ĐẠI HỌC THÁI NGUYÊN
TR- ỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

TRẦN THU HIỀN DỊU

NGHIÊN CỨU GIẢI PHÁP BẢO MẬT THƯ ĐIỆN TỬ TRÊN HỆ MÃ NGUỒN MỞ

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

THÁI NGUYÊN - NĂM 2014

LỜI CAM ĐOAN

Tôi cam đoan luận văn này là do bản thân nghiên cứu và thực hiện theo sự hướng dẫn khoa học của thầy giáo **TS. Hồ Văn Hương**.

Tôi hoàn toàn chịu trách nhiệm về tính pháp lý quá trình nghiên cứu khoa học của luận văn này.

Thái Nguyên, ngày 29 tháng 09 năm 2014

Người cam đoan

Trần Thu Hiền Dịu

LỜI CẢM ƠN

Trước tiên em xin chân thành cảm ơn thày giáo **TS.Hồ Văn Hương** công tác tại **Ban Cơ yếu Chính phủ** đã tận tình hướng dẫn, giúp đỡ, chỉ bảo và luôn tạo điều kiện cho em hoàn thành luận văn này.

Em xin chân thành cảm ơn các thày, các cô trong trường **Đại Học Công Nghệ Thông Tin và Truyền Thông Thái Nguyên và Viện Công Nghệ Thông Tin** đã giảng dạy, giúp đỡ và tạo điều kiện thuận lợi cho em trong suốt thời gian học tập tại trường.

Em xin gửi lời cảm ơn tới các bác, các chú và các anh chị công tác tại **Công Ty ECOIT** đã cho em một môi trường rất tốt để em được thực tập, học hỏi trong suốt quá trình thực tập và nghiên cứu luận văn tốt nghiệp.

Em đã cố gắng để hoàn thành luận văn trong phạm vi và khả năng cho phép nhưng chắc chắn sẽ không tránh khỏi những khiếm khuyết. Em rất mong nhận được sự cảm thông và tận tình chỉ bảo, nhận xét đóng góp ý kiến quý báu của quý thày cô.

Thái Nguyên, ngày 29 tháng 09 năm 2014

Tác giả luận văn

Trần Thu Hiền Dịu

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

CA	Certificate Authority
CRC	Cyclic Redundancy Check
DNS	Domain Name System
HĐH	Hệ điều hành
IMAP	Internet Message Access Protocol
MTA	Message Transfer Agent
MD	Message Digest
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
POP	Post Office Protocol
RA	Registration Authority
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
S/MIME	Secure/Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
ZCS	Zimbra Collaboration Suite

DANH MỤC CÁC HÌNH VẼ

MỞ ĐẦU

Lý do chọn đề tài

Trong những năm gần đây, Internet phát triển mạnh mẽ và đã trở thành nền tảng chính cho sự trao đổi thông tin trên toàn cầu. Nhờ có Internet mà việc trao đổi thông tin cũng được trở nên tiện lợi và nhanh chóng hơn. Các thông tin nhạy cảm và quan trọng cũng được lưu trữ và trao đổi dưới hình thức điện tử. Chính vì thế nguy cơ lừa đảo, can thiệp, tấn công, phá hoại và ăn cắp thông tin ngày càng trở nên nghiêm trọng và nhu cầu sử dụng mật mã càng cao. Mật mã không chỉ đơn thuần phục vụ cho chính phủ, cho quân đội…mà nó còn được sử dụng cho mọi người để đảm bảo tính riêng tư của mỗi người. Hiện nay, nhu cầu trao đổi thông tin được phát triển rộng khắp, một trong những phương thức phổ biến nhất trên Internet đó là thư điện tử (email), thư điện tử giúp mọi người sử dụng máy tính kết nối Internet có thể trao đổi thông tin với nhau. Do đó, có một số yêu cầu được đặt ra đối với việc trao đổi thông tin trên mạng:

- Bảo mật tuyệt đối thông tin trong giao dịch.
- Đảm bảo tính toàn vẹn của thông tin.
- Chứng thực được tính đúng đắn về pháp lí của thực thể tham gia trao đổi thông tin.

Từ những yêu cầu trên vấn đề đặt ra là cần có phương pháp bảo mật thông tin nhằm cải thiện an toàn trên Internet. Việc tìm ra giải pháp bảo mật dữ liệu, cũng như việc chứng nhận quyền sở hữu của cá nhân là một vấn đề luôn luôn mới. Bảo mật phải được nghiên cứu và cải tiến để theo kịp sự phát triển không ngừng của cuộc sống.

- Làm thế nào để bảo mật dữ liệu?
- Làm sao để tin tức truyền đi không bị mất mát hay bị đánh tráo?

- Làm sao để người nhận biết được thông tin mà họ nhận được có chính xác hay không? đã bị thay đổi gì chưa?

- Làm sao để biết được thông tin này do ai gửi đến? thuộc quyền sở hữu của ai?

Những câu hỏi được đặt ra là một thách thức rất lớn đối với những người nghiên cứu bảo mật. Có rất nhiều cách thức để bảo vệ thông tin trên đường truyền, nhiều giải pháp được đề xuất như: Sử dụng mật khẩu, mã hóa dữ liệu, hay giấu sự tồn tại của dữ liệu…cùng với sự phát triển của các biện pháp bảo mật ngày càng phức tạp, thì các hình thức tấn công ngày càng tinh vi hơn, do đó vấn đề là làm sao đưa ra một giải pháp thích hợp và có hiệu quả theo thời gian và sự phát triển mạnh mẽ của khoa học kỹ thuật.

Với mong muốn nghiên cứu tìm hiểu giải pháp bảo mật cho thư điện tử em đã quyết định lựa chọn đề tài : *"**Nghiên cứu giải pháp bảo mật thư điện tử trên hệ mã nguồn mở** "*.

Đối tượng và phạm vi nghiên cứu

Đối tượng và phạm vi nghiên cứu của đề tài:

- Tổng quan về thư điện tử
- Tìm hiểu về hệ điều hành mã nguồn mở
- Tìm hiểu về lý thuyết mật mã
- Tìm hiểu các giải pháp bảo mật thư điện tử
- Xây dựng ứng dụng chữ ký số trong bảo mật thư điện tử với hệ thống thư điện tử Zimbra Mail Server.

Hướng nghiên cứu của đề tài.

Đề tài tập trung tìm hiểu, nghiên cứu về thư điện tử, xây dựng ứng dụng chữ ký số trong bảo mật thư điện tử trên hệ thống Zimbra Mail Server để ký số, mã hóa, giải mã và xác thực mail.

Những nội dung chính nghiên cứu

Luận văn gồm 3 chương tập trung nghiên cứu những nội dung chính sau:

Chương 1. Tổng quan về an toàn thư tín điện tử

Chương 2. Bảo mật thư điện tử dựa trên mã hóa

Chương 3. Xây dựng phần mềm demo bảo mật thư tín điện tử

Ý nghĩa khoa học của đề tài

Xây dựng và triển khai ứng dụng chữ ký số trong bảo mật thư điện tử tích hợp trên hệ thống thư điện tử Zimbra Mail Server: Cài đặt hệ thống Zimbra Mail Server, tích hợp bảo mật trên hệ thống Zimbra gồm các nhiệm vụ là gửi thư mã hóa, thư kèm chữ ký, giải mã thư mã hóa, và xác thực người gửi.