HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÙI QUANG MINH

NGHIÊN CỨU GIẢI PHÁP BẢO MẬT CHO HỆ THỐNG THANH TOÁN ĐIỆN TỬ

Chuyên ngành: Hệ Thống Thông Tin
Mã số: 8.48.01.04

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI - NĂM 2020

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: **TS. VŨ VĂN THỎA**

Phản biện 1: ……

Phản biện 2: ……..

Luận văn sẽ được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: ..... giờ ..... ngày ..... tháng .... năm .....

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông

MỞ ĐẦU

Hiện nay, các hình thức thanh toán không dùng tiền mặt, đã và đang nhận được sự quan tâm, hưởng ứng tại Việt Nam. Hình thức thanh toán này sẽ góp phần giảm tối đa lượng tiền mặt trong lưu thông, đem lại những lợi ích to lớn cho doanh nghiệp, khách hàng, được nhà nước khuyến khích sử dụng. Ngoài ra, khi sử dụng các dịch vụ thanh toán không dùng tiền mặt giúp cho người sử dụng như: không phải mang theo tiền mặt mà có thể chi trả cho các giao dịch mua bán, tăng tính an toàn cho bản thân và tài sản, rất dễ sử dụng và kiểm soát tài chính trong tài khoản.

Các hệ thống thanh toán điện tử được triển khai đã hỗ trợ tích cực cho hình thức thanh toán không dùng tiền mặt. Tuy nhiên, các giao dịch dựa trên các phương tiện điện tử đặt ra các đòi hỏi rất cao về bảo mật và an toàn. Khi làm việc với thế giới của máy tính kết nối mạng, người dùng phải đối mặt với hiểm họa liên quan đến việc bảo mật các luồng thông tin trên đó. Mặt khác, người dùng sẽ không sử dụng các dịch vụ thanh toán điện tử khi còn có những lo ngại về rủi ro có thể gặp phải như: không thực hiện được các giao dịch do lỗi mạng, mất tiền trong tài khoản, lộ các thông tin cá nhân, … . Vì vậy vấn đề bảo mật thanh toán là một trong những vấn đề trọng yếu nhất của Thanh toán điện tử.

Trong thời gian qua, các vụ trộm cắp tài khoản và gian lận thanh toán đang ngày càng gia tăng trên các nền tảng giao dịch online. Vấn đề an toàn và bảo mật đã trở thành mối quan tâm hàng đầu của khách hàng và yêu cầu tất yếu đối với các doanh nghiệp thương mại điện tử và bán lẻ khi sử dụng hệ thống thanh toán điện tử.

Do yêu cầu phát triển to lớn của dịch vụ thanh toán nên cần phải nâng cao, tăng cường bảo mật hơn cho hệ thống thanh toán điện tử.

Xuất phát từ thực tế và mục tiêu như trên, học viên chọn thực hiện đề tài luận văn tốt nghiệp chương trình đào tạo thạc sĩ có tên: "**Nghiên cứu giải pháp bảo mật cho hệ thống thanh toán điện tử**".

Mục đích của luận văn là nghiên cứu các giải pháp bảo mật cho hệ thống thanh toán điện tử. Trên cơ sở đó đề xuất xây dựng các giải pháp bảo mật hệ thống thanh toán điện tử phù hợp cho Tổng công ty Viễn thông MobiFone có thể triển khai ứng dụng trong thực tế.

Đối tượng nghiên cứu của luận văn là Hệ thống thanh toán điện tử và các vấn đề liên quan đến an toàn, bảo mật hệ thống.

Phạm vi nghiên cứu của luận văn là các giải pháp bảo mật hệ thống thanh toán điện tử nói chung và đề xuất các giải pháp bảo mật hệ thống thanh toán điện tử phù hợp cho Tổng công ty Viễn thông MobiFone.

Phương pháp nghiên cứu:

- ***Về mặt lý thuyết***: Thu thập, khảo sát, phân tích các tài liệu và thông tin có liên quan đến bảo mật hệ thống thanh toán điện tử.

- ***Về mặt thực nghiệm***: Khảo sát thực tế về hệ thống thanh toán điện tử của Tổng công ty Viễn thông MobiFone và đề xuất các giải pháp bảo mật phù hợp.

Bố cục của luận văn gồm 3 chương chính với các nội dung sau:

Chương 1: Tổng quan về hệ thống thanh toán điện tử

Nội dung nghiên cứu của chương 1 là khảo sát tổng quan hệ thống thanh toán điện tử và các vấn đề liên quan.

Chương 2: Giải pháp bảo mật cho hệ thống thanh toán điện tử

Nội dung của chương 2 luận văn tập trung nghiên cứu một số giải pháp bảo mật cho hệ thống thanh toán điện tử nhằm bảo đảm các yêu cầu bảo mật hệ thống và các vấn đề liên quan.

Chương 3: Xây dựng giải pháp bảo mật cho hệ thống thanh toán điện tử của Tổng công ty Viễn thông MobiFone

Chương 3 của luận văn nghiên cứu đề xuất giải pháp bảo mật hệ thống thanh toán điện tử phù hợp cho Tổng công ty Viễn thông MobiFone.

Chương 1: Tổng quan về hệ thống thanh toán điện tử

Chương 1 luận văn khảo sát tổng quan về hệ thống thanh toán điện tử, các yêu cầu kỹ thuật công nghệ đối với hệ thống, một số vấn đề về bảo mật trong hệ thống thanh toán điện tử và các vấn đề liên quan.

1.1 Giới thiệu chung về hệ thống thanh toán điện tử

1.1.1 Thương mại điện tử và thanh toán điện tử

Thương mại điện tử (hay còn gọi là e-commerce, e-comm hay EC) hiểu một cách đơn giản là hoạt động mua bán sản phẩm hay dịch vụ thông qua Internet và các phương tiện điện tử khác. Các giao dịch này gồm tất cả hoạt động như: mua bán, thanh toán, đặt hàng, quảng cáo và giao hàng ... Có nhiều tổ chức lớn trên thế giới đưa ra các định nghĩa khác nhau cho khái niệm của thương mại điện tử.

Thanh toán bằng thẻ

Thanh toán qua cổng thanh toán điện tử

Thanh toán bằng ví điện tử

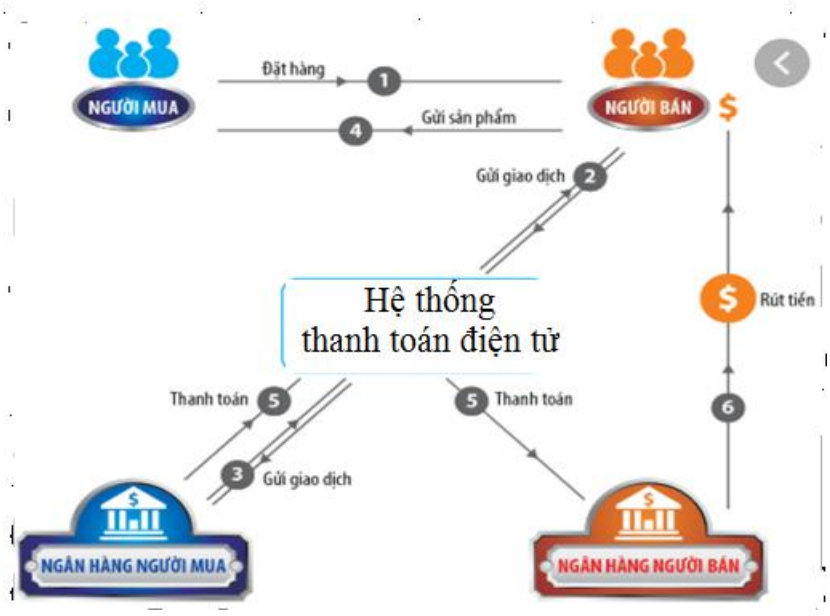
Thanh toán bằng thiết bị điện thoại thông minh

Thanh toán qua Mobile Banking:

Thanh toán qua QR Code:

1.1.2 Mô hình hệ thống thanh toán điện tử

Các hệ thống thanh toán điện tử triển khai trong thực tế rất đa dạng về hình thức và công nghệ sử dụng. Hình 1.1 dưới đây trình bày mô hình chung cho một hệ thống thanh toán điện tử.



Hình 1.1: Mô hình hệ thống thanh toán điện tử

Trong mô hình trên, hệ thống thanh toán điện tử là trung gian kết nối giữa người mua, người bán, thực hiện thanh toán cho các giao dịch dựa trên kết nối với ngân hàng của người mua và người bán.

1.1.3 Lợi ích của thanh toán điện tử và nhu cầu thực tế

Thanh toán điện tử mang lại nhiều lợi ích cho người sử dụng.

