

CSE592: Security Policy Frameworks
Scott Stoller, Stony Brook University
Homework 1 (19 Sep 2007), Due 27 Sep 2007

Choose *one* kind of large organization, and try to think of parts of its security policy that could reasonably involve the following aspects. If you get stuck trying to illustrate all of these concepts using one kind of organization, you can use a second kind of large organization to illustrate some of them (if you do this, make sure each answer clearly indicates which kind of organization it is about).

The goal of this homework is for you to improve and demonstrate your understanding of these security policy concepts. It is a good idea to explain (justify) every answer, unless its correctness is so obvious that you can't think of anything useful to say to explain it. Some problems mention specific points that the explanation should address.

Do not use examples that appear in [samarati01access]. If you get some or all examples from other sources (textbooks, articles, lectures, etc.), cite the sources, as always.

All homework assignments should be done individually, unless the assignment specifies otherwise.

Homework submission instructions are on the CSE592 home page.

Here are some suggestions for kinds of large organizations: financial institution, consulting company, computer products and services company (e.g., IBM), health insurance company, hospital, university, government agency for tax collection (e.g., the U.S. Internal Revenue Service), government agency for immigration (e.g., the U.S. Citizenship and Immigration Services), military organization. You can choose one of these, or think of one yourself.

0. What kind of large organization did you choose?

1. Give two examples of permissions that should be controlled using DAC, and give specific DAC policies for those permissions. To justify the use of DAC, explain why controlling those permissions using MAC would be less appropriate.

Note: Two closely related permissions, such as "read permission for X" and "write permission for X" will be treated as one example. This applies to the questions below, too.

2. Give two examples of permissions that should be controlled using secrecy-based MAC [samarati01access, section 4.2]. Explain why controlling those permissions using DAC would be less appropriate.

3. Give two examples of permissions that should be controlled using integrity-based MAC [samarati01access, section 4.4]. Explain why controlling those permissions using DAC would be less appropriate. Discuss whether Biba's integrity-preserving policy (no read-up, no write-down) or one of the low-water mark policies is more appropriate for these permissions.

4. Give two examples of roles in the policy, and describe the permissions granted to each of those roles.

5. Give two examples of permissions that should be controlled using attribute-based access control (ABAC), and give specific ABAC policies for those permissions. Explain why simpler approaches, such as ACLs and RBAC, are unsuitable for controlling these permissions.

6. Give an example of a separation of duty requirement in the policy.

7. Give an example of permissions that should be controlled using a policy based on hierarchical relationships [samarati01access, section 6.1], and give a specific policy for those permissions.
8. Give an example in which it is desirable to use both positive and negative permissions. Discuss which conflict resolution strategy is most appropriate.
9. Give an example in which temporal authorizations should be used.
10. Discuss which kinds of administrative policy (centralized, hierarchical, cooperative, ownership, decentralized) [samarati01access, section 6.4] are appropriate for managing the policy.

Glossary

Please base your answers to questions 1-3 on the following definitions.

Discretionary access control (DAC): security models in which (1) access decisions are based on the identity of the requester, and (2) some users having a permission can pass it on to other users. Typically, there is a notion of "owner" of an object (resource), and the owner has permissions for the object and can pass those permissions on to other users. Less common, those other users can pass the permissions on to yet other users.

Mandatory access control (MAC): security models in which access decisions are based on the clearance of the subject, and the sensitivity (classification) of the information contained in the resource. There is an implicit assumption that users cannot change their clearance, or the sensitivity classification of information, so users cannot pass permissions on to other users.

References

[samarati01access] Pierangela Samarati and Sabrina De Capitani di Vimercati. [Access Control: Policies, Models, and Mechanisms](#). In R. Focardi and R. Gorrieri, editors, *Foundations of Security Analysis and Design*, volume 2171 of LNCS. Springer-Verlag, 2001.