CONSTRUCTOR UNIVERSITY

Security and Authorization

Ramakrishnan & Gehrke, Chapter 21


NAUTOMAT


YOU REMEMBER MY PIN?

Overview

- Introduction
- Internet security
- Database access control
- How to hack a database

Intro to DB & Web Service Security

- Secrecy:
  Users should not be able to see things they are not supposed to
  - Ex: student can't see other students' grades
- Ex: *TJX*. owns many dept stores in US
  - Attacks exploited WEP used at branches
  - Over 47 million CC #s stolen dating back to 2002
  - *…sue filed by consortium of 300 banks*
- Ex: *CardSystems, Inc:* US credit card payment processing company
  - 263,000 CC #s stolen from database via SQL injection (June 2005)
  - 43 million CC #s stored unencrypted, compromised
  - *…out of business*

Intro to DB & Web Service Security

- Secrecy:
  Users should not be able to see things they are not supposed to
  - Ex: student can't see other students' grades
- Ex: *Equifax 2017* [Siliconbeat]
  - Collecting most sensitive citizen data for credit assessment
    - ssn, name, address, birth dates, credit cards, driver's license, history, …
    - 143m customers affected
  - "maybe dozens" of breaches, fix only 6 months after warning
  - hacked due to insufficient internal security; patch not installed, but got known
  - *BTW, senior execs sold 1.8m in stock*

It would be nice to think that perhaps the company was a victim […] of clever hackers using social engineering […], but it appears […] that there is gross incompetence involved.

Intro to DB & Web Service Security

- Secrecy:
  Users should not be able to see things they are not supposed to
  - Ex: student can't see other students' grades
- Integrity:
  Users should not be able to modify things they are not supposed to
  - Ex: Only instructors can assign grades
- Availability:
  Users should be able to see and modify things they are allowed to
  - Ex: professor can see and set students' grades(but possibly not modify after release)

Database Access Control

- A security policy specifies who is authorized to do what
  - Authentication: “let me in”
  - Authorization: “let me do this”
- A security mechanism allows us to enforce a chosen security policy
  - Implemented in DBMS
- Two main mechanisms at DBMS level:
  - Discretionary access control (=security at users’ discretion)
  - Mandatory access control (=security enforced)

GRANT Command

GRANT privileges ON object TO users [WITH GRANT OPTION]

- The following privileges can be specified:
  - SELECT: Can read all columns (incl those added later via ALTER TABLE command)
  - INSERT(col-name): Can insert tuples with non-null or non-default values
    - *INSERT means same right with respect to all columns*
  - DELETE: Can delete tuples
  - REFERENCES (col-name): Can define foreign keys (other tables) to this column
- If a user has a privilege with the GRANT OPTION, can pass privilege on to other users (with or without passing on the GRANT OPTION)
- Only owner can execute CREATE, ALTER, and DROP

GRANT and REVOKE of Privileges

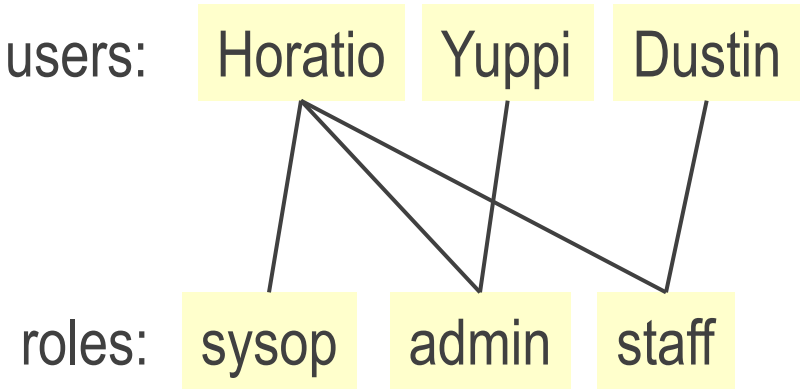
- GRANT INSERT, SELECT ON Sailors TO Horatio
  - Horatio can query Sailors or insert tuples into it
- GRANT DELETE ON Sailors TO Yuppy WITH GRANT OPTION
  - Yuppy can delete tuples, and also authorize others to do so
- GRANT UPDATE (rating) ON Sailors TO Dustin
  - Dustin can update (only) the rating field of Sailors tuples
- GRANT SELECT ON ActiveSailors TO Guppy, Yuppy
  - This does NOT allow the 'uppies to query Sailors directly!
- REVOKE cascades: When a privilege is revoked from X, it is also revoked from all users who got it solely from X

