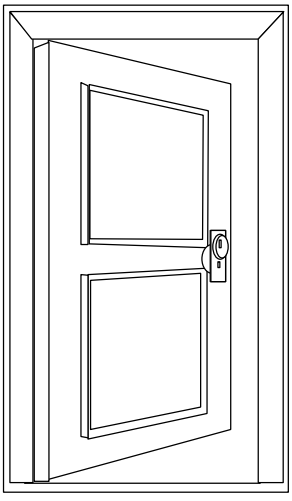
Composer 3
Security Mechanisms Applied

Session 360

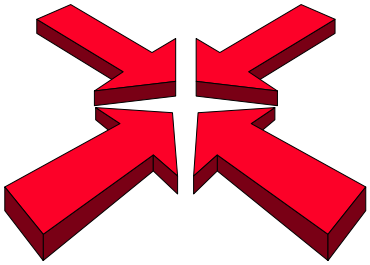
Mary Russell
Texas Instruments

Overview



- Focus
- Remote Data Access
  - Security Mechanisms
  - Security Strategies
- Remote Presentation
  - Security Mechanisms
  - Security Strategies
- Distributed Processing
  - Security Mechanisms
  - Security Strategies
- Summary

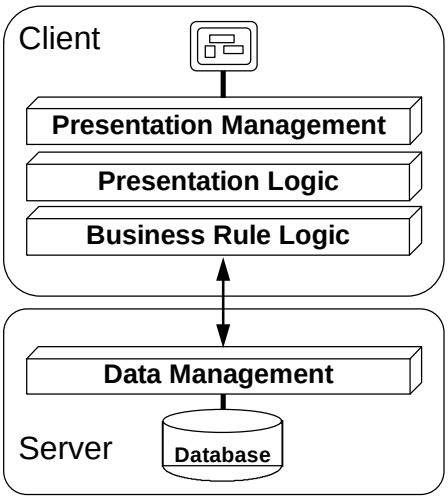
Focus



- Remote Data Access
- Remote Presentation
- Distributed Processing
- UNIX-based implementations
- UNIX-based transaction enabler
- UNIX and Windows 3.1 Clients
- Oracle Databases

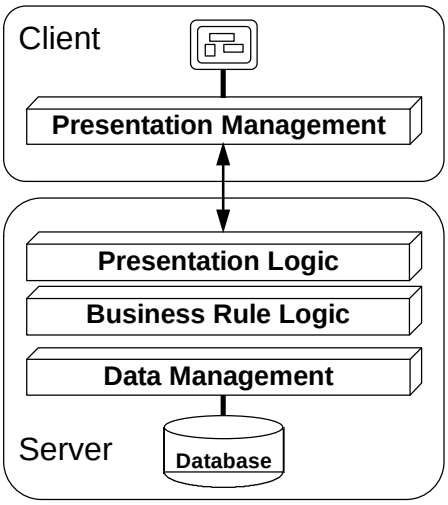
- Not intended to cover every platform or possible security strategy

Remote Data Access



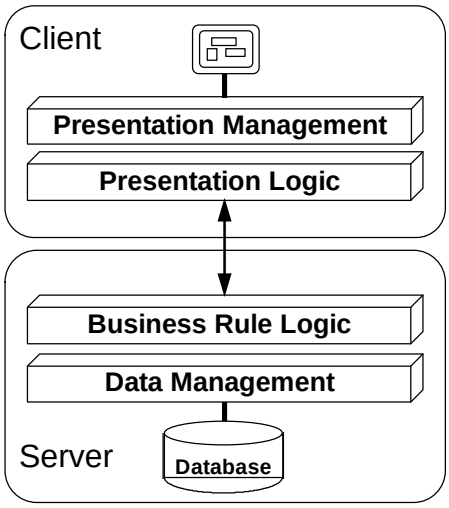
- All logic resides on client
- Uses DBMS product to communicate with database
- Security validation remote to database and located on each client

Remote Presentation



- All logic resides on server
- Visibility to remote application
  - Telnet session
  - Screen-scraping
  - UNIX X-terminal
- Security validation local to database and application logic

Distributed Processing

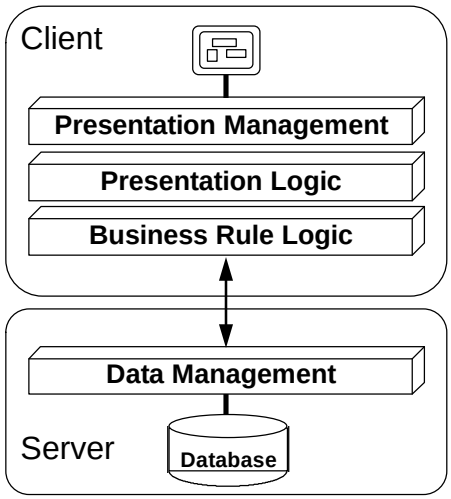


- Distributed logic
- Composer paradigm designed for distributed processing
- Security validation local to the database and server modules

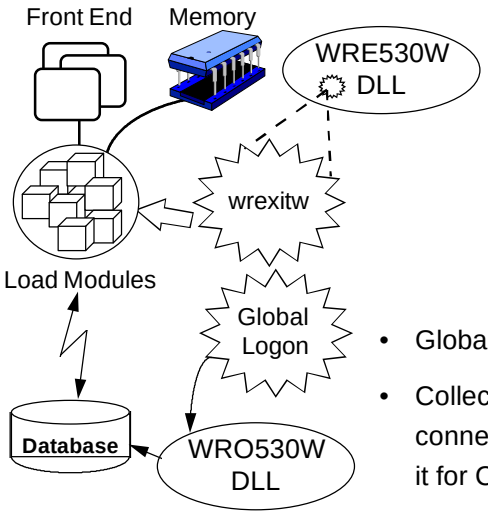
Types of Security

- Operating System Authentication
  - User access validation
  - Operating system Logon validation
- Database Access Authentication
  - Database connect security
- Application Level Security
  - Restricted access to row-level data
  - Restricted access to menu options
  - Restricted access to trancodes

