
LUT
University
LAND
OF THE
CURIOUS

TABLE OF CONTENTS

CT60A7650 – DATABASE SYSTEMS MANAGEMENT

DATABASE SECURITY

Lecture

Jiri Musto, D.Sc.

DATA BREACH

- Unauthorized disclosure of information
  - Compromises security, integrity or confidentiality of personally identifiable information
  - → Personal information accessed or stolen in unauthorized manner
- Examples of data breaches:
  - Lost data transfer devices, stolen computers
  - Hacking, malware, cyber attacks
  - Mailing personal information to the wrong person
- Data breaches can be accidental or intentional
  - Reading another person’s email or SMS accidentally or on purpose

DATABASE SECURITY BASICS

- Database resources are controlled by the DBMS
- To perform any DBMS operation, a condition must be met:
  - User has been granted the ability to perform the operation
  - The operation has been granted to all users
- DBA is typically responsible for administering database security

DB SECURITY IN A NUTSHELL

- Authentication
  - Who is it?
- Authorization
  - Who can do it?
- Encryption
  - Who can see it?
- Audit
  - Who did it?

AUTHENTICATION

- Authentication is the cornerstone of security
- Required for controlling authorization and auditing
- A login needs to be established for each user of the DBMS
  - Login / account / user ID
  - Username and password
  - May be the same as the operating system login information

PASSWORD

- Avoid short passwords
  - The longer the better (to a limit)
- A combination of letters and numbers and other possible characters
  - 4g1v34nd4g3t0rUw1!!N3v3rL34rn
- Avoid complete words
- Avoid personal statistics
  - Names, birthdates, etc.
- Avoid common passwords
  - password, passw0rd, p4ssw0rd

LOGIN

- Drop a login when a user no longer requires access to the DBMS
  - Cannot be done if user is logged in or owns any database objects
  - Limit the database users who can create database objects
- Another option is to lock the login
  - Disables access but not dropped from the system

GRANT AND REVOKE

- GRANT – Assign a permission to a database user
  - Specify the privileges to be given to the target user
  - Requires the invoker to be the owner of the database or have the authority to GRANT
- WITH GRANT OPTION
  - Grant a permission to grant permission → E.g. Distribute GRANT rights to users
- REVOKE – Remove a permission from a database user
  - Remove privileges previously given with GRANT
  - Beware of cascading revokes
    - Happens when using WITH GRANT OPTION

PRIVILEGE TYPES

- Table / View – Enable user to access tables, views or columns
  - Select, insert, update, delete, all
- Database object – Permission to create database structures
  - Databases, tablespaces, tables, indices, triggers, defaults, user-defined data types
- System – Ability to use DBMS commands
  - Archive logs, shutdown and restart database server, monitoring, manage storage
- Program & procedure – Permission to execute programs or procedures
  - Execute command

PUBLIC AUTHORITY

- Authorization can be granted to PUBLIC
- Anyone who logs in is given the privilege

- Makes database vulnerable to hacking
- Proceed with caution!

LABEL BASED ACCESS CONTROL (LBAC)

- Specify who can read and modify data in individual rows/columns
- For example
  - Employee can only view their own information
  - Supervisor can see their own and their employees' information
- SECURITY LABEL functionality in PostgreSQL
- When user tries to access data, users' security label is compared to the label of the data

ROLES AND GROUPS

- Roles
  - Grant privileges to roles and users automatically get the privileges when assigned
  - A collection of privileges
- Groups
  - Similar to roles
  - Can have users or roles to be part of groups
  - DBMS may have prebuilt groups such as admin groups
- In PostgreSQL, there is no specific keyword for creating groups
  - A group is just a role named after a group
  - A role can have roles = a role can be a “member” of another role (group)

USING VIEWS FOR SECURITY

- Views are stored SELECT statements
  - Sensitive information can be omitted from VIEWs
- VIEWS are normally not-updatable
  - No need to worry about modifications
- Users can be given access only to VIEWs
  - User can then only see what is predefined

ENCRYPTION

- Transform data using an algorithm
- Require a decryption key to decrypt encrypted data
- Two types of encryption
  - At rest
    - Encrypt data in the database
  - In transit
    - Encrypt data when it is transferred
- Encryption is commonly supported by DBMS (by default or with addons)

SQL INJECTION

- Form of web hacking
- A poorly designed web application dumps database content to the attacker
- Using SQL statements, gain access to database content
- Avoid by:
  - Using static SQL if possible
  - Validate user input
  - Do not make assumptions of what data is received
  - Reject input containing special characters

CT60A7650 – DATABASE SYSTEMS MANAGEMENT

REGULATORY COMPLIANCE AND DATABASE ADMINISTRATION

Lecture

Jiri Musto, D.Sc.

