An toàn an ninh trong thương mại điện tử, giao dịch điện tử và các doanh nghiệp lớn (Electronic Transaction, e-Commerce, Enterprise security)

Mục tiêu

Tổng quan đề tài

Phân loại các vấn đề và giải pháp

Tập trung làm rõ một hoặc hai giải pháp

Thử nghiệm

Kết luận

**Mục tiêu**

Hiện nay, cùng với sự phát triển của các dịch vụ được cung cấp trên nền tảng công nghệ cao, thương mại điện tử đã trở nên phổ biến trong cuộc sống thường ngày, giúp thực hiện các giao dịch, thanh toán và gia tăng giá trị của các sản phẩm hàng hóa hoặc truyền những cơ sở dữ liệu liên quan tới thẻ tín dụng, các phương tiện thanh toán khác của khách hàng. Thông qua các nhà cung cấp trực tuyến như amazon hay ebay, chỉ bằng các click chuột và khai báo một số thông tin thẻ cá nhân, mỗi người đều có thể mua bán các mặt hàng ở khắp nơi trên thế giới.

Việc trực tiếp cho phép thay đổi số tiền trong tài khoản của khách hàng đã đặt ra một vấn đề nóng hổi về bảo mật và an ninh trên mạng trong hoạt động thực tiễn của giao dịch điện tử. Liệu khách hàng có tin tưởng khi thực hiện các giao dịch trên mạng không? Và liệu những nhà cung cấp dịch vụ giao dịch trực tuyến có đảm bảo được những thông tin của khách hàng giao dịch được an toàn không?

Việc đảm bảo an toàn cho các thông tin trên là rất quan trọng, song đang phải đối diện với một vấn đề: làm thế nào để tìm ra được một trạng thái cân bằng hợp lý giữa một bên là an toàn và một bên là tiện dụng (gồm các chức năng, đặc tính dễ thao tác của hệ thống này). Một hệ thống càng an toàn thì khả năng xử lý, thực thi thao tác càng phức tạp. Còn ngược lại, một hệ thống dễ thao tác có thể sẽ không đảm bảo an toàn.

Trong nội dung bài tiểu luận này, em xin trình bày những tìm hiểu về định nghĩa thương mại điện tử (E-commerce) là gì, tập trung vào phân tích giao dịch điện tử (electronic transaction), giới thiệu một số phương thức bảo mật trong giao dịch điện tử và trình bày một giải pháp cụ thể.

**Tổng quan đề tài**

Thương mại điện tử và các loại hình giao dịch

Thương mại điện tử (E-commerce – TMĐT), mô tả quá trình mua, bán, vận chuyển hay trao đổi sản phẩm, dịch vụ và thông tin, thông qua các mạng máy tính, bao gồm cả Internet. Phần lớn thương mại điện tử được thực hiện trên Internet. Nhưng thương mại điện tử cũng có thể được tiến hành trên các mạng dùng riêng, ví dụ như các mạng giá trị gia tăng (VAN), hay trên các LAN, hay thậm chí là trên một thiết bị duy nhất đã được điện toán hoá. Ví dụ, mua thực phẩm từ một máy bán hàng tự động và trả bằng thẻ thông minh hay điện thoại di động có thể coi là hoạt động thương mại điện tử.

Giao dịch điện tử (E-transaction), là giao dịch mua bán các mặt hàng, dịch vụ giữa các doanh nghiệp, tổ chức, chính phủ, hay cá nhân được thực hiện thông qua các phương tiện điện tử và cũng có giá trị pháp lý như nó được ghi chép, hoặc mô tả bằng văn bản theo phương pháp truyền thống.

Các loại hình giao dịch thương mại điện tử trong hoạt động thương mại điện tử:

* B2B (business to business): là loại hình giao dịch qua các phương tiện điện tử giữa doanh nghiệp với doanh nghiệp. Giao dịch B2B chiếm gần 90% tỷ trong trong TMĐT. Các giao dịch B2B chủ yếu được thực hiện trên các hệ thống ứng dụng TMĐT như mạng giá trị gia tăng, các sàn giao dịch TMĐT. TMĐT B2B đem lại nhiều lợi ích thực tế cho doanh nghiệp, đặc biệt giúp giảm các chi phí về thu thập thông tin tìm hiểu thị trường, quảng cáo, tiếp thị, đàm phán, tăng các cơ hội kinh doanh,…
* B2C (business to consumer): là loại hình giao dịch giữa doanh nghiệp và người tiêu dùng qua các phương tiện điện tử. Giao dịch B2C tuy chiếm tỷ trọng ít (khoảng 10%) trong TMĐT nhưng phạm vi ảnh hưởng rất rộng. Để tham gia hình thức kinh doanh này, thông thường doanh nghiệp sẽ thiết lập website, hình thành cơ sở dữ liệu về hàng hoá, dịch vụ; tiến hành các quy trình tiếp thị, quảng cáo, phân phối trực tiếp tới người tiêu dùng. TMĐT B2C đem lại lợi ích cho cả doanh nghiệp lẫn người tiêu dùng. Doanh nghiệp tiết kiệm nhiều chi phí bán hàng do không cần phòng trưng bày hay thuê người giới thiệu bán hàng, chi phí quản lý cũng giảm hơn. Người tiêu dùng sẽ cảm thấy thuận tiện vì không phải tới tận cửa hàng, có khả năng lựa chọn và so sánh nhiều mặt hàng cùng một lúc.
* B2G (business to government): là loại hình giao dịch giữa doanh nghiệp với cơ quan nhà nước, trong đó cơ quan nhà nước đóng vai trò khách hàng. Quá trình trao đổi thông tin giữa doanh nghiệp với cơ quan nhà nước được tiến hành qua các phương tiện điện tử. Cơ quan nhà nước cũng có thể thiết lập những website tại đó đăng tải thông tin về nhu cầu mua hàng của các cơ quan nhà nước, tiến hành việc đấu thầu hàng hoá, dịch vụ và lựa chọn nhà cung cấp trên website. Điều này một mặt giúp tiết kiệm các chi phí tìm nhà cung cấp, đồng thời giúp tăng cường tính minh bạch trong hoạt động mua sắm công.
* C2C (consumer to consumer): là loại hình giao dịch giữa các cá nhân với nhau. Sự phát triển của các phương tiện điện tử làm cho nhiều cá nhân có thể tham gia hoạt động thương mại với tư cách là người bán, người cung cấp dịch vụ. Một cá nhân có thể tự thiết lập website để kinh doanh những mặt hàng do mình làm ra hoặc sử dụng một website có sẵn để đấu giá một số mặt hàng mình có.
* G2C (government to consumer): là loại hình giao dịch giữa cơ quan nhà nước với cá nhân. Đây chủ yếu là các giao dịch mang tính hành chính, nhưng có thể mang những yếu tố của TMĐT. Ví dụ khi người dân đóng tiền thuế qua mạng, trả phí khi đăng ký hồ sơ trực tuyến, v.v…

Các hệ thống thanh toán trong TMĐT

* Giao dịch thẻ tín dụng trực tuyến (Online Credit Card Transactions)
* Ví điện tử (Digital Wallets)
* Tiền điện tử (Digital Cash)
* Hệ thống giao dịch theo giá trị được tích lũy trực tuyến (Online Stored Value Payment Systems)
* Hệ thống số dư tích lũy điện tử (Digital Accumulating Balance Systems)
* Hệ thống thanh toán Séc điện tử (Digital Checking Payment Systems)
* Hệ thống thanh toán di động (Mobile Payment Systems)

Ở nước ta hiện tại, cổng thanh toán NAPAS (National Payment Service) cho phép khách hàng sử dụng để giao dịch điện tử như thanh toán hóa đơn dịch vụ, thanh toán mua hàng trực tuyến, chuyển rút tiền tại máy ATM/máy POS mà chỉ với thẻ ATM của một ngân hàng nội địa liên kết.

Chứng thư điện tử - Chứng thực chữ ký điện tử - Chương trình ký điện tử

Giao dịch điện tử sử dụng thẻ Credit-card

**Phân loại các vấn đề và giải pháp**

Các yêu cầu bảo mật

Trong thương mại điện tử, các vấn đề kĩ thuật về an toàn thông tin sau cần quan tâm:

– Tính bảo mật (Confidentiality / Privacy): thông tin trong thương mại điện tử được bảo vệ khỏi các truy cập trái phép.

– Tính xác thực (Authentication): người dùng cần xác thực trước khi tiếp cận thông tin cá nhân của họ hoặc các thông tin có quyền hạn.

– Tính toàn vẹn (Integrity): thông tin giao dịch không bị thay đổi trên đường truyền

– Tính chống chối bỏ (Non-Repudiation): hai bên giao dịch không thể từ chối thông tin do chính mình đã gửi/nhận.

