

Introduction to Information Security

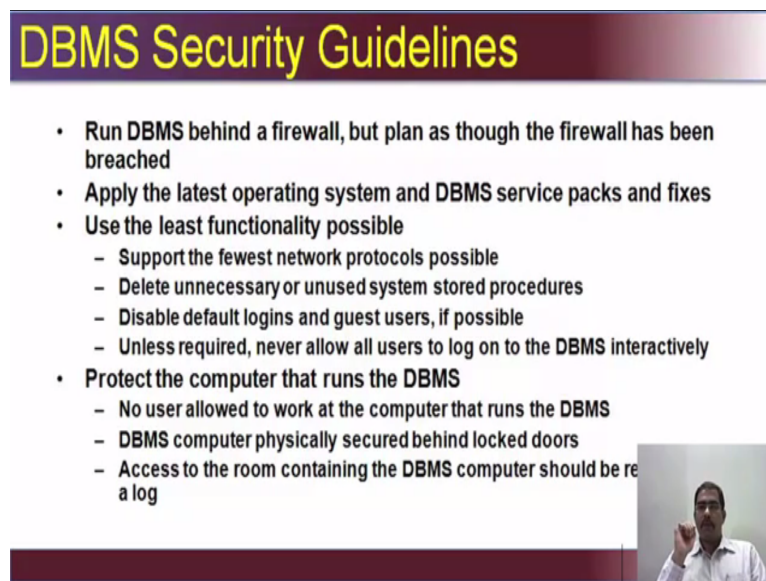
Prof. Dilip H. Ayyar

Department of Computer Science and Engineering

Indian Institute of Technology, Madras

Lecture - 50

(Refer Time Slide: 00:10)



DBMS Security Guidelines

- Run DBMS behind a firewall, but plan as though the firewall has been breached
- Apply the latest operating system and DBMS service packs and fixes
- Use the least functionality possible
 - Support the fewest network protocols possible
 - Delete unnecessary or unused system stored procedures
 - Disable default logins and guest users, if possible
 - Unless required, never allow all users to log on to the DBMS interactively
- Protect the computer that runs the DBMS
 - No user allowed to work at the computer that runs the DBMS
 - DBMS computer physically secured behind locked doors
 - Access to the room containing the DBMS computer should be recorded in a log

What are the DBMS security guidelines, so you run the DBMS behind a firewall, but plan as though that the firewall has been breached, meaning you put in security measures, that you would not put in case of firewall was present. So, you try to put in additional security measures, so that even if the firewall is breached, the DBMS is safe. Then apply the latest operating system, and DBMS service parts, and bits.

So, this is a very important and ongoing process for any organization, as and when the patches are released, by the security patches or other patches are released by the vendors of the operating system and DBMS. The organization, should ensure that they are applied, ask for the testing, and then that the database or your OS is current always, then use the least functionality as possible.

That is, you support fewer network protocols possible. So, only what is required to be configured, you configure, what is not required disabled it, delete unnecessary or unused

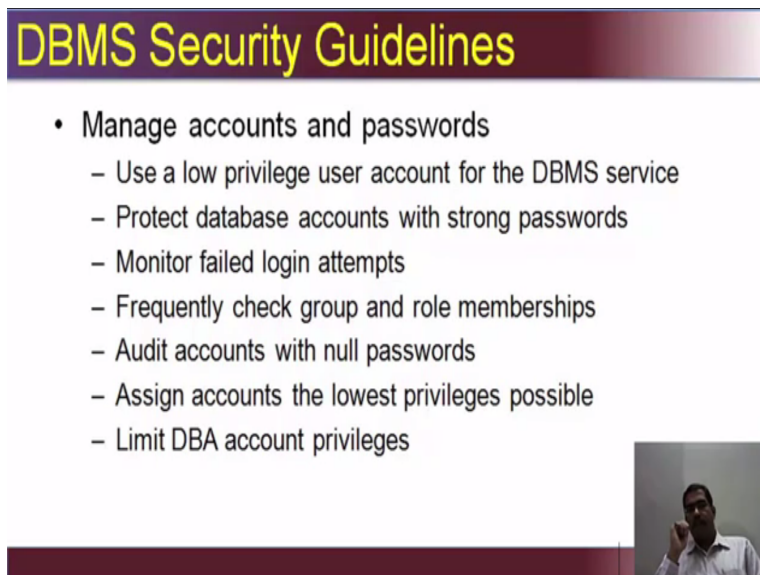
system stored procedures, which is which will be there within, then disable default logins and guest users. So, if is that if possible should be compulsorily, you have to default disabled default logins, and guest users.

