Database Security 1
Access Controls

Dorothy E. Denning

SRI International

The objective of database access controls is to ensure the secrecy and integrity of data stored in the database. *Secrecy* requires that the data be protected from unuathorized disclosure through direct retrievals, browsing, inference, and leakage. *Integrity* or *authenticity* requires that the data be protected from unauthorized modification through updates, insertions, and deletions.

Access controls are modelled in terms of subjects (users), data objects, and access rights, where a subject is permitted access to an object in accordance with the authorized access rights. This authorization information can be represented as an *access matrix*, where the rows correspond to users, the columns to objects, and the entries within the matrix to access rights [1, 7, 4]. The access rights can be simple database operations such as *retrieve*, *insert*, etc., or they can be more complex and include predicates over the database or execution of access functions [6]. The authorization information can be implemented using *authorization lists*, which are lists of users permitted access to a given object, *capability lists*, which are lists of objects permitted to a given user, or *general rules*, which apply to all users and objects (e.g., a user's clearance must be at least that of the object's security classification level).

The talk discusses issues related to both security policy and its enforcement, including the unit of protected object, the dissemination and revocation of access rights, and the specification and representation of access rights.

An important issue is the unit of protection or level at which the model is applied. Many database systems protect objects at a low level corresponding to the physical structures in the database: relations (files), tuples (records), attributes (fields), and individual data elements. A few systems provide a high level of protection, where the objects can be either physical structures or database views (derived data). A low level approach is useful for attaching security classification labels to stored data (as mandated by some Department of Defense policies). The protected view approach, however, has several advantages over a low level approach: views give context to data, they provide a high level of abstraction corresponding to the way users see the database, they can incorporate access predicates in their definition, they allow the authorization data to remain static even when the underlying data is dynamic, they are independent of the physical representation of the data, they provide a means of addressing inference problems, and they allow for the release of sanitized views over sensitive data.

IBM's System R (SQL/DS) is an example of a relational database system that supports a high level approach through protected views [2, 5]. The protection mechanisms of System R are briefly described, including the specification, dissemination, and revocation of access rights. These mechanisms are contrasted with those of INGRES, which supports a somewhat different high level approach [8].

Many of the concepts described in this talk are also developed in my book [3], which gives an introduction to the entire area of cryptography and data security.

References

1. Conway, R. W., Maxwell, W. L. and Morgan, H. L. "On the Implementation of Security Measures in Information Systems." *Comm. ACM 15*, 4 (Apr. 1972), 211-220.

2. Date, C. J.. *An Introduction to Database Systems.* Addison-Wesley, 1983.

3. Denning, D. E.. *Cryptography and Data Security.* Addison-Wesley, Reading, Mass., 1982.

4. Graham, G. S. and Denning, P. J. Protection -- Principles and Practice. Proc. Spring Jt. Computer Conf., Vol 40, AFIPS Press, Montvale, N. J., 1972, pp. 417-429.

5. Griffiths, P. P. and Wade, B. W. "An Authorization Mechanism for a Relational Database System." *ACM Trans. on Database Syst. 1*, 3 (Sept. 1976), 242-255.

6. Hoffman, L. J. "The Formulary Model for Flexible Privacy and Access Control." *Proc. Fall Jt. Computer Conf. 39* (1971), 587-601.

7. Lampson, B. W. Protection. Proc. 5th Princeton Symp. of Info. Sci. and Syst., Princeton Univ., Mar., 1971, pp. 437-443. Reprinted in ACM Oper. Syst. Rev., Vol. 8 (1), 18-24, (Jan. 1974)

8. Stonebraker, M. and Wong, E. Access Control in a Relational Data Base Management System by Query Modification. Proc. 1974 ACM Annual Conf., ACM, Nov.1974, pp. 180-186.