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.

**Chương 1 - 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 gần 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…

Ưu và nhược điểm của các hệ thống thanh toán điện tử

https://unichange.me/articles/advantages\_of\_electronic\_payment\_systems

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.

Giao dịch điện tử sử dụng thẻ tín dụng Credit-card

Thẻ tín dụng đã trở thành một phương tiện thanh toán phổ biến theo hai hình thức chính.

+ Quẹt thẻ trực tiếp trên các máy pos

+ Thanh toán các giao dịch trên mạng (không quẹt thẻ trực tiếp)

Khi khách hàng mua một món đồ trực tiếp ở cửa hàng, nhân viên thường sử dụng máy pos để nhập số tiền và thanh toán bằng cách quẹt thẻ của khách. Thông tin giao dịch được gửi tới cổng thanh toán (payment gateway) xác nhận cấp quyền cho bên bán, đồng thời trả về hóa đơn cho khách hàng. Khi có sự cố xảy ra, cửa hàng sẽ được bồi thường do họ đã được cổng thanh toán cấp quyền giao dịch.

Trước đây, có thời điểm mua bán được diễn ra thông qua điện thoại, bên bán thường chấp nhận sử dụng số thẻ tín dụng của khách hàng để hoàn thành giao dịch. Tất nhiên, họ không được cấp quyền bởi các cổng thanh toán nên loại hình này ẩn chứa rất nhiều rủi ro với bên bán hàng.

Vào năm 1996, Mastercard và Visa thông báo họ hỗ trợ phát triển một chuẩn cho giao dịch thẻ tín dụng điện tử. Và tới năm 1997, Secure Electronic Transaction LLC (SETCo) được hình thành dựa trên các tiêu chí kĩ thuật của SET.

Trong phần tiếp theo em trình bày về các vấn đề và giải pháp cho thương mại điện tử và tập trung vào tìm hiểu cơ chế hoạt động của giao thức SET.

Chương 2 – Các giải pháp bảo mật

**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 (bao gồm thông tin trong hệ thống máy tính cũng như thông tin chuyển tải trên mạng) được bảo vệ khỏi các truy cập trái phép, chỉ được truy cập (đọc, in, hiển thị) bởi những người được ủy quyền.

– 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): đảm bảo thông tin giao dịch không bị thay đổi trên đường truyền và chỉ có những người được ủy quyền mới có thể thay đổi tài nguyên của hệ thống máy tính và truyền tải thông tin.

– Tính chống phủ định (Non-Repudiation): hai bên giao dịch không thể phủ định được 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.

- Kiểm soát truy cập (Access Control): yêu cầu mọi sự truy cập tới tài nguyên thông tin đều được kiểm soát chặt chẽ từ hệ thống.

– 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

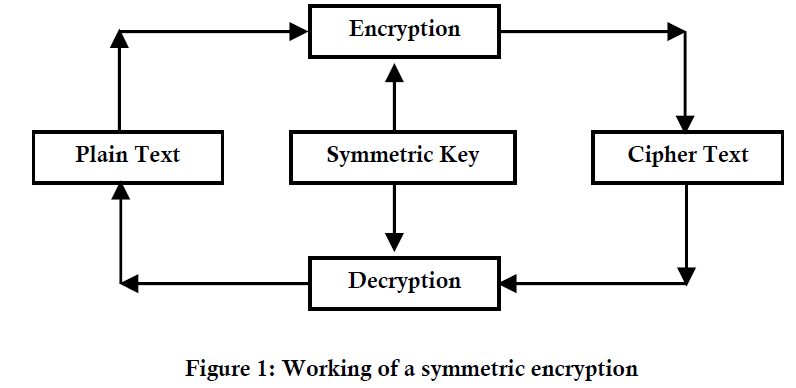
Câu hỏi đặt ra là làm thế nào để đáp ứng được các yêu cầu đã được đưa ra?

