Introduction to Information Security

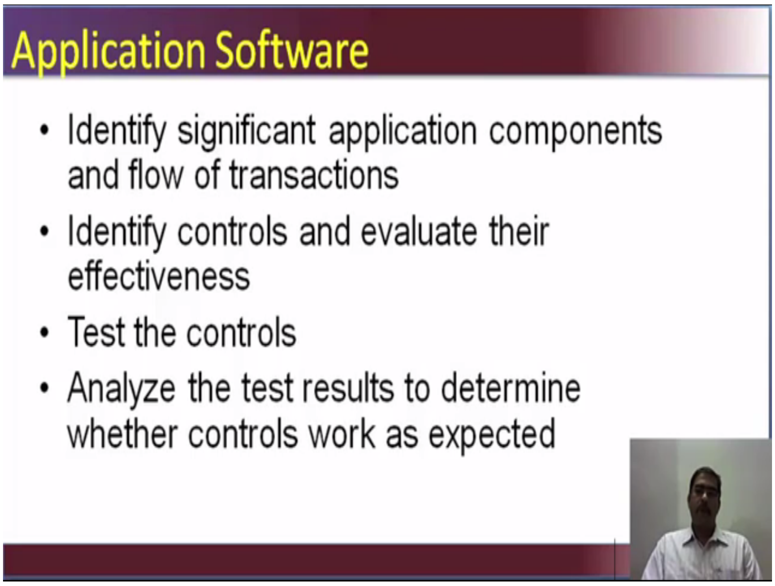
Prof. Dilip H. Ayyar

Department of Computer Science and Engineering

Indian Institute of Technology, Madras

Lecture - 49

(Refer Time Slide: 00:10)



Application Software

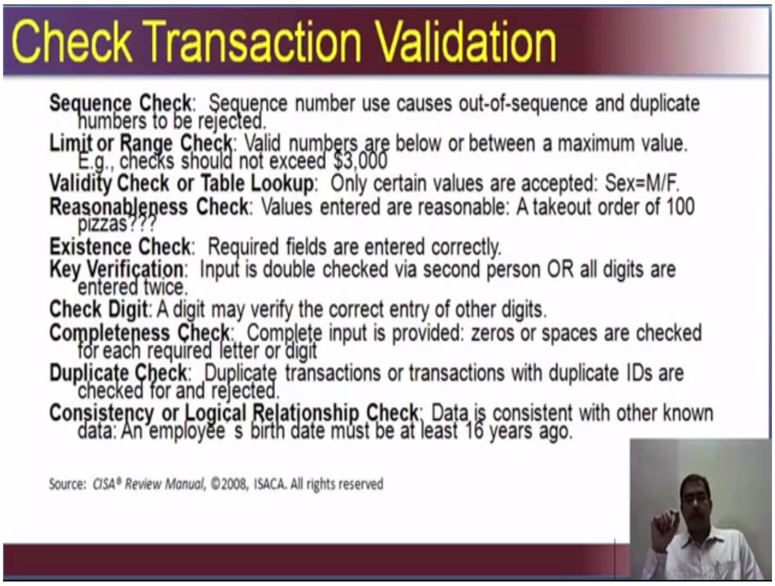
- Identify significant application components and flow of transactions
- Identify controls and evaluate their effectiveness
- Test the controls
- Analyze the test results to determine whether controls work as expected

We have seen how data centre, audit is conducted. Now, let us see how the application software will audited, what are the things that you have to see, you have to identify significant application, components and flow of transactions. We need what is the architecture of the application. Whether it is a 2 tier application, or a 3 tier application, what is the flow of transaction, what is the intended use of the application, how the application works.

Does it need any dependencies, for running the software, then identifying the controls which present at the software, and evaluate their effectiveness. For example, if it is a web based application, and if there is a login screen, what are the controls within their, whether there is the translation goes via https, whether password policies are implemented, if it is a 2 tier application, or a client server based application.

Then, how the login management works, when you test the controls, input, processing, output ,when you analyze the results to determine whether control is working as expected. If it is not working, then you write a report and submit it to the management, for corrective actions to be taken. Then you conduct the compliance audit, a one more form of audit to make sure or ensure that, the vulnerability or weaknesses that are found during the audit are rectified.

(Refer Time Slide: 02:06)



Check Transaction Validation

Sequence Check: Sequence number use causes out-of-sequence and duplicate numbers to be rejected.
Limit or Range Check: Valid numbers are below or between a maximum value. E.g., checks should not exceed $3,000
Validity Check or Table Lookup: Only certain values are accepted: Sex=M/F.
Reasonableness Check: Values entered are reasonable: A takeout order of 100 pizzas???
Existence Check: Required fields are entered correctly.
Key Verification: Input is double checked via second person OR all digits are entered twice.
Check Digit: A digit may verify the correct entry of other digits.
Completeness Check: Complete input is provided: zeros or spaces are checked for each required letter or digit
Duplicate Check: Duplicate transactions or transactions with duplicate IDs are checked for and rejected.
Consistency or Logical Relationship Check: Data is consistent with other known data: An employee s birth date must be at least 16 years ago.

