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

LUẬN VĂN THẠC SĨ KỸ THUẬT
(*Theo định hướng ứng dụng*)

NGƯỜI HƯỚNG DẪN KHOA HỌC : TS. VŨ VĂN THỎA

HÀ NỘI - NĂM 2020

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

LUẬN VĂN THẠC SĨ KỸ THUẬT
(*Theo định hướng ứng dụng*)

NGƯỜI HƯỚNG DẪN KHOA HỌC : TS. VŨ VĂN THỎA

HÀ NỘI - NĂM 2020

LỜI CAM ĐOAN

Tôi xin cam đoan, luận văn này là công trình nghiên cứu khoa học thực thụ của cá nhân, được thực hiện dưới sự hướng dẫn khoa học của TS. Vũ Văn Thỏa. Nội dung của luận văn có tham khảo và sử dụng các tài liệu, thông tin được đăng tải trên những tạp chí khoa học và các trang web được liệt kê trong danh mục tài liệu tham khảo. Tất cả các tài liệu tham khảo đều có xuất xứ rõ ràng và được trích dẫn hợp pháp.

Tôi xin hoàn toàn chịu trách nhiệm và chịu mọi hình thức kỷ luật theo quy định cho lời cam đoan của mình.

Học viên

Bùi Quang Minh

LỜI CẢM ƠN

Lời đầu tiên, học viên xin chân thành cảm ơn TS. Vũ Văn Thỏa – Học viện Công nghệ Bưu chính Viễn thông, người đã trực tiếp hướng dẫn tôi thực hiện luận văn. Với sự hướng dẫn cung cấp tài liệu, động viên của Thầy đã giúp học viên vượt qua nhiều khó khăn về chuyên môn trong suốt quá trình thực hiện luận văn.

Học viên xin chân thành cảm ơn Ban Giám đốc, Lãnh đao và cán bộ Khoa Sau Đại học và Khoa Công nghệ Thông tin, cùng các Thầy, Cô đã giảng dạy và quản lý đào tạo trong suốt 2 năm theo học tại Học viện Công nghệ Bưu chính Viễn thông.

Cuối cùng, học viên xin cảm ơn gia đình, các đồng nghiệp, bạn bè tại Tổng công ty viễn thông MobiFone đã động viên, tạo điều kiện cho học viện trong suốt 2 năm học tập và nghiên cứu.

Xin chân thành cảm ơn!

MỤC LỤC

DANH MỤC BẢNG VẼ

DANH MỤC CÁC KÝ HIỆU, CÁC TỪ VIẾT TẮT

Từ viết tắt	Tiếng Anh	Tiếng việt
PIN	Personal Identification Number	Mã số cá nhân
E-Check	Electronic Check	Séc điện tử
SMS	Short Message Services	Dịch vụ tin nhắn ngắn
WAP	Wireless Application Protocol	Giao thức Ứng dụng Không dây
NFC	Near-Field Communications	Kết nối trường gần
DoS	Denial Of Service	Từ chối dịch vụ
DDoS	Distributed Denial Of Service	Từ chối dịch vụ phân tán
	Secure Element	Yếu tố bảo mật
OTP	One Time Password	là mật khẩu một lần
	Tokenization	Mã thông báo
PAN	Primary Account Number	Số tài khoản chính
SSL	Secure Sockets Layer	Lớp socket bảo mật
PCT	Private Communication Technology	Công nghệ truyền thông cá nhân
IETF	Internet Engineering Task Force	Nhóm đặc trách kỹ thuật Internet
TLS	Transport Layer Security	Giao thức bảo mật tầng giao vận
DES	Data Encryption Standard	Tiêu chuẩn Mã hóa Dữ liệu
DSA	Digital Signature Algorithm	Giải thuật ký số
KEA	Key Exchange Algorithm	Thuật toán trao đổi khóa
MD5	Message-Digest algorithm 5	Giải thuật Tiêu hóa tin 5
SHA	Secure Hash Algorithm	Thuật toán băm an toàn
MAC	Message Authentication Code	Mã xác thực thông điệp

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.

Theo Ủy ban Kinh tế Liên Hiệp Quốc châu Âu (UNECE) [15]: "Thương mại điện tử nội địa bao gồm các giao dịch trong nước qua Internet hoặc các mạng máy tính trung gian, trong khi đó, thương mại điện tử quốc tế liên quan đến các giao dịch xuyên biên giới. Các giao dịch này là giao dịch mua/bán hàng hóa hoặc dịch vụ, sau đó, quá trình chuyển giao hàng hóa có thể được thực hiện trực tuyến hoặc thủ công".

Theo Tổ chức Hợp tác và Phát triển Kinh tế (OECD) [15]: "Thương mại điện tử được định nghĩa là các giao dịch thương mại, bao gồm cả những giao dịch giữa các tổ chức hoặc cá nhân thông qua quá trình thực hiện và chuyển giao dữ liệu số. Các dữ liệu này bao gồm chữ, âm thanh và hình ảnh được truyền qua các mạng lưới mở (như Internet) hoặc mạng kín (như AOL hay Mintel) có cổng kết nối với mạng mở".

Theo Tổ chức Thương mại Thế giới (WTO)[15]: "Thương mại điện tử bao gồm việc sản xuất, quảng cáo, bán hàng và phân phối sản phẩm được mua bán và thanh toán trên mạng Internet, nhưng được giao nhận một cách hữu hình, cả các sản phẩm giao nhận cũng như những thông tin số hoá thông qua mạng Internet".

Theo Ủy ban Thương mại điện tử của Tổ chức Hợp tác Kinh tế Châu Á – Thái Bình Dương (APEC)[15]: "Thương mại điện tử liên quan đến các giao dịch

thương mại trao đổi hàng hóa và dịch vụ giữa các nhóm (cá nhân) mang tính điện tử chủ yếu thông qua các hệ thống có nền tảng dựa trên Internet".

Tuy nhiên, thương mại điện tử không chỉ là kinh doanh sử dụng công nghệ. Thương mại điện tử là toàn bộ quá trình kinh doanh được thực hiện bằng điện tử và được thiết kế để giúp hoàn thành mục tiêu kinh doanh.

Hai công nghệ chủ chốt để xây dựng và phát triển thương mại điện tử là trao đổi dữ liệu điện tử (EDI) và chuyển tiền điện tử (EFT). Ngày nay, công nghệ chuyển tiền điện tử được ứng dụng để xây dựng các hệ thống thanh toán điện tử.

Thanh toán điện tử hay thanh toán trực tuyến là một mô hình giao dịch không sử dụng tiền mặt được thực hiện trên môi trường internet. Thông qua hệ thống thanh toán điện tử, người sử dụng có thể thực hiện các hoạt động thanh toán, chuyển, nạp hay rút tiền, … [15]

Thông thường, thanh toán điện tử được thực hiện qua các cổng thanh toán trực tuyến (giữ vai trò trung gian thực hiện các giao dịch lưu chuyển tiền tệ trực tuyến, có sự liên kết với các ngân hàng thương mại) hoặc các tài khoản ngân hàng trực tuyến của người dùng.

Một số hình thức thanh toán điện tử được sử dụng rộng rãi trong các hệ thống thanh toán điện tử được trình bày dưới đây [1].

Thanh toán bằng thẻ

Đây là hình thức thanh toán đặc trưng nhất, chiếm tới 90% trong tổng số các giao dịch thanh toán điện tử. Thẻ thanh toán (thẻ chi trả) là một loại thẻ có khả năng thanh toán tiền mua hàng hóa, dịch vụ tại một vài địa điểm, kể cả website mua hàng trực tuyến nếu chấp nhận tiêu dùng bằng thẻ đó. Thẻ có thể dùng để rút tiền mặt trực tiếp từ các ngân hàng hay các máy rút tiền tự động.

Thanh toán qua cổng thanh toán điện tử

Cổng thanh toán điện tử về bản chất là dịch vụ cho phép khách hàng giao dịch tại các website thương mại điện tử. Cổng thanh toán cung cấp hệ thống kết nối an toàn giữa tài khoản (thẻ, ví điện tử,…) của khách hàng với tài khoản của website

bán hàng. Cổng thanh toán điện tử giúp người tiêu dùng và doanh nghiệp thanh toán, nhận tiền trên internet đơn giản, nhanh chóng và an toàn.

Thanh toán bằng ví điện tử

Ví điện tử là một tài khoản online có thể dùng nhận, chuyển tiền, mua thẻ điện thoại, vé xem phim, thanh toán trực tuyến các loại phí trên internet như tiền điện nước, cước viễn thông, cũng có thể mua hàng online từ các trang thương mại điện tử. Người dùng phải sở hữu thiết bị di động thông minh tích hợp ví điện tử và liên kết với ngân hàng thì mới có thể thanh toán trực tuyến bằng hình thức này.

Hiện nay, tại Việt Nam có khoảng 20 ví điện tử được cấp phép và theo Ngân hàng nhà nước dự báo đến năm 2020 sẽ đạt ngưỡng 10 triệu người dùng.

Thanh toán bằng thiết bị điện thoại thông minh

- Thanh toán qua Mobile Banking:

Hình thức này đang dần trở nên phổ biến bởi hầu hết người dùng đều sử hữu một chiếc điện thoại thông minh. Chính vì vậy, khi đi mua sắm, khách hàng không cần phải mang theo tiền mặt, thay vào đó là thanh toán qua điện thoại với dịch vụ Mobile Banking. Hệ thống thanh toán qua điện thoại được xây dựng trên mô hình liên kết giữa ngân hàng, các nhà cung cấp viễn thông, và người dùng.

- Thanh toán qua QR Code:

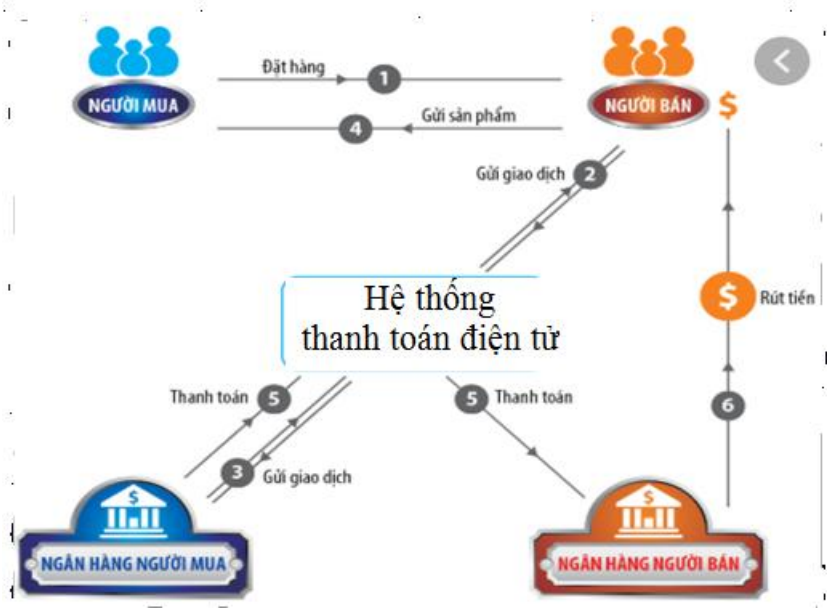
Tiến bộ công nghệ cũng là lý do khiến thanh toán bằng QR Code ngày càng được ưa chuộng. Phương thức thanh toán này khá đơn giản, gọn nhẹ, dễ sử dụng và thân thiện cho người dùng. Tính năng QR Code hiện đang được tích hợp sẵn trên ứng dụng di động của các ngân hàng, các sản phẩm và dịch vụ của Google như Google Chart hay Google Map, trên bảng hiệu, xe buýt, danh thiếp, tạp chí, website, hàng hóa tại siêu thị, cửa hàng tiện lợi,… Thậm chí là trên một số siêu ứng dụng như VinID của Tập đoàn Vingroup.

Người dùng sử dụng camera điện thoại quét mã QR để thực hiện nhanh các giao dịch chuyển khoản, thanh toán hóa đơn, mua hàng. Chỉ với một lần quét, sau vài giây, người dùng đã thanh toán thành công tại các nhà hàng, siêu thị, cửa hàng

tiện lợi, taxi, thậm chí là các website thương mại điện tử hay trên bất cứ sản phẩm nào có gắn mã QR mà không cần sử dụng tiền mặt, thẻ, không lo lộ thông tin cá nhân tại các điểm thanh toán.

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:

Người tiêu dùng dễ dàng thực hiện thanh toán điện tử cho hoạt động mua sắm tại siêu thị, cửa hàng tiện lợi, giao dịch các món hàng xa xỉ, có giá trị cao hay các dịch vụ giải trí, du lịch, trả tiền hóa đơn (điện, nước, viễn thông…). Quá trình

thanh toán dễ dàng được thực hiện qua các thiết bị di động có kết nối mạng. Nhờ đó, người dùng có thể thực hiện chuyển tiền nhanh chóng ở bất cứ đâu thông qua điện thoại mà không cần phải tới ngân hàng nữa.