Remote Data Access Mechanisms

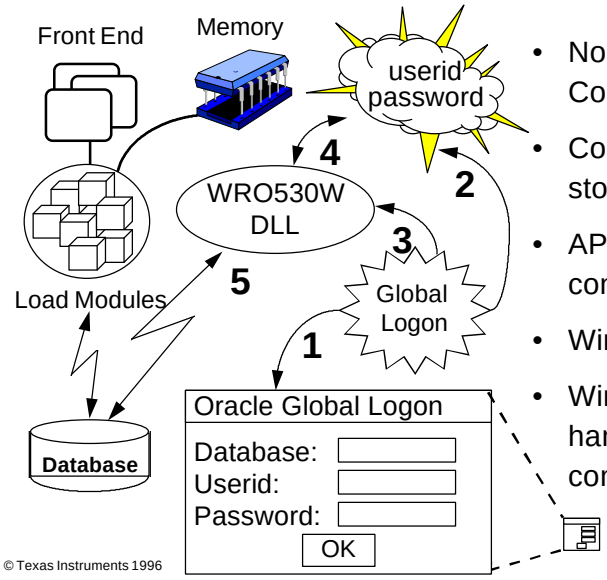


Remote Data Access Security



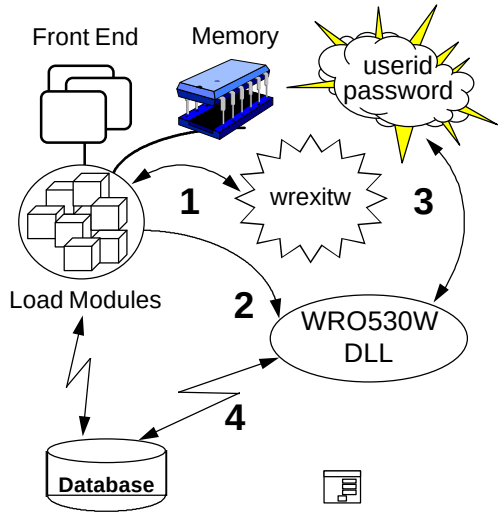
- Windows Runtime Exit (wrexitw)
- Sets special attributes:
  - systemid = Win3.1
  - termid = <NONE>
  - userid = <NONE>
- Cannot be modified in PStep
- Global Logon is standalone executable
- Collects and validates connect data using connect function in WRO530W, then stores it for Composer to use for its connects

Global Logon Call Sequence



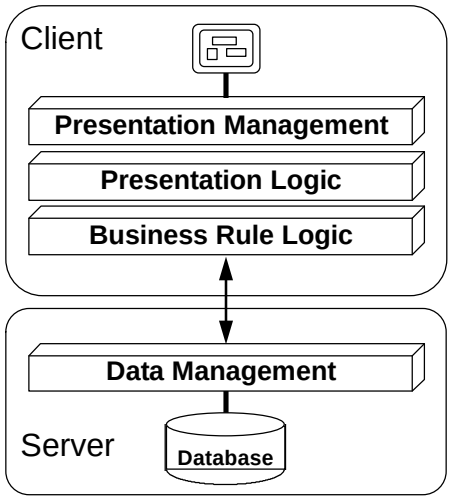
- No communication between Composer & GLogon
- Connect data accepted, then stored in memory location
- API call to WRO530W to connect /disconnect to Oracle
- Window iconizes - keep active
- Windows Runtime Oracle DLL handles connect, disconnect commit, and rollback

Composer Connect Sequence

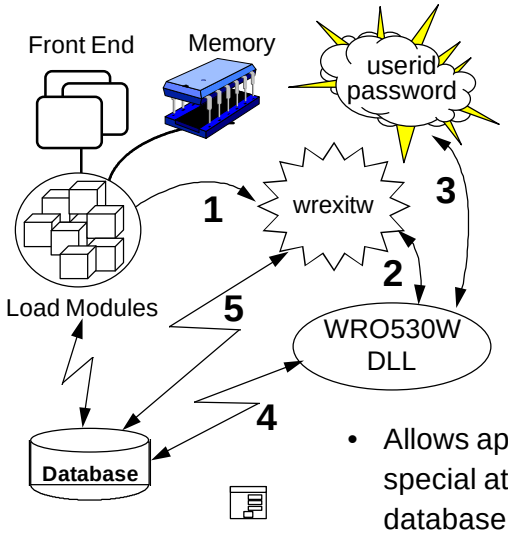


- Window Manager calls wrexitw
- Each Window Manager calls wro530w function to perform database connect
  - Global logon memory location checked
  - dsuser/dspswd checked
  - Oracle connect attempted
  - Failure calls process logon

Remote Data Access Security Strategies



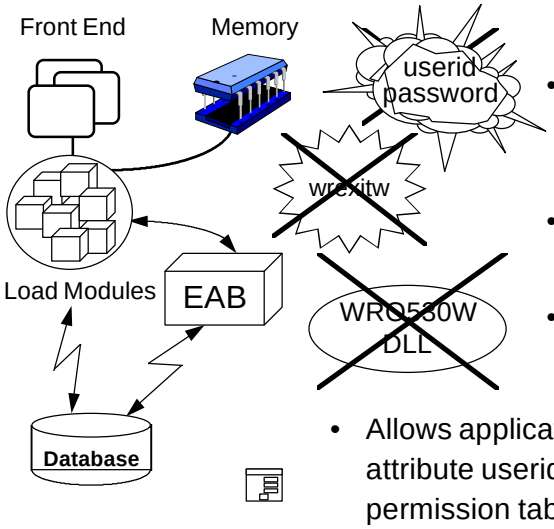
Populating Special Attribute *Userid*



- Cannot establish database connect data within Composer
- Modify WREXITW.c to obtain userid Oracle uses to connect
- Set special attribute userid to userid value returned

