Trends in security and data restortation

KEYWORDS

Zarana C. Padia	Shweta S. Kulshreshtha	Ketan Bhimani
MCA, Shree Laxminarayan Dev College of Computer Applications, Bharuch, Gujarat, India	MBA, R.K.School of Business Management,Rajkot Gujarat, India	CTO, Epitome Corporation Pvt. Ltd., Ahmedabad, Gujarat, India

ABSTRACT *In traditional database security research, the database is usually assumed to be trustworthy. Under this assumption, the goal is to achieve security against external attacks (e.g. from hackers) and possibly also against users trying to obtain information beyond their privileges, for instance by some type of statistical inference. However, for many database applications such as health information systems there exist connecting interests of the database owner and the users or organizations interacting with the database, and also between the users.*

Therefore the database cannot necessarily be assumed to be fully trusted. In this extended abstract we address the problem of dining and achieving security in a context where the database is not fully trusted, i.e., when the users must be protected against a potentially malicious database. Moreover, we address the problem of the secure aggregation of databases owned by mutually mistrusting organizations.

INTRODUCTION :
Information stored in databases is often considered as a valuable and important corporate resource. Many organizations have become so dependent on the proper functioning of their systems that a disruption of service or a leakage of stored information may cause outcomes ranging from inconvenience to catastrophe. Corporate data may relate to financial records, others may be essential for the successful operation of an organization, may represent trade secrets, or may describe information about persons whose privacy must be protected. Thus, the general concept of database security is very broad and entails such things as moral and ethical issues imposed by public and society, legal issues where control is legislated over the collection and disclosure of stored information, or more technical issues such as how to protect the stored information from loss or unauthorized access, destruction, use, modification, or disclosure.

1.1 Identification, Authentication
Usually before getting access to a database each user has to identify himself to the computer system. Authentication is the way to verify the identity of a user at log-on time. Most common authentication methods are passwords but more advanced techniques like badge readers, biometric recognition techniques, or signature analysis devices are also available.

1.2 Authorization, Access Controls
Authorization is the specification of a set of rules that specify who has which type of access to what information. Authorization policies therefore govern the disclosure and modification of information. Access controls are procedures that are designed to control authorizations. They are responsible to limit access to stored data to authorized users only.

1.3 Auditing
The requirement to keep records of all security relevant actions issued by a user is called auditing. Resulting audit records are the basis for further reviews and examinations in order to test the adequacy of system controls and to recommend any changes in the security policy.

2. Fundamental Data Security Requirements
The following sections describe the basic security standards that technology must ensure:

2.1) Confidentiality
A secure system ensures the confidentiality of data. This means that it allows individuals to see only the data that they are supposed to see. Confidentiality has several different aspects, discussed in these sections:

- Privacy of Communications
- Secure Storage of Sensitive Data
- Authenticated Users
- Granular Access Control

2.1.1 Privacy of Communications
How can you ensure the privacy of data communications? Privacy is a very broad concept. For the individual, it involves the ability to control the spread of confidential information such as health, employment, and credit records. In the business world, privacy may involve trade secrets, proprietary information about products and processes, competitive analyses, as well as marketing and sales plans. For governments, privacy involves such issues as the ability to collect and analyze demographic information, while protecting the confidentiality of millions of individual citizens. It also involves the ability to keep secrets that affect the country's interests

2.1.2 Secure Storage of Sensitive Data
How can you ensure that data remains private, once it has been collected? Once confidential data has been entered, its integrity and privacy must be protected on the databases and servers where it resides.

2.1.3 Authenticated Users
How can you designate the persons and organizations who have the right to see data? Authentication is a way of implementing decisions about whom to trust. Authentication methods seek to guarantee the identity of system users: that a person is who he says he is, and not an impostor.

2.1.4 Granular Access Control
How much data should a particular user see? Access control is the ability to cordon off portions of the database, so that access to the data does not become an all-or-nothing proposition. A clerk in the Human Relations department might need some access to the emp table—but he should not be permitted to access salary information for the entire company. The granularity of access control is the degree to which data access can be differentiated for particular tables, views,

rows, and columns of a database.

2.2) Integrity

A secure system ensures that the data it contains is valid. Data integrity means that data is protected from deletion and corruption, both while it resides within the database, and while it is being transmitted over the network.

Integrity has several aspects:

- System and object privileges control access to application tables and system commands, so that only authorized users can change data.
- Referential integrity is the ability to maintain valid relationships between values in the database, according to rules that have been defined.
- A database must be protected against viruses designed to corrupt the data.
- The network traffic must be protected from deletion, corruption, and eavesdropping.

2.3) Availability

A secure system makes data available to authorized users, without delay. Denial-of service attacks are attempts to block authorized users' ability to access and use the system when needed. System availability has a number of aspects.

Resistance: A secure system must be designed to fend off situations or deliberate attacks that might put it out of commission. For example, there must be facilities within the database to prohibit runaway queries. User profiles must be in place to define and limit the resources any given user may consume. In this way, the system can be protected against users consuming too much memory or too many processes (whether maliciously or innocently), lest others be prevented from doing their work. Scalability System performance must remain adequate regardless of the number of users or processes demanding service.