- Dễ dàng theo dõi và kiểm soát

Tất cả các khoản tiền thanh toán điện tử đều lưu lại trong lịch sử giao dịch và cho phép bạn tra cứu một cách dễ dàng chỉ với vài thao tác đơn giản. Từ đó, người dùng có thể quản lý tài chính và có những cân đối chi tiêu hợp lý.

Hạn chế rủi ro:

Khi thực hiện thanh toán bằng tiền mặt thường có các rủi ro về thất thoát, thiếu tiền, quên ví, đặc biệt với những sản phẩm/dịch vụ có giá trị lớn. Còn với thanh toán điện tử, mọi giao dịch đều nhanh chóng, chính xác tới từng con số, minh bạch, rõ ràng và bảo mật.

Hỗ trợ kinh doanh trực tuyến:

Hầu hết người tiêu dùng, nhất là các khách hàng trẻ đều đang sử dụng thanh toán điện tử như internet banking, ví điện tử, mã QR, … bởi tính tiện dụng. Do vậy, doanh nghiệp hay hộ kinh doanh không có hệ thống thanh toán điện tử sẽ gặp nhiều bất lợi so với đối thủ cạnh tranh.

Về lâu về dài, khi đã tạo được niềm tin của người tiêu dùng về chất lượng hàng hóa, việc thanh toán tiền mặt khi mua hàng trực tuyến sẽ không còn nữa. Các sàn thương mại điện tử ngày nay cũng đã đa dạng hóa hình thức thanh toán, giúp người dùng có nhiều sự lựa chọn hơn.

Những lợi ích mà các hệ thống thanh toán điện tử mang lại đã làm gia tăng đáng kể nhu cầu thực tế của người dùng đối với thanh toán điện tử.

Thanh toán điện tử đang phổ biến rất nhiều trên các quốc gia phát triển trên thế giới cũng như tại Việt Nam với khối lượng giao dịch khổng lồ mỗi ngày. Theo Worldpay 2017, thanh toán điện tử đã tăng trưởng cao nhất trong thập kỷ qua, với khối lượng tăng 11,2% trong suốt thời gian 2014 - 2015 đạt 433,1 tỷ USD. Thị trường châu Á với tốc độ tăng trưởng 43,4%. Hầu hết các nước đã và đang triển

khai công cuộc cải cách hệ thống thanh toán hiện đại, đáp ứng nhu cầu thanh toán ngày càng cao của người dân.

Tại Việt Nam, Theo Bộ Thông tin và Truyền thông (2017), Việt Nam với dân số hơn 90 triệu dân, trong đó 52% tỷ lệ số người sử dụng internet, tỷ lệ phủ sóng di động là 98% là những điều kiện rất thuận lợi cho phát triển các hệ thống thanh toán điện tử.

Theo Worldpay, đến năm 2019, thanh toán qua di động (hiện chiếm 27,6% thị phần thanh toán bán lẻ toàn cầu) sẽ thay thế thẻ thanh toán như: Visa, MasterCard và trở thành phương thức thanh toán được ưa chuộng nhất khi tận dụng tốt các đặc điểm nổi bật.

Trên thế giới, số lượng dịch vụ thanh toán di động đã tăng lên và cung cấp nhiều chức năng hơn. Ở các nước đang phát triển, các dịch vụ thanh toán di động là một công cụ quan trọng cho hoạt động giao dịch, đặc biệt là các dòng tiền xuyên biên giới như kiều hối. Ở các nền kinh tế phát triển, thế hệ trẻ có khả năng áp dụng và ưa thích sử dụng các dịch vụ mới chiếm tỷ lệ cao và có xu hướng gia tăng mạnh mẽ.

Các trang thương mại điện tử lớn đều cung cấp hình thức thanh toán điện tử và luôn luôn ưu tiên việc thanh toán điện tử. Amazon – Trang thương mại điện tử lớn nhất thế giới luôn ưu tiên phát triển dịch vụ thanh toán không tiền mặt, thậm chí họ còn phát triển cả cửa hàng không tiền mặt.

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. Đồng thời. trong thanh toán điện tử đảm bảo tính không chối bỏ của giao dịch. Do đó, các công nghệ chữ ký số và chứng chỉ số thường được áp dụng.

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

Hệ thống thanh toán điện tử thường được triển khai trên mạng internet hoặc các mạng di động. Do đó hạ tầng mạng để triển khai hệ thống thanh toán điện tử phải đảm bảo các yêu cầu sau đây.

- Hạ tầng mạng phải được phân tách thành các phân vùng mạng để đảm bảo kiểm soát được các truy cập hệ thống.

- Hạ tầng mạng phải có khả năng phát hiện và phòng chống xâm nhập trái phép, phòng chống phát tán mã độc hại cho hệ thống và người dùng.

- Hạ tầng mạng phải có khả năng dự phòng cho các vị trí quan trọng có mức độ ảnh hưởng cao tới hệ thống mạng hoặc có khả năng gây tê liệt toàn bộ hệ thống mạng của nhà cung cấp dịch vụ khi xảy ra sự cố.

- Hạ tầng mạng phải đảm bảo các kết nối không dây phải sử dụng các biện pháp xác thực đảm bảo an toàn.

- Hạ tầng mạng phải đảm bảo yêu cầu về băng thông đối với việc cung cấp dịch vụ thanh toán điện tử.

- Thường xuyên cập nhật các bản vá lỗi hệ thống, cập nhật cấu hình cho các thiết bị mạng và các thiết bị bảo mật. Trong trường hợp phát hiện lỗi hạ tầng mạng phải thực hiện cập nhật ngay.

- Các trang thiết bị mạng, an ninh, bảo mật, phần mềm chống vi rút, công cụ phân tích, quản trị mạng được cài đặt trong mạng của đơn vị phải có bản quyền và nguồn gốc, xuất xứ rõ ràng.

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

Trong hệ thống thanh toán điện tử hạ tâng máy chủ và các phần mềm sử dụng có vai trò hết sức quan trọng. Một số yêu cầu kỹ thuật đối với phần cứng, phần mềm hệ thống thanh toán điện tử như sau.

- Đảm bảo có hạ tầng máy chủ và các thiết bị đi kèm phục vụ hệ thống thanh toán điện tử đủ công suất, đạt hiệu năng yêu cầu, đảm bảo tốc độ xử lý truy xuất đáp ứng yêu cầu của khách hàng sử dụng dịch vụ.

- Đối với máy chủ hệ thống thanh toán điện tử phải có tính năng sẵn sàng cao, cơ chế dự phòng linh hoạt để đảm bảo tính hoạt động liên tục.

- Đối với phần mềm hệ thống thanh toán điện tử phải được rà soát, cập nhật các phiên bản vá lỗi phần mềm hệ thống theo khuyến cáo của nhà cung cấp.

- Các phần mềm ứng dụng trong hệ thống thanh toán điện tử phải đảm bảo các yêu cầu an toàn, bảo mật của nghiệp vụ, phải được xác định trước và tổ chức, triển khai vào toàn bộ chu trình phát triển phần mềm từ khâu phân tích, thiết kế đến triển khai vận hành và bảo trì. Các tài liệu về an toàn, bảo mật của phần mềm phải được hệ thống hóa và lưu trữ.

- Trước khi triển khai phần mềm ứng dụng mới, phải đánh giá những rủi ro của quá trình triển khai đối với hoạt động nghiệp vụ, các hệ thống công nghệ thông tin liên quan và lập, triển khai các phương án hạn chế, khắc phục rủi ro.

- Thực hiện kiểm tra thử nghiệm phần mềm ứng dụng nhằm phát hiện và loại trừ các lỗi, các gian lận có thể xảy ra khi nhập số liệu đầu vào và các lỗ hổng bảo mật trong quá trình kiểm tra thử nghiệm hệ thống. Đồng thời, ghi lại các lỗi và quá

trình xử lý lỗi, đặc biệt là các lỗi về an toàn, bảo mật trong các báo cáo về kiểm tra thử nghiệm. Việc sử dụng dữ liệu cho quá trình thử nghiệm phải có biện pháp phòng ngừa tránh bị lợi dụng hoặc gây nhầm lẫn.

- Quản lý và nâng cấp phiên bản phần mềm phải tuân thủ các yêu cầu sau:

+ Đối với mỗi yêu cầu thay đổi phần mềm, phải phân tích đánh giá ảnh hưởng của việc thay đổi đối với các hệ thống hiện tại cũng như các nghiệp vụ và các hệ thống công nghệ thông tin có liên quan khác của hệ thống.

+ Các phiên bản phần mềm bao gồm cả chương trình nguồn cần được quản lý tập trung, lưu trữ, bảo mật và có cơ chế phân quyền cho từng thành viên trong việc thao tác với các tập tin.

+ Mỗi phiên bản được nâng cấp phải được kiểm tra thử nghiệm các tính năng an toàn, bảo mật và tính ổn định trước khi triển khai chính thức.

+ Các phiên bản phần mềm sau khi thử nghiệm thành công phải được quản lý chặt chẽ; tránh bị sửa đổi bất hợp pháp và sẵn sàng cho việc triển khai.

- Cần có cơ chế kiểm soát chương trình nguồn nhằm loại trừ các đoạn mã độc hại, các lỗ hổng bảo mật (back-door).

1.2.3 Yêu cầu đối với cơ sở dữ liệu

Cơ sở dữ liệu đảm bảo hoạt động của hệ thống thanh toán điện tử phải tuân thủ các yêu cầu như sau.

- Hệ quản trị cơ sở dữ liệu sử dụng cho hệ thống thanh toán điện tử phải đáp ứng được yêu cầu hoạt động ổn định; xử lý, lưu trữ được khối lượng dữ liệu lớn theo yêu cầu nghiệp vụ; có cơ chế bảo vệ và phân quyền truy cập đối với các tài nguyên cơ sở dữ liệu.

- Rà soát, cập nhật các bản vá, các bản sửa lỗi hệ quản trị cơ sở dữ liệu định kỳ hoặc ngay sau khi có khuyến cáo của nhà cung cấp.

- Thực hiện phân quyền và có quy định chặt chẽ với từng cá nhân truy cập đến cơ sở dữ liệu. Phải ghi nhật ký đối với các truy cập cơ sở dữ liệu, các thao tác đối với cấu hình cơ sở dữ liệu.

- Có giải pháp ngăn chặn các hình thức tấn công cơ sở dữ liệu.

- Quá trình mã hóa dữ liệu phải đảm bảo các yêu cầu:

+ Lựa chọn thuật toán mã hóa đáp ứng yêu cầu đảm bảo tính bí mật và khả năng xử lý của hệ thống thanh toán điện tử.

- Các khóa mã hóa phải được khởi tạo, thay đổi, phân phối, lưu trữ một cách an toàn và bảo đảm khôi phục được các thông tin đã mã hóa khi cần thiết.

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.

Theo báo cáo an ninh website của CyStack, chỉ trong quý 3 năm 2018 đã có 1.183 website của Việt Nam bị tin tặc tấn công và kiểm soát. Trong đó, các website giới thiệu sản phẩm và dịch vụ của doanh nghiệp là đối tượng bị tin tặc tấn công nhiều nhất (chiếm 71,51%). Vị trí thứ hai là các website thương mại điện tử (chiếm 13,86%).

Tháng 11/2018, Diễn đàn RaidForums đã đăng tải thông tin được cho là dữ liệu của hơn 5 triệu khách hàng của chuỗi bán lẻ thiết bị Thế giới di động. Những thông tin bị rỏ rì bao gồm địa chỉ email, lịch sử giao dịch và thậm chí là cả số thẻ

ngân hàng. Ngay sau đó, dữ liệu được cho là các hợp đồng trong chương trình F.Friends của FPT Shop cũng bị rò rỉ. Một số công ty Việt Nam như: Công ty cổ phần Con cưng, Ngân hàng hợp tác xã Việt Nam, ... cũng trở thành đích nhắm cho tin tặc.

Theo thống kê từ Trung tâm Giám sát an toàn không gian mạng quốc gia trực thuộc Cục An toàn thông tin (Bộ Thông tin và Truyền thông), có khoảng 4,7 triệu địa chỉ IP của Việt Nam thường xuyên nằm trong các mạng mã độc lớn (số liệu tháng 11/2018).

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.

1.3.2 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

- Đảm bảo bí mật thông tin liên quan đến tài khoản, tiền gửi và các giao dịch của khách hàng theo quy định của pháp luật.

- Mật khẩu khách hàng, khóa mã hóa và các mã khóa khác phải được mã hóa trong quá trình giao dịch, trên đường truyền và lưu trữ tại đơn vị cung cấp dịch vụ.