– Tính sẵn sàng (Availability): thông tin cần thiết phải sẵn sàng cung cấp khi có yêu cầu, truy cập từ người dùng.

– Tính mã hóa (Encryption): thông tin cần được mã hóa chỉ để những người dùng hợp lệ truy xuất

– Tính kiểm toán (Auditing): lưu trữ dữ liệu để đối soát khi có sự cố, hoặc khi cần thiết.

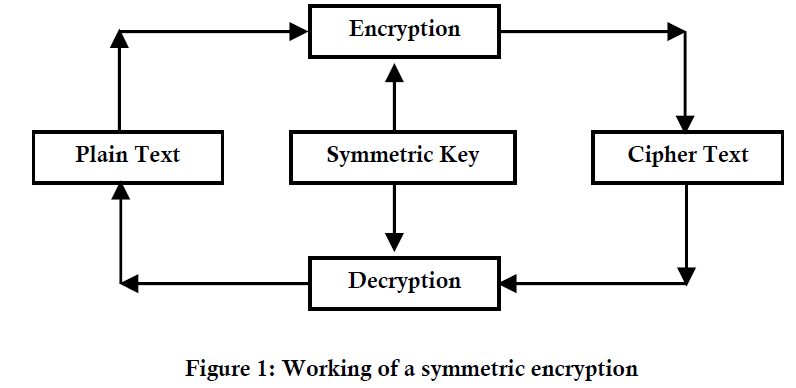
Các kỹ thuật mã hóa

Câu hỏi đặt ra là làm thế nào để đáp ứng được các yêu cầu đã được đưa ra?

Hiện nay, phương pháp phổ biến là sử dụng kỹ thuật mã hóa. Kĩ thuật mật mã được phân loại thành kỹ thuật mã hóa khóa đối xứng và kỹ thuật mã hóa khóa bất đối xứng.

Kỹ thuật mã hóa khóa đối xứng

Ở kỹ thuật mã hóa khóa đối xứng, một khóa sẽ được dùng cho cả mã hóa và giải mã. Bên gửi phải có một bản sao của khóa cho quá trình mã hóa và bên nhận cũng phải có một bản sao của khóa đó cho quá trình giải mã. Hình dưới mô tả hoạt động của một quá trình mã hóa đối xứng



Kỹ thuật mã hóa khóa đối xứng hoạt động hiệu quả, nhanh, và tiêu thụ ít tài nguyên máy như vi xử lý và bộ nhớ. Tuy nhiên, nó tồn tại một số nhược điểm sau:

+ Bên gửi phải truyền một bản sao của khóa tới bên nhận để phục vụ giải mã.

+ Bên gửi phải sử dụng các khóa khác nhau cho các người dùng khác nhau.

+ Không thể tạo ra chữ ký điện tử cho bản tin (message)

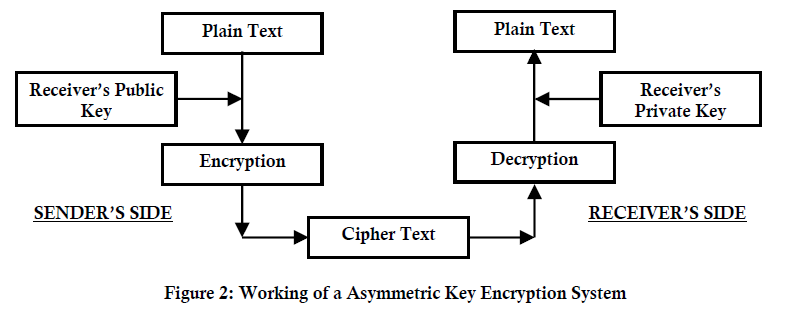
+ Rất khó để áp dụng tính chống chối bỏ (non-repudiation) cho các nhóm giao tiếp chia sẻ chung một khóa.

Các ví dụ tiêu biểu của thuật toán mã hóa đối xứng là: Data Encryption Standard (DES), Triple Data Encryption Standard I(3DES), và Advanced Encryption Standard (AES)

Kỹ thuật mã hóa khóa bất đối xứng

Các hạn chế của phương pháp mã hóa đối xứng được giải quyết bằng kỹ thuật mã hóa khóa bất đối xứng. Ở đây, mỗi người dùng có một cặp khóa bao gồm một khóa công khai và một khóa mật. Mỗi khóa là những số cố định sử dụng trong quá trình mã hóa và giải mã. Khóa công khai được công bố rộng rãi cho mọi người và được dùng để mã hóa. Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng. Nói cách khác, mọi người đều có thể mã hóa nhưng chỉ có người biết khóa mật mới có thể giải mã được. Tất cả bản tin được gửi thì được mã hóa sử dụng khóa công khai và giải mã sử dụng khóa mật riêng của bên nhận.

