Security Challenges in Mobile Computing

Dr.B. Prabhakar Reddy, P. Imran Khan, S. Mahaboob Basha

Professor[1], Assistant Professor[2,3]

1,2 Bheema Institute of Technology and Sciences, Adoni-518301.

3 Brundavan Institute of Technology and Sciences, Kurnool.

Article Info
Page Number: 471-475
Publication Issue:
Vol. 69 No. 1 (2020)

Article History
Article Received: 25 June 2020
Revised: 30 July 2020
Accepted: 15 August 2020

Abstract

Today, mobile computing and applications are rapidly growing in popularity and playing an increasingly important role in improving the internet's underlying computer infrastructure. There has been a shift to a new computing paradigm due to the proliferation of wireless technology and handheld computers. Within the scope of mobility, disconnections, data access modalities, and scale of operation, this study provides security difficulties in mobile computing and some researched concerns addressing the security of mobile computing system.

Unlike prior work that has focused on wireless communication security, our main concern is the safety of crossings that rely on wireless networks.

Keywords

Mobile Devices, Mobile Communication, Mobile networks, Mobile Computing, Communication Security

I. Introduction

With mobile computing, users are expected to move about with their devices while working. Communication, hardware, and software may all be made portable for use in mobile computing. Information may be published and subscribed to regardless of the user's physical location, thanks to mobile computing. The phrase "mobile computing" refers to the use of tiny, portable, and wireless computer and communication devices to connect wirelessly to and use centralized information and application software.

The advent of "mobile computing" heralded the beginning of a new era for the IT industry. The idea of mobile computing stems from the recognition that, as computer hardware shrinks in size in tandem with increases in computing power, users would expect that this equipment be a regular part of their lives for the purpose of completing routine chores. Future mobile computing devices, like today's laptops and palmtops, will be able to communicate with one other over wireless networks while concealing their whereabouts from the user, according to researchers in this emerging subject. This idea of openness stems from the fact that with distributed computing, the user is often not aware of the actual geographical location of the resources being used by the system.

.Fig.1: Distributed Computing System

The ever-expanding capabilities of mobile devices pose growing information and security concerns. This makes the question of how to keep data and apps safe on mobile devices an urgent one. The proliferation of wireless data networks poses new threats to data safety.

II. Methodology

Studies included in the selected sources must be related to our problem, and these sources must be web-available; the selection criteria we used to evaluate them were based on the authors' collective research experience.

Mobile ad hoc network protocols may be found. Table-driven routing protocols seek to ensure that all network nodes have access to accurate and up-to-date routing information. When a source node requests a new route, only then will it be created. When a node in the network needs to go somewhere, it starts the process of finding the best path there. To further enhance the review's efficiency, relevant work areas of the chosen papers are also searched in order to guarantee that no useful reference is missed notice throughout the explore process. After identifying potential data sources, it was required to elaborate on how studies would be chosen and evaluated.

Thirdly, Safety and Portability

The fact that individuals and the data they carry have become mobile has brought a new set of security issues into computers, which are distinct from those that existed in static environments. In the past, when computers were stationary and not mobile, physical security was simply achieved by isolating the hardware responsible for processing and storing data from the rest of the system. If set up in this manner, the system could function independently of any outside input or interaction. Newer firewall methods may also be used to accomplish the same goal. This degree of independence and autonomy is challenging to accomplish in mobile computing owing to the restricted resources available to a mobile unit, requiring the unit's interaction with the mobile support station. From the perspective of the presence and position of a user (which are considered data in itself), and the data that they carry, the mobility of people and their data poses security challenges.

data integrity and privacy while communicating with other users or a server. In particular, a user on a mobile wireless network has the option of maintaining the privacy of his or her personal details. That is, a person may remain anonymous to the vast majority of other users on the network while revealing their true identity only to a small group of trusted friends. The security of a user's location data when it is stored or transferred between nodes as the user moves in a nomadic fashion is related to the more difficult problem of the trust level afforded by each node in the wireless network, making the issue of user anonymity in mobile computing a subset of the larger problem of trust in wireless networks. These nodes, regardless of their individual trustworthiness, must provide the user confidence in his or her anonymity. When a user moves between various trusted zones, each administered by a different node, this condition becomes very crucial. Secure data transmission between databases at nodes that store location data and other information or attributes in the user profile is also crucial. Here, it is crucial that all network-level traffic that is hidden from the perspective of a nomadic user be kept safe and legitimate.