2. Đảm bảo tính sẵn sàng

- Cam kết khả năng hoạt động liên tục của hệ thống thanh toán điện tử một cách công khai, rõ ràng và được nêu rõ trong hợp đồng cung cấp dịch vụ với khách hàng. Cam kết này tối thiểu phải bao gồm cam kết về tổng thời gian dừng hệ thống trong năm, khoảng thời gian cung cấp dịch vụ trong ngày, thời gian phục hồi hệ thống sau khi gặp sự cố.

- Sử dụng các công cụ giám sát, theo dõi hiệu năng của hệ thống chính và hệ thống dự phòng đảm bảo hệ thống thanh toán điện tử hoạt động liên tục.

3. Đảm bảo tính toàn vẹn

- Đảm bảo tính toàn vẹn của thông tin trong quá trình xử lý, lưu trữ và truyền nhận giữa đơn vị cung cấp dịch vụ và khách hàng.

- Kết hợp các biện pháp an ninh về mặt hành chính và kỹ thuật trong: truy cập vật lý; truy cập lô gíc và quá trình nhập, xử lý, truyền dẫn, kết xuất, lưu trữ, khôi phục dữ liệu.

4. Xác thực khách hàng và xác thực giao dịch

- Đảm bảo xác thực và nhận dạng được khách hàng khi khách hàng truy cập và sử dụng dịch vụ thanh toán điện tử.

- Sử dụng xác thực hai yếu tố trên hệ thống thanh toán điện tử khi thực hiện giao dịch thanh toán và các giao dịch quan trọng như: tạo kết nối giữa các tài khoản, đăng ký thanh toán cho bên thứ ba, thay đổi hạn mức giao dịch trong ngày, thay đổi thông tin tài khoản liên quan đến dữ liệu cá nhân của khách hàng (như địa chỉ cơ quan hoặc nhà riêng, số điện thoại liên lạc, địa chỉ thư điện tử và các thông tin khác nhằm xác thực khách hàng).

5. Bảo vệ khách hàng

- Cung cấp đầy đủ thông tin về quyền lợi và nghĩa vụ của khách hàng trước khi ký kết hợp đồng cung cấp dịch vụ với khách hàng. Trong hợp đồng cung cấp dịch vụ phải nêu rõ việc đơn vị cung cấp dịch vụ đảm bảo các khoản nêu ra tại Điều này đối với khách hàng. Đơn vị cung cấp dịch vụ chịu trách nhiệm thực hiện đầy đủ các điều khoản thuộc trách nhiệm của mình nêu trong hợp đồng cung cấp dịch vụ ký kết với khách hàng.

- Trong hợp đồng cung cấp dịch vụ, đơn vị cung cấp dịch vụ phải nêu rõ trách nhiệm bảo mật các thông tin cá nhân của khách hàng khi sử dụng dịch vụ Internet Banking; nêu rõ cách thức ngân hàng thu thập; sử dụng thông tin khách hàng, cam kết không bán, tiết lộ, rò rỉ các thông tin đó.

- Có biện pháp đảm bảo an toàn, bảo mật trong trường hợp đơn vị cung cấp dịch vụ phân phối phần mềm cho khách hàng qua môi trường Internet.

- Chịu trách nhiệm kiểm tra, cảnh báo và thực hiện các biện pháp phòng, chống giả mạo website cung cấp dịch vụ thanh toán điện tử của đơn vị cung cấp dịch vụ; đồng thời có trách nhiệm thông báo phương thức xác định website thật đến 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)

Thẻ thông minh sử dụng thẻ plastic với chip mạch tích hợp nhúng cung cấp cho người dùng tính di động của thẻ và cũng như tính di động của dữ liệu. Nó kết hợp thẻ nhựa và thẻ từ được sử dụng cho các mục đích nhận dạng khác nhau trong một thẻ, có thể truy cập nhiều dịch vụ, mạng và Internet cho phép nó được sử dụng cho nhiều chức năng và ứng dụng.

Hệ thống thanh toán thẻ thông minh cung cấp cơ chế bảo mật xác thực ba yếu tố để xác minh và xác thực của một người dùng nhất định. Đó là số nhận dạng cá nhân (PIN), chữ ký số và sinh trắc vân tay. Cơ chế này làm tăng mức độ bảo mật của hệ thống thanh toán này. Thẻ tín dụng, thẻ ghi nợ và thẻ trả trước hiện đại diện cho hình thức thanh toán điện tử phổ biến nhất.

1.4.2 Hệ thống thanh toán điện tử dựa trên Internet Banking

Thanh toán điện tử dựa trên Internet Banking và liên quan đến việc chuyển tiền hoặc mua hàng trực tuyến qua Internet. Người tiêu dùng có thể chuyển tiền cho bên thứ ba từ tài khoản ngân hàng của họ hoặc họ có thể sử dụng thẻ tín dụng, thẻ ghi nợ và thẻ trả trước để mua hàng trực tuyến.

Hệ thống thanh toán điện tử cho phép khách hàng của tổ chức tài chính thực hiện các giao dịch tài chính trên một Website được bảo mật, có thể là ngân hàng bán lẻ, ngân hàng ảo, liên minh tín dụng hoặc xây dựng xã hội. Để truy cập cơ sở ngân hàng trực tuyến của tổ chức tài chính, một khách hàng sử dụng kết nối Internet của mình phải có tài khoản để xác minh. Điều này cho phép khách hàng liên kết các chi phí của mình với một số tài khoản mà anh ta kiểm soát như hóa đơn, tiết kiệm, khoản vay, thẻ tín dụng và các tài khoản khác

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

Hệ thống này cho phép người dùng sử dụng điện thoại di động của họ để thanh toán cho các giao dịch theo nhiều cách. Người tiêu dùng có thể gửi tin nhắn SMS, truyền số PIN, sử dụng WAP để thanh toán trực tuyến hoặc thực hiện các phân đoạn giao dịch khác của họ với điện thoại.

Khi điện thoại phát triển hơn, người dùng có thể sử dụng hồng ngoại, Bluetooth, NFC và các thiết bị khác để truyền dữ liệu tài khoản đầy đủ để thanh toán an toàn và dễ dàng từ điện thoại của họ. Các thiết bị di động có thể bao gồm điện thoại di động, PDA, máy tính bảng không dây và bất kỳ thiết bị nào khác thiết bị kết nối với mạng di động và cho phép thanh toán được thực hiện. Thanh toán di động có thể trở thành một lựa chọn thay thế cho tiền giấy, séc, thẻ tín dụng và thẻ ghi nợ. Nó cũng có thể được sử dụng để thanh toán hóa đơn, chuyển tiền điện tử, thanh toán qua ngân hàng Internet, ghi nợ trực tiếp và xuất trình hóa đơn điện tử. SMS bank là dịch vụ được cung cấp từ ngân hàng cho khách hàng của mình, cho phép họ vận hành các dịch vụ ngân hàng được chọn qua điện thoại di động của họ bằng tin nhắn SMS.

1.4.4 Hệ thống thanh toán sử dụng ví điện tử

Ví điện tử (ví điện tử) cung cấp tất cả các chức năng của ví hôm nay trên một thẻ thông minh tiện lợi. Ví điện tử cũng sẽ cung cấp nhiều tính năng bảo mật, không như cho các công ty cung cấp ví thông thường.

Ví dụ phổ biến nhất về ví điện tử Paypal. PayPal cho phép thanh toán và chuyển tiền được thực hiện thông qua Internet. Đó là một cách nhanh chóng để thanh toán và được trả tiền trực tuyến. Với tiền Paypal được gửi mà không chia sẻ thông tin tài chính. Mọi người cũng có thể linh hoạt thanh toán bằng số dư tài khoản, tài khoản ngân hàng và thẻ tín dụng của họ ..

Một ví dụ phổ biến khác về ví điện tử trên thị trường có thể được sử dụng cho thanh toán vi mô là Ví điện thoại Windows được phát triển bởi Microsoft. Ví điện tử này giúp loại bỏ việc nhập lại thông tin cá nhân trên các biểu mẫu, dẫn đến tốc độ và hiệu quả cao hơn cho người mua hàng trực tuyến.

Một ví điện tử mới nổi là Google Wallet, có chức năng tương tự PayPal để tạo điều kiện thanh toán và chuyển tiền trực tuyến. Nó bảo đảm tính bảo mật chưa bị bẻ khóa và khả năng gửi thanh toán dưới dạng tệp đính kèm qua email. Google Wallet cho phép cách thanh toán dễ dàng hơn trong các cửa hàng, trực

tuyến hoặc cho bất kỳ ai ở Mỹ có địa chỉ Gmail. Nó hoạt động với bất kỳ thẻ ghi nợ hoặc thẻ tín dụng, trên mọi nhà mạng di động. Các chức năng như "Chạm và thanh toán" là các yếu tố chính cho phép người dùng thanh toán ở cửa hàng tại hàng triệu địa điểm khác nhau.

1.4.5 Hệ thống sử dụng cổng thanh toán điện tử

Cổng thanh toán điện tử về bản chất là dịch vụ mà khách hàng có thể sử dụng thanh toán tại các website thương mại điện tử. Theo đó, nó cho phép kết nối an toàn giữa tài khoản khách hàng sử dụng (thẻ, ví điện tử,...) với tài khoản website bán hàng, giúp người sử dụng dịch vụ có thể chuyển - nhận tiền một cách an toàn và nhanh chóng.

Với nhu cầu sử dụng ngày càng tăng cao, các cổng thanh toán điện tử tại việt nam được triển khai ngày càng nhiều. Với mỗi nhu cầu khác nhau, người dùng có thể lựa chọn sử dụng các cổng thanh toán điện tử cung cấp các dịch vụ có những tính năng tương ứng để thỏa mãn mong muốn của mình.

Hiện nay, tại Việt Nam đang triển khai chính phủ điện tử, trong đó các dịch vụ công được triển khai trực tuyến. Do đó hệ thống thanh toán điên tử thường được triển khai trong các cổng thanh toán.

Hình 1.2 là giao diện cổng thanh toán điện tử của Tổng cục thuế Việt Nam.

Hình 1.2: Giao diện cổng thanh toán điện tử của Tổng cục thuế Việt Nam

Chẳng hạn như, nếu người dùng muốn nộp thuế điện tử thì hoàn toàn có thể sử dụng dịch vụ dịch vụ nộp thuế điện tử ngay qua Cổng thông tin điện tử của Tổng cục Thuế tại website https://nopthue.gdt.gov.vn/.

Việc nộp thuế qua cổng thanh toán điện tử của Tổng cục thuế không những giúp các doanh nghiệp tiết kiệm tối đa thời gian, chi phí mà còn chủ động hơn trong việc nộp thuế đúng hạn, tránh trường hợp nộp thuế quá hạn dẫn đến tình trạng bị phạt.

1.5 Kết luận chương 1

Chương 1 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 hướng tới nhằm giảm thiểu rủi ro trong các hệ thống thanh toán điện tử. Các nội dung này là các kiến thức cơ bản nền tảng để nghiên cứu tiếp theo của luận văn.

Trên cơ sở đó, chương 2 luận văn sẽ khảo sát về bảo mật của hệ thống thanh toán điện tử và các giải pháp bảo mật trong hệ thống thanh toán điện tử.

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

Trong mùa dịch mùa dịch COVID-19, đi kèm với xu hướng "giãn cách toàn xã hội", các công cụ thanh toán điện tử cũng được người dân ưu tiên sử dụng, thay cho phương thức thanh toán tiền mặt truyền thống.

Đi kèm với việc phương thức thanh toán điện tử "lên ngôi" thì rủi ro về bảo mật với các vấn đề về lộ thông tin cá nhân, giao dịch thanh toán càng có khả năng xảy ra. An toàn trước các cuộc tấn công là một vấn đề mà các hệ thống giao dịch trực tuyến cần giải quyết. Vì vậy, các hệ thống thanh toán điện tử cần phải có cơ chế đảm bảo an toàn trong quá trình giao dịch điện tử. Một hệ thống thông tin trao đôi dữ liệu an toàn, trong đó có hệ thống thanh toán điện tử phải đáp ứng tối thiểu các yêu cầu sau:

- Hệ thống phải đảm bảo dữ liệu trong quá trình truyền đi là không bị đánh cắp.
- Hệ thống phải có khả năng xác thực, tránh trường hợp giả danh, giả mạo.

Do vậy, hệ thống thanh toán điện tử cần cần tập trung vào việc bảo vệ các tài sản của khách hàng khi chúng được chuyển tiếp giữa máy khách và máy chủ từ xa. Để thực hiện mục tiêu trên, trong các hệ thống thanh toán điện tử thường sử dụng các hệ mật mã, các chứng chỉ số và sử dụng chữ ký số trong quá trình thực hiện giao dịch.