Views and Security

- Views can be used to present necessary information (or a summary), while hiding details in underlying relation(s)
  - Given ActiveSailors, but not Sailors or Reserves, we can find sailors who have a reservation, but not the bid's of boats that have been reserved
- Creator of view has a privilege on the view if (s)he has the privilege on all underlying tables
- Together with GRANT/REVOKE commands, views are a very powerful access control tool

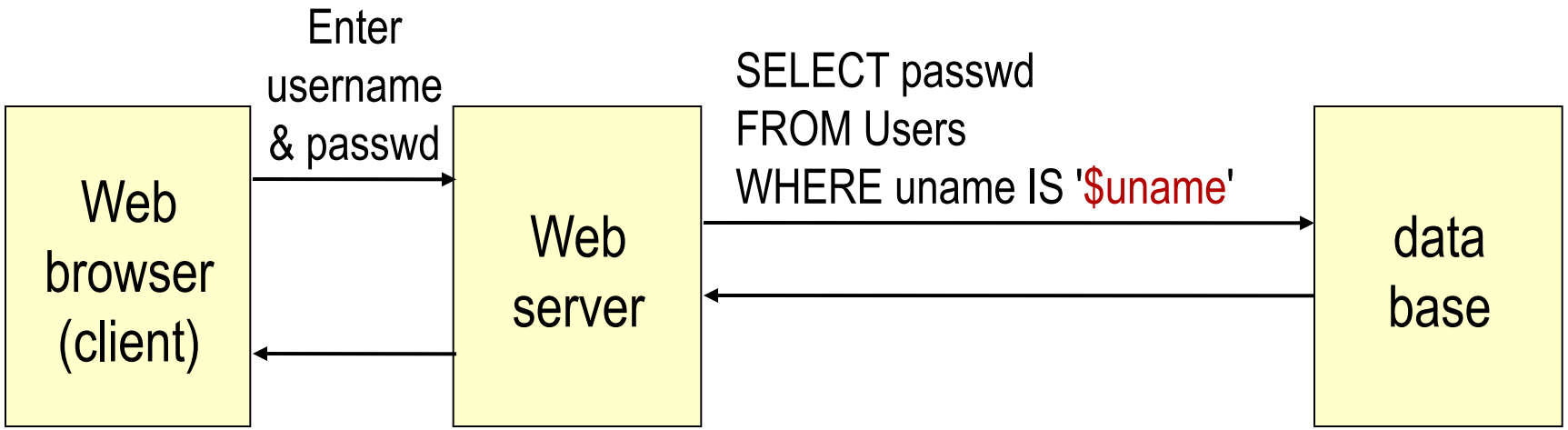
Role-Based Authorization

- In SQL-92, privileges were actually assigned to authorization ids, which can denote a single user or a group of users
- In SQL:1999 (and in many current systems), privileges are assigned to roles
  - Roles can then be granted to users and to other roles
  - Reflects how real organizations work
  - Illustrates how standards often catch up with “de facto” standards embodied in popular systems



