Database Security, Compliance and Audit

By Charles Le Grand and Dan Sarel

A major control objective for any organization is to protect sensitive data. Data protection or information security is protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction to provide confidentiality, integrity and availability.1

In the early years of database management systems (DBMS), such a system was acclaimed as a tool for centralizing control over data access. But as controls frequently migrate around within the information infrastructure, data access controls have tended to migrate to other points, such as network perimeter controls, user identity and access management, and the application systems that access databases. The tendency has been to presume a database is protected because of the broad and diverse set of controls applicable to data access. However, the breadth and diversity of controls have taken away the centralized access control at the database itself, opened key weaknesses in data protection and allowed some of the most serious threats to data to go largely unmanaged.

The world is characterized by technology that makes the news almost daily with stories of loss, theft or disclosure of sensitive information. The 2007 Computer Crime and Security Survey, by the Computer Security Institute (www.goci.org), identifies respondents that actually detected attacks and abuse in the last 12 months. Insider abuse of net access is at 59 percent, unauthorized access to information 25 percent, and theft of customer or employee data 17 percent. (Because of the general lack of monitoring, one can safely assume most threats remain undetected!) These numbers also seem low based on media accounts. And, people are beyond the point of being shocked or even surprised when yet another employee, executive or management team betrays a trust and costs the company and its stakeholders millions or even billions.

Clearly there is a strong need for improved and enforced accountability management. This article will review first the nature of access controls in general and where they are found, and then will discuss access controls at the database level.

Where Are Data Access Controls?

Data access controls tend to be distributed in many organizations. They have evolved to that state by systems groups attacking the problem of the moment, placing controls where they can protect against a given threat, and avoiding performance bottlenecks and impacts on performance caused by using controls such as native logging and protection in the commercial DBMS. Commercial enterprise resource planning (ERP) systems have also contributed to the distribution of controls by seeking to be the all-in-one system solution with minimal reliance on other controls.

The following are some key distributed control types:

- **Perimeter controls** (e.g., firewalls, intrusion protection, malware detection) attempt to keep the bad guys out. But they have two fundamental weaknesses. First, the bad guys are frequently a step ahead of the protection, and once they get in they are hard to find and block. Second, the insider threat is now recognized to be at least as serious as the threat of attack from outside the organization. Perimeter controls have reached a state of maturity where they are recognized as essential, but they are also known to be inadequate against certain attacks and in need of supplementation by other controls.
- **User identity and access management** is the essence of deciding who is allowed to do what and then monitoring to ensure things are as they are supposed to be. However, these controls tend to be dispersed across a wide variety of business functions including policy administration, personnel administration (e.g., keeping up with access privileges as people move to new positions), managing group access rights (e.g., people in payroll can see some human resources [HR] data, but cannot access payroll info), separation of duties (e.g., not allowing the same person to approve new vendors and payments to them), monitoring access rights for application of the least-privilege principle (e.g., access to only the data needed for the position, limited access for changing or deleting data, special privileges required to override controls), revoking rights when employees or other users leave the company or change roles, and monitoring all changes and exceptions to access privileges rules.

The subject is complex and requires close coordination across diverse business functions—some of which do not hold information security high on their priorities or the list of things that will get them recognized and promoted. Identity and access management is an area in need of some serious audit attention, but that is the subject of another article.

- **Application systems** (particularly ERP systems) are a focal point for data access protection. And, if user identity and access management is complex, application systems can be more so. Applications administer remote (sometimes global) access by customers, remote and local employees, and often business partners. Multiple applications may access the same database and be subject to differing sets of controls.
Independent audit software tools\(^2\) are available to audit the management of separation of duties and other controls applicable to the popular ERP systems and other means of addressing user identity and access privileges.

Application systems are subject to changes including security patching, maintenance and enhancements by the software provider's and/or system's employees, and emergency fixes to restore operations in the event of outages. Application systems may be maintained and enhanced by the original vendors and/or by outsourced vendors, including offshore providers.

- Privileged users have access rights beyond those needed for routine business operations. Database technical and operational controls (such as backup/recovery, system upgrades, checkpoint/restart, maintaining pointer integrity, optimizing physical data storage and performance) take place outside of the access constraints of application systems and most of the identity and access management processes, but must also be closely coordinated with application and user requirements. They are perhaps the most important point for knowing exactly who did what with the data.

