Julian Satran
IBM Research Lab in Haifa
Julian_Satran@il.ibm.com
+972 4 8296264

November 4, 2003

To: All

Towards a Common Scalable Security Infrastructure for Storage Access

1. Motivation

Any non-trivial storage access solution involving data or space sharing on persistent storage requires some for of access protection and security. The primary area of concern is securing data access. It can also be argued that securing data at rest is also a major concern but we will not approach this issue here except for where it touches data access security.

Security mechanisms developed for network file access (e.g., the security mechanisms for NFS-V4 of for AFS(DFS)) are mostly based on the assumption that the "control channel and data channel" are the same and/or the data and control information are manipulated by the same entity.

Any "asymmetrical" scheme – in which the metadata and access control are taken out of the data access path will have different entities handling the access control and data access.

It seems to us than any such scheme shares many requirements with those of Object Storage.

Any access control mechanism to storage is a central piece of hardware and software in the user computing environment. Making it as "uniform" as possible and enable easy migration of users and machines from one for of storage infrastructure to other is of major interest to users.

2. Requirements

We will assume a storage access scheme in which access control (and perhaps overall management of a "closed storage universe" is handled by an out-of-band server (or server-cluster). Let us call this unit Admin. It may handle some "work distribution" function but it may also handle the primary access control function. The other two types of entities in this scheme are Clients (units that access storage on behalf of users) and the Storage entities.

A primary requirement for access control would be for this Unit handle user/process/machine authentication for the entities requiring data access (Clients) and to handle it effectively – i.e., clients will have access Admin when first needing data access and very rarely afterwards.

This requirement can be met by an unforgeable capability-credential mechanism.

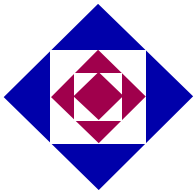
To be effective such a mechanism should work well both over secure networks as well as insecure networks.

In a credential-based access control system accesses to the storage entity must be accompanied with a valid capability that allows the client to perform the requested operation. A credential is a cryptographically secured capability and a capability is a set of rights the holder has on a stored object or storage entity.

The role of the Admin is to generate credentials for authorized clients at the request of the host. The

The role of the Storage Unit is to validate a capability presented by a Client:

- The requested operation is permitted by the capability based on a) the type of operation (e.g., read, write) and b) a logical match of the some other operation parameters



Julian Satran
IBM Research Lab in Haifa
Julian_Satran@il.ibm.com
+972 4 8296264

- The capability has not been tampered with, i.e., it was generated by the Admin and was rightfully obtained by the Client that presents it (either directly or via delegation).

Any scheme should allow for different security levels including data and request integrity and privacy.

The granularity at which the access control will operate must correspond to the granularity at which the storage can effectively "segregate" data (files, objects, volumes).

Computational requirements for a security framework should be adequate even for low-end devices but should enable more powerful devices to have improved security.

The trust assumptions should be made explicit in the framework.

As a base-line we should consider Admin and Storage as trusted entities and Clients as untrusted by other than its own users.

All forms of "operational" attacks should be considered (but not media removal).

3. What elements of the infrastructure should be standardized

To enable different providers for different elements (Admin, Storage, Clients) protocols between Admin and Clients as well as between Admin and Storage will have to be standardized. There is no legacy in this area!. For Client to Storage adjustments or extensions to existing protocols will be needed.

For Volume access control one can envision either extensions to different session establishment protocols or solutions based on access through management ports (newer and more amenable to change).

4. What is already there

A comprehensive security scheme for NFS-V4 and Object Storage. Both will have to be accommodated (not necessarily without any change).

A very weak SCSI access control mechanism for block storage – highly unlikely that it can be used directly but may become part of a larger solution.

5. What else should we tackle?

Uniform attribute sets (at least those concerned with access) ?