- Allows application-level security using special attribute userid and possible database permission table or file

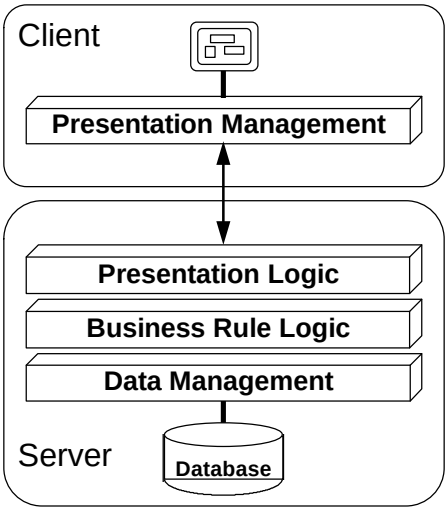
Populating Work Attribute *Userid*



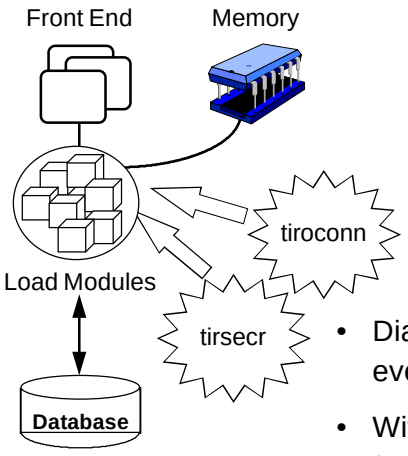
- Write EAB to issue Oracle query of userid currently connected
- Set work attribute to userid value returned
- No API call to Composer DLL

- Allows application-level security usingwork attribute userid and possible database permission table or file

Remote Presentation Mechanisms

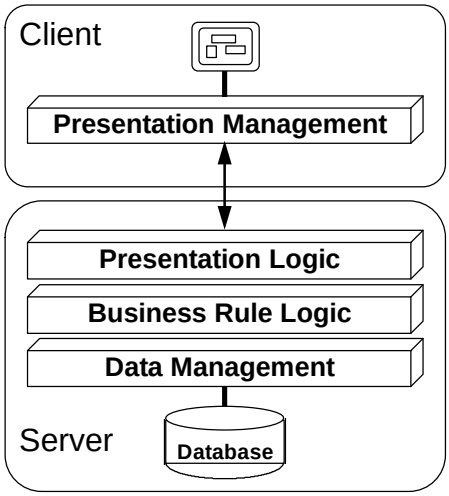


Load Module Security Exits

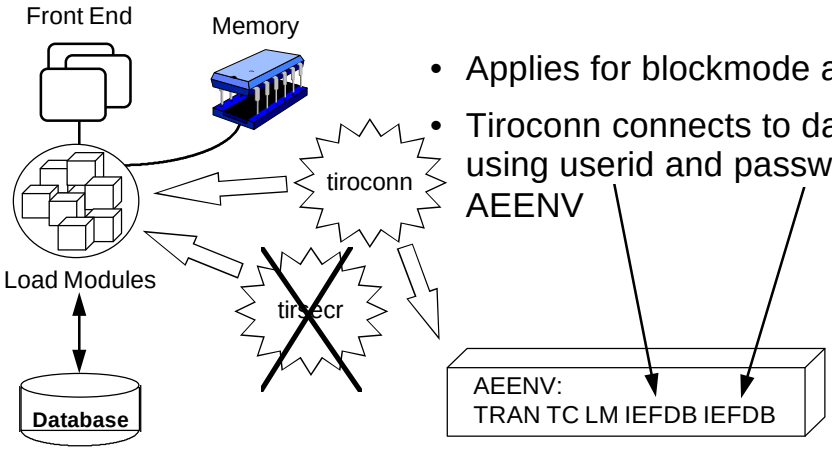


- Applies for blockmode and GUI
- Dialog/Window Manager calls tiroconn to perform database connect using userid/password stored in AEENV
- May be modified as desired
- Dialog Manager also calls tirsecr for every trancode request
- Without modification, tirsecr has no functionality

Remote Presentation Security Strategies

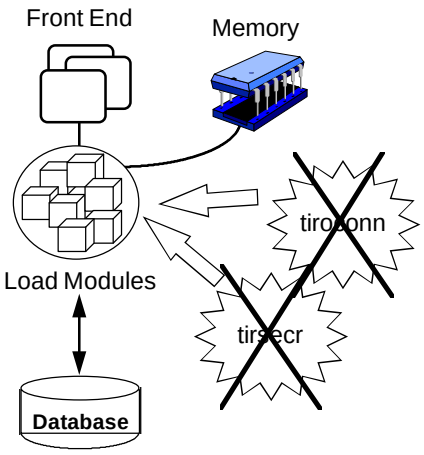


No Security Required



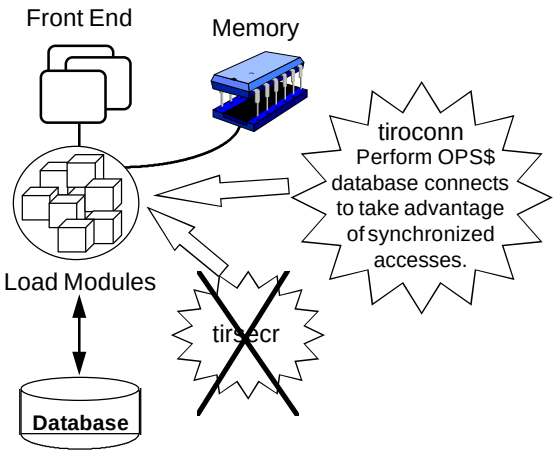
- Applies for blockmode and GUI
- Tiroconn connects to database using userid and password in AEENV

