14 SECURITY ISSUES IN MOBILE DATABASE ACCESS

Astrid Lubinski

Abstract: Mobile computing and communication is a rapidly developing area. But mobility is associated with problems for security and privacy beyond those in open networks. A well known threat is tracking user movements. New risks are caused by the mobility of users, the portability of computers, and wireless links which include dynamics, resource dependencies and additional information to ensure the communication. This paper surveys the new challenges and the research on security issues in mobile data management, access and transfer. We investigate the issues concerning database specific security which have to be reconsidered. We will identify a basic characteristic of these security issues, adaptability, to answer the dynamics.

14.1 INTRODUCTION

The development of mobile devices make new applications conceivable through ubiquitous computing. For example, mobile work "on-the-spot" like disaster recovery and maintenance tasks as well as business trips are possible. Mobile computing and communication start up to be an important factor in business. On the one hand we have really inspiring possibilities, but on the other hand, security and privacy becomes more eminent with wireless computing and communication. Dynamics of the mobile environment is confronted with static security services, often scarce resources hinder the correct application of security mechanisms, and additionally managed information needs particular protection. Moreover, it is obvious that there is a chance to integrate security and privacy issues in an early design phase of this new kind of computing.

S. Jajodia (ed.), *Database Security XII*

14.1.1 Mobility

In the first place, we have to explain our interpretation of mobility. While it is beyond the scope of this paper to present mobile agents, we focus on user and terminal mobility. In the case of terminal mobility a user is identifiable through his mobile terminal [10]. User mobility keeps users in the foreground. The customers roaming to pursue their aims are mobile with respect to their environments, to their locations, other persons, and terminals. They are not fixed to use one and the same device and sort of link. Every arrangement of terminal kinds (fixed or portable) and networks (wired or wireless) is conceivable (see figure 14.1). The user can for example use a laptop with a fixed network in a hotel or the same mobile device in a radio network environment. To manage user mobility, detailed information of the current computing and communication environment is necessary besides the user location information. The protection comprises safeguard of content data and the described environment data.

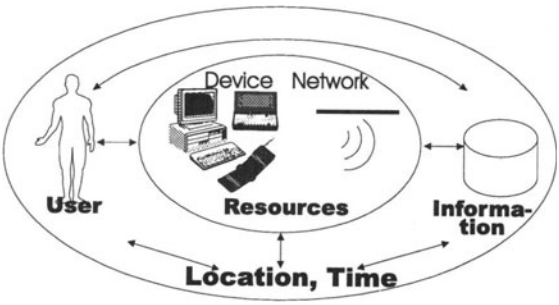

Figure 14.1 General Mobile Scenario

14.1.2 Mobile Databases

We assume a distribution of the database content over the whole network, e.g. there is no central database on a fixed host which will be accessed from fixed and mobile hosts, but a distribution (or replication) of fragments over both mobile and fixed hosts.
We will organize this paper according to groups of the security issues. One possible grouping contains the consideration of security goals and associated threats. The basic objectives are confidentiality, integrity and availability including accountability and non-repudiation. Main threats are information leakage, integrity violation, denial of services, illegitimate use, and unaccountability. Such a classification seems to be too general because most of security problems are confidentiality related. [3] focuses on communication problems and proposes a grouping into

- content privacy,
- unlinkability of sender and recipient and

- location privacy.

In [7] a framework of the categories of

- mobility,
- disconnection,
- data access mode and
- scale of operation

is used.

We introduce in this paper a more database-related approach to mobile security. We ask what are the objects which have to be protected, and in which situations. Even in mobile environments, there are risks

- for the information itself and
- for the metadata.

The metadata concern in the mobile environment in particular the additional data accompanying the communication (also: telemetadata [16] or communication context) which are personal data and have to be protected. The safeguard should effect the data

- management and access and
- transfer.

We distinguish between actions on the mobile and the fixed site.
In the next chapter we will survey the security threats for data and metadata in the data transfer (communication) over a wireless link. Most of them are problems of the underlying operating system and network layer. Also the following chapter about security issues contains the rather database-related security issues, e.g. data and metadata protection in the management and access operations and we will specify the dangerous situations in such an environment. Afterwards we show the necessary preconditions and protection approaches like contradiction between transparencies, different levels of anonymity and separation of metadata. The conclusion closes this paper with some resulting remarks.

