Database Security meets Mobile Requirements *

Astrid Lubinski
University of Rostock, Computer Science Dept., D-18051 Rostock
lubinski@informatik.uni-rostock.de

Abstract
Mobile work including mobile devices and wireless links comprehends a row of problems concerning security issues like availability, confidentiality, and accountability. Mobile processed information in database systems are distributed, heterogeneous, and replicated. They are endangered by various threats based on user's mobility and restricted mobile resources of portable devices and wireless links. Since mobile circumstances can be very dynamic, standard protection mechanisms do not work very well in such an environment. This paper presents various possibilities of an adaptation in order to dynamically adjust security belonging to changing contexts and to consider characteristics of the data. The purpose is achieving both, suitable protection and saving mobile resources.
Keywords
Mobile Database Security

1 Mobile Database Security

Mobile work using mobile devices and wireless links comprehends a row of problems concerning security issues like availability, confidentiality, integrity and accountability. These requirements occur for network components as well as database systems. Mobile work including mobile database access makes ubiquitous computing, anywhere and anytime possible. The mobility requires suitable hardware and software. Mobile devices like handhelds connected via wireless networks support mobile users, especially in connection with position searching tools. New risks and challenges for security and privacy occur in this environment. The goal is the protection of mobile users and their data.
Security measures must take into account the distribution of data and their heterogeneous handling regarding to security models. Scarce mobile resources make insecure communication necessary to replicate used data and increase the risk of restricting or dismissing security measures.

1.1 Mobile Conditions

Mobile work is context-sensitive work with contexts describing environmental characteristics and the relationships between them. In [Lubinski, 1998], the special problems of database systems in such a mobile environment are described more detailed. In this section, we summarize the main mobile circumstances causing various threats. Applications and required data are location dependent, but their access must be location transparent. Determined tasks are applicable on special whereabouts. The mobile infrastructure

*This work is part of the Mobile Visualization Project (MoVi) and has been supported by the German Research Association under contract Schu 887/3-2

restricts the available volume and type of data and the data transfer. Context information comprehends further which people and objects in the environment stay. Supporting mobile work involves providing access to interesting data at the appropriate location, time and device, i.e. where and when the data are used based on user aims, preferences, knowledge and skills.
For this purpose we require different information regarding the current infrastructure, available mobile resources, connectivity, costs and duration of connections, and bandwidths. Mobile work is characterized by infrequent and temporary short connections to the fixed network (low connectivity) and by a variety of access types (register and query data). The mobile user accesses data that are also accessed by other users or itself on different locations and devices, respectively. The mobile context includes mobile work and communication attending metadata to support users. This meta-information is covered in four parts of the *mobile context*:

- human factors, their tasks, roles, other persons
- location (and changing location in time),
- hard- and software (mobile site and network characteristics, equipment and tools)
- information, application characteristics (like type, size)

These mobile circumstances, and especially their dynamics, and restrictions like frequent disconnections make a mobile work with database systems difficult. This is the reason for various difficulties in securing mobile work and for requiring a new viewpoint to well known security measures, or demand new ones.

1.2 Protection Objects and Actions

Assuming distributed and/or replicated databases, we must take into account protection of the main action types *management*, *accesses* and *transfer* to protection objects *data* and *metadata*.
Metadata are used on different levels. Database systems manage object types, keys, and integrity rules. Transfer components need at least receiver and sender addresses of messages. Metadata include necessarily mobile context data and security relevant information like security policies. Data and metadata are the items which must be protected, whereas metadata are additionally used for their protection. Combining possible actions with protection items gets the following table. The first row and column shows the possible items and actions to be protected and characterize them in a short manner. The body of the table illustrates the special problems, threats or desired security characteristics, respectively, for the particular combinations of actions and items appearing in the special mobile environments. E.g., the distribution and heterogeneity leads to typical distributed security problems including data exchange between systems with differing models and aims. Moreover, mobile systems are characterized by very mobile hardware. The thread of lost confidence by loss of devices is often underrated. Wireless links are predestinated to be eavesdropped on. Profiles of communicating users are simply creatable. Attacks and security for mobile communication are described in [Federrath, 1999]. We focus in this paper database related mobile security issues and ignore communication security. Our approach consists in three main tasks to keep mobile work secure (see also [Lubinski, 1998]), the restriction of database transparencies, a horizontal and vertical separation of metadata and an adaptation of security.

Item *Action*	*Data* in mobile used database systems are distributed, heterogeneous, replicated	*Metadata* are DBMS metadata, mobile (dynamic) context, communication context, security relevant information
management, access: restricted resources and resource disproportions	lost devices, need for isolated computing, restricted security	different trust levels (objectives, security models, etc.), patterns of user movements by location dependencies
transfer: infrequent and short connections, air interface	inconsistencies, masquerade, eavesdropping	anonymity against various parties, reachability management, context and especially user management, traffic analysis

Table 1: Security Requirements in Mobile Environments

- restrict transparencies:
  Database transparencies like distribution and replication transparency is soften to allow user's participation. This requirement concerns transparent security management and control, too. However, every transparency must be remain controlled by the system to avoid insecure system states.

