ĐẠI HỌC THÁI NGUYÊN
ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NGUYỄN THỊ HẢI AN

BẢO MẬT TRONG MOBILE AGENT VÀ ỨNG DỤNG TRONG CÁC GIAO DỊCH ĐIỆN TỬ

LUẬN VĂN THẠC SỸ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN – 2014

ĐẠI HỌC THÁI NGUYÊN
ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

NGUYỄN THỊ HẢI AN

BẢO MẬT TRONG MOBILE AGENT VÀ ỨNG DỤNG TRONG CÁC GIAO DỊCH ĐIỆN TỬ

Chuyên ngành : KHOA HỌC MÁY TÍNH
Mã số : 60 48 01

LUẬN VĂN THẠC SỸ KHOA HỌC MÁY TÍNH
NGƯỜI HƯỚNG DẪN KHOA HỌC : TS. PHẠM THẾ QUẾ

THÁI NGUYÊN – 2014

LỜI CAM ĐOAN

Tôi cam đoan đây là công trình nghiên cứu của riêng tôi.

Các số liệu, kết quả nêu trong luận văn là trung thực và chưa từng được ai công bố trong bất kỳ công trình nào khác.

Tác giả luận văn

Nguyễn Thị Hải An

MỤC LỤC

LỜI CAM ĐOAN
.....**Error! Bookmark not defined.**
MỤC LỤC 4
DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT 7
DANH MỤC CÁC HÌNH 8
MỞ ĐẦU 9
CHƯƠNG 1 : TỔNG QUAN VỀ MOBILE AGENT.....10
1.1 KHÁI NIỆM VỀ MOBILE AGENT.....10
1.1.1 Giới thiệu chung 10
1.1.2 Mobile Agent là gì.....10
1.1.3 Phát triển từ các mô hình ứng dụng phân tán.....11
1.1.4 Mục đích thiết kế mô hình Mobile Agent 14
1.2 CÁC ĐẶC TRƯNG KỸ THUẬT CỦA MOBILE AGENT.....16
1.2.1 Kiến trúc hệ thống Mobile Agent.....16
1.2.2 Các đặc tính của Mobile Agent 18
1.2.3 Các thành phần của một Mobile Agent.....19
1.2.4 Các nền tàng một Mobile Agent.....21
1.3 NGUYÊN LÝ HOẠT ĐỘNG CỦA MOBILE AGENT.....22
1.3.1 Kỹ thuật pull code 22
1.3.2 Kỹ thuật push code 22
1.4 MOBILE AGENT TRONG THIẾT KẾ ỨNG DỤNG PHÂN TÁN.....24
1.4.1 Vòng đời của một Mobile Agent.....24
1.4.2 Tạo Agent 25
1.4.3 Huỷ Agent.....26
1.4.4 Di chuyển Agent.....26
1.4.5 Liên lạc 29
1.5 CÔNG CỤ PHÁT TRIỂN MOBILE AGENT 30
1.5.1 Java – ngôn ngữ hiệu quả dùng để phát triển tác tử 30
1.5.2 Công cụ phát triển Aglets Workbench. 31
1.6 LỢI ÍCH MOBILE AGENT.....32
1.6.1 Giảm lưu lượng tải trên mạng 33
1.6.2 Khắc phục độ trễ mạng.....33
1.6.3 Đóng gói các giao thức.....33
1.6.4 Thi hành một cách không đồng bộ và tự trị.....33
1.6.5 Thích ứng nhanh.....34
1.6.6 Khắc phục tình trạng không đồng nhất 34
1.6.7 Mạnh mẽ và có khả năng tự sửa lỗi.....34
1.7 MỘT SỐ ỨNG DỤNG MOBILE AGENT.....34

1.7.1 Thu thập thông tin phân tán 34
1.7.2 Tìm kiếm và lọc dữ liệu 35
1.7.3 Kiểm tra dữ liệu (Monitoring) 35
1.7.4 Đàm phán 35
1.7.5 Đặt hàng 36
1.7.6 Giải trí 36
1.7.7 Thương mại điện tử 36
1.7.8 Hỗ trợ các thiết bị di động 36
Kết luận chương: 37
CHƯƠNG 2: NHỮNG VẤN ĐỀ BẢO MẬT TRONG MOBILE AGENT 38
2.1 Đặt vấn đề 38
2.2 Các phương thức tấn công trong mobile agent 38
2.2.1 Các dạng tấn công tiêu cực 38
2.2.2 Các dạng tấn công tích cực 39
2.3 Những trường hợp có thể gây lỗi. 42
2.3.1 Sự bảo vệ agent 42
2.3.2 Sự bảo vệ máy phục vụ 42
2.3.3 Sự bảo vệ hệ thống mạng 43
2.4 Các dịch vụ an toàn 43
2.4.1 Xác nhận 43
2.4.2 Tính toàn vẹn 43
2.4.3 Bảo mật 44
2.4.4 Cấp phép 44
2.4.5 Không chối bỏ 44
2.4.6 Kiểm toán 44
2.5 Các vấn đề liên quan đến sự bảo vệ agent 44
2.5.1 Sự thi hành agent 45
2.5.2 Các thông tin agent cần bảo mật đối với server 45
2.5.3 Các thông tin của agent cần được bảo mật với các agent khác 45
2.6 Các vấn đề liên quan đến sự bảo vệ máy chủ 46
2.6.1 Agent giả dạng như là một người dùng được tin tưởng 46
2.6.2 Agent bị can thiệp, xâm phạm 46
2.6.3 Agent vượt quá quyền hạn của nó và làm hại đến server 47
2.7 Mô hình an toàn của Aglet. 47
2.7.1 Các chủ sở hữu 47
2.7.2 Sự cấp phép 49
2.7.3 Các biện pháp bảo vệ 50
2.7.4 Chính sách an toàn và thi hành 50
2.8 Các giải pháp an toàn trong Internet Banking 52
2.8.1 Xây dựng hệ thống xác thực mạnh 52

