ĐỀ XUẤT NÂNG CẤP CHO CHƯƠNG TRÌNH BẢO MẬT 3D SECURE

Đỗ Hoàng Việt, Nguyễn Chí Thành, Nguyễn Thanh Phong, Trần Thái Bảo, Võ Thanh Toàn

Trường Đại học Kinh tế - Tài chính TP.HCM

Tóm tắt: *Chương trình bảo mật thương mại điện tử gần đây là một chủ đề mới nổi do sự gia tăng của gian lận thẻ tín dụng và đánh cắp thông tin tài khoản người dùng. Nhìn chung, thông tin người dùng bị đánh cắp xảy ra ở các công ty thương mại điện tử do nhiều yếu tố khác nhau, chẳng hạn như sai sót trong thiết kế hệ thống lưu trữ thông tin hay các chương trình bảo mật hiện tại không đạt tiêu chuẩn dẫn đến các công ty thương mại điện tử buộc phải đầu tư chi phí tốn kém cho hệ thống bảo mật. Chính vì vậy, các chương trình bảo mật buộc phải không ngừng phát triển mạnh mẽ để đạt được kết quả tốt nhất cho các công ty thương mại điện tử cũng như người dùng. Trong nghiên cứu này, chúng tôi đề xuất nâng cấp một chương trình bảo mật đã có sẵn (3D Secure) dựa trên kết quả nghiên cứu của chương trình thương mại điện tử an toàn (SES) nhằm mục đích: loại bỏ các chi phí không cần thiết, cải thiện tính năng và an toàn bảo mật thông tin người dùng. Đề xuất nâng cấp này được phân tích và so sánh với chương trình bảo mật 3D Secure hiện tại.*

Từ khoá: *Chương trình bảo mật 3D Secure, đề xuất nâng cấp*

1. Giới thiệu

Ngày nay, với sự phát triển không ngừng của công nghệ, chúng ta đang sống trong một giai đoạn hầu hết cuộc sống của mỗi cá nhân đều phụ thuộc vào các giao dịch trực tuyến như mua sắm, thanh toán hoá đơn… Sự phụ thuộc thuộc ngày càng nhiều vào Internet tạo ra những cơ hội cho các tội phạm mạng. Đặc biệt, sự gia gian lận thẻ tín dụng và đánh cắp thông tin tài khoản người dùng là mối lo ngại đáng kể và luôn được quan tâm trong cộng đồng bảo mật thông tin trong hệ thống thương mại điện tử. Chính vì vậy các chương trình bảo mật thương mại điện tử lần lượt được ra đời nhằm mục đích đảm bảo an toàn, bảo vệ thông tin người dùng trong môi trường trực tuyến.

2. Nội dung

2.1.Tổng quan nghiên cứu

Sự gian lận thẻ tín dụng và đánh cắp thông tin tài khoản người dùng là những vấn đề quan trọng trong lĩnh vực an ninh thông tin vào giao dịch trực tuyến. Trong thời đại số hoá ngày nay, việc sử dụng thẻ tín dụng và chia sẻ thông tin cá nhân trực tuyến đã trở thành một phần không thể thiếu trong cuộc sống hằng ngày. Tuy nhiên, cùng với sự tiện lợi và phát triển của công nghệ, cũng làm tăng lên những nguy cơ về an ninh và xâm phạm quyền riêng tư. Theo các nhà nghiên cứu tại Aite Group và Arxan Technologies đã phát hiện ra hơn 80 trang web thuộc lĩnh vực công nghệ ô tô và thời trang cao cấp có trụ sở tại Hoa kì, Canada, Châu Âu và Châu Á bị tấn công Magecart, các cuộc tấn công này nhằm mục đích đánh cắp chi tiết thông tin thẻ thanh toán của người dùng [1]. Vấn đề nan giải nhất là lưu trữ thông tin người dùng dưới bất kỳ cơ sở dữ liệu nào ngay cả khi đã được mã hoá cũng không loại bỏ được mối lo ngại về bảo mật vì phần lớn thủ phạm là người bên trong. Chẳng hạn như vào năm 2016, Alibaba, một trang web mua sắm trực tuyến nổi tiếng đã bị xâm nhập và 20 triệu tài khoản người dùng đã bị đánh cắp. Theo các báo cáo, thủ phạm đã sử dụng các tài

khoản bị tấn công để đặt hàng giả trên Taobao nhằm tăng xếp hạng người bán [2].

