ĐẠI HỌC THÁI NGUYÊN
KHOA CÔNG NGHỆ THÔNG TIN

VŨ ANH TUẤN

BẢO MẬT VÀ AN TOÀN THÔNG TIN TRONG THƯƠNG MẠI ĐIỆN TỬ

LUẬN VĂN THẠC SĨ KHOA HỌC
CÔNG NGHỆ THÔNG TIN

Chuyên ngành : Khoa học máy tính
Mã số : 60 . 48 . 01

Người hướng dẫn khoa học:
PGS.TS NGUYỄN GIA HIỂU

THÁI NGUYÊN – 2008

MỤC LỤC

Nội dung *Trang*

Nội dung *Trang*

LỜI NÓI ĐẦU

Với sự phát triển mang tính toàn cầu của mạng Internet và TMĐT, con người có thể mua bán hàng hoá và dịch vụ thông qua mạng máy tính toàn cầu một cách dễ dàng trong mọi lĩnh vực thương mại rộng lớn . Tuy nhiên đối với các giao dịch mang tính nhạy cảm này cần phải có những cơ chế đảm bảo bảo mật và an toàn vì vậy vấn đề bảo mật và an toàn thông tin trong thương mại điện tử là một vấn đề hết sức quan trọng. Đề tài sẽ đề cập đến các kỹ thuật chính của lĩnh vực Bảo mật và an toàn thông tin trong thương mại điện tử.

Hiện nay vấn đề Bảo mật và an toàn thông tin trong TMĐT đã và đang được áp dụng phổ biến và rộng rãi ở Việt Nam và trên phạm vi toàn cầu. Vì thế vấn đề Bảo mật và an toàn đang được nhiều người tập trung nghiên cứu và tìm mọi giải pháp để đảm bảo Bảo mật và an toàn cho các hệ thống thông tin trên mạng. Tuy nhiên cũng cần phải hiểu rằng không có một hệ thống thông tin nào được bảo mật 100% bất kỳ một hệ thống thông tin nào cũng có những lỗ hổng về bảo mật và an toàn mà chưa được phát hiện ra

Vấn đề bảo mật và an toàn thông tin trong TMĐT phải đảm bảo bốn yêu cầu sau đây:

- Đảm bảo tin cậy : Các nội dung thông tin không bị theo dõi hoặc sao chép bởi những thực thể không được uỷ thác.
- Đảm bảo toàn vẹn : Các nội dung thông tin không bị thay đổi bởi những thực thể không được uỷ thác
- Sự chứng minh xác thực : Không ai có thể tự trá hình như là bên hợp pháp trong quá trình trao đổi thông tin
- Không thể thoái thác trách nhiệm : Người gửi tin không thể thoái thác về những sự việc và những nội dung thông tin thực tế đã gửi đi

Xuất phát từ những khả năng ứng dụng trong thực tế và những ứng dụng đã có từ các kết quả của nghiên cứu trước đây về lĩnh vực Bảo mật và an toàn trong TMĐT. Đề tài sẽ đi sâu nghiên cứu các kỹ thuật và các phương pháp Bảo mật và an toàn thông tin trong thương mại điện tử

I. Nội dung nghiên cứu của đề tài

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

- Đề tài nghiên cứu các kỹ thuật và phương pháp để thực hiện nhiệm vụ Bảo mật và an toàn trong thương mại điện tử, quá trình thực hiện và các kiến thức khoa học và thuật toán liên quan như: Xác thực, Bảo mật, Bảo toàn dữ liệu, Mật mã, Chữ ký số...
- Áp dụng các kết quả đã nghiên cứu để triển khai hệ thống Bảo mật và an toàn trong TMĐT

2. Ý nghĩa khoa học của đề tài

- Áp dụng các kết quả đã nghiên cứu để xây dựng các kỹ thuật Bảo mật và an toàn trong thương mại điện tử với một số tính năng cơ bản như: Hệ thống chứng thực, Các cơ chế phân bố khoá tự động, Mã hoá các thông tin cần thiết, kỹ thuật ngăn ngừa các rui ro trong TMĐT.
- Vấn đề Bảo mật và an toàn trên mạng là một trong những vấn đề nóng hổi trong hoạt động thực tiễn của TMĐT, giải quyết tốt vấn đề bảo mật và an toàn trong TMĐT sẽ mang lại ý nghĩa hết sức to lớn như: Làm cho khách hàng tin tưởng khi thực hiện các giao dịch trên mạng, và các nhà cung cấp dịch vụ giao dịch trực tuyến cũng như các ISP đảm bảo được những thông tin của khách hàng giao dịch trên mạng được an toàn.

