Securing Databases

Chapter 10

Computer System Security

- *Computer system security:* the process of preventing and detecting unauthorized access to an organization's computer system assets.
- Four main areas of concern:
  - **Confidentiality**: Only authorized users should have access to the computer system and the data stored on it.
  - **Authentication**: The computer user's identity should be verified by the computer system, and the computer user should be confident they are communicating with an authentic system, as opposed to a fraudulent copy of the system.

Computer System Security

- **Integrity**: Only authorized users should be able to modify data, and the data modified should be limited to that which is necessary in order for the user to carry out their normal activities on the system.
- **Availability**: Data should be protected in such a way that it is available to users when needed.

Why Is Security Necessary?

- Murphy's Law: Anything that can go wrong will go wrong
  - Some believe Murphy was an optimist
- Servers placed on the internet with default installs have been compromised within minutes
- Default passwords and common vulnerabilities are widely known
- 80% of computer fraud is committed by and with the assistance of insiders
- Honest people make mistakes
- Security controls keep people honest

Security Breaches Happen Far Too Often

- **United States Office of Personnel Management**: During 2015, 25.7 million records of federal employees and contractors, including personally identifiable information (PII), as well as security clearance status information, was exposed.
  - Probably an espionage operation sponsored by a foreign government.
- **Target**: In 2013, 110 million records were compromised, which led to one of the largest incidents of credit card fraud and identity theft in history.
  - The financial impact hit not only Target, but also banking organizations, insurance organizations, and credit card issuers.

Security Breaches (continued)

- **Ashley Madison**: In 2015, 32 million private accounts were compromised. The users' identities were posted on another web site for all to see, which given the nature of the site, proved highly embarrassing to the individuals involved.
  - A domestic hacking group is suspected of carrying out this act of *hacktivism* (hacking, or breaking into a computer system, for a politically or socially motivated purpose).
- **Home Depot**: During 2014, 56 million payment cards were compromised by an offshore cybercrime ring.

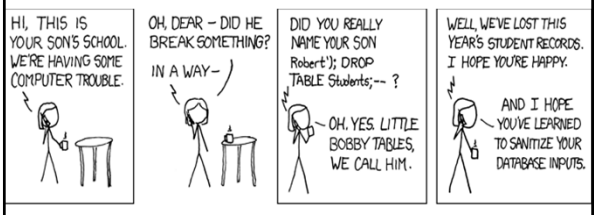
Security Breaches (continued)

- **IRS**: In 2014, 14 million individual records were compromised, along with an additional 334,00 records in 2015.
  - The cybercrime ring was probably after information it could use to file fraudulent tax returns.
  - The second part of the scam is estimated to cost the IRS $21 billion annually.
    - All you need to file a tax return is a name, date of birth, and SSN; and you can file as early as January 1, yet employers are not required to file employment information with the IRS until March, by which time roughly half of all refunds have been paid out. By the time the IRS matches the return to the employer record, often not until summer, the thieves are long gone.

Security Breaches (continued)

- **Anthem Blue Cross**: In 2015, 87.6 million records were compromised, probably by an offshore cybercrime organization interested in identity theft. The exposed information included names, addresses, e-mail addresses, social security numbers (SSNs), dates of birth, and income information.
  - The loss of personally identifiable information, the risk of identity theft in this case is extreme.
  - Another Blue Cross – Blue Shield affiliated company, Premera Blue Cross, lost 11 million records in 2015, probably to the same cybercrime organization.

SQL Injection



Security Policy

- Every organization should have published security policies and procedures
- To be effective, policy must spell out:
  - Specific rules
  - Who enforces the rules
  - Procedures for requesting exceptions
  - Procedures for reporting violations
  - Layers of security work best

A Holistic Approach is Required

- Database Server Security
- Network Security
- System-Level Security
- Database Client and Application Security
- Database Access Security
- Security Monitoring and Auditing
- Security Training (for everyone!)

