

Xác định các tiêu chí đánh giá an toàn thông tin cho các website theo tiêu chuẩn ISO/IEC 15408

Vũ Thị Hương Giang, Nguyễn Mạnh Tuấn, Đặng Bá Tú, Lê Hồng Dương

Tóm tắt— Trong quá trình thiết kế và sử dụng website, người quản trị cũng như chủ sở hữu website luôn có nhu cầu xác định các thành phần cấu thành và vận hành website có được áp dụng các biện pháp và kỹ thuật an toàn phù hợp hay không, với mức độ an toàn như thế nào (mức đảm bảo đánh giá). Bài báo giới thiệu một giải pháp xác định các tiêu chí đánh giá an toàn thông tin cho website đáp ứng các nhu cầu trên. Bên cạnh đó, bài báo cũng đề xuất mô hình kết nối các tiêu chí đánh giá an toàn thông tin theo ISO/IEC 15408, các yêu cầu an toàn thông tin theo hồ sơ bảo vệ của các thành phần cấu thành và vận hành cho một hệ thống website. Trên mô hình các tiêu chí đã kết nối, bài báo xây dựng cơ chế tạo lập các bản khảo sát dành cho người phát triển, người vận hành, người đánh giá, cung cấp thông tin đầu vào cho việc đánh giá ban đầu khả năng đáp ứng với một mức đảm bảo đánh giá xác định. Các mô hình và cơ chế nói trên được thử nghiệm dưới dạng công cụ có khả năng tùy biến, hỗ trợ xác định tập các tiêu chí đánh giá an toàn thông tin phù hợp với một mức đảm bảo đánh giá cho các hệ thống website; xác định mức đảm bảo đánh giá (Evaluation Assurance Level – EAL) mà một website có thể đạt được.

Abstract— Before and after the website deployment, it needs to determine whether the website components and operations are subject to appropriate security measures and techniques, and how secure they are (assurance levels). This article introduces an approach for identifying the website security assessment criteria. The ISO/IEC 15408-based assessment criteria are put in connection with the security requirements according to the protection profiles of the website's components and operation. Then, a mechanism for creating surveys for developers, operators, and evaluators that provide input to evaluations based on connected criteria is proposed. These are experimented as a customized tool, which supports to identify security

assessment criteria accordingly to a given assurance level of a website; and determine the assurance level (EAL) that a website can achieve.

Từ khóa— đánh giá an toàn; mức đảm bảo đánh giá; hồ sơ bảo vệ; ISO/IEC 15408.

Keywords— security evaluation; EAL; PP; ISO/IEC 15408.

I. TỔNG QUAN

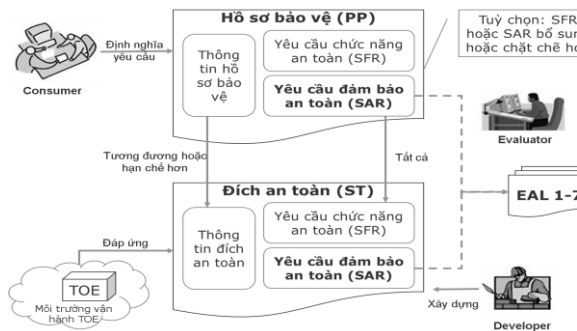
Đánh giá an toàn thông tin của các website là một nhu cầu thực tế, giúp người dùng xác định xem các thành phần cấu thành và vận hành website (thiết bị phần cứng, phần mềm) có đủ an toàn và tin cậy khi đưa vào sử dụng hay không. Việc đánh giá mức độ an toàn không chỉ giúp người quản lý nắm được khả năng bảo mật của hệ thống mà còn giúp các doanh nghiệp trong việc phát triển các sản phẩm và hệ thống công nghệ thông tin (CNTT) đảm bảo các yêu cầu về an toàn thông tin (ATTT).

ISO/IEC 15408 [1-3] là một tiêu chuẩn quốc tế để đánh giá và chứng nhận cấp độ an toàn cho các hệ thống thông tin (sau đây được gọi tắt là ISO 15408). Theo tiêu chuẩn này mỗi sản phẩm, thiết bị hoặc hệ thống CNTT cần được đánh giá gọi là một đích đánh giá (Target of Evaluation – TOE). Chúng có các yêu cầu về ATTT được mô tả trong hồ sơ bảo vệ (Protection Profile – PP), tương ứng với một EAL nào đó. EAL sẽ chỉ ra một sản phẩm công nghệ thông tin được kiểm thử kỹ đến mức nào. Đánh giá EAL gồm 7 mức từ thấp đến cao. Hình 1 mô tả các thành phần trong ISO 15408.

Lưu ý rằng, các tiêu chí trong ISO 15408 và 7 mức của EAL là những đánh giá tổng quát chung cho các thiết bị và hệ thống CNTT, chưa có sự gắn kết với nghiệp vụ và ngữ cảnh triển khai cụ thể. Việc áp dụng các tiêu chí này để đánh giá một loại sản phẩm cụ thể như website vẫn còn rất hạn chế. Bên cạnh đó, việc xác định mức độ đảm bảo không sử dụng tất cả các tiêu chí mà ISO/IEC

Bài báo được nhận ngày 29/01/2018 Bài báo được nhận xét bởi phản biện thứ nhất vào ngày 31/01/2018 và được chấp nhận đăng vào ngày 19/03/2018. Bài báo được nhận xét bởi phản biện thứ hai vào ngày 31/01/2018 và được chấp nhận đăng vào ngày 09/04/2018.