Bộ Thông tin và Truyền thông cũng đã ban hành hướng dẫn một số giải pháp tăng cường bảo mật an toàn cho hệ thống thông tin theo công văn số 3024/BTTT-VNCERT "V/v hướng dẫn một số giải pháp tăng cường bảo đảm an toàn cho hệ thống

thông tin" đã có giải pháp cụ thể là Tổ chức triển khai hoạt động tổng kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho các hệ thống thông tin, máy chủ, máy trạm… vì thế việc đảm bảo an toàn an ninh bảo mật trên không gian internet đặc biệt là với hệ thống thanh toán điện tử là cực kỳ cấp bách, hệ trọng.

Trong chương 1 luận văn đã khảo sát một số vấn đề bảo mật đối với hệ thống thanh toán điện tử. Trong chương này, luận văn sẽ nghiên cứu các giải pháp bảo mật cho hệ thống thanh toán điện tử.

Trước hết, luận văn khảo sát một số phương thức tấn công điển hình vào các hệ thống thanh toán điện tử.

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

Kẻ xâm nhập tấn công hệ thống thanh toán điện tử với mục tiêu làm cho các giao dịch thanh toán bị từ chối hoặc giảm sự khả dụng của hệ thống. Ví dụ, kẻ tấn công có thể làm tràn ngập dịch vụ chuyển tiếp cuộc gọi chuyển tiền với các yêu cầu chuyển tiếp cuộc gọi. Điều này có thể gây ra sự từ chối dịch vụ.

Nghe trộm sự truyền dẫn thông tin thanh toán điện tử

Kẻ tấn công xoay sở để can thiệp vào sự truyền dẫn thông tin trong hệ thống thanh toán điện tử. Điều này có thể xảy ra trong suốt quá trình nhận thực, báo hiệu và chuyển tiếp thông tin. Nghe trộm thông tin có thể gây ra các vấn đề về lộ, sai lệch thông tin. Dữ liệu nhận được nhờ nghe trộm có thể được sử dụng để thực hiện các tấn công trên mạng 3G. Ví dụ, kẻ tấn công có thể xem số chuyển tiếp cuộc gọi và tìm ra vị trí của máy di động nạn nhân.

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

Kẻ xâm nhập xoay sở để điều khiển sự truyền dẫn thông tin giữa hai thực thể trong thống thanh toán điện tử nhằm biến đổi các bản tin. Sau đó, có thể làm ngừng các giao dịch giữa hai thực thể hoặc làm thay đổi nội dung các gói tin trao đổi.

Các tấn công ở giữa

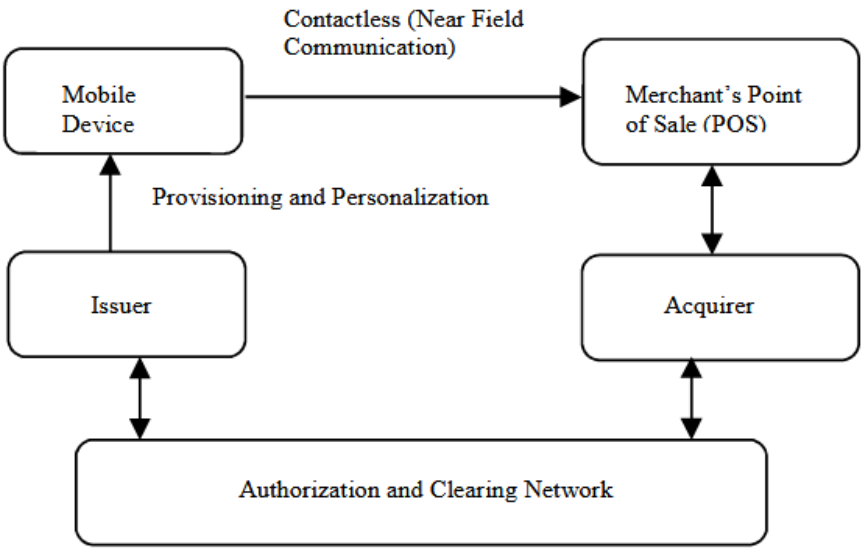
Kẻ xâm nhập ở giữa hai thực thể truyền thông trong thống thanh toán điện tử. Không thực thể nào cảnh giác về sự có mặt của kẻ xâm nhập và cả hai thực thể vẫn nghĩ rằng họ thực sự đang truyền thông với nhau. Trong khi đó, kẻ xâm nhập đang giao tiếp với họ và tạo ra các rủi ro cho các giao dịch thanh toán điện tử.

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

Kẻ tấn công xoay sở để có thể truy nhập bất hợp pháp tới các dịch vụ của thống thanh toán điện tử bằng cách giả mạo hoặc sử dụng sai lệch quyền truy nhập.

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. Trong đó, truyền dẫn vô tuyến sẽ dễ bị nghe trộm và giả mạo hơn so với truyền dẫn hữu tuyến. Tính di động của người sử dụng và truy nhập mạng toàn cầu làm nảy sinh các nguy cơ bảo mật tiềm tàng. Các kiểu dữ liệu khác nhau như dữ liệu người sử dụng, dữ liệu tính cước, dữ liệu thông tin khách hàng, và dữ liệu quản lý mạng sẽ yêu cầu kiểu và mức độ bảo mật khác nhau. 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

Trong kiến trúc trên, hệ thống thanh toán điện tử bao gồm các thực thể sau đây: khách hàng sử dụng, nhà phát hành, người mua và người bán. Quá trình bảo mật giao dịch thanh toán điện tử là quá trình ủy quyền giám sát các giao dịch thanh toán di động để phát hiện việc sử dụng gian lận và đưa ra quyết định liên quan đến việc chấp thuận hay từ chối giao dịch bằng cách xác nhận mã hóa động.

Thông thường, thiết bị di động được sử dụng như là một token thanh toán và nó chứa thông tin tuân thủ tiêu chuẩn EMV và các khóa mã hóa được lưu trữ trên thành phần chống giả mạo của thiết bị di động được gọi tên là phần tử an ninh (Secure Element).

Secure Element trong thiết bị di động cung cấp môi trường chống giả mạo để lưu trữ dữ liệu thanh toán, thực hiện các chức năng mã hóa và bảo mật giao dịch. Secure Element có thể là một vi mạch chuyên dụng được nhúng vào thiết bị di động hỗ trợ NFC.

Trong các mục tiếp theo, luận văn sẽ khảo sát một số giải pháp bảo mật cho hệ thống thanh toán điện tử bao gồm: giải pháp bảo mật 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.

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.

Một ví dụ phổ biến xảy ra trong các kết nối dial-up từ xa. Người dùng từ xa, chẳng hạn như những người đi du lịch nhưng vẫn làm việc tại công ty, họ phải kết nối tới hệ thống modem của công ty để truy nhập mạng và tài nguyên dữ liệu. Để xác định và xác nhận các truy nhập đấy với máy chủ quản lý, họ phải nhập một tên đăng nhập và mật khẩu. Bởi vì chính sự trao đổi giữa người dùng và mật khẩu có thể bị theo dõi bởi những kẻ xâm nhập, điều quan trọng là nó không thể sử dụng lại. Nói cách khác, kẻ xâm nhập không thể tái sử dụng mật khẩu để giả mạo truy cập của một người dùng hợp pháp mà kẻ xâm nhập đã bắt được mật khẩu.

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.

Quá trình tạo mật khẩu mới sẽ lặp lại mỗi lần người dùng đăng nhập vào hệ thống được bảo mật bằng OTP. Công nghệ OTP được dùng nhiều trong chứng thực trực tuyến (thương mại trực tuyến). Hiện nay người dùng các thiết bị cầm tay như

iPhone, Blackberry cũng có thể tự cài đặt cơ chế bảo mật OTP bằng các chương trình như VeriSign, RSA SecureID hay SafeNet MobilePASS.

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.

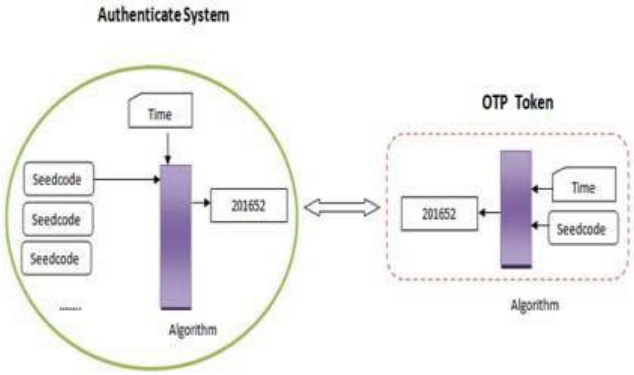
Mô hình sinh mã OTP theo thời gian

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.

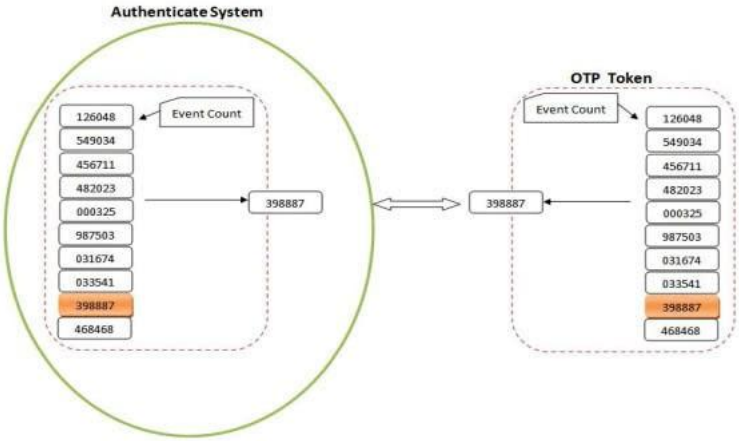


Hình 2.2: Mô hình của cơ chế sinh mã ngẫu nhiên dựa theo thời gian.

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). Nó hoạt động với tài nguyên và đăng nhập được trên tất cả các nền tảng máy tính, và trình duyệt không cần phần mềm cài đặt Client. Nhanh chóng và tích hợp dễ dàng vào bất kỳ ứng dụng web nào (Windows, Linux, Mac, Internet Explorer, Firefox,...).

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.

Hiện tại, Tokenization là phương thức cực kỳ hấp dẫn, do nhu cầu ngày càng tăng đối với các ứng dụng thanh toán di động. Về cơ bản, Tokenization là mã hóa thông tin nhạy cảm của thẻ tín dụng để tăng cường mức độ bảo mật cho dữ liệu.

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. Mã Token này được sử dụng thay cho thông tin thẻ trong các giao dịch sau này, đảm bảo an toàn tuyệt đối. Nếu xảy ra lỗ hổng dữ liệu, kẻ gian sẽ không thể truy cập được vào dữ liệu thẻ thật sự, bởi những mã Token được lưu trong hệ thống sẽ không có giá trị đối với tất cả mọi khách hàng, ngoại trừ với người dùng thanh toán hợp pháp.

Đây là một giải pháp mà những tổ chức tín dụng, tài chính lớn trên thế giới đã áp dụng khi phát hành các thẻ thanh toán cho khách hàng của mình.

Thông thường, token được sử dụng để ngăn chặn gian lận thẻ tín dụng. Trong token thì thẻ tín dụng, số tài khoản chính của khách hàng (PAN) được thay thế bằng một loạt các số được tạo ngẫu nhiên. Các mã token này sau đó có thể được truyền qua internet hoặc các mạng không dây khác nhau cần thiết để xử lý thanh toán mà không bị lộ chi tiết thực tế của ngân hàng. Số tài khoản ngân hàng thực tế được đảm bảo an toàn.

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. Trước đó, nhà cung cấp sẽ lưu trữ dữ liệu thẻ tín dụng trên máy chủ của họ, điều đó có nghĩa là bất kỳ ai có quyền truy cập hệ thống đều có thể xem thông tin nhạy cảm.

Hệ thống mà TrustC Commerce đã phát triển đã thay thế số tài khoản chính (PAN) bằng một số ngẫu nhiên, được gọi là Token. Khi một thương gia cần xử lý thanh toán, họ có thể tham chiếu mã thông báo và TrustC Commerce sẽ xử lý khoản thanh toán thay cho họ.