Source: *CISA® Review Manual*, ©2008, ISACA. All rights reserved

You check transaction validations, now this particular slide, the contents have been taken from the CISA review manual of 2009, where we check for transaction validations, like sequence check where the sequence use causes out of sequence, and duplicate numbers to be rejected. Suppose you have an application, where it indexes or the primary key is auto generated, you will have to see under the sequence numbers are in order, or if anything has been missed, or if something has been missed, why it has been missed, then you check for the limit or range check; if you have specified that one particular field, will take only a range between 1 dollar and 3000 dollars, whether the checks exceed 3000 dollars or are below 1, that has to be checked.

Validity checks or table lookup, only certain values can be accepted, for example, the gender which is male, or female, which should not accept numerical values. Then reasonableness check, suppose nut and bolts are ordered from a particular supplier, and the order say 100 nuts and bolts, that is the limit that is set for the tender, whether you can buy 1000 from them. Or here an example, is given a takeout odder of 100 pizza is not reasonable.

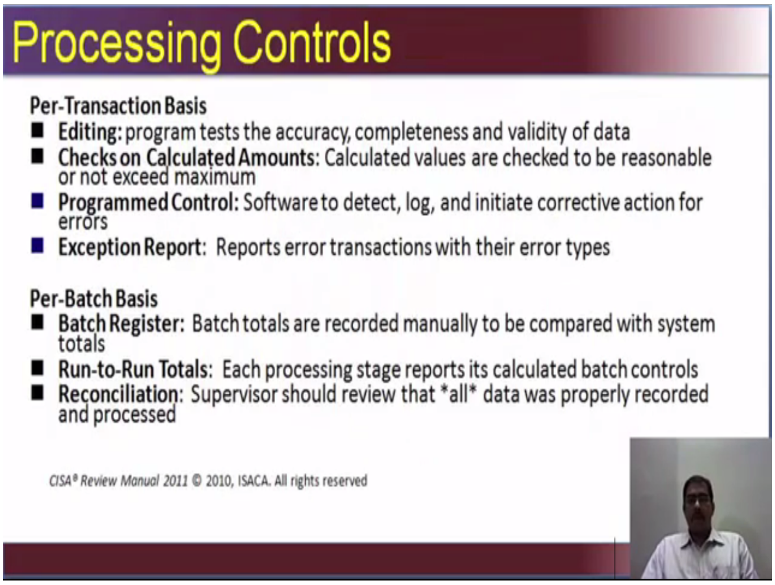
It can be 1 pizza, 2 pizzas, 10 pizzas, and a value of 100. So, the reasonability of the quantity entered is also verified. Then existence checks, required fields are entered correctly. When you go to a website, or when you go to an application, where it asks you for filling in the details, that will be read as swift marks, which says that these are mandatory values and then there are optional fields also.

So, existence check will verify whether the required fields are entered correctly. Key verification, this generally happens in the financial or informing symbols where, input is double checked via second person, which is a maker defect also or all digits are entered twice. Just to identify the content or that field. In some places you would have encountered, enter your email twice, the content based is test, to ensure that the value you entered is correct.

So, if the first one does not matches with the second one and then, the transaction is rejected. Check digit, a digit may verify the correct entry of the other digits. Completeness check, if complete input is provided, zeros or spaces are checked for each. So, instead of entering a value, you just put 0 and 0 or press space 5 times. Whether that is checked, then duplicate transactions or with duplicated ids are checked, if it is duplication it is rejected.

So, in account entries you will find that this facility is there. Accounting software packages like tally, have information of any other, can check this. Then consistency or logical relationship check, that is to ensure that the data is consistent with other known data. For example, an employee’s data of birth must be, at least 16 years ago or 18 years ago. Or when the bank opens the account for a minor, it will verify the data of birth field to check that, he is less than 18 years old to be classified as a minor. So, these are the transaction validation checks, that will have to be performed on application software.

