

# Security I

Good fences make for good neighbors

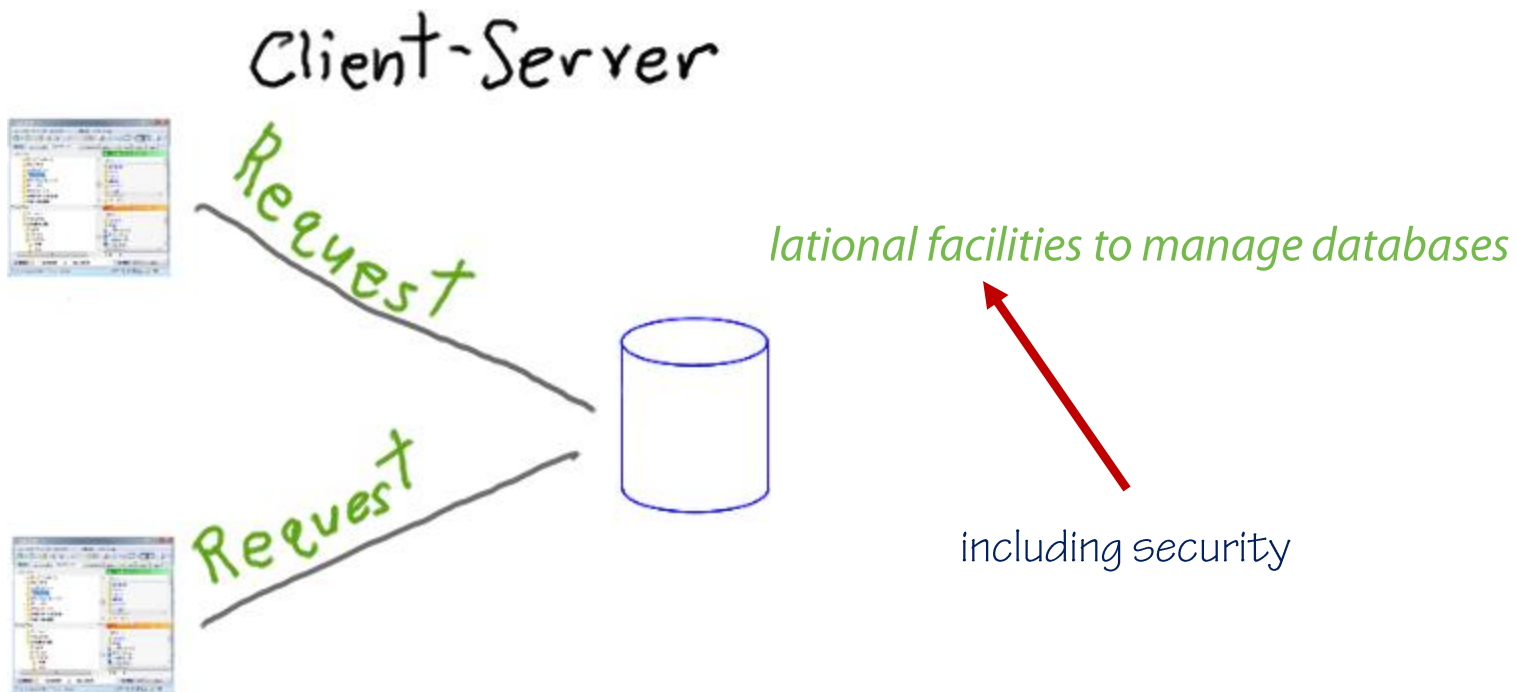


# Overview

- Data must be protected
- Data must be available to many users
- principal -> authenticate -> permissions -> authorize