Only authorized users should be allowed into the system, and default credentials are the first attempt for any hacker who will try to go, and see if a default is used. So, now if there is a default credential then his access is very easy, then unless required never allow all users to log on, to the DBMS interactively.. So, any interactions from the users should be to the front end, and not directly to the OS.

Then you have to physically and logically protect the computer that runs the database management system. That means no user allowed to work, at that computer that runs the DBMS. And DBMS computer should be physically secure, behind locked doors or it should be secured in data center, with proper access control mechanisms. Then access to the room containing the DBMS computer, also should also be recorded in the log.

So, whenever somebody enters, if it is a proximity touch sensor or biometric, the log would be available. If it is a ordinary lock, then there should be a register kept where it should be noted, who access what time, why how much you are there with the signature and contact info, or employee id, then manage the accounts and passwords.

(Refer Time Slide: 02:58)



DBMS Security Guidelines

- Manage accounts and passwords
 - Use a low privilege user account for the DBMS service
 - Protect database accounts with strong passwords
 - Monitor failed login attempts
 - Frequently check group and role memberships
 - Audit accounts with null passwords
 - Assign accounts the lowest privileges possible
 - Limit DBA account privileges

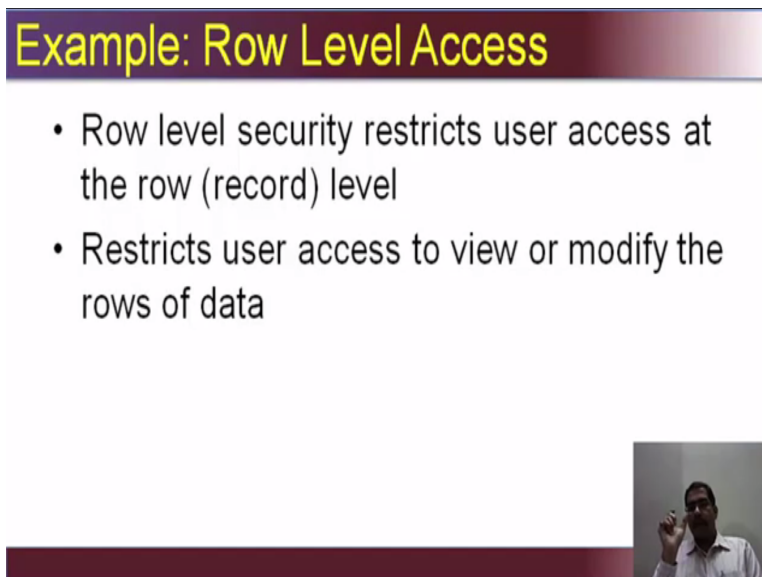
That is use a low privileged account, for database management services. Then do not use system admin, or SA account, or group account always. Use low privileged user account for DBMS service itself, do not run it as a group, protect database accounts with strong

passwords. So, follow the password criteria, minimum 8, alphanumeric special, then monitor the failed login attempts, unsuccessful attempts to login, should be monitored to see whether it really the person who has done, or someone is trying to hack in.