(Refer Time Slide: 06:10)



Processing Controls

Per-Transaction Basis

- **Editing:** program tests the accuracy, completeness and validity of data
- **Checks on Calculated Amounts:** Calculated values are checked to be reasonable or not exceed maximum
- **Programmed Control:** Software to detect, log, and initiate corrective action for errors
- **Exception Report:** Reports error transactions with their error types

Per-Batch Basis

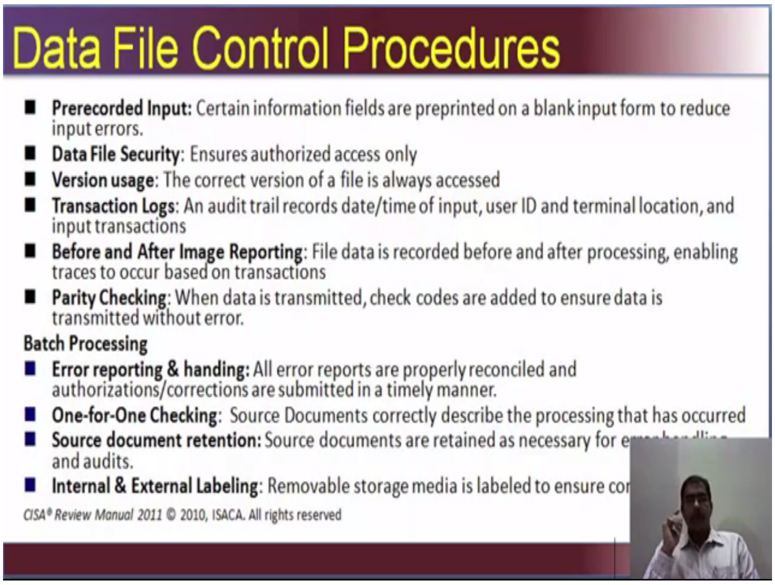
- **Batch Register:** Batch totals are recorded manually to be compared with system totals
- **Run-to-Run Totals:** Each processing stage reports its calculated batch controls
- **Reconciliation:** Supervisor should review that *all* data was properly recorded and processed

CISA® Review Manual 2011 © 2010, ISACA. All rights reserved

Then you have processing controls, where transactions are checked per transaction basis. Editing is one of the criterion, that iis the program tests the accuracy, completeness and validity of data. Then it check on the calculated amounts, that is calculated values are checked to be reasonable or not exceed the maximum limit. Programmed control, that is the software to detect log, and initiate corrective actions for errors.

So, it is kind of a self error correction mechanism. Per batch; batch means, a group of transactions, so batch totals are recorded manually to be compared with system totals, run to run totals, each processing stage reports its calculated batch controls. Then, reconciliation, supervisor should review that all data was properly recorded and processed. So, why a star is given before all, because each and every transaction, that has been entered should be verified to ensure that, that has been properly recorded, and it has been properly processed.

(Refer Time Slide: 07:24)



Data File Control Procedures

- **Prerecorded Input:** Certain information fields are preprinted on a blank input form to reduce input errors.
- **Data File Security**: Ensures authorized access only
- **Version usage**: The correct version of a file is always accessed
- **Transaction Logs**: An audit trail records date/time of input, user ID and terminal location, and input transactions
- **Before and After Image Reporting**: File data is recorded before and after processing, enabling traces to occur based on transactions
- **Parity Checking**: When data is transmitted, check codes are added to ensure data is transmitted without error.

Batch Processing

- **Error reporting & handing:** All error reports are properly reconciled and authorizations/corrections are submitted in a timely manner.
- **One-for-One Checking**: Source Documents correctly describe the processing that has occurred
- **Source document retention:** Source documents are retained as necessary for e
  and audits.
- **Internal & External Labeling**: Removable storage media is labeled to ensure co

CISA® Review Manual 2011 © 2010, ISACA. All rights reserved

Then we have data file controls, here we check for prerecorded, input certain information fields are preprinted on a blank input form, to reduce input errors. Then data file security ensures that, only authorized people can access. The correct insert, version of a file should always be used. An audit trail which records, date, the time, the input that has made, user id, from which terminal it was made, and what transactions are gone through that also should be there.

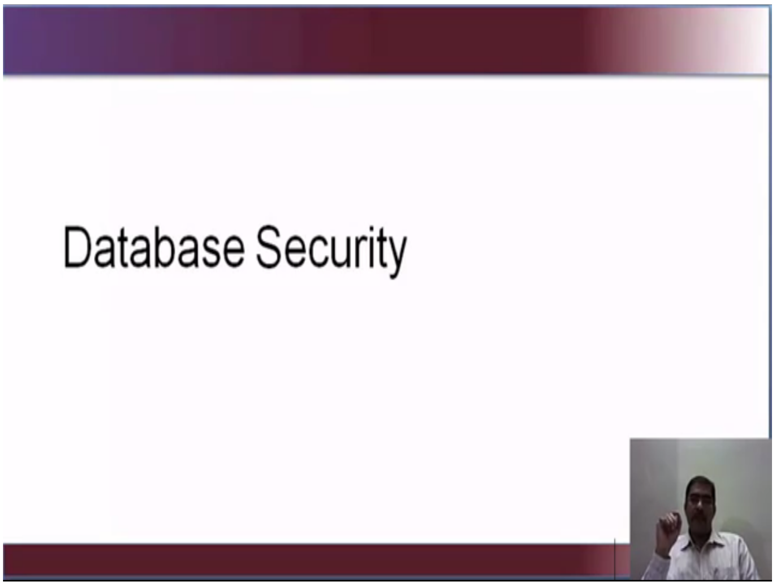
An audit trial is a very crucial aspect of any software, where in the organization and the auditors can check for any happenings, which are out of our money. Then you have before and after image reporting, where the file data is recorded before processing and after processing. So, you have two images, 1 how the data was, what was input, what was processed, what is the output, so you then, you have data with a different characteristics.