15408 đề xuất, nên người đánh giá cần tham khảo lượng lớn các tài liệu liên quan trước khi thực hiện đánh giá. Hiện tại, chưa có một công cụ tự động nào hỗ trợ người đánh giá trong việc xác định cấp độ đảm bảo, phần lớn các thao tác phải thực hiện thủ công. Với một hệ thống tiêu chí cần xem xét từ các nguồn tài liệu đa dạng, các hoạt động trong quá trình đánh giá, nhiều kết quả đánh giá trung gian, việc xác định mức đảm bảo là một quá trình phức tạp, khó khăn, rất tốn kém thời gian và công sức.



Hình 1. Các thành phần trong ISO/IEC 15408

Để xác định mức đảm bảo đánh giá cho một sản phẩm, nhà cung cấp cần xây dựng mô tả đích an toàn (Security Target - ST) gồm các thông tin về sản phẩm và những tính năng bảo mật của sản phẩm, đánh giá về những rủi ro bảo mật mà sản phẩm có thể gặp phải, tự đánh giá chi tiết sản phẩm có thỏa mãn với PP liên quan hay không, ứng với EAL mà nhà cung cấp sẽ chọn để kiểm tra sản phẩm.

PP đưa ra một tập các yêu cầu ATTT cho một loại đích đánh giá ví dụ như tường lửa, trình duyệt,... Một PP có thể sử dụng như một bản mẫu cho nhiều ST để sử dụng cho các phép đánh giá khác nhau. Nếu như một ST mô tả các yêu cầu cho một TOE nhất định và được viết bởi người phát triển của TOE đó thì PP lại đưa ra các yêu cầu chung cho một kiểu TOE. Do đó, PP thường được viết bởi các đối tượng sau: cộng đồng người dùng tìm kiếm sự đồng thuận về các yêu cầu cho một kiểu TOE cho trước; nhà phát triển TOE, nhóm các nhà phát triển TOE tương ứng mong muốn lập ra một mức tối thiểu cho kiểu TOE này; chính phủ, hoặc tập đoàn lớn chỉ rõ các yêu cầu của họ là một phần của quá trình thu thập thông tin. Thông thường, một PP sẽ chỉ ra một tập các tiêu chí đảm bảo cho một loại TOE nhất định gồm các yêu cầu chức năng an toàn (Security Function Requirements - SFR) và các yêu cầu đảm bảo an toàn (Security Assurance Requirements - SAR). Việc đánh giá một sản phẩm hay hệ thống CNTT

theo một mức bảo đảm đánh giá EAL được dựa trên các yêu cầu đảm bảo an toàn. Chính vì vậy, với mục đích xác định các tiêu chí đánh giá ATTT cho các website, chúng tôi sẽ tiến hành tổng hợp các yêu cầu đảm bảo an toàn từ các PP của các thành phần cấu thành và vận hành một website. Trong các hồ sơ bảo vệ cấu thành một website, ngoài các yêu cầu đảm bảo an toàn tuân thủ theo ISO 15408 còn có thêm các yêu cầu bổ sung hoặc chặt chẽ hơn so với các mức được đưa ra trong ISO. Những yêu cầu bổ sung hoặc mở rộng này cũng cần phải được bao gồm trong quá trình xác định các tiêu chí đánh giá phù hợp cho các hệ thống website.

Tại Việt Nam, một số tiêu chuẩn quốc gia (TCVN) về ATTT đã được xây dựng, công bố trên cơ sở chấp nhận nguyên vẹn các tiêu chuẩn ISO/IEC. Cụ thể là sự ra đời của bộ tiêu chuẩn về đánh giá ATTT (TCVN 8709:2011) bao gồm 3 phần: giới thiệu và mô hình tổng quát, các thành phần chức năng an toàn và các thành phần đảm bảo an toàn. Nhằm hỗ trợ việc xác định các tiêu chí đánh giá một cách có hệ thống, [4] đề xuất xây dựng một cơ sở dữ liệu lưu trữ các tiêu chí của tài liệu ISO 15408 và ISO 18045. Tuy nhiên, cơ sở dữ liệu này mới chỉ dừng ở mức độ lưu trữ tập tiêu chí, chưa có đủ liên kết để hỗ trợ xác định EAL tương ứng. Bên cạnh đó, các nhà cung cấp cũng đã chú trọng xây dựng các PP cho các thiết bị phần cứng (Web Server [6], Authorization Server, Server Virtualization [5]) và phần mềm (Web Browser [9], Application Software [8], Web service [7]) cụ thể cho việc cấu thành và vận hành website. Các PP này đều đã được chứng nhận ở cấp quốc gia (như [7]) hay quốc tế ([5,6,8,9]). Các hồ sơ bảo vệ này mới chỉ ra các tiêu chí đảm bảo cho từng thành phần cấu thành và vận hành, chưa có tập các tiêu chí chung áp dụng cho cả hệ thống website cũng như không hướng dẫn việc ánh xạ các tiêu chí này tới các mức độ đảm bảo EAL.