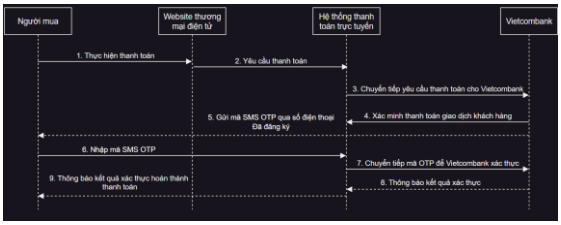
Tại Việt Nam, theo ông Nguyễn Đặng Hùng, phó tổng giám đốc công ty cổ phần Thanh toán Quốc gia Việt Nam (Napas), thẻ nội địa Việt Nam có sự phát triển vượt bậc trong 5 năm trở lại đây, tốc độ tăng trưởng của số lượng giao dịch chi tiêu qua thẻ đạt 45% và giá trị giao dịch đạt 40%. Nếu xét trực tuyến, con số này là 87% về số lượng giao dịch và 107% về giá trị giao dịch. Điều này cho thấy ngoài việc rút tiền tại ATM, người dân đã biết sử dụng thẻ nội địa để chi tiêu. Chính vì vậy mà các cuộc gian lận thẻ tín dụng và đánh cắp thông tin tài khoản người dùng ngày càng gia tăng [3]. Do đó, các công ty thương mại điện tử đã thêm vào hệ thống lưu trữ thông tin các chương trình bảo mật tiên tiến hiện nay và phát triển một số công cụ giúp việc mua sắm trực tuyến trở nên an toàn nhất có thể. Ví dụ, vào năm 2018, ngân hàng Thương Mại Cổ Phần Ngoại thương Việt Nam (Vietcombank) đã triển khai chương trình bảo mật 3D Secure – giải pháp bảo mật tiên tiến nhất hiện nay nhằm đảm bảo cho các giao dịch mua hàng trực tiếp bằng thẻ được an toàn hơn thông qua việc định danh khách hàng chính xác tại thời điểm thực hiện giao dịch. Mặc dù các chương trình bảo mật tiên tiến đã được thêm vào hệ thống lưu trữ thông tin nhưng chỉ giảm một phần đáng kể mối lo ngại từ phía người dùng và các công ty thương mại điện tử. Một số mối lo ngại mới được hình thành chẳng hạn như chi phí đầu tư, vận hành hệ thống vẫn còn cao hay một số tính năng bảo mật gây khó chịu cho người dùng. Chính vì mối lo ngại đó mà một nhóm nghiên cứu (Sena Efsun Cebeci, Kubra Nari & Enver Ozdemir, 2021) đã nghiên cứu ra chương trình thương mại điện tử an toàn (SES) dựa trên thuật toán khoá bất đối xứng với mục tiêu nhằm cung cấp một giao thức thương mại điện tử an toàn, bảo vệ quyền riêng tư của người dùng, giảm chi phí bảo mật hệ thống lưu trữ và loại bỏ sự cần thiết phải nhập lại thông tin người dùng trong mỗi giao dịch [4]. Mặc dù chương trình thương mại điện tử (SES) đã đưa ra được những ưu điểm vượt trội hơn so với hai chương trình bảo mật nổi tiếng hiện tại là giao dịch điện tử an toàn (SET) và 3D Secure, nhưng đó chỉ là giả thuyết và chưa được đưa vào thực tế. Tuy nhiên, cũng không thể phủ định những mục tiêu mà chương trình thương mại điện tử (SES) đã đưa ra là hợp lý.

