Status Quo and Prospect on Mobile Database Security

Tao Zhang*[1], Shi Xing-jun[2]
[1]Information Commission Office, Heilongjiang University, Harbin 150080, China
[2]School of Economy & Trade, Zhejiang Industry & Trade Vocational College, Wenzhou, 325003, China
*Corresponding author, e-mail: zhangtao2668@126.com[1], sxj96@163.com[2]

Abstract

Mobile database is a specialized class of distributed systems. There are some security challenges because of the dispersed nature of the mobile database application and hardware device constraints. Therefore, the security issue of mobile database is analyzed in this paper. We will research the security in terms of mobile device, operating system on mobile device, mobile network and mobile database. Moreover, various security vulnerabilities on mobile database is recognized. Some appropriate technique is used to deal with side affect for mobile database security. For the sake of more security, Comprehensive solution that is applied to distributed database is proposed.

Keywords: *mobile database, security threats, security vulnerabilities*

1. Introduction

Databases continue to grow in size and complexity, and they are used in many diverse applications. Formany real world applications, it is necessary toincorporate some type of uncertainty management intothe underlying data model. One characteristic of manyimprecise databases is that they allow sets of values intheir tuples. This is referred to as a non-first form ornested database [1-2]. If the value of an attribute is non-atomic, i.e. set-valued, then there is uncertainty as to which one of the values in the set corresponds to the attribute, or whether more than one does. There arespecific aspects in different uncertain database modelsbut all share use of set values. Of particular interest inthis research is the rough relational database, a modelbased on rough sets [3].

The objective of this paper is the global interoperability of mobile users and organizations to provide information on the security features of the database system, and provide suggestions to protect the users of mobile database technology and the organizations that hire them. The security of any database system support is compulsory. Mobile database systems to protect users and equipment well the support of database security is even more important. For the attacker, it is easy to access the network because that wireless medium is open. Therefore, database is more vulnerable. In the current study, there is no integrated presentation of solutions to solve all the security problems of mobile database systems. However, it is significant important for user. The security issues in mobile database systems and mobile networks are discussed in this paper. Moreover, the corresponding solutions are also analyzed. Moreover, a novel solution to deal with security is proposed. First of all, security issues are divided into four fields. They are mobile device, operating system on mobile device, mobile database and mobile network, respectively. The integrated presentation is important to researchers and developer to understand theproblem domain effectively and probably propose more securemechanisms in the future. The purpose of this article is to conduct a comprehensive survey on existing security mechanisms and explore disadvantage security of them. In addition, a new solution for any security issue is alsoprovided. For distributed database, some possible solution is proposed and appropriate techniques are used to meet the security requirements.

2. Security of Mobile Device

For Windows Mobile Application Developers, Security is asignificant important issue. So some applications might need to be protected by signing, which used a privileged or

Received February 5, 2013; Revised May 21, 2013; Accepted June 12, 2013

unprivileged certificate. In addition, Understanding of the application running on Layer 1 and Layer 2 security equipmentis an extremely important. The window mobile devices security model is classified into application execution security, device configuration security and remote access security.

2.1. Application Execution Permissions

Applications might be allowed to run or might be blocked from execution on the device, which depend on the security configuration of a particular Windows Mobile device. For Windows Mobile devices, the application execution permissions are defined as follow:

(1) Blocked: all application is not allowed to execute.
(2) Normal: in execution, the application is restricted. Moreover, it cannot call trusted Win32 APIs, write to protected areas of the Registry, write to system files, or install certificates.
(3) Privileged: The application has full write access to the file system and to the system Registry. Moreover, it is also allowed to install certificates that might allow other applications to run on a particular Windows Mobile device.

2.2. On-Device Security Policies

Device-level security involves managing who has access toa device and its data, controlling which applications can run on the device, and establishing how data is transmitted to and from the device. User access is managed through a PIN or password authentication. A device can be set to lock automatically after a period of inactivity or after being turned off, requiring a user to unlock the device again to use it.

2.3. Best Security Practices for Windows Mobile Devices

(1) Prompt the user before running normal applications. Microsoft highly recommended that you keep the UserPrompt mode on for unsigned application for all Windows Mobile devices.
(2) Keep your Bluetooth off.
(3) Devices corrupt deleted information on memory cards to prevent access to it.