3. Phương pháp nghiên cứu

- Thu thập, phân tích các tài liệu và những thông tin liên quan đến đề tài.
- Tìm hiểu các giao dịch trong thương mại điện tử của một số Website trong và ngoài nước, thu thập các thông tin về bảo mật các giao dịch thương mại điện tử đã có.
- Kết hợp các nghiên cứu đã có trước đây của các tác giả trong nước cùng với sự chỉ bảo, góp ý của thầy hướng dẫn để hoàn thành nội dung nghiên cứu

4. Phạm vi nghiên cứu

- Các vấn đề về bảo mật chứng thực trong thương mại điện tử Hàm băm, các thuật toán mã hoá đối xứng DES và và bất đối xứng như mã khoá công khai RSA, sử dụng chữ ký số DSA và RSA, các giao thức bảo mật trên mạng như: SSL, TLS, SET...
- Các kỹ thuật sử dụng và các phương pháp kết hợp các hệ mật mã trong bảo mật.

- Do có những hạn chế nhất định về cơ sở vật chất và điều kiện tiếp cận thực tế với lĩnh vực an toàn và bảo mật trong thương mại điện tử nên việc cài đặt các ứng dụng chủ yếu mang tính thử nghiệm.

5. Các kết quả nghiên cứu dự kiến cần đạt được

- Các vấn đề về bảo mật chứng thực trong thương mại điện tử, sử dụng chữ ký số, Các kỹ thuật sử dụng và các phương pháp kết hợp các hệ mật mã trong bảo mật.
- Cài đặt thử nghiệm vấn đề về bảo mật và an toàn trong thương mại điện tử đã nghiên cứu.

II, Bố cục của luận văn

Chương I : CÁC KHÁI NIỆM VỀ TMĐT VÀ CÁC ĐẶC TRƯNG CỦA TMĐT

1. Khái niệm về TMĐT
2. Lợi ích của thương mại điện tử
3. Các đặc trưng cơ bản của TMĐT
4. Các loại thị trường điện tử.
5. Các hệ thống thanh toán trong TMĐT
6. Công nghệ thanh toán điện tử
7. Quy trình thanh toán điện tử

Chương II : HỆ MẬT MÃ, MÃ KHOÁ ĐỐI XỨNG, MÃ KHOÁ CÔNG KHAI, CHỮ KÝ SỐ

I, Tổng quan về các hệ mật mã

1. Mã hoá khoá đối xứng: Thuật toán và quá trình tạo khoá
2. Mã hoá khoá công khai: Hoạt động, tạo khoá, mã hoá, giải mã, chuyển đổi văn bản rõ

II, Chữ ký số

1. Khái niệm chữ ký số
2. Phân loại chữ ký số
3. Một số sơ đồ chữ ký số cơ bản
4. Đánh giá tính an toàn của các sơ đồ chữ ký số

Chương III : BẢO MẬT VÀ AN TOÀN TRONG TMĐT

1. An toàn thông tin
2. Cơ chế mã hoá
3. Chứng thực số hoá
4. Một số giao thức bảo mật ứng dụng trong TMĐT

- Các vấn đề bảo mật ứng dụng WEB
- Cơ chế bảo mật SSL và TSL
- Cơ chế bảo mật SET

Chương IV: CÀI ĐẶT VÀ PHÁT TRIỂN CÁC ỨNG DỤNG

- Cài đặt ứng dụng bảo mật và an toàn thông tin, chứng thực số hoá, chữ ký số trên WEBSITE mua bán máy tính trên mạng INTERNET

Kết luận

CHƯƠNG I : CÁC KHÁI NIỆM VỀ TMĐT VÀ CÁC ĐẶC TRƯNG CỦA TMĐT

1. Khái niệm về TMĐT

Thương mại điện tử là hình thức mua bán hàng hoá và dịch vụ thông qua mạng máy rính toàn cầu. TMĐT theo nghĩa rộng được định nghĩa trong luật mẫu về thương mại điện tử của Uỷ ban LHQ về luật thương mại quốc tế:

"*Thuật ngữ thương mại cần được diễn giải theo nghĩa rộng để bao quát các vấn đề phát sinh từ mọi quan hệ mang tính chất thương mại dù có hay không có hợp đồng. Các quan hệ mang tính chất thương mại bao gồm các giao dịch sau đây: Bất cứ giao dịch nào về thương mại nào về cung cấp hoặc trao đổi hàng hoá hoặc dịch vụ, thoả thuận phân phối, đại diện hoặc đại lý thương mại, uỷ thác hoa hồng, cho thuê dài hạn, xây dựng các công trình, tư vấn, kỹ thuật công trình, đầu tư, cấp vốn, ngân hàng, bảo hiểm, thoả thuận khai thác hoặc tô nhượng, liên doanh các hình thức khác về hợp tác công nghiệp hoặc kinh doanh, chuyên chở hàng hoá hay hành khách bằng đường biển, đường không, đường sắt hoặc đường bộ*"

Như vậy, có thể thấy rằng phạm vi của Thương mại điện tử rất rộng, bao quát hầu hết các lĩnh vực hoạt động kinh tế, việc mua bán hàng hoá và dịch vụ chỉ là một trong hàng ngàn lĩnh vực áp dụng của Thương mại điện tử. Theo nghĩa hẹp TMĐT chỉ gồm các hoạt động thương mại được tiến hành trên mạng máy tính mở như Internet. Trên thực tế chính các hoạt động thương mại thông qua mạng Internet đã làm phát sinh thuật ngữ Thương mại điện tử.

Thương mại điện tử gồm các hoạt động mua bán hàng hoá và dịch vụ qua phương tiện điện tử, giao nhận các nội dung kỹ thuật số trên mạng, chuyển tiền điện tử, mua bán cổ phiếu điện tử, vận đơn đơn điện tử, đấu giá thương mại, hợp tác thiết kế, tài nguyên mạng, mua sắm công cộng, tiếp thị trực tuyến tới người tiêu dùng và các dịch vụ sau bán hàng. Thương mại điện tử được thực hiện đối với cả thương mại hàng hoá (ví dụ như hàng tiêu dùng, các thiết bị y tế chuyên dụng) và thương mại dịch vụ (ví dụ như dịch vụ cung cấp thông tin, dịch vụ pháp lý, tài chính). Các hoạt động truyền thống như chăm sóc sức khoẻ, giáo dục và các hoạt động mới (như siêu thị ảo). Thương mại điện tử đang trở thành một cuộc cách mạng làm thay đổi cách thức mua săm của con người.

2. Lợi ích của TMĐT

Xuất phát từ những kinh nghiệm thực tế trong quá trình hoạt động của thương mại điện tử thì TMĐT đã mang lại cho con người và xã hội các lợi ích sau:

2.1. Thu thập được nhiều thông tin

TMĐT giúp cho mỗi cá nhân khi tham gia thu được nhiều thông tin về thị trường, đối tác, giảm chi phí tiếp thị và giao dịch, rút ngắn thời gian sản xuất, tạo dựng và củng cố quan hệ bạn hàng. Các doanh nghiệp nắm được các thông tin phong phú về kinh tế thị trường, nhờ đó có thể xây dựng được chiến lược sản xuất và kinh doanh thích hợp với xu thế phát triển của thị trường trong nước, trong khu vực và quốc tế. Điều này đặc biệt có ý nghĩa đối với các doanh nghiệp vừa và nhỏ, hiện nay đang được nhiều nước quan tâm coi là một trong những động lực phát triển kinh tế.

2.2. Giảm chi phí sản xuất

TMĐT giúp giảm chi phí sản xuất, trước hết là chi phí văn phòng. Các văn phòng không giấy tờ chiếm diện tích nhỏ hơn rất nhiều, chi phí tìm kiếm chuyển giao tài liệu giảm nhiều lần trong đó khâu in ấn gần như bỏ hẳn. Theo số liệu của hãng General Electricity của Mỹ tiết kiệm trên lĩnh vực này đạt tới 30 %. Điều quan trọng hơn, với góc độ chiến lược là các nhân viên có năng lực được giải phóng khỏi nhiều công đoạn sự vụ và có thể tập trung vào nghiên cứu phát triển, sẽ đưa đến những lợi ích to lớn lâu dài.

2.3. Giảm chi phí bán hàng, tiếp thị và giao dịch

TMĐT giúp giảm thấp chi phí bán hàng và chi phí tiếp thị. Bằng phương tiện Internet / Web một nhân viên bán hàng có thể giao dịch với rất nhiều khách hàng, catalogue điện tử trên web phong phú hơn nhiều so với catalogue in ấn chỉ có khuôn khổ giới hạn và luôn luôn lỗi thời, trong khi đó catalogue điện tử trên web được cập nhật thường xuyên.