14.2 SECURITY ISSUES IN MOBILE DATABASE ENVIRONMENTS

14.2.1 Data Security in Mobile Data Transfer

Disconnections occur often in wireless communication. They can be forced by the user because of saving communication costs or be induced by faults. This situation can endanger the data consistency, even without considering replicas. Disconnections are primarily a problem of the underlying layers of a database, but the database system is also responsible for avoiding data loss in case of such

unexpected disconnections with the help of transaction recovery. The higher frequency of network partitioning requires a more powerful error recovery than in fixed networks. Besides error recovery, this situation offers attackers the possibility to masquerade as either the mobile unit or the base station. With the help of masking the identity, data are at risk to be released improperly. Moreover, the use of a wireless link facilitates eavesdropping, because air-emitted information is accessible in a simple way without any additional effort required. This kind of security violation is hard to detect. In both cases, security relies on cryptography to achieve user authentication and data privacy. Mobile users are registered their real identity or with a pseudonym with that domain's authentication server. The authentication service should provide to the communicating parties the confidence that they are in fact communicating with each other [8, 12]. The subsequent communication should protect the data transfer content against attacks and eavesdropping. Authentication in mobile environments is e.g. described in [6, 13, 17, 18]. Most of the authors propose to use asymmetric encryption for the authentication and symmetric cryptography for a secure communication. It is essential, that also inner-database communication between distributed fragments has to be realized securely.

14.2.2 Metadata Security in Mobile Data Transfer

We named the metadata in a mobile communication area (see figure 14.1) the *mobile context.* It consists of a user profile, information about the current resource situation, information characteristics, location and time. The current whereabouts and especially the movement of users are a matter of privacy, and ideally only the user herself should have knowledge about these data [7, 17]. Its protection is regarded as the main special mobile security aim. The threat of keeping user whereabouts appears on different layers. On the network layer, user location or presence in a particular radio cell, respectively, is managed in order to reach a mobile user to communicate with him. All user identification information including message origin and destination have to be protected with the help of cryptography to conceal a communication from other network users. In order to achieve anonymous communication, aliases or pseudonyms are used. Furthermore the identity of users should be kept secret against the service provider, even if they consume services which have to be paid. It is not necessary to know the identity of users to get solvency information from their home base node. The home site is informed about the aliases and the real identity. Safeguarding of anonymity additionally against the home base node requires a trusted third party to manage the pseudonyms.
An implicit method to disclose the location lies in the possibility to carry out a traffic analysis. Prevention against traceability of network connections in mobile environments can be offered through either MIXes [2, 14] or the Non-Disclosure-Method [5]. Both methods use cryptography. MIXes delay and collect different messages and send it in a shuffled sequence to the receivers or another MIX. Using MIXes requires only a modification of the available networks, but a sufficient amount of messages with equal length is necessary,

otherwise dummy traffic will be created.
In the Non-Disclosure-Method, introduction of Security Agents (SA) is proposed. The communication path is masked through a sender selected route (with detours) over a number of different SA's. Each SA only knows his predecessor and successor in the routing chain. Security increases in case of widely scattered SA's, possibly among different providers. But the detours assume an intact and wired network. In case of database requests, MIXes and detours extend the response time in a dynamic way and hinder an efficient optimization.
Another aspect of wireless communication security, the permanent reachability of persons, endangers the user's claim of self-determined communication. In [15], an implemented approach for personal reachability management is proposed. The main idea is to evaluate and negotiate a communication request and to decide automatically by a Reachability Management System whether a personal contact is made or not, to allow chosen calls or avoid disturbances. The connection with the called subscriber will only be established on certain situations, namely if the negotiated communication context has fulfilled certain conditions, which can contain information for example about communication partners and the urgency of requests. This aspect increases the problem of keeping data consistency in often partitioned mobile networks.
While a user crosses cell boundaries, his information - the telemetadata - like location and user profile will be transferred and replicated to the adjacent Base Stations. That way, risks for the very sensitive personal data are increased due to "the multiplication of the points of attack" [7] and the possibly different trust levels afforded by each node. The difficulties will be stronger with respect to different security models.

14.2.3 Data Security in Mobile Database Management and Access

The effects of disconnections as a special resource condition are described above. An often neglected aspect in mobile communication contains the loss of mobile units. They are more likely to get lost than fixed hosts and the consequences are lost data and confidentiality. The only means to prevent loss of confidentiality is the usage of encryption and powerful identification, authentication and access control mechanisms. These are no specific challenges to mobile computing. Just mobile devices are provided only with a very simple protection.
In particular situations, isolated computing without communication and its range of security threats is necessary. But scarce resources like small storage or power capacity could prevent such a computing situation. In addition, scarce resources may cause faulty situations. The system may not be able or the user may renounce from carrying out security methods. Both user or resource driven security can lead to restricted or dismissed protection. A decision instance is required to establish what is to do, or to omit in such a situation.
Another problem can consist in a disproportion between the amount of requested data and the available resources, which can lead to a violation of availability or integrity.