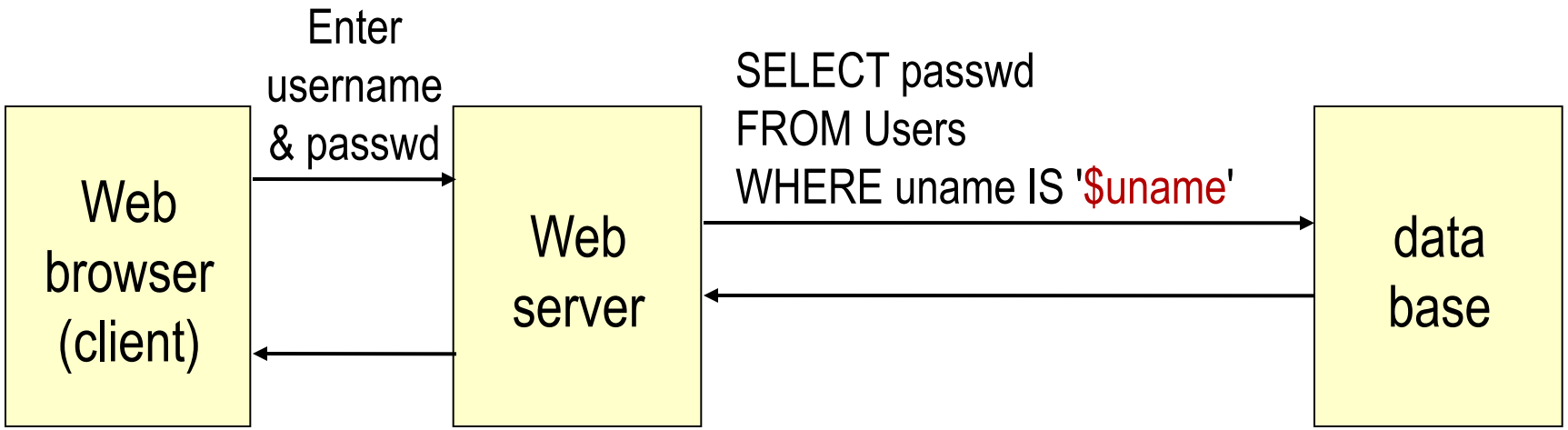
How To Hack a Database

- Most common: SQL injection
  - Compromise database query



How To Hack a Database (contd.)

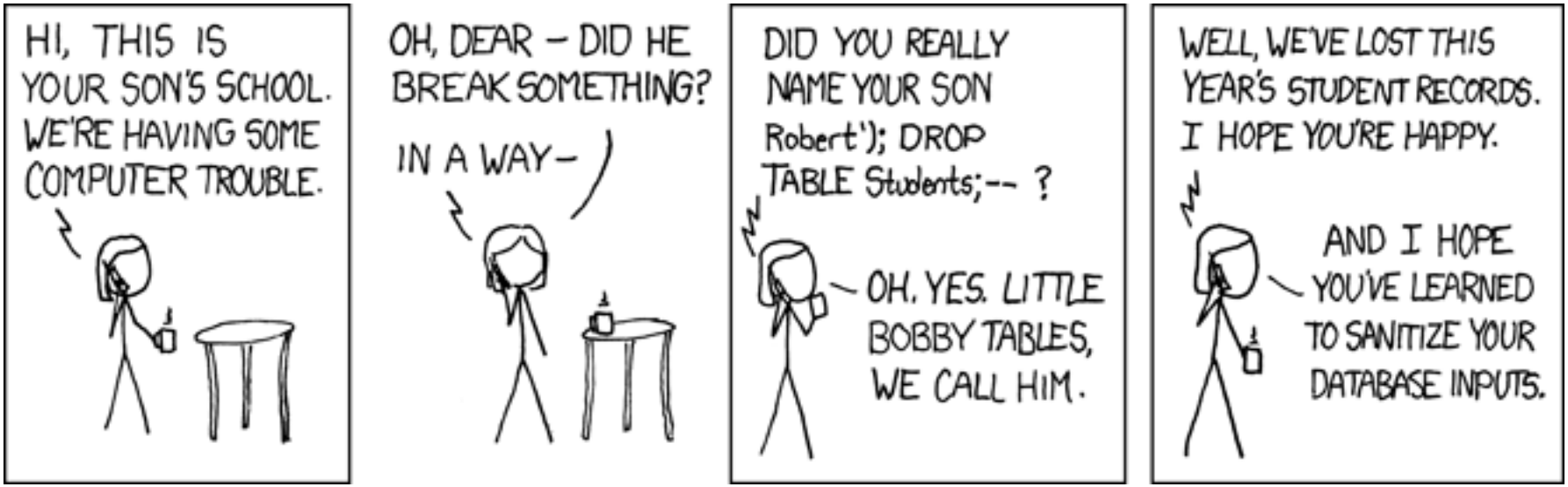
- Most common: SQL injection
  - Compromise database query



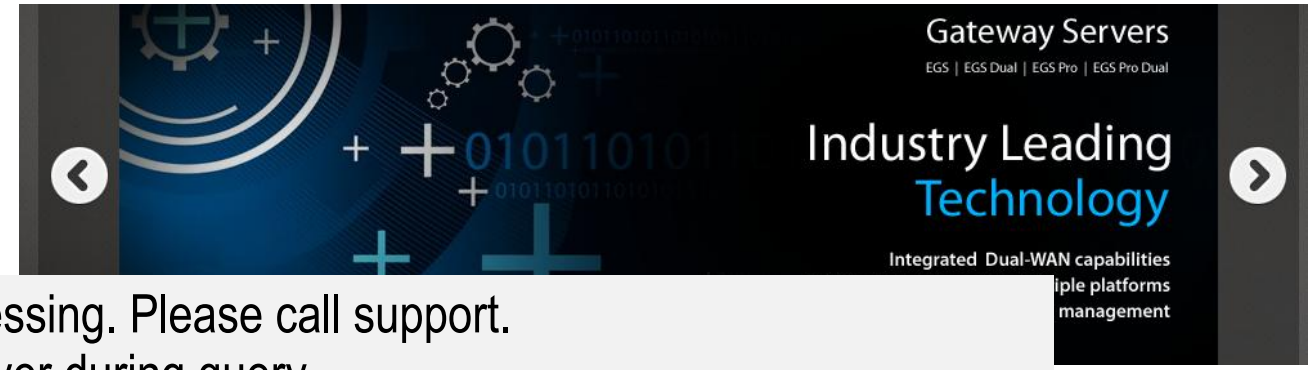
- What will happen at input of '; DROP TABLE Users; -- ? (keyword: DoS)
- *Name 2 independent techniques to prevent!*