Here it is notable that, you should also lock out the attempts, after three unsuccessful attempts or five unsuccessful attempts. So, that the administrator or the person involved in administration of database, will come to know that the account has been locked, due to either a attempted bad, or somebody else from within, trying to penetrate the system. Then frequently check group, and role memberships who is there in what group, and what roles they have, so that has to be checked.

When you audit accounts with null password, or no password, frequently assign, accounts, the lowest privilege as possible, do not get too many privileges. Then limit DBA account privileges so that, the database administrator should be given privileges, on again need to know, and need to do nothing beyond that.

(Refer Time Slide: 04:40)



Example: Row Level Access

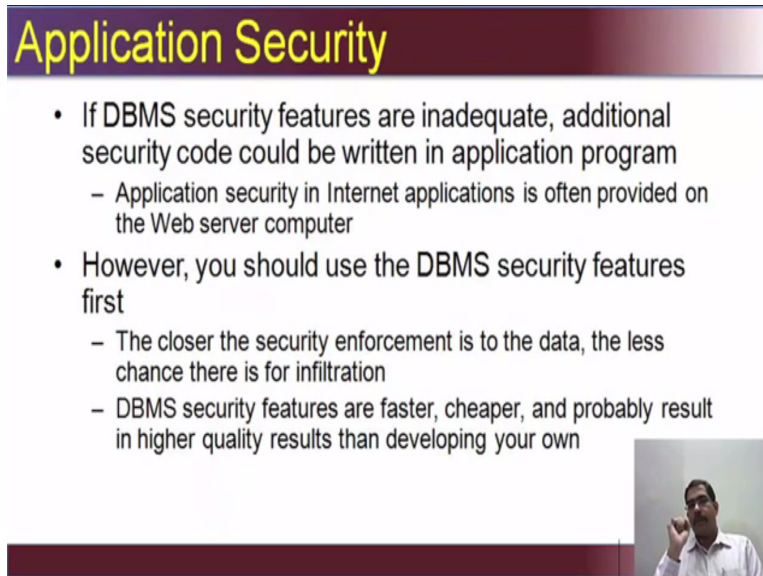
- Row level security restricts user access at the row (record) level
- Restricts user access to view or modify the rows of data

Video inset showing a man speaking.

Let us take an example, row level access. Now, the row level security restricts the user access, at the record level, row level. It restricts user access to view, or modify the rows of data. So, that means then you when you implement a row level security, it restricts the user at the record level. So, that means if it is specified there, that he can access only this, and this record he will be able to do that only, and that too view it will restrict the user access to view,


or modify the rows of data. If he is the owner of the data, he will be allowed to modify, otherwise he will be able to google it, if it is not both, it may not permit that access at all.

(Refer Time Slide: 05:46)



Application Security

- If DBMS security features are inadequate, additional security code could be written in application program
 - Application security in Internet applications is often provided on the Web server computer
- However, you should use the DBMS security features first
 - The closer the security enforcement is to the data, the less chance there is for infiltration
 - DBMS security features are faster, cheaper, and probably result in higher quality results than developing your own



So, application security also plays an important part, when your DBMS is limited. If the DBMS security features are inadequate, then additional security code would be written to application program itself. So, application security in the internet application is often provided on the web server computer. You should know, what is a web based application, web servers, there are different kinds, you can run on UNIX, and run on windows, IAS is kind of web server, apache is kind of web server. Engine x is kind of web server Tomcat. So, you should know additional security features can be built on these web servers. The applications, to additionally protect the database, but the primary thing is you should use the DBMS security reports first. So, it should be you should secure on both the places, but you should secure DBMS first. The closer the security enforcement is to the data, the less chances are there for infiltration.

Then DBMS security features are faster, it is cheaper, and it will also result in higher quality result, than developing your own algorithm, or your own security feature to protect database from these kinds of threat. We can have or as we discussed about those, there are four kinds of security that can be done, one is access control, then inference control, and then it is flow control and then encryption.