- Thanh toán điện tử được thực hiện nhanh chóng, tiện dụng:

- Dễ dàng theo dõi và kiểm soát

Hạn chế rủi ro:

Hỗ trợ kinh doanh trực tuyến:

1.2 Các yêu cầu kỹ thuật đối với hệ thống thanh toán điện tử

Hệ thống thanh toán điện tử phải đảm bảo các tính năng chính như sau:

Tính sẵn sàng:

Hệ thống thanh toán điện tử có thể thực hiện thanh toán vào bất cứ thời điểm nào và bất cứ nơi nào (mọi lúc, mọi nơi) cho mọi giao dịch hợp pháp.

Tính chính xác:

Hệ thống thanh toán điện tử phải đảm bảo chính xác tuyệt đối trong các giao dịch gửi tiền, thanh toán và quản lý.

Tính toàn vẹn:

Các thuộc tính của các thông tin giao dịch vẫn còn nguyên vẹn trong quá trình truyền và không thể được thay đổi.

Tính bí mật:

Mọi thông tin về tài khoản và nội dung các giao dịch của khách hàng phải được giữ bí mật. Do đó các kỹ thuật mã hóa thường được sử dụng trong các hệ thống thanh toán điện tử.

Để đảm bảo các tính năng trên cho hệ thống thanh toán điện tử cần có các yêu cầu kỹ thuật cho hạ tầng mạng, hệ thống phần mềm sử dụng và cơ sở dữ liệu [2].

1.2.1 Yêu cầu đối với hạ tầng mạng

1.2.2 Yêu cầu đối với phần cứng và phần mềm hệ thống

1.2.3 Yêu cầu đối với cơ sở dữ liệu

1.3 Một số vấn đề bảo mật trên thanh toán điện tử

Vấn đề bảo mật hệ thống thanh toán điện tử có vai trò cực kỳ quan trọng trong triển khai và vận hành hệ thống. Hiện nay, các vấn đề bảo mật đe dọa hệ thống thanh toán điện tử đang thay đổi liên tục và diễn ra cực kỳ nhanh chóng. Các mối đe dọa phổ biến nhất bao gồm tấn công mạng và lan truyền virus.

1.3.1 Thực trạng tấn công mạng tại Việt nam

Các tấn công mạng tại Việt Nam thường là các tấn công vào các trang web, trong đó có các hệ thống thanh toán điện tử. Trong năm 2017, Việt Nam đã hứng chịu rất nhiều các vụ tấn công mạng và để lại rất nhiều hậu quả nặng nề. Chỉ riêng quý 1 năm 2017, Việt Nam đã có gần 7700 sự cố tấn công mạng tại Việt Nam. Đến giữa tháng 9 số lượng các sự cố tấn công mạng đã lên đến gần 10000 (số liệu của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam – VNCERT) [14]. Trong đó có 1762 sự cố website lừa đảo, 4595 sự cố phát tán mã độc và 3607 sự cố tấn công thay đổi giao diện.

Trong quý I/2019, VNCERT ghi nhận có 4.770 sự cố tấn công mạng vào các trang web của Việt Nam. Cũng trong thời gian này hệ thống giám sát của VNCERT ghi nhận tổng cộng có hơn 78,3 triệu sự kiện mất an toàn thông tin tại Việt Nam.

Các thông tin và số liệu trên cho thấy một thực trạng đáng báo động về bảo mật mạng nói chung và bảo mật các hệ thống thanh toán điện tử tại Việt Nam hiện nay.

1.3.1 Các yêu cầu bảo mật hệ thống thanh toán điện tử

Các hệ thống thanh toán điện tử thường được triển khai liên quan đến ngân hàng và các tổ chức tín dụng và hạ tầng mạng kèm theo. Do đó, cần xác định các vấn đề và biện pháp bảo mật phù hợp áp dụng cho từng thành phần trong mô hình triển khai như sau:

- Các vấn đề và biện pháp bảo mật ứng dụng (Application security).
- Các vấn đề và biện pháp bảo mật máy chủ (Host security)
- Các vấn đề và biện pháp bảo mật theo tô pô hệ thống triển khai (Deployment topologies), trong đó có các biện pháp áp dụng cho thành phần ứng dụng cục bộ (Local application tier) và các biện pháp áp dụng cho thành phần ứng dụng ở xa (Remote application tier).
- Các vấn đề và biện pháp bảo mật hạ tầng mạng (Network insfrastructure security) để chống được các cuộc tấn công mạng như DoS, DDoS, ….
- Các chính sách và thủ tục an toàn (Security policies and procedures) cho toàn bộ hệ thống thanh toán điện tử được triển khai.

Theo quy định của ngân hàng nhà nước Việt Nam [2], các hệ thống thanh toán điện

tử phải đảm bảo các yêu cầu về an toàn bảo mật sau đây.

Một số yêu cầu chung

1. Đảm bảo tính bí mật

2. Đảm bảo tính sẵn sàng

3. Đảm bảo tính toàn vẹn

4. Xác thực khách hàng và xác thực giao dịch

5. Bảo vệ khách hàng

1.4 Một số giải pháp xây dựng hệ thống thanh toán điện tử

Hiện nay, rất nhiều hệ thống thanh toán điện tử được triển khai trong thực tế của các ngân hàng, các tổ chức tài chính cũng như các hãng cung cấp các dịch vụ công nghệ thông tin và truyền thông. Trong mục này luận văn sẽ khảo sát một số hệ thống thanh toán điện tử tiêu biểu [4], [5].

1.4.1 Hệ thống thanh toán điện tử dựa trên thẻ thông minh (Smart-card)

1.4.2 Hệ thống thanh toán điện tử dựa trên Internet Banking

1.4.3 Hệ thống thanh toán điện tử dựa trên điện thoại di động

1.4.4 Hệ thống thanh toán sử dụng ví điện tử

1.4.4 Hệ thống sử dụng cổng thanh toán điện tử

1.5 Kết luận chương 1

Chương II: Giải pháp bảo mật cho hệ thống thanh toán điện tử

Chương 2 luận văn sẽ khảo sát tổng quan về bảo mật trong thanh toán điện tử. Từ đó, luận văn nghiên cứu một số giải pháp bảo mật cho hệ thống thanh toán điện tử và một số vấn đề liên quan.

2.1. Tổng quan về bảo mật trong thanh toán điện tử

2.1.1. Giới thiệu

2.1.2 Một số phương thức tấn công hệ thống thanh toán điện tử điển hình

Tấn công làm sai lệch các giao dịch thanh toán điện tử

Nghe trộm sự truyền dẫn thông tin thanh toán điện tử

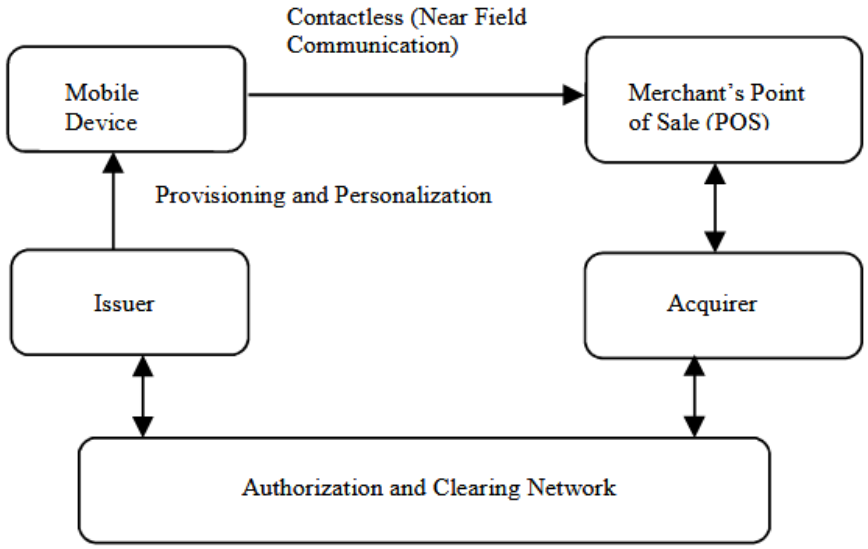
Các tấn công chống lại các bản tin giao dịch thanh toán điện tử

Các tấn công ở giữa

Truy nhập bất hợp pháp đến các dịch vụ của thống thanh toán điện tử

2.1.3 Kiến trúc bảo mật trong hệ thống thanh toán điện tử

Trong hệ thống thanh toán điện tử, vấn đề bảo mật là yêu cầu xem xét một số khía cạnh và các quá trình như truy nhập vô tuyến, tính di động của người sử dụng đầu cuối, các nguy cơ bảo mật đặc biệt, các kiểu thông tin cần phải được bảo vệ, và độ phức tạp của kiến trúc mạng. Hơn nữa, các topo mạng phức tạp và tính không đồng nhất của các công nghệ làm tăng thách thức bảo mật. Hình 2.1 dưới đây mô tả kiến trúc bảo mật điển hình trong hệ thống thanh toán điện tử dựa trên điện thoại di động theo đề xuất của tiêu chuẩn EMV [8].



