


**Achieving Database Security Through  
Data Replication: The SINTRA  
Prototype**

Myong H. Kang, Judith N. Froscher, John  
McDermott, Oliver Costich, Rodney Peyton  
Information Technology Division  
Naval Research Laboratory


February 19, 2003                      Khandys A. Polite                      1



**Preview**

- ❖ **Multilevel Secure (MLS) Database Systems**
- ❖ **Secure INFORMATION Through Replicated Architecture (SINTRA)**
  - ❖ **Architecture**
  - ❖ **Security Model**


February 19, 2003                      Khandys A. Polite                      2



## Multilevel Secure (MLS) Database Systems (DBS)

- ❖ Contain data that has multiple levels of security
- ❖ Provides a form of access control that is an advantage over traditional DBSs
  - ❖ Mandatory Access Controls (MACs) vs. Discretionary Access Controls (DACs)
- ❖ Security attributes are used to label DB objects based on the sensitivity of the data being stored in that object
- ❖ Each user is given a range of labels (group of objects) to which they will be allowed access


February 19, 2003                      Khandys A. Polite                      3



## Multilevel Secure (MLS) Database Systems (DBS)

- ❖ Approaches recommended by The Multilevel Data Management Security Summer Study [Air83]:
  - ❖ Integrity lock
    - ❖ Uses a trusted front end, single untrusted back end DBS, and encryption techniques to protect data
    - ❖ Vulnerable to Trojan Horse attacks
  - ❖ Kernelized
    - ❖ Uses a trusted OS to enforce separation of data at different security levels
    - ❖ Uses several untrusted back end DBSs, one for each security level; untrusted back ends DBSs are controlled by security kernel that enforces a MAC policy
    - ❖ Security of this approach is as strong as the security of the trusted operating system


February 19, 2003                      Khandys A. Polite                      4



## Multilevel Secure (MLS) Database Systems (DBS)

- ❖ Approaches recommended by The Multilevel Data Management Security Summer Study [Air83], continued:
  - ❖ Distributed
    - ❖ Non-replicated
      - ❖ Each DBS has data belonging to a single security level
      - ❖ Uses a trusted front end and several untrusted back end DBSs
    - ❖ Replicated...
      - ❖ Used by SINTRA

February 19, 2003                      Khandys A. Polite                      5



## SINTRA

- ❖ Multilevel Trusted Database System based on a replicated data approach
  - ❖ Physical separation of classified data
  - ❖ Achievement of High Performance
    - ❖ All information that a user can rightfully access is stored in one location
  - ❖ Untrusted Backend DBS (UBD)
    - ❖ Contains information at a given class/level
    - ❖ Contains replicated information from all lower UBDs
  - ❖ Trusted Front End (TFE)
    - ❖ Controls user access to separate Untrusted Backend DBSs (UBD)
    - ❖ Role includes authenticating users, directing user queries to proper UDB, and maintaining data consistency among UDBs

February 19, 2003                      Khandys A. Polite                      6



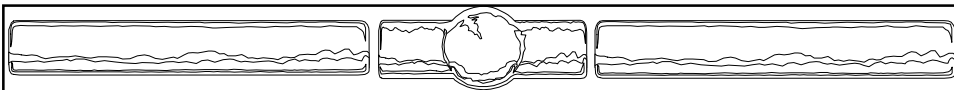
# SINTRA

- ❖ Uses many commercial DBSs
  - ❖ Advantages:
    - ❖ Easy testing and evaluation
    - ❖ Easy to connect
    - ❖ Easy to upgrade
    - ❖ Minimal development and maintenance costs
  - ❖ All in all – little new work is required to construct the MLS system known as SINTRA

February 19, 2003

Khandys A. Polite

7



# SINTRA

- ❖ Architecture
  - ❖ TFE - Honeywell XTS-200 system
    - ❖ A high assurance trusted OS
    - ❖ B3 rated system
  - ❖ UBD – Oracle 7
    - ❖ Untrusted database system
  - ❖ Network Interface - TFE and UDBs are connected through dedicated Ethernet connections
  - ❖ Custom processes
    - ❖ Query preprocessor
    - ❖ Global scheduler

February 19, 2003

Khandys A. Polite

8



# SINTRA

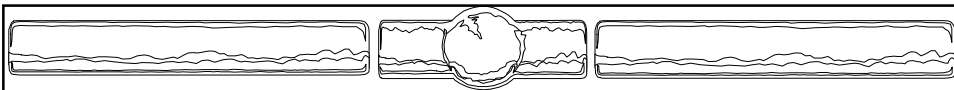
## ❖ Query Preprocessor

- ❖ Modifies user queries, if necessary
- ❖ Assists in the maintenance of data consistency among UBDs and data integrity
  - ❖ Ex. If a high-level user is allowed to modify low-level data located at the high-level UBD, then inconsistencies appear between high-level UBD and low-level UBD
  - ❖ Ex. Users might have read-only access to some data that is only modified by the system

