

Collaboration requirements - A point-of-failure in protecting Information

Gio Wiederhold

Dep. of Computer Science

Stanford University, Stanford CA 94305

gio@cs.stanford.edu

Abstract

In settings where we have to collaborate with individuals and organizations who, while not being enemies, should not be fully trusted. The systems that collaborators must be authorized to access typically contain information that they should be able to receive, as well as information that should be withheld. Solutions based on extending access control methods to the problems raised in this setting are either awkward and costly, or unreliable.

An alternative approach to protection of mixed source information, complementing basic access control, is to provide filtering of results. Filtering of contents is also costly, but provides a number of benefits not obtainable with access control alone. The most important one is that the complexity of setting up and maintaining specific, isolated information cells for every combination of access rights held by collaborators is avoided. New classes of collaborators can be added without requiring a reorganization of the entire information structure. There is no overhead for internal use, i.e., for participants that are wholly trusted. Finally, since documents contents rather than their labels is being checked, cases of misfiled information will not cause inappropriate release.

The approach used in the TIHI/SAW projects at Stanford uses simple rules to drive filtering primitives. The filters run on a modest, but dedicated computer managed by the organization's security officer. The rules implement the institution's security policy and balance manual effort and complexity. By not relying on the database systems and network facilities, and their administrators a better functional allocation of responsibilities ensues.

Result filtering can also be used to complement access monitoring for pure intrusion detection since it can be implemented invisibly. The intruder can be given the impression of success, while becoming a target for monitoring or cover stories.