UNIX Authentication



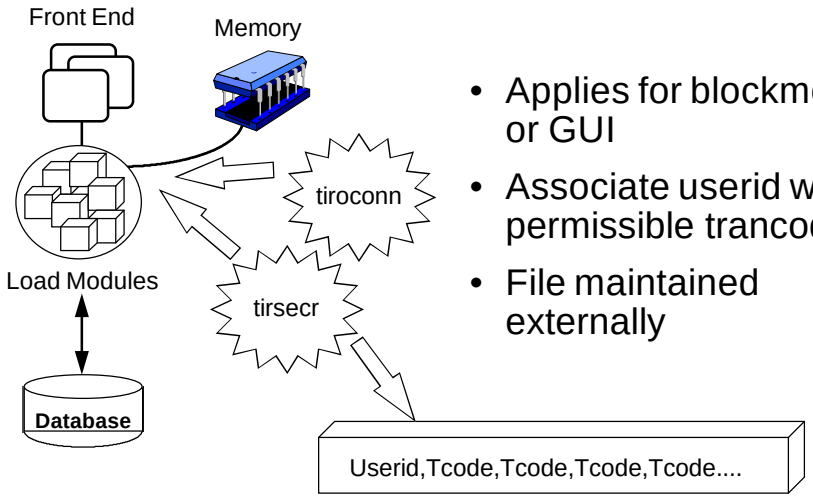
- Applies for blockmode or GUI
- UNIX authentication is automatic and external, via telnet into UNIX system
- UNIX userid present in special attribute USERID within application
- Valid UNIX userid enables application level security

OPS$ UNIX/Database Authentication



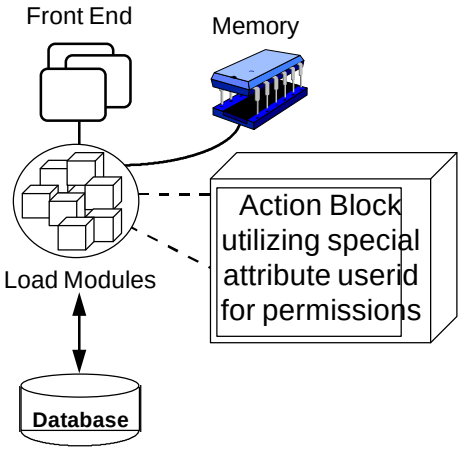
- Oracle-specific
- Uses UNIX account to access database
- AEENV file, connect data, and AEDB can be removed

Trancode-Level Security



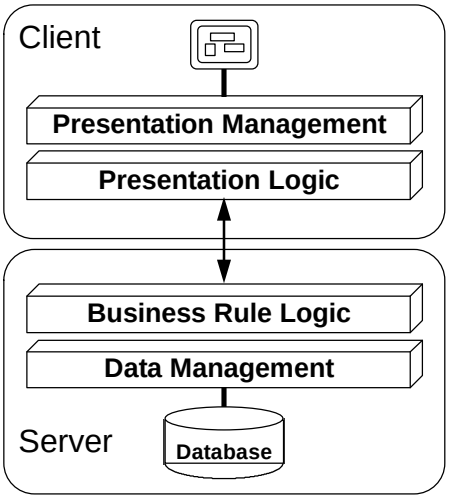
- Applies for blockmode or GUI
- Associate userid with permissible trancodes
- File maintained externally

Application-Level Security

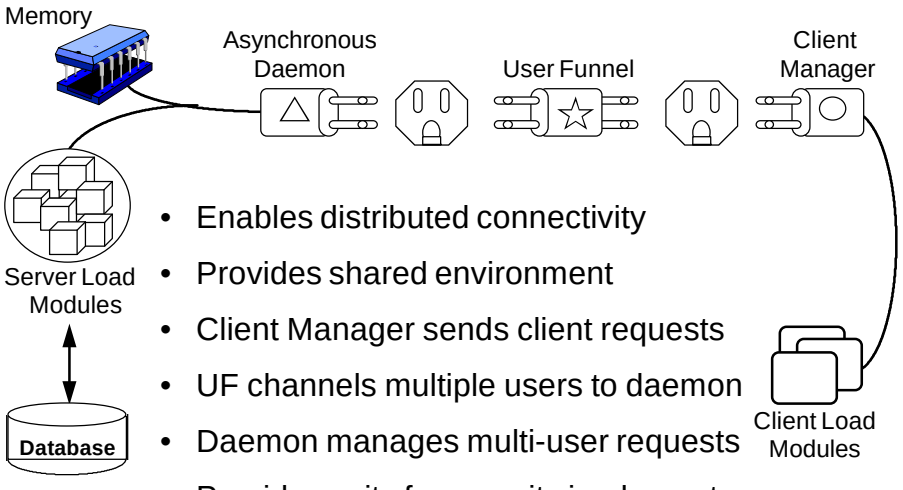


- Applies to blockmode or GUI
- Special attribute userid populated with UNIX account automatically
- Presence of userid implies correct password entered
- Validate userid with associated permission via database table or ASCII file

