

Replay: use previously captured user response

use challange response protocol equasdropping: gain password by observing user/ read withen password! keyshoke logging. use multiple factors Static biometrics,

use device auth.

Trojan Horse: device prevends to be auth derice to gain password

> Penial of service: disable user auth by flooding host with requests can be done to a selective user by exceeding log-in limit. use multiple auth factors.

=> Database Security :

5-1: Need for database security

\* Organizations need to provide access to databases but also prevent it from internal & external security threats.

continued ...

SQL is more complex than HTTPS

requires full understanding of sal to

have

effective

security measures

Dahabase Security not up to pace

new rearuses in o pems has inmoduced new vulnerabilities 2 poventian for misuse.

Catalogge Staff has limited knowledge of security 1 vice versa

in an enterprise, mixture of database pratforms are used hence implemenwww.sanpak.biz tation of seconing 15 difficult.

# 5.2: Parabase management systems

- by one or more applications.
- & DBMS a suit of program to consmoct & maintain the database.
- & Query language provides a uniform inverface to database for users & applicants.
- \* DDL used to define database logical smoothre \*

  Procedural properties.
- x DML provides a powerful set of tools for developers.
- Permission to non query on database.
- \* concurrent access take prevents conflicts when simultaneous conflicting commands are executed.
- \* Database os complexity & criticality generales security requirements beyond os-based security mechanisms.
- \* 05 only controls read | write access control whereas

  Dems provides more operations like select lineert |

  update | delete. Hence requires seperate security mechanism.

## 5.3: Relational Databases

\* A two dimensional file (rows 2 columns) is called a fatfile.



- \* Rows referred as topies .
- \* columns referred as attributes.
- \* Phony key to uniquily identify each column.
- \* Foreign key primary key of another take, used to creave relations.
- of a query. Used for security purposes to restrict access so user can only view certain rows columns.
- + Sal used to define schema | manipulate | query data.

#### 5-4 - SQL injection attacks

- \* SOL injection attack is one of the most prevenant? dangerous attack.
- \* 19 designed to exploit nature of web application pages. When dynamic data is send I retrived from database senter through API calls. Malicious SQL commands can be send.
- execute arbitally of commands, launch bos or delete data.
- \* SOLI can take place when input not correctly fillered for sming liveral escape characters / not smongly typed.

- traffic to be executed on database senier. This mill neturn desired results.
- appending a new command, and use in to make it seem like a comment.
- Second-order injection: Occur due to incomplete prevention mechanisms for SOLi can rely on dara already user in

present to migger an

user input: Suitably
crafted user
input send through
72 USET | POST
requests.

cookies: can f

So when sovies

Smuchure & Function are modified.

Physical user input:

Use external inputs

like RFID tags I barcodes

to pass to DBMS

to perform SOLi

SOL: AMACK OVERUES

2 types

Sener variables:

in calection of variables

that contain HTTP

headens, network

protocals & environment

variables. used for

logging usage statistics

& browsing trends.

If logged to database

without sanitinzation. can

cause soli winerability.

Hide attack in headers.

- \* There are 3 main categories of attack types:
  - inband: uses same communication channel for SOLI & retrieve results to be displayed on same webpage.
  - inferential:- no transfer of data. Attack sends

    petricular requests to observe behaviour of

    database server & reconstruct information.
  - out of bound :- data retrieved using different channels . Used when limitations on data retrieval byt. outbound connectivity of database sever is relaxed .

# end-of-line-comment:

add -- after injecting

code into a

particular

fied to inleand

nullify it attack

tautology: inject
code in one I more
conditional
conditional
statement so they
always
return the

Piggybacked queries: add more query instead of the inverded query. Relies on server configuration allowing different queries in a single stringe of code.

Blind SQL

injection: allows Inferential

to infer data attack

present even though

System glues no such

info . Ask server

true! false

questions.

incorrect queries:

chather hype 1
smuchure of backend
database.

perautt emor page of
an application is too
descriptive

- of techniques are used.
- « countermeasures have 3 categories. Defensive coding, detection & run-time prevention.
- insertion:
  more accurately
  expecify
  sal query structure.
  Pass parameters
  separately instead of
  unsanitized user input

manual defensive coding practices: Insufficient input validation is exploited by soli use pattern matching & input type checking.

