RECORDING ACCESS TO SENSITIVE DATA

In today's distributed IT environments, protecting sensitive and confidential corporate data is of vital importance. However, it is often difficult for system security personnel to determine how and where such data are accessed.

- DB2 provides access controls to ensure that only authorized users access the data.
- The DB2 audit trace facility will record how users access sensitive tables.
- DB2 log analysis will show the actual modifications to the data.

However, these DB2 facilities are not sufficient to fully record all access to sensitive data, for the following reasons:

- Log Analysis will not show read (SELECT) access.
- The audit trace records only the first read or write SQL statement in a logical unit of work.
- The trace records do not provide the contents of the input variables submitted with the SQL statement. Without this information, full access recording is not possible.
- DB2 auditing requires that an auditing trace be enabled. If many tables are audited or intensely used, the operating cost of tracing may be excessive.

DBARS

DB2 Access Recording Services ("**DBARS**") is a product developed by Software Product Research.

- DBARS records all accesses to sensitive DB2 tables. Depending on the degree of auditing requested, read (SELECT) and write (DELETE, INSERT and UPDATE) access is recorded.
- DBARS records SQL statements with their associated input variables ("host variables").
- DBARS provides a powerful **Recorder Scan** utility.
- Because DBARS has its own interface to DB2 and does not depend on DB2 tracing, recording overhead will be acceptable.

The DBARS Recorder

For each access to an audited table, **DBARS** inserts following data into its **Recorder**:

- The **text of the SQL statement**, with all input variables in the statement replaced by their contents.
- The **context** of statement execution:
  - the date and time of execution
  - the identification of the user submitting the statement
  - the z/OS job name
  - the name of the program used for access
  - the number of rows modified
  - the SQLCODE indicating successful or failing access
  - if distributed access: the names of the external server, application and workstation

During product installation, the DBARS Recorder is implemented as a DB2 table or a VSAM cluster.

Inspecting the Recorder

The **Recorder Scan** utility searches the Recorder for specific access events. The user supplies one or more of the following search criteria:

- **Recorder Columns**.
- **Audited table column names** used in the recorded SQL statement. This will show all SQL statements that reference the table column.
- **Audited table column values**. This will show all SQL statements that reference the column with the specified value. This option may be used to report all recorded access for a given table "key".

Archiving the Recorder

The DBARS archiving function transfers the Recorder to a sequential dataset or to a DB2 table, so that recorded information can be kept for a longer period of time. An archive operation does not disrupt the recording process. The product supplies a utility to scan an archived Recorder using the search criteria, described above.

Customizing DBARS

Recorded data can be stored in a DB2 table, which can subsequently be processed by customer procedures. In addition, an installation may provide a REXX user exit to be invoked when an access is stored in the Recorder. The exit receives the Recorder columns as its input arguments.