Vol 5 Issue 3 April 2015

ISSN No : 2230-7850

International Multidisciplinary Research Journal

Indian Streams Research Journal

Executive Editor
Ashok Yakkaldevi

Editor-in-Chief
H.N.Jagtap

Welcome to ISRJ

RNI MAHMUL/2011/38595 **ISSN No.2230-7850**

Indian Streams Research Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial board.Readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

International Advisory Board

Editorial Board

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.isrj.org

Indian Streams Research Journal ISSN 2230-7850 Impact Factor : 3.1560(UIF)
Volume-5 | Issue-3 | April-2015 Available online at www.isrj.org

MOBILE DATABASE SECURITY THREATS

Mapkar Atiqua Yunus
I.T. Department D.G.Tatkare College Mangaon- Raigad

Co-Author Details :

Priyanka Sawant (T.Y.B.Sc.I.T.) [1] and Pawar Sonal (T.Y.B.Sc.I.T.) [2]
I.T. Department D.G.Tatkare College Mangaon- Raigad

ABSTRACT:

Ubiquitous use of mobile phones has caused an emergence of applications targeted to mobile platforms. Since mobile devices become the major mobile platforms for users to transfer and exchange diverse mobile data over the wireless networks or wireless internet, mobile security for mobile accesses becomes very important and critical to assure secured mobile transactions, mobile data integrity and confidentiality. Mobile security also is critical to protect mobile users and mobile-based application systems from unauthorized accesses and diverse attacks. This paper shows different mobile database security threats that may be occurs for mobile database in the real world and gives possible solution to eliminate them. This paper discusses all the security issues in both mobile database system and mobile network and discusses their solutions.

KEYWORDS
Mobile Database , Since mobile , transactions,

I.INTRODUCTION

Mobile phones have become the breath and soul of technologies in today's fast emerging world. Mobile database is a specialized class of distributed systems. There are security challenges due to the distributed nature of the mobile database application and the hardware constraints of mobile devices. In this paper, we will deals with the subject of security in four fields. These four areas include: Security of mobile device, security of operating system on mobile device, security of mobile database and security of mobile network. We identify a set of security vulnerabilities on mobile database and try to apply appropriate technique to decrease side affect for mobile database security. Security support is mandatory for any database system. For mobile database systems, security support is even more important to protect the users and devices as well as the database. In mobile communication, since wireless medium is available to all, the attackers can easily access the network and the database becomes more vulnerable for the user and the central computer that located distributed database on it. First, security issues divided to four fields that they are important from many aspects. Mobile device, operating system on mobile device,\mobile database and mobile network are four fields that we will discuss security issues.

II. Understanding Basic Mobile Security Concepts, Threats, and Needs:

What are the mobile security threats in mobile access?

Whenever discussing mobile security, we must understand mobile security threats to mobile phones and mobile accesses. Mobile phones have certain specific features (such as mobility) which make these devices more vulnerable to security attacks. The list of features is following.

- Mobility: This is the most important characteristic of the mobile phones. Since mobile users can take them to anywhere, the chances of getting stolen, lost, or physically tempered increases as compared to stationary devices.
- Strong Personalization: As a personal device, mobile devices usually are not shared among multiple users.
- Strong Connectivity: Mobile phones are commonly used to connect to other devices over the wireless networks (or wireless Internet) for data exchanges.
- Technology Convergence: Today numerous functional features are integrated in the mobile phones, for example gaming, video and data sharing, and internet browsing.
- Limited Resources and Reduced Capabilities: Comparing with stationary devices, mobile devices have four major limitations: a) limited battery life, b) limited computing power, c) very small display screen size, and d) very small sized keys for inputs. These limits bring the challenges in building mobile security technology.

These features render mobile devices vulnerable to certain types of attacks. Table 2.1 summarizes these attacks, relating causes, and potential affects.

TABLE 2.1: Categorization of Attacks Causes (Features)	**Type of Attack**	**Mobile Security Affects**
Mobility	Lost or theft device	Authentication, Confidentiality
Limited resources	DoS (Denial of Service)	Data Integrity, Confidentiality, Availability
Strong Connectivity Requirement	Viruses or worms (malware)	Data Integrity, Confidentiality, and Charging
O.S. Weaknesses, Code Exploitation	Break-In Attacks	Prepare ground for other attacks

What are Mobile Security Requirements and Needs?

Although the fundamental concepts of security remain the same while considering mobile security relating mobile accesses, some new needs and requirements must be considered to manage with the above threats in mobile accesses. They are summarized as followings.

• Mobile access confidentiality: This makes sure that only the authorized persons are allowed to access to mobile data though mobile devices.
• Mobile data integrity: This makes sure that mobile data are consistent, correct and accessible.
• Mobile service availability: This requires the mobile resources on mobile devices only be accessed and used by the legitimate owners.
• Disputed mobile service charging: This refers to the case in which a mobile subscriber may be charged for mobile services and connection times because someone else caused the mobile device to access such mobile services without the user's knowledge.

These mobile security threats bring new requirements and needs for more effective mobile security solutions and technologies to ensure mobile access security on mobile devices so that the end-to-end protection between mobile devices can be assured.

What are the Implementation Challenges in Mobile Security?

Because of the limits of mobile devices, implementing mobile security solutions must address the following needs and challenges in building mobile security.
• *Energy saving security solutions:* The limited battery life and operation time requires mobile security solutions to be implemented in an energy saving approach.
• *Limited applications of existing security solutions* – The limited computing capability and processing power of mobile devices restrict the applications of many existing complex security solutions, which require heavy processors.
• *Restricted size of screen and keyboard:* It restricts the input and output capabilities of mobile phones, which in turn cause some security related applications, for example, password protection may not be easy for mobile users.
• *Higher portability and inter-operation issues* – Since mobile devices may be equipped with different

mobile platforms and operation environments, mobile security technologies and solutions must be implemented with a higher portability to address interoperation issues.

