Scalable Privilege Management for a Net-Centric World

Arnon Rosenthal, Don Faatz
{arnie, dfaatz}@mitre.org

Abstract: Information will be widely shared only if it is seen to be protected appropriately. Protectors (security professionals and data providers) cannot make informed decisions on huge numbers of strangers, so access may be either too broad or too narrow. We propose an approach to managing privileges on data and services, as we move to a net-centric world?

Keywords: Security policy, authorization, net-centric, scalable

Research Objective: A new approach, model, and tools for administering privileges within a giant enterprise or collaborative (e.g., the US and state governments). The method will allow setting appropriate protections for large numbers of unanticipated uses.

Technical Approach:

Agencies are rightly skeptical of the net-centric security strategy: "allow everyone access to everything and monitor actual usage". This does not prevent damage (to confidentiality or integrity), and anomaly detectors overwhelm security officers with false positives. Yet, asking data providers or system administrators to determine who might benefit from access to each item negates net-centricity. These protectors lack the time, knowledge, and incentive to respond to myriad requests. Hence, access will be too broad and vulnerable to the increased insider threat (everyone can access everything), or else too narrow and slow, granting access to familiar collaborators (with little information flow, and no flexibility for emergencies).

We focus only on administering privileges on application level information (e.g., in databases or image repositories). We assume that other means provide prerequisites, such as:

- *Good faith* (but not necessarily diligence) from nearly all users and organizations.
- *Semantic understanding of data:* The data can be converted to a form the consumer understands – without this, there is no reason to request access. Security piggybacks on this, to ask about Location, Destination, etc.
- *Some shared roles:* (e.g., officer ranks, or functional roles, e.g., Operations, Logistics, Intelligence, …)
- *General security services:* authentication, secure transport, a trust infrastructure, auditing, protection from hacking attacks.

Our goal is to enable widespread data sharing with acceptable risk, by enabling more appropriate protection policies to be specified. The approach has three pillars. First, *user organizations* (still within the government) will help define the need to access information, in terms of suitably general privilege sets. Second, multiple gradations of enforcement will be provided, for improved flexibility. Third, unified management of enforcement actions will increase consistency of the enforcement policies and reduce workload. We discuss these pillars, in turn.

Users define "need to access" and review other users' requests. Rather than impose a large, uncompensated administrative load on data providers (and their security officers), we enlist consumer organizations that are deemed somewhat trustworthy to review requests from their own people. Thus, the provider delegates coarsely, and user organization does fine grained delegation. We also enlist help from consumers and tools that will suggest general privileges that are appropriate, allowing wholesale rather than retail consideration. Reviewers will normally be shown generalized requests (e.g., data about types of targets, or locations in a region), rather than rule on single accesses.

Graduated enforcement: This work defines intermediate levels of enforcement, that provide a significant level of protection with less burden on data owners. Examples include “allow if level-2 manager concurs”, or “notify data owner and person described”, or “flag for intensive auditing”. Administrative actions such as privilege upgrades (for self or others) are incorporated in the model, and hence also subject to these controls.

Unified enforcement: Today’s practice creates the nightmare of multiple enforcers (access controllers, notifiers, anomaly detectors), each managed in a different formalism by different managers. A change made in one enforcer requires manual intervention to become visible to others.

We hope to create a unified model by extending technologies such as attribute (and role) based access controls, plus trust management to provide very flexible controls on delegation. In particular, an administrator may grant exemption from an enforcement action (e.g., from dual signature, or from anomaly reports). Anomaly detection algorithms may be adapted to guess general classes of privileges that a user requests, and present the general issue for an administrator’s decision.

Conclusion: We need new techniques of *scalable* administration of privileges in a net-centric world. This research effort addresses the fundamental difficulties – too much low level enforcement in too many formalisms, with too little tool support.

Appendix: Illustrative Examples

A provider-specified coarse-grained policy (direct grant of a consumer’s privilege).

```
    Grant to US_Military: Read Access MediumResImage
    Enforce appropriateness of user request by
        Requires Officer-level-3 signature, Audit intensity = medium
```

Delegation of admin from a provider to a consumer-side administrator.

```
Grant to Officer-level-3 where assignment = planning
      /* administrative privilege to */ grant Read
                        on IMAGE where Image.Theater = $grantor.Theater
      /* safeguards on the act of granting, and on use of granted privilege */
      upon granting:   Requires Officer-3 confirmation, Audit_Intensity= High
      upon use: Audit-Intensity = medium, Imagery.Theater = $user.Theater
```

A customer request for privilege . Instead of asking about just the dock at Aden, the user describes her general need:

Request rights for High-Res-Imagery: Location =$User.Ship.NextPort

A different user, the Yemen expert might issue:

Request rights for High-Res-Imagery   Location =Aden