Hiện nay, phương pháp phổ biến là sử dụng các kỹ thuật mật mã để mã hóa dữ liệu. Trước khi truyền qua mạng Internet, người gửi thực hiện mã hóa dữ liệu, trong quá trình truyền, dù có “chặn” được các dữ liệu này, kẻ trộm cũng không thể đọc được vì bị mã hóa. Khi tới đích, người nhận sẽ sử dụng một công cụ để giải mã. Phương pháp mã hóa và bảo mật phổ biến nhất đang được thế giới áp dụng là chứng chỉ số (Digital Certificate). Với chứng chỉ số, người sử dụng có thể mã hóa thông tin một cách hiệu quả, chống giả mạo (cho phép người nhận kiểm tra thông tin có bị thay đổi không), xác thực danh tính của người gửi. Ngoài ra chứng chỉ số còn là bằng chứng giúp chống chối cãi nguồn gốc, ngăn chặn người gửi chối cãi nguồn gốc tài liệu mình đã gửi.

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)

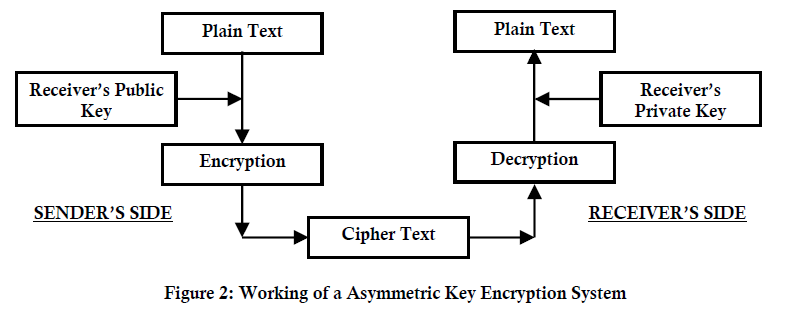
+ Rất khó để áp dụng tính chống chối bỏ (non-repudiation) cho các nhóm giao tiếp chia sẻ chung một khóa.

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.

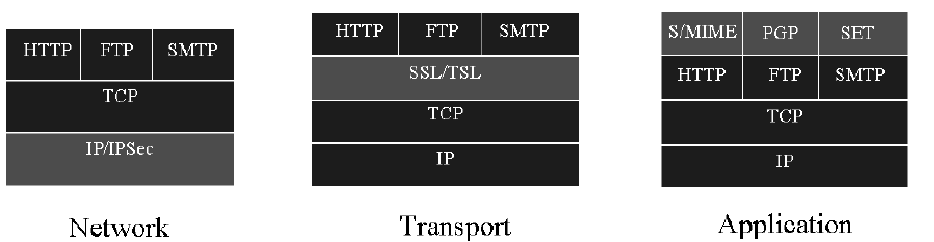
Các giao thức đảm bảo giao dịch – SSL, SET

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 dựa trên chức năng chính của tầng đó và các dịch vụ cung cấp bởi tầng dưới. Kiến trúc module này có lợi thế là xác định rõ nhiệm vụ của mỗi bộ phận, dễ dàng bảo trì và nâng cấp hệ thống (ví dụ thay đổi bên trong một bộ phận không ảnh hưởng tới các bộ phận khác). Ngoài hai tầng dưới cùng là tầng vật lý và tầng data-link, ba tầng trên 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 mạng (Network layer), 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 riêng một cá nhân là không thể.