Systems and network administration, data and database administration, security operations, systems development and maintenance, systems programming, and other technical functions (sometimes called “superusers”) are a security management topic in their own right. All have legitimate needs for access to databases to perform maintenance, test changes, correct problems, and restore or continue operations. Some believe the people in these functions cannot be controlled or monitored. While that is not true, such control may be difficult and one can count on those people to resist control changes they may see as making their jobs more difficult or impossible.

It is important to note that the technical people with access to databases for the most part reliably perform a crucial function, and the enterprise’s systems and services could not operate without their ongoing support. However, as recent breaches have clearly shown,\(^4\) they also represent significant risk as they could easily corrupt, destroy or steal copies of sensitive data, and must be subject to separation-of-duties controls and monitoring, as appropriate to their elevated level of authority and trust. Physical and logical controls within and outside their sphere of operational control are needed to provide evidence of their actions, and must be sufficient to clearly establish fault or innocence.

**Centralized Data Access Controls**

A time-proven rule for protection and monitoring is to provide controls as close as possible to the functions subject to the controls. In the case of database access controls, the ideal location is on the database server. Not only does this simplify the access protection model, it supports separation of duties, forensics and audit requirements, and can make it difficult for anyone to avoid or bypass those controls.

The controls can also be provided via a network security appliance.\(^4\) But those controls are apart from the device that actually manages the database and, therefore, can be bypassed by people with physical or superuser access to the server. They are also less effective than host-based solutions in monitoring privileged users (such as database administrators and application developers). This discussion addresses the controls as implemented via the agent and monitoring system depicted in figure 1.

This simple solution employs a software agent that runs on the database server, enabling policy-based data access protection and monitoring.\(^5\) By communicating with a separate system (i.e., the database control agent monitor), the agent can ensure that it has not been modified by persons with administrative access to the database. Note, the agent should be capable of operating in a monitoring-only mode for analysis, discovery or audit purposes, or in a full-protect mode to enforce security policy at the database level.

This type of centralized database access control provides a focal point for knowing exactly who accessed what data—not just that access was granted to a trusted application, in which case one would have to turn to the application for such evidence. It is also not subject to the limitations of identity access management or applications, because the policy can be specified right in the agent itself. And, if protection (preventive controls) is enabled, rather than just monitored (detective controls including alerts for inappropriate access attempts), the agent can be tuned to specifically manage known threats to data.

**Protection From Software Vulnerabilities**

Software vulnerabilities subject to exploit can occur in many places throughout systems and networks: web pages and other Internet-facing systems; systems that communicate across the Internet, such as through e-mail and file transfer; and even DBMS. Vendors frequently provide patches for software vulnerabilities, but change management (particularly patch management) is fraught with its own challenges and changes, and patches may not be applied in a timely manner (if at all). This leaves the vulnerabilities to be managed by “some other means.”\(^6\)
While many exploit attempts today still seek to satisfy the attacker's ego or perhaps embarrass the target enterprise, the real threats are in stealing or manipulating data for profit whether by insiders, outside attackers or perhaps insiders cooperating with outsiders (including organized crime). Inasmuch as the database is a prime target for attacks, it makes sense to place controls around the database to enforce access policies and protect the data, even if other protective controls are compromised. The concepts of compensating, complementary and redundant controls recognize that individual controls are fallible and secondary controls are needed to detect when primary controls fail.

An effective access protection control will recognize inappropriate data access attempts, because they violate an information security policy, even if they appear to come from a trusted application system or a trusted individual with the ability to bypass other system and network controls. Of course, not every exception can be determined in advance, so it may be necessary to apply monitoring controls to certain privileged users, such as the database administrator (DBA), rather than taking a chance on preventing them from performing necessary tasks. But, it is still essential to log and monitor every procedure performed against a database, especially when the procedure affects sensitive data.

