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

ĐỖ QUỐC TRƯỞNG

ĐẢM BẢO AN TOÀN THÔNG TIN TRÊN WEB SỬ DỤNG KỸ THUẬT MÃ HÓA ỨNG DỤNG VÀO GỬI NHẬN CÔNG VĂN TÀI LIỆU TRONG HỆ THỐNG MẠNG QUÂN SỰ

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên - 2020

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

ĐỖ QUỐC TRƯỞNG

ĐẢM BẢO AN TOÀN THÔNG TIN TRÊN WEB SỬ DỤNG KỸ THUẬT MÃ HÓA ỨNG DỤNG VÀO GỬI NHẬN CÔNG VĂN TÀI LIỆU TRONG HỆ THỐNG MẠNG QUÂN SỰ

Chuyên ngành: Khoa học máy tính
Mã số chuyên ngành: 8480101

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH
Người hướng dẫn khoa học: TS PHẠM THẾ QUẾ

Thái Nguyên - 2020

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn này là công trình nghiên cứu của chính bản thân, luận văn này hoàn toàn được hình thành và phát triển từ quan điểm của chính cá nhân tôi, dưới sự hướng dẫn chỉ bảo của TS Phạm Thế Quế. Các kết quả nghiên cứu trong luận văn là trung thực và chưa được công bố trong các công trình nào khác.

Học viên

Đỗ Quốc Trưởng

LỜI CẢM ƠN

Để hoàn thành luận văn "Đảm bảo an toàn thông tin trên web sử dụng kỹ thuật mã hóa ứng dụng vào gửi nhận công văn tài liệu trong hệ thống mạng Quân sự" học viên đã nhận được sự hướng dẫn và giúp đỡ nhiệt tình của nhiều tập thể và cá nhân.

Trước hết, học viên xin bày tỏ lòng biết ơn chân thành đến ban lãnh đạo cùng quý thầy cô trong khoa Công nghệ thông tin - Trường Đại học Công nghệ thông tin và truyền thông, Đại học Thái Nguyên đã tận tình dạy dỗ, truyền đạt kiến thức, kinh nghiệm và tạo điều kiện thuận lợi cho học viên trong suốt thời gian học tập và thực hiện đề tài.

Đặc biệt, xin bày tỏ lòng biết ơn sâu sắc đến thầy hướng dẫn TS. Phạm Thế Quế, người đã gợi cho học viên những ý tưởng về đề tài, đã tận tình hướng dẫn và giúp đỡ để đề tài được thực hiện và hoàn thành.

Tôi cũng xin cảm ơn cơ quan, bạn bè đồng nghiệp, gia đình và những người thân đã cùng chia sẻ, giúp đỡ, động viên, tạo điều kiện thuận lợi để tôi hoàn thành tốt nhiệm vụ học tập và hoàn thành bản luận văn.

Thái nguyên, ngày.... tháng…. năm 2020

Học viên

Đỗ Quốc Trưởng

MỤC LỤC

DANH MỤC CÁC THUẬT NGỮ, TỪ VIẾT TẮT

Từ viết tắt	Tiếng anh	Nghĩa tiếng việt
CA	Certificate Authority	Cơ quan chứng thực chữ ký số
DS	Digital Signatures	Chữ ký số
DSA	Digital Signature Algorithm	Giải thuật ký điện tử
DES	Data Encryption Standard	Chuẩn mã hóa dữ liệu
DSS	Digital Signature Standard	Chuẩn chữ ký số
DoS	Denial of Service	Tấn công từ chối dịch vụ
FTP	File Transfer Protocol	Giao thức truyền tập tin
HTML	Hypertext Markup Language	Ngôn ngữ đánh dấu siêu văn bản
HTTP	Hypertext Transfer Protocol	Giao thức truyền siêu văn bản
LDAP	Lightweight Directory Access Protocol	Giao thức ứng dụng truy cập các cấu trúc thư mục
RSA	Rivest, Shamir and Adleman	Giải thuật mã hóa công khai
PKI	Public Key Infrastructure	Cơ sở hạ tầng khóa công khai
SHA	Secure Hash Algorithm	Giải thuật băm an toàn
SSL	Secure Socket Layer	Giao thức an ninh thông tin

Từ viết tắt	Tiếng anh	Nghĩa tiếng việt
SQL	Structured Query Language	Ngôn ngữ truy vấn
TCP/IP	Transmission Control Protocol/Internet Protocol	Một hệ thống các giao thức hỗ trợ việc truyền thông tin trên mạng
TLS	Transport Layer Security	Bảo mật tầng giao vận
URL	Uniform Resource Locator	Định vị tài nguyên thống nhất

DANH MỤC HÌNH VẼ

MỞ ĐẦU

1. Đặt vấn đề

1.1. Sự cần thiết lựa chọn đề tài

Hiện nay tình hình an toàn thông tin số ở nước ta diễn biến phức tạp đe dọa nghiêm trọng đến ứng dụng công nghệ thông tin phục vụ phát triển kinh tế xã hội và đảm bảo Quốc phòng an ninh. Bảo mật và đảm bảo an toàn thông tin dữ liệu đang nhiều nhà khoa học tập trung nghiên cứu, là một chủ đề rộng có liên quan đến nhiều lĩnh vực, trong thực tế có thể có nhiều phương pháp được thực hiện để đảm bảo an toàn thông tin dữ liệu. Ngày nay, với sự phát triển nhanh chóng của hạ tầng truyền thông, người sử dụng dựa trên nền tảng này để truyền các thông tin trên mạng thì các nguy cơ xâm nhập vào các hệ thống thông tin, các mạng dữ liệu ngày càng gia tăng. Nhiều chuyên gia đang tập trung nghiên cứu và tìm mọi giải pháp để đảm bảo an toàn, an ninh cho hệ thống, đặc biệt là các hệ thống mạng máy tính trong Quân sự. Việc bảo mật cho hệ thống mạng máy tính có thể thực hiện theo nhiều phương diện, ở nhiều tầng khác nhau, bao gồm từ phương diện kiểm soát truy nhập vật lý vào hệ thống, thực hiện sửa chữa, cập nhật, nâng cấp hệ điều hành cũng như vá mọi lỗ hổng về an ninh, quản lý các hoạt động gửi nhận công văn và truyền tải văn bản trên mạng (Giám sát qua tường lửa, các bộ định tuyến Router, phát hiện và phòng ngừa sự xâm nhập,…) xây dựng các giải pháp bảo mật ở mỗi phần mềm để quản lý người dùng thông qua việc cấp quyền sử dụng, mật khẩu, mật mã, mã hóa dữ liệu để che giấu thông tin.

Trên thực tế hiện nay các chiến lược Quân sự Quốc phòng các phương án tác chiến, các bí mật về khoa học Quân sự cho đến các công văn tài liệu bí mật, tuyệt mật đều được tạo lập soạn thảo lưu trữ trên các máy tính. Do không kiểm soát được việc sử dụng các thiết bị lưu trữ di động như USB, thẻ nhớ, ổ cứng di động hay các thiết bị thu phát sóng như USB 3G, Wifi…nên tất các các tài nguyên thông tin Quân sự đang nằm trên không gian mạng đều có thể bị lộ lọt, bị làm giả, bị chỉnh sửa…Nhận thức được vấn đề nêu trên nên em đã chọn đề tài: “Đảm bảo an toàn thông tin trên web sử dụng kỹ thuật mã hóa ứng dụng