- separate metadata:
  Because of the opportunity to misuse context information, a useful protection lies in separation or anonymization of it. The sensitive aggregation of user identifying data and other contexts must be avoided. A powerful access control realize this type of separation. Separated physical context management improves the access control.
  We distinguish two kinds of data separation, vertical and horizontal. The accessed and as a rule location dependent data gives information to the whereabout of users. Vertical separation supports confidentiality requirements by protecting users from tracing their movement. It allows only a view to a (role dependent) section or a facet of mobility patterns and behavior. Additionally, audit data should be anonymized or pseudonymized.
  Horizontal separation represents a layered view and constitutes a prevention of undesired information flow between different system layers outside the controlled area. Inner-database-communication has to be unobservable by intruders (encrypted) as well as by underlying services.

- adapt security:
  There are a few papers which focus security in heterogeneous database systems meeting requirements of integration and access to data of various policies. But the essential criterion in mobile environments is their dynamics due to possibly very dynamic mobile contexts. A flexible adaptation to the changing environment characteristics decides about suitable choice of applicable security mechanisms. We enforce a resource aware approach but assure a minimal security.

A flexible adaptation is a very new approach. In the following section, we explain an architecture meeting this requirements and their resource dependencies. In section 3, we

outline related work and section 4 concludes the paper.

2 Security Adaptation

We now describe accesses mediated by a mediating adaptation and discuss its connectivity and resource related application. We assume a simplified *mobile scenario*: There is a mobile site communicating with fixed hosts via a wireless link. Both sites access data on each site.

2.1 Access Mediation

The way to perform adaptation requires any additional functionality between usual mobile and fixed functionality. Such a middleware component fulfills the following tasks outlined in [Lubinski, 1998]: model adaptation, enforcing stand alone computing, resource related adaptation, maintaining minimal and obligatory security.
The *Adaptation Component (AC)* mediates all accesses and manages security relevant context modifications.
It mediates every access from one to another site. It decides about accomplishing of accesses and activation of security measures and triggers system components. Figure 1 shows a mobile site communicating with a fixed site mediated by an Adaptation Component. We assume that a communication contains in the one direction database accesses to data (like queries) and metadata (including security relevant metadata) and in the opposite direction the accessed metadata or data, respectively.
The adaptation results in an adjusted access or query result, respectively, or in a repu-

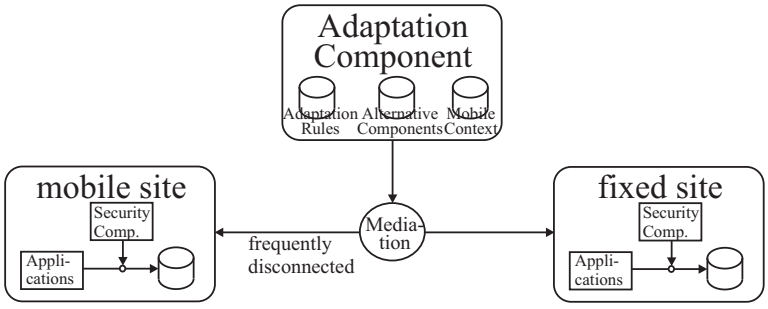

Figure 1: Access Mediation by an Adaptation Component

diation of the aspired access. This serves a security for both sides. The AC gives security guarantees for the accessing and the accessed site. No data will be transferred into an unprotected area and the accessing site does not get insecure data and applications.
Furthermore the AC manages disconnections, supports local security components to handle disconnections and enforces disconnections in order to enable stand alone computing. This type of computing is necessary in case of processing very sensitive data. An existing connection will be cut in order to avoid current security threats or to enforce undisturbed processing. The user as well as the adaptation component can initiate a network partitioning.
We argue that the component itself must be distributed (this is discussed later). Moreover, the tasks of this component require communication and cooperation with under-

lying layers like the operating system and network layer. Mobile links are often disconnected because of failures or explicit disconnections to save monetary costs. Information about disconnections/connections are helpful to foresee and respond to them. We developed replication strategies based on different connection states (see [Heuer and Lubinski, 2000]) and use the basic information for connectivity related security, too.

2.2 Connectivity Related Adaptation

There are the following states of mobile sites and connections:

- mobile site (including the link connection) is switched off:
  No access to and from another site is possible. Disadvantages are similar to a disconnection (see next points), but stand alone computing is not possible to realize.