While they are not yet common, it is possible to implement controls specifically to compensate for known system vulnerabilities and their related exploits.\(^7\)

Other solutions include custom designed procedures and programs specifically to monitor or protect against (or mitigate) known vulnerabilities that cannot feasibly be eliminated. An example of this type of control is one of a broader nature, focused on specific vulnerabilities in change management. This solution establishes a signature for sensitive components within a network configuration and terminates any task that attempts at processing and would change the signature.\(^8\) In this example solution, the software provider must be constantly vigilant to ensure that new and emerging threats are addressed in the protection.

**Hardening System Components to Enhance Database and Access Controls**

Applications, network devices and even personal computers can be “hardened” to enhance their protection against known types of attacks. Hardening is the process of securing a system especially to protect it against attackers. It is one of the most efficient ways to combat vulnerabilities.

Hardening typically includes removal of unnecessary usernames or logins and disabling or removing unnecessary services. By removing all system components that are never used, an enterprise can remove all the known, and as-yet-unknown, vulnerabilities that these components bring with them.

Database security may require hardening of the security settings of the database management software upon installation and once a specific database (often referred to as an instance) is established and configured. Additionally, many database utilities have their own enhanced security that can be enabled, but is disabled by default. An example is establishing the password on the Oracle listener process, to ensure that unauthorized users cannot change configurations related to the database management software.

The Center for Internet Security (CIS)\(^9\) provides how-to guidance and tools to harden systems. CIS benchmarks support available high-level standards that deal with the why, who, when and where aspects of IT security by detailing how to secure an ever-widening array of workstations, servers, network devices and software applications in terms of technology-specific controls. CIS scoring tools analyze and report system compliance with the technical control settings in the benchmarks. Hardening of databases is not a one-time procedure. Any new database must be hardened, and hardening must be undertaken with every upgrade of the DBMS as well as the operating system that runs it. New threats can also bring about changes in hardening processes. Resources such as those from CIS must be constantly monitored for new hardening guidelines, as they change frequently.

**Database Access Protection and Compliance Requirements**

Information security requirements must provide a proper balance between too much access control and too much freedom of access. Compliance requirements vary by industry and type of company, and each enterprise must interpret the requirements and manage its activities accordingly. There is no silver bullet to ensure compliance. Compliance is best accomplished by meeting requirements and ensuring that the ways in which requirements are met actually provide effective security and accountability.

Compliance alone is merely meeting a baseline set of minimum requirements, and the minimum is rarely sufficient. An organization can be in compliance with many requirements, but still not have effective security. The goal is to provide security first, and compliance as required.

The Payment Card Industry (PCI) Data Security Standard (DSS) is a good example of information security requirements with broad applicability. PCI requirements have gained stature in recent years and they apply to any enterprise that processes, stores and transmits cardholder account data. PCI compliance must be demonstrated and documented through automated and manual system audits.

The 12 major PCI DSS requirements (see figure 2) are structured to promote effective information security policies, secure networks, protected cardholder data, vulnerability management, strong access controls, and regular monitoring and testing. Central to all PCI requirements is the need to protect data access to ensure accountability, privacy and data integrity. The simple goal is to ensure that only authorized individuals have access and all access is monitored. To limit access to only people whose jobs require it, access protection must apply to identifying the sensitive data elements; the
methods for managing user credentials and access rights; and the records of who accessed what, when and what they did with it.

A particular enterprise’s compliance requirements may not include those of PCI DSS. If that is the case, they can accumulate their own list of compliance requirements from policies, procedures, agreements with customers and business partners, industry guidelines and requirements, regulations, and legislation. But PCI DSS is innovative, strong and quite clear guidance (as opposed to many other standards), and is applicable to any sensitive data in a database.

However, regardless of the solution, one should find information access protection at the heart of the requirements.

**Database Access Control Objectives**

A key component for identifying the steps in a database access protection audit is to identify the risks associated with the data maintained in the database and the potential impacts if risks materialize. For each control objective, the auditor must assess the specific controls in place and consider the risks and consequences if the objectives are not consistently and continuously met. Database access control objectives include:

- Appropriate assignment of responsibilities including separation of duties
- Access allowed only as appropriate (no unauthorized access)
- Completeness and accuracy of data in the database
- Evidence that each transaction or update is accurately applied and recorded
- Appropriate management of data sharing
- Adequate transaction/access audit trails
- Adequate service level for database users
- Data recorded in the appropriate calendar period
- Ability to detect and recover any failure of the DBMS
- Sufficient evidence and analysis to detect and recover from attack, fraud or embezzlement
- Current and adequate documentation. Documentation to include for database structure:
  - How security is achieved
  - Recovery actions
  - Reorganization changes

