ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

TẠ THỊ THÙY LINH

NGHIÊN CỨU TÌM HIỂU HẠ TẦNG CƠ SỞ KHÓA CÔNG KHAI DỰA TRÊN DẤU HIỆU SINH TRẮC HỌC VÀ ỨNG DỤNG

Chuyên ngành : Khoa học máy tính

Mã số : 60.48.01

Thái Nguyên 2012

MỤC LỤC

Trang

LỜI MỞ ĐẦU

Trong kỷ nguyên của công nghệ thông tin, với sự phát triển mạnh mẽ, rộng rãi và phổ biến của Internet một mặt nó đem lại cho con người nhiều ứng dụng tiện lợi, các hoạt động truyền thống trong thế giới thực đang dần được số hóa. Mặt khác nó đặt ra nhiều vấn đề về sự an toàn, an ninh và tính tin cậy của những giao dịch trên Internet. Người dùng vẫn luôn cảm thấy không an toàn khi thực hiện các giao dịch trên mạng khi mà hàng loạt tội phạm máy tính như lừa đảo, phá hoại, vi phạm bí mật riêng tư ngày càng phát triển tinh vi và phức tạp. Chẳng hạn khi gửi một mẫu tin có thể là: văn bản, giọng nói, hình ảnh, phim video…Người nhận có quyền nghi ngờ: thông tin đó có phải là của đối tác không, nó có bị ai xâm phạm, và nó đã bị ai giải mã chưa …Những thử thách này đã thu hút sự chú ý của nhiều nhà khoa học trong lĩnh vực nghiên cứu về mật mã để bảo mật thông tin.

Năm 1976, hệ mật mã khó a công khai (Public key) ra đời là một cuộc cách mạng trong bước tiến của ngành mật mã . Ở đây người ta đã giải quyết được vấn đề trao đổi khoá , ký số cũng như xác thực thông điệp mà ở hệ mật mã khoá bí mật chưa giải quyết được . Trong mật mã khoá công khai , một khoá dùng để mã hoá thì được công khai hoàn toàn gọi là khoá công khai , một khoá dùng để giải mã thì được giữ bí mật không cần phải phân phối hay trao đổi gọi là khoá bí mật . Quan hệ giữa khoá công khai và khoá bí mật là quan hệ 1-1, nhưng biết được khoá này thì rất khó để suy ra khoá kia và ngược lại. Vấn đề đặt ra là việc sinh ra các cặp khoá công khai/bí mật như thế nào, làm sao để quản lý và phân phối được khoá công khai, làm sao để để đảm bảo an toàn , xác thực được thông tin của người gửi đến đúng địa chỉ người nhận trong một xã hội có hàng trăm triệu người ? Những khó khăn trên sẽ được giải quyết bởi một tổ chức gọi là cơ sở hạ tầng khoá công khai PKI (Public key Infrastracture). PKI đảm bảo sự an toàn, thông suốt cho các giao dịch điện tử, đảm bảo sự tin cậy cho các trao đổi thông tin nhạy cảm giữa các tổ chức cho dù mỗi liên hệ kinh doanh giữa họ trước đó còn chưa được thiết lập. PKI chính là bộ khung

của các chính sách, dịch vụ và phần mềm mã hóa, đáp ứng nhu cầu bảo mật, an toàn cho người sử dụng.

Tuy nhiên một vấn đề then chốt của PKI là bảo vệ khóa cá nhân do nó dễ bị lộ hoặc đánh cắp. Chính vì vậy một hướng nghiên cứu nhằm giải quyết vấn đề trên là tích hợp các dấu hiệu sinh trắc học vào hạ tầng khóa công khai PKI gọi là BioPKI (Biometrics Public Key Infrastructure). Sinh trắc học là các đặc điểm về sinh học hay các đặc trưng riêng của con người như khuôn mặt, vân tay, giọng nói, dáng điệu, chiều cao... Đây là những thông tin mang tính duy nhất của mỗi cá nhân, do vậy không thể bị ăn cắp cũng như giả mạo. Hiện nay dấu hiệu sinh trắc học vân tay đang được sử dụng rộng rãi nhất và có tính tin cậy cao. Theo hướng nghiên cứu này hệ thống BioPKI không chỉ vượt qua được các hạn chế về bảo mật của hệ PKI mà còn có khả năng thẩm định xác thực người dùng.

Xuất phát từ những vấn đề trên, em đã chọn đề tài **"Nghiên cứu tìm hiểu cơ sở hạ tầng khóa công khai dựa trên dấu hiệu sinh trắc học và ứng dụng**" làm chủ đề cho việc nghiên cứu trong luận văn của mình. Đối với Việt Nam ta thì đây là những vấn đề còn mới nên chưa có nhiều tài liệu trong nước . Do đó chắc chắn nội dung đề tài luận văn còn nhiều thiếu sót , em mong được các thầy cô góp ý để luận văn được hoàn chỉnh hơn.

1. Mục tiêu và nhiệm vụ nghiên cứu của đề tài

Luận văn tập trung nghiên cứu tìm hiểu các thành phần, mô hình và các dịch vụ lõi của PKI, bước đầu nghiên cứu khảo sát hệ thống BioPKI và các giải pháp tiếp cận hệ thống BioPKI; tìm hiểu mô hình chữ ký số và ứng dụng chữ ký số trong bài toán xác thực bảng điểm.

