IMPLEMENTATION OF EFFICIENT PROTECTION FOR MOBILE AGENTS AGAINST MALICIOUS HOSTS

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

In

COMPUTER AND INFORMATION SCIENCES

By

Marwa Mohamed Essam

Supervisors

Prof. Dr. Mohamed Said Abdel-Wahab

Prof. Dr. Mohamed Ali El-Sharkawy

FACULTY OF COMPUTER AND INFORMATION SCIENCES

AIN-SHAMS UNIVERSITY

Acknowledgment

I would like to express my deep gratitude to the dean of my faculty, Prof. Dr. Mohamed Essam Khalifa, for his encouragement, advice and fundamental support throughout my work in this thesis.

I would also like to thank Prof. Dr. Mohamed Hashem, the head of the Information Systems department, for his useful discussions, comments and invaluable advice on mobile agents and security.

Sincere thanks go to my supervisor, Prof. Dr. Mohamed Said Abdul-Wahab, for the time and effort he devoted to me, for helping me in structuring this work, for ideas and suggestions and for great encouragement.

I am also indebted to my supervisor, Prof. Dr. Mohamed Ali El- Sharkawy for all the comments and help, for sharing his expertise and knowledge and for the great support throughout this work.

Last but not least, this thesis would not have been written if not for my family's unwavering support throughout these years. I am especially grateful for them for their continued belief in my abilities and their encouragement throughout every step of the way.

Abstract

Free-roaming mobile agents have evoked strong interest due to the enormous potential they extend to distributed systems programming. However, it is generally agreed that without the proper security for an agent against a potentially malicious executing host, the use of agent-based applications will be severely impeded. Several models have been proposed to secure free-roaming agents. One class of these models tries to detect the tampering on the agent's data using the concept of partial results encapsulation. That is to securely save the results of an agent's actions, at each platform visited, for subsequent verification when the agent returns to his point of origination.

In this thesis, we proceed to propose a new mobile agent security approach that aims to provide both data integrity and confidentiality through partial results encapsulation. The basic idea in the proposed approach is to incorporate a trusted server in the mobile agent system to discourage and detect bad behavior by malicious hosts. The trusted server will act as the controller of the mobile agent execution process. It will force each execution host to encapsulate its computational results without compromising the agent's security.

We present two different execution models for our trusted-server based approach: In the first model; named the

Trusted-Entity based Agent Protection Approach (TEAPA), the agent execution process is totally controlled by the trusted server. The server is responsible of sending the mobile agents on behalf of their owners. It is also responsible of detecting the manipulation in the agent's collected results. In the second execution model; named the modified- TEAPA (M-TEAPA), the dependency on the trusted server is reduced by using it only to authenticate the visited hosts and allowing the agent's owner itself to test the collected results for tampering detection.

In the data encapsulation phase in the two proposed execution models, the agent constructs a symmetric encryption key at each visited host and uses that key to encrypt and encapsulate the obtained results. The construction of an encryption key at any host builds a chaining relation that links that key forwards to the host's successor and backwards to all the previously constructed keys.

We proved through security analysis that having the trusted server in the system and adopting the chaining relation in creating the encryption keys enabled the proposed security approach to satisfy most of the security requirements for mobile agent's data integrity protection. We also proved by experiments that the new approach outperforms the previous partial results encapsulation models in terms of the time needed for securing the results and the encapsulation size overhead.

Table of Contents

List of Figures

1 Introduction

2 Background on Mobile Agents

3 Data Integrity of Mobile Agents

4 Partial Results Encapsulation Models

5 The Proposed Data Encapsulation Approach

List of Tables

4 Partial Results Encapsulation Models

5 The Proposed Data Encapsulation Approach

List of Abbreviations

COD	Code On Demand
DES	Data Encryption Standard algorithm
DSA	Digital Signature Algorithm
M-TEAPA	Modified Trusted-Entity based Agent Protection Approach
OKGS	One-time Key Generation System
OTCM	One-hop forwards Two-hop backwards Chaining Model
PKI	Public Key Infrastructure
PRE	Partial Results Encapsulation
PVCSP	Publicly Verifiable Chained Signature Protocol
PVDS-CS	Publicly Verifiable Digital Signature with Co-Signing
RASPS	Random Access Stored Program plus Stack machine
REV	Remote Evaluation
RPC	Remote Procedure Call
RSA	An encryption algorithm named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman
TEAPA	Trusted-Entity based Agent Protection Approach
WFMS	Work Flow Management System

Chapter 1

Introduction

1.1 Overview

In recent years the inter-networking and communication infrastructure has steadily increased. Today the Internet allows even the smallest company to do business on a global scale. As the density and capacity of the internet will continue to expand, the amount of available on-line information will expand as well. The issue of how to efficiently find, gather and retrieve this information has led to the research and development of systems and tools that attempt to provide a solution to this problem. These systems and tools are based on the use of mobile agents [1].