2.8.2 Cơ bản về tường lửa.....55
2.8.3 Xây dựng hệ thống phòng chống xâm nhập.....60
2.8.4 Xây dựng lửa ứng dụng web (Web Application Firewall WAF).....64
2.8.5 Triển khai hệ thống phòng chống mã độc.....66
2.8.6 Triển khai chữ ký số và chứng thực số.....70
2.8.7 Mã hóa thông tin.....71
2.8.8 Triển khai các phương pháp bảo vệ dữ liệu ở người dùng cuối.....73
2.8.9 Triển khai mạng riêng ảo VPN.....75
Kết luận chương.....76
CHƯƠNG 3 : THƯƠNG MẠI ĐIỆN TỬ VÀ ỨNG DỤNG MOBILE AGENT TRONG THANH TOÁN ĐIỆN TỬ.....78
3.1 Thanh toán điện tử và các mô hình thanh toán điện tử.....78
3.1.1 Giới thiệu về thanh toán và các vấn đề đặt ra đối với thanh toán điện tử.....78
3.1.2. Các hệ thống thanh toán trực tuyến.....78
3.2. Mobile agent trong thương mại điện tử.....79
3.2.1. Bảo mật trong giao dịch mua bán trực tuyến.....79
3.2.2 Bảo mật trong giao dịch đấu giá trực tuyến.....83
3.3 Bảo mật trong giao dịch thanh toán qua mạng.....85
3.3.1. Một mô hình thanh toán điện tử dựa trên Agent - The Secure Agent Fabrication, Evolution & Roaming (SAFER).....86
3.3.2. Hệ thống thanh toán hóa đơn nhà hàng dựa trên Mobile Agent.....86
3.3.3 Giao thức thanh toán sử dụng Mobile Agent.....86
3.4. Sử dụng Aglet cài đặt ví dụ thanh toán điện tử.....87
Kết luận chương.....89
KẾT LUẬN.....91
TÀI LIỆU THAM KHẢO.....93

DANH MỤC CÁC KÝ HIỆU, CÁC CHỮ VIẾT TẮT

STT	Chữ viết tắt	Tiếng Anh
1	**ACL**	Agent Communication Language
2	**ASDK**	Aglets Software Development Kit
3	**ATP**	Agent Transfer Protocol
4	**CORBA**	Common Object Request Broker Architecture
5	**DES**	Data Encryption Standard
6	**KQML**	Knownledge Query and Manipulation Language
7	**MA**	Mobile Agent
8	**MAE**	Mobile Agent Environment
9	**REV**	Remote Evaluation
10	**RMI**	Remote Method Invocation
11	**RPC**	Remote Procedure Call
12	**SA**	Service Agent
13	**SSL**	Secure Socket Layer
14	**TTP**	Trusted Third Party
15	**US**	User Agent

DANH MỤC CÁC HÌNH

Số hiệu hình vẽ	Tên hình vẽ	Trang
Hình 1.1.	Sự khác phát triển các phương thức truy nhập từ xa	11
Hình 1.2.	So sánh Client/Server với Mobile Agent	12
Hình 1.3.	So sánh Jini với Mobile Agent	13
Hình 1.4.	Sự khác biệt của Mobile Agents so với RPC, REV,COD	15
Hình 1.5.	Tổng quát kiến trúc Mobile Agent	17
Hình 1.6.	Các thành phần của một hệ thống Mobile Agent	19
Hình 1.7.	Place và Bộ vi xử lý	21
Hình 1.8.	Vòng đời của một Mobile Agent	25
Hình 1.9.	Di chuyển Agent trên mạng	28
Hình 1.10.	Di chuyển lớp của Agent	29
Hình 1.11.	Thông báo kiểu Now	30
Hình 1.12.	Thông báo kiểu Future	30
Hình 1.13.	Thông báo kiểu one - way	30
Hình 1.14.	Mô hình vòng đời và hoạt động	33
Hình 2.1.	Dạng nghe trộm	41
Hình 2.2.	Dạng giả mạo	42
Hình 2.3.	Dạng Trojan	42
Hình 2.4.	Dạng sửa đổi	43
Hình 2.5.	Dạng làm lại	43
Hình 3.1.	Mô hình thương mại điện tử sử dụng mobile agent	59
Hình 3.2.	Sơ đồ hoạt động của hệ thống	61
Hình 3.3.	Tổng quan về hệ thống đấu giá	62
Hình 3.4.	Các dịch vụ bảo mật nền tảng	63
Hình 3.5.	Lớp bảo mật mobile agent	64
Hình 3.6 a.	Giao diện : Chức năng Đặt vé	67
Hình 3.6 b	Giao diện : Chức năng chọn Điểm đi – Điểm đến	67
Hình 3.7 a.	Giao diện : Chức năng Thanh toán	68
Hình 3.7 b	Giao diện : Nhập mã bảo mật cho giao dịch thanh toán	68
Hình 3.8.	Giao diện : Thông báo Giao dịch thanh toán thành công	69