Distributed Process Mechanisms

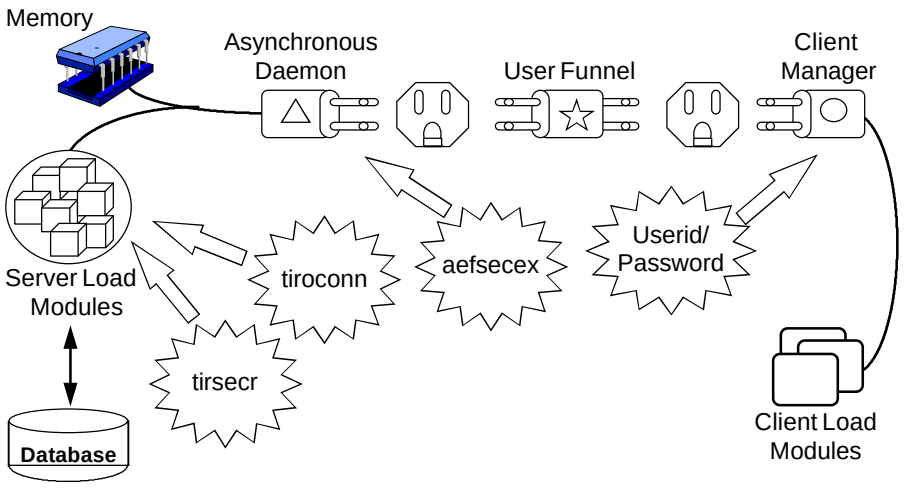


Transaction Enabler Defined

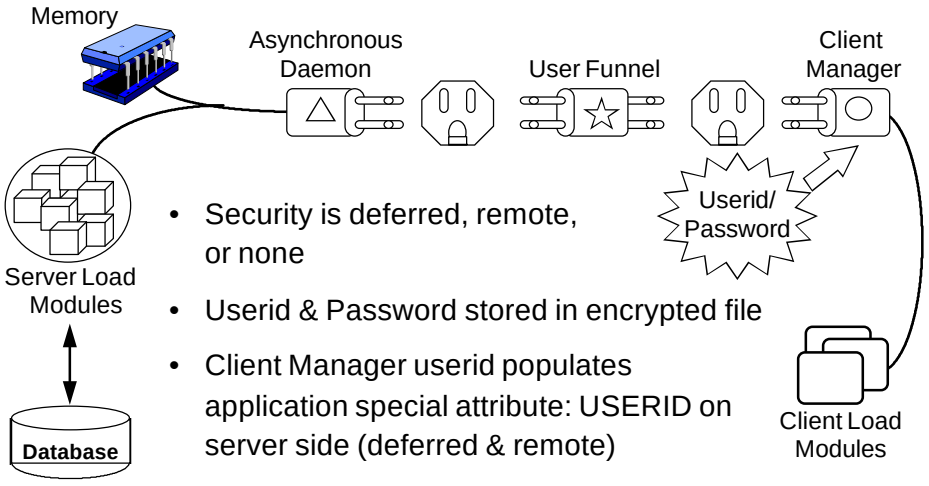


- Enables distributed connectivity
- Provides shared environment
- Client Manager sends client requests
- UF channels multiple users to daemon
- Daemon manages multi-user requests
- Provides exits for security implements

Distributed Processing Security

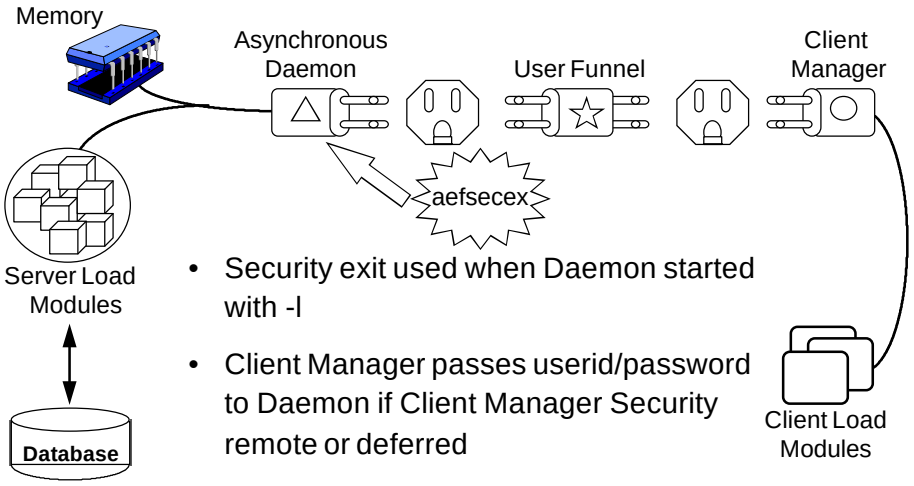


Client Manager Security



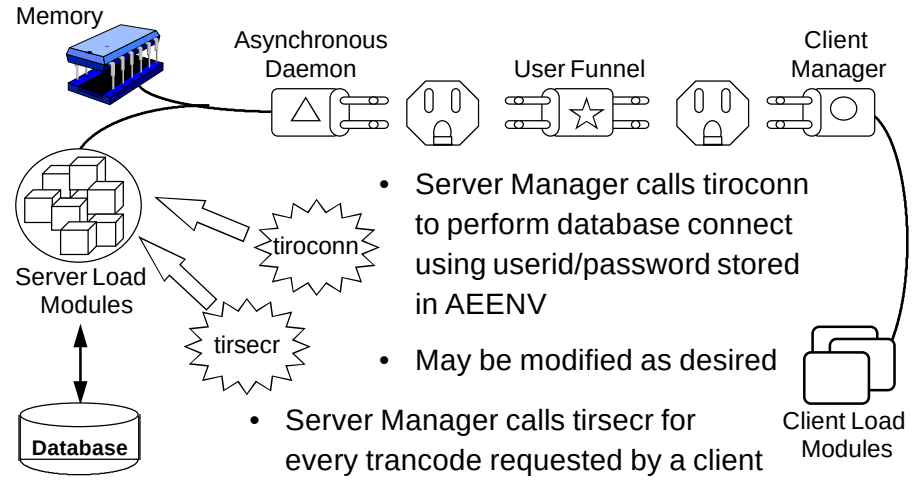
- Security is deferred, remote, or none
- Userid & Password stored in encrypted file
- Client Manager userid populates application special attribute: USERID on server side (deferred & remote)
- Designed for operating system authentication