Hình 2.1: Kiến trúc bảo mật trong hệ thống thanh toán điện tử

2.2 Giải pháp bảo mật dựa trên mật khẩu sử dụng 1 lần

2.2.1 Khái niệm mật khẩu sử dụng 1 lần

Mật khẩu sử dụng 1 lần (One Time Password - OTP) là một mật khẩu chỉ có giá trị trong một phiên đăng nhập làm việc. OTP có thể được sử dụng một lần cho việc xác thực người dùng hoặc cho người dùng xác thực một giao dịch. OTP thường được sử dụng trong các giao dịch thanh toán điện tử hoặc các hệ thống xác thực chặt chẽ.

2.2.2 Nguyên lý hoạt động của OTP

Sau khi đã đăng ký dịch vụ, mỗi lần muốn đăng nhập (log in), người dùng sẽ được cung cấp một mật khẩu tạo ra bởi đầu đọc và thẻ thông minh hay thiết bị tạo mật khẩu dạng cầm tay (token) nhờ vào kết nối internet với máy chủ cung cấp dịch vụ OTP; hoặc cũng có thể thông qua thẻ OTP được tạo sẵn hay điện thoại di động. Mật khẩu này sẽ tự mất hiệu lực sau một khoảng thời gian nhất định. Như vậy, nếu bị lộ mật khẩu thì người có được mật khẩu đó cũng không thể dùng được, và do đó giải pháp OTP có tính bảo mật cao.

2.2.3 Các mô hình sinh OTP

Có hai mô hình thường được sử dụng để sinh mã OTP là: sinh mã OTP theo thời gian và sinh mã OTP theo sự kiện.

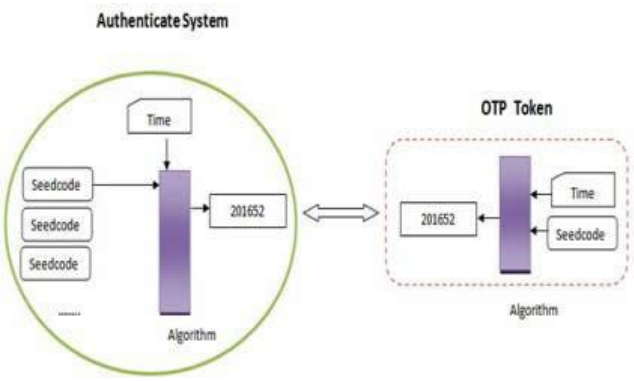
Mô hình sinh mã OTP theo thời gian

Theo cơ chế này, người dùng sẽ được cấp một thiết bị sinh mã được gọi là token (Hình 2.2) [6]. Bên trong token gồm có ba thành phần là: một mã seedcode, một đồng hồ đếm thời gian, và một thuật toán mã hóa một chiều.

- Mã seedcode: là mã được nhà sản xuất cài đặt sẵn trong token. Mỗi token có một mã seedcode khác nhau. Và mã seedcode này cũng được lưu lại trong hệ thống của nhà cung cấp dịch vụ tương ứng với tên truy nhập của người dùng.

- Đồng hồ đếm thời gian: là đồng hồ của token, nó được đồng bộ với đồng hồ của hệ thống trước khi giao cho người dùng. Mỗi khi người dùng bấm nút sinh mã, token sẽ lấy biến thời gian của đồng hồ. Biến thời gian được lấy chi tiết đến từng phút, hoặc 30 giây.

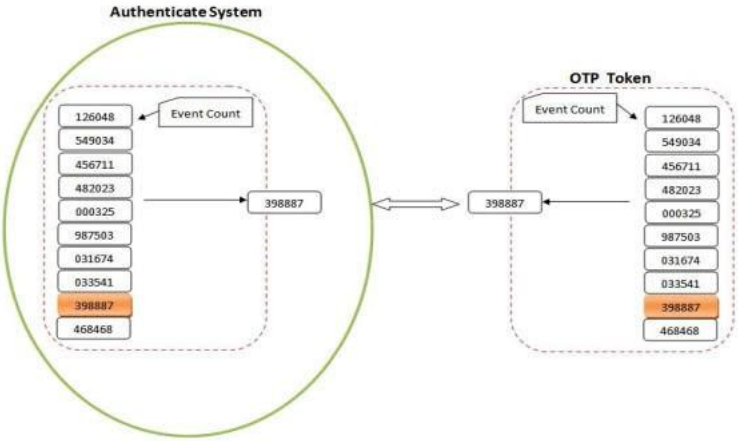
- Thuật toán mã hóa: sử dụng thuật toán băm SHA.



Hình 2.2: Mô hình của cơ chế sinh mã ngẫu nhiên dựa theo thời gian.

Mô hình sinh mã OTP theo sự kiện

Trong cơ chế này người dùng cũng được cấp một token như ở trên, nhưng bên trong token sẽ có một bộ đếm sự kiện thay vì đồng hồ đếm thời gian (Hình 2.3) [6]. Sự kiện được nhắc đến ở đây là sự kiện mà người dùng bấm nút sinh mã trên Token. Mỗi token sẽ chứa một số mã hữu hạn, có thứ tự và không thay đổi. Số lượng các mã hữu hạn đó được gọi là cửa sổ. Kích thước của cửa sổ này càng lớn thì độ bảo mật của giải pháp càng cao.



Hình 2.3: Mô hình của cơ chế sinh mã ngẫu nhiên dựa theo sự kiện

2.2.4 Các khuyến nghị tiêu chuẩn của OTP

Thuật toán băm: Độ an toàn của mã OTP phụ thuộc tính bảo mật của hàm băm. Tất cả các hệ thống sử dụng OTP phải hỗ trợ MD5, nên hỗ trợ SHA và có thể hỗ trợ MD4. Các thuật toán băm chấp nhận đầu vào tùy ý nhưng đầu ra cố định.

Khuôn dạng đầu vào:

Cấu trúc của từ đố:

otp-<tên thuật toán> <chuỗi số nguyên> <seed>

Khuôn dạng đầu ra: OTP tạo bởi thủ tục trên có 64 bit chiều dài. Việc nhập vào 64 bit khó khăn và dễ gây lỗi cho người sử dụng khi nhập bằng tay. Do vậy OTP có thể

chuyển đổi thành một chuỗi 6 từ ngắn (mỗi từ bao gồm 4 ký tự) theo chuẩn ISO-646 IVCS. Mỗi từ được chọn từ một từ điển gồm 2048 từ, 11 bit cho mỗi từ, tất cả OTP có thể được mã hóa.

2.2.5 Ưu điểm của OTP

Giải pháp bảo mật dựa trên mật khẩu sử dụng 1 lần có các ưu điểm như sau.

An toàn: Giải quyết tốt các vấn đề giả mạo, đánh cắp, Key logger. Đối với hai yếu tố xác thực, thiết bị này có thể được kết hợp với một mã PIN hoặc mật khẩu.

Dễ dàng sử dụng: Việc nhận dạng và xác thực được thực hiện trong vài giây tránh được nguy cơ bị lỗi khi gõ các mã OTP dài qua các mã từ một thiết bị chứng thực vào một máy tính (Ví dụ OTP Token sử dụng màn hình hiển thị).

Linh hoạt: Người dùng dễ dàng sử dụng cho các máy tính khác nhau và dễ mang theo bên mình.

Mã nguồn mở: Sẵn sàng tích hợp với nhiều ứng dụng mã nguồn mở.

Các giải pháp có thể ứng dụng OTP gồm: Web mail server; CRM (Hệ quản lý khách hàng); ERP (Hoạch định nguồn lực doanh nghiệp); Hệ thống quản lý tài liệu; Thương mại điện tử...

2.3 Giải pháp bảo mật dựa trên công nghệ Tokenization

2.3.1. Tổng quan về Tokenization

Tokenization (Số hóa thẻ) là giải pháp bảo mật dữ liệu dựa trên công nghệ thay thế những dữ liệu thanh toán "nhạy cảm" bằng mã token, nhằm nâng cao khả năng an toàn bảo mật trong thanh toán điện tử.

Tokenization là quá trình bảo vệ dữ liệu nhạy cảm bằng cách thay thế nó bằng một số được tạo bằng thuật toán gọi là token.

2.3.2. Lịch sử cuả Tokenization

Token vật lý từ lâu đã được sử dụng để thay thế tiền thật. Sòng bạc là một ví dụ như tiền giấy và tiền xu, biểu thị quyền sở hữu hợp pháp đối với loại tiền cơ bản.