- mobile site is going to switch off or on:
  It can be useful to inform other participants of the distributed environment about these steps. Following accesses are only possible after the next switch-on and reregister. The latter mode requires user identification and authentication.

- mobile site is switched on:
  We distinguish four possible combinations of this state with connectivity modes. The link is

  - disconnected (d):
    No access from and to outside a mobile site is possible. This state reduces threats and facilitates access control. There are a few security measures not necessary to be activated, only one rule subset will be applied. That is, the system changes from a multi-user system to a stand alone system permitting only one user to perform accesses. According to the small available resources, resource saving reduction of functionality is possible. We will explain it later. Beside other database aspects, a disadvantage of a disconnection consists of occurring inconsistencies of replicated authorization. Assuming an optimistic replication protocol, modifications are stored in a log-file to reintegrate them after a reconnection. Replication problems in mobile environments are considered in [Heuer and Lubinski, 2000] and [Samarati et al., 1996] dealt with replication strategies especially for authorization.
  - connected (c):
    Despite of the disconnected case, the connected state needs full access control. Data transfers have to be handled securely. The AC is working for mediation.
  - c-d- and d-c- transition:
    Changing the state between the connected and the disconnected mode is interesting to influence mobile systems. The transition to the disconnected mode is usable to prepare a disconnected work. This phase is used to inform other participants about the imminent disconnection and allows a reduction of active security measures to save mobile resources and answer time. In the opposite transition phase a disconnection is subsequently treated. It includes the reintegration of log files, a reregistration, and an activation of all functionality necessary in the connected state. Transitions are related to the changing context. Therefore the AC applies to invoke transition actions. Tasks of the AC are shown in the following description.

2.3 Flexible Adaptation

The AC has two main tasks: It

- mediates accesses,
- handles modifications of the mobile environment (like connectivity).

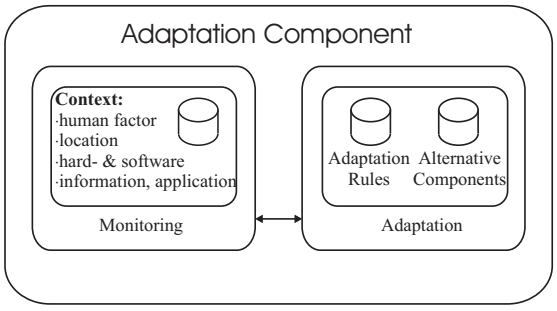

Figure 2: Adaptation Component

Figure 2 illustrates both task. A mediation includes an adaptation which results in forwarding the adapted access or in rejecting it. The adaptation process applies a set of adaptation rules. Alternative components or modules are not necessarily used. An access or query result can be changed suitable to the current policy on the base of modification rules. By this means, an access is adapted to any model and to any integration in same models of a distributed and replicated database system. The AC is used as a global component or employs piggy-back transferred security data. The first approach assumes a global management of security policies and rules of the distributed database systems, the last one integrates accesses from and to autonomously processing database systems which delivers relevant information piggy-back with queries or query results.
The AC just works without an access. It replies to modifications of the mobile environment. Therefore the AC contains additionally to the adaptation a monitoring function. The AC invokes an adaptation if it observes a relevant context modification. Components are replaced by alternative functions or functions are activated or deactivated. A replacement is made if the communicating database systems are changing and another security policy is applied. In this scenario, the AC acts like a global access control layer in federated database systems. Each database system has its own coupling module in order to map access rights. Decisions about adaptation or rejection made by the AC facilitates user's tasks.
Another effect of access independent work is an application dependent enforcing of a disconnection. This measure is necessary to avoid an inadequate data transfer, if required data and available resources are in an evident contradiction. Moreover, disconnections support a stand alone computing.
A third adaptation of this type reduces or extends activated functions to adjust functions accordingly to the available mobile resources. Security is often an additional, not integrated feature. Even in environments of restricted resources, it is obvious to sacrifice security to other functionality. To avoid user or system driven suppressing of security measures, we have introduced different layers of security needs.

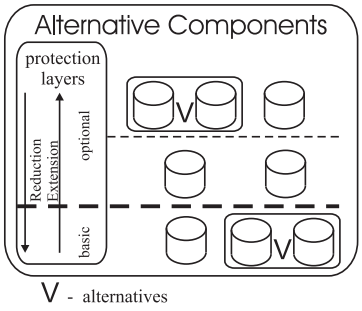

Figure 3: Alternative Components

2.4 Resource Restricted Security

The data pools in the figure above represent security measures or sets of access control rules. They realize different protection layers, i.e. more or less strong protection, possibly per item. Users select a desired degree of protection. Decreasing the protection layer includes deactivating functionality or exchange by resource saving components and effects reduced power assumption, storage needs and answer times. This is possible because of adaptation of database functionality to the mobile context. Reduced database functionality makes a reduction of security measures possible.
But there is a set of measures which are not reducible and users and applications can not deactivate it, because it builds a minimal protection base. It is necessary to realize a set of security measures not restrictable by users or in case of system failures like frequent power failures. That is, resource restrictions of the mobile environment must not influence protection purposes.