Asynchronous Daemon Security



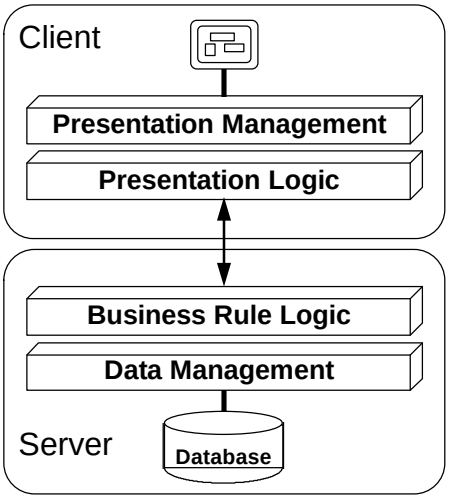
- Security exit used when Daemon started with -l
- Client Manager passes userid/password to Daemon if Client Manager Security remote or deferred
- Daemon validates userid against UNIX password file

Load Module Security Exits

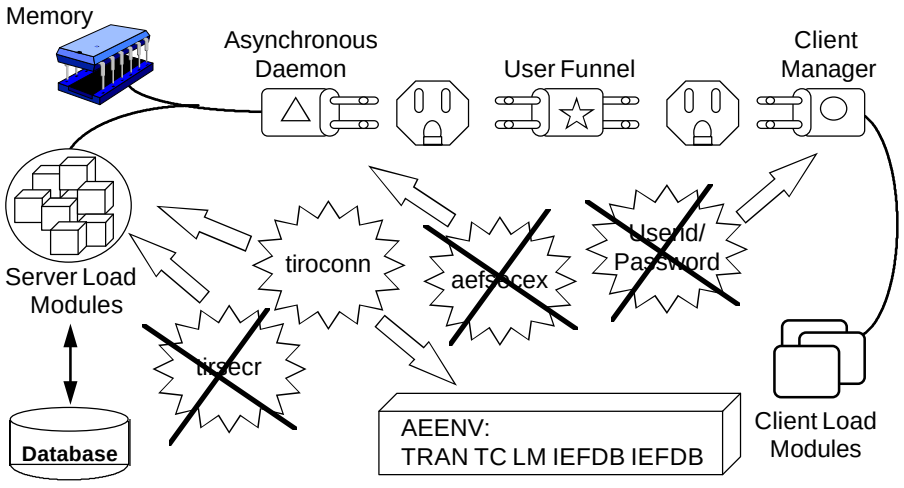


- Server Manager calls tiroconn to perform database connect using userid/password stored in AEENV
- May be modified as desired
- Server Manager calls tirsecr for every trancode requested by a client
- No functionality, without modification

