Lecture notes for 6.1-6.3 database security

Today: database security
Next week: data confidentiality

DBMS

- Database management system
- Frontend mediating access to physical database
    - Reference monitor to the DB
    - Similar to access control portion of OS

Database integrity

- Access control
    - Authorization: only authorized users update data
    - Protection: outside illegal program, power failure, fire, etc should not corrupt data
- DB integrity maintained by DBMS, OS, admins
    - Regular backups
    - Transaction log
- Element integrity maintained by DBMS performing access control
- Element accuracy: DBMS identify human data entry mistakes
    - Field format checks
- Changelog

Access control

- DB manager specifies level of access for all users
- DBMS manages access, similar to OS
- Hard problem: user can infer data without reading it (discussed on Wed)
- Hard problem: field permissions much smaller granularity than files

Authentication

- May require user authentication beyond OS user ID

Reliability

- No corruption in database
    - No half-completed updates
    - Must recover from update interrupted midway (e.g. By power cut)

- Two-phase commit
  - Phase 1: Intent
    - Create a log of the changes that will be made
    - Gather data, create dummy records, lock out other users, calculate final results
      - Shadow value: locally stored value for DB field
    - Make no permanent changes to the DB
    - If system fails during phase 1, no harm: simply restart phase 1
  - Phase 2: Commit
    - Set commit flag, begin making permanent changes
      - Write shadow values to DB fields
    - Phase 1 cannot be repeated at this point
    - Phase 2 can be repeated as many times as necessary
    - If system fails during phase 2, DB can repair data by repeating phase 2
    - Clear commit flag as final step, DB back in good state
- Error detection / correction
  - CRCs, Hamming codes, parity bits
  - Allow recovery from bit errors in storage
- Recovery
  - Maintain log of changes since last backup
  - If restore from backup, replay log
  - Log should be on storage medium that will not simultaneously fail with DB

Concurrency

- Atomic operation: query-update
  - Handled via field / record locking
- No reading during writing
  - Handled via field / record locking

Monitors

- Part of DBMS maintaining DB integrity
- Test data entry format correctness
- Enforce assertions over data
  - (e.g. only one president in the entire DB)