Việc sử dụng token trong thế giới kỹ thuật số ra đời như một phương tiện thay thế dữ liệu nhạy cảm bằng một kỹ thuật số tương đương không nhạy cảm. Tokenization được TrustC Commerce giới thiệu lần đầu tiên vào năm 2001 như một phương tiện bảo vệ thông tin thẻ tín dụng.

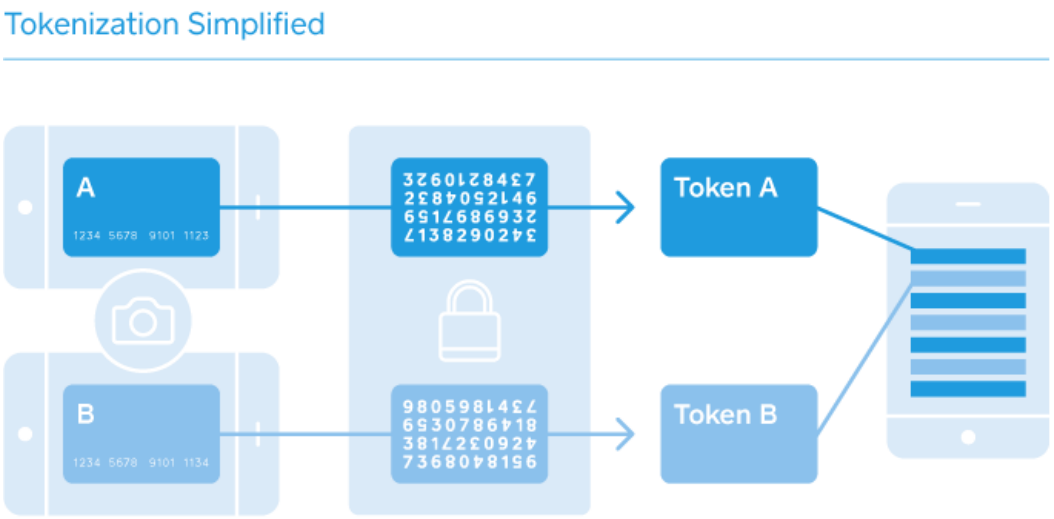
2.3.3. Mô hình của Tokenization trong thanh toán điện tử

Gần đây, ngày càng nhiều tổ chức chuyển từ mã hóa sang token hóa như một phương

pháp hiệu quả và an toàn hơn để bảo vệ thông tin nhạy cảm.

Một trong những cách sử dụng mã thông báo phổ biến nhất hiện nay là trong thanh toán điện tử. Tokenization cho phép người dùng lưu trữ thông tin thẻ tín dụng trong ví di động, giải pháp thương mại điện tử và phần mềm POS để cho phép thẻ được nạp lại mà không làm lộ thông tin thẻ gốc.

Hình 2.4 [13] dưới đây mô tả phương thức hoạt động của Tokenization.



Hình 2.4: Phương thức hoạt động của Tokenization

Tokenization thay thế chi tiết chủ thẻ nhạy cảm bằng các token độc lập. Điều này giúp bảo mật chi tiết tài khoản ngân hàng của khách hàng trong các giao dịch thẻ tín dụng và thương mại điện tử.

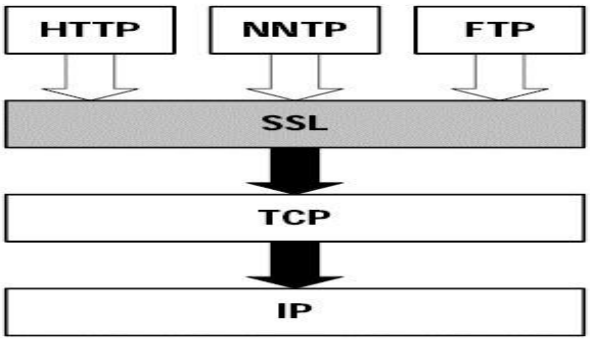
Tokenization sẽ mã hóa end-to-end thông tin dữ liệu (hay còn gọi là mã hóa trường dữ liệu), mã hóa dữ liệu chủ thẻ ở đầu, sau đó giải mã nó ở đích cuối.

2.4 Giải pháp bảo mật dựa trên SSL

2.4.1 Tổng quan về SSL

SSL (Secure Socket Layer) là giao thức đa mục đích được thiết kế để tạo ra các giao tiếp giữa hai chương trình ứng dụng trên một cổng định trước (socket 443) nhằm mã hoá toàn bộ thông tin đi/đến, mà ngày nay được được sử dụng rộng rãi cho giao dịch thanh toán điện tử như truyền số hiệu thẻ tín dụng, mật khẩu, số bí mật cá nhân (PIN) trên Internet.

Hình 2.5 [11] dưới đây mô tả vị trí của SSL trong mô hình OSI



Hình 2.5: Vị trí SSL trong mô hình OSI

SSL cho phép một server có hỗ trợ SSL tự xác thực với một Client cũng hỗ trợ SSL, cho phép client tự xác thực với server, và cho phép cả hai máy thiết lập một kết nối được mã hoá. Khả năng này đã định ra các mối quan tâm căn bản về giao tiếp trên mạng Internet và trên các mạng sử dụng TCP/IP:

Chứng thực SSL Server

Chứng thực SSL Client

Mã hoá kết nối

Các thuộc tính cơ bản của SSL

Kết nối là bí mật: quá trình mã hóa dữ liệu được áp dụng sau khi quá trình bắt tay (handshake) đầu tiên xác định được một khoá bí mật. Mật mã đối xứng được sử dụng cho quá trình mã hoá dữ liệu (ví dụ DES, RC4…).

Kết nối là tin cậy: việc vận chuyển các thông điệp bao gồm một quá trình kiểm tra tính toàn vẹn của thông điệp sử dụng một hàm kiểm tra MAC có khoá. Các hàm băm an toàn (ví dụ SHA, MD5…) được sử dụng cho quá trình thực hiện hàm MAC, nhằm đảm bảo thông tin không bị sai lệch và thể hiện chính xác thông tin gốc gửi đến.

2.4.2 Các hệ mã hóa sử dụng SSL

Giao thức SSL hỗ trợ rất nhiều hệ mã hoá sử dụng cho các hoạt động chứng thực server và client, cho quá trình truyền thông chứng chỉ số và trong quá trình thành lập khoá phiên. Bộ mã hoá mô tả sau đây có liên quan tới các thuật toán :

• DES. Data Encryption Standard, thuật toán mã hoá sử dụng bởi chính phủ Mỹ.

• DSA. Digital Signature Algorithm, một phần của chuẩn chứng thực số được sử dụng bởi chính phủ Mỹ.

• KEA. Key Exchange Algorithm, một thuật toán trao đổi khoá cho chính phủ Mỹ

• MD5. Message Digest, thuật toán băm được phát triển bởi Rivest

• RC2-RC4. Hệ mã hoá của Rivest được phát triển cho RSA Data Security

• RSA. Hệ mã hoá khoá công khai cho cả mã hoá và xác thực, được phát triển bởi Rivest, Shamir và Adleman.

• RSA key exchange: thuật toán trao đổi khoá cho SSL dựa trên thuật toán RSA.

• SHA-1: Secure Hash Algorithm, thuật toán băm sử dụng cho chính phủ Mỹ.

• SKIPJACK. Thuật toán mã hoá đối xứng cổ điển được cài đặt trong phần cứng tương thích FORTEZZA, cũng sử dụng bởi chính phủ Mỹ.

• Triple-DES.DES được cài đặt 3 vòng.

2.4.3 Bảo mật của SSL

Mức độ bảo mật của SSL phụ thuộc chính vào độ dài khoá hay phụ thuộc vào việc sử dụng phiên bản mã hoá **40bit** và **128bit**. Phương pháp mã hoá 40bit được sử dụng rộng rãi không hạn chế ngoài nước Mỹ và phiên bản mã hoá 128bit chỉ được sử dụng trong nước Mỹ và Canada.

Một số thách thức và phá khoá về bảo mật

Trong cộng đồng những người làm bảo mật, một trong các phương pháp kiểm tra độ độ bảo mật/an toàn của các thuật toán bảo mật, ngoài cơ sở lý thuyết của thuật toán, là đưa ra các "thách thức" (challenge) với số tiền thưởng tượng trưng, nhằm kiểm tra tính thực tiễn của thuật toán.

2.4.4 Các loại chứng thực SSL

Domain Validation (DV SSL)

Organization Validation (OV SSL)

Extended Validation (EV SSL)

Subject Alternative Names (SANs SSL)

Wildcard SSL Certificate (Wildcard SSL)

Sản phẩm lý tưởng dành cho các cổng thương mại điện tử. Mỗi e-store là một sub-domain và được chia sẻ trên một hoặc nhiều địa chỉ IP. Khi đó, để triển khai giải pháp bảo bảo mật giao dịch trực tuyến (đặt hàng, thanh toán, đăng ký & đăng nhập tài khoản,…) bằng SSL, chúng ta có thể dùng duy nhất một chứng chỉ số Wildcard cho tên miền chính của website và tất cả sub-domain.