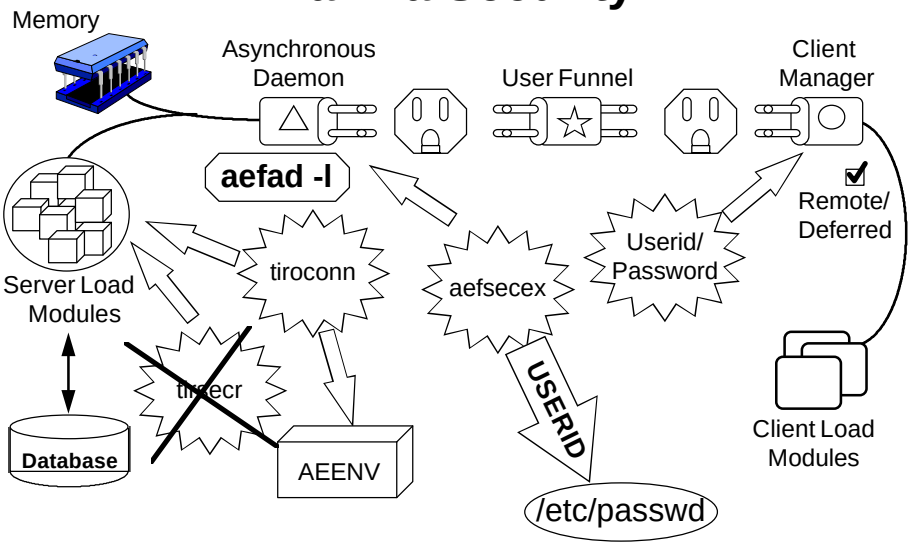
Distributed Process Security Strategies



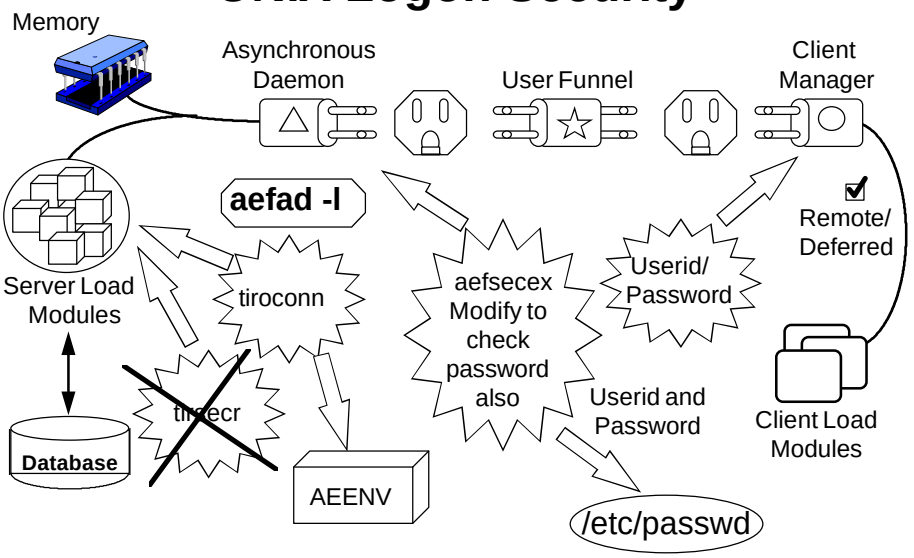
No Security Required



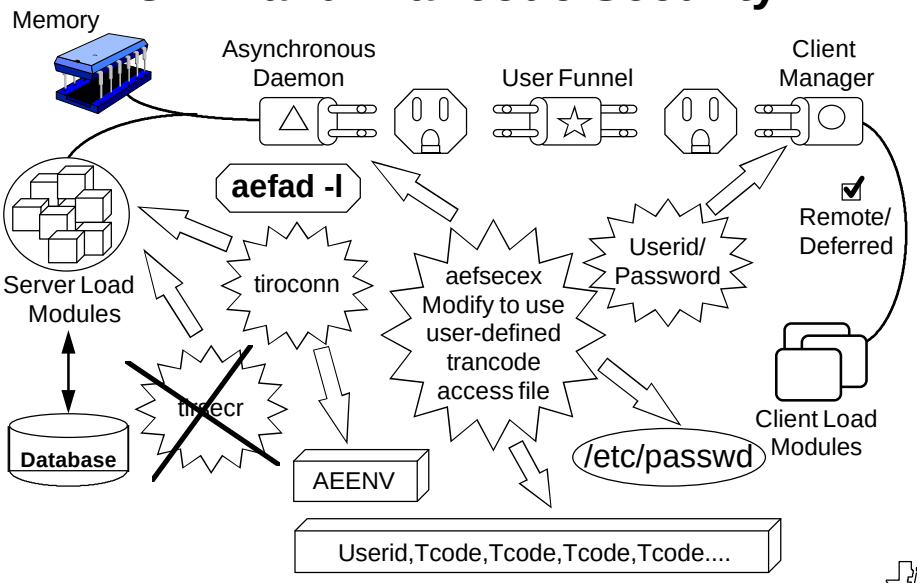
Vanilla Security



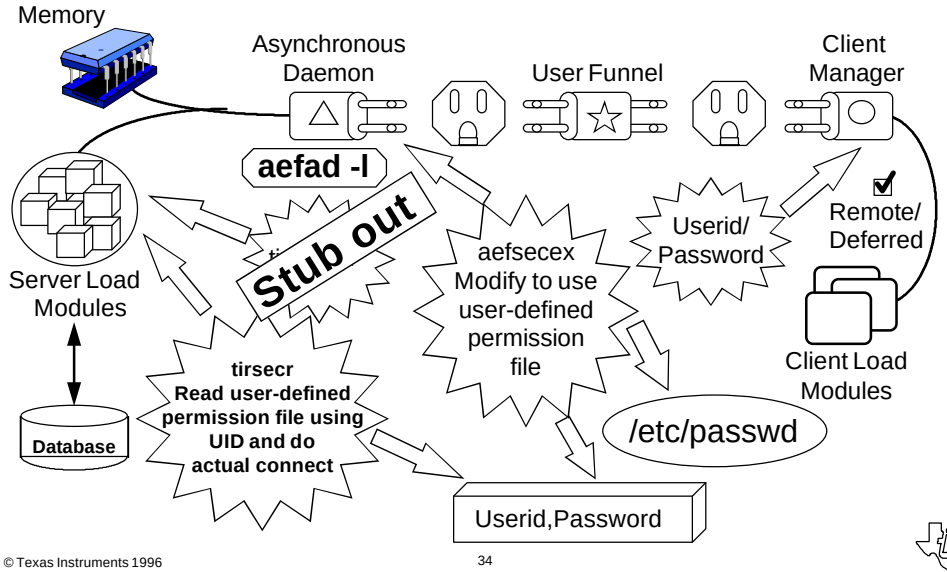
UNIX Logon Security



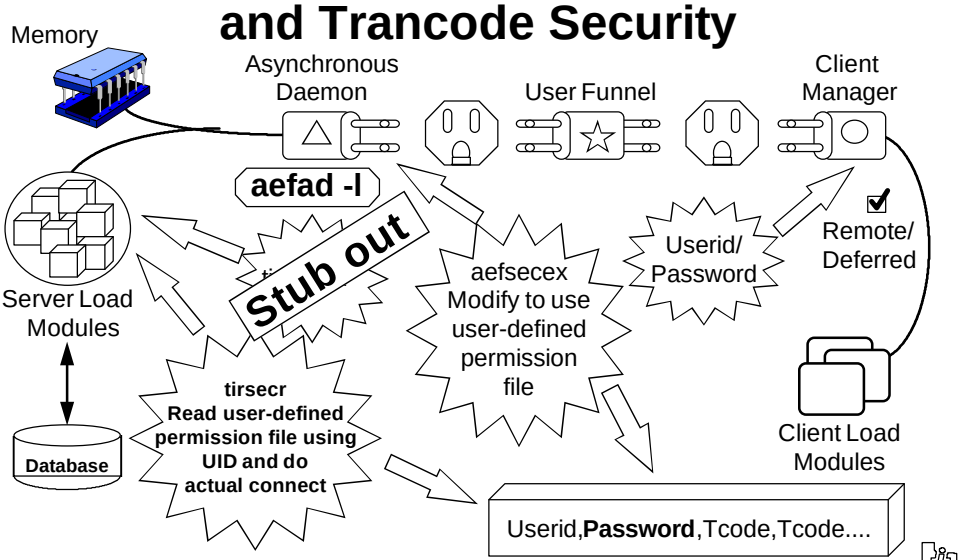
UNIX and Trancode Security



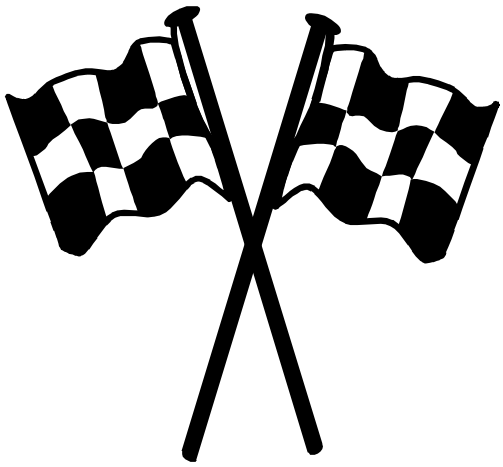
UNIX and Database Security



User Access, Database, and Trancode Security



Summary

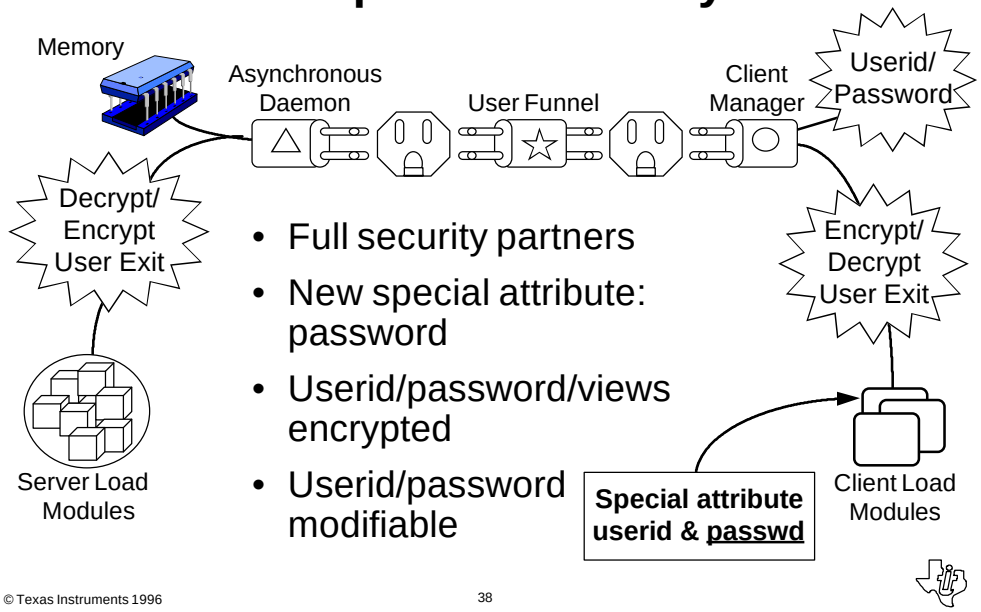


Security Support Anatomy