TMĐT qua Internet / Web giúp người tiêu thụ và các doanh nghiệp giảm đáng kể thời gian và chi phí giao dịch. Thời gian giao dịch qua Internet chỉ bằng 7% thời gian giao dịch qua FAX, và bằng khoảng 0.5 phần nghìn thời gian giao dịch qua bưu điện chuyển phát nhanh, chi phí thanh toán điện tử qua Internet chỉ bằng 10% đến 20% chi phí thanh toán theo lối thông thường.

2.4. Xây dựng quan hệ đối tác

Thương mại điện tử tạo điều kiện cho việc thiết lập và củng cố mối quan hệ giữa các thành viên tham gia quá trình thương mại thông qua mạng Internet các thành viên tham gia có thể giao tiếp trực tiếp (liên lạc trực tuyến) và liên tục với nhau, có cảm giác như không có khoảng cách về địa lý và thời gian nữa, nhờ đó sự hợp tác và quản lý đều được tiến hành nhanh chóng một cách liên tục, các bạn hàng mới, các cơ hội kinh doanh mới được phát hiện nhanh chóng trên phạm vi toàn thế giới và có nhiều cơ hội để lựa chọn hơn.

2.5. Tạo điều kiện sớm tiếp cận kinh tế tri thức

Trước hết TMĐT sẽ kích thích sự phát triển của nghành CNTT tạo cơ sở cho phát triển kinh tế tri thức. Lợi ích này có một ý nghĩa lớn đối với các nước đang phát triển, nếu không nhanh chóng tiếp cận nền kinh tế tri thức thì sau khoảng một thập kỷ nữa nước đang phát triển có thể bị bỏ rơi hoàn toàn. Khía cạnh lợi ích này mang tính chiến lược công nghệ và tính chính sách phát triển cần cho các nước công nghiệp hoá.

3. Các đặc trưng cơ bản của TMĐT

So với các hoạt động thương mại truyền thống, TMĐT có một số các đặc trưng cơ bản sau:

3.1. Các bên tiến hành giao dịch trong thương mại điện tử không tiếp xúc trực tiếp với nhau và không đòi hỏi phải biết nhau từ trước.

Trong thương mại truyền thống các bên thường gặp gỡ nhau trực tiếp để tiến hành giao dịch. Các giao dịch được thực hiện chủ yếu theo nguyên tắc vật lý như chuyển tiền, séc, hoá đơn, vận đơn, gửi báo cáo. Các phương tiện viễn thông như: Fax, telex,... chỉ được sử dụng để chao đổi số liệu kinh doanh. Tuy nhiên việc sử dụng các phương tiện điện tử trong thương mại truyền thống chỉ để chuyển tải thông tin một cách trực tiếp giữa 2 đối tác của cùng một giao dịch.

Thương mại điện tử cho phép tất cả mọi người cùng tham gia từ các vùng xa xôi hẻo lánh đến các khu vực đô thị rộng lớn, tạo điều kiện cho tất cả mọi người ở khắp mọi nơi đều có cơ hội ngang nhau tham gia vào thị trường giao dịch toàn cầu và không đòi hỏi nhất thiết phải có mối quen biết với nhau.

3.2. Các giao dịch thương mại truyền thống được thực hiện với sự tồn tại của khái niệm biên giới quốc gia, còn thương mại điện tử được thực hiện trong một thị trường không có biên giới (thị trường thống nhất toàn cầu). Thương mại điện tử trực tiếp tác động tới môi trường cạnh tranh toàn cầu.

Thương mại điện tử càng phát triển thì máy tính cá nhân trở thành cửa sổ cho doanh nghiệp hướng ra thị trường trên khắp thế giới. Với TMĐT một doanh nhân dù mới thành lập đã có thể kinh doang ở Nhật Bản, Đức và Chi lê..., mà không hề phải bước ra khỏi nhà, một công việc trước kia phải mất nhiều năm.

3.3. Trong hoạt động giao dịch TMĐT đều có sự tham gia của ít nhất ba chủ thể, trong đó có một bên không thể thiếu được là người cung cấp dịch vụ mạng, các cơ quan chứng thực.

Trong TMĐT ngoài các chủ thể tham gia quan hệ giao dịch giống như giao dịch thương mại truyền thống đã xuất hiện một bên thứ 3 đó là nhà cung cấp dịch vụ mạng, các cơ quan chứng thực... là những người tạo môi trường cho các giao