2.4.5 Ứng dụng SSL bảo mật hệ thống thanh toán điện tử

Ưu điểm của SSL

Tính năng mạnh nhất của SSL/TLS là chúng xác định mối quan hệ với các tầng giao thức khác như thế nào trong hệ thống kiến trúc mạng OSI.

Một sức mạnh khác của SSL đó là ngăn chặn cách thức tấn công từ điển.

Giao thức SSL còn bảo vệ chính nó với đối tác thứ 3. Đó là các client xâm nhập bất hợp pháp dữ liệu trên đường truyền. Client xâm nhập này có thể giả mạo client hoặc server, SSL ngăn chặn sự giả mạo này bằng cách sử dụng khoá riêng của server và sử dụng chứng chỉ số.

Phương thức bắt tay trong TLS cũng tương tự. Tuy nhiên, TLS tăng cường sự bảo mật bằng cách cho phép truyền phiên bản giao thức, số hiệu phiên làm việc, hệ mã hoá và cách thức nén được sử dụng. TLS bổ xung thêm hai thuật toán băm không có trong SSL.

Hạn chế của SSL

Giao thức SSL, cũng giống như bất kỳ công nghệ nào, cũng có những hạn chế.. Đầu tiên là do những ràng buộc cơ bản của bản thân giao thức SSL. Đây là một hệ quả của việc thiết kế SSL và ứng dụng chịu tác động của nó. Tiếp theo, giao thức SSL cũng thừa kế một vài điểm yếu từ các công cụ mà nó sử dụng, cụ thể là các thuật toán ký và mã hoá. Nếu các thuật toán này có điểm yếu, SSL thường không thể khắc phục chúng. Cuối cùng, các môi trường trong đó SSL được triển khai có những thiếu sót và giới hạn.

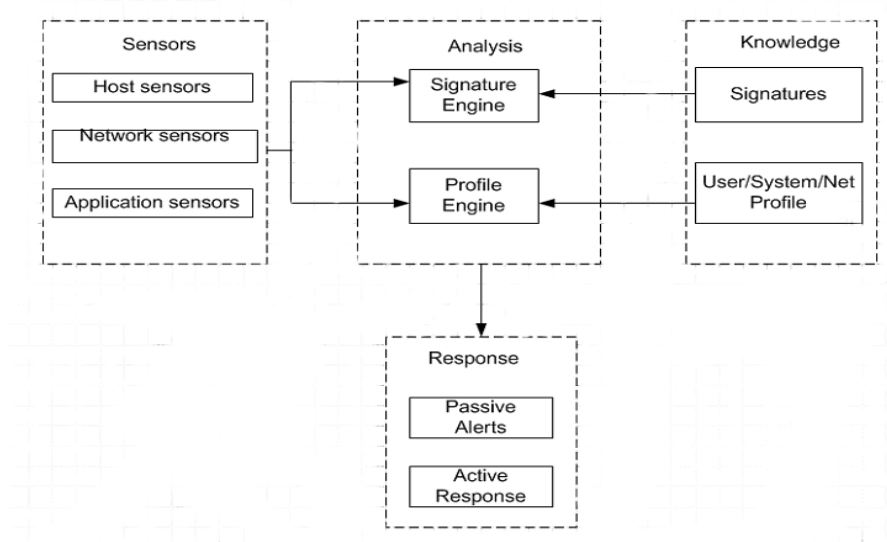
2.5 Giải pháp bảo mật dựa trên hệ thống phát hiện và ngăn chặn xâm nhập mạng

2.5.1. Hệ thống phát hiện xâm nhập IDS

Hệ thống phát hiện xâm nhập (Intrusion Detection System – IDS) là một hệ thống phần cứng hoặc ứng dụng phần mềm theo dõi, giám sát và thu thập thông tin từ các hoạt động ra vào của mạng.

Các thành phần của IDS

Các thành phần của hệ thống IDS được mô tả trong hình 2.6.



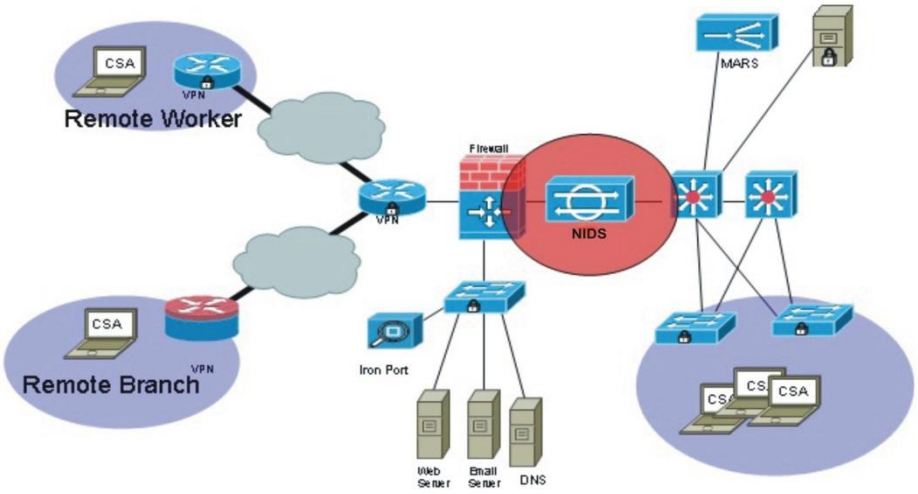
Hình 2.6: Các thành phần của hệ thống IDS [10]

Hệ thống IDS bao gồm các thành phần: Thành phần thu gói tin (Sensors); Thành phần phân tích gói tin (Analysis); Thành phần tri thức (Knowledge) hỗ trợ quá trình phân tích gói tin và Thành phần phản hồi (Respontion) xuất các thông tin cảnh báo.

Phân loại IDS:

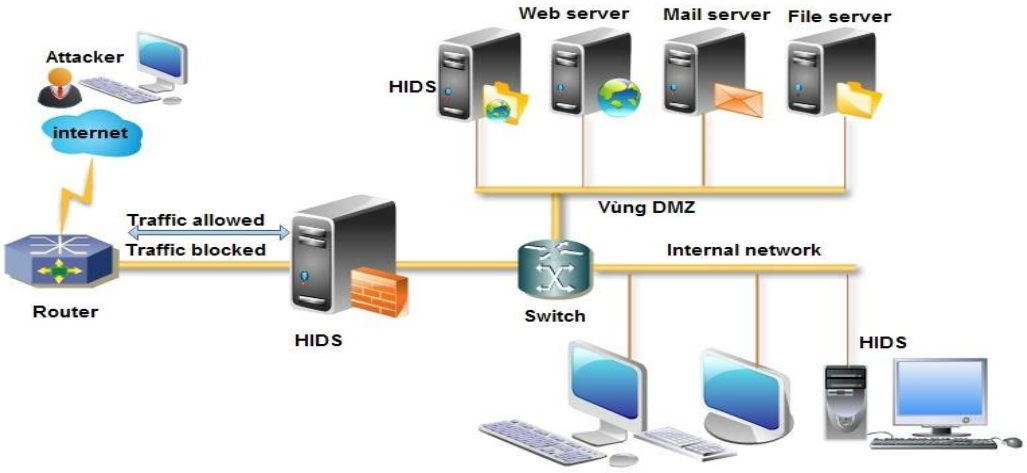
Dựa trên phạm vi giám sát, IDS được chia thành 2 loại:

(1) Network-based IDS (NIDS): Là những IDS giám sát trên toàn bộ mạng. Nguồn thông tin chủ yếu của NIDS là các gói dữ liệu đang lưu thông trên mạng. NIDS thường được lắp đặt tại ngõ vào của mạng, có thể đứng trước hoặc sau tường lửa. Hình 2.7 [10] mô tả mô hình hệ thống NIDS.



Hình 2.7: Mô hình hệ thống NIDS

(2) Host-based IDS (HIDS): Là những IDS phát hiện xâm nhập máy chủ được cài đặt trên các máy tính (host). Hình 2.8 [10] mô tả mô hình hệ thống HIDS.



Hình 2.8: Mô hình hệ thống HIDS

HIDS tìm kiếm dấu hiệu xâm nhập vào host cục bộ. Chúng tìm kiếm các hoạt động bất thường, lưu lượng đã gửi đến host được kiểm tra và phân tích trong file log lưu lại rồi chuyển qua host nếu cảm thấy không có dấu hiệu đáng nghi ngờ.

