

An Overview To Database Server Security

Amarjot Walia
amarjot.walia@hub.nic.in

CERT-In

Department of Information Technology
Ministry of Communications & Information Technology
Electronics Niketan, 6 C.G.O. Complex
New Delhi- 110 003

Purpose

- Goals of Database Server Security
- Threats to Database Servers
- Create Awareness Among DBAs

Introduction

- **Role of a Database Server in an Organization**
 - Central repository of information.
 - Contains all the data for viability of business.
- **Role of Database Administrator**
 - Ensure availability of data to everyone all the time.
 - Ensure confidentiality and integrity of data.
 - Ensure security of database server.
- **Role of Database Application Developers**
 - Implement secure coding practices.
 - Ensure that their application are not used as a platform to compromise the database.

Issues Faced by DBA

- Privacy of Communication
 - Can the data be read while in transmission?
- Confidential Data
 - Is confidential data stored in plain text?
- Fine Grained Access Control
 - Which user can view which data?
- Identifying The Users
 - Who all are trying to access the database?
- Ease of Use
 - Is it easy for a normal user and an administrator to use the database?
- Flexibility
 - Can you support different security needs for different users?

Database Security : For?

- Data Confidentiality
- Data Integrity
- Data Availability

Database Security : From?

- **People Outside Perimeter**
 - » Secure Network Perimeter

- **People Inside Perimeter**
 - » Secure Data at Source

Database Servers : Threats

- Vendor Bugs / Complex Configurations
- Network Eavesdropping
- Unauthorized Server Access
- SQL Injection
- Password Cracking
- Virus / Worms

Database Servers : Threats

Vendor Bugs / Complex Configurations

- Buffer Overflow
- Programming Errors
- Poor Design (eg. Weak form of encryption.)
- Complex configurations

Eg. : In Oracle, init.ora parameter '*Remote_OS_Authent = True*' means remote users can connect **WITHOUT** authentication.

Countermeasures

- Stay updated with latest service packs.
- Apply all relevant patches.
- Refer to relevant documentation while configuring the database server.

Database Servers : Threats

Network Eavesdropping

- Insecure network channels
- Passing credentials in plain text over network
- Insecure authentication protocols

Countermeasures

- Install server certificates.
- Avoid passing sensitive information in plain text.
- Use secure and recommended authentication protocols.

Database Servers : Threats

Unauthorized Server Access

- Failure to block database ports at perimeter firewall.
- Lack of access control procedures.
- Lack of physical security of database server.

Countermeasures

- Block database ports at perimeter firewall.
- Restrict access to database server from trusted systems only.
- Secure database server behind its own firewall in addition to perimeter firewall.
- Restrict physical access to authorized personnel only.

Database Servers : Threats

SQL Injection

- Improper input validation in web applications.
- Dynamically created SQL statements.
- Excessive privileges accorded to application logins.
- Weak permissions which fail to restrict an attacker and allow him to elevate his privileges.

Countermeasures

- Validate and sanitize input data before passing it to SQL query.
- Use the principle of least privileges when granting privileges to logins.
- Use stored procedures or extended procedures as far as possible to avoid granting access to tables.
- Enforce strict password policy.
- Enable auditing and check the logs regularly.

Database Servers : Threats

Virus / worms

- Absence of Anti-virus software for database servers.
- Failure to apply upto date patches.
- Failure to block database ports at network perimeter.

Countermeasures

- Ensure that database server is protected by an Anti-Virus software.
- Apply the latest available patches to the database server.
- Ensure that the database is not exposed to internet directly unless absolutely necessary.

