© 2016 IJSRSET | Volume 2 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Mobile Computing : Security Threats

Sweety, Jabir Singh
Computer Science and Engineering, Shanti Niketan College , Hisar, Haryana, India

ABSTRACT

This paper deals with the security issues and different security schemes in mobile computing system. We classify these schemes based on types the infrastructure used in the mobile computing system-Mobile Ad Hoc Networks (MANET) and Mobile Agent model. Mobile Ad Hoc Networks are permeative, present anywhere at once and without any centralized authority. These unique characteristics will increasing security threats, demand solutions in securing ad hoc networks. This paper reviews the prevailing mobile ad hoc network security threats, the existing solution schemes, their limitations and open research issues. With respect to Mobile Agent based mobile computing system, we have presented the classification of various types of security attacks in Mobile Agent based model and presented the security solutions for those type of attacks proposed by the various schemes and the open research issues in providing security for Mobile Agent based mobile computing system. Such classification enhances the understanding of the proposed security schemes in the mobile computing system, assists in the development and enhancement of schemes in the future and helps in choosing an appropriate scheme while implementing a mobile computing system.

Keywords: Mobile Ad-Hoc Network, Mobile Agent Model, Network Security.

I. INTRODUCTION

With the rapid growth in the wireless mobile communication technology, small devices like PDAs, laptops are able to communicate within motion. Because of its flexibility and provision of providing ubiquitous infrastructure, the need to provide security increases to a great degree. As wireless communication takes place mainly through the radio signals rather than wires, it is easier to intercept or eavesdrop on the communication channels. Therefore, it is important to provide security from all these threats. Mobile security or mobile phone security has become increasingly important in mobile computing. The security of personal and business information now stored on smartphones. There are still some technical obstacles that must be overcome before mobile networking can become widespread. The most fundamental is the security management, which is almost an afterthought until the recent years. Providing security services in the mobile computing environment is challenging because it is more vulnerable for intrusion and eavesdropping. Authentication mechanisms are designed to protect a system from unauthorized access to its resources and data.

II. METHODS AND MATERIAL

1. Classification of Mobile Computing System Security

We classify these schemes based on types the infrastructure used in the mobile computing system-Mobile Ad Hoc Networks (MANET) and Mobile Agent model.

Mobile Ad-hoc Network(MANET)

A Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary network without any centralized authority. In a MANET, each wireless mobile node operates not only as an end-system, but also as a router to forward packets.

Mobile Agent Model

A distributed mobile agent system model for a wireless internet host environment involves the following parties, mobile agents and fixed base stations. The Mobile Agent (MA) is a software component like a thread as in Telescript, that can migrate among different nodes carrying its execution state (i.e., program counter, call stack etc.).

2. Security Attacks in Manet

A MANET can be classified to active attacks and passive attacks.

Active attacks

Active attacks refer to the direct attacks by a hostile entity during execution or transmission phase.

Types of Active Attacks

Routing Attack

Routing attack is a major problem because nodes within the ad hoc network themselves performs routing functions and the security concepts are not incorporated in most of the routing protocols. Also, routing tables form the basis of network operations and any corruption to the routing table may lead to significant adverse con-sequences.

Some of the important and common methods of routing attacks are:

i) **Router Protocol Poisoning:** In this attack an intruder causes the disruption by poisoning the routing protocol.

ii) **Injecting incorrect information in the routing table:** In this type of routing attack, malicious nodes or an intruder would inject incorrect routing information, which in turn would poison the routing tables.

Active DoS Attacks

These attacks can be defined as the direct denial of service attacks on a node by another hostile node through packet flooding, packet modification, deletion or forging of packets or routing table**.**

Passive Attack

Passive attacks refer to the indirect attacks by an entity in the network during collaboration. Passive attacks could be caused by selfishness, eavesdropping and traffic analysis.

III. RESULTS AND DISCUSSION

1. Security Attacks In Mobile Agent

In the mobile agent-host model the security attacks or threats could be classified into four categories:

Mobile agent attacked by another mobile agent.

Mobile agent attacking by the host.

Host attacked by a mobile agent.

Host attacked by external unauthorized party like an agent or host.

2. MANET Security Schemes

MANET security work classified into two broad categories based on the type of attack: active attack or passive attack.