Dựa trên kỹ thuật thực hiện, IDS cũng được chia thành 2 loại:

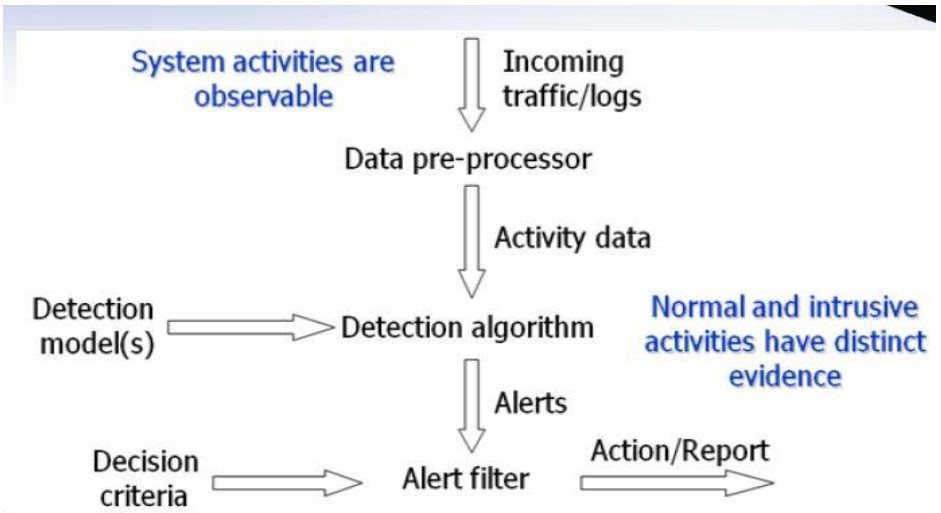
- **Signature-based IDS**
- **Anomaly-based IDS**

Snort

Snort là một ứng dụng IDS hiện đại với ba chức năng chính: chức năng là một bộ phận lắng nghe gói tin, chức năng lưu lại thông tin gói tin hay chức năng là một hệ thống phát hiện xâm nhập mạng (NIDS).

2.5.1. Hệ thống ngăn chặn xâm nhập IPS

Hệ thống phòng chống xâm nhập (IPS) là một kỹ thuật, kết hợp các ưu điểm của kỹ thuật tường lửa với hệ thống phát hiện xâm nhập IDS, có khả năng phát hiện các cuộc tấn công và tự động ngăn chặn các cuộc tấn công nhằm vào điểm yếu của hệ thống. Sơ đồ hoạt động của hệ thống IPS mô tả trong hình 2.8 [10].



Hình 2.8: Sơ đồ hoạt động của IPS

Ý tưởng của công nghệ IPS là mọi cuộc tấn công chống lại bất cứ thành phần nào của dịch vụ được bảo vệ sẽ bị làm chệch hướng bằng các giải pháp ngăn ngừa xâm nhập.

Các kiểu triển khai IPS

Có hai kiểu chính khi triển khai IPS là out-of-band IPS và in-line IPS:

- **Out-of-band IPS (OOB IPS)**: Với hệ thống này luồng dữ liệu vào hệ thống mạng sẽ cùng đi qua đồng thời firewall và IPS.
- **In-line IPS**: Vị trí IPS nằm trước firewall, luồng dữ liệu phải đi qua chúng trước khi tới firewall.

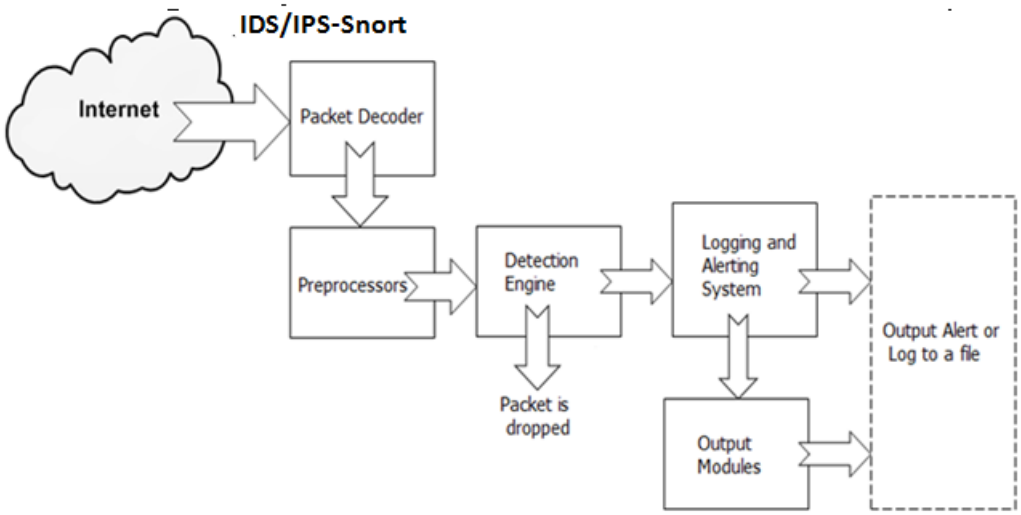
Chức năng chính và các Modul trong IPS

IPS có hai chức năng chính là phát hiện các cuộc tấn công và chống lại các cuộc tấn công đó. Hệ thống IPS gồm 3 modul chính:

- **Modul phân tích luồng dữ liệu**
- **Modul phát hiện tấn công**
- **Modul phản ứng**

2.5.3 Ứng dụng hệ thống IDS/IPS chống tấn công hệ thống thanh toán điện tử

Các hệ thống IDS/IPS có khả năng ứng dụng phát hiện và chống tấn công hệ thống thanh toán điện tử. Trong hình 2.9 dưới đây mô tả mô hình ứng dụng hệ thống IDS/IPS dựa trên Snort chống tấn công hệ thống thanh toán điện tử.



Hình 2.8 Mô hình hệ thống IDS/IPS chống tấn công hệ thống thanh toán điện tử sử dụng Snort

Giải pháp sử dụng hệ thống IDS/IPS chống tấn công hạ tầng mạng của hệ thống thanh toán điện tử là giải pháp khá hữu hiệu nhằm phát hiện và chống tấn công hệ thống thanh toán điện tử đang hoạt động.

2.6 Kết luận chương 2

CHƯƠNG 3 : XÂY DỰNG GIẢI PHÁP BẢO MẬT HỆ THỐNG THANH TOÁN ĐIỆN TỬ CHO TỔNG CÔNG TY VIỄN THÔNG MOBILEFONE

Trong chương 3 luận văn sẽ nghiên cứu và đề xuất ứng dụng các giải pháp bảo mật hệ thống thanh toán điện tử đã nghiên cứu trong chương 2 cho hệ thống thanh toán điện tử của Tổng công ty Viễn thông MobiFone. Trên cơ sở đó, luận văn tiến hành thử nghiệm một số giải pháp bảo mật cho hệ thống thanh toán điện tử của Tổng công ty Viễn thông MobiFone.

3.1. Tổng quan về hệ thống thanh toán điện tử của Tổng công ty Viễn thông MobiFone

3.1.1 Giới thiệu về Tổng công ty Viễn thông MobiFone

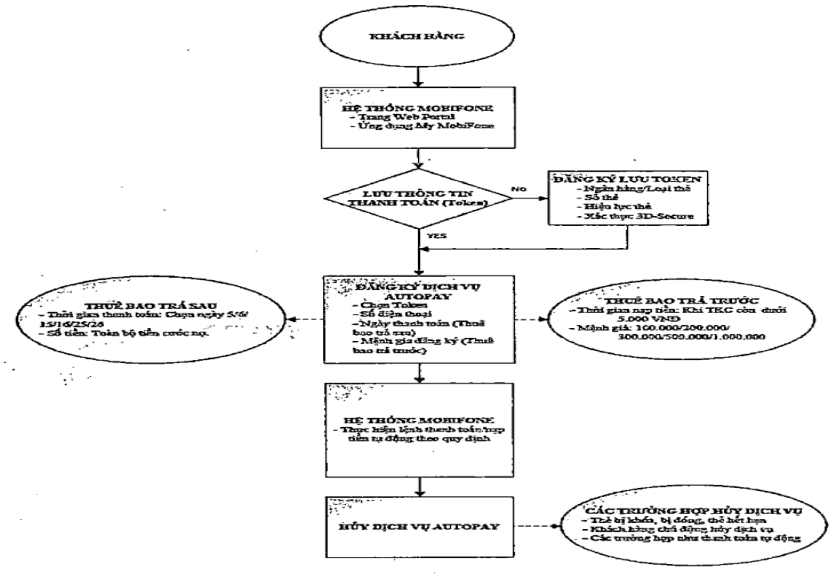
3.1.2 Hệ thống thanh toán điện tử Tổng công ty Viễn thông MobiFone

3.2 Đề xuất giải pháp bảo mật cho hệ thống thanh toán điện tử của Tổng công ty Viễn thông MobiFone

3.2.1 Giải pháp sử dụng mã OTP và công nghệ Tokenization

Giải pháp sử dụng mã OTP và công nghệ Tokenization cho hệ thống thanh toán điện tử của MobiFone nhằm bảo đảm an toàn các giao dịch thanh toán của khách hàng và bảo mật các thông tin liên quan của khách hàng.