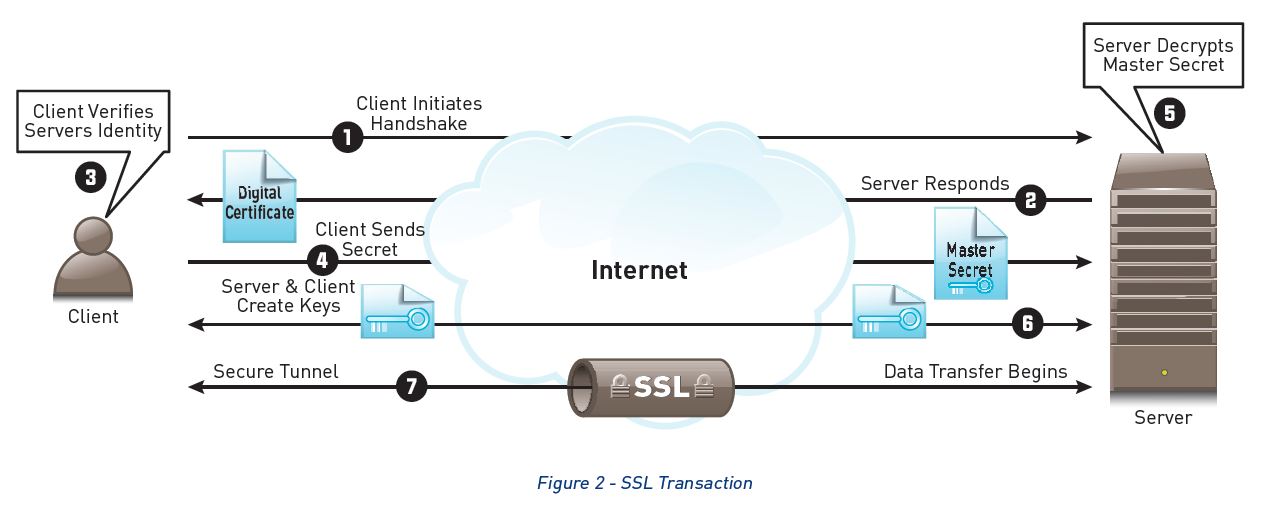
Secure Socket Layer

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 là một ứng dụng cung cấp chức năng bảo mật được cài đặt ở tầng cao nhất – tầng App. Khác với SSL, dù có thể bảo vệ được thông tin nhưng hacker vẫn có thể lấy được danh tính các bên tham gia giao dịch, SET được tích hợp với các cổng thanh toán (payment gateway) bên bán, giúp giải quyết vấn đề bảo mật danh tính cũng như các thông tin được trao đổi.

Em sẽ trình bày rõ hơn về cơ chế hoạt động của giao thức SET ở chương tiếp theo.

Chương 3 -

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

Giao thức SET

Các khái niệm

Chữ ký số (digital signature): là phương tiện được sử dụng để xác thực nhận dạng của người gửi tin nhắn hoặc người ký tài liệu và để đảm bảo một điều chắc chắn rằng nội dung gốc của tin nhắn hoặc tài liệu đã gửi sẽ không bị thay đổi. Chữ ký số dễ kiểm tra và nhận dạng, tuy nhiên phải không thể tính toán để giả mạo được. Nó có năng lực đảm bảo tài liệu gốc sẽ được gửi đến nơi và cả người gửi cũng không dễ để không công nhận nó sau này.

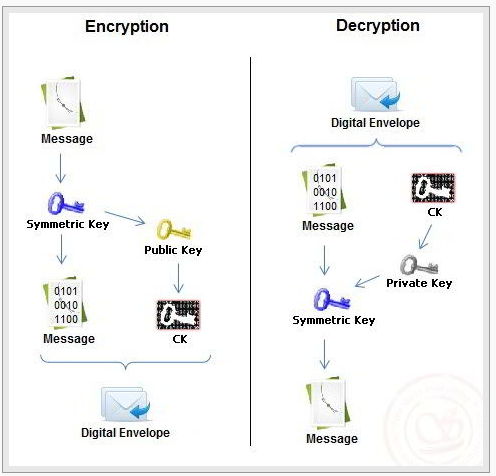
Chứng chỉ số (digital certificate): là một tệp tin điện tử dùng để xác minh danh tính một cá nhân, một máy chủ, một công ty… trên Internet. Nó giống như bằng lái xe, hộ chiếu, chứng minh thư hay những giấy tờ xác minh cá nhân và phải được cơ quan có thẩm quyền cấp. Tổ chức đứng ra chứng nhận những thông tin của bạn là chính xác được gọi là Nhà cung cấp chứng thực số (CA – Certificate Authority). CA phải đảm bảo về độ tin cậy, chịu trách nhiệm về độ chính xác của chứng chỉ số mà mình cấp.

<http://inet.edu.vn/tin-tuc/2150/chung-chi-so-cong-cu-bao-mat-thong-tin-truyen-qua-internet.html>

Phong bì số (digital envelope): Thuật toán phong bì số kết hợp được ưu điểm của cá khóa đối xứng và khóa bất đối xứng. Nội dung được mã hóa và giải mã bằng khóa đối xứng và khóa đối xứng được mã hóa bằng khóa công khai được chuyển đến cho người nhận trong một khối gọi là phong bì số.