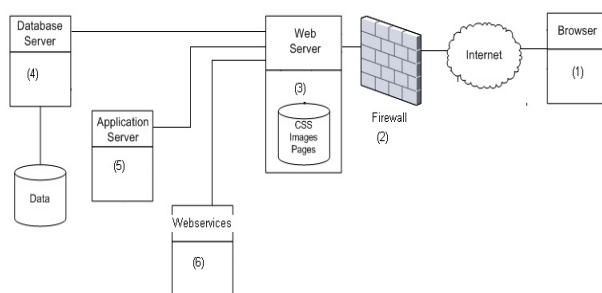
Trong nghiên cứu này chúng tôi phân tích, lựa chọn để xây dựng tập tiêu chí đánh giá an toàn thông tin phù hợp cho các hệ thống website. Đầu tiên, chúng tôi đề xuất mô hình kết nối các tiêu chí sử dụng để đánh giá ATTT cho website theo ISO 15408 dựa trên các yêu cầu đảm bảo an toàn trong hồ sơ bảo vệ của các thành phần cấu thành và vận hành website. Mô hình đề xuất nhận đầu vào là tập các tiêu chí trong ISO 15408 tập trung vào khía cạnh các yêu cầu đảm bảo an toàn của sản phẩm (SAR). Mô hình cho phép người quản lý đánh giá có thể quản lý lưới tiêu chí và khả năng tùy chỉnh phù hợp với đối tượng đánh giá. Đầu

vào thứ hai của mô hình là tập yêu cầu trong các hồ sơ bảo vệ thành phần được xác định phù hợp cho các website. Mô hình kết nối là cơ sở đề xuất cơ chế tạo lập các bản khảo sát dành cho người phát triển, người vận hành, người đánh giá cung cấp thông tin đầu vào cho việc đánh giá. Dựa trên cơ chế này chúng tôi xây dựng bộ công cụ cung cấp các chức năng cho người quản lý đánh giá có thể quản lý lưới tiêu chí được sử dụng, có thể tùy chỉnh (thêm/bớt) các tiêu chí trong hai tập đầu vào là ISO 15408 và các hồ sơ bảo vệ theo yêu cầu của đối tượng đánh giá. Công cụ cho phép người phát triển, người vận hành có thể nhập thông tin về hệ thống đích thuận tiện qua các bản khảo sát, cung cấp thông tin đầu vào cho quá trình đánh giá. Qua công cụ này người đánh giá có thể quản lý nội dung các bản khảo sát, nhận kết quả đánh giá sơ bộ về khả năng đáp ứng thực tế về mức đảm bảo của sản phẩm và cung cấp cho lãnh đạo quản lý.

Bài báo này có cấu trúc như sau: Sau Mục Tổng quan, Mục II giới thiệu mô hình quản lý các tiêu chí đánh giá ATTT cho website theo tiêu chuẩn ISO 15408 và theo hồ sơ bảo vệ. Mục III mô tả kết quả thử nghiệm xây dựng công cụ quản lý lưới tiêu chí được sử dụng và quản lý đánh giá sơ bộ mức đảm bảo cho website. Mục IV tổng hợp các kết quả nghiên cứu chính và đề xuất các phương hướng phát triển tiếp theo.

II. QUẢN LÝ CÁC TIÊU CHÍ ĐÁNH GIÁ AN TOÀN THÔNG TIN CHO WEBSITE

Các thành phần cấu thành một hệ thống website được mô tả trong Hình 2 theo mô hình client/server



Hình 2. Các thành phần cơ bản cấu thành một hệ thống website

Các yêu cầu truy nhập được gửi từ máy khách với phần mềm trình duyệt (Browser (1)). Phía máy chủ nơi đặt hệ thống website được bảo vệ với các thành phần an toàn như tường lửa (Firewall (2)) hoặc các hệ thống phòng chống, ngăn chặn xâm nhập. Nội dung của website được đặt trên một máy chủ web (Web Server (3)). Website

trong quá trình hoạt động có thể tương tác với các hệ thống Back end khác như máy chủ cơ sở dữ liệu (Database Server (4)), các máy chủ ứng dụng (Application Server (5)) và các dịch vụ web (Web Services (6)).

Với mỗi thành phần của hệ thống website có ảnh xạ các PP tương ứng. Trên cơ sở tổng hợp các yêu cầu đảm bảo an toàn của từng thành phần và mục tiêu hỗ trợ xác định mức đảm bảo đánh giá theo ISO 15408, chúng tôi đề xuất một mô hình quản lý các tiêu chí đánh giá.

Mô hình này được xây dựng với 2 nhiệm vụ chính: thứ nhất là kết nối các tiêu chí sử dụng để đánh giá an toàn thông tin cho website theo ISO 15408 và các yêu cầu an toàn thông tin theo hồ sơ bảo vệ của các thành phần cấu thành và vận hành website; thứ hai là tạo lập các bản khảo sát dành cho người phát triển, người vận hành, người đánh giá cung cấp thông tin đầu vào cho việc đánh giá dựa trên các tiêu chí đã kết nối.

Như vậy, mô hình này cần định nghĩa đầy đủ các yêu cầu đảm bảo an toàn phục vụ cho việc đánh giá. Hơn nữa, mô hình cần có khả năng thay đổi để thích nghi với các thành phần cấu thành hoặc vận hành website trong từng bối cảnh cụ thể. Mô hình dữ liệu này cũng cần tương ứng với cấu trúc dữ liệu mô tả trong chuẩn ISO 15408 nhằm đảm bảo các kết nối và tham chiếu. Các thành phần dữ liệu cần được mô hình hóa bao gồm: yêu cầu đảm bảo đánh giá, mức đảm bảo đánh giá, tiêu chí đánh giá đặc thù (Specific Criteria), câu hỏi (Question) và bảng khảo sát (Survey).

