What Can Researchers Do to Improve Security of Data and Documents? (panel description)

Arnon Rosenthal
The MITRE Corporation
202 Burlington Road / K308
Bedford, MA 01730
+1-781-271-7577
arnie@mitre.org

ABSTRACT

Data security (protection of *information* rather than systems) goes far beyond the traditional questions of RDBMS grant/revoke, or security markings on documents. We will discuss what the new research agenda should be to impact the masses of systems.

Categories and Subject Descriptors

H.2.7 Database Administration–*security, integrity, and protection* D.4.6 Security and Protection–*access controls, information flow controls* K.5.1 Hardware/Software Protection –*proprietary rights*

General Terms

Security

Keywords

Security, Document Server, Database, Intellectual Property, Application Server, Information Release

1. Panel Statement

Universal access to the WWW has made security a top issue for all large web sites. Collaborative arrangements need to be created and ended, both safely and rapidly. One must enforce legally mandated privacy policies, and protect intellectual property. Traditional access control is much more difficult in today's complex architectures which include document managers, databases, middleware, and untrusted clients. Additionally, there are too few people skilled either in specifying policies, or in the technical means of enforcing them.

For many years, *data* security research (i.e., data model- or content-aware facilities) has had little impact on practice. Relevance will be even tougher now that the needs are spread far beyond the DBMS. Document security has been explored in a separate world from database security, leading to duplication and gaps, e.g., when documents are generated from and stored in databases.

The CIKM research community, with its expertise in modeling, [semi] structured data, declarative semantics, query compilation, constraints, triggers, indexes, etc. can play an important role in making future security systems more robust and easier to use. We need to focus on the key practical issues and to adapt ideas to vendor and administrator needs. Proposed techniques should emphasize *simplicity,* and pass the "giggle test" i.e. not be ridiculous ways for an enterprise to invest its resources.

The panel will ask what major advances are needed in data and document security, and what research questions do they raise *for the database and IR research communities.* Topics may include:

1. How can we handle *new kinds of policies* (e.g., privacy, intellectual property) in ever more *complex architectures* (enterprise, web, coalition), with *few skilled administrators*.
2. What concepts can we contribute to *simplify* implementation and management for the mix of release guards, DBMSs, policy management tools, systems management tools, …
3. For policy specification, can we push the work to domain experts, or should we emphasize powerful languages for use by experts? Can anyone (even experts) understand the effect of large number of policies?
4. What are the data security issues raised by fault tolerance (with reconfiguration of entire systems) and by defense in depth (where information may remain protected after an intrusion into the operating system)?
5. How can we best manage tradeoffs among the need for access versus desires to restrict access, between flexibility and the need for vital information highly resistant to attack?
6. What *research tasks* need to be done first? What new mechanisms will they depend on (e.g., PKI)?

Panel Members (partial list)

Arnon Rosenthal	(MITRE)
Carl Landwehr	(Mitretek)
Ken Moody	(U. Cambridge, UK)