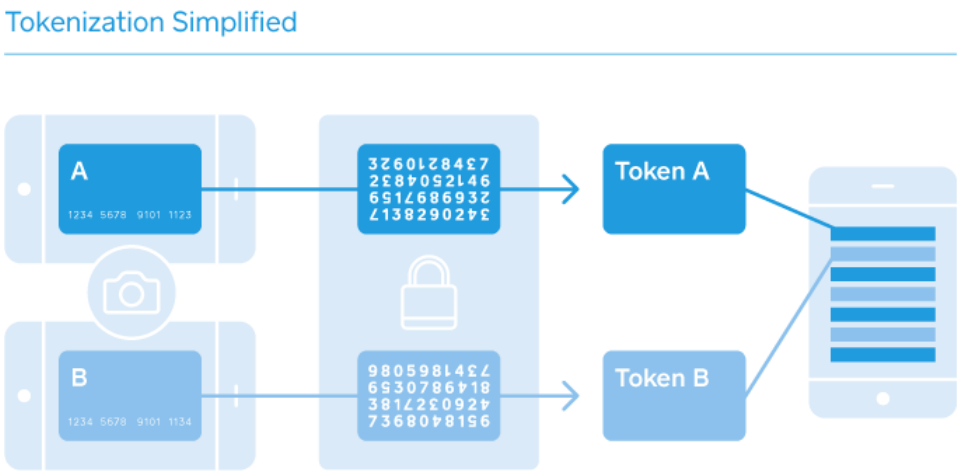
Hệ thống này đã loại bỏ sự cần thiết của các nhà cung cấp để tự lưu trữ dữ liệu thẻ tín dụng và do đó làm tăng đáng kể tính bảo mật của dữ liệu chủ thẻ. Mã thông báo là không thể mã hóa ngược - nó không thành vấn đề nếu tin tặc chặn các chi tiết thanh toán vì không có số tài khoản nào có thể hiểu được từ token được mã hóa.

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.

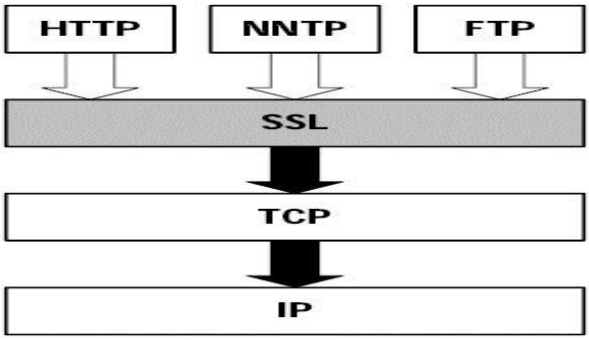
2.4 Giải pháp bảo mật dựa trên SSL

2.4.1 Tổng quan về SSL

Để hiểu rõ hơn về SSL, trước hết cần cần tìm hiểu ***Certificate Authority* (CA)** là gì. CA là tổ chức phát hành các chứng thực các loại chứng thư số cho người dùng, doanh nghiệp, máy chủ (server), mã code, phần mềm. Nhà cung cấp chứng thực số đóng vai trò là bên thứ ba (được cả hai bên tin tưởng) để hỗ trợ cho quá trình trao đổi thông tin an toàn.

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. Giao thức SSL được hình thành và phát triển đầu tiên năm 1994 bởi nhóm nghiên cứu Netscape dẫn dắt bởi Elgammal và ngày nay đã trở thành chuẩn bảo mật thực hành trên mạng Internet. Phiên bản SSL hiện nay là 3.0 và vẫn đang được hoàn thiện, bổ sung. Tương tự như SSL, một giao thức khác có tên là PCT – Private Communication Technology được đề xướng bởi Microsoft hiện nay cũng được sử dụng rộng rãi trong các mạng máy tính chạy trên hệ điều hành WindowNT. Ngoài ra, một chuẩn của IETF (Internet Engineering Task Force) có tên là TLS (Transport Layer Security) dựa trên SSL cũng được hình thành và xuất bản dưới khuôn khổ nghiên cứu của IETF Internet Draff được tích hợp và hỗ trợ trong sản phẩm của Netscape. Điểm cơ bản của SSL là được thiết kế độc lập với tầng ứng dụng để đảm bảo tính bí mật, an toàn và chống giả mạo luồng thông tin qua Internet giữa hai ứng dụng bất kỳ, thí dụ như webserver và các trình duyệt khách (browsers), do đó được sử dụng rộng rãi trong nhiều ứng dụng khác nhau trên môi trường Internet. Toàn bộ cơ chế và hệ thống thuật toán mã hoá sử dụng trong SSL được phổ biến công khai, trừ khoá phiên (session key) được sinh ra tại thời điểm trao đổi giữa hai ứng dụng là ngẫu nhiên và bí mật đối với người quan sát trên mạng máy tính. Ngoài ra, giao thức SSL còn đòi hỏi ứng dụng chủ phải được chứng thực bởi một đối tượng lớp thứ ba (CA) thông qua giấy chứng thực điện tử (digital certificate) dựa trên mật mã công khai (ví dụ RSA).

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: cho phép người sử dụng xác thực được server muốn kết nối. Lúc này, phía trình duyệt sử dụng các kỹ thuật mã hóa công khai để chắc chắn rằng chứng chỉ và publicID của server là có giá trị và được cấp phát bởi một CA (Certificate Authority) trong danh sách các CA đáng tin cậy của client. Sự xác thực này có thể quan trọng nếu người sử dụng gửi số thẻ tín dụng qua mạng và muốn kiểm tra định danh server nhận.

Chứng thực SSL Client : cho phép server xác thực được người sử dụng muốn kết nối. Phía server cũng sử dụng các kỹ thuật mã hoá khoá công khai để kiểm tra chứng chỉ của client và publicID là đúng, được cấp phát bởi một CA trong danh sách các CA đáng tin cậy của Server hay không. Điều này rất quan trọng đối với các nhà cung cấp. Ví dụ như khi một ngân hàng định gửi các thông tin tài chính mang tính bảo mật tới khách hàng thì họ rất muốn kiểm tra định danh người nhận.

Mã hoá kết nối : tất cả các thông tin trao đổi giữa client và server được mã hoá trên đường truyền nhằm nâng cao khả năng bảo mật. Điều này rất quan trọng đối với cả hai bên khi có các giao dịch mang tính riêng tư. Ngoài ra tất cả các dữ liệu được gửi đi trên một kết nối SSL đã được mã hoá còn được bảo vệ nhờ cơ chế tự động phát hiện các xáo trộn, thay đổi trong dữ liệu.

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…). Đảm bảo thông tin không thể bị truy cập bởi đối tượng thứ ba. Danh tính của người bên kia có thể được xác thực bằng mật mã phi đối xứng, hoặc khoá công khai (ví dụ RSA, DSS…). Xác thực tức là đảm bảo tính xác thực của trang mà chúng ta sẽ làm việc ở đầu kia của kết nối. Cũng như vậy, các trang Web cũng cần phải kiểm tra tính xác thực của người sử dụng.

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.

Các thuật toán trao đổi khoá như KEA và RSA key exchange được sử dụng để hai bên client và server xác lập khoá đối xứng mà họ sẽ sử dụng trong suốt phiên giao dịch SSL, thuật toán được sử dụng phổ biến là RSA key exchange.

Các phiên bản SSL 2.0, 3.0 hỗ trợ cho hầu hết các bộ mã hoá. Người quản trị có thể tuỳ chọn bộ mã hoá sẽ dùng cho cả client và server. Khi một client và server trao đổi thông tin trong giai đoạn bắt tay (handshake), họ sẽ xác định bộ mã hoá mạnh nhất có thể và sử dụng chúng trong phiên giao dịch SSL.

Các quyết định về bộ mã hoá tuỳ thuộc vào quyết định của tổ chức dựa trên các thoả hiệp giữa dữ liệu nhạy cảm, tốc độ mã hoá và việc áp dụng các quy tắc. Một vài tổ chức có thể không hỗ trợ các hệ mã hoá yếu nhằm loại bỏ các kết nối SSL với hệ mã hoá yếu. Nhằm phục vụ một khối lượng người dùng lớn, người quản trị có thể muốn hỗ trợ càng nhiều hệ mã hoá trong SSL càng tốt. Theo cách thức này, khi một client hay server trong cùng một nước kết nối tới client và server khác trong cùng nước tương ứng, chúng sẽ thoả hiệp nhằm sử dụng các hệ mã hoá mạnh nhất có thể. Và khi client, server trong nước kết nối tới client hay server trên thế giới, chúng sẽ thỏa hiệp để sử dụng các hệ mã hoá được cho phép bởi chính phủ Mỹ. Tuy nhiên do hệ mã hoá 40 bit có thể bị phá vỡ dễ dàng, các nhà quản trị có thể sử dụng các hệ mã hoá hợp pháp mạnh hơn và cần loại bỏ việc hỗ trợ các hệ mã hoá 40 bit.

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. Theo luật pháp Mỹ, các mật mã "mạnh" được phân

loại vào nhóm "vũ khí" (weapon) và do đó khi sử dụng ngoài Mỹ (coi như là xuất khẩu vũ khí) phải được phép của chính phủ Mỹ hay phải được cấp giấy phép của Bộ Quốc phòng Mỹ (DoD). Đây là một lợi điểm cho quá trình thực hiện các dịch vụ thương mại và thanh toán điện tử trong Mỹ và các nước đồng minh phương Tây và là điểm bất lợi cho việc sử dụng các sản phẩm cần có cơ chế bảo mật và an toàn trong giao dịch điện tử nói chung và thương mại điện tử nói riêng trong các nước khác.

Các phương thức tấn công (hay bẻ khoá) của các thuật toán bảo mật thường dùng dựa trên phương pháp "tấn công vét cạn" (brute-force attack) bằng cách thử-sai miền không gian các giá trị có thể của khoá. Số phép thử-sai tăng lên khi độ dài khoá tăng và dẫn đến vượt quá khả năng và công suất tính toán, kể cả các siêu máy tính hiện đại nhất. Thí dụ, với độ dài khoá là 40bit, thì số phép thử sẽ là 2^{40}=1,099,511,627,776 tổ hợp. Tuy nhiên độ dài khoá lớn kéo theo tốc độ tính toán giảm (theo luỹ thừa nghịch đảo) và dẫn đến khó có khả năng áp dụng trong thực tiễn. Một khi khoá bị phá, toàn bộ thông tin giao dịch trên mạng sẽ bị kiểm soát toàn bộ. Tuy nhiên do độ dài khoá lớn (thí dụ 128, 256 bít), số phép thử-sai trở nên "không thể thực hiện" vì phải mất hàng năm hoặc thậm chí hàng nghìn năm với công suất và năng lực tính toán của máy tính mạnh nhất hiện nay.

Ngay từ năm 1995, bản mã hoá 40bit đã bị phá bởi sử dụng thuật toán vét cạn. Ngoài ra, một số thuật toán bảo mật (như DES 56bit, RC4, MD4,...) hiện nay cũng bị coi là không an toàn khi áp dụng một số phương pháp và thuật toán tấn công đặc biệt. Đã có một số đề nghị thay đổi trong luật pháp Mỹ nhằm cho phép sử dụng rộng rãi các phần mềm mã hoá sử dụng mã hoá 56bit song hiện nay vẫn chưa được chấp thuận.

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. Sau đây là một số thông tin tham

khảo:

- Ngày 14 tháng 7 năm 1995, Hal Finney đặt một thách thức SSL đầu tiên một bản ghi phiên làm việc của trình duyệt Netscape sử dụng thuật toán RC4-128-EXPORT-20. Ngày 16 tháng 8 năm 1995, David Byers và Eric Young cùng với Adam Back đã phá thách thức này trong vòng 2 giờ, chi phí ước tính 10,000 USD.
- Ngày 19 tháng 8 năm 1995, Hal Finney đặt một thách thức SSL thứ hai cho cộng đồng những người làm mật mã một "key cracking ring" và cũng đã bị phá trong 32 giờ.
- Ngày 17 tháng 9 năm 1995, Ian Goldberg và David Wagner đã phá được thuật toán sinh số giả ngẫu nhiên (cơ sở cho việc sinh ra số nhận dạng phiên SSL - session ID) của phiên bản Netscape 1.1 trong vòng vài giờ trên một máy trạm làm việc. Điều này dẫn đến việc Netscape sau đó phải nhanh chóng đưa ra phiên bản để sửa "lỗ hổng" của bảo mật trong trình duyệt của mình. Hiện nay phiên bản mới nhất của Netscape có khả năng bảo mật an toàn cao nhưng chỉ được phép dùng trong phạm vi nước Mỹ.

2.4.4 Các loại chứng thực SSL

Domain Validation (DV SSL)

Chứng thư số SSL chứng thực cho Domain Name – Website. Khi 1 Website sử dụng DV SSL thì sẽ được xác thực tên domain, website đã được mã hoá an toàn khi trao đổi dữ liệu.

Organization Validation (OV SSL)

Chứng thư số SSL chứng thực cho Website và xác thực doanh nghiệp đang sở hữu website đó .

Extended Validation (EV SSL)

Cho khách hàng của bạn thấy Website đang sử dụng chứng thư SSL có độ bảo mật cao nhất và được rà soát pháp lý kỹ càng.