Chính vì vậy, mục đích của chúng tôi trong nghiên cứu này là dựa vào những mục tiêu mà nhóm nghiên cứu chương trình thương mại điện tử (SES) đã đưa ra để cải thiện và nâng cấp chương trình bảo mật đã có sẵn (3D Secure).

2.2.Cơ sở nghiên cứu

Mặc dù có rất nhiều chương trình bảo mật tốt được sử dụng trong lĩnh vực thương mại điện tử như: SSL/TLS, 3D Secure, Tokenization, MFA…, nhưng không có chương trình bảo mật nào là tuyệt đối hoàn hảo và không thể bị xâm phạm. Việc áp dụng các biện pháp bảo mật phù hợp cùng với việc cập nhật và tuân thủ các quy định bảo mật là quan trọng để đảm bảo an toàn trong thương mại điện tử. Tại Việt Nam, hiện nay hầu hết chương trình bảo mật 3D Secure được đăng ký mặc định và sử dụng miễn phí cho tất cả các chủ thẻ quốc tế khi phát hành thẻ tại ngân hàng. Các ngân hàng cung cấp dịch vụ 3D Secure gồm có: Vietcombank, Vietinbank, ACB, Sacombank, VP bank… Dịch vụ này sẽ được kích hoạt sau khi người dùng được ngân hàng xác nhận đã đăng ký thành công [5]. Chương trình bảo mật 3D Secure, trong tiếng anh còn được gọi là “Verified by Visa”, “MasterCard SecureCode” hoặc “American Express SafeKey” đã được phát triển bởi các tổ chức với từng hãng thẻ tín dụng nhằm mục đích tăng cường các biện pháp bảo mật cho người mua sắm và nhà

cung cấp. Sau khi điền đầy đủ thông tin cần thiết, một mã OTP sẽ được gửi đến số điện thoại di động của người dùng. Trong trường hợp giao dịch xác thực, chủ sở hữu sẽ nhập OTP vào trang web của người bán để xác nhận mua hàng. Nếu không, giao dịch sẽ được coi là thất bại và ngừng giao dịch. Ngoài những ưu điểm mà chương trình 3D Secure mang lại như tăng cường bảo mật, tăng cảm giác tin tưởng cho người dùng, giảm rủi ro cho ngân hàng và người bán thì còn có các nhược điểm gây ra một số bất tiện cho người dùng như cần phải nhập thông tin xác thực hoặc mã xác nhận trong quá trình thanh toán. Theo các chuyên gia ChronoPay (2019) đã cảnh báo về khả năng giả mạo dữ liệu người nhận đối với một số giao dịch thanh toán trực tuyến bằng thẻ ngân hàng do có lỗ hổng trong yêu cầu xác thực thanh toán, kẻ thanh toán có thể đánh lừa người tiêu dùng bằng cách thay đổi dữ liệu của người nhận thanh toán trên trang xác nhận giao dịch [6]. Chính vì vậy, chúng tôi quyết định lựa chọn chương trình bảo mật 3D Secure của Vietcombank cho đề xuất nâng cấp lần này. Dưới đây là mô hình quy trình hoạt động chương trình bảo mật 3D Secure của Vietcombank (Hình 1).



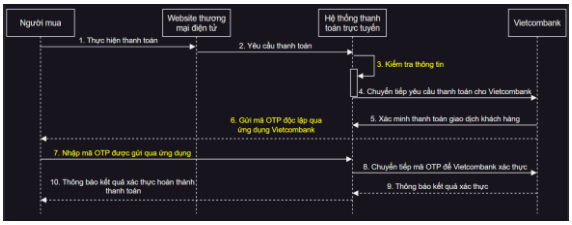
Hình 1: *Mô hình quy trình hoạt động của Vietcombank*