Database Server Security

- Physical Security
  - Locked room where only authorized personnel have access
  - Access Controls
    - Something you know (password, pass phrase, PIN)
    - Something you have (security token device)
    - Something you are (fingerprint or retinal scan)
  - Other possible measures:
    - Encryption, particularly of backup media
    - Video surveillance system
    - "No one works alone" policy
    - Policy provisions for removal of hardware/software
    - Outbound mail/package inspection policy

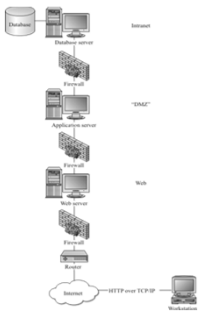
Database Server Security

- Network Security
  - Physical security is not enough for network-connected database servers
  - Network security is only as good as the weakest link on the network
  - Isolate the enterprise network from the Internet (upcoming slide)
  - Secure any wireless network access (upcoming slide)

Isolate the Enterprise Network from the Internet

- Properly configured router
- Firewall to protect every network layer
- Firewall options available:
  - Packet filtering (disallow suspicious content; disallow outbound IP spoofing)
  - Application gateway (shut down unnecessary ports)
  - Circuit level gateway (all connections originate from inside the firewall)
  - Proxy server (Network Address Translation)

Network Security



Firewall Configuration

- **Packet filtering:** Rules can be defined for inspection of the contents of each packet entering or leaving the network in order to block suspicious or unauthorized content.
- **Application gateway** Network applications (HTTP, FTP, Telnet, and so on) use different default ports. For example, HTTP uses port 80 as a default.
- **Circuit-level gateway** This feature applies security mechanisms when a connection is established; then, after the connection is established, it allows packets to flow freely for that established connection.
- **Proxy server** Firewalls can include a proxy server function that translates all the IP addresses used within the protected network into different addresses as packets pass through.

Precautions for Remotely Connected Employees

- Require the use of a combination router/hub/firewall on the remote (home) network
- Encrypt communications with the corporate network
  - Use HTTPS for all web connections
  - VPN (Virtual Private Network) is also a popular method

Secure Any Wireless Network Access

- Wireless access points are inexpensive and the default is “wide open” security
- Recommendations:
  - Firm policy on users connecting their own devices, particularly wireless ones
  - Mandatory encryption using at least 128 bit key
  - MAC (Media Access Control) list
    - Unfortunately, easy to hack because MAC address transmitted on the network in plain text

System-Level Security

- Install only minimal OS software
- Use minimal OS services
- Install only minimal DBMS software
- Apply security patches in a timely manner
- Change all default passwords

Database Client and Application Security

- Login Credentials
  - Required for all users (never shared)
  - Passwords that are not easily guessed
  - Passwords change periodically
  - Exposed passwords immediately changed
  - Passwords never written down (even in scripts), and must be encrypted when stored

Database Client and Application Security

- Data Encryption
  - Symmetric vs. Asymmetric keys
  - Keys with minimum length of 128 bits
  - Loss of key is essentially loss of the data
  - Sensitive data must be encrypted
  - All data not public knowledge should be encrypted when transmitted on public networks
  - E-mail is not to be considered secure

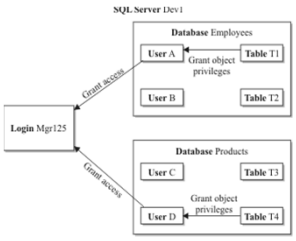
Other Client Considerations

- Web Browser Security Level
  - Plug-ins (Extensions)
  - Cookies
  - Scripting languages (VBScript, JavaScript, Jscript)
- Minimal use of other software
- Malware Scanner
- Test all potential application exposures
  - SQL injection
  - URL spoofing
  - Buffer overflows

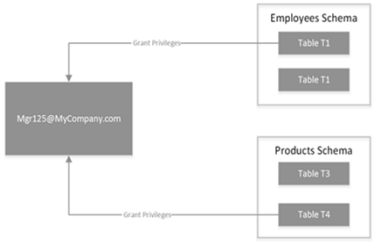
Database Access Security

- Each database user, whether a person or an application, gets exactly the access they need – nothing more; nothing less
- All data access must be on a "need to know" basis