Subject Alternative Names (SANs SSL)

Nhiều tên miền hợp nhất trong 1 chứng thư số:

- Một chứng thư số SSL tiêu chuẩn chỉ bảo mật cho duy nhất một tên miền đã được kiểm định. Lựa chọn thêm SANs chỉ với chứng thư duy nhất bảo đảm cho nhiều tên miền con. SANs mang lại sự linh hoạt cho người sử dụng, dễ dàng hơn trong việc cài đặt, sử dụng và quản lý chứng thư số SSL. Ngoài ra, SANs có tính bảo mật cao hơn Wildcard SSL, đáp ứng chính xác yêu cầu an toàn đối với máy chủ và làm giảm tổng chi phí triển khai SSL tới tất cả các tên miền và máy chủ cần thiết.
- Chứng thư số SSL SANs có thể tích hợp với tất cả các loại chứng thư số SSL của GlobalSign bao gồm: *Chứng thực tên miền (DV SSL)*, *Chứng thực tổ chức doanh nghiệp (OV SSL)* và *Chứng thực mở rộng cao cấp (EV 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

Khi thực hiện các giao dịch thanh toán điện tử trên mạng, thông tin/dữ liệu trên môi trường mạng internet có khả năng gặp nhiều rủi ro. Do đó, trong các hệ thống thanh toán điện tử, hạ tầng mạng cần được bảo đảm bởi cơ chế bảo mật SSL thực hiện trên tầng vận tải. Giải pháp kỹ thuật bảo mật này có thể được sử dụng các phân đoạn mạng của hạ tầng mạng phục vụ 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. Tại mức cao nhất là phần mềm ứng dụng hoặc các trình duyệt. Chạy phía dưới các ứng dụng này là giao thức tầng ứng dụng bao gồm Telnet, FTP, HTTP…Bên dưới nữa là giao thức SSL và các thuật toán mã hoá được sử dụng để kết nối. Bên dưới SSL là tầng giao vận. Hầu hết các trường hợp đó là TCP/IP. Tuy nhiên, giao thức SSL là duy nhất,

không phụ thuộc vào giao thức mạng. Bởi vì SSL không phụ thuộc vào các tầng giao thức cho nên SSL trở thành một nền tảng độc lập hay là một thực thể mạng độc lập.

Một sức mạnh khác của SSL đó là ngăn chặn cách thức tấn công từ điển. Cách thức này sử dụng từ điển để phá khoá trong hệ mã hoá. SSL khắc phục được điều này bởi cho phép không gian khoá là rất lớn đối với hệ mã hoá được sử dụng. SSL cung cấp hai mức độ tin cậy : 40 bit và 128 bit tuỳ thuộc khả năng của browser. SSL 128 bit và SSL 40 bit ý nói độ dài của khoá phiên dùng để mã hoá dữ liệu sau khi đã định danh và được thiết lập bằng giải thuật khoá công khai (RSA hoặc Diffie-Hellman). Độ dài của khoá phiên càng lớn thì độ bảo mật càng cao. Hiện nay SSL 128 bit có độ tin cậy lớn nhất. Theo RSA phải mất hàng tỉ năm mới có thể giải mã được bằng các kỹ thuật hiện nay. Cách thức tấn công từ điển có thể bị ngăn chặn bởi sử dụng phương pháp số nonce (nonce number). Số này được sinh ngẫu nhiên được server sử dụng, nonce number là một số không thể bị phá khoá.

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. Và bởi vì SSL cung cấp các dịch vụ bảo mật, cần quan tâm đặc biệt tới các giới hạn của nó. Giới hạn của SSL thường là trong ba trường hợp. 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.

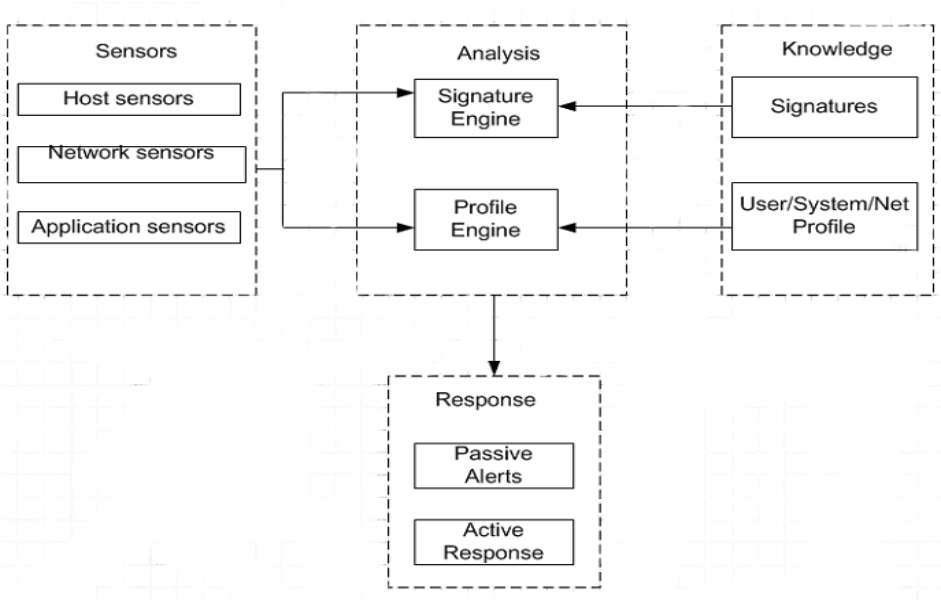
2.5 Giải pháp bảo mật dựa trên hệ thống phát hiện và ngăn chặn xâm nhập mạng

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. Sau đó hệ thống sẽ phân tích để tìm dấu hiệu của sự xâm nhập hoặc tấn công hệ thống trái phép và cảnh báo đến người quản trị hệ thống. Do đó, IDS có khả năng ứng dụng phát hiện tấn công hệ thống thanh toán điện tử.

Các thành phần của IDS

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



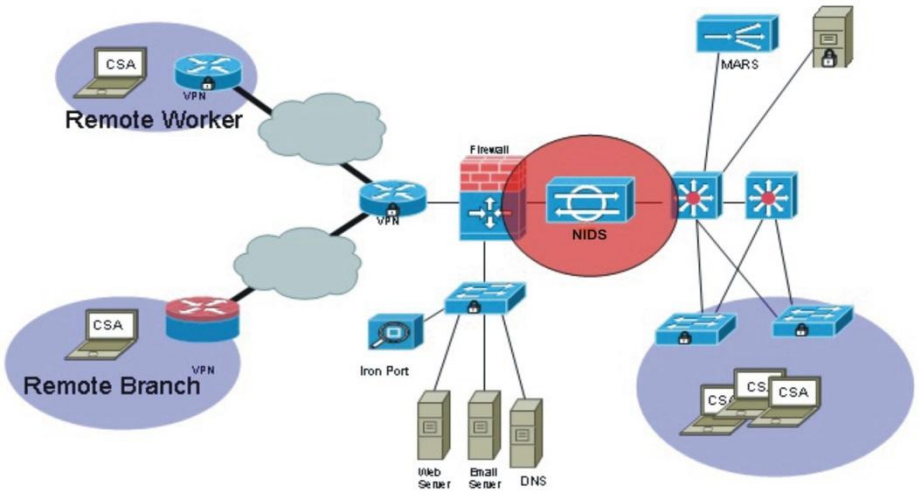
Hình 2.6: Các thành phần của hệ thống IDS [10]

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:

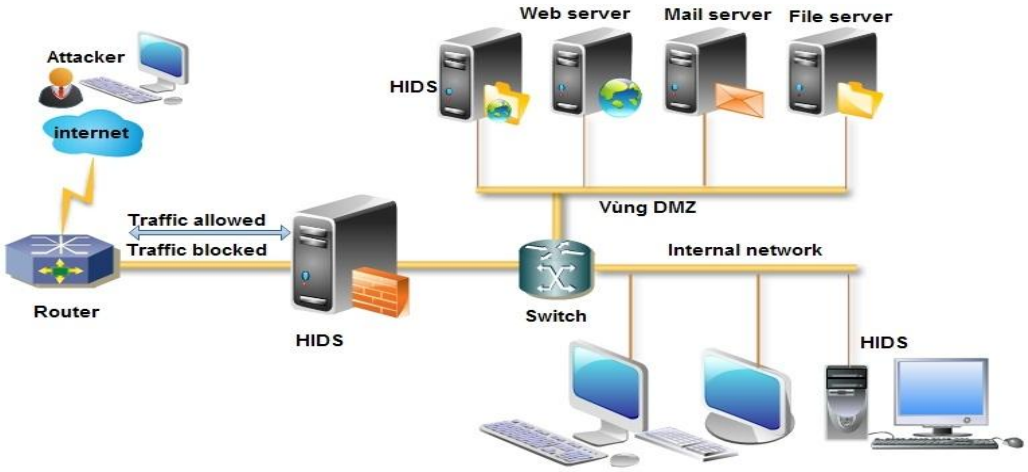
Dựa trên phạm vi giám sát, IDS được chia thành 2 loại:

(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.

HIDS thường dựa trên các tập luật (rule-based) để phân tích các hoạt động. Nhiệm vụ chính của HIDS là giám sát sự thay đổi trên hệ thống.

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

- **Signature-based IDS:** Signature-based IDS phát hiện xâm nhập dựa trên dấu hiệu của hành vi xâm nhập, thông qua phân tích lưu lượng mạng và nhật ký hệ thống. Kỹ thuật này đòi hỏi phải duy trì một cơ sở dữ liệu về các dấu hiệu xâm nhập (signature database), và cơ sở dữ liệu này phải được cập nhật thường xuyên mỗi khi có một hình thức hoặc kỹ thuật xâm nhập mới.

- **Anomaly-based IDS**: phát hiện xâm nhập bằng cách so sánh (mang tính thống kê) các hành vi hiện tại với hoạt động bình thường của hệ thống để phát hiện các bất thường (anomaly) có thể là dấu hiệu của xâm nhập. Ví dụ, trong điều kiện bình thường, lưu lượng trên một giao tiếp mạng của server là vào khoảng 25% băng thông cực đại của giao tiếp. Nếu tại một thời điểm nào đó, lưu lượng này đột ngột tăng lên đến 50% hoặc hơn nữa, thì có thể giả định rằng server đang bị tấn công DoS.

Hệ thống IDS có khả năng ứng dụng phát hiện tấn công hệ thống thanh toán điện tử dựa trên các dữ liệu thu thập được kết hợp với các kỹ thuật phát hiện tấn công.

Snort

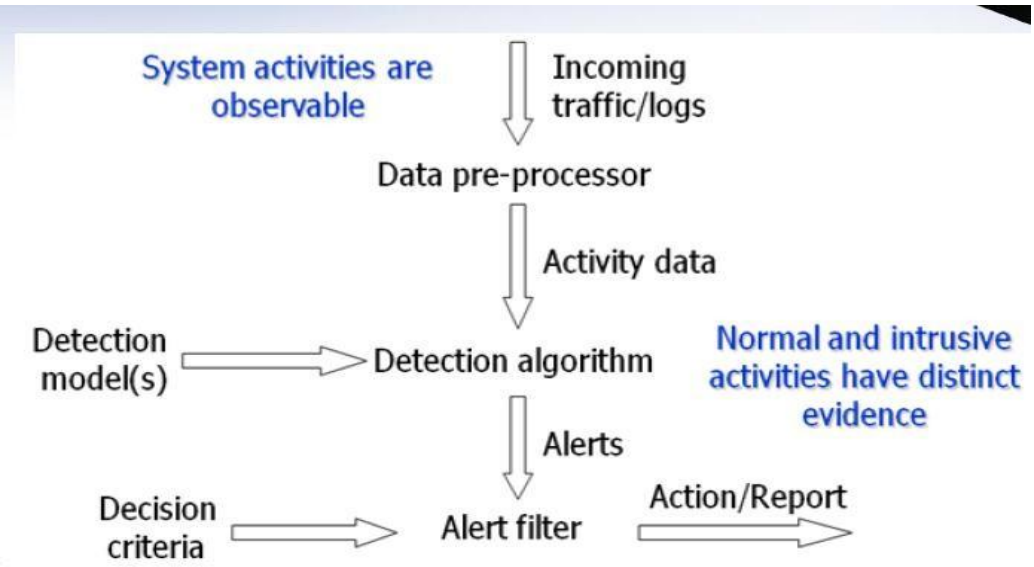
Một trong những phần mềm IDS phổ biến hiện nay là Snort. Đây là một sản phẩm NIDS mã nguồn mở với hệ thống signature database (gọi là rule database) được cập nhật thường xuyên bởi nhiều thành viên trong cộng đồng Internet.