2.3.Đề xuất nâng cấp mô hình quy trình hoạt động đã có sẵn

Mục đích của chúng tôi là loại bỏ các chi phí không cần thiết, cải thiện tính năng và an toàn bảo mật của người dùng dựa vào kết quả của nhóm nghiên cứu chương trình bảo mật thương mại (SES). Trong chương trình bảo mật 3D Secure hiện tại, giao thức được sử dụng khi chấp nhận thanh toán bằng thẻ ngân hàng trực tuyến. Để xác nhận các thanh toán được thực hiện bởi chủ tài khoản, người dùng cũng cần có mã xác nhân đến số điện thoại di động được liên kết với thẻ qua số điện thoại (SMS). Do đó, người dùng phải nhập mã xác nhận vào một trang riêng và kẻ lừa đảo có thể giảo mạo thông tin người nhận. Như vậy, chương trình bảo mật 3D Secure hiện tại được thiết kế bảo vệ thông tin tài khoản người dùng chống lại hành vi đánh cắp dữ liệu nhưng không có khả năng chống gian lận trực tuyến từ chính người nhận thanh toán. Chính vì vậy, chúng tôi đề xuất nâng cấp chương trình bảo mật 3D Secure hiện tại của Vietcombank được thể hiện ở Hình 2.

Trong mô hình này, chúng tôi thay đổi quy trình "Gửi mã SMS OTP điện thoại đã đăng ký" bằng một quy trình mới hơn đó là "Gửi mã OTP độc lập qua ứng dụng Vietcombank". Quy trình mới này nhằm mục đích loại bỏ chi phí liên quan đến dịch vụ viễn thông, chẳng hạn như chi phí tin nhắn gửi mã OTP về số điện thoại người dùng. Đồng thời, chúng tôi cũng thay đổi quy trình "Nhập mã SMS OTP" bằng quy trình "Nhập mã OTP được gửi qua ứng dụng". Mục đích của chúng tôi trong quy trình này là giúp người dùng cảm thấy thân thiện trong quá trình thực hiện thanh toán. Chẳng hạn, trong quá trình xác thực 3D Secure có thể làm chậm quá trình thanh toán và gây khó chịu cho người dùng. Việc phải nhập thông tin bổ sung và xác minh qua một cửa sổ mới làm gián đoạn trải nghiệm mua hàng trực tuyến của người dùng. Ngoài ra, chúng tôi còn bổ sung thêm quy trình "Kiểm tra thông tin" nhằm tăng cường bảo mật cũng như mức độ tin cậy trong quá trình người dùng thực hiện mua sắm và thanh toán trực tuyến qua các trang thương mại điện tử. Bởi vì theo nhận định của các chuyên gia ChronoPay

(2019), trong chương trình bảo mật Secure hiện tại, các yêu cầu xác thực thanh toán từ người dùng được gửi đến ngân hàng không được mã hoá bằng mật mã và không được kiểm tra bởi hệ thống thanh toán. Chính vì lỗ hổng đó, các kẻ giả mạo có thể dễ dàng thay thế bất kỳ dữ liệu nào trong dòng yêu cầu và đánh lừa người trên trang xác nhận thanh toán [6].



Hình 2: *Mô hình quy trình hoạt động của Vietcombank sau khi nâng cấp*

2.4.Phương pháp nghiên cứu

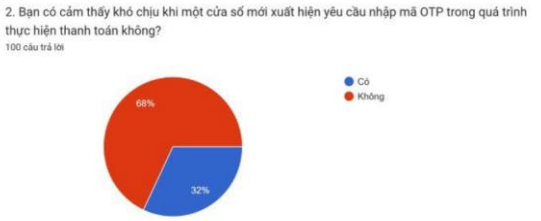
Trong đề xuất nâng cấp lần này, chúng tôi sử dụng hai phương pháp nghiên cứu đó là phương pháp nghiên cứu tài liệu và phương pháp nghiên cứu định lượng.

Chúng tôi sử dụng phương pháp nghiên cứu tài liệu nhằm mục đích thu thập các thông tin liên quan đến đề xuất nâng cấp mà chúng tôi đưa ra dựa trên kết quả nghiên cứu của chương trình thương mại điện tử (SES) cũng như mô hình quy trình hoạt động chương trình bảo mật 3D Secure hiện tại của Vietcombank. Từ đó chúng tôi phân tích và sử dụng phần StarUML để xây dựng mô hình quy trình hoạt động mới dựa trên mô hình quy trình hoạt động đã có sẵn là chương trình bảo mật 3D Secure của Vietcombank.