14.2.4 Metadata Security in Mobile Database Management and Access

As mentioned above, there is a security threat because of different trust levels of the base stations. In database environments, we have to extend our attention on the one hand from Base Stations to all concerned fixed and mobile hosts and on the other hand to access control models. We have to take into account heterogeneity of access control models (multilevel, discrete, role-based) and heterogeneous integration of data in homogeneous models (apart from heterogeneous security aims and strategies). The same information may be classified different in distinct systems. We will call this effect security model incompatibility.
We indicated tracking user movements as the central mobile security issue. The whereabouts and movements can be taken from the communication overhead or deduced from traffic analysis. But there is also another indirect way to detect them. It is obvious, that mobile users working on databases access data necessary in their current computing environment, e.g. at their current location like the city or the building where they are, dependent on communication partners and so on. The information which data the user has accessed (created, read or modified) at which time make a deduction of his movements possible because of the location dependencies of data. This is a totally new threat we are confronted with in mobile database access.

14.3 SECURITY APPROACHES FOR MOBILE DATABASE ENVIRONMENTS

Now we have spread out a wide range of security problems and challenges. While there is a broad research effort in the area of network security for mobile environments, databases in connection with mobility is rather neglected badly. Even we assume a secure and confidential data transfer there are various database security problems. We will offer in the next chapter safeguards to resolve some problems of data management, access and transfer security. First, we investigate the difference between database systems and security related transparencies. Then we explain location and user movement security and after this we present an approach to answer the dynamic and resource restricted mobile environment.

14.3.1 Transparencies

There are basic security challenges tightening up due to mobility. Included in these challenges is the contradiction of transparencies, the transparency in the database sense against the transparency in the privacy sense. The first one means the user will be relieved from internal system knowledge. For example, he sees his database query and the related result, while the operations in the system like parsing and optimization are hidden from the customer. We can compare it with a view through a window, where the window glass is transparent and not visible. The contrary privacy influenced transparency requires

to expose operations for user views. Users can view the structure and operations in the system to control it. They want to know the nature of the window to find out whether there is a transparent glass, not a mirror, or whether the window distorts the real world behind the glass improperly. Mobile used systems are intended to support the user, to reduce remote query processing and to avoid discrepancies between the amount of data and available resources through intelligent preprocessing and influencing during the processing phase. The management and evaluation of context data is a necessary precondition [9]. These metadata are on the one hand pretty sensible (see also [11]) and on the other hand users have to be granted the right to read and influence context data. This is important since a transparent adaptation of query process is not understandable and can lead to misinterpretations of query results. Moreover, the user must have the possibility to influence the adaptation process (see figure 14.2) carefully. The database transparency needs to be restricted for the benefit of privacy related transparency.

14.3.2 Secure Locations and Movements

The location is a sensible information only in connection with user identities. The best protection of user whereabouts consists in the avoidance of management of location information or user information, respectively. Movement information can be achieved by location information in relation to time information, since movement is defined by changing locations in time.
Mobile computing should work as much as possible data thrifty, e.g. as anonymous as possible. Data thrift is a concept in the privacy area and addresses a thrifty management and use of personal data. "Personal data shall mean any information relating to an identified or identifiable natural person" ([4], article 2). The usage of pseudonyms represents a weak kind of data thrift. Since database systems do not support anonymous or pseudonymous computing, pseudonyms must be created either outside of the database system, or users have to act in roles (as described in [11]). We recommend a design of data thrift during the design phase of database systems. In a matrix connecting different levels of data thrift with data and metadata (context), a detailed overview of the necessary and possible data thrift is definable. This model is tested for communication systems in [1].
Let us assume, that data thrift is not applicable. It is possible to deduce the user location

- directly from its management on the network layer and in the mobile context and
- indirectly through traffic analysis and access compromising.