So, you have the original data, you have the processed data, you have the new data. Then, you have parity checking, when data is transmitted, check codes are added to ensure data is transmitted without errors. Similarly, here for batch processing, error reporting and handing all error, reports are properly reconciled and authorizations, or corrections are submitted in a timely manner.

One for one checking, source documents correctly describe the processing that has occurred. Then the source document retention, source documents are retained as necessary, for an error handling, and audits. Here source handling document retention, is for also to make your deposit slip, this is source document.

So, that the bank will prohibit in a facility, for regulatory requirements, for audits, for other requirements, also like error handling, where the problem is happened, who has made that particular entry so all those things. Then the internal and external labeling, the storage media, should be labeled correctly to ensure that, the correct processing happens you do an inadvertently insert the tape, which is outdated. So, these are the data file control procedures.

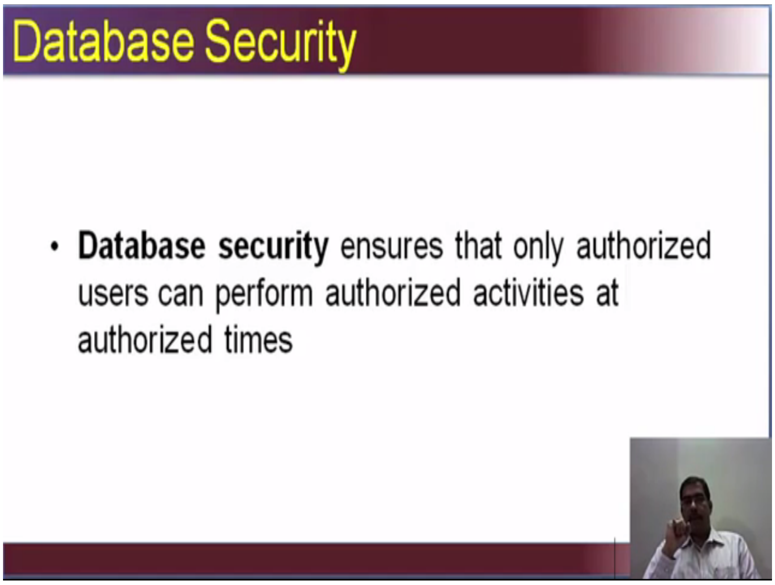
(Refer Time Slide: 10:10)



Database Security

So, an extension of the data files control procedure, which is big goal into database security.

(Refer Time Slide: 10:17)

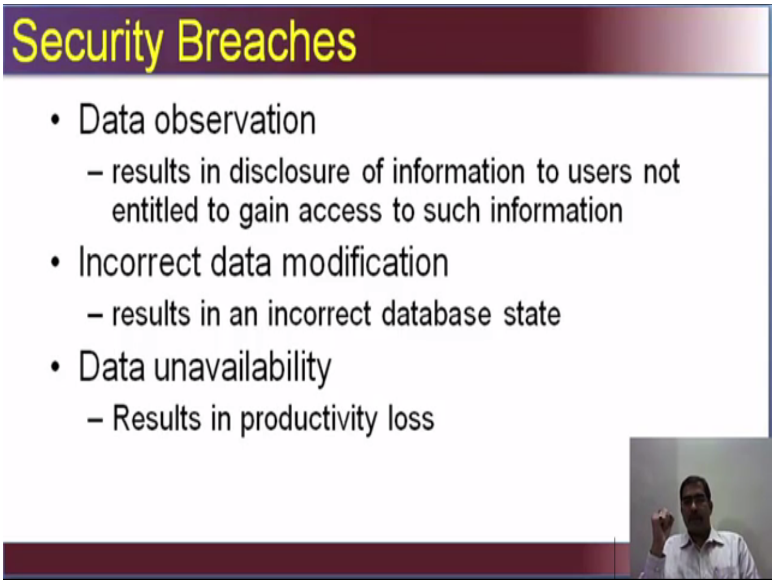


Database Security

- **Database security** ensures that only authorized users can perform authorized activities at authorized times

What is that ensure, database security have, when you secure a data base, it ensure that only authorized users can perform authorized activities, at authorized times. Now, here the key word is authorized. So, users perform activity at different times so that is basically what database security aims to achieve.