A. Yêu cầu đảm bảo đánh giá (Evaluation Assurance Requirement)

Theo ISO 15408, để xác định mức đảm bảo đánh giá của một website, cần xác định PP, ST tương ứng. Như vậy, chỉ cần chú trọng đến việc mô hình hóa các yêu cầu đảm bảo an toàn cho TOE là website.

Khảo sát các yêu cầu đảm bảo và các mức đảm bảo đánh giá, chúng tôi nhận thấy việc xác định mức độ đảm bảo một website không cần đến tất cả các tiêu chí đã được đưa ra trong ISO 15408.

Do vậy, ngoài các thông tin thể hiện yêu cầu đảm bảo an toàn như trong chuẩn (GroupingInfo), chúng tôi bổ sung thêm các thông tin TOEMatchingList, ST MatchingList nhằm xác định sự phù hợp của tiêu chí đánh giá với từng đích đánh giá, đích an toàn cụ thể.

1. GroupingInfo

Phần này bao gồm các thông tin định danh một yêu cầu đảm bảo an toàn theo các quy tắc phân loại của ISO 15408.

- RequirementID: định danh của yêu cầu đảm bảo an toàn
- ClassCode: tên viết tắt của các lớp: Protection Profile Evaluation, Development, Guidance Documents, Life-cycle Support, Security Target Evaluation, Tests và Vulnerability Assessment. Thuộc tính này được sử dụng để định danh các lớp.
- FamilyCode: một trong các họ APE_CCL, APE_ECD, APE_INT, APE_OBJ, APE_REQ, APE_SPD, ADV_ARC, ADV_FSP, ADV_IMP, ADV_INT, ADV_SPM, ADV_TDS, AGD_OPE, AGD_PRE, ALC_CMC, ALC_CMS, ALC_DEL, ALC_DVS, ALC_FLR, ALC_LCD, ALC_TAT, ASE_CCL, ASE_ECD, ASE_INT, ASE_OBJ, ASE_REQ, ASE_SPD, ASE_TSS, ATE_COV, ATE_DPT, ATE_FUN, ATE_IND, AVA_VAN.
- ComponentIdentification: mô tả định danh và tham chiếu đến một trong 78 thành phần bảo đảm an toàn được ISO 15408 đề xuất thuộc các họ đã nêu ở trên.
- ComponentIndex: chỉ số được thiết lập sẵn cho từng thành phần đảm bảo an toàn.
- Các thuộc tính khác như Objectives, Dependencies, ContentAndPresentations, DevActions, EvaluatorActions có tên và vai trò tương ứng với các phần tử được mô tả theo ISO 15408.

2. TOEMatchingList

Đây là danh sách các yêu cầu đảm bảo an toàn theo ISO có khả năng sử dụng như các tiêu chí đánh giá cho từng website cụ thể.

- TOEID: là định danh của các website cần đánh giá.
- Value: có giá trị TRUE khi yêu cầu đảm bảo an toàn được lựa chọn như tiêu chí dùng để đánh giá website, FALSE trong các trường hợp khác.
- ApplicationNote: các thông tin bổ sung trong trường hợp yêu cầu đảm bảo an toàn được lựa chọn.

3. ST MatchingList

Đây là các yêu cầu đảm bảo an toàn theo PP có khả năng sử dụng như các tiêu chí đánh giá cho từng website cụ thể.

- STID: là định danh của ST, tương ứng với định danh của tập PP được lựa chọn.
- Value: có giá trị TRUE khi tiêu chí này được quy hoạch từ hồ sơ bảo vệ với ID tương ứng.
- ApplicationNote: bao gồm các thông tin bổ sung trong trường hợp tiêu chí đánh giá được lựa chọn.

B. Mức đảm bảo đánh giá

Các yêu cầu đảm bảo an toàn nêu trên cho phép xác định mức đảm bảo đánh giá từ 1 đến 7 cho website. Mức cao hơn được xây dựng trên cơ sở mức an toàn thấp hơn kế cận nhưng yêu cầu cao hơn về phạm vi, chiều sâu và độ nghiêm ngặt khi kiểm thử. Do mức đảm bảo đánh giá là khách quan, các thông tin về mức đảm bảo đánh giá sẽ giống như quy định trong ISO 15408. Ngoài ra còn có ảnh xạ các mức đảm bảo đánh giá EAL cho các tiêu chí đặc thù theo PP.

1. GroupingInfo

Phần này bao gồm các thông tin định danh một mức đảm bảo đánh giá theo các quy tắc phân loại của ISO 15408.

- EalName: là tên của mức đảm bảo đánh giá.
- EalLevel: mức đảm bảo đánh giá từ 1 đến 7.
- ApplicationNote: các thông tin bổ sung trong trường hợp lựa chọn 1 EAL cho một TOE cụ thể.
- Objectives: mục đích đảm bảo đánh giá tương ứng với mức đảm bảo đánh giá đã chọn.