Hình 3.1 dưới đây mô tả mô hình đăng ký dịch vụ thanh toán điện tử của khách hàng sử dụng công nghệ Tokenization.



Hình 3.1: Mô hình sử dụng Tokenization trong thanh toán điện tử

3.2.2 Giải pháp sử dụng SSL

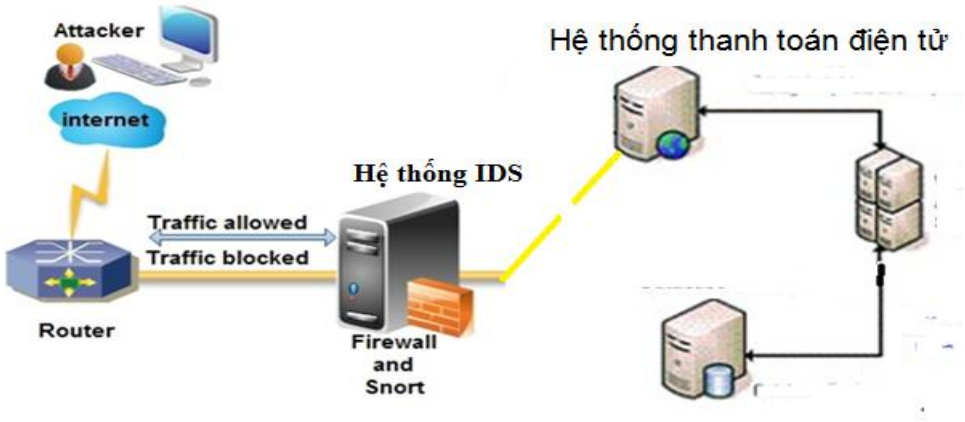
Trong hệ thống thanh toán trực tuyến của Tổng công ty MobiFone có sử dụng hệ thống web và cổng thông tin điện tử như MobiFone Portal, My MobiFone. Các hệ thống web cần phải được cài đặt sử dụng SSL/TSL.

Mặt khác, để quá trình trao đổi dữ liệu giao dịch thanh toán điện tử được an toàn trên hạ tầng mạng, cũng cần phải cài đặt SSL.

Trong mục 3.3.2, luận văn sẽ thực hiện cài đặt thử nghiệm SSL cho hệ thống thanh toán trực tuyến của Tổng công ty Viễn thông MobiFone.

3.2.3 Giải pháp xây dựng hệ thống IDS sử dụng Snort

Luận văn đề xuất mô hình hệ thống IDS sử dụng Snort để phát hiện tấn công hệ thống thanh toán điện tử được trình bày trong hình 3.2.



Hình 3.2: Mô hình thử nghiệm hệ thống IDS sử dụng Snort

Hệ thống IDS sẽ bao gồm các thành phần chính như sau: Module giải mã gói tin (Packet Decoder); Module tiền xử lý (Preprocessors); Module phát hiện (Detection Engine); Module log và cảnh báo (Logging and Alerting System) và Module kết xuất thông tin (Output Module).

Trong mô hình trên, nếu tin tặc sử dụng các gói tin tấn công vào hệ thống thanh toán điện tử thì trước tiên chúng phải đi qua hệ thống IDS. Khi đó Module giải mã gói tin và Module tiền xử lý sẽ phân tích các gói tin và gửi kết quả đến Module phát hiện. Module phát hiện sẽ phân tích và dựa trên tập luật của hệ thống để nhận dạng và phân loại các gói tin đầu vào. Các thông tin này sẽ được Module log và cảnh báo lưu vào cơ sở dữ liệu. Sau đó, chúng được Module kết xuất thông tin xử lý và đưa ra các phản hồi phù hợp của hệ thống IDS.

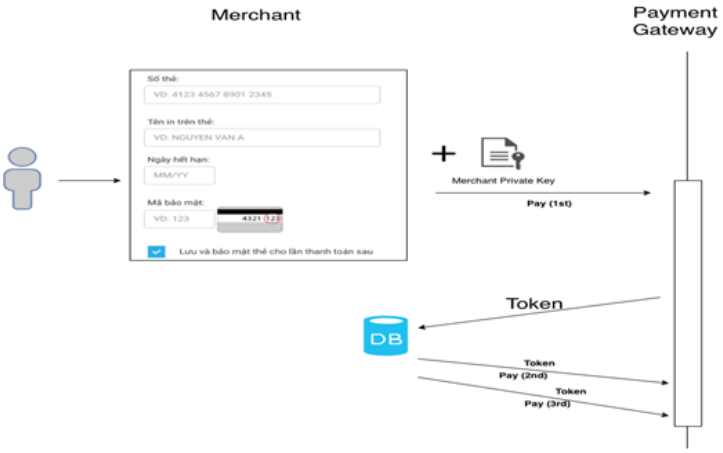
Hệ thống IDS cần sớm đưa ra cảnh báo về "giao dịch thanh toán đáng ngờ" nhằm theo dõi và phát hiện sớm các dấu hiệu gian lận. Để thực hiện được chức năng này, có thể xây dựng tập luật để sử dụng trong Module phát hiện hoặc sử dụng các kỹ thuật học máy

3.3. Cài đặt thử nghiệm và kết quả

3.3.1 Triển khai Tokenization

Khi khách hàng nhập thông tin mã số thẻ, tên chủ thẻ, ngày hết hạn cùng mã bảo mật của thẻ, Token thẻ của khách hang sẽ là chuỗi ký tự được mã hóa từ các thông tin trên và được lưu vào DB. Khác với lộ thẻ thông tin thẻ tín dụng thì kẻ xấu sử dụng để thanh toán ở bất kỳ đâu, Token chỉ có tác dụng duy nhất lên một Merchant ID. Token được mã hóa 2 chiều bằng gặp khóa private + public key, do đó bất kể khi nào, có nghi vấn lộ thông tin đều trở nên vô tác dụng rất khác so với lộ mã thẻ tín dụng.

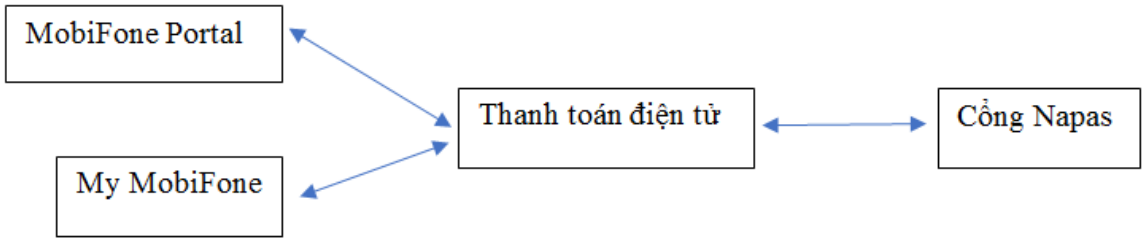
Hình 3.3 mô tả quá trình tạo ra và hoạt động của Tokenization.



Hình 3.3: Mô tả Tokenization được tạo ra và hoạt động

Cung cấp API cho hệ thống MobiFone Portal và My MobiFone để khách hàng tạo Token lần đầu:

Hình 3.4 trình bày mô hình giao tiếp giữa MobiFone Portal, My MobiFone với hệ thống Thanh toán điện tử để tạo Token lần đầu:



Hình 3.4: Mô hình giao tiếp giữa MobiFone Portal, My MobiFone với hệ thống Thanh toán điện tử

- Giao diện đăng ký dịch vụ được thiết kế trên MobiFone Portal và My MobiFone.

- Hệ thống Thanh toán điện tử bổ sung các API sau cung cấp cho hệ thống MobiFone Portal và My MobiFone:

o Hàm getBanksAuto(): cung cấp danh sách thẻ Ngân hàng có hỗ trợ dịch vụ . Hiện nay, đối tác Napas mới hỗ trợ thẻ Quốc tế có thể sử dụng dịch vụ .

o Link tạo token :

epayment.mobifone.vn/gateway/create_token_napas.jsp?cardtype=&from_msisdn=&environment=

Hệ thống sẽ redirect trang của khách hàng sang Cổng Napas để đăng ký thông tin thẻ lần đầu.

- Khi chuyển tiếp sang Cổng thanh toán Napas, hệ thống TTĐT sẽ gọi API riêng mà Napas cung cấp để tạo Token mà không thanh toán. Token này sẽ dùng riêng cho dịch vụ .