A mobile agent is an executing program, capable of migrating from host to host within an agent enabled network. The agent can suspend execution on its originator, transfer itself with code and data to another host and resume execution there (Figure 1.1). The mobile agent is firstly created on some machine, and it is dispatched to a remote host for execution. The accommodating host would provide suitable runtime environment for the piece of software, the mobile agent, to execute. The mobile agent would execute, collect host-specific information, and generate runtime states and variables ready to migrate to another host. This process continues until the mobile agent returns to the first machine that sent him with useful information gathered through his visits to other hosts.

The mobile agent migrates to the host and performs computations on the host, thereby reducing communication

costs. This is in contrast to the client/server paradigm where the clients and the server exchange information via remote procedure calls or other messaging systems. The mobile agent paradigm promises to open up exciting computing possibilities, especially with the popularity of wireless networks where bandwidth is at a premium and communication links are not always reliable. Some of the possible applications of mobile agents are in the areas of Electronic Commerce, Distributed System Management and Workflow System Management.

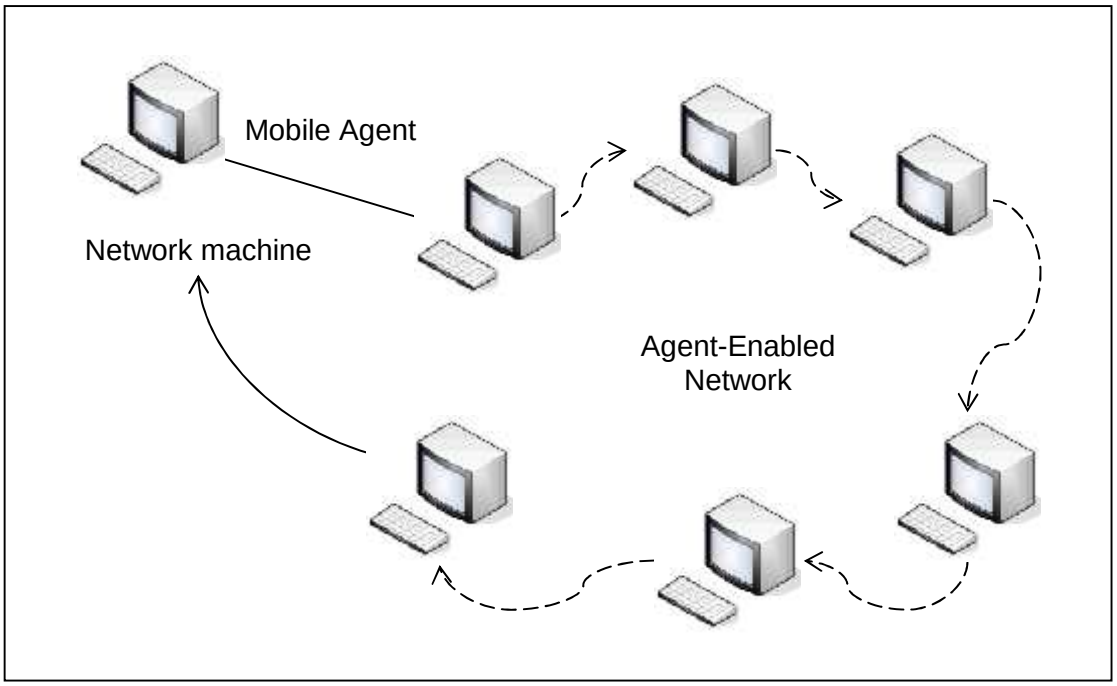

Figure 1.1 The Mobile Agent Paradigm

1.2 Security in mobile agent systems

Significant research and development into mobile agents have been conducted in recent years. Yet, because of some