2. RequirementMatchingList

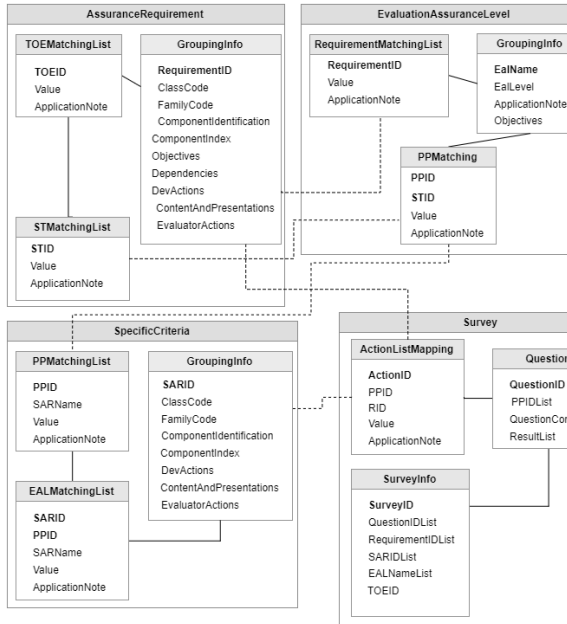
Ảnh xạ EAL đến các yêu cầu đảm bảo đánh giá liên quan.

- RequirementID: yêu cầu đảm bảo an toàn.
- Value: TRUE khi mức đảm bảo đánh giá có thể hiện yêu cầu đảm bảo an toàn với ID tương ứng.
- ApplicationNote: các thông tin bổ sung trong trường hợp mức đảm bảo đánh giá được lựa chọn.

3. PPMatchingList

Ảnh xạ EAL đến các tiêu chí đánh giá đặc thù, chỉ xuất hiện trong PP mà không xuất hiện trong các yêu cầu đảm bảo an toàn theo chuẩn.

- PPID: định danh của PP.
- STID: định danh của ST đang được xét.
- Value: có giá trị TRUE khi mức đảm bảo đánh giá có thể hiện yêu cầu đảm bảo an toàn với ID tương ứng.
- ApplicationNote: các thông tin bổ sung trong trường hợp mức đảm bảo đánh giá được lựa chọn.



Hình 3. Mô hình quản lý các tiêu chí đánh giá ATTT cho website

Tập các yêu cầu đảm bảo phù hợp trên cũng là cơ sở thực hiện xây dựng các bài khảo sát người quản lý, người phát triển của website giúp đưa ra được dự báo mức độ đảm bảo phù hợp mà website đó có thể đạt được. Nghĩa là với những yêu cầu đảm bảo mà website đã đáp ứng, website đó sẽ phù hợp với mức độ đảm bảo nào khi xét đến một hồ sơ bảo mật tương ứng.

C. Tiêu chí đánh giá đặc thù

PP đưa ra một tập các yêu cầu ATTT cho một loại đích đánh giá đặc thù. Trong các hồ sơ bảo vệ, luôn luôn có SAR sử dụng để đánh giá EAL của sản phẩm. Các yêu cầu đảm bảo an toàn này có thể được trích ra, được mở rộng từ các tiêu chí đảm bảo được định nghĩa trong tiêu chuẩn ISO/IEC 15408, ngoài ra cũng có một số tiêu chí đảm bảo an toàn được định nghĩa mới tương ứng với từng TOE mà PP đó mong muốn mô tả. Các tiêu chí mới này được mô hình hóa như sau:

1. GroupingInfo

Bao gồm các thông tin định danh và phân loại tiêu chí đánh giá đặc thù trong PP (các tiêu chí có trong 5 PP liên quan đến website).

- SARID: định danh tiêu chí đặc thù.
- ClassCode: Thuộc tính này được sử dụng để định danh các lớp (có thể mở rộng so với các lớp của yêu cầu đảm bảo).
- FamilyCode: định danh các họ (có thể mở rộng so với các họ của yêu cầu đảm bảo).
- ComponentIdentification: mô tả định danh và tham chiếu đến một trong 78 thành phần bảo đảm an toàn được ISO 15408 đề xuất thuộc các họ đã nêu ở trên.
- ComponentIndex: mức độ đánh giá của tiêu chí đảm bảo đặc thù.
- DevActions, ContentAndPresentations, EvaluatorActions: tập các hành động người phát triển, người quản lý cần thực hiện để có thể đạt được tiêu chí đảm bảo này.

2. PPMatchingList

Xác định ánh xạ giữa tiêu chí đặc thù và các PP được sử dụng cho cùng một TOE.

- PPID: định danh cho một PP.
- SARName: tên của tiêu chí đặc thù xuất hiện trong các PP.
- Value: TRUE khi tiêu chí đặc thù xuất hiện trong PP được sử dụng.
- ApplicationNote: các thông tin bổ sung trong trường hợp tiêu chí đặc thù được lựa chọn.

3. EALMatchingList

Xác định ánh xạ giữa tiêu chí đặc thù (xuất hiện trong tập yêu cầu đảm bảo của các PP) và mức đảm bảo đánh giá cho cùng một TOE.

- SARID: yêu cầu đảm bảo an toàn.
- PPID: PP chứa yêu cầu đảm bảo an toàn.
- Value: TRUE khi mức đảm bảo đánh giá có thể hiện yêu cầu đảm bảo an toàn với ID tương ứng.
- ApplicationNote: các thông tin bổ sung trong trường hợp mức đảm bảo đánh giá được lựa chọn.

Các tiêu chí đánh giá đặc thù mô hình hóa các yêu cầu an toàn mở rộng, đây là các yêu cầu an toàn không dựa trên các thành phần từ ISO/IEC 15408. Các thành phần này thường được định nghĩa bởi tác giả của hồ sơ bảo vệ nhằm đưa ra

các yêu cầu đảm bảo với mức độ tuân thủ chặt chẽ hơn. Các yêu cầu mở rộng phải được mô tả rõ ràng và đòi hỏi tuân thủ đầy đủ trong các hồ sơ bảo vệ.