MANET Attack Prevention Security Schemes for Active attacks

In ad hoc networks, a mobile node or host may depend on other node(s) to route or forward a packet to its destination. The security of these nodes could be compromised by an external attacker or due to the selfish nature of other nodes. So the usual authentication and encryption methods would not apply to a MANET the same way they would in a wired network . However, both authentication and encryption are even more important in a MANET. For authentication and encryption, we use different models like Group key Diffie-Hellman (GDH) model, that provides a flexible solution to group key management. Public Key Infrastructure (PKI) technology. Maximum Degree Algorithm (MDA), for preventing denial of service due to poor key management

MANET Attack Prevention Security Schemes for Passive Attacks

Selfish nodes not performing their role properly in a MANET. Actions of a selfish node could lead to congestion, lower throughput and denial of service. Selfish node does not participate actively in packet forwarding in order to conserve electrical energy. to solve the selfish node problem, Michiardi et al. [39] have developed a model called CORE (Collaborative REputation). Under CORE's approach, every node monitors the behaviour of the neighboring nodes for a particular requested function and collects data about the execution of that function. If the observed result of the function matches with the expected result, then the observation takes a positive value. This mechanism al-lows a node to detect if any of its neighbors are selfish nodes and gradually isolate them.

3. Mobile Agent Security Schemes

Security Approaches for Mobile Agent Attacked by Another Agent

This scheme takes care of the unauthorized access, masquerade attacks, which is achieved through secret keys for secure communication with network and the other users.

It has some advantages like location and identification privacy in addition to just content privacy.

Security Approaches for Mobile Agent Attacked by the Host

Mobile code cryptography [21] provides solution through encrypted functions and digital signing. This proposal uses cryptographic primitives and homomorphic encryption schemes (public key) and function composition schemes. This solution tries to prove that mobile code holds the key to uncouple the secure execution of programs from the trustworthiness of the underlying execution support. This solution tries to prove that one can obtain a system where a host can execute an encrypted function without having to decrypt it. This scheme provide a solution for masquerade and eavesdropping attacks by host on agent. This is achieved with the help of cryptography and encrypting agent functions that are executed by the host.

Security Approaches for Host Attacked by Mobile Agents

Authentication protects host by preventing agent pretending as host. This is achieved through shared key for encryption messages or privacy. The issues that face this model are the authentication is needed whenever the agent traverses each new cell, especially with network partitions.

Security Approaches for Host Attacked by Other Unauthorized External Parties Including Host and Agents

Protection of dumb host by a scheme for authenticating host in a secure mobile network attempts to provide solution for masquerade and unauthorized attacks. This is achieved using a hierarchy of mobile agents and relies upon the computation priorities to determine which agent is to be active in each authentication request. This scheme proposes a hierarchical simulation model and analyse several factors involved in the computation of priorities, to determine the optimal weightings of each factor involved and the dependence.

IV. CONCLUSION

In this paper we have presented the taxonomy of security schemes for mobile computing systems. We have classified them based upon the infrastructure that makes up the mobile computing system and then by the type of attacks. The classification helps increasing our understanding of the security issues and requirements of the mobile computing and the schemes that could solve these issues and requirements. The taxonomy developed in this paper highlights the contributions for different types of attacks and shows the different types of approaches taken to provide security. This taxonomy should help researchers focus on underlying methods.

V. REFERENCES

[1] Y. Hu, D. B. Johnson and A. Perrig, "SEAD: Secure Effi-cient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proceedings of 4th IEEE Workshop on Mobile Computing Systems & Applications, New York, 2002, pp. 3-13.

[2] H. Reiser and G. Vogt, "Security Requirements for Man-agement Systems Using Mobile Agents," Proceedings of the 5th IEEE Symposium on Computers and Communica-tions, Antibes-Juan Les Pins, 2000, pp. 160-165.

[3] A. Fugetto, G. P. Pivvo and G. Vigna, "Understanding Code Mobility" IEEE Transactions on Software Engi-neering, Vol. 24, No. 5, 1998, pp. 342-361.

[4] D. Johansen, R. V. Renessee and F. B. Schneider, "An Introduction to the TACOMA Distributed System-Version 1.0," Technical Report, Department of Computer Science, University of Tromso and Cornell University, 1995.