Khác với chữ ký số chỉ sử dụng cặp khóa bất đối xứng chủ yếu đảm bảo tính toàn vẹn, chứng thực nội dung, phong bì số sử dụng cả khóa đối xứng và khóa bất đối xứng để bảo vệ nội dung an toàn, ngăn cản xem trộm và đánh cắp nội dung. Cặp khóa bất đối xứng cũng bao gồm khóa công khai và khóa riêng. Sử dụng cặp khóa bất đối xứng để mã hóa an toàn hơn nhưng tốc độ lại chậm hơn. Do đó phong bì số không dùng cặp khóa bất đối xứng để mã hóa thông điệp mà dùng nó để mã hóa khóa đối xứng, giúp độ an toàn vẫn được dữ nguyên nhưng tốc độ nhanh hơn (do khóa đối xứng chỉ 128 bit).

Sơ lược cách làm việc của phong bì số



Thông điệp sẽ được mã hóa bởi khóa đối xứng

Sau đó khóa đối xứng được mã hóa bởi khóa công khai của người nhận để tạo thành khóa CK

Thông điệp đã mã hóa kết hợp với CK tạo thành phong bì số và được gửi đi.

Muốn xem được thông điệp, người nhận phải có được khóa đối xứng, muốn có được khóa đối xứng người nhận phải sở hữu khóa riêng tương ứng. Do đó, thông điệp khá an toàn do các cặp khóa này được sinh ngẫu nhiên và duy nhất.

Các thuật toán

SHA (Secure Hash Algorithm – giải thuật băm an toàn) là thuật toán dùng để chuyển một đoạn dữ liệu nhất định thành một đoạn dữ liệu có chiều dài không đổi với xác suất khác biệt cao. Những giải thuật này được gọi là “an toàn” vì theo chuẩn FIPS 180-2:

Cho một giá trị băm nhất định được tạo nên bởi một trong những giải thuật SHA, việc tìm lại được đoạn dữ liệu gốc là không khả thi.

Việc tìm được hai đoạn dữ liệu khác nhau có cùng kết quả băm tạo ra bởi một trong những thuật giải SHA là không khả thi. Bất cứ thay đổi nào trên đoạn dữ liệu gốc, dù nhỏ, cũng sẽ tạo nên một giá trị băm hoàn toàn khác với xác suất rất cao.

Thuật toán SHA-1 trả lại kết quả dài 160 bit.

Ví dụ sử dụng thuật toán SHA-1 (dữ liệu gốc được ngầm hiểu sử dụng bảng mã ASCII)

SHA1("The quick brown fox jumps over the lazy dog")

= 2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12

Ngay cả một thay đổi nhỏ trong đoạn dữ liệu gốc sẽ tạo nên một giá trị băm hoàn toàn khác. Ví dụ sửa “d” thành “c” ở chữ cuối cùng.

SHA1("The quick brown fox jumps over the lazy cog")

= de9f2c7f d25e1b3a fad3e85a 0bd17d9b 100db4b3

Giá trị băm của một đoạn dữ liệu rỗng

SHA1("")

= da39a3ee 5e6b4b0d 3255bfef 95601890 afd80709

RSA: Thuật toán được Ron Rivest, Adi Shamir và Len Adleman mô tả lần đầu tiên vào năm 1977 tại học viện công nghệ Massachusetts(MIT). Tên của thuật toán lấy từ 3 chữ cái đầu của tên 3 tác giả.

Ý tưởng then chốt để đảm bảo tính an toàn của RSA là dựa trên sự khó khăn trong việc phân tích nhân tử của 2 số nguyên tố lớn. (a x b = c, tìm ngược lại a, b từ c là phân tích nhân tử).

Thuật toán RSA có hai khóa: khóa công khai (hay khóa công cộng) và khóa bí mật (hay khóa cá nhân). 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 cá nhân (bí mật) mới có thể giải mã được.