Bài báo xây dựng mô hình các tiêu chí đặc thù nhằm tổng hợp các yêu cầu an toàn mở rộng từ các hồ sơ bảo vệ của các thành phần cấu thành và vận hành hệ thống website.

D. Khảo sát

Mỗi website muốn đánh giá mức độ đảm bảo, người quản lý cần kiểm tra xem người phát triển và vận hành website đã đáp ứng được các tiêu chí đảm bảo cần thiết theo PP xác định. Cụ thể hơn, người đánh giá muốn biết được, các hành động được nêu ra trong mỗi tiêu chí đã được người phát triển, quản lý website thực hiện hay chưa. Công việc này trên thực tế rất phức tạp, tốn nhiều thời gian. Chính bởi lý do đó, nghiên cứu đưa ra một giải pháp giúp người đánh giá có thể đánh giá sơ bộ được mức độ đảm bảo của một website thông qua việc khảo sát các tiêu chí đảm bảo dưới dạng một tập các câu hỏi hay còn được gọi là bảng khảo sát. Thông qua việc trả lời các câu hỏi cho người đánh giá có thể kiểm tra sơ bộ được một website đã đáp ứng được các yêu cầu về đảm bảo nào, từ đó có thể đưa ra được mức độ đảm bảo phù hợp với website đang được đánh giá.

Với mỗi website cần được đánh giá, người quản lý sẽ định ra một tập các câu hỏi được dùng để đánh giá website đó. Các tiêu chí này được người quản lý tổng hợp, chọn lọc từ các PP mà họ cho là cần thiết đối với việc đánh giá. Điều này cũng tương tự như việc chúng ta tạo nên một tập các tiêu chí cho một website cụ thể, và survey sẽ giúp người quản lý khảo sát được website đó có thỏa mãn với tập tiêu chí vừa được người đánh giá tạo ra hay không.

Với mục đích trên, các bản khảo sát được tạo nên từ các thành phần sau:

1. Question

- QuestionID: Định danh cho câu hỏi để khảo sát các hành động người phát triển, người quản lý website cần thực hiện để có thể đạt được một tiêu chí đảm bảo.
- PPIDList: danh sách định danh hồ sơ bảo vệ chứa thông tin đầu vào thiết lập các câu hỏi khảo sát
- QuestionContent: nội dung câu hỏi khảo sát - mặc định ở dạng đóng (Yes/No question).
- ResultList: danh sách các câu trả lời.

2. ActionListMapping

Xác định ánh xạ giữa câu hỏi và các hành động được sử dụng để đánh giá cùng một yêu cầu.

- ActionID: định danh cho một hành động mà người phát triển, người quản lý website cần hoàn thành.
- PPID: định danh của PP chứa hành động.
- RID: định danh của yêu cầu đánh giá.
- Value: TRUE khi câu hỏi được sử dụng để đánh giá hành động được thực hiện tương ứng với một yêu cầu đánh giá.
- ApplicationNote: các thông tin bổ sung trong trường hợp câu hỏi được lựa chọn.

3. SurveyInfo

- SurveyID: định danh bản khảo sát.
- QuestionIDList: danh sách các câu hỏi sử dụng trong bản khảo sát.
- RIDList: danh sách các định danh yêu cầu đảm bảo (RequirementID) hoặc yêu cầu đảm bảo an toàn (SARID) cần đánh giá thông qua bản khảo sát.
- SARIDList: danh sách các yêu cầu đảm bảo an toàn/tiêu chí đặc thù cần đánh giá thông qua bản khảo sát.
- EALNameList: danh sách các mức đảm bảo đánh giá có khả năng đáp ứng khi xét đến các tiêu chí đánh giá trong bảng khảo sát. Đây cũng là các yêu cầu đảm bảo được người đánh giá sử dụng để đánh giá mức đảm bảo cho một website.
- TOEID: định danh đích đánh giá (website).

III. THỬ NGHIỆM

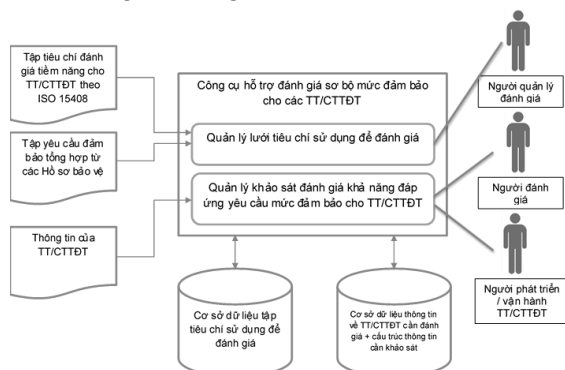
Mô hình quản lý các tiêu chí đánh giá ATTT được cài đặt thử nghiệm như một công cụ hỗ trợ cho người quản lý, người đánh giá và người phát triển /vận hành các Trang tin/Công thông tin điện tử (TT/CTTĐT) có thể đánh giá sơ bộ khả năng phù hợp với một mức đảm bảo đánh giá cho sản phẩm của họ.

Hai kịch bản thử nghiệm có thể triển khai gồm:

- Người dùng công cụ trả lời các câu hỏi trắc nghiệm, công cụ sẽ cho biết TT/CTTĐT phù hợp với mức đảm bảo đánh giá nào.
- Người dùng công cụ chọn trước EAL và sau đó trả lời các câu hỏi trắc nghiệm, công cụ sẽ cho biết hiện trạng triển khai các biện pháp đảm bảo ATTT cho các

thành phần cấu thành và vận hành TT/CTTĐT có phù hợp với mức đảm bảo đánh giá đã chọn hay không.