(Refer Time Slide: 10:42)



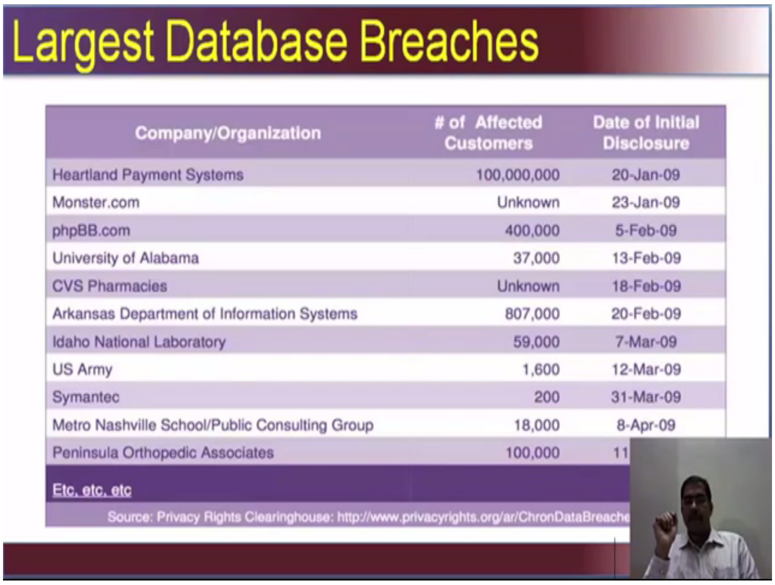
Security Breaches

- Data observation
  - results in disclosure of information to users not entitled to gain access to such information
- Incorrect data modification
  - results in an incorrect database state
- Data unavailability
  - Results in productivity loss

Now, breaches can happen in databases also, data observation is long time of breach where, that results and disclosure of information to users, who are not entitled to gain access to such information. For example, in some websites, you have database errors popping out, which show the information of database version number, may be the path of the table, where that particular part is stored.

So, data observation is one kind of a breach, so you manipulate the system to bring out data observation errors. The second is incorrect data modification, which results in an incorrect database state, that means when we do something incorrect modification of data, the database state is not stable. Something else happens either it crashes , or some other processing errors occurs. Then the third is data unavailability or non availability, which results in database, not being accessed by the users which is again written productivity loss, because data base is not available.

(Refer Time Slide: 11:59)



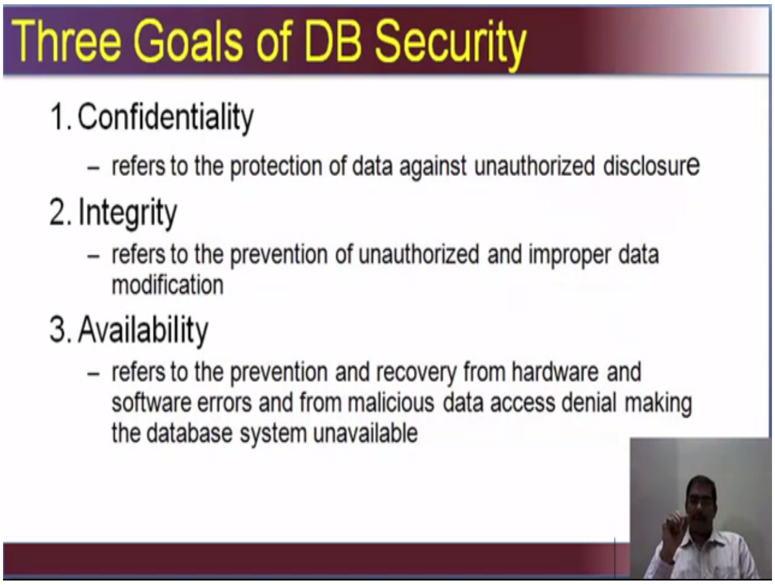
Largest Database Breaches

Company/Organization	# of Affected Customers	Date of Initial Disclosure
Heartland Payment Systems	100,000,000	20-Jan-09
Monster.com	Unknown	23-Jan-09
phpBB.com	400,000	5-Feb-09
University of Alabama	37,000	13-Feb-09
CVS Pharmacies	Unknown	18-Feb-09
Arkansas Department of Information Systems	807,000	20-Feb-09
Idaho National Laboratory	59,000	7-Mar-09
US Army	1,600	12-Mar-09
Symantec	200	31-Mar-09
Metro Nashville School/Public Consulting Group	18,000	8-Apr-09
Peninsula Orthopedic Associates	100,000	11
Etc. etc. etc		

Source: Privacy Rights Clearinghouse: http://www.privacyrights.org/ar/ChronDataBreache

Look at some of the largest database breaches, including the one which happened in 2014 Sunil corporation. This source is from privacy rights clearinghouse, the urls also given. Now, if you see the amount or number of affected customers, it is a huge number, the smallest one is 1600 of US army oh! Sorry Symantec is 200, but the largest goals in millions. So, the database breaches also happened by the law, sony being one, the latest one, which happened in 2015.