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). Ngoài ra còn có rất nhiều chương trình add-on cho Snort để có thể quản lý các file log, các tập luật và cảnh báo cho quản trị viên khi phát hiện sự xâm nhập hệ thống. Tuy không phải là phần lõi của

Snort, nhưng những thành phần này cung cấp rất nhiều tính năng phong phú để có được một hệ thống phát hiện và phòng chống xâm nhập tốt.

2.5.2. 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 2.9: 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. Với "quyền tối thượng", các hệ thống phòng chống xâm nhập có thể "nắm" lấy bất cứ lưu lượng nào của các gói tin mạng và đưa ra quyết định có chủ ý – liệu đây có phải là một cuộc tấn công hay một sự sử dụng hợp pháp – sau đó thực hiện hành động thích hợp để hoàn thành tác vụ một cách trọn vẹn. Kết quả cuối cùng là một nhu cầu có hạn định cho các giải pháp phát hiện hay giám sát xâm nhập một khi tất cả những gì liên quan đến mối đe doạ đều bị ngăn chặn.

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. Hệ thống IPS có thể kiểm soát luồng dữ liệu vào, phân tích và phát hiện các dấu hiệu của sự xâm nhập. Với vị trí này, OOB IPS có thể quản lý firewall, chỉ dẫn nó chặn lại các hành động nghi ngờ.

- **In-line IPS**: Vị trí IPS nằm trước firewall, luồng dữ liệu phải đi qua chúng trước khi tới firewall. Điểm khác chính so với OOB IPS là có thêm chức năng traffic-blocking. Điều đó làm cho IPS có thể ngăn chặn lưu lượng nguy hiểm nhanh hơn so với OOB IPS. Tuy nhiên vị trí này sẽ làm cho tốc độ luồng thông tin qua ra vào mạng chậm hơn.

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.

- **Modul phân tích luồng dữ liệu**: Modul này có nhiệm vụ lấy tất các gói tin đi đến mạng để phân tích. Thông thường các gói tin có địa chỉ không phải của một card mạng thì sẽ bị card mạng đó hủy bỏ nhưng card mạng của IPS được đặt ở chế độ thu nhận tất cả. Tất cả các gói tin qua chúng đều được sao chụp, xử lý, phân tích đến từng trường thông tin. Bộ phân tích đọc thông tin từng trường trong gói tin, xác định chúng thuộc kiểu gói tin nào, dịch vụ gì ... Các thông tin này được chuyển đến modul phát hiện tấn công.

- **Modul phát hiện tấn công**: Đây là modul quan trọng nhất trong hệ thống có nhiệm vụ phát hiện các cuộc tấn công. Có hai phương pháp để phát hiện các cuộc tấn công: Misuse Detection (dò sự lạm dụng) và Anomaly Detection (dò sự không bình thường).

- **Modul phản ứng**: Khi có dấu hiệu của sự tấn công hoặc thâm nhập, modul phát hiện tấn công sẽ gửi tín hiệu báo hiệu có sự tấn công hoặc thâm nhập đến modul

phản ứng. Lúc đó modul phản ứng sẽ kích hoạt tường lửa thực hiện chức năng ngăn chặn cuộc tấn công hay cảnh báo tới người quản trị. Tại modul này, nếu chỉ đưa ra các cảnh báo tới các người quản trị và dừng lại ở đó thì hệ thống này được gọi là hệ thống phòng thủ bị động. Modul phản ứng này tùy theo hệ thống mà có các chức năng và phương pháp ngăn chặn khác nhau.

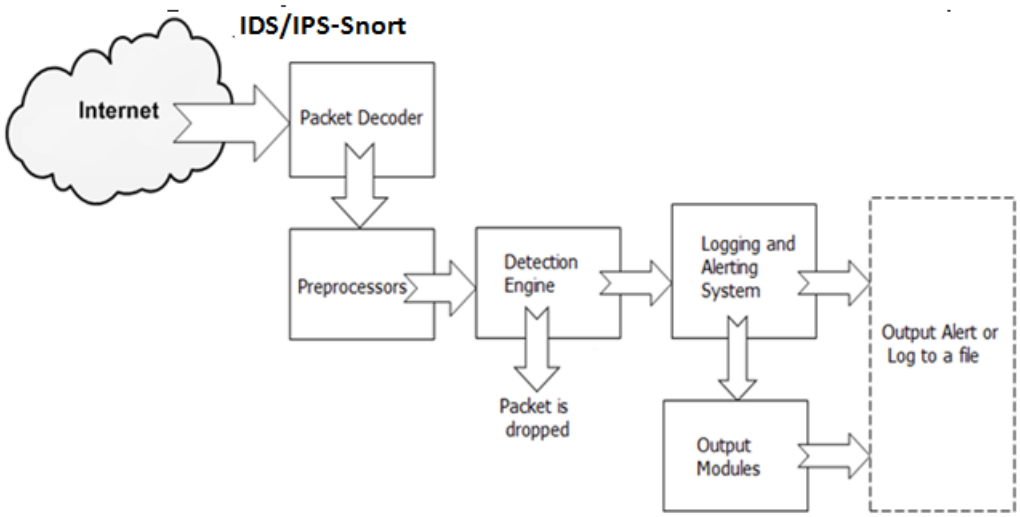
Hai kỹ thuật ngăn chặn thường được áp dụng:

- Kết thúc tiến trình (Terminate session): Cơ chế của kỹ thuật này là hệ thống IPS gửi các gói tin nhằm phá huỷ tiến trình bị nghi ngờ.

- Huỷ bỏ tấn công (Drop attack): Kỹ thuật này dùng tường lửa để hủy bỏ gói tin hoặc chặn đường một gói tin đơn, một phiên làm việc hoặc một luồng thông tin tấn công.

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 2.10: 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 2 luận văn đã khảo sát tổng quan các vấn đề về bảo mật cho hệ thống thanh toán điện tử. Từ đó, luận văn đã khảo sát một số 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.

Trên cơ sở đó, chương 3 luận văn sẽ đề xuất giải pháp bảo mật phù hợp cho hệ thống thanh toán điện tử của Tổng công ty viễn thông MobiFone.

.

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

Tổng công ty Viễn thông MobiFone (thường gọi tắt là MobiFone) được thành lập ngày 16/04/1993 với tên gọi ban đầu là Công ty thông tin di động (VMS). Ngày 01/12/2014, Công ty được chuyển đổi thành Tổng công ty Viễn thông MobiFone.

Hiện nay, Tổng công ty Viễn thông MobiFone có 20 Phòng, Ban chức năng và 20 đơn vị trực thuộc khác bao gồm 9 Công ty Dịch vụ MobiFone tại 9 khu vực, Trung tâm Viễn thông quốc tế MobiFone, Trung tâm Dịch vụ đa phương tiện và giá trị gia tăng MobiFone, Trung tâm Công nghệ thông tin MobiFone, Trung tâm Quản lý và điều hành mạng (NOC), Trung tâm Mạng lưới MobiFone miền Bắc, Trung, Nam, Trung tâm Đo kiểm và sửa chữa thiết bị viễn thông MobiFone, Trung tâm Tính cước và Thanh khoản, Trung tâm Nghiên cứu và Phát triển, Trung tâm Tư vấn thiết kế MobiFone.

Ngoài ra, MobiFone có bốn Công ty con bao gồm Công ty cổ phần Dịch vụ kỹ thuật MobiFone, Công ty cổ phần Công nghệ MobiFone toàn cầu, Công ty cổ phần Dịch vụ gia tăng MobiFone, và Công ty cổ phần nghe nhìn toàn cầu.

Tại Việt Nam, MobiFone là một trong ba mạng di động lớn nhất với hơn 30% thị phần. Tổng doanh thu năm 2017 của MobiFone đạt xấp xỉ 2 tỷ đô la Mỹ. Các lĩnh vực kinh doanh chủ yếu của MobiFone gồm: dịch vụ viễn thông truyền thống, VAS, Data, Internet & truyền hình IPTV/cable TV, sản phẩm khách hàng doanh nghiệp, dịch vụ công nghệ thông tin, bán lẻ và phân phối và đầu tư nước ngoài [16].

Hạ tầng mạng di động của MobiFone cũng không ngừng phát triển rộng khắp trên cả nước. Vào đầu năm 2020, MobiFone đã chính thức thử nghiệm thành công hệ thống mạng 5G.

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

Hiện nay, MobiFone cung cấp khá nhiều dịch vụ khác nhau trên nền tảng mạng di động ngoài dịch vụ thoại và nhắn tin truyền thống [16].

Mobile Internet

Mobile Internet là dịch vụ truy cập Internet trực tiếp từ máy điện thoại di động thông qua các công nghệ truyền dữ liệu GPRS/EDGE/3G/4G của mạng MobiFone. Khách hàng có thể truy cập Internet trực tiếp từ máy điện thoại di động thông qua các công nghệ truyền dữ liệu GPRS/EDGE/3G/4G của mạng MobiFone.

Okara data

Okara data là dịch vụ cho phép khách hàng xem, thu âm hoặc ghi hình theo các giai điệu bài hát ưa thích trên ứng dụng Okara Mobile mọi lúc, mọi nơi.

Với số lượng khách hàng đông đảo và dịch vụ đa dạng hệ thống thanh toán điện tử tại MobiFone luôn đóng vai trò quan trọng. Tại MobiFone, hệ thống thanh toán điện tử thường được gọi tên là thanh toán trực tuyến.

Các khách hàng của MobiFone được phân thành hai nhóm là thuê bao trả trước và thuê bao trả sau. Thuê bao trả trước là thuê bao phải có sẵn tiền trong tài

khoản thì mới được sử dụng dịch vụ và bị trừ cước phí tức thời. Thuê bao trả sau sẽ thanh toán cước phí dịch vụ định kỳ trong tháng hoặc tuần.

Các hình thức thanh toán trực tuyến tại MobiFone

Thanh toán bằng thẻ cào

Thanh toán bằng thẻ cào là cách thanh toán cước MobiFone khá thông dụng hiện nay.

Thanh toán và nạp tiền tự động AutoPay

Thanh toán và nạp tiền tự động là một dịch vụ cung cấp cho các thuê bao MobiFone tiện ích tự động thanh toán cước định kỳ cho thuê bao trả sau và nạp tiền cho thuê bao trả trước được khách hàng sử dụng thẻ/tài khoản ngân hàng đăng ký dịch vụ trên trang web Portal của MobiFone và ứng dụng My MobiFone.

M2U

M2U là dịch vụ giúp thuê bao trả trước của MobiFone (thuê bao A) có thể chuyển tiền trong tài khoản chính của mình sang tài khoản chính của một thuê bao trả trước cùng mạng (thuê bao B). Thuê bao trả trước của MobiFone có thể chuyển tiền trong tài khoản chính cho nhau.

Fast Credit

Fast Credit là dịch vụ ứng cho thuê bao trả trước của MobiFone một số tiền nhất định khi tài khoản chính của thuê bao không còn nhiều tiền (từ 5,000 đồng trở xuống) nhưng vẫn còn thời hạn sử dụng (chưa bị khóa 1 chiều).

Pay for me (P4M)

Pay for me (P4M) là dịch vụ giúp thuê bao nhận cuộc gọi hoặc nhận tin nhắn (Thuê bao B) có thể trả tiền cước phát sinh cho thuê bao gọi/ gửi tin nhắn (thuê bao A).

FastPay

FastPay là dịch vụ thanh toán dành cho mọi thuê bao trả sau đang hoạt động 2 chiều trên hệ thống.

Ngoài ra, MobiFone cũng kết hợp với các đơn vị khác cung cấp các hình thức thanh toán điện tử khác như ví điện tử.

Do có nhiều hình thức thanh toán trực tuyến như trên nên vấn đề bảo mật hệ thống Thanh toán điện tử của Tổng công ty Viễn thông MobiFone có một ý nghĩa hết sức quan trọng. Điều đó đảm bảo cho khách hàng thực hiện các giao dịch thanh toán điện tử một cách thuận tiện và an toàn.

Trong các mục tiếp theo, luận văn sẽ đề xuất các giải pháp bảo mật phù hợp cho hệ thống thanh toán điện tử của 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.

Các thuật toán mã hóa được lựa chọn phải đáp ứng yêu cầu đảm bảo tính bí mật và khả năng xử lý của hệ thống. Thuận toán mã hóa đang sử dụng phải được định kỳ mỗi năm một lần kiểm tra, đánh giá lại mức độ an toàn và xử lý kịp thời những yếu điểm nếu có. Không để một cá nhân thực hiện toàn bộ quá trình tạo khóa mã hóa. Các khóa mã hóa phải được khởi tạo, thay đổi, phân phối, lưu trữ một cách an toàn. Có những quy định chặt chẽ về việc thu hồi các khóa mã hóa, bao gồm cả việc hủy khóa và phục hồi khóa.