Directly available location information has to be protected with the help of cryptography and suitable access control techniques. In the case of a correctly working system, only the adaptation systems use the location information. Such a mobile context therefore should be accessible only by that system with

exception of user accesses for ensuring privacy intended transparency.
Indirect location inquiries can be avoided by means of disguising real information flows. We have described above disguising techniques in data transfer. In database systems, the information flow between sender and receiver is asynchronous because of storing the data in the database between writing and reading them. That is why we are interested in information about data accesses. To avoid deducing whereabouts by accessed data we will consider location dependencies of database data. The protection of user locations against such a compromising attack requires the knowledge of location attributes in the databases. Databases can include

- location attributes like city, address, district, country etc.,
- attributes relating to identifiable locations like special sights (Akropolis, Statue of Liberty, Brandenburg Gate, etc.).

Location dependencies moreover are based on the user context knowledge. Location attributes mostly build a location hierarchy. Assume further, that the location and location referable attributes are well known. We now define

- aggregation separation,
- vertical separation and
- horizontal separation

to achieve the guarding of directly managed whereabouts in the mobile context as well as indirectly managed locations.

Aggregation Separation As we mentioned above, location and time information endangers privacy only if it is joined with user identities or information relating to identifiable users.
Let {p} be the managed context or audit properties, respectively. Then the separation divides the properties into {u, l, t, r}, where u are user identification properties or contexts, l the location and identifiable location properties, t the time information and r the remaining properties or context information. The protection is obtained by an projective separation.
The aggregation of these data should be accessible just for authorized users. Authorized users are administrators, but with the restriction of vertical separation, and each affected user ("data subject"). The protection is achieved by a separation of user identities and/or location and time. It has to be realized with the help of access control, but also thanks to their physical separation. While in general user identities are simply determined, the establishing of location attributes is a very complex process and needs knowledge discovery methods. General mobility introduced in chapter 1 is a concept to support this separation, thanks to modeled separation of user and location in contexts. The movement of a site does not actually disclose the user movement.

Vertical Separation The more information a user is accessing, the more complete information about user movements and local activities results. A separation of the personal data is advisable to prevent a generation of an extensive user view. The separation can be vertical, or selective. This means the audit information or mobile contexts, respectively, must be guarded with views based on database selections. The selections split location data for example according to their activated role into accesses to databases, fragments, domains, devices, systems and so on. Consequently, only small sections of user whereabouts are visible.

Horizontal Separation The requirement of horizontal separation represents a classical database challenge. Data are handled through the underlying operating system and network to store and transfer them. There must not exist an opportunity to undermine the database security through services of underlying layers. In other words, user dependent location information should not cross the database boundaries. The mobile context is of course common for various applications and layers, but should be accessible only in particular views.

14.3.3 Dynamic and Resource Restricted Mobile Environment

Moreover, security and privacy methods are often very static whereas the mobile communication environment is dynamic and necessitates adjustments of queries and results. As we have explained above, automatical adjustment is a basic concept in mobile computing research within the MoVi-project (see [9] and figure 14.2). The adaptation is applied dynamically. Based on the mobile context, the suitable component will be selected.

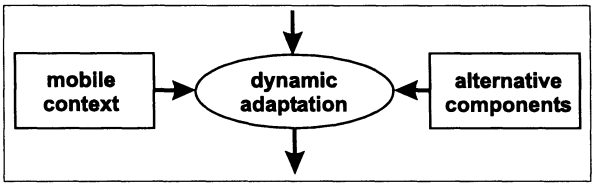

Figure 14.2 Basic Adaptation Concept

The dynamics of mobile database environments arises from the changing mobile context; namely the changing location, dynamic and scarce resources and the varying user and application context. Summarizing, the security and privacy problems caused by the dynamics are:

- heterogeneous access control models on the mobile and the fixed site, heterogeneous integration of information into the same access control model,
- isolated computing,
- no or reduced application of security measures because of scarce resources.

According to the adaptation of database functionality we will try to use the **adaptation concept** to respond to security problems in the mobile environment.
An access from a database system on the mobile site to a fixed database can raise the problem of heterogeneous access control models. The information is managed for example in a matrix model while the access control model of the accessing mobile site is realized multilevel. A similar problem concerns several introduction of data in the same model. For example, the address of employees are accessible for the personnel department in one database system. In another database, a list of special employees is determined who have access.
These model incompatibilities are not specific for mobile computing. They are characteristical for distributed and especially federated databases. But the very heterogeneous mobile hard- and software preconditions increases the problems. An adaptation process is needed to select the suitable model and to execute a **model adaptation**. The precondition for an adaptation process is the existence of additional security information. We recommend a pick-a-back security, e.g. a transfer of information about the original access control model, and data integration in it in connection with the data itself. If an adaptation is not possible (the differences of security levels are unbridgeable), the access fails. The adaptation process can ensure that no data will be accessed from or transfered into an unsecured domain. The other favorable effect of an adaptation process is, the burden of security controls is not only of the user alone.
Moreover, an adaptation component could **control stand alone computing**. This implies to disallow an access to a remote database. A monitoring of the current application is necessary to decide on disconnecting a network connection. The adaptation component has to cooperate with the underlying system layers to realize this task.
Another task for an adaptation process is conceivable, the **resource related adaptation**. It adjusts the database accesses to the available resources. Small mobile devices have likely frequent a lack of resources. Current techniques are not able to recover from these errors. Another effect is, that the user decides in such a case to perform the intended operation by dismissing security measures. The adaptation process can reduce security methods according to reduced functionality and still **maintain a minimal and obligatory security**.