(Refer Time Slide: 12:50)

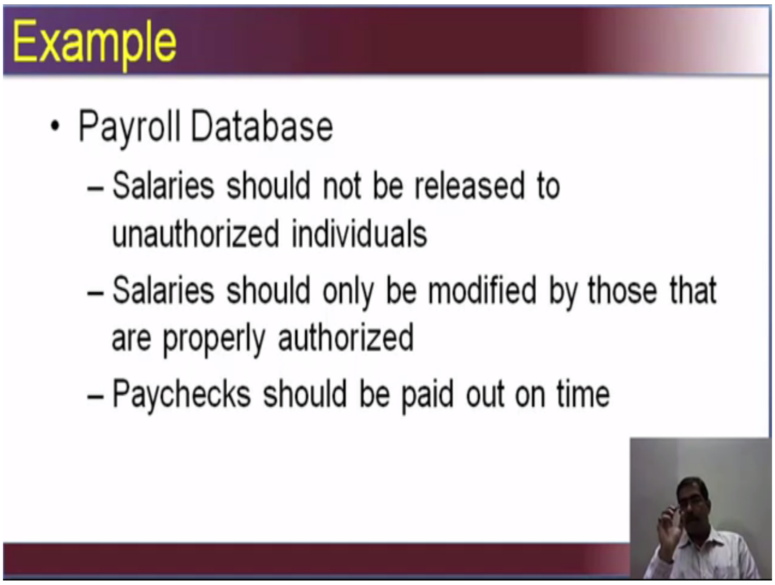


Three Goals of DB Security

1. Confidentiality
   - refers to the protection of data against unauthorized disclosure
2. Integrity
   - refers to the prevention of unauthorized and improper data modification
3. Availability
   - refers to the prevention and recovery from hardware and software errors and from malicious data access denial making the database system unavailable

So, but what are the goals of database security, three goals of database security, we have seen over and over again in this course. CIA, the confidentially, integrity, availability, the same goals applied to database security also. Now, in this context, confidentiality refers to protection of data, against unauthorized disclosure. Integrity refers to the prevention of unauthorized and improper data modification. And availability refers to the prevention and recovery from hardware, and software errors, and from malicious data access , making the database system unavailable.

(Refer Time Slide: 13:38)



Example

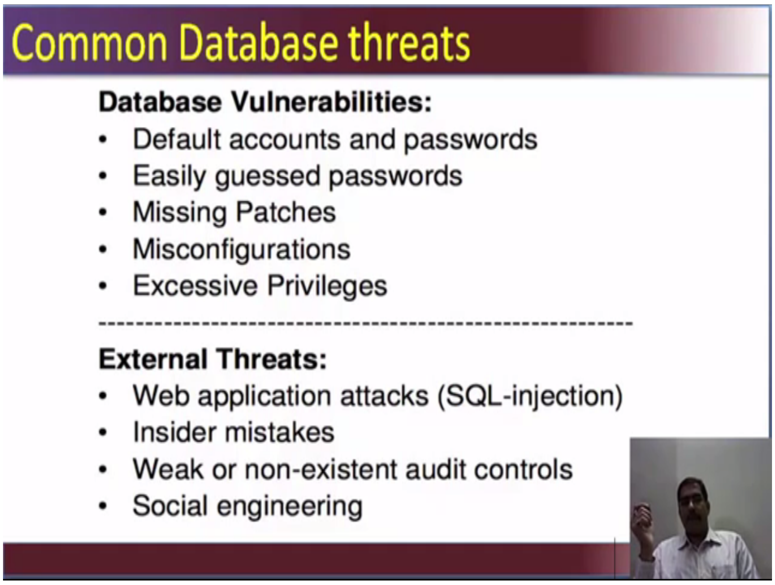
- Payroll Database
  - Salaries should not be released to unauthorized individuals
  - Salaries should only be modified by those that are properly authorized
  - Paychecks should be paid out on time

So, basically protect against destruction of database or loss of data. Let us see a simple example, let us consider a payroll database, the salaries should not be released to unauthorized individuals, nobody else should know the other employer, the database itself. Then, the salaries should only be modified, by those who are properly authorized do so.