Thông thường, việc đánh giá dựa vào các PP của các thành phần cấu thành, vận hành của website, cách làm này làm cho việc đánh giá là khá phức tạp do tập các tiêu chí đảm bảo trong mỗi hồ sơ bảo vệ là không giống nhau. Như đã đề cập trong Mục II, cơ sở dữ liệu tiêu chí đánh giá ATTT sẽ được tổng hợp từ tập các tiêu chí đảm bảo trong ISO/IEC 15408 và tập các tiêu chí đảm bảo trong các PP của các thành phần cấu thành, vận hành một website. Chúng tôi lựa chọn những tiêu chí phù hợp với việc đánh giá mức độ ATTT cho các website từ hai tập tiêu chí trên. Để đảm bảo tính đúng đắn của hệ thống, tập các tiêu chí phù hợp được tổng hợp từ các Hồ sơ bảo vệ luôn là tập con của tập các tiêu chí được lựa chọn từ tiêu chuẩn ISO/IEC 15408. Với cơ sở dữ liệu tiêu chí đánh giá được thiết kế như trên, tập các tiêu chí trong ISO/IEC 15408 sẽ được sử dụng cho việc khảo sát tổng quan một trang web, còn tập các tiêu chí được tổng hợp từ các Hồ sơ bảo vệ sẽ được sử dụng với mục đích ánh xạ kết quả việc khảo sát với các mức đảm bảo phù hợp của một website ứng với từng PP.

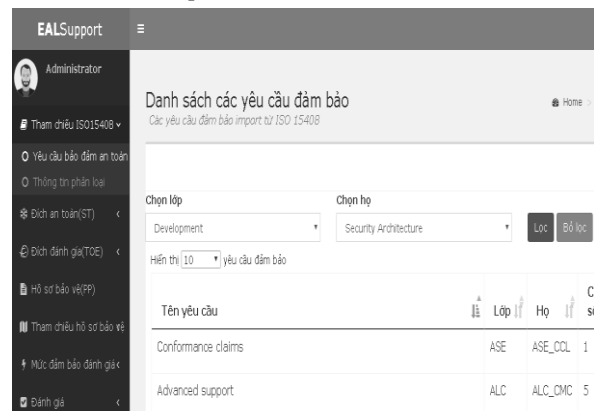


Hình 4. Công cụ quản lý tiêu chí và đánh giá khả năng đáp ứng yêu cầu mức đảm bảo

Bộ công cụ được xây dựng trên nền Web với ngôn ngữ PHP và engine Elasticsearch thuận tiện cho việc quản lý, truy vấn tìm kiếm cơ sở dữ liệu tập tiêu chí sử dụng để đánh giá. Hình 4 mô tả tổng quan về các thành phần và đối tượng sử dụng mà sản phẩm hướng đến.

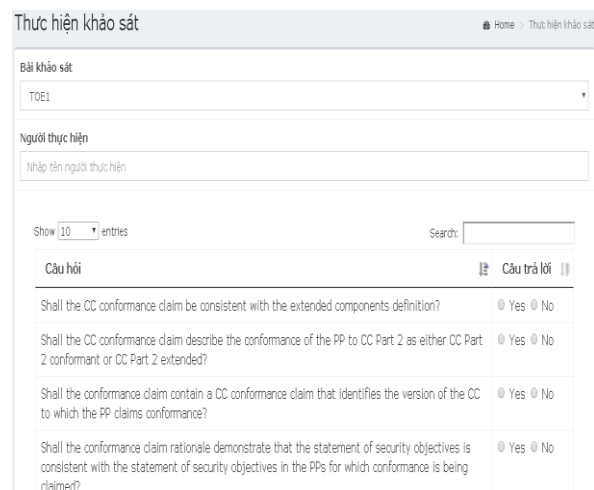
Người quản lý đánh giá có thể tùy biến tập các tiêu chí phù hợp với việc đánh giá một website. Điều này sẽ giúp cho việc đánh giá mức độ ATTT cho một website trở nên linh hoạt, dễ dàng hơn mà vẫn đảm bảo tuân thủ các tập tiêu chí được nêu ra

trong tiêu chuẩn ISO/IEC 15408, cũng như trong các PP có liên quan.



Hình 5. Giao diện tạo lập bảng khảo sát dành cho người đánh giá

Người đánh giá tạo ra các bảng khảo sát với tập các câu hỏi tương ứng với các tiêu chí đánh giá (Hình 5). Các bảng khảo sát này được tạo ra với mục đích giúp người đánh giá có thể thực hiện việc đánh giá sơ bộ khả năng đáp ứng yêu cầu mức độ đảm bảo ATTT của một website xác định.



Hình 6. Giao diện bảng khảo sát dành cho người dùng cuối

Người quản lý, người phát triển sẽ thực hiện trả lời các câu hỏi có trong bảng khảo sát (Hình 6) và người đánh giá sẽ dựa vào kết quả khảo sát thu được để có thể từ đó đưa ra được mức đảm bảo phù hợp với website tương ứng. Sau khi người phát triển, quản lý website hoàn thành bài survey, cũng là trả lời xong tất cả các câu hỏi mà người đánh giá đặt ra, kết quả khảo sát sẽ được gửi lại cho người đánh giá.

Dựa vào kết quả khảo sát thu được này, người đánh giá sẽ tổng hợp và đưa ra được các yêu cầu đảm bảo mà một website có thể đáp ứng được.