MỞ ĐẦU

Sự phát triển nhanh chóng của các kỹ thuật tiên tiến về máy tính, đặc biệt là các giải pháp mạng, cùng với sự bùng nổ mạnh mẽ các dịch vụ và nguồn thông tin trên mạng đã làm gia tăng số người sử dụng Internet đến con số hàng trăm triệu người. Dựa vào nền tảng đó, lĩnh vực thương mại điện tử đã phát triển nhanh chóng để phục vụ tốt hơn cho người mua và người bán trong giao dịch hàng hóa.

Tuy nhiên, các giao dịch này cần được bảo mật để đảm bảo lợi ích cho người bán hàng và người mua hàng. Việc bảo mật này nhằm ngăn chặn bên thứ 3 tác động vào giao dịch và đảm bảo giao dịch được hoàn thành một cách chính xác. Từ đó tránh được thiệt hại về kinh tế cho họ.

Để hiểu thêm về vấn đề này, em chọn đề tài "**Bảo mật trong mobile agent và ứng dụng trong các giao dịch điện tử_ Mobile agent security and electronic transactions applications"** nhằm nắm được những khái niệm cơ bản về mobile agent đồng thời đề cập đến vấn đề bảo mật trong mobile agent và đi vào chi tiết ứng dụng của bảo mật mobile agent trong các giao dịch điện tử.

CHƯƠNG 1 : TỔNG QUAN VỀ MOBILE AGENT

1.1 KHÁI NIỆM VỀ MOBILE AGENT

1.1.1 *Giới thiệu chung*

Với sự phát triển của Internet, đứng trước sự bùng nổ về thông tin, người dùng có thể tiếp cận và khai thác nguồn thông tin khổng lồ, phong phú, đa dạng và phân tán khắp nơi trên mạng. Tuy nhiên, để có thể khai thác một cách có hiệu quả nguồn tài nguyên này, người dùng cần phải biết thông tin mình cần nằm ở đâu và làm thế nào để tìm ra nó. Do đó các phần mềm hỗ trợ người dùng ngày nay phải có khả năng hoạt động độc lập không cần sự can thiệp thường xuyên của con người và duy trì hoạt động liên tục cho đến khi đạt được kết quả.

Các ứng dụng phải có khả năng xử lý phân tán: Các ứng dụng ngày nay cần phải có khả năng trao đổi, liên lạc với các thành phần xử lý khác được phân bố trên nhiều máy có cấu hình khác nhau trong mạng để có thể tận dụng được toàn bộ tài nguyên của hệ thông. Ví dụ, một chương trình xử lý văn bản có thể sử dụng một thành phần xử lý trên máy A để phục vụ cho chức năng soạn thảo, trong khi lại sử dụng một thành phần xử lý khác trên máy B cho chức năng kiểm lỗi chính tả.

Môi trường làm việc không đồng nhất : Internet kết nối hàng triệu triệu máy tính lại với nhau, mỗi máy tính có các cấu hình khác nhau về phần cứng cũng như hệ điều hành và các phần mềm ứng dụng. Do đó thật không đơn giản khi một chương trình có thể chạy trên một máy bất kỳ trên mạng.

Sự đa dạng của các kết nối mạng : Các mạng cục bộ kết nối băng thông rộng, nhanh và tin cậy. Trong khi các máy di động có các kết nối chậm hơn , không thường xuyên, thiếu tin cậy. Một ứng dụng có thể làm việc được trên các kết nối mạng như vậy phải chiếm ít đường truyền mạng và có khả năng làm việc không đồng bộ (off-line).

Vấn đề an toàn: Thông tin lưu truyền trên mạng rất dễ bị đánh cắp, cũng như bị sửa đổi, giả mạo, ... Do đó cần phải các cơ chế an toàn để có thể tăng tính tin cậy của các ứng dụng trên mạng.

1.1.2 *Mobile Agent là gì*

Mobile Agent là mô hình tiến hóa tiên tiến nhất so với các mô hình trước đó. Mobile Agent là danh từ ghép giữa Agent (tác tử) và Mobile (di động). Một Mobile Agent là một phần mềm, bao gồm mã chương trình, dữ liệu và trạng thái hoạt động có