Chip-Secured Data Access: Confidential Data on Untrusted Servers

L. Bouganim, P. Pucheral

University of Versailles
The need for Open Trusted Data Stores

• Virtual teams
  – distributed among space, time and organizations
  – collaborative work on confidential data
  – e.g., cyberworkers.com …

• Shared personal folders
  – accessible anywhere, anytime and shared by authorized persons
  – e.g., primadoc.com …

• Corporate DB hosted by a DSP
  – permanent access to travelling salesmen
  – e.g., caspio.com, quickbase.com …
Attackers

- **Intruder**
  - tries to attack the DB footprint or usurp the identity of a regular user (or DBA)

- **Insider**
  - tries to get information exceeding her own access rights

- **Administrator (SA or DBA)**
  - has enough privileges to tamper the access right definition and spy the DBMS behavior

---

*Access rights can be bypassed*

*Encryption is required*
Server-based approach

- DB footprint protected by encryption
  - Oracle Obfuscation toolkit, ...
- Restrict the DBA privileges, … as far as possible
  - Protegrity, [Ideas’01] …

\[\text{Weakness} = \text{decryption occurs on the server}\]
Client-based approach

• Decryption on the client
  – who owns the keys?

• Privacy (exclusive access)
  – the client manages the keys
  – efficiency is the main concern [Sigmod’02]

• Confidentiality (shared access)
  – a security mechanism is required on the client side to manage keys and access rights

Weakness = client can tamper the security mechanism
Chip-Secured Data Access (C-SDA)

- Making the security mechanism tamper-resistant
  - Access right manager hosted by a Secured Operating Environment (SOE) (e.g., a smartcard)
  - Access right defined on views
    - query translation in the SOE
    - part of query execution in the SOE
Equi-Predicate-Only Queries

X.com Privacy Policy: X.com does not rent, sell, or share personal information about its customers with other people or companies.

• Traveling salesman asks for customers living in France
• Equi-Predicate-Only query
  – 100% processed by the server
  – result decrypted by C-SDA
General Queries

X.com Privacy Policy: X.com vendors cannot access detailed information about customer’s orders, but can get statistic data about them.

- Traveling salesman asks for the total amount of orders passed by customer #22
- Aggregation must be computed on decrypted data by C-SDA

```sql
Select sum(amount) from orders where CustId = 22
```
Smartcard’s Characteristics

- Cheap and highly secured computer
  - Powerful RISC processor ($\approx 40$ Mips)
  - Limited communication bandwidth (10 to 100 Kbps)
  - Tiny RAM, writes in EEPROM stable storage very costly

- Impact on C-SDA
  - Internal processing must be done in pipeline
  - Processing must be pushed down to the server
  - Data flows must be minimized
Query decomposition

- \( Q = Q_{\text{term}} \circ Q_{\text{card}} \circ Q_{\text{server}} \)

Equi-Predicate-Only Queries

Inequi-predicates, aggregations ...

Presentation

SELECT C.Id, C.name, sum(O.amount) FROM Customers C, Orders O WHERE C.Id = O.CustId and O.date > 1996 GROUP BY C.Id, C.name HAVING count(*) >= 10 ORDER BY C.name
Query optimization: example

- Minimize the flow of irrelevant data traversing the card
- Inequi-predicates
  - evaluated by a subquery
  - result semi-joined with the initial table
Conclusion

• Other contributions exploiting smartcard’s storage
  – Insulate highly sensitive data
  – database depersonnalization
  – Multiple key repository

• Future works
  – Performance assessment
  – Experimentation in the EDI context
    • founded by the French ANVAR agency
    • extends C-SDA towards XML databases
  – impact of the SOE technology on query optimization