. Discovery

The protocol draft must specify how clients discover what rights are available on a resource as well as what rights have been assigned to which principals for a particular resource. Discovery is itself subject to access control.

6.7. Security

It should be acceptable to deny unprotected transactions.

7. Recommendations

7.1. Functionality goals

It is recommended that users be able to add access control

information to an object without having to reset all access control settings. This is recommended because certain systems or implementations may allow a user to add certain kinds of access rights but not others (i.e. grant "read" but not grant "delete").

Similarly, it should be possible for users to be able to remove, delete or clear access rights without having to reset all rights.

7.2. Achieving predictability

Users SHOULD be able to predict what rights another user has, based on looking at the DAV access rights granted and denied. This may be impossible if another user has access to the resource without using DAV, in which case other access control mechanisms may apply. The underlying implementation may have advanced access control which is more restrictive than the DAV access control.

There are several issues which much be dealt with carefully in order to maintain as much predictability as possible.

7.2.1. Evaluation Rules

Precise evaluation rules, with no ambiguity, are needed to achieve predictability.

7.2.2. Inheritance

If the underlying system uses inheritance, then users of the DAV access control mechanism should still be able to predict its behavior. This could be achieved if the type of inheritance is discoverable, or if the type(s) of inheritance is/are specified by the DAV access control protocol draft.

7.2.3. Ownership

Systems in which resources have owners also must be treated with care. Predictability can be achieved on systems with owners by including owner functionality in DAV access control. Systems which do not support owner functionality could refuse requests to change or set ownership.

There may be other ways to preserve predictability with inheritance and ownership.

8. Areas Out of Scope

8.1. Groups

Modeling groups is out of scope. There is currently no concept of groups to deal with in HTTP [2] or DAV. The protocol draft MAY support specifying (naming) groups which already exist on a given underlying system. It is recommended that the protocol draft avoid issues such as the enumeration of group members or administration of groups.

8.2. Roles

Those with experience building complex document management or workflow systems on top of stores with simple ACLs know how hard

it is to define roles for individuals. For example, the document management system can map the role "author" to grant the rights read/write/delete, but it is more difficult to go the other way. Is an individual with read/write/delete permissions an author, an editor, or somebody with no role and just a list of rights? Many systems employ the concept of assigning roles, more temporary than identities, to more flexibly define access.

Roles are important. However, roles would appear to be difficult and not necessarily related to ACLs. The protocol draft MAY define how roles may be assigned.

8.3. Certificate-based security

Certificates are out of scope for the DAV ACL protocol.

8.4. Time-based access control

Time-based access control is out of scope for the DAV ACL protocol.

9. SECURITY CONSIDERATIONS

This document is intended to specify how security can be enhanced in WebDAV systems. Many security considerations have already been discussed in [1].

Authentication mechanisms, which will be used by DAV ACL implementations to identify principals, are defined elsewhere for HTTP 1.1 [2]. The same goals for security identified in [1], such as not using the HTTP Basic authentication scheme, apply even more strongly when access control functionality is considered.

Inappropriate implementations or use of access control functionality can make a system less secure in these ways:

- by potentially allowing non-administrators to change the access settings for items on a server,

- by providing a way for access control information to be read and set (may be snooped), and potentially snooped, hackers may find it easier to discover names of accounts to use in attacks.

The "Security" goals section (6.7) includes some goals to counterbalance these insecurities. Also, the ability to specify who has access rights to read and to change the rights themselves (section 6.3) lessens the chance of hackers being able to learn access information or set access levels.

Access control functionality also improves security, by giving resource owners much more control and flexibility over who can access their resources in what way.

10. REFERENCES

[1] Y. Goland, J. Whitehead, A. Faizi, S. Carter, D. Jensen,

"Extensions for Distributed Authoring on the World Wide Web", <draft-ietf-webdav-protocol-08>, April 1998.

[2] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1." RFC 2068. U.C. Irvine, DEC, MIT/LCS. January, 1997.

H. Palmer, "Requirements for Access Control within Distributed Authoring and Versioning Environments on the World Wide Web", <draft-ietf-webdav-acreq-01.txt>, November 1997

P. J. Leach, Y. Y. Goland, "WebDAV ACL Protocol", <draft-ietf-webdav-acl-00.txt> November 1997

M. Satyanarayanan, "Integrating Security in a Large Distributed System", ACM transactions on computer systems 7(3), August 1989.

11. Authors' Addresses

Lisa Lippert
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
EMail: lisadu@microsoft.com