Security Component	Operating System Authentication	Database Authentication	Application Level Security
Client Manager	☑	☒	☒
AEFSECEX (Daemon)	☑	☒	☒
TIROCONN (SVR MGR)	☐	☑	☐
TIRSECR (SVR MGR)	☐	☒	☒
Global Logon	☐	☑	☐
WREXITW (WIN MGR)	☐	☐	☒
Client Application	☐	☐	☑
Server Application	☐	☐	☑

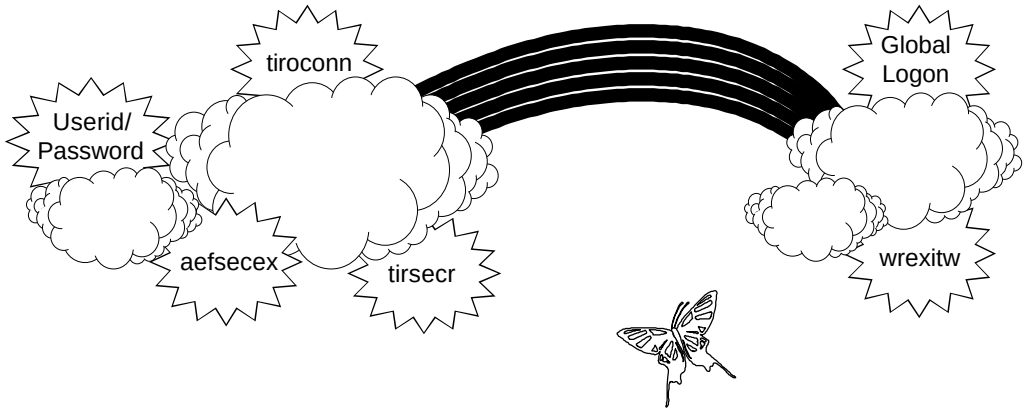
☑ = Default role ☒ = Modified role

Composer 4 Security



- Full security partners
- New special attribute: password
- Userid/password/views encrypted
- Userid/password modifiable

Choose Your Strategy...



Composer 3
Security Mechanisms Applied

Session 360

Mary Russell
Texas Instruments