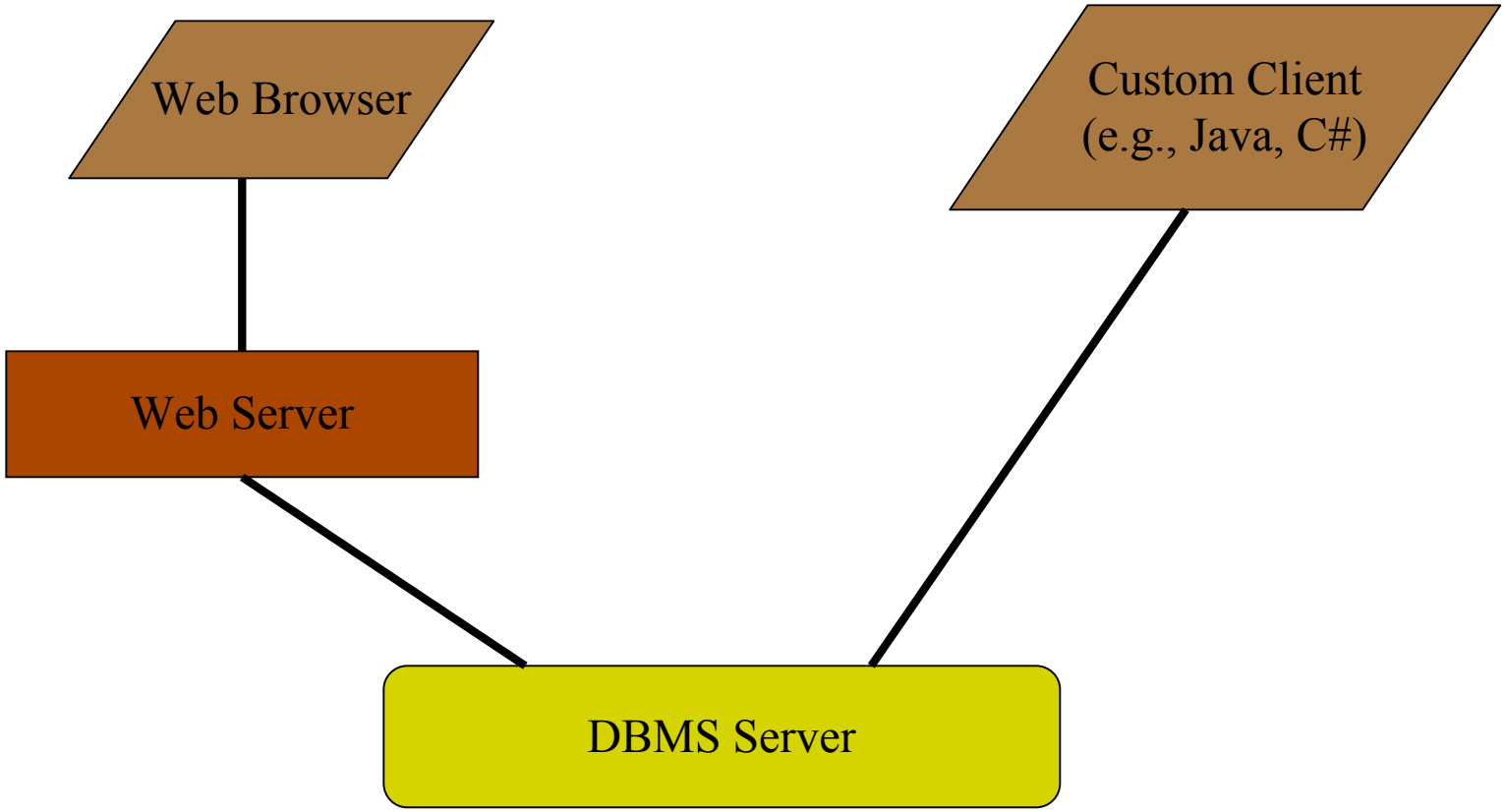
Database Connectivity

Rose-Hulman Institute of Technology

Curt Clifton

Recall Multi-Tier Architectures



Why use stored procedures?

- Could just send individual SQL commands from UI
- Use stored procedures to:
  - Optimize performance
  - Keep SQL code on the server
  - Improve security by preventing casual table browsing and modifications
  - More easily create atomic transactions (more next week)
  - Prevent SQL injection attacks

Another Problem: Injection Attacks

- Consider:
  - Interface presents form prompting for username
    String username = userNameField.getText();
  - Interface builds query to get user's custom picture from database
    "SELECT IDPicture FROM Users WHERE Username = '" + username + "'"
  - Interface sends query to backend database
- So what's the problem?

Another Problem: Injection Attacks

- Consider:
  - Interface presents form prompting for username
    String username = userNameField.getText();
  - Interface builds query to get user's custom picture from database
    "SELECT IDPicture FROM Users WHERE Username = '" + username + "'"
  - Interface sends query to backend database
- User enters: smith; DELETE FROM Users

Guidelines

- Do not build queries using concatenation
- Do not use a highly privileged SQL account for access from the application
- Encrypt the DB connection string
- Cache static information in the application
- Always explicitly define the table columns you wish to fetch
- Use parameter validation at all layers