HIPAA

- Health Insurance Portability and Accountability Act
- National standard to protect medical records and other personal health information
- Requires the healthcare provider to:
  - Notify patients about their privacy rights
  - Adopt and implement privacy procedures
  - Train employees
  - Secure records containing individually identifiable health information

GLB

- Gramm-Leach-Bliley Act, a.k.a the Financial Modernization Act of 1999
- Regulate the collection and disclosure of private financial information
- Financial institutions must implement security programs to protect personal information
- Prohibits accessing private information using false pretenses
- Give written privacy notices to customers

BASEL III

- A regulatory framework developed by the Basel Committee on Banking Supervision (BCBS) in Basel, Switzerland
- Goal is to produce uniform method of approaching risk management across national borders
- Specifies the following:
  - Capital buffers
  - Leverage and liquidity measures
  - Minimum capital requirements

PCI-DSS

- Payment Card Industry Data Security Standard
- Industry regulation
- Includes requirements for:
  - Security management
  - Policies
  - Procedures
  - Network architecture
  - Software design

GDPR

- General Data Protection Regulation
- European companies or companies handling information of European citizens need to comply
- Places specific requirements for collecting, storing and managing personal information
- Gives rights to the data subject

COMPLIANCE RELATED TASKS

- Metadata management
- Data quality
- Data masking and obfuscation
- Data retention and archivingg

METADATA

- Characterizes data
- Provide documentation
- Who, what, when, where, why, how
- Data about data
- Metadata gives context / identity / meaning to the data
- Important to manage and keep updated

DATA QUALITY

- Many decision are based on data
  - If data quality is poor, decision is poorly justified
  - Low data quality leads to low information quality
- If data comes from unknown sources, the quality of data is unknown
  - How credible the source is?
- Low quality data can cost trillions of USD each year
- Build appropriate data types and constraints
  - Referential integrity
  - Triggers
  - Checks

DATA GOVERNANCE PROGRAM

- Includes
  - A governing council or body
  - Defined set of procedures
  - Plan to execute the procedures
- Oversees the management of
  - Availability
  - Usability
  - Integrity
  - Security

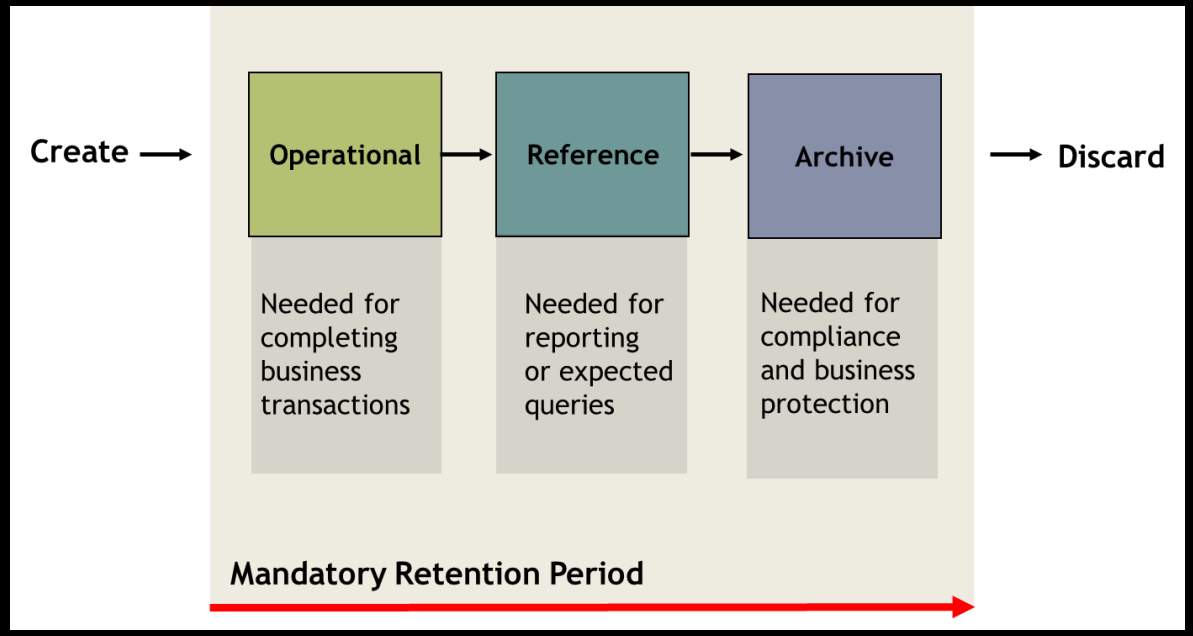
DATABASE AUDITING, DATA ACCESS TRACKING

- Monitor database access
  - Who did what, when, how
- Audit is an evaluation of an organization / system / process / project / product
- Database auditing software can produce useful reports
- Possible auditing techniques:
  - Adding extra columns to tables (last modified)
  - DBMS traces
  - Log based
  - Network sniffing
  - Request capture

DATA MASKING AND OBFUSCATION

- Protecting sensitive and personally identifiable information (PII)
- Use false names, invalid email addresses, card numbers, etc
- Change location information from precise to abstract
- Different masking techniques:
  - Substitution
  - Shuffling
  - Number and date variance
  - Encryption
  - Nulling out

DATA LIFECYCLE



DATA RETENTION AND ARCHIVING

- Required to store data for a period of time
- Can be internal or external requirement
  - Internal: business rule
  - External: laws and regulations
- Data needs to be archived
  - Removed from operational databases
  - Not expected to be references again
  - Stored for just in case


LUT
University