3. Security of mobile database

3.1. Distributed Databases

A distributed database is defined that data is distributed across multiple databases. Its system is comprised of a DDBMS (distributed database management system) and a distributed database and a network for interconnection.The distributed database is managed by DDBMS. For database management systems, the requirement should is including: multi-level access control, authentication, reliability, integrity, and recovery.

Mobile database is a specialized class of distributed systems where some nodes can disengage from joint distributed operations, move from the cell serviced by onebase station to that serviced by another base station to make continuous connected operation possible. Mobile databases can be distributed under two possible scenarios:

1) The entire database is distributed mainly among the wired components, possibly with full or partial replication.
2) The database is distributed among wired and wireless components. Data management responsibility is shared among base stations and mobile units.

3.2. Problems, Security Challenges and Solutions for Mobile Distributed Database

Some of the software problems in distributed database systems may involve data management, transaction management, and database recovery. In mobile computing, however, these problems are more difficult, mainly because of the limited and intermittent connectivity afforded by wireless communications, the limited life of the power supply (battery) of mobile units, and the changing topology of the network. Therefore, it is necessary to manage data on the mobile unit that such disconnected operation is possible. In the case of a mobile database application that it is a distributed database, there are security challenges due to the distributed nature of the application and the hardware constraints of mobile devices. The major issues in multi level security on Distributed Security Manager are authentication, data confidentiality, identification and enforcing appropriate access controls.

(1) Authentication.

User authentication is the primary lineof defence for mobile and handheld devices such as Personal Digital Assistants (PDAs). Authentication determines and verifies the identity of a user in the system, i.e., providing an answer to the question: “Who is the user?” Traditional authentication mechanisms rely on maintaining a centralized database of user identities, making it difficult to authenticate users in a different administrative domain as depicted [5]. This mechanism for providing security in mobile device is adifficulty for every system providing safe access to precious, private information, or personalized services. Issue here is the authentication mechanism should be distributed, and the various components of the authenticator need to communicate with each other to authenticate a user. In centralized environment, the authenticator needs to have information about all of the users of the system.

Mobile device user need only authenticate him to the first device he logs into and that device passes the authentication data to each of the other devices then the user can to access. This scheme requires that all of the devices on the network are capable of reliably handling this authentication data. Standardization efforts such as Open System Environment (OSE), Portable Operating System Interface (POSIX) and Government Open Systems Interconnection Profile (GOSIP) can contribute to this goal of transparent authentication across networks.

By notation to three basic authentication means that we describe, PIN based authentication is a method for verifying the identity of actual device users, but this method have considerable drawbacks, because pick PIN or passwords can be easily guessed. For prevent guess a password, user have to define a complex password, then it is often hard to remember. To address this problem in handheld devices, have developed comparatively more secure, affordable and memorable authentication schemes based on graphical assistance or Biometric authentication, such as fingerprints, voice recognition, iris scans, and facial recognition are not yet widely adopted [6]. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable.

(2) Data confidentiality.

Typically, the increasing connection of travelling users to corporate databases to make personal data available to mobile users introduce new threats on data privacy and confidentiality. Nowadays, one solution is considered that called C-SDA (Chip- Secured Data Access), which allows querying encrypted data while controlling personal privileges. C-SDA is a client-based security component acting as an incorruptible mediator between aclient (potentially mobile) and an encrypted database. This component is embedded into a smart card to prevent any tampering to occur on the client side. It is better to embed theuser's confidential data into its own mobile device (e.g., aPDA). Apart from their limitation in terms of storage capacity, even these devices cannot be fully trusted because they can be stolen, lost or destroyed (thus a copy of the data they host has to be maintained in the network to guarantee data resiliency). Another way to provide confidentiality is through encryption, either using the public key of the receiving principal or using a combined symmetric key and public keymethod. For instance, the agent can be encrypted using asymmetric key and the symmetric key protected using the public key of the receiving principal. Encryption often used to protect data on insecure networks or storage devices.

(3) Identification.

The process of verifying a user's identityis typically referred to as user identification and authentication. Passwords are the common method used for authenticating computer users, but information as name (e.g.,first or last) or a Passwords, email address provides no assurance of identity, in preventing unauthorized access to computer resources when used as the sole means of authentication, so some users are beginning to use biometricsas methods of user identification.