Then paychecks should be paid on time. So, in this example, you can have let us say that, there are 20 employees in an organization one particular employee, wants to know what the other person is drawing. So, he tells the SQL coding on the database. First, he asks how many employees are there in the organization. So, then the database prints out 20, how many are male it prints out 6, how many are female are automatically inferred.

Then what is the average salary, total salary paid to all male employees. It gives the figure, if so he gets the value of what is the salary paid to all female employers, then he further filter out on this side for this row, or this position in the organization, what is the salary paid. So, he selects that particular thing from the table, and then he transferred. So, he can do a inference check, and find out what is the salary paid to some other employee .so, this is an example for payroll database.

(Refer Time Slide: 15:18)



Common Database threats

Database Vulnerabilities:

- Default accounts and passwords
- Easily guessed passwords
- Missing Patches
- Misconfigurations
- Excessive Privileges

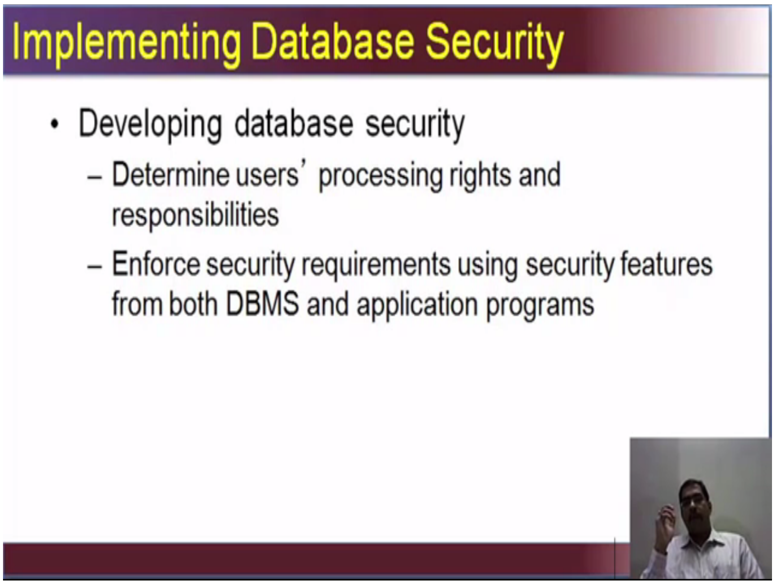
External Threats:

- Web application attacks (SQL-injection)
- Insider mistakes
- Weak or non-existent audit controls
- Social engineering

Now, let us see some common database threats. Default accounts and passwords as in the network, or as in the server, as in the application, same thing applies here. Default account and passwords, easily guess our password. Let say you pick simple one like abc or 12345 and 6. So, that is a issue. Missing patches, again like OS, the security patches, as when the relieved vendor should be applied immediately.

The database not configured properly, or default database, which come along with the database when installing it, is there, so no proper is there. Then excessive privileges are given to certain users, that is the vulnerability. From the external perspective, web application attacks like SQL injection happened, insider errors or mistakes that happen, weak or nonexistent audit controls. So, the audit login criteria is not there, it is there, but no control over what is logged. Then social engineering could be another threat which can happen from outside.

(Refer Time Slide: 16:36)

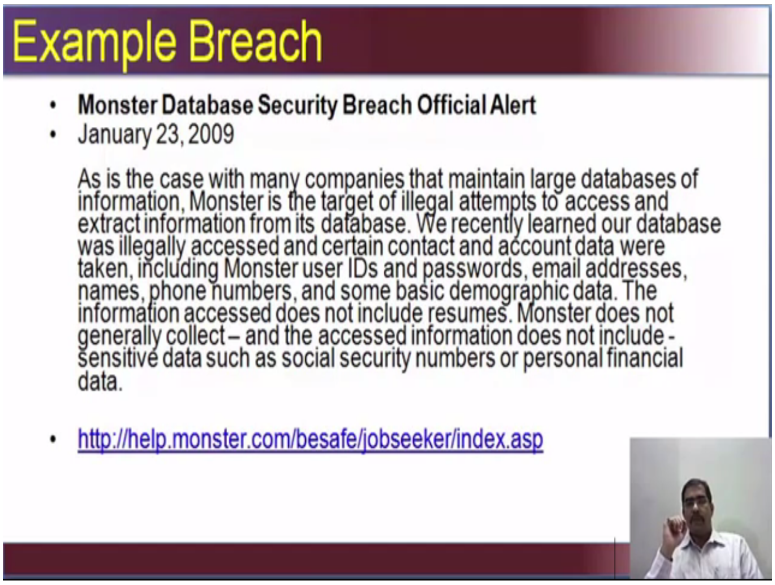


Implementing Database Security

- Developing database security
  - Determine users' processing rights and responsibilities
  - Enforce security requirements using security features from both DBMS and application programs

How do you implement database security, determine users processing rights, and responsibility. So, the first thing you do is understand what the use or needs, what rights you requires to perform this job, then enforce the security requirements, using security features from both database management system, and the application programs. So, it is not enough to restrict your dbms itself, you need to provide controls in the application, that connects to the database also.