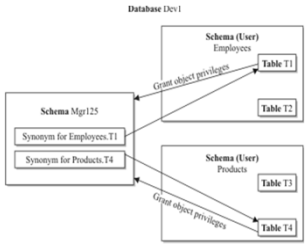
Database Security in MS SQL Server and Sybase



Database Security in MySQL



Database Security in Oracle



Schema Owner Accounts

- In Microsoft SQL Server and Sybase, database users (including applications) should never connect with the "sa" account or any account that has the "DBA" or "DBO" role
- In Oracle, database users should never connect with the user account that owns the schema where the data is stored

Database Privileges

- *Role:* A named collection of privileges that may be granted/revoked as a unit
- *System Privileges*: General permissions to perform server and database management functions. Often assigned via roles.
- *Object Privileges:* Privileges to perform specific actions on specific options (e.g. update a particular table). May be assigned via roles.

Microsoft SQL Server System (Server and Statement) Privilege Examples

- **SHUTDOWN**: Provides the ability to issue the server shutdown command.
- **CREATE DATABASE**: Provides the ability to create new databases on the SQL server.
- **BACKUP DATABASE**: Provides the ability to run backups of the databases on the SQL server.

MySQL Global Privilege Examples

- **CREATE USER:** Provides the ability to create new user accounts on the MySQL database server.
- **SHOW DATABASES:** Provides the ability to display the names of all the databases (schemas).
- **SHUTDOWN:** Provides the ability to shut down the MySQL database server.
- Privileges such as SELECT, INSERT, UPDATE and DELETE can be granted globally, allowing the grantee to perform the operation on any table in any schema.

Oracle System Privilege Examples

- **CREATE SESSION**: Provides the ability to connect to the database.
- **CREATE TABLE**: Provides the ability to create tables in your own schema. Similar privileges exist for other object types, such as indexes, synonyms, procedures, and so on.
- **CREATE ANY TABLE**: Provides the ability to create tables in *any* user's schema. Similar privileges are available for other object types, such as indexes, synonyms, procedures, and so on.
- **CREATE USER**: Provides the ability to create new users in the database.

Object Privileges

- Granted to users with the SQL GRANT statement
- Revoked with the REVOKE statement
- *Grantee: d*atabase user (login) who receives the privileges
- WITH GRANT OPTION clause that allows the recipient to grant the privilege to others
  - Not recommended
    - Control easily lost
    - Revoke cascades to downstream grantees

GRANT Statement

- General syntax:

```
GRANT <privilege list> ON <object>
   TO <grantee list>
   [WITH GRANT OPTION];
```

- Examples:

```
GRANT SELECT, UPDATE, INSERT
   ON T1
   TO Mgr125;
GRANT SELECT
   ON T2
   TO User1, User2, User3;
```

REVOKE Statement

- General syntax:

```
REVOKE <privilege list> ON <object>
  FROM <grantee list>;
```

- Examples:

```
REVOKE SELECT, UPDATE, INSERT ON T1
  FROM Mgr125;
REVOKE SELECT ON T2
  FROM User1, User2, User3;
```


Roles

- *Role*: a named collection of privileges that can, in turn, be granted to one or more users
- Advantages:
  - May exist before user accounts do
  - Relieve the administrator of a lot of tedium
    - This can also be a disadvantage if roles are granted without attention to the detailed list of privileges included in the role
  - Survive when user accounts are dropped

Security Benefits of Views

- Unnecessary columns may be left out of views (not all DBMS products provide for privileges at the table column level)
- A WHERE clause may be included to limit visible table rows
- Joins to "lookup" tables may be used to replace code values with descriptions (but obfuscation alone is not an effective security technique)

Security Monitoring and Auditing

- Monitoring systems can detect security breaches so corrective measures can be taken
  - Intrusion detection software
  - Database auditing features
- Independent Auditor review
  - Policies and procedures
  - Existing security measures

Measures to Prevent Security Breaches

- Change administrator passwords regularly
- Force users to change passwords regularly
- Discourage the sharing of passwords
- Remove inactive user accounts
- Remove non-employee user accounts
- Perform random monitoring of all activities
- Perform database auditing
- Educate the end user
- Conduct security training sessions

Simplified 1040