February 19, 2003

Khandys A. Polite

9



# SINTRA

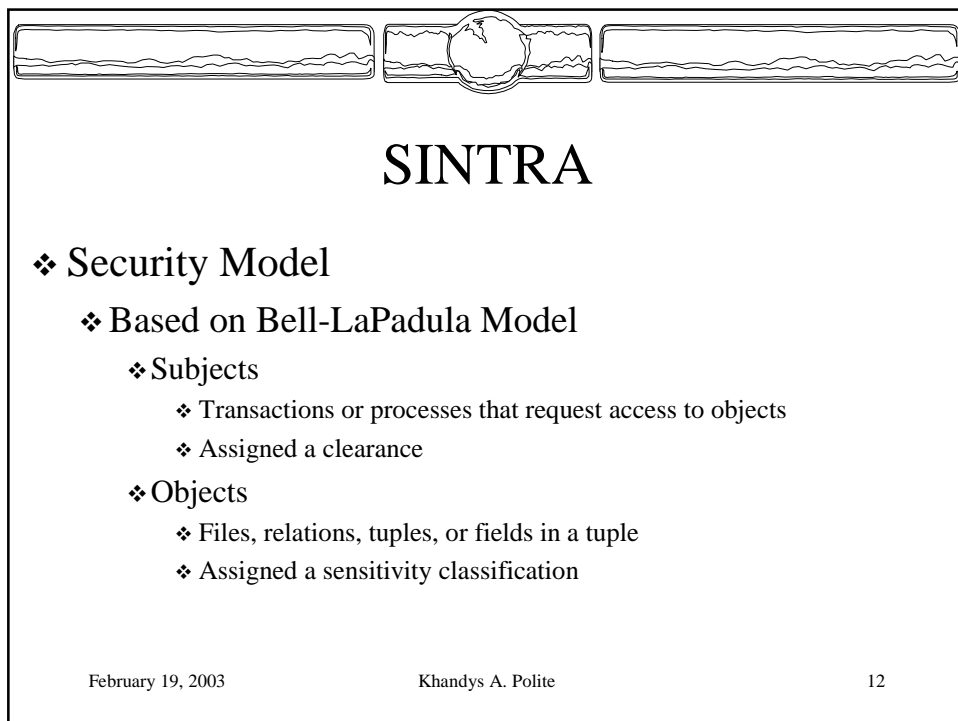
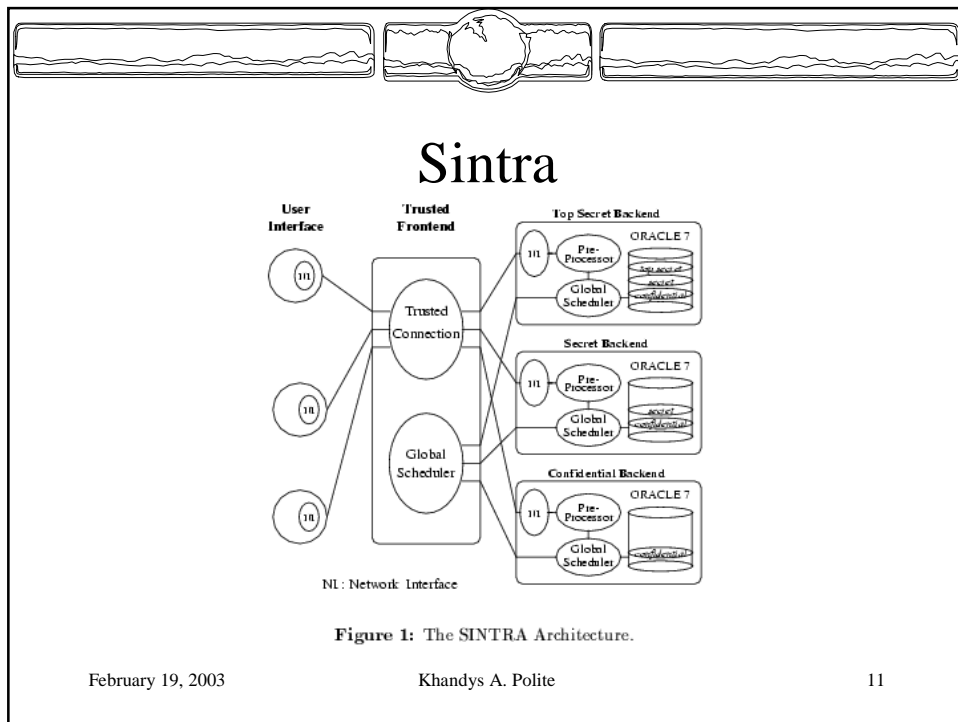
## ❖ Global and Local Schedulers

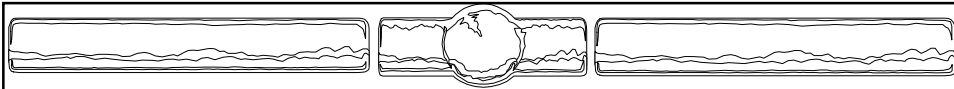
- ❖ Local – manages transactions and update projections at the UBD
- ❖ Global - Enforces data consistency among different security levels
  - ❖ Guarantees that the serialization order introduced by the local scheduler at the user's session level is maintained at the higher-level UBD

February 19, 2003

Khandys A. Polite

10





# SINTRA

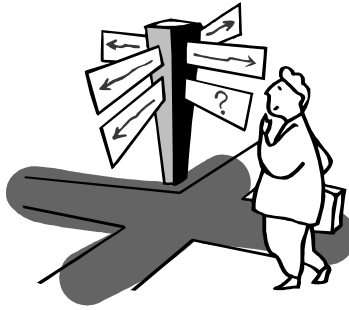
- ❖ Security Model, continued
  - ❖ Simple Security Property (ss-property)
    - ❖ Allows a transaction to read data if the security level of the transaction dominates the security level of the data
  - ❖ Restricted ★ - Property
    - ❖ Allows a transaction to write data if the security level of a transaction is the same as that of the data



# Review

- ❖ Multilevel Secure (MLS) Database Systems (DBS)
- ❖ Secure Information Through Replicated Architecture (SINTRA)
  - ❖ Architecture
    - ❖ Trusted Front End (TFE)
    - ❖ Untrusted Backend DBSs (UBD)
    - ❖ Network Interface
    - ❖ Query Preprocessor
    - ❖ Global and Local Schedulers
  - ❖ Security Model

# ?? Questions ??



February 19, 2003

Khandys A. Polite

15