DES (Data Encryption Standard):

DES là thuật toán mã hóa khối: nó xử lý từng khối thông tin của bản rõ có độ dài xác định và biến đổi theo những quá trình phức tạp để trở thành khối thông tin của bản mã có độ dài không thay đổi. Trong trường hợp của DES, độ dài mỗi khối là 64 bit. DES cũng sử dụng khóa để cá biệt hóa quá trình chuyển đổi. Nhờ vậy, chỉ khi biết khóa mới có thể giải mã được văn bản mã. Khóa dùng trong DES có độ dài toàn bộ là 64 bit. Tuy nhiên chỉ có 56 bit thực sự được sử dụng; 8 bit còn lại chỉ dùng cho việc kiểm tra. Vì thế, độ dài thực tế của khóa chỉ là 56 bit.

Hiện nay DES được xem là không đủ an toàn cho nhiều ứng dụng. Nguyên nhân chủ yếu là độ dài 56 bit của khóa là quá nhỏ. Gần đây DES đã được thay thế bằng AES (Advanced Encryption Standard, hay Tiêu chuẩn Mã hóa Tiên tiến).

Yêu cầu kĩ thuật của SET

Các thành phần của hệ thống SET

Các thành phần chính tham gia một hệ thống SET bao gồm:

Người mua (cardholder): chủ nhân thẻ tín dụng và mua hàng qua mạng Internet

Người bán (merchant): người hoặc tổ chức bán hàng và dịch vụ cho người mua

Nhà phát hành thẻ (issuer): tổ chức tài chính cung cấp thẻ tín dụng cho người mua và chịu trách nhiệm thanh toán

Bên cung cấp dịch thanh toán (Acquirer): là tổ chức tài chính cung cấp dịch vụ thanh toán, xử lý các giao dịch trực tuyến và đảm bảo về mặt tài chính cho giao dịch. Acquirer đóng vai trò liên hệ với các ngân hàng phát hành xin chuẩn chi cho một giao dịch xin cấp phép

Cổng thanh toán (Acquirer payment gateway): hoạt động như một giao diện giữa SET và mạng máy tính của ngân hàng.

Nhà cung cấp chứng thực số (Certifying Authority – CA): tổ chức cung cấp chứng chỉ khóa công khai, tiêu biểu là Verisign. Họ cung cấp nhiều loại chứng chỉ, trong đó chứng chỉ cấp 1 thấp nhất chỉ ràng buộc địa chỉ email với khóa liên kết tương ứng. Chứng chỉ cấp 4 cao nhất được dùng cho các máy chủ và tổ chức.

SET hoạt động như thế nào?

Trước hết cả người mua và người bán đều phải đăng kí với cơ quan chứng nhận.

Các bước giao dịch SET

Khách hàng sử dụng trình duyệt Web và lựa chọn món hàng cần mua bằng cách thêm nó vào danh mục mua.

Khách hàng giao tiếp với người bán và cổng giao dịch bằng một bản tin, bao gồm hai phần:

Phần a: Yêu cầu mua hàng tới người bán

Phần b: thông tin thẻ cho ngân hàng của bên bán

Bên bán chuyển tiếp thông tin thẻ (phần b) tới ngân hàng của họ.

Ngân hàng liên lạc với đơn vị cung cấp thẻ cho người mua và kiểm tra quyền thanh toán

Đơn vị cung cấp thẻ xác thực thanh toán và phản hồi về ngân hàng.

Ngân hàng gửi một bản sao xác thực tới cửa hàng

Cửa hàng hoàn thành yêu cầu mua hàng và gửi xác nhận tới khách hàng

Cửa hàng nhận giao dịch từ ngân hàng

Đơn vị cung cấp thẻ in hóa đơn thẻ tín dụng cho khách hàng.

Quá trình mã hóa trong SET

Thuật toán sử dụng:

Thuật toán RSA 1024 bit cho quá trình mã hóa bất đối xứng

Thuật toán DES 56 bit cho quá trình mã hóa đối xứng

SHA-1 (Secure Hash Algorithm) để tính toán băm các bản tin

Quá trình mã hóa ở bên gửi S:

Bước 1. Bên gửi S tạo một thông điệp ban đầu. Thông qua thuật toán băm (hash) để biến thông điệp ban đầu thành một tóm lược thông điệp (message digest). SET sử dụng thuật toán SHA-1.