# To Protect and Serve

- Authentication
- Authorization



# Principal

- Authenticated identity
- Server
- Database

Principals

Joe  
Mary  
Jim  
Jane

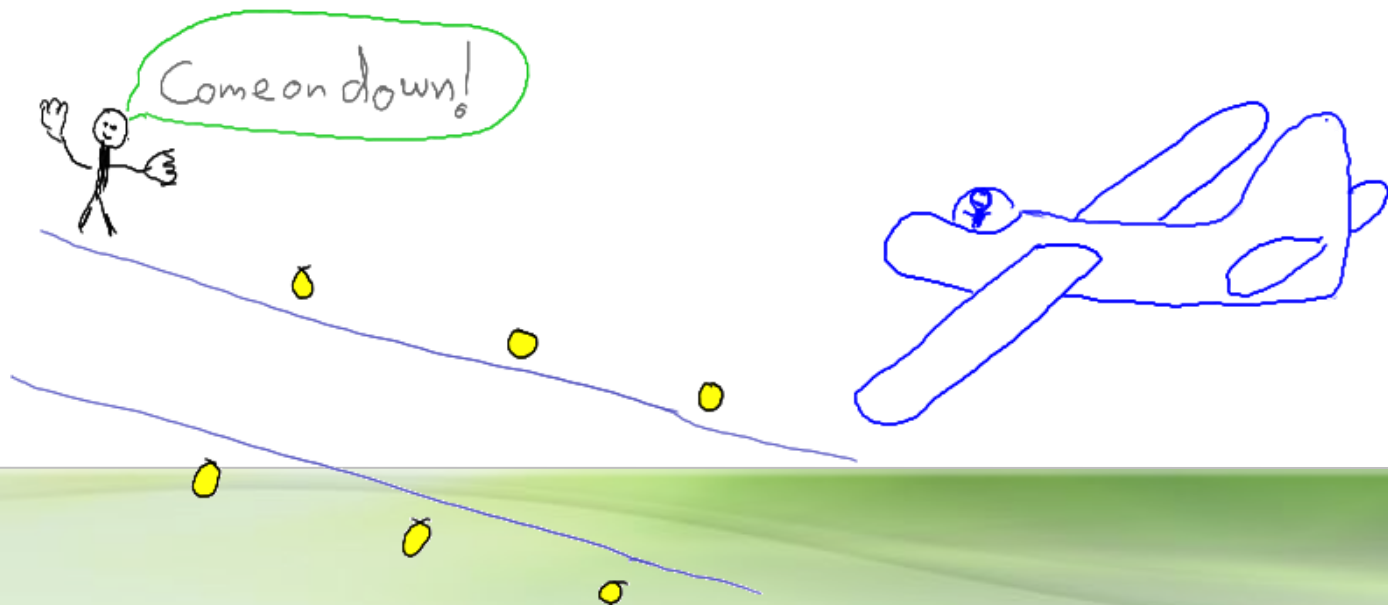


# Object

- **Principals use objects**
  - *e.g.* server, database, table
- **Use specific to object**
  - table : select
  - stored procedure : execute

# Authorization

- **Associates principal, object, authorization to use**
  - *Joe is authorized to select rows from the accounts table.*
- **Ad hoc**
  - login
- **Permission**
  - framework for managing many authorizations, principals, objects
  - used for most authorizations




# Permissions

- Applied On **object** To **principal**
- Positive or negative
  - grant, deny, revoke

sys.server\_permissions

sys.database\_permissions

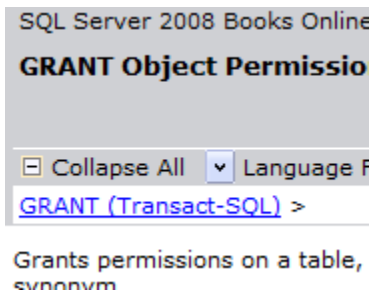
sys.fn\_my\_permissions



my authorizations

# Covering Permissions

- Applying a permission applies the permissions it covers
- Relationship defined in BOL
- `fn_builtin_permissions`



Object permission	Implied by object permission
ALTER	CONTROL
CONTROL	CONTROL
DELETE	CONTROL
EXECUTE	CONTROL
INSERT	CONTROL
RECEIVE	CONTROL
REFERENCES	CONTROL
SELECT	RECEIVE



# Groups\Roles

- Windows group/ database role is a principal
- Easier to manage users in groups/roles than individual users

# Summary

- **Principals & Permissions**
- **Principals are authenticated**
  - User principals are typically based on Windows credentials
- **Permissions determine authorization**
- **Some permissions cover others**
  - effective permissions
- **Permissions can be managed on a set of principals**

# References

- Codd's Rules [http://en.wikipedia.org/wiki/Codd%27s\\_12\\_rules](http://en.wikipedia.org/wiki/Codd%27s_12_rules)
- Turtles [http://en.wikipedia.org/wiki/Turtles\\_all\\_the\\_way\\_down](http://en.wikipedia.org/wiki/Turtles_all_the_way_down)