Hình dưới mô tả nguyên lý hoạt động của hệ thống mã khóa khóa bất đối xứng.



Nhược điểm của hệ thống này là hoạt động chậm, không hiệu quả bằng phương pháp mã hóa khóa đối xứng và tiêu tốn tài nguyên máy.

RSA là thuật toán mã hóa khóa công khai tiêu biểu cho kỹ thuật mã hóa khóa bất đối xứng. RSA đang được sử dụng phổ biến trong thương mại điện tử và được cho là đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.

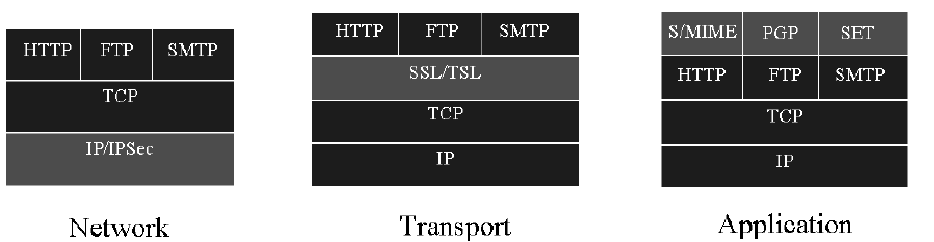
Các giao thức đảm bảo giao dịch – SSL, SET

Một số giao thức được triển khai nhằm bảo đảm an toàn cho các giao dịch điện tử là:

+ Giao thức Internet Protocol Security (IPSec)

+ Giao thức Secure-Socket Layer (SSL)

+ Giao thức Secure Electronic Transaction (SET)



Như chúng ta đã biết, TCP/IP được chia thành 5 tầng riêng biệt. Mỗi tầng đảm nhiệm một vai trò khác nhau và chỉ giao tiếp với tầng trên và tầng dưới. Kiến trúc module này có lợi thế… Có một vài tầng có thể triển khai được các giao thức bảo mật để bảo vệ kết nối Internet khỏi các xâm nhập có hại.

Internet Protocol Security

Giao thức IPSec được áp dụng ở tầng Network, cung cấp khả năng mã hóa và xác thực dữ liệu người dùng (payload). Hacker chỉ có thể biết được đích đến của bản tin (có thể là địa chỉ IP) nhưng không thể lấy được thông tin. Hơn nữa, IPSec có tùy chọn mã hóa một bản tin IP gốc và đặt nó vào một bản tin mới với một header ngụy trạng. Tùy chọn “tunnel mode” này cho phép người dùng có thể thiết lập các nhóm cá nhân trên Internet (các mạng riêng ảo).

Ưu điểm của bảo mật ở tầng Network:

+ Chức năng bảo mật hoàn toàn “trong suốt” đối với người dùng

+ Danh tính của các bên tham gia được bảo vệ do các địa chỉ IP được ngụy trang

Nhược điểm của bảo mật ở tầng Network:

+ Chỉ có thể bảo mật từ lớp IP trở xuống. Khi dữ liệu được gửi lên các lớp cao hơn thì không còn được bảo vệ nữa. Nếu có nhiều người dùng trên cùng một hệ thống, thông tin của một cá nhân có thể được nhìn thấy bởi những người khác.

+ Danh tính của nhiều người dùng trên cùng hệ thống chỉ có thể chuyển thành một địa chỉ IP duy nhất. Do đó việc xác thực một cá nhân là không thể.