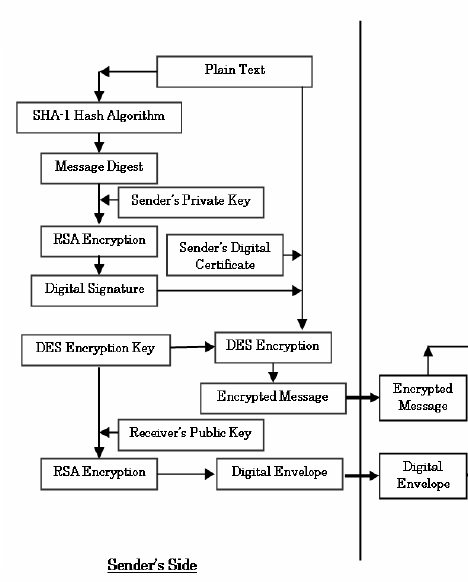
Bước 2. S mã hóa tóm tắt thông điệp đó bằng khóa riêng RSA. Đầu ra của bước này là một chữ kí số.

Bước 3. S tạo một khóa cho quá trình mã hóa đối xứng DES

Bước 4. S lấy toàn bộ thông điệp ban đầu (bước 1), chữ ký số (bước 2), và chứng chỉ số của nó rồi mã hóa bằng khóa đối xứng theo thuật toán DES. Kết quả của bước này là thông điệp đã được mã hóa.

Bước 5. S lựa chọn khóa một công khai của bên nhận R. Mã khóa khóa công khai (bước 3) và tạo ra một phong bì số.

Thông điệp đã mã hóa ở bước 4 và phong bì số ở bước 5 được gửi tới bên nhận R.



Quá trình giải mã trong SET

Thuật toán sử dụng: Giống như quá trình mã hóa

Quá trình giải mã ở bên nhận R.

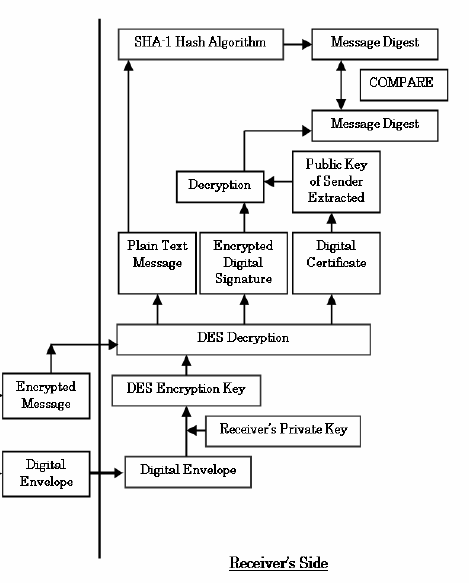
Bước 1. Bên nhận R giải mã phong bì số bằng khóa riêng RSA và nhận được khóa đối xứng DES.

Bước 2. Sử dụng khóa đối xứng DES ở bước 1, bên nhận giải mã thông điệp mã hóa nhận được từ bên gửi S thu được thông điệp text (plain text message), chữ kí số và chứng chỉ số của bên gửi S.

Bước 3. Từ chứng chỉ số của S vừa thu được, R giải nén lấy khóa công khai RSA của S.

Bước 4. Sử dụng khóa công khai RSA của S, thông điệp mã hóa được giải mã thành tóm lược thông điệp số 1.

Bước 5. Thông điệp text (nhận được ở bước 2) được R đưa qua thuật toán băm SHA-1 thu được tóm lược thông điệp số 2. Hai tóm lược thông điệp số 1 và số 2 được so sánh với nhau, nếu chúng giống nhau thì xác thực của bên gửi S được bảo đảm.



Chữ ký kép (Dual Signatures)

Do người mua giao tiếp với người bán và cổng thanh toán bằng một thông điệp duy nhất bao gồm hai phần là yêu cầu đặt hàng và thông tin thẻ, cần đảm bảo rằng:

Bên bán không thể nhìn thấy được thông tin các lệnh giao dịch chuyển tiền

Bên cung cấp dịch vụ thanh toán không thể biết được thông tin cụ thể các đơn hàng

Đồng thời khách hàng cũng cần được biết là khoản thanh toán là cho chính đơn hàng mình đã mua. Các yêu cầu trên có thể đạt được bằng khái niệm “chữ ký kép” trong SET.

Chữ kí kép được tạo ra như thế nào?