Mặt khác, hệ thống phải quản lý nhật ký khách hàng và của bộ phận quản lý với các thông tin:

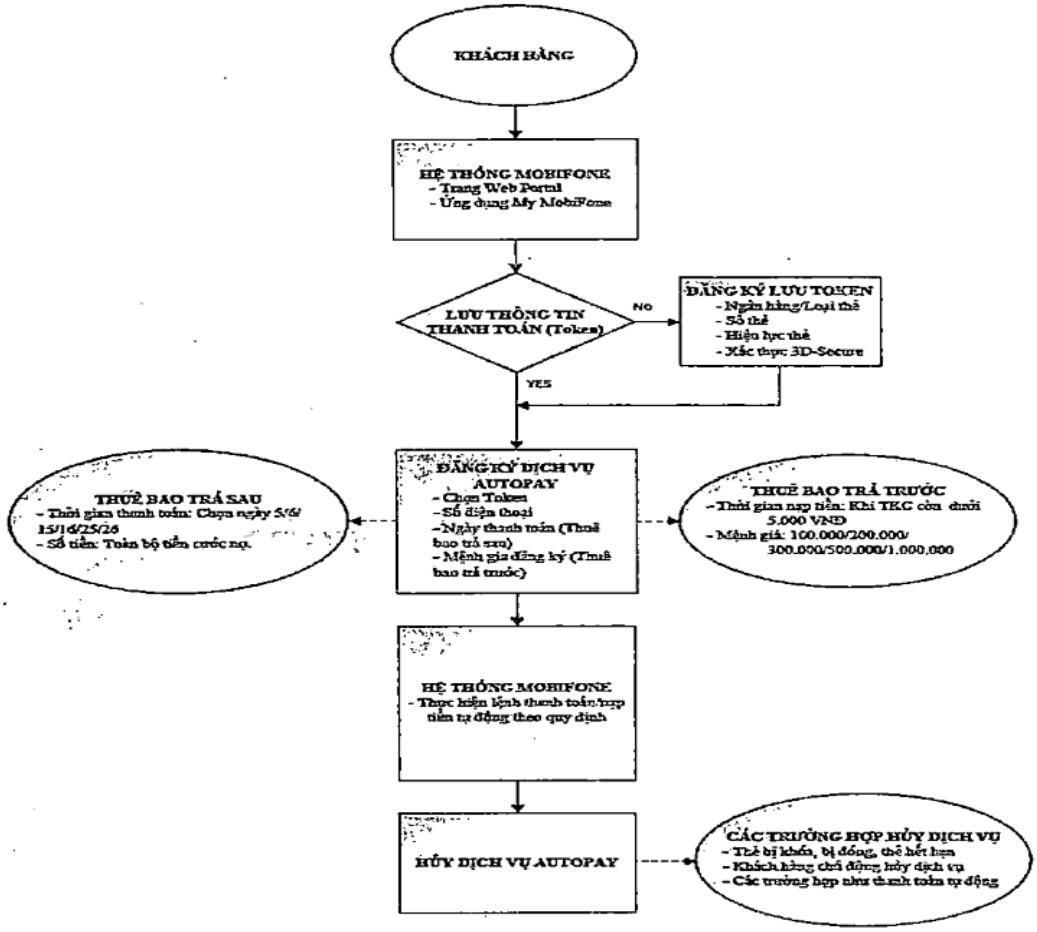
- Quá trình truy cập hệ thống.
- Các thao tác cấu hình hệ thống.
- Các sự kiện xác thực.
- Các sự kiện cấp, thu hồi quyền truy cập hệ thống và sử dụng dịch vụ.

- Xử lý giao dịch.

- Các truy cập bất thường.

Nhật ký giao dịch của khách hàng và giám sát các giao dịch tài chính trên hệ thống và nhật ký của hệ thống phải được lưu trữ, bảo vệ an toàn và truy xuất được khi cần thiết. Thời gian lưu nhật ký tối thiểu là 03 năm.Kiểm tra nhật ký truy cập để phát hiện, phòng ngừa những truy cập bất thường, bất hợp pháp tối thiểu mỗi tháng một lần.

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

Đồng thời, cần có hướng dẫn cho khách hàng các nội dung tự bảo đảm an toàn trong quá trình sử dụng dịch vụ:

- Cách đặt mật khẩu và bảo vệ mật khẩu.

- Không chia sẻ các thiết bị lưu trữ mật khẩu, chữ ký số.

- Không đặt tùy chọn của trình duyệt web cho phép lưu lại tên và mật khẩu người dùng.

- Thoát khỏi hệ thống khi không sử dụng.

- Thận trọng, hạn chế dùng máy tính công cộng, mạng không dây công cộng để truy cập vào hệ thống thanh toán điện tử.

- Cảnh báo các rủi ro khác.

3.2.2 Giải pháp sử dụng SSL

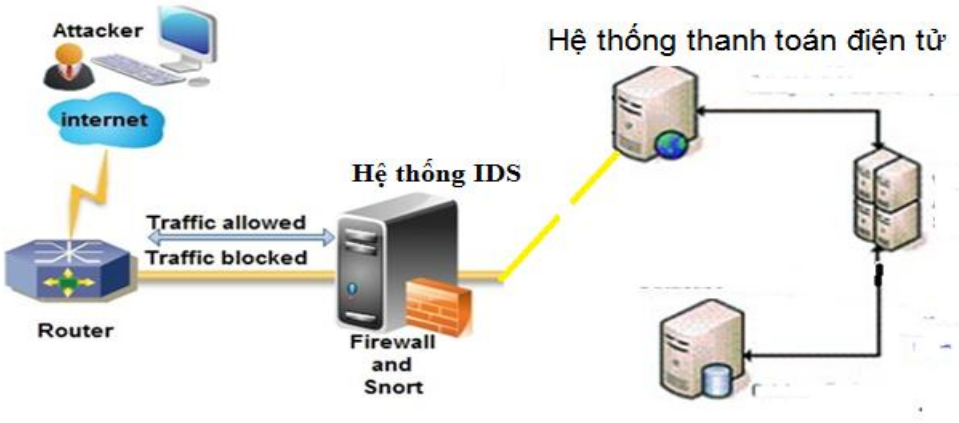
Trong hệ thống thanh toán trực tuyến của Tổng công ty MobiFone có sử dụng hệ thống web và cổng thông tin điện tử như MobiFone Portal, My MobiFone. Các hệ thống web cần phải được cài đặt sử dụng SSL/TSL.

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.

Luận văn đã nghiên cứu, thiết kế, xây dựng các API để phục vụ trong việc triển khai Tokenization trên hệ thống Thanh toán điện tử của MobIFone

Để đáp ứng bao gồm:

- Tính mới: triển khai một API hoàn toàn mới với Cổng thanh toán Napas, thay vì khách hàng trừ thẻ trên trang của Napas, thì MobiFone nhận ủy thác của khách hàng để thanh toán/nạp tiền tự động cho thuê bao. Khi đã có sẵn API này, MobiFone có thể nhanh chóng mở ra nhiều dịch vụ ủy nhiệm thanh toán khác như mua dịch vụ VAS định kỳ, mua gói cước định kỳ, trả góp mua máy đầu cuối, thiết bị truyền hình…

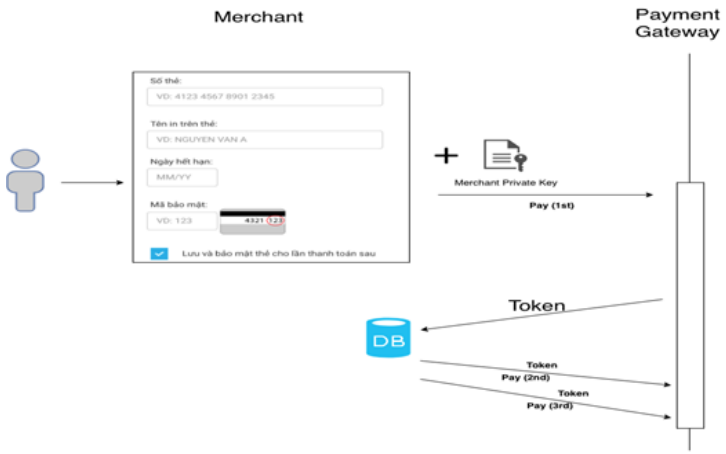
- Hệ thống Thanh toán điện tử xây dựng và cung cấp API cho hệ thống MobiFone Portal và My MobiFone để khách hàng tạo Token lần đầu khi đăng ký dịch vụ .

- Hệ thống Thanh toán điện tử cung cấp API cho hệ thống Payment Gateway để định kỳ thực hiện trừ thẻ Ngân hàng theo thông tin khách hàng đăng ký dịch vụ .

- Xây dựng cơ chế QueryDR cho giao dịch trừ thẻ không thành công khi gọi sang Cổng thanh toán.

- Đồng bộ dữ liệu thanh toán/nạp tiền từ hệ thống Payment Gateway để cung cấp dữ liệu cho các báo cáo đối soát về giao dịch .

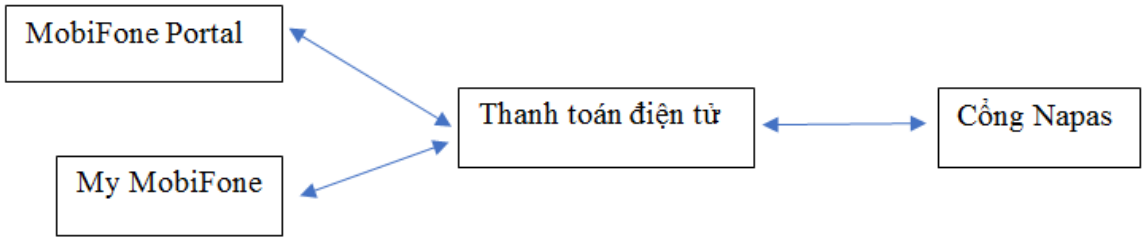
Hình 3.3 mô tả quá trình tạo ra và hoạt động của Tokenization.



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:
  - 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 .

- 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	kzB8qRmirZsGKehR4O6Mf//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 nghiêm, 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.

- Luận văn đã cài đặt thành công SSL trên hệ thống Thanh toán điện tử của MobiFone.

3.4 Kết chương 3

Chương 3 của 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 thanh toán thẻ tín dụng quốc tế trong hệ thống thanh toán điện tử của Tổng công ty Viễn thông MobiFone.

Luận văn đã thử nghiệm cài đặt SSL cho các hệ thống web trong hệ thống thanh toán điện tử của Tổng công ty Viễn thông MobiFone.

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.

- Do thuận tiện và bảo mật cao nên khách hàng đã tin tưởng sử dụng dịch vụ và đạt được kết quả với hơn 200.000 khách hàng đang sử dụng Tokenization để thanh toán cước thuê bao hàng tháng, mang lại hàng tỷ doanh thu cho 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.

DANH MỤC TÀI LIỆU THAM KHẢO

Tiếng Việt

[1] Đào Mỹ Hằng. Nguyễn Thị Thảo, Đặng Thu Hoài, Nguyễn Thị Lệ Thu (2018), "Các nhân tố tác động đến quyết định sử dụng dịch vụ Fintech trong hoạt động của khách hàng cá nhân tại Việt Nam", Tạp chí Khoa học & Đào tạo Ngân hàng, Số 194, T. 11-19.

[2] Thông tư số 29/2011/TT- NHNN (2011), "Quy định về an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet".

Tiếng Anh

[3] Fourcan Karim Mazumder,Israt Jahan (2015), Utpal Kanti Das, "Security in Electronic Payment Transaction".

[4] Jan L. Camenisch, Jean-Marc Piveteau (2000), Markus A. Stadler, "Security in Electronic Payment Systems".

[5] Siamak Solat (2017), "Security of Electronic Payment Systems: A Comprehensive Survey".

[6] Alzomai, Mohammed, Audun and Josang (2010),"The Mobile Phone as a Multi OTP Device Using Trusted Computing".

[7] Kjell Jorgen Hole, Lars Hopland Nestas, and Havard Raddum (2010), "Security Analysis of Mobile Phones Used as OTP Generators".

[8] M. Gusev, L. Antovski, G. Armenski (2017), "Models of Mobile Payment".

[9] Online Based Authenticationand Secure PaymentMethodsfor M-Commerce Applications (2011).

[10] Ali A. Ghorbani, Wei Lu and Mahbod Tavallaee (2010) – "Network Intrusion Detection and Prevention: Concepts and Techniques", Springer Publishing, Canada..

[11] Network Security with OpenSSL. O'Reilly & Associates (2002) , Inc

Trang Web

[12] https://medium.com/coreledger/what-is-tokenization-everything-you-should-know

[13] https://squareup.com/us/en/townsquare/what-does-tokenization-actually-mean

[14] http://vncert.gov.vn

[15] https://vi.wikipedia.org/wiki

[16] https://www.mobifone.vn/