(Refer Time Slide: 07:10)

Security Breach TJ Maxx

- Considered to be the largest database security breach
- IPLocks, a compliance and database security company, estimated that the TJX breach will eventually cost the company \$100 per lost record, or a total of \$4.5 billion.
 - The company based the estimate on the accumulated costs of fines, legal fees, notification expenses, and brand impairment.
- <http://www.informationweek.com/news/global-cio/compliance/showArticle.html?articleID=201800259>



Let us see, another example of a security breach at t j maxx. It is considered to be, the largest database security breach. IPLocks, a compliance and database security company estimated that, t j x breach will eventually cost the company 100 dollars per lost record, or a total of 4.5 billion us dollars. So, the company based the estimate on the accumulated cost of fines, the legal fees, notification expenses, brand impairment. More details on of this particular breach, is available in the link provided in the slide, you can take a look at it like.

(Refer Time Slide: 07:53)

Database Vulnerabilities

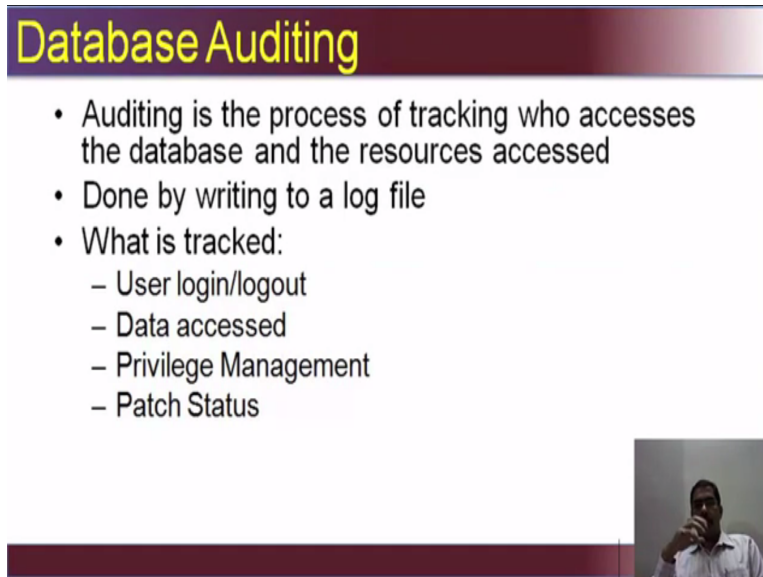
	Oracle	Microsoft SQL Server	Sybase	IBM DB2	MySQL
Default & Weak Passwords	✓	✓	✓	✓	✓
Denial of Services & Buffer Overflows	✓	✓	✓	✓	✓
Misconfigurations & Privilege Management Issues	✓	✓	✓	✓	✓



We discussed any database you say, whether it is Oracle, Microsoft SQL, Sybase, IBM DB 2 or MySQL. The common vulnerabilities, which affect them, are default and weak passwords. Denial of service and buffer overflows, mis-configurations and privilege management issues,

that is giving excessive privileges. So, it is common across all databases, it does not occur at a single database vendor.

(Refer Time Slide: 08:23)



Database Auditing

- Auditing is the process of tracking who accesses the database and the resources accessed
- Done by writing to a log file
- What is tracked:
 - User login/logout
 - Data accessed
 - Privilege Management
 - Patch Status

The slide features a dark red header with the title 'Database Auditing' in yellow. The content is a bulleted list. In the bottom right corner, there is a small video inset showing a man in a white shirt speaking into a microphone.

How to do a database audit, so auditing is the process of tracking two accesses in the database, and what are the resources accessed. It is done or evidenced by writing up to a log file. So, at the time of creation of database, the logging requirements, what is to be logged is also checked, basically what is tracked user login level is, what is the data accessed, what is the privilege level given to the user, and the patch status. So, these are the four things that are tracked.