III. SECURITY OF MOBILE DATABASE :

A. Distributed Databases: A distributed database system includes a distributed database management system (DDBMS), a distributed database and a network for interconnection. The DDBMS manages the distributed database. Distributed database system functions include distributed query management, distributed transaction processing and enforcing security and integrity across the multiple nodes. Requirements for database management systems are:

- Multi-Level Access Control
- Authentication
- Confidentiality
- Reliability
- Integrity
- Recovery

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.

B. 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.

1) Authentication. User authentication is the primary line of defense 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. This mechanism for providing security in mobile device is a difficult for every system providing safe access to precious, private information, or personalized services. There are three basic authentication means by which an individual may authenticate his identity.

a) Something an individual data (e.g., a password, Personal ID Number (PIN), the combination to a lock, a set of facts from a person's background).

b) Something an individual POSSESSES (e.g., a token or card, a physical key to a lock).

c) Something an individual IS (Intermediate System) (e.g., personal characteristics or "biometrics" such

as a fingerprint or voice pattern), this technique works on the Fingerprint basis whereby the phone can be accessed when it identifies the Fingerprint of the user(s).

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 a client (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 the user's confidential data into her own mobile device (e.g., a PDA). Apart from their limitation in terms of storage capacity, even these devices cannot be fully trusted because they can be stolen, lost or destroyed.

3) Identification: The process of verifying a user's identity is 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 biometrics as 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.

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.

IV. 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 them protocols used in 3G cellular data networks. To protect their networks and customers, then, mobile operators need to:

- Take an architecture approach to implementing security solutions in their network; point solutions are not sufficient

- Deploy a variety of products in their networks, such as firewalls, intrusion detection and prevention (IDP) and virtual private networks (VPNs).
- 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)
- 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 IP Multimedia System (IMS) standard. 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.

Cellular data networks are vulnerable for several reasons:

1) Mobile operators are building out high speed wireless networks that are based on the Internet Protocol (IP) which allow users to do more while connected.

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.

TABLE II. TYPES OF ATTACKS AGAINST MOBILE NETWORK

Purpose	**Target**	**Types 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	content servers, signaling nodes	Denial of service, SYN flood, application layer attacks
Fraud	Operator's management elements	Overbilling attack
Service theft	User sessions	Spoofed PDP context
Attack ability to provide service	Signaling nodes	Signaling-level attacks which involve modification, interception, DoS

The security implication here is that with more users of varied 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 higher likelihood of attacks occurring from any number of sources.

At a high level, there are numerous vulnerable elements in mobile operators data networks:

- The mobile equipment (ME) itself, such as laptop computers, cell phones, PDAs, Smartphone
- Interfaces to other mobile networks – on GPRS/UMTS networks this is the Gp interface
- Interfaces to the data networks – the Internet or private data networks; on GPRS/UMTS networks this is the Gi interface
- Management and service elements such as the Home Location Register (HLR) which stores subscriber data (the Ga interface on GPRS/UMTS networks). In IMS, the HSS (home subscriber server) performs the function of the HLR.
- Application / content servers
- Signaling protocols and/or interfaces within a network and inter-networks.

Solution for Securing of Mobile Network:

For mobile operators, the first step in defeating attacks on their networks is to recognize their new found role as an ISP. This means implementing a layered defense for their network that:

- Changes security policies and practices to better reflect the new threats
- Concentrates, whenever possible, wireless data services into a smaller number of data centers. Many mobile operators in Europe have already taken these types of steps to protect their core networks.
- Protects end users by implementing technology on their devices and in the network – e.g., anti-virus, firewalls, content scanning – that provides file-level security
- Deploys security products such as firewalls, virtual private networks (VPNs) and intrusion detection and prevention (IDP) systems at appropriate points in the network, which provides packet level, session level and application level protection securing the Mobile Network.

V. CONCLUSION:

Distributed Database Security is integral to the design and function of a distributed database. There are three important pieces to Distributed database security; Physical, User, and Network. 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.

REFERENCES:

[1] http://www.windowsmobileinyourpocket.com
[4] Security Model for Windows Mobile 5.0 and Windows Mobile 6, February 2007
[5] S. Miltchev and J. M. Smith, V. Prevelakis, A. Keromytis, S. Ioannidis,
Decentralized Access Control in Distributed File Systems, 2003
[6] M. N. DOJA, NAVEEN KUMAR, user authentication schemes for
mobile and handheld devices, Jamia Millia Islamia - New Delhi,2007

Publish Research Article
International Level Multidisciplinary Research Journal
For All Subjects

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication,you will be pleased to know that our journals are

Associated and Indexed,India

- International Scientific Journal Consortium
- OPEN J-GATE

Associated and Indexed,USA

- Google Scholar
- EBSCO
- DOAJ
- Index Copernicus
- Publication Index
- Academic Journal Database
- Contemporary Research Index
- Academic Paper Databse
- Digital Journals Database
- Current Index to Scholarly Journals
- Elite Scientific Journal Archive
- Directory Of Academic Resources
- Scholar Journal Index
- Recent Science Index
- Scientific Resources Database
- Directory Of Research Journal Indexing

Indian Streams Research Journal
258/34 Raviwar Peth Solapur-413005,Maharashtra
Contact-9595359435
E-Mail-ayisrj@yahoo.in/ayisrj2011@gmail.com
Website : www.isrj.org