If we want use from passwords as security means so have to management use of passwords by Periodic changing of passwords that it depends on the sensitivity of the data, or use of deliberately misspelling words, combining two or more words together, or including numbers and punctuation in a password, so that prevent the guess of passwords. The identity must be unique so that the system can distinguish among different users. The identity should also be non-forgeable so that one person cannot impersonate another. An important distinction between identification and authentication is that identities are public whereas authentication information is kept secret and thus becomes the means by which an individual proves that he actually is who he claims to be. In addition, identification and authentication provides the basis for future access control [7].

Table 1. Protection against Threats and Risks

Threat or Risk	Windows Mobile 6 Security Features
Access to data because of device theft or loss	Device lock requires a password or PIN to access the device when it is turned on Local and remote device wipe occurs after a specified number of incorrect login attempts Local and remote storage card wipe erases data and helps to prevent unauthorized use Storage card encryption helps to prevent unauthorized use Custom Local Authentication Subsystem (LAS) and Local Authentication (LAP) providethe infrastructure for authentication by sophisticated third-party hardware and software methods. Password policyenforcement,such as required password for synchronization
Unauthorized penetration into corporate network	Flexible client authentication: SSL TLS, Exchange ActiveSync, Certificate-based,RSA SecureID-protected Users can add root certificates without compromising device management security and without being a manager of thedevice
Unauthorized penetration into mobile device	Security policies help to control over-the-air access to device Bluetooth discovery mode can be prohibited to help guard device integrity (Supported in Windows Mobile 6 Standard only)
Device corruption	Security policies help control acceptance of unsigned attachments, applications, or files Attachments for download can be denied or size-restricted
Malicious software or viruses on mobile devices	Office Moble applications do not support mocros,so viruses cannot leverage them to do damage Code execution control allows the device to be locked so that only applications signed with a trusted certificate can run

(4) Access control.

Access control protects data integrity by limiting who can alter data. The access control rules enforced in a distributed environment may be distributed, centralized or replicated. If the rules are centralized, then the central server needs to check all accesses to the database. If the rules are distributed, then appropriate rules need to be located and enforced for a particular access. Often the rules associated with a particular database may also be stored at the same site. If the rules are replicated, then each node can carry out the access control checks for the data that it manages [8]. Relational database systems implement access control in theSQL language, using the GRANT and REVOKE commands.The GRANT command is used to give privileges to users.

In SQL, object may be a base table or a view and a list of column names. The privileges include SELECT, allowing read access to the named columns of the indicated table, as well as INSERT, UPDATE, DELETE, with expected meanings. The user's parameter may refer to a single user or a group of users. The REVOKE command is used to remove previously granted privileges.

Multilevel secure database management system (MLS/DBMS), users cleared at different security levels accessand share a database with data at different security levels (alsocalled sensitivity levels) without violating security, and is based on distributed data and distributed control, all data in the database must receive an access classification and a user at a lower classification level will be unaware that data exists at a higher classification level. From the design point of view and security policy of MLS/DBMSs, access control systems can be classified into, discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC)[9].

a) *Discretionary Access Control (DAC):*
This approachhinges upon the granting and revoking of privileges.Typically, a lattice is maintained in the DBMS that stores the access privileges of individual users. When a user logs on, the interface obtains the specific privileges for the user. These privileges are identified with a user or account, and can be of two types. The first type, account level, allows the user system privileges such as Create/Delete Table, or ability to add/delete table columns. The second type, or table level, is more granular. It allows the user to access, or not, specific data within the database [11].

b) *Mandatory Access Control (MAC):*
This mechanism restricts access to data depending on the sensitivity levels of the data and the clearance level of the user. By classification level of the user, Users can read or modify data in their view. The view is a logical table, which is created with the SQLVIEW command, this table contains data from the database obtained by additional SQL commands such as JOIN and SELECT. If the database is unclassified, the source for theview is the entire database. On the other hand, the database issubject to multilevel classification, and then the source for theview is that subset of the database. If the view is properly designed, a user at a lower classification level will be unawarethat data exists at a higher classification level; In fact, the view prohibits users from accessing data. These constraints are mandatory and automatic. The system must review these constraints each time it encounters a request for a read orwrite.

c) *Role Based Access Control (RBAC):*
RBAC isevolution from those older policies. The main concept under RBAC is that privileges are encapsulated into roles. Users are then assigned to roles, and acquire those privileges. A role is defined as "an explicit (i.e., named) representation of acollection of privileges which are defined and used by system administrators and users." With RBAC, database administrators may create roles, assign privileges to thoseroles, and then assign users to roles based on their specific job responsibilities and roles. MAC and RBAC models have been used in conjunction with one another. The data items are assigned to classification levels (as in MAC) and the user privileges are concatenated into roles (as in RBAC).