Từ đó, ánh xạ kết quả này vào 7 mức đảm bảo EAL được nêu ra trong tiêu chuẩn ISO/IEC 15408 và đưa ra được mức đảm bảo sơ bộ phù hợp với website đang được khảo sát. Thông qua việc sử dụng Survey_ID, kiểm tra các yêu cầu đảm bảo mà website đạt được qua việc khảo sát, từ đó so sánh với các yêu cầu trong 7 mức EAL và đưa ra được đánh giá sơ bộ về mức đảm bảo của website được khảo sát đến trong bài survey.

Kết quả của các khảo sát cung cấp cho người quản lý, vận hành website thông tin về các tiêu chí đảm bảo mà hệ thống đó có thể đạt được.

IV. KẾT LUẬN

Trong bài báo này, chúng tôi đã giới thiệu một phương thức mô hình hóa các tiêu chí đánh giá ATTT cho các website. Mô hình này được xây dựng cho hai nhiệm vụ chính: thứ nhất là kết nối các tiêu chí sử dụng để đánh giá ATTT cho website theo ISO 15408, và các yêu cầu ATTT theo hồ sơ bảo vệ của các thành phần cấu thành và vận hành website; thứ hai là tạo lập các bản khảo sát dành cho người phát triển, người vận hành, người đánh giá cung cấp thông tin đầu vào cho việc đánh giá dựa trên các tiêu chí đã kết nối. Trên cơ sở mô hình này, chúng tôi đã xây dựng công cụ hỗ trợ người quản lý, người phát triển website đánh giá sơ bộ các yêu cầu ATTT và dự đoán mức đảm bảo đánh giá cho website. Công cụ này sử dụng các các yêu cầu về đảm bảo được đề cập đến trong bản tiêu chuẩn ISO/IEC 15408, dựa vào việc phân tích mức độ quan trọng, phù hợp của các tiêu chí, bài báo đưa ra một tập các tiêu chí đảm bảo cần thiết cho việc đánh giá một website. Từ đó, công cụ giúp người sử dụng có thể tìm được mức độ đảm bảo phù hợp với website qua các bước sau:

Bước 1: Người quản lý/người đánh giá định nghĩa lưới tiêu chí đánh giá phù hợp cho website từ cơ sở dữ liệu các tiêu chí theo tiêu chuẩn ISO/IEC 15408 và các yêu cầu đảm bảo trong các hồ sơ bảo vệ liên quan.

Bước 2: Người đánh giá tùy biến tập các tiêu chí đảm bảo được tổng hợp từ tiêu chuẩn ISO/IEC 15408, tập các câu hỏi khảo sát (Yes/No) với mục đích khảo sát các yêu cầu đảm bảo từ website.

Bước 3: Người sử dụng công cụ (người phát triển, quản lý website, người đánh giá) hoàn thành bài khảo sát.

Bước 4: Từ kết quả khảo sát, công cụ sẽ ánh xạ đến tập các yêu cầu đảm bảo được đề cập trong các PP liên quan và đưa ra dự báo về mức đảm

bảo đánh giá phù hợp với các yêu cầu đảm bảo mà website đã đạt được.

Với cách thức vận hành như trên, công cụ cho phép người dùng biết được website của họ có khả năng đạt được mức đảm bảo đánh giá nào. Điều này đồng nghĩa với bộ công cụ sẽ giúp người sử dụng đánh giá sơ bộ được độ đảm bảo của website, giúp người sử dụng yên tâm với việc sản phẩm đã được đảm bảo thông qua một bên thứ ba. Tuy nhiên, khi đặt một website trong một hoàn cảnh cụ thể, mức đảm bảo đánh giá của mỗi website là khác nhau. Chính vì vậy, trong tương lai, bộ công cụ đánh giá này sẽ được phát triển với một số chức năng nâng cao hơn như lưu kết quả đánh giá phù hợp, tiến hành nâng cấp xử lý kết quả và kết hợp kết quả này với việc đánh giá cấp độ ATTT của một website.

TÀI LIỆU THAM KHẢO

- [1]. ISO/IEC 15408-1, "Information technology - Security techniques - Evaluation criteria for IT security", Part 1: Introduction and general model.
- [2]. ISO/IEC 15408-2, "Information technology - Security techniques - Evaluation criteria for IT security", Part 2: Security functional components.
- [3]. ISO/IEC 15408-3, "Information technology - Security techniques - Evaluation criteria for IT security", Part 3: Security assurance components.
- [4]. Huilin Chen, Da Bao, Hongbiao Gao and Jingde Cheng: "A Security Evaluation and Certification Management Database Based on ISO/IEC Standards". In Proceedings of 12th International Conference on Computational Intelligence and Security. IEEE 2016.
- [5]. Information Assurance Directorate. U.S. Government "Protection Profile Web Server For Basic Robustness Environments". Version 1.0. December 26, 2006.
- [6]. NIAP. "Protection Profile for Server Virtualization". Version 1.0. 29 October 2014.
- [7]. "Turkish standards institution. Common criteria protection profile for security of web services". Version 1.0. 2012.
- [8]. NIAP. U.S. Government "Approved Protection Profile - Protection Profile for Application Software". Version 1.2. 2016.
- [9]. NIAP. "Protection Profile for Web Browsers". Version 1.0. 2014.
- [10]. NIAP. "US Government Protection Profile Authorization Server For Basic Robustness Environments". Version 1.1. 2007.

SƠ LƯỢC VỀ