(Refer Time Slide: 17:09)



Example Breach

- **Monster Database Security Breach Official Alert**
- January 23, 2009

  As is the case with many companies that maintain large databases of information, Monster is the target of illegal attempts to access and extract information from its database. We recently learned our database was illegally accessed and certain contact and account data were taken, including Monster user IDs and passwords, email addresses, names, phone numbers, and some basic demographic data. The information accessed does not include resumes. Monster does not generally collect – and the accessed information does not include - sensitive data such as social security numbers or personal financial data.

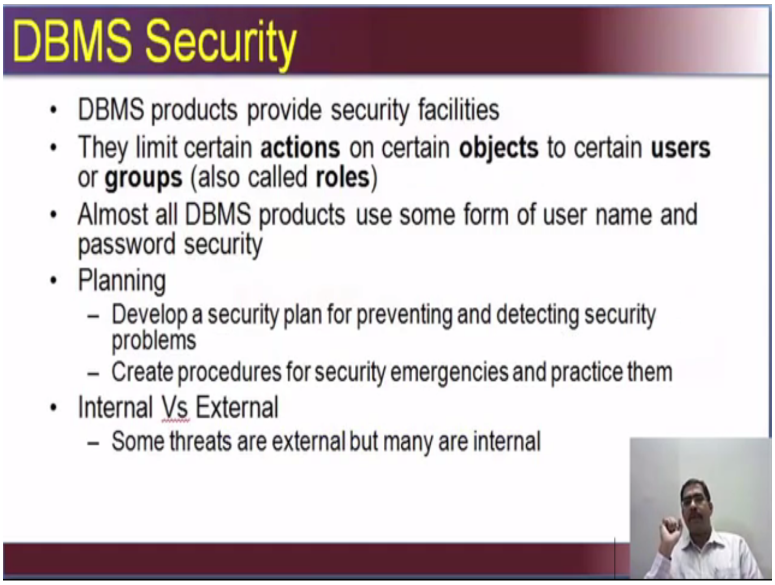
- http://help.monster.com/besafe/jobseeker/index.asp

There is an example, breach, monster database, there was a security breach on January 23rd, 2009. The article is given there. Now, here there are non server ,target of illegal attempts, if some people try to access it and extract information from the database. So, monster learned that their database was illegally accessed, and certain contract , and account data were taken including user ids, and password, email addresses, names, phone numbers, and some other basic data.

Now, the information accessed does not include resumes. So, basically monster is a portal where the resumes are uploaded and downloaded. But this particular attack did not involve hacking the resumes. And then it also says that, monster does not generally collect, and the access information, does not include sensitive data, such as social security numbers, or personal financial data, this is what the statement was given by monster.

But then, the hackers manage to to find the user ids, and password, find email addresses, name, phone numbers. So, they have the lot of information by which, they can do impersonation attack, which is not mentioned here. So, there are other attacks, that can happen which has not been mentioned here, but according to monster, they say that since financial data was not stolen, and financial data here is critical and social security numbers are not stolen. They say it is pretty ok.

(Refer Time Slide: 19:00)



DBMS Security

- DBMS products provide security facilities
- They limit certain **actions** on certain **objects** to certain **users** or **groups** (also called **roles**)
- Almost all DBMS products use some form of user name and password security
- Planning
  - Develop a security plan for preventing and detecting security problems
  - Create procedures for security emergencies and practice them
- Internal Vs External
  - Some threats are external but many are internal

Most of the database management products, which are available in the market, whether it will open source or commercial, they provide security facilities and features, they limit certain actions on certain objects to certain users, or certain groups. So, certain actions means, read, write, execute is an action on certain objects; object can be a table with in that database to certain users, means it is available or accessible only by the, say the administrator or the group or groups may be the administrator group, the user group. So, whatever role has been allocated, so we can limit actions, some certain objects to certain users, and all database products use some form of user name, and password security. So, the basic security of accessing the database, that is user name and password will be available with almost every database product.

Then planning, develop a security plan for preventing, and detecting security problems. So, you need to have proper plan to prevent, and detect security problems. So, for that you will have to understand how the DBMS is configured, what is its intent to serve, and then create procedures for security emergencies and practice them like, if there is a database failure that happens, if there is virus attack, or major attack from an internal source happens. Again here, internal versus external.

So, some threats are external, but many are internal. When it comes to database acts, many are internal. So, we need to particularly emphasize, the importance of database in an environment where more.