- Kết quả Token được lưu trữ trong cơ sở dữ liệu:

Row #	ID	FROM_MSISDN	TOKEN_CODE	TOKEN_ID	TOKEN_NAME	TOKEN_TYPE	BANK_CODE	BANK_TYPE	BANK_OTP
1	382	0901019990	gPvu/OKQFKVSsf7ZyiknirIxRO378KRop54tIpFcZDg=	382	412975xxxxxx7000	VISA	VISA	1	0
2	400	0901019168	S7v4Cvz/n3RVZBWKiwuhSpNb0xXBj4Nt7xACFKAbrws=	400	422109xxxxxx1658	VISA	VISA	1	0
3	408	0908882545	kzB8qRmirZsGKehR406Mf//Uci4ehT9159CI+hCnCpM=	408	486282xxxxxx9491	VISA	VISA	1	0
4	436	0907577511	cxRYHUQZ1cL8Dvof/N/uFpW4dp7DGtREI/5qiDW8hZ8=	436	412975xxxxxx2008	VISA	VISA	1	0

Trong đó:

ID: là định danh của Token

From_msidsn: là tài khoản MobiFone Portal đã lưu thông tin thẻ (Token).

Token_code: là giá trị Token đã được mã hóa, trước khi gửi sang Napas cần giải mã.

Token_name: là tên gợi nhớ của Token, tên này được hiển thị khi khách hàng chọn loại thẻ khi thanh toán/nạp tiền.

- Sau khi đã tạo được Token, khách hàng sẽ đăng ký các thông tin về dịch vụ như ngày thanh toán cho thuê bao trả sau, mệnh giá nạp tiền cho thuê bao trả trước khi tài khoản xuống dưới ngưỡng quy định …Các thông tin này sau đó được lưu trên hệ thống Thanh toán điện tử.

3.3.2 Cài đặt SSL

Để đáp ứng việc thử nghiệm, quá trình cài đặt SSL trong hệ thống thanh toán điện

tử sử dụng Platform Apache (Do Web server Apache đang là một trong những Web server thịnh hành nhất trên toàn thế giới). Các platform khác có thể áp dụng tương tự, nhưng cần thay đổi đường dẫn (path) và tên tập tin cấu hình/thư mục (file configuration/folder). Luận văn đề xuất yêu cầu về phần cứng thử nghiệm tối thiểu như sau

- ***Cài đặt Certificate Authority***

- Tạo tập tin cấu hình mặc định cho CA

- Truy cập vào thư mục \apache\bin, tập tin openssl.cnf (Đây là tập tin cấu hình gốc của OpenSSL), có thể chỉnh sửa tùy theo nhu cầu sử dụng

```
#
# OpenSSL example configuration file.
# This is mostly being used for generation of certificate requests.
#

# This definition stops the following lines choking if HOME isn't
# defined.
HOME                    = .
RANDFILE                = $ENV::HOME/.rnd

# Extra OBJECT IDENTIFIER info:
#oid_file               = $ENV::HOME/.oid
oid_section             = new_oids

# To use this configuration file with the "-extfile" option of the
# "openssl x509" utility, name here the section containing the
# X.509v3 extensions to use:
# extensions            =
# (Alternatively, use a configuration file that has only
# X.509v3 extensions in its main [= default] section.)

[ new_oids ]

# We can add new OIDs in here for use by 'ca' and 'req'.
# Add a simple OID like this:
# testoid1=1.2.3.4
# Or use config file substitution like this:
# testoid2=${testoid1}.5.6

####################################################################
[ ca ]
```

- Lưu ý dòng ***default_days*** là thời hạn của certificate. Có thể chỉnh lên 3650 (10 năm) để tránh bị hết hạn certificate.

- Tiến hành đăng ký trở thành CA

- Tạo tập tin makecert.ca.bat : Truy cập vào thư mục \apache, tập tin makecert.ca.bat (Đây là tập tin tạo chứng chỉ bảo mật SSL của Apache), có thể chỉnh sửa tùy theo nhu cầu sử dụng. Lưu ý tham số ***-days 3650*** nghĩa là CA mà chúng ta đang tạo sẽ có quyền lực trong 10 năm. Chúng ta có thể tái sử dụng CA này để cấp chứng chỉ cho vô số tên miền trong vòng 10 năm tới.

```
@echo off
set RANDFILE=.rnd
set OPENSSL_CONF=./conf/openssl-ca.cnf

if not exist .\conf\ssl.ca mkdir .\conf\ssl.ca
if not exist .\conf\ssl.key mkdir .\conf\ssl.key
if not exist .\conf\ssl.csr mkdir .\conf\ssl.csr
if not exist .\conf\ssl.pem mkdir .\conf\ssl.pem

bin\openssl req -x509 -newkey rsa:4096 -sha256 -nodes -out cacert.pem -days 3650 -outform PEM
bin\openssl x509 -outform der -in cacert.pem -out cacert.crt
bin\openssl rsa -in cakey.pem -out ca.key

set OPENSSL_CONF=
move /y cacert.pem .\conf\ssl.ca
move /y cacert.crt .\conf\ssl.ca
move /y cakey.pem .\conf\ssl.ca
move /y ca.key .\conf\ssl.ca
del .rnd

echo.
echo Chung nhan CA cua ban da duoc tao - Your CA certificate was created.
echo.
echo Chung nhan CA cua ban da duoc cap phat - The certificate was provided.
echo.
```

- Thực thi makecert.ca.bat: Chạy bằng Terminal của máy chủ

```
Generating a 4096 bit RSA private key
.....................................................................++
.........................++
writing new private key to 'cakey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

Tạo yêu cầu ký chứng chỉ : tương tự bước 2.1, nhưng thay tên tập tin là openssl-localhost.cnf, mục đích là tạo CSR cho miền localhost

- Tạo tập tin cấu hình SSL mặc định cho localhost
- Tạo tập tin thực thi makecert.localhost.bat
- Thực thi makecert.localhost.bat

Cấu hình và cài đặt SSL cho máy chủ

- Truy cập thư mục ***\apache\conf\extra*** tìm đến tập tin ***httpd-vhosts.conf,*** đổi tên tập tin này và tạo một tập tin httpd-vhosts.conf mới. Mục đích là để backup tập tin gốc, sau đó chỉnh lại theo nhu cầu sử dụng (IP, Port, đường dẫn file log,…)

```
    ServerAlias www.localhost
    ErrorLog "logs/localhost-error.log"
    CustomLog "logs/localhost-access.log" common
</VirtualHost>
```

- Tương tự, cũng trong thư mục ***\xampp\apache\conf\extra***, tìm đến tập tin ***httpd-ssl.conf*** backup nó và tạo lại tập tin mới. Sau đó chỉnh sửa lại nội dung tùy theo nhu cầu sử dụng.

3.4 Kết chương 3

KẾT LUẬN

1. Các kết quả đạt được của luận văn

Với mục tiêu nghiên cứu các giải pháp bảo mật cho hệ thống thanh toán điện tử và ứng dụng cho hệ thống thanh toán trực tuyến của Tổng công ty Viễn thông MobiFone, luận văn đã đạt được một số kết quả sau đây:

- Luận văn đã khảo sát tổng quan về hệ thống thanh toán điện tử, các yêu cầu kỹ thuật của hệ thống thanh toán điện tử và các vấn đề bảo mật của hệ thống thanh toán điện tử nhằm giảm thiểu rủi ro trong các hệ thống thanh toán điện tử.

- Luận văn đã khảo sát tổng quan các vấn đề về bảo mật cho hệ thống thanh toán điện tử.

- Luận văn đã khảo sát bốn giải pháp bảo mật cho hệ thống thanh toán điện tử: giải pháp dựa trên mật khẩu sử dụng 1 lần (One Time Password – OTP), giải pháp dựa trên công nghệ Tokenization, giải pháp dựa trên giao thức SSL (Secure Sockets Layer) và giải pháp bảo mật dựa trên hệ thống phát hiện và ngăn chặn xâm nhập mạng IDS/IPS.

- Luận văn đề xuất một số giải pháp bảo mật cho hệ thống thanh toán trực tuyến của Tổng công ty Viễn thông MobiFone.

- Luận văn đã thực hiện thực hiện thử nghiệm triển khai Tokenization cho các thuê bao và thử nghiệm cài đặt cho hệ thống thanh toán điện tử của Tổng công ty Viễn thông MobiFone.

2. Hướng phát triển

Luận văn có thể được phát triển xây dựng các hệ thống bảo mật có khả năng triển khai thực tế cho hệ thống thanh toán trực tuyến của Tổng Công ty Viễn thông MobiFone. Từ đó, có thể nghiên cứu triển khai các giải pháp bảo mật cho các hệ thống cung cấp dịch vụ của Tổng công ty viễn thông MobiFone.