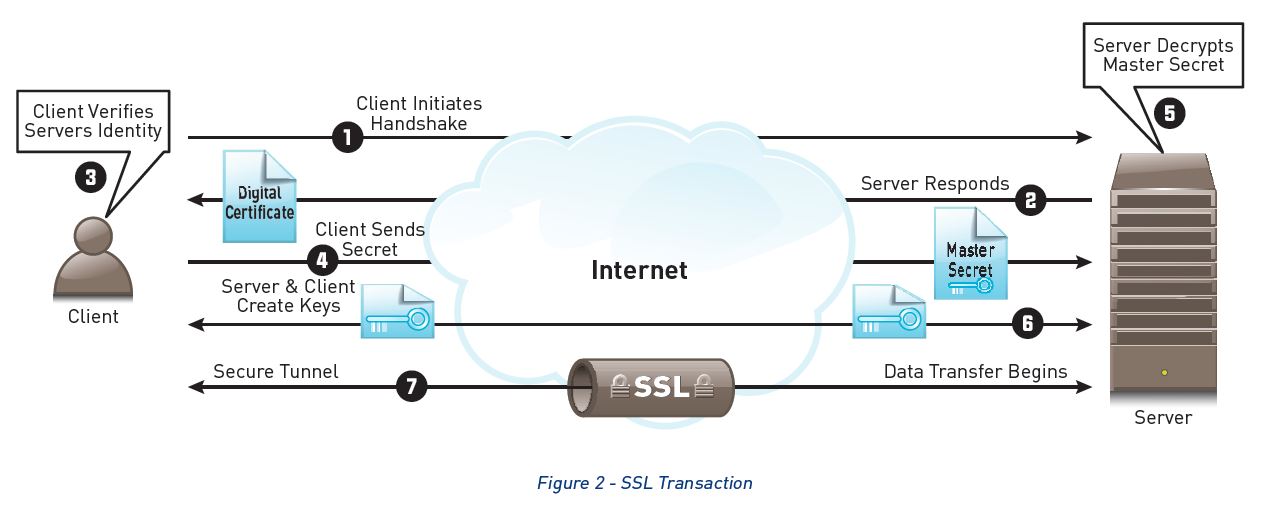
Secure Socket Layer

SSL được bắt nguồn và phát triển bởi Netscape và hiện tại được áp dụng rộng rãi cho tất cả các trình duyệt Web và máy chủ Web. SSL là công nghệ mã hóa trao đổi dữ liệu giữa máy chủ Web (server) và máy tính cá nhân (client). Đảm bảo việc trao đổi thông tin không thể bị khai thác và giải mã bởi đối tượng thứ ba. Ngoài ra SSL còn có nhiệm vụ như chứng thực Website, bảo mật FTP, Mail Service, VPN…

Giao thức SSL bao gồm hai giao thức:

+ Giao thức bắt tay SSL (The SSL handshake protocol): client và server xác thực lẫn nhau và thỏa thuận một chìa khóa mã hóa.

+ Giao thức bản ghi SSL (The SSL record protocol): dữ liệu các phiên giao dịch được mã hóa khi trao đổi giữa client và server.



Các bước trong một giao dịch SSL:

+ Client gửi một yêu cầu giao dịch

+ Server nhận yêu cầu từ client

+ Server gửi chứng chỉ (certificate) của nó tới client

+ Client kiểm tra nếu chứng chỉ đó được phát hành bởi một nhà cung cấp đã được nó tin cậy (Certificate Authority – CA)

+ Client so sánh thông tin trong chứng chỉ với thông tin nó vừa nhận được từ site

+ Client thông báo tới server sử dụng thuật toán mã hóa nào

+ Client sinh ra một khóa phiên sử dụng mật mã đã được đồng ý

+ Client mã hóa khóa phiên sử dụng khóa công khai của server và gửi nó tới server

+ Server nhận khóa phiên đã được mã hóa và giải mã nó bằng khóa riêng

+ Client và server sử dụng khóa phiên đó cho các giao dịch tiếp theo.

Mặc dầu giao thức SSL được áp dụng cho tất cả các trình duyệt, nó vẫn tồn tại hai điểm yếu sau:

+ Chủ nhân của thẻ tín dụng không được bảo vệ trước bên bán. Nếu bên bán gian lận và thu nhiều tiền hơn thì người mua sẽ chịu mất mát.

+ Tương tự, bên bán cũng không được bảo vệ trước những người mua gian lận cung cấp thẻ tín dụng giả mạo.

Tóm lại:

+ SSL là một giao thức bảo mật bản tin, không phải là một giao thức thanh toán

+ SSL yêu cầu các bên phải được chứng thực bằng các chứng chỉ

+ Giao thức SSL không hỗ trợ chống phủ nhận (non-repudiation)

Kế thừa SSL, IBM phát triển một chuẩn mới gọi là Internet Keyed Payment Protocol (iKP) dẫn tới sự ra đời của Secure Electronic Transaction Protocol (giao thức SET)

Secure Electronic Transaction (SET) Protocol

SET giúp bảo mật ở tầng cao nhất – tầng App.

**Tập trung làm rõ một hoặc hai giải pháp**

Giao thức SET

Thử nghiệm

Kết luận