Access control—the key to information security in a remote user system

by BRUCE E. SPIRO
Advanced Information Management Inc.
Woodbridge, Virginia

We are moving to remote user systems with alarming speed and often with little thought for security. Market forces and operational necessity are the driving factors that make this movement necessary. We cannot obstruct this movement with overzealous protestations. On the other hand, we must not overlook the essential need for security in this expanding environment. The proper people must have relatively easy and convenient access to the data and processing support to which they are authorized—and only to that which is authorized.

Effective access control is not a simple matter of installing IDs and passwords, and trusting that things will work out. We start with a security analysis of the communications network to determine where there are weak points and what controls can be applied that decrease the likelihood that an unauthorized individual can use the communication capability of the system.

We then proceed inward, looking at each level of the system to determine what protection is required and what controls are available. When a series of processors are coupled together, each will have different requirements based on the criticality and sensitivity of the data and programs contained. Each will have different protective capabilities based on the specific operating system and security features installed. The objective is to ensure separation and control of datasets and programs so that there is no opportunity to crossover from an authorized process to one that is not authorized.

The integrity of the operating system is critical. What is possible may not be what is there. A close review by qualified people is essential. Often techniques to bypass security features are installed to make work a bit easier for test and development effort. Sometimes these bypasses remain in a production system and create openings that destroy the protective barriers that have been built.

Finally, the entire security process must be reviewed to ensure that it is consistent across the board. All too often we see technically accurate and well thoughtout security systems that in reality provide no protection at all because there is no administrative procedures to manage passwords or something else as seemingly innocuous.

Effective security is the combination of network control, system integrity, identification, protection, and procedures brought together in a consistent access control package. Weakness in any area may mean that you have no security at all.
Systems software and languages encompass the tools used to build, maintain, and operate application systems. While many of these tools are implemented in software, others are based on concepts and techniques (i.e., methodology). Recent explosive growth in the number and variety of vigorously acclaimed software and methodology components is generating uncertainty and controversy over their value to a user organization, their impact on development organizations, and their relationship to one another.

Among the specific topics in this area are:

- Computer languages, including specification languages, very-high level languages, database query languages, and distributed languages.
- Methodologies and tools for design and coding, including structured programming, libraries of reusable code, in-house standards, design reviews, workbench facilities, and design methods for distributed software systems.
- Data management tools, including data modeling, design, and analysis methods, entity-relationship approaches, relational technology, data dictionary and directory systems, information retrieval systems, and techniques of data administration.
- Tools for systems analysis, including structured analysis concepts, structured documentation software, prototyping, generalized transaction processors, and methods for choosing packaged application software.
- Project management tools, including standardized life cycles, project planning techniques, project control techniques, project management software, productivity measurement methods, software maintenance strategies and tools, and quality assurance programs.
- Operational tools, including operating systems, storage management methods, sorting and searching techniques, resource scheduling algorithms, resource accounting methods, system performance measurement facilities, and teleprocessing monitors.
- Support structures, including methodology development, training, methodology integration, and revised role and skill definitions.