Problems with Mobile Security, Part IV

Mobile internet security issues were explored. The primary goals were to assess the security issues, create viable safe solutions across all tiers, prototype those solutions, and then encourage standardization.

There is a wealth of data available to us online, including that produced by private businesses, academic institutions, and government agencies. Some of this information is certain to be useless, but the real issue is that it is often unclear to the user whether information is reliable, even when they are dealing with a reputable organization, since the material itself (or the website itself) might be a forgery.

Protocols such as Internet Protocol Security (IPSec) and Secure Sockets Layer (SSL)/Transport Layer Security (802.11 and Bluetooth) incorporate well-established, standardized security measures. However, it remains challenging to manage public key information on a massive scale across several channels of communication. The difficulty increases when the network topology is dynamic and constantly changing. It is also not obvious how mobile IP and firewalls interact with other communication security techniques like IPSec. The problem of developing effective cryptographic algorithms in low power conditions, such as those often found in Ad hoc networks, remains open despite the growing computational capability of PCs and workstations. People come up with workarounds, such filing their passwords under "s" for "secret" in their address book, since security methods are too hard to utilize. The sheer number of passcodes and PINs that modern users must keep straight is enough to drive many individuals to frustration.

A. Mobile device security concerns

Security concerns hinder the growth of mobile services, thus these gadgets need careful examination. All security concerns must be resolved at the onset of service creation. Developers of mobile services have a number of challenges when it comes to mobile security, the most significant of which are the complexity of technological solutions, the

unlawful copying of applications and material, and Internet-based dangers.

B. Mobile Network Security Concerns

The need for network connectivity via mobile or roaming devices is propelling the development of mobile networks. Despite the

Despite the obvious requirement for wireless network connectivity, there are several challenges that come with using a wireless medium.However, wireless does not always mean portable. Some wireless networks, such wireless local loops, have both ends of the connection permanently installed. This means that research into wireless data networks may cover ground distinct from that of traditional networking.

Concerns about mobile phone security

In comparison to their wired equivalents, wireless gadgets like mobile phones, PDAs, and pagers provide a greater security risk. Reasons for this include increased bandwidth, storage, and computing power. The other factor is the temporary loss of data during transmission. One of the primary needs in PCs is the establishment of a safe wireless communication channel. Autonomy of communicating entities, user mobility, and hardware constraints are all factors that must be taken into account while creating a security solution for mobile communication.

III. Conclusion

In order to present a comprehensive picture of the security issues facing mobile devices, networks, and communication, this research combed through a variety of papers and conference proceedings. It has been discovered that mobile device security is a major problem. In order to resolve the security concerns plaguing this field, researchers need to provide it the attention it deserves. Because of limitations in mobile device interfaces, evolving mobile networks, and cutting-edge mobile communication technologies, none of the existing solutions provide a comprehensive fix. These portable gadgets will soon be able to join a variety of networks. Thus, the subject of how to complete new security problems is a reasonable one to consider.

References

1. An Identity-Based Broadcast Encryption Scheme for Mobile Ad Hoc Networks. [1] Sharad Kumar Verma, Dr. D.B. Ojha. Here's a link to it: http://www.ijceronline.com/papers/Vol2_issue5/CK02516951698.pdf.
2. Architecture of Mobile Application, Security Issues and Services in Mobile Cloud Computing Environment, [2] Swarnpreet Singh, Ritu Bagga, Devinder Singh, Tarun Jangwal. For further information, please visit: http://www.ijcer.org/index.php/ojs/article/viewFile/9/7.
3. According to [3] A Hierarchical Framework Model of Mobile Security by Jun-Zhao Sun, Douglas Howie, Antti Koivisto, and Jaakko Sauvola. The document may be seen at http://www.mediateam.oulu.fi/ publications/pdf/76.pdf.

4. Security in Mobile Payments and Proximity Mobile Payments [4] http://www.academia.edu/Documents/in/Security_in_Mobile_Payments_Security_in_Proximity>
5. You may get a paper written by Jon Oltsik titled "Addressing Mobile Device Security and Management Requirements in the Enterprise" at http://investor.juniper.net/files/doc_downloads/resources/ JNPResg-addressing-mobile-device-security-and-management-requirements.[1].pdf