ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

HOÀNG VĨNH HÀ

NGHIÊN CỨU GIẢI PHÁP XÁC THỰC WEB ỨNG DỤNG TRONG GIAO DỊCH ĐIỆN TỬ

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Chuyên ngành: KHOA HỌC MÁY TÍNH

Mã số: 60.48.01

Người hướng dẫn khoa học: TS. HỒ VĂN HƯƠNG

Thái Nguyên, 2014

LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu của bản thân. Các số liệu kết quả trình bày trong Luận văn này là trung thực. Những tư liệu được sử dụng trong Luận văn có nguồn gốc rõ ràng, đầy đủ.

Thái nguyên, tháng 9 năm 2014

LỜI CẢM ƠN

Lời đầu tiên, tôi xin gửi lời cảm ơn chân thành nhất tới thầy giáo, TS. Hồ Văn Hương, Ban Cơ yếu Chính phủ, người đã hướng dẫn và chỉ bảo tận tình cho tôi trong suốt quá trình thực hiện Luận văn.

Tôi cũng xin gửi lời cảm ơn tới các thầy, cô giáo đã dìu dắt tôi trưởng thành trong suốt quá trình học tập tại trường Đại học CNTT-TT Thái Nguyên.

Cảm ơn các anh, chị, em trong Công ty EcoIT đã chỉ bảo tận tình trong thời gian tôi học tập thực tế tại Công ty. Đồng thời, cảm ơn anh Hoàng Chiến Thắng, Ban Cơ yếu Chính phủ đã giúp tôi hiểu rõ hơn về hệ thống đăng nhập duy nhất SSO, CAS, SSL, Chữ ký số và ứng dụng trong thực tế.

Cuối cùng tôi muốn gửi lời cảm ơn sâu sắc nhất tới gia đình và bạn bè – nguồn động viên lớn lao mỗi khi tôi gặp khó khăn.

Cảm ơn tất cả mọi người đã luôn bên cạnh giúp đỡ tôi!

Thái Nguyên, ngày 29 tháng 09 năm 2014

Học viên thực hiện

(ký và ghi họ tên)

Hoàng Vĩnh Hà

MỤC LỤC

DANH MỤC CÁC CHỮ VIẾT TẮT

TỪ VIẾT TẮT	TÊN ĐẦY ĐỦ	DỊCH RA TIẾNG VIỆT
ATTT		An Toàn Thông Tin
CNTT		Công Nghệ Thông Tin
CA	Certificate Authority	Thẩm quyền chứng thực
DES	Data Encrytion Standard	Chuẩn mã hóa dữ liệu
DNS	Domain Name System	Hệ thống tên miền
HTTP	Hypertext Transfer Protocol	Giao thức truyền tải siêu văn bản
HTTPS	Secure Hypertext Transfer Protocol	Giao thức truyền tải siêu văn bản an toàn
LDAP	Lightweight Directory Access Protocol	Lightweight Directory Access Protocol
PKCS	Public Key Cryptography Standards	Chuẩn mật mã khóa công khai
PKI	Public Key Infrastructure	Cơ sở hạ tầng khóa công khai
RA	Registration Authority	Thẩm quyền đăng ký
RSA	Rivest Shamir Adleman	Thuật toán mã hóa RSA
SHA	Secure Hash Algorithm	Thuật toán băm
SPKC	Simple Public Key Certificate	Chứng thư khoá công khai đơn giản
SSL	Secure Socket Layer	Giao thức bảo mật web
TLS	Transport Layer Security	Giao thức bảo mật tầng truyền thông

DANH MỤC CÁC HÌNH

LỜI MỞ ĐẦU

Ngày nay, công nghệ thông tin phát triển rất nhanh và được ứng dụng vào hầu hết những lĩnh vực trong cuộc sống. Vai trò của công nghệ thông tin ngày càng được nâng cao, không chỉ dừng lại ở những ứng dụng văn phòng, công nghệ thông tin còn được triển khai ở nhiều lĩnh vực khác trong đời sống, kinh tế xã hội và an ninh quốc phòng. Bên cạnh những lợi thế trong việc áp dụng công nghệ thông tin, việc sử dụng CNTT còn tiềm ẩn nhiều vấn đề còn tồn tại, trong đó có việc đảm bảo an toàn thông tin ví dụ như bị đánh cắp dữ liệu, được phép đọc các tài liệu mà không đủ thẩm quyền, dữ liệu bị phá hủy … Do đó, bên cạnh việc triển khai và sử dụng CNTT, chúng ta cũng phải đảm bảo ATTT. Đảm bảo ATTT chính là đảm bảo hệ thống có được ba yếu tố:

- Tình toàn vẹn
- Tính bí mật
- Tính sẵn sàng

Trong lĩnh vực ATTT, sử dụng chứng thư số đã trở thành một trong các phương pháp giúp chúng ta có thể bảo mật thông tin. Với chứng thư số, người sử dụng có thể mã hóa thông tin một cách hiệu quả, chống giả mạo thông tin, xác thực người gửi. Ngoài ra, chứng thư số còn là bằng chứng giúp chống chối cãi nguồn gốc, ngăn chặn người gửi chối cãi nguồn gốc tài liệu mình đã gửi.

Bố cục đề tài Luận văn gồm có 3 phần, với nội dung từng phần cụ thể như sau:

Chương 1. TỔNG QUAN VỀ AN TOÀN THÔNG TIN VÀ BẢO MẬT THÔNG TIN TRONG GIAO DỊCH ĐIỆN TỬ

Chương này chúng tôi sẽ tìm hiểu về giao dịch điện tử, phân loại giao dịch điện tử, an toàn thông tin trong giao dịch điện tử, một số giải pháp bảo mật giao dịch điện tử, tổng quan về web và ứng dụng web, an toàn dịch vụ web, mật mã khóa đối xứng, mật mã khóa công khai, hàm băm, chữ ký số.

Chương 2. MỘT SỐ GIẢI PHÁP XÁC THỰC WEB

Chương này trình bày về một số giải pháp xác thực web bao gồm: Giải pháp xác thực người dùng Web, hệ thống đăng nhập duy nhất, giải pháp ký số, xác thực nội dung Web và giải pháp sử dụng giao thức SSL/TLS trong quá trình trao đổi giữa Web client và WebServer để xây dựng ứng dụng cho chương tiếp theo.

Chương 3. XÂY DỰNG VÀ TÍCH HỢP GIẢI PHÁP XÁC THỰC WEB TRÊN CỔNG THÔNG TIN NGUỒN MỞ LIFERAY

Chương này xây dựng ứng dụng cụ thể: Xây dựng, tích hợp hệ thống đăng nhập duy nhất CAS với cổng thông tin nguồn mở Liferay, xây dựng ứng dụng ký số, xác thực trên nền tảng Web, cấu hình, tích hợp giao thức SSL/TLS cũng như tích hợp với thiết bị Etoken.

Do thời gian hoàn thành đề tài có hạn cũng như khả năng nghiên cứu còn hạn chế cho nên em không tránh khỏi những khiếm khuyết, em rất mong có được những góp ý và giúp đỡ của các thầy cô giáo để em có thể tiếp tục đề tài này ở mức ứng dụng cao hơn trong tương lai.

Em xin chân thành cảm ơn.

Học viên

Hoàng Vĩnh Hà