3) Security Requirements in the Internet Environment

The Internet environment expands the realm of data security in several ways, as discussed in these sections:

- Promises and Problems of the Internet
- Increased Data Access
- Much More Valuable Data
- Larger User Communities
- Hosted Systems and Exchanges

3.1 Promises and Problems of the Internet

Information is the cornerstone of e-business The Internet allows businesses to use information more effectively, by allowing customers, suppliers, employees, and partners to get access to the business information they need, when they need it

Customers can use the Web to place orders that can be fulfilled more quickly and with less error, suppliers and fulfillment houses can be engaged as orders are placed, reducing or eliminating the need for inventory, and employees can obtain timely information about business operations. The Internet also makes possible new, innovative pricing mechanisms, such as online competitive bidding for suppliers, and online auctions for chain—too often cuts out the information security the middleman provides. Likewise, the user community expands from a small group of known, reliable users accessing data from the intranet, to thousands of users accessing data from the Internet. Application hosting providers and exchanges offer especially stringent—and sometimes contradictory—requirements of security by user and by customer, while allowing secure data sharing among communities of interest. While putting business systems on the Internet offers potentially unlimited opportunities for increasing efficiency and reducing cost, it also offers potentially unlimited risk. The Internet provides much greater access to data, and to more valuable data, not only to legitimate users, but also to hackers, disgruntled employees, criminals, and corporate spies.

3.2 Increased Data Access

One of the chief e-business benefits of the Internet is disintermediation. The intermediate information processing steps that employees typically perform in traditional businesses, such as typing in an order received over the phone or by mail, are removed from the busyness process. Users who are not employees and are thus outside the traditional corporate boundary (including customers, suppliers, and partners) can have direct and immediate online access to business information that pertains to them.

3.3 Much More Valuable Data

E-business relies not only on making business information accessible outside the traditional company, it also depends on making the best, most up-to-date information available to users when they need it. For example, companies can streamline their operations and reduce overhead by allowing suppliers to have direct access to consolidated order information. This allows companies to reduce inventory by obtaining exactly what they need from suppliers when they need it. Companies can also take advantage of new pricing technology, such as online competitive bidding by means of exchanges, to obtain the best price from suppliers, or offer the best price to consumers.

3.4. Larger User Communities

The sheer size of the user communities that can access business systems by way of the Internet not only increases the risk to those systems, but also constrains the solutions that can be deployed to address that risk. The Internet creates challenges in terms of scalability of security mechanisms, management of those mechanisms, and the need to make them standard and interoperable.

3.4.1 Scalability

Security mechanisms for Internet-enabled systems must support much larger communities of users than systems that are not Internet-enabled. Whereas the largest traditional enterprise systems typically Supported thousands of users, many Internet enabled systems have millions of users.

3.4.2 Manageability

Traditional mechanisms for identifying users and managing their access, such as granting each user an account and password on each system she accesses, may not be practical in an Internet environment. It rapidly becomes too difficult and expensive for system administrators to manage separate accounts for each user on every system.

3.4.3 Interoperability

Unlike traditional enterprise systems, where a company owns and controls all components of the system, Internet-enabled e-business systems must exchange data with systems owned and controlled by others: by customers, suppliers, partners, and so on. Security mechanisms deployed in e-business systems Must therefore be standards-based, flexible, and interoperable, to ensure that they work with others 'systems. They must support thin clients, and work in multitier architectures.

3.5 Hosted Systems and Exchanges

The principal security challenge of hosting is keeping data from different hosted user communities separate. The simplest way of doing this is to create physically separate systems for each hosted community. The disadvantage of this approach is that it requires a separate computer, with separately installed, managed, and configured software, for each hosted user community. This provides little in the way of economies of scale to a hosting company. Several factors can greatly reduce costs to hosting service providers. These factors include mechanisms that allow multiple user communities to share a single hardware and software instance; mechanisms that separate data for different user communities; and ways to provide a single administrative interface for the hosting provider.

Conclusion

The Chapter has proposed models and techniques which provide a conceptual framework to counter the possible threats to database security. Emphasis has been given to the discussion of techniques with the main goal to assure a certain amount of confidentiality, integrity, and availability of the data. Discussed to a lesser degree was the privacy and related legal issue of database security. Although we have directed the main focus towards the technological issues involved in protecting a database, it should be recognized that database security includes organizational, personnel, and administrative security issues as well. Database security is not an isolated problem - in its broadest sense it is a total system problem. Database security depends not only on the choice of a particular DBMS product or on the support of a certain security model, but also the operating environment, and the people involved.

REFERENCE 1. www.safetica.com/data-security | 2. www.snia.org/.../MichaelFishman_Trends_in_Data_Protection-r9.pdf | 3. www.databasejournal.com/.../Oracle-10g-Security-Part-2-Virtual-Priv... | 4. www.in-oracle.com/Oracle-DBA/.../vpdvirtual-private-database.php | 5. www.dba-oracle.com/t_wallet_manager.htm | 6. www.books.google.com |