14.4 SUMMARY AND CONCLUSIONS

We have described in this paper mobility related security and privacy issues. We grouped the problems by risks for data and metadata in their management, access and transfer. A basic challenge in this environment is to bridge the gap between different transparencies, namely the database-related and the privacy-related transparency. We identified the protection of user whereabouts and movements to be a central threat in mobile environments and propose three kinds of separation in access and management to guard this additional information. In the last chapter we considered with the adaptability concept to respond to dynamic and often scarce resources. We are going to develop

the security adaptation model and to do small implementations to test this concept.

References

[1] Arbeitskreis Technik der Datenschutzbeauftragten, Schwerin. *Privacy Friendly Technologies (in GERMAN)*, 1998.

[2] D. Chaum. Untraceable electronic mail. *Communications of the ACM*, 24(2):84–88, 1981.

[3] D.A. Cooper and K.P. Birman. The design and implementation of a private message service for mobile computers. *Wireless Networks*, 1(3):297–310, 1995.

[4] *Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data*, 1995.

[5] A. Fasbender, D. Kesdogan, and O. Kubitz. Variable and scalable security: Protection of location information in mobile IP. In *Proc. of the 46th IEEE Vehicular Technology Society Conference*, Atlanta, 1996.

[6] H. Federrath, A. Jerichow, D. Kesdogan, A. Pfitzmann, and D. Trossen. Minimizing the average cost of paging on the air interface - an approach considering privacy. In *Proc. of the IEEE 47th Annual Vehicular International Technology Conference(VTC97)*, 1997.

[7] T. Hardjono and J. Seberry. Information issues in mobile computing. In J.H.P. Eloff and S.H. von Solms, editors, *Proc. of the IFIP TC 11 Int. Conf. on information security, IFIP/Sec'95*, London, 1995. Chapman & Hall.

[8] A. Herzberg, H. Krawczyk, and G. Tsudik. On travelling incognito. In *Proc. of the IEEE WS on Mobile Systems and Applications*, 1994.

[9] A. Heuer and A. Lubinski. Database access in mobile environments. In *Proc. of the Database and Expert Systems Applications (DEXA'96)*, 1996.

[10] T . Imielinski and B.R. Badrinath. Data management for mobile computing. *SIGMOD RECORD*, 22(1):34–39, 1993.

[11] A. Lubinski. A model with roles an norms for the conceptual design of security requirements in enterprise information systems (in german). In G. Weck and P. Horster, editors, *Proc. of the VIS '93 (Reliable Information Systems)*, 1993.

[12] R. Molva, D. Samfat, and G. Tsudik. Authentication of mobile users. *IEEE Network, Special Issue on Mobile Communication*, 1994.

[13] I. Nurkic. Difficulties in achieving security in mobile communications. In *Proc. of the IFIP World Conference on Mobile Communications*, 1996.

[14] A. Pfitzmann, B. Pfitzmann, and M. Waidner. ISDN–MIXes: Untraceable communication with very small bandwidth overhead. In *Proc. Of the IFIP/Sec'91*, 1991.

[15] M. Reichenbach, H. Damker, H. Federrath, and K. Rannenberg. Individual management of personal reachability in mobile communication. In *Proceedings of the IFIP TC11 SEC 97, 13th International Information Security Conference*, 1997.

[16] D. Sayer. The erosion of privacy and security in public telecommunication networks: Growing significance of telemetadata in advanced communication services. Working Paper 13, European Commission's FAIR project, Sussex, 1997.

[17] V. Varadharajan and Y. Mu. Design of secure end-to-end protocols for mobile systems. In *Proc. of the IFIP World Conference on Mobile Communications*, Canberra, 1996.

[18] Y. Zheng. An authentication and security protocol for mobile computing. In *Proc. of the IFIP World Conference on Mobile Communications*, Canberra, 1996.