Documentation to include for each data element:

- Precise and unambiguous definition
- Source
- Frequency of change
- Individual accountable for correctness
- Relationship to other data items
- Program(s) and individuals with authorized access and the type of access
- Physical devices authorized to access (e.g., payroll department only)
- Continuity of processing
- Compliance with internal and external policies, standards and requirements
- Effective management of systems development, maintenance and changes/patches
- Periodic independent database audits

This list of control objectives was selected for relevance to database security and access control. A broader scope audit program is required for audits with a different purpose or objective.

**Auditing Database Access**

Conceptually, database auditing focuses on answering some fairly basic questions: How does one know, and how can one verify who accessed and/or changed the data? When? How was the content changed? The difficult part lies in assessing the full scope of controls to determine their effectiveness in fully recording all accesses; ensuring only authorized access; and maintaining unimpeachable evidence for management, audit, assurance and forensics purposes.

Database controls and audits must address:

- User interfaces
- Operation of the DBMS
- Database administration
- Data definition and documentation
- Security and access
- Organizational policies and priorities
- Backup and recovery
- Business continuity
- Compliance with standards and requirements

However, not all of these areas are necessarily relevant to an audit of database access management and compliance. Each area of database management has its own set of control objectives, and the objectives frequently apply to multiple areas.

Auditors must audit, evaluate and test the controls they find in place for database protection and monitoring, and their assessment must be of the existing controls rather than the controls they believe should be in place. However, audit
recommendations can focus on moving the enterprise to a more reliable and efficient approach to information protection and access control.

Conclusion

To summarize, access protection begins with understanding who accesses the data, for what purposes and with what permission. The set of controls relevant to database access management is broad and complex, and touches many areas of the business and technology.

The way to solve a set of problems as large and complex as information access protection is to establish priorities and begin solving the most significant problems first, one at a time, within an overall plan to provide and maintain a reasonable level of risk and substantial compliance with requirements.

At the core of business controls over information is the need to protect data access to ensure accountability, privacy and data integrity. The simple goal is to ensure only authorized individuals have access and all access is monitored. To limit access to only people whose jobs require it, access protection must apply to identifying the sensitive data elements; the methods for managing user credentials and access rights; and the records of who accessed what, when and what they did with it.

A single source for recording all access to the database is an efficient approach to controls, assurance and auditing, and can be significantly less demanding than the effort needed to manage or audit controls based in multiple locations. When controls are centralized in a single source, they facilitate the ability to verify compatibility across multiple operational areas. One may hear that the DBMS controls cannot be activated because they impact performance too severely. And, while that may be true, the alternative controls described above can provide a reliable centralized access control and can do it efficiently without negatively impacting system performance.

Author's Note

This article is based on a larger work authored by Charles Le Grand and Dan Sarel, published in the April 2008 issue of EDPACS, available at www.informaworld.com/smpp/content~content=a792908951~db=all~order=page.

Endnotes

3 See, for example, the case of Fidelity National Information Services where a database administrator stole 8.5 million customer records and sold the information to data brokers.
5 The only example of such a solution that the authors are aware of is Hedgehog by Sentrigo, www.sentrigo.com.
6 A treatise on change and patch management, with clues as to why patches may not be applied, can be found in The Institute of Internal Auditor (IIA)’s Global Technology Audit Guide. More technical documents include the IT Process Institute (ITPI)’s Visible Ops Security, the update to the Visible Ops Handbook (www.itpi.org).
7 The authors are only aware of one solution for database protection that provides vulnerability protection at the database server for known vulnerabilities in DBMS software: Sentrigo.
8 Tripwire (www.tripwire.com) and Network Authority, by AlterPoint (www.alterpoint.com) are examples of this type of control that protects against unauthorized changes.
9 Center for Internet Security, www.cisecurity.org

Charles Le Grand

is a principal advisor of the TechPar Group, and the former director of research and technology for The IIA Inc.

Dan Sarel

is the vice president of Sentrigo Inc. and is responsible for directing Sentrigo’s product definition and design.