

Security

Threats

- see private data
- corrupt data
- availability

Control

- encryption
- Grant/Revoke
- validate data
- flow control
- inference control

User's files

Data = ' ' |

SELECT * FROM users

WHERE uname = ' ' AND
pword = ' ' |

~~bob~~ OR 'x'='x

USER
password

precision: protect sensitive data
while disclosing nonsensitive
data.

Access control (Role based)

assign a class to

subjects: users, programs

objects: relation, tuples, columns
views, operations

rules:

subject S can't read

object O unless
 $class(S) \geq class(O)$

subject S can't write object O
unless $class(S) \leq class(O)$