Again there are several tools available to audit database access, there are oracle auditing tools, then there is approved by mcafee itself, for auditing database, enforcive is another tool, softtree is another tool, APEX SQL is another tool, db audit. So, there are several tools also available to audit the databases.

So, we have discussed a brief about, what database security is, what are the measures, we can secure the database, what are the methods by which the data can be stolen, some of the bigger database hacks. And then finally, how we audit the database. With this, we will end the database section and move onto SAP security.

(Refer Time Slide: 09:59)

SAP Security

- Many organizations see SAP as specialist software requiring similarly specialist resources with SAP experience. Whilst it is true that most organizations require some form of assistance from SAP experts to implement the software, there are a number of ways that in-house security resources and personnel can contribute to the implementation and maintenance of a secure SAP environment.



SAP stands for, systems, applications, products. The most crucial aspect in SAP security is segregation of duties. And many organizations, see SAP as a specialist software requiring, similarly specialist resources with SAP experience. While it is true that most organization require, some form of assistance from SAP expert to implement the software itself, there are number of ways that in house security resources and personnel can contribute to the implementation, and maintenance of a secure SAP environment. Security is the first and foremost concern, in any SAP audit. There should be proper segregation of duties, and access control which is paramount to establishing the integrity of, controls for the SAP system. When a company first receives SAP, it will devoid or it does not have any security measures, or it will devoid of almost all security measures. At the time of implementation of SAP the company must, go through an extensive process of outlining their processes, building their system security from ground up, for what to ensure proper segregation of duties, and proper access, proper profile design, and avoidance of redundant user ids, super user access will be a important phase of all part of operation in a SAP environment. So, along with this comes the importance of ensuring restricted access, to terminal servers and restricted access to the data center to prevent tampering.

So different Organizations have different modules of SAP installed, so every company or organization security structure, will be distinctly different from the other. Because of the number of modules, that they have implemented, but the underlying fact is that segregation of duties, should be enforced properly in a SAP environment, like or other environments, so that your SAP security can complement, or enhance the security of your overall IT infrastructure.

SAP itself has got several modules, where the security settings have been set as, default you can set your own setting. So, lot of it is parameterized right from your logging requirements, your password strength to what can be logged. So, there are a lot of features built into the SAP software, there are also physical SAP vulnerability assessment tools like onapsis, available in the market, to do a vulnerability assessment or penetrating testing in a SAP environment.

Then there is something, called a SAP router itself which interacts with all SAP servers, which are present. Then ISACA itself has brought out COBIT checklist for auditing a SAP infrastructure. So, there are several methods of doing or conducting the audit for a setting, but what you have to remember is, whenever you audit the SAP environment apart from your password criteria, and initial login, the most important aspect to check is segregation of duties; whether it has been done properly, any failure on implementing, proper segregation of duties will run the entire system wrong in terms of somebody misusing the system.

(Refer Time Slide: 14:00)



The image shows a presentation slide with a dark red header containing the text "Desktop Security" in yellow. Below the header, there is a white area with a bullet point "• Measures???" and a 3D illustration of a laptop with a silver padlock and a chain wrapped around its screen. In the bottom right corner of the slide, there is a small inset video frame showing a man in a white shirt.

Then we will look at desktop security, what we will basically implement again as we have discussed about proper password controls, update your system's properly, install an antivirus software, enforce the built in firewalls in the system. Lock your computer when you go out, keep your password strong, enable logging in the desktop application, or root it to a log manager, keep your security badges, or update all the required badges on the system. Keep your Microsoft office updates proper.

So, basically whatever you want to do to protect the server and then, if possible encrypt the data on your laptop. So, there are several methods to secure. We have gone through all the measures, desktop is no different. So, you need to protect your desktop as you would protect a server because anybody with a physical access to a location, and a weakly configured desktop can still access your server, and create havoc.

With that we come to the end of module 4. In module 5, we will talk about windows, and Linux security. We hope that, you have gathered a lot of information from module 4, or the basics of what needs to be done.