4. Security of Mobile Network

Mobile operator’s 3G networks are not only exposed to all the virtual pathogens already in circulation, but also to mobile specific viruses and Trojans, as well as to direct attacks such as Denial of Service (DoS) on their networks from hackers and criminal organizations. These types of attacks employ methods which wired ISPs have been dealing with for a much longer period of time. There are also variations on these attacks which exploit weaknesses in the architecture and some of the protocols used in 3G cellular data networks. To protect their networks and customers, then, mobile operators need to:

(1) Be vigilant and adopt appropriate security policies that reflect the threats in the 3G world. This has additional ramifications given the widespread use of Wi-Fi and the general evolution toward networks based on the IPMultimedia System (IMS) standard.

(2) Make client-side anti-virus and firewall software readily available to their subscribers who use data devices (e.g., feature phones with data capabilities, Smartphone, notebook computers) [12].

(3) Take an architecture approach to implementing security solutions in their network; point solutions are not sufficient.

(4) Vigorously protect signaling as the migration of signaling traffic over IP creates new risks. Mobile operators carry much more signaling traffic than their wired Counterparts and signaling is mission critical traffic.

(5) Be aware that their networks are only as secure as the weakest link. Mobile operators need to work with each other, the ISP community and other telecom providers to ensure that even the minimum amount of security is quite strong [13].
Next, in this paper will explore the following topics:
1) Why 3G wireless networks are now vulnerable and at what points they are vulnerable.
2) Mobile operators have opened up their networks to the public Internet and to other data networks, making their 3G networks more vulnerable to attacks.

3) Mobile operators are evolving their networks to IMS, enabling interconnected networks all running on IP.

The security implication here is that with more users ofvaried data-capable devices who are accessing content and communicating with one another across multiple networks, there will be more traffic on the cellular networks. That implies a higher likelihood of attacks occurring from any number of sources [14]. For example, many sophisticated attacks disguise themselves in data flows across sessions and ports – the more traffic there is, the harder it is to identify the threats [15]. At a high level, there are numerous vulnerable elements inmobile operators' data networks:

(1) The mobile equipment (ME) itself, such as laptopcomputers, cell phones, PDAs, Smartphone.
(2) Interfaces to other mobile networks-onGPRS/UMTS networks this is the interface.
(3) Signaling protocols and or interfaces within a network and inter-networks.
(4) The over-the-air wireless link between the ME and the cellular base station (BS)-this is the UMTS/HSDPAor EV-DO connection.
(5) Management and service elements such as the Home Location Register (HLR) which stores subscriber data In IMS, the HSS (home subscriber server) performs the function of the HLR.
(6) Application and content servers.

Table 2. Types of Attacks against Mobile Networks

Purpose	Target	Type of Attack
Harassment, denial of service / service interruption	Other users, network elements (content servers)	Worm, Virus, Trojan, SMS/MMS spam
Attack ability to provide service	HLR, AAA, content servers, signaling nodes	Denial of service, SYN flood, application layer attacks(on RADIUS servers, buffer overflows, SIP flooding, RTP flooding)
Fraud	Operator's management elements (AAA, HLR, VLR, etc.)	Overbilling attack
Service theft	User sessions	Spoofed PDP context
Attack ability to provide service	Signaling nodes	Signaling-level attacks (SIGTRAN, SIP) which involve modification interception,DoS

5. Conclusion

Distributed Database Security is integral to the design andfunction of a distributed database. There are three important pieces to Distributed database security; Physical, User, andNetwork. These pieces work in conjunction with policies, standards, and procedures. Policies are directions that support a goal. Solutions described above must be applied to a distributed database on a goal. Also, human factor and traits should not be ignored in this system. Because, a user as who one uses this system, would be considered as an effective factor for security. Of course, we could emphasis that only concentration on reviewed items could not be enough and for more security, during implementation would be considering an appropriate architecture.