Đối với phương pháp nghiên cứu định lượng, chúng tôi tiến hành khảo sát trực tuyến thông qua công cụ Google Form. Các đối tượng nghiên cứu mà chúng tôi hướng đến là những người đã sử dụng giao thức 3D Secure một hoặc nhiều lần trong giao dịch thanh toán trực tuyến. Đối tượng sẽ trả lời các câu hỏi liên quan đến mức độ hài lòng cũng như vấn đề bảo mật trong quá trình thanh toán trực tuyến.

2.5.Phân tích kết quả

Theo kết quả khảo sát mà chúng tôi đã thu thập từ 100 đối tượng nghiên cứu cho rằng, "họ cảm thấy khó chịu khi một cửa sổ mới xuất hiện yêu cầu nhập mã OTP trong quá trình thực hiện thanh toán" và chiếm tỷ lệ 68%. Điều đó, chúng tôi nhận định rằng chương trình bảo mật 3D Secure hiện tại vẫn chưa mang lại mức độ thân thiện cao dành cho người dùng. Đối với câu hỏi "Đề xuất mã OTP sẽ được gửi trực tiếp thông qua ứng dụng thay vì bằng phương thức gửi tin nhắn (SMS) tới số điện thoại của người dùng" thì có tới 85% đối tượng nghiên cứu chấp nhận đề xuất này. Chính vì vậy, đây là cơ sở giúp chúng tôi có thể xác định được mục tiêu nghiên cứu trong việc đưa ra đề xuất nâng cấp cũng như thay đổi quy trình dựa vào mô hình quy trình hoạt động trong chương trình bảo mật 3D Secure hiện tại của Vietcombank.



Hình 3: *Kết quả khảo sát từ 100 đối tượng nghiên cứu*

3. Kết luận

Trong nghiên cứu lần này, chúng tôi đề xuất nâng cấp chương trình bảo mật 3D Secure hiện tại nhằm mục đích loại bỏ các chi phí không cần thiết, cải thiện tính năng và an toàn bảo mật thông tin người dùng. Mặc dù đây chỉ là giải pháp được đưa ra dựa trên kết quả nghiên cứu của chương

trình bảo mật điện tử SES nhưng trong đó chúng tôi đã phân tích, thu thập, chọn lọc dữ liệu và xác định được mong muốn của người dùng trong quá trình thực hiện giao dịch thanh toán điện tử cũng như mức độ bảo mật an toàn sẽ cao hơn. Chính vì vậy, chúng tôi hi vọng đề xuất trong bài nghiên cứu này sẽ được các nhà bảo mật trong hệ thống thương mại điện tử quan tâm cũng như xem xét mô hình của chúng tôi.

Tài liệu tham khảo

[1] N. Dang, Tin tặc Magecart tấn công hơn 80 website thương mại điện tử, đánh cắp thẻ tín dụng, cystack, 2023.

[2] A. Kharpal, Alibaba denies blame for 20 million hack attempt, FRI, 2016.

[3] Đ. Hưng, Thẻ tín dụng nội địa đang nỗ lực chiếm thị phần, VnEconomy, 2022.

[4] K. N. E. O. Sena Efsun Cebeci, Secure E-Commerce Scheme, IEEE Access, 2022.

[5] D. Ngọc, Bảo mật thẻ thanh toán: Hiệp hội Ngân hàng Việt Nam nói gì?, diendandoanhnghiep, 2021.

[6] TADVISER, 3-D Secure, tadviser, 2023.

[7] CAND, Tin tặc đánh cắp thông tin thẻ tín dụng của hàng triệu người dân Mỹ, CAND, 2018.

[8] vietnamnet, Ngân hàng cảnh báo khách hàng cẩn thận khi quẹt thẻ thanh toán tại quầy, vietnamnet, 2022.