2.5 Distribution of the AC

An access of any type is initiated by a subject and effects an object. Each access includes a special action type. It is not interesting for our purposes if the access follows an explicit or an implicit access right.
We say on the one hand that the AC is a mediating component between two communicating sites, on the other hand it is responsible to observe changing contexts. There are different possibilities to assign the AC to the sites effecting advantages and disadvantages.

- *middleware component.* Assigning the AC to a separate middleware component requires distributed AC's over the whole network. This is easy to realize if we use the base stations of radio cells. Every communication containing accesses and query results are transferred via these base stations. But this solution assumes a big confidence in these components, which are neither the owner of the data nor the receiver of the aspired data. A trust center is needed to authorize AC's for their work. AC's are always strange and sources of threats and security attacks.

- *accessing site.* An assignment to the access-initiating site serves a control by the site itself. It requires knowledge about the accessed and maybe unknown site. Hence, an access is two-stage. After getting necessary metadata, an access can be initiated. This process increases communication costs (time and monetary costs).

- *accessed site.* In this type of assignment, resources of the accessed site are consumed for mediation. This is not desired if the mediation is expensive and processed on a mobile site.

Depending on current purposes, it is necessary to find a compromise for a suitable distribution of the AC functionality.

3 Related Work

Mobile information systems are distributed systems, therefore security requirements are referred to all of the problems of distributed database systems like federated security policies and using wrappers in order to mediate accesses to distributed data with or without the help of trusted third parties, or encrypted transfer of remote accessed data.There are various approaches in this field of research, e.g., [Jonscher and Dittrich, 1996] presented detailed a fundamental approach for configurable access control for federated DBS. ARGOS is able to coordinate various local authorizations and to serve different access control policies on the global layer. [Gudes and Olivier, 1998] discussed accesses in an environment of replicated information in autonomous systems. The authors addressed the problem of handling conflicting local and global authorization rules in federated database systems, but don't consider differing security policies. While in [Gudes and Olivier, 1998] autonomous authorization of replicas is described, in [Samarati et al., 1996] optimistic handling of replicated authorizations is discussed.
Mobile communication security with requirements like unobservability, accountability, and anonymity are described in [Federrath, 1999] with the focus on privacy requirements in the location management.

4 Conclusion

Based on a previous paper [Lubinski, 1998] which described requirements in mobile database security, we proposed opportunities to make a user's participation possible, to protect appearing metadata to avoid mobility patterns, and to adapt security measures to mobile requirements. We subsequently extended the adaptation and suggested a framework meeting the requirements with the help of a mediating component (AC). We looked at the mediation tasks of such a component and shows how to select a suitable adaptation for the current mobile environment. The selection is working depending on the possibly restricted mobile resources, and on the current connectivity. We considered handling of dynamic changes in the mobile context. We observed that restricted resources can suppress security measures and therefore we introduced an obligatory basic security layer which is nor reducible, but extendable to more restrictive layers. Each layer includes alternative security components differing in power consumption.
Our approach using the Adaptation Component serves an adaptation of security and especially confidentiality requirements of data in a mobile environment with the help of middleware functionality. We assumed a distribution of this component. Access mediation is a topic of several research groups whereas alternative protection components and resource - driven adaptation is a new approach.

References

[Federrath, 1999] Federrath, H. (1999). *Sicherheit mobiler Kommunikation*. Vieweg, Wiesbaden.

[Gudes and Olivier, 1998] Gudes, E. and Olivier, M. (1998). Security in replicated and autonomous databases. In *Proc. of the IFIP WG 11.3 Twelfth Int. Conf. on Database Security*.

[Heuer and Lubinski, 2000] Heuer, A. and Lubinski, A. (2000). Configured replication for mobile applications. In *Proc. of the BalticDB&IS'2000*.

[Jonscher and Dittrich, 1996] Jonscher, D. and Dittrich, K. (1996). Argos - a configurable access control system for interoperable environments. In Spooner, D., Demurjian, S., and Dobson, J., editors, *Database Security IX: Status and Prospects*.

[Lubinski, 1998] Lubinski, A. (1998). Security issues in mobile database access. In *Proc. of the IFIP WG 11.3 Twelfth Int. Conf. on Database Security*.

[Samarati et al., 1996] Samarati, P., Ammann, P., and Jajodia, S. (1996). Maintaining replicated authorizations in distributed database systems. *Data & Knowledge Engineering*, (18):55–84.