2. Ý nghĩa khoa học của đề tài:

Những nội dung nghiên cứu của đề tài một mặt trình bày khái quát về thực trạng ứng dụng thương mại điện tử ở thế giới và Việt Nam và nhu cầu cấp thiết về thiết lập môi trường an ninh đảm bảo an toàn cho các giao dịch điện tử trên internet hiện nay. Trong luận văn trình bày những kiến thức cơ bản về hạ tầng cơ sở khóa công khai PKI và giải pháp cơ sở hạ tầng khóa công khai dựa trên dấu hiệu sinh trắc học BioPKI. Với hệ thống BioPKI, sử dụng dấu hiệu sinh trắc học vân tay là một

giải pháp khả thi và giải quyết vấn được vấn đề mấu chốt về bảo vệ khóa cá nhân trong hệ thống PKI. Kết quả nghiên cứu bước đầu về hệ thống BioPKI và chương trình thử nghiệm về ứng dụng chữ ký số tạo cơ sở để tiếp tục nghiên cứu và cải tiến giải pháp an toàn thông tin trong tương lai dựa trên mô hình ứng dụng tích hợp dấu hiệu sinh trắc học vào các thiết bị kỹ thuật nhằm tăng cường an toàn cho các giao dịch điện tử. Đó là nhu cầu và cũng là nhiệm vụ có tính chất then chốt trong công cuộc xây dựng và phát triển bền vững toàn diện các ngành kinh tể quốc dân, thực hiện công nghiệp hóa – hiện đại hóa đất nước, hội nhập quốc tế và đầu tư nước ngoài.

3. Phương pháp nghiên cứu:

Phương pháp nghiên cứu chủ yếu của luận văn là tra cứu, phân tích, tổng hợp, nội dung các tài liệu tham khảo, các bài báo khoa học liên quan đến nội dung nghiên cứu của đề tài được công bố trong những năm gần đây kết hợp với phương pháp cài đặt, thử nghiệm chương trình và đánh giá.

4. Phạm vi nghiên cứu:

- Phạm vi nghiên của luận văn khảo sát thực trạng giao dịch điện tử, nhu cầu các giải pháp về an toàn thông tin ở Việt Nam; nghiên cứu giải pháp hạ tầng khóa công khai PKI như các mô hình và giải pháp triển khai PKI ở Việt Nam; thuật toán RSA; ELGAMAL, chữ ký số; khảo sát hệ thống an ninh BioPKI dựa trên dấu hiệu sinh trắc và phân tích một số giải pháp tích hợp dấu hiệu sinh trắc trong hệ thống BioPKI;
- Do hạn chế nhất định về cơ sở vật chất và điều kiện tiếp cận thực tế với lĩnh vực an toàn bảo mật thông tin trong giao dịch điện tử nên việc cài đặt chương trình ứng dụng chỉ mang tính thử nghiệm.

5. Bố cục của luận văn

Ngoài phần mở đầu và kết luận, luận văn được tổ chức thành 3 chương như sau:

Chương 1: Khảo sát thực trạng ứng dụng thương mại điện tử và hệ thống an ninh BioPKI, khả năng triển khai – vân tay, thẻ thông minh ở Việt Nam.

Khảo sát thực trạng ứng dụng thương mại điện tử ở trên thế giới nói chung và ở Việt Nam nói riêng, tìm hiểu một số vấn đề cản trở sự phát triển của TMĐT ở

Việt Nam; khảo sát hệ thống BioPKI, khả năng triển khai thẻ thông minh ở Việt Nam; tìm hiểu hệ thống cơ sở pháp lý cho giao dịch điện tử. Từ thực trạng đó đề tài tiếp tục tìm hiểu một cách khái quát về các giải pháp công nghệ bảo mật an toàn thông tin và an ninh mạng hiện nay.

Chương 2: Hạ tầng khóa công khai – PKI và mô hình triển khai hệ thống PKI tại Việt Nam.

Trong chương này trình bày tổng quan về lý thuyết mật mã, hệ mật mã bí mật, hệ mật mã công khai, khái niệm, thuật toán hệ RSA, ELGAMAL. Đề tài đi sâu vào nghiên cứu hạ tầng cơ sở khóa công khai PKI với những chức năng, thành phần, các mô hình, dịch vụ về chữ ký số, chứng chỉ số....giúp ta nhận thấy được tại sao chúng ta phải xây dựng hệ thống PKI.

Tiếp đó là phần trình bày khái quát về hạ tầng khóa công khai dựa trên dấu hiệu sinh trắc học gọi là BioPKI như: khái niệm, kiến trúc tổng quan, chức năng, dịch vụ của BioPKI, và phân tích một số hướng tiếp cận nghiên cứu hệ BioPKI.

Chương 3: Thiết kế và ứng dụng chữ ký số.

Phân tích, thiết kế và cài đặt demo chương trình ứng dụng về chữ ký số dựa trên thuật toán RSA trong bài toán xác thực bảng điểm.