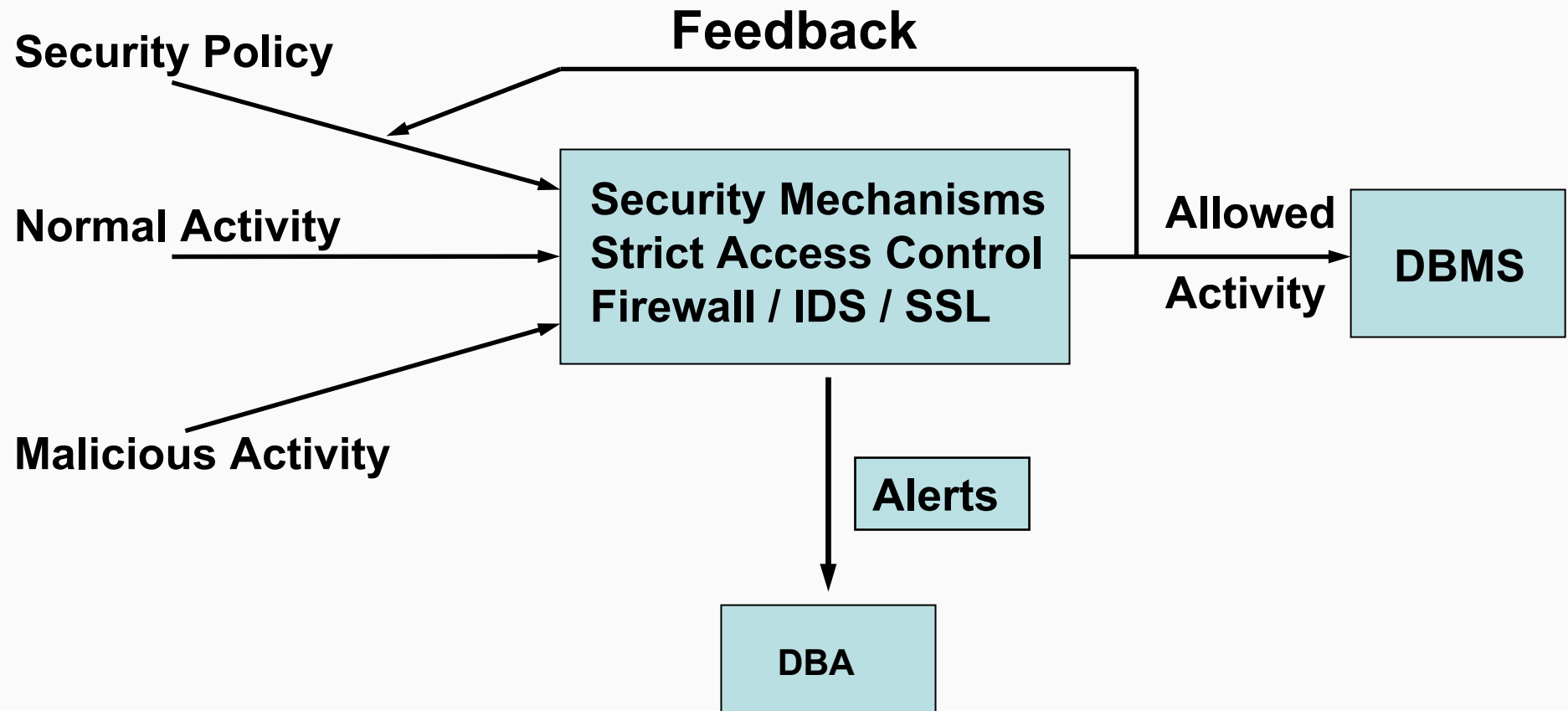
Database Server Security : Implications

- The first target, Web Server, does not contain information.
- It's the Database behind it which stores information.
- Compromised Database : Business Viability at Risk.
- Insecure Database : Can be used to compromise underlying OS and Network.
- Increasing number of Database Servers are getting exposed to Internet directly increasing the risk.

Database Server Security : How?

- Stay updated with latest Service Packs and Patches.
- Remove unnecessary services and protocols.
- Depending on importance of data, consider encryption.
- Secure the database server behind a firewall and IDS.
- Enforce a strict access control policy.
- Enforce secure coding practices in application developers.
- Enable auditing for database servers.
- Depending upon importance of data, fine grain auditing should be considered.

Secure Database



Afterthoughts

- Default/standard installation is NOT secure.
- Plan to make the database secure from the beginning itself.
- Upgradation provides an opportunity to implement more security features.
- Implement as many auditing/monitoring features as possible and store the results in different places.
- A lot of tools are available to limit access to your database, harden it, track unauthorized activities etc. But what use you put them to is upto you.

Thank You

References

- <http://otn.oracle.com/documentation/index.html>
- <http://www.microsoft.com/security/default.mspix>
- <http://www.appsecinc.com/>
- <http://www.oreilly.com/catalog/orasec/>