Mom 's a Hacker

[found by: Prashant Vaibhav]



How to Expose Yourself



An error occured durring processing. Please call support.
Lost connection to MySQL server during query
SQL: select count(*) from LoginsActive where MacAddress=\'00:21:70:6E:04:AE\' and MacAddress!=\'\' and Iface=\'br0\' and PropertyID=\'51225\'
IP:sql.ethostream.com
DBU:remote
DB:

OK, that was in 2011.

Command Injection: Another Example

- Target: Web browser login page, credentials input
- Enter this as user name:

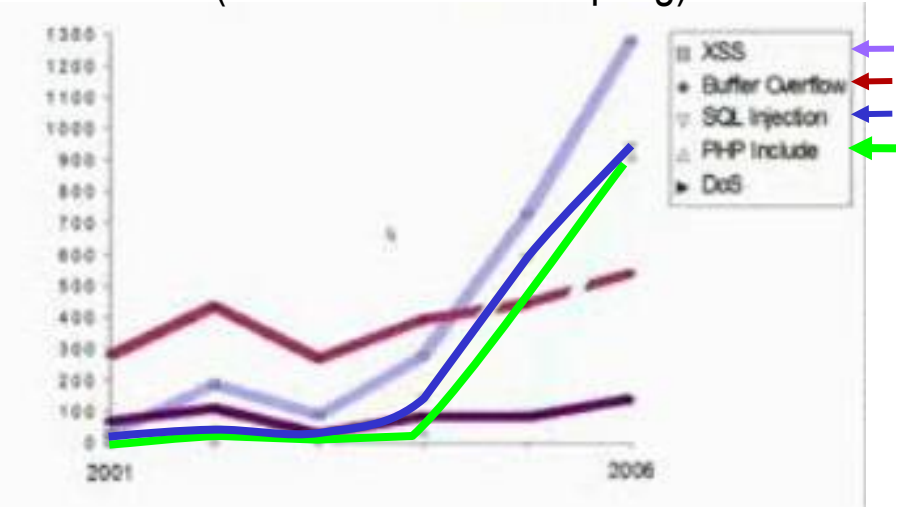
```
<script>alert(1)</script>
```

- What do you expect to happen?
- What type of security leak does this point at?

SW Reasons for Service Attacks

- Missing input validation
- Design errors
- Boundary conditions
- Exception handling
- Access validation

Vulnerability trends [Mitre]
(XSS = cross-site scripting)



- *Red = targets with increasing stats*
  - *See also: OWASP Top 10*

Case Study: Common Security Neglicences

- In 2014, Sony Pictures suffered major break-in
  - possibly by North Korea, in relation to movie *The Interview*
  - "mostly facilitated by unprecedented negligence"
- Problems included:
  - unencrypted storage of sensitive information
  - password stored in plain text files, sometimes even called "passwords" or placed in same directory as encrypted files
  - easily guessable passwords
  - large number of unmonitored devices
  - lack of accountability and responsibility for security, ignorance towards recommendations and audits
  - lack of systematic lesson-learning from previous failures (which included 2011 hacks of Sony PlayStation Network and Sony Pictures that stole account information including unsalted or plain text passwords)
  - weak IT and information security teams
- Stolen data included employee data (including financial data), internal emails, and movies

„salted" ?

Afterthoughts: Security and Software Engineering

- Additional security related engineering principles, such as: [Neil Daswani]
  - least privilege
    - *No more rights for any app than absolutely necessary*
  - fail-safe stance
    - *Always return to safe, stable state, after any kind of deviation*
  - protecting against weakest link
    - *Rank vulnerability of components, pay particular attention to "champions"*

mobile apps?

- 3 P security management:
  Process,
  People,
  Probing your defences