



DBARS From Software Product Research

Protecting Sensitive DB2 Table Data

Around the world, confidential information is stored within DB2 databases. While mainframe security software and DB2 privileges protect against unauthorized access to systems, files and DB2 tables, they do little to conveniently and comprehensively report all accesses to DB2 tables and what was done within those tables. In the wrong hands, confidential information can have a negative impact on a corporation and affect the privacy of customers and employees. Furthermore, in many countries, privacy laws have been instituted to protect against unauthorized disclosure of such information.

DB2 Access Recording Services—DBARS—from Software Product Research adds a level of security auditing for DB2. Unlike a DB2 audit trace that records only the first read or write SQL statement in a logical unit of work, DBARS records all accesses to sensitive data in auditable DB2 tables. Additionally, DBARS monitors the contents of the input variables submitted with the SQL statement. DBARS has its own DB2 interface and does not depend on DB2 tracing. This eliminates the performance constraints inherent with a DB2 audit trace. With DBARS in place, it becomes exceedingly difficult for a hacker to “fake” out the system using an innocent read or write SQL statement prior to statements designed for mischief.

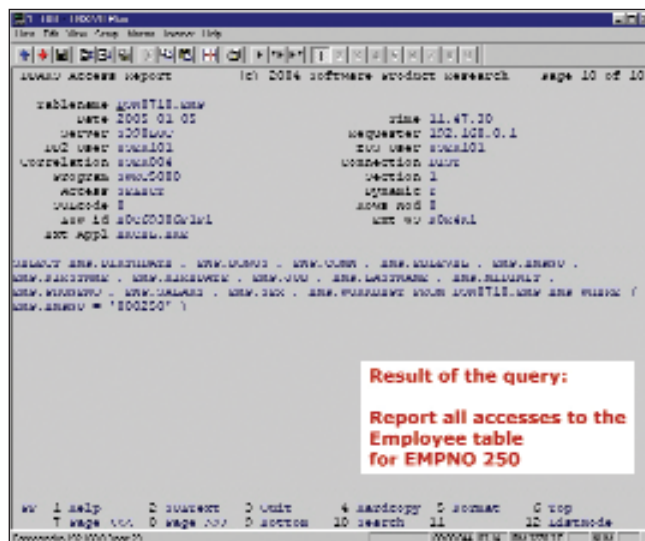
How DBARS Works

Operating most efficiently as a started task, DBARS records all SQL read (SELECT) and write (DELETE, INSERT, and UPDATE) access to all DB2 tables defined with the AUDIT ALL or AUDIT CHANGE attribute. All SQL statements intercepted by DBARS, along with their accompanying variables, are stored in a DB2 table named the Recorder. The Recorder table provides the text of the SQL statement as well as the context of execution, which includes:

- Date and time of access
- Name of the DB2 application server
- DB2 and z/OS userid, program name, z/OS job name
- Connection type, LUW_id, access type (dynamic or static)
- Distributed access information: external server name, application name, workstation name
- SQLCODE and number of rows modified by the statement.

DBARS Reporting

DBARS reports are obtained interactively through a TSO interface or through batch processing. Information security and auditing professionals, as well as people responsible for



ensuring compliance to government regulations, can use the reports produced by DBARS.

DBARS reporting searches the Recorder table for DB2 accesses, using as search criteria the columns of the Recorder table and the expressions contained in the recorded SQL statement.

Sample Recorder Query

An insurance company keeps medical information about its customers in a DB2 table. According to privacy legislation, a customer can request to inspect all accesses to his medical dossier. Such a customer request could be handled using the following DBARS report query:

```
report all accesses to table "customer_medinfo" where "custno = x"
```

The DBARS report would show when and by whom the customer’s medical data has been viewed or altered.

DBARS can be used across a variety of industries. Information stored in DB2 databases is of enormous value to corporations. Misuse of this information can launch competitive and legal challenges and penalties. The additional layer of audit protection provided by DBARS helps companies monitor access. DBARS is available for a free 60-day trial via a zipped e-mail file. **Z**

Software Product Research, Binnenheide 30A, B-2288 Bouwel, Belgium
Voice: +32 14 501305; e-mail: inf@sprdb2.com;
Website: www.sprdb2.com.