I SOL DOM: uses a type checking API to process systematically regulated query

MON	TUE	WED	THU	FFU		SUM



V

Anomaly-based:

Delect behavioural a

Pallems outside

normall range

Training phase

followed by

detection phase

Detection

Signature-based:

match epecific

attack patterns.

constrainty updated

will not work against

self-modifying

attacks.

code analysis: use of test suite to detect uninerabilities. Generate wide range of soli attacks 2 assess system?s response.

\* Run-time prevention: techniques to check queries conform to model of expected queries at run time.

#### 5.5: Database Access control

\* DBMS operates on the assumption computer has authenticated each user.

\* Ownership - based a

administration: owner may

grant | revoke

rights.

Centralized administration: Some priveleged

ministrative revoke rights.

support administrative policies

Decentralized administration: Owner can grant revoce access rights to table &

www.sanpak.biz authorization rights to

user.



- x Access rights can be entire table | databases | Scieded DWS/ columns.
- \* 8 OL provides two commands GRANT REVOKE. can be use to give access rights / assign a role to an user.
- \* Ranges of access rights include: select, Insert, Update, Delete, Reference - define Poreign keys in another table.
- \* If an user revokes the access rights all coscoded access is granted are also revoked.
- Database systems support dozens of applications unlike a file system. Hence we use RBAC.

end user other than application owner: operate

on darabase objects via

Database user application but do not own them categories

Application owner:

End user who owns

database Objects.

> objects generaled by application or prused.

Administrator: have administrative responsibility for part or all of the database.

Administrators can assign users administrative based roles.



- \* RBAC needs to provide:
  - create & delete roles.
  - Define permissions for a role.
  - Assign & cancel assignment of users to roles.
- \* Administrator cannot add/delete/modify fixed roles. They can only add/remove users as members to fixed roles.
- \* Fixed server roles defined at server level are independent of any user. Have different permissions and intend to distribute administrative responsibilities.
- \* Fixed database roles at the level of individual database · some roles designed to help DBA to dismibute administrative privaleges while others for an end user.
- \* User-defined roles users create roles . Are 2 types
  Standard:- authorized user can assign users to roles,
  and applications:- associated with application &
  requires password.
- \* user that has access to application can use application role.

#### 5.6: Inference

\* Performing authorized queries & deducing unauthorized information from legitimate responses.



- is more sensitive can be used to intersensitive data.
- \* metadata is corelation / dependencies between data liens.
- \* Information transfer path of unauthorized data is called inference channel.

Inference detection at a query time:

Eliminate inference Approaches dealing with inference inference inference

query denied lanered.

Inference detection
during database

higger design:
Alter database
smuchure / change
access control regime.

Remo Split data into
multiple tables /
fine-grained access
control of roles.

Unnecessary access
control limits availability.

### 5.7: Database encryption

k Encryption is last line of defense in database security

Disadvantages

Difficult to Perform record

channel detected

searching on encrypted database

enthorized users
should have
decryption key
Providing secure
keys is complex.



- \* Encryption can be applied at record level , attribute level (column) / individual field.
- \* DBMS requires skilled personnel to maintain, update, protect from disaster & secure database.
- \* To user encrypted database: (Not flexible method).
  - user sends sall query with specific value of primary key.
    - client query processor encrypts query's primary key.
    - Server processes query & returns appropriate record.
    - Query process decrypts response & displays.
- \* To provide more flexibility each row is encrypted as a block.
- \* mapping function is stored at clients & data owner's.
- \* Each data is divided in a range and each range is assigned an attribute.
- \* Indexing scheme prevents attacker from understanding data because metadata is not stored on senier.
- \* Different chunks of database should be encrypted with different keys so user only access those which they have keys to decrypt. (RBAC).