Bước 1. Khách hàng lấy dữ liệu thanh toán (Payment Information – PI) và đưa vào hàm xử lý băm SHA-1 nhận được tóm lược thông điệp thanh toán (Payment Information Message Digest – PIMD)

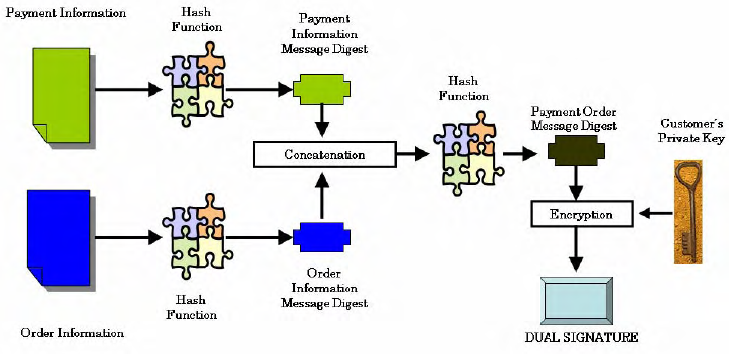
Bước 2. Khách hàng lấy dữ liệu đơn hàng (Order Information – OI) và đưa vào hàm xử lý băm SHA-1 nhận được tóm lược thông điệp đơn hàng (Order Information Message Digest – OIMD).

Bước 3. Nối PIMD với OIMD lại thành một chuỗi

Bước 4. Đưa chuỗi kết hợp đó vào xử lý băm SHA-1 nhận được tóm lược thông điệp thanh toán đơn hàng (Payment Order Message Digest – POMD)

Bước 5. Mã hóa POMD bằng khóa RSA công khai của khách hàng nhận được chữ kí kép.

Quá trình được minh họa như sau:



Chữ ký kép đem lại lợi ích gì đối với ngân hàng?

Quá trình mã hóa

Các bước thực hiện của khách hàng C sau khi tạo ra chữ ký kép

Bước 1. Khách hàng C tạo ra một khóa cho mã hóa đồng bộ DES

Bước 2. C sử dụng phương pháp mã hóa DES để mã hóa thông điệp PI, chữ kí kép, chứng chỉ của C, và OIMD. Kết quả nhận được thông điệp mã hóa.

Bước 3. C lấy một khóa công khai RSA của ngân hàng B. Mã hóa khóa đồng bộ DES ở bước 1 nhận được phong bì số.

Thông điệp mã hóa và phong bì số được gửi tới ngân hàng B

Quá trình giải mã

Các bước xử lý của ngân hàng B sau khi nhận được thông điệp mã hóa và phong bì số:

Bước 1. Ngân hàng B sử dụng khóa riêng RSA của B để giải mã phong bì số nhận được khóa đối xứng DES.

Bước 2. B sử dụng khóa đối xứng DES để giải mã phần đầu tiên của thông điệp mã hóa nhận được PI, chữ kí kép, chứng chỉ của khách hàng và OIMD.

Bước 3. B đưa PI vào xử lý băm SHA-1 để lấy PIMD.

Bước 4. B nối PIMD và OIMD lại thành mỗi chuỗi và xử lý hàm băm SHA-1. Kết quả nhận được POMD.

Bước 5. B giải mã phần còn lại của thông điệp mã hóa là chữ kí kép bằng khóa công khai của khách hàng (nhận được từ chứng chỉ số của khách hàng). Kết quả thu được một bản sau của POMD.

Bước 6. So sánh POMD nhận được ở bước 4 và bước 5. Nếu chúng giống nhau chứng tỏ thông điệp được gửi tới từ đúng khách hàng.

Đăng ký cấp chứng chỉ cho các bên tham gia giao dịch điện tử

Sự bảo đảm giao dịch của SET được xây dựng dựa trên các chứng chỉ được cấp cho các bên tham gia quá trình giao dịch điện tử. Để nhận được một chứng chỉ, người dùng phải có một định danh duy nhất (ID) và khóa công khai tương ứng được chứng nhận bởi một cơ quan có thẩm quyền (Certificate Authority - CA).

Nếu CA xác thực người dùng là thật, CA sẽ kết hợp ID và khóa công khai lại thành một chữ kí số (sử dụng khóa riêng của họ, thường bằng cách tạo tóm lược thông điệp). Chữ kí số này có thể được xác thực lại bằng khóa công khai của CA. Như vậy, khi các bên còn lại muốn xác thực một khóa công khai của một người dùng cụ thể, họ sẽ yêu cầu một bản sao khóa công khai của CA và tiến hành xác thực.

Có ba bên tham gia một giao dịch cần phải được đăng ký xác thực

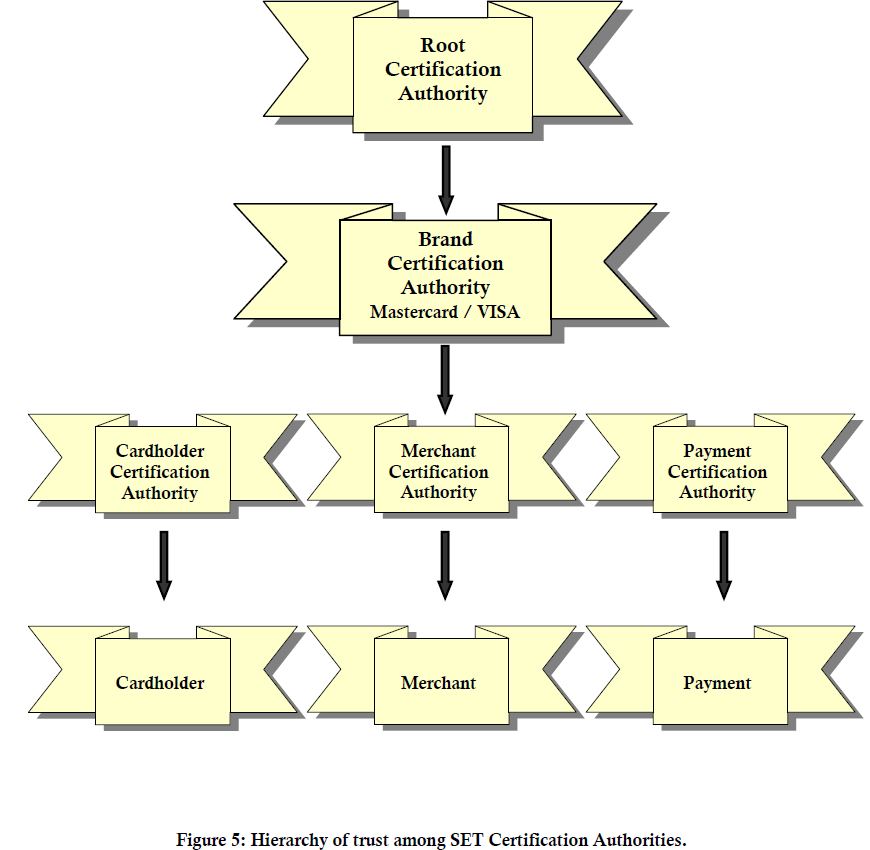
+ Khách hàng (chủ nhân thẻ tín dụng)

+ Cửa hàng / người bán

+ Cổng thanh toán điện tử

SET định nghĩa một hệ thống phân cấp cho việc tạo và phân phối chứng chỉ khóa công khai cho các bên tham gia giao dịch. Thành viên cao nhất của hệ thống là cơ quan cấp chứng chỉ gốc (root certificate authority) điều hành bởi SETCo. Cơ quan này cung cấp chứng chỉ khóa công khai cho các tổ chức thanh toán tài chính. Các tổ chức tài chính này lại trở thành cơ quan chứng nhận (brand certificate authority) cấp quyền cho các ngân hàng thành viên.

Mỗi cơ quan chứng nhận có chức năng cấp chứng chỉ cho từng loại đối tượng khác nhau. Cơ quan cung cấp quyền thẻ tín dụng cấp chứng chỉ khóa công khai cho khách hàng. Ngân hàng kinh doanh hoặc cơ quan cấp quyền cấp chứng chỉ khóa công khai cho người bán hàng. Các đơn vị cấp chứng chỉ riêng cho cổng thanh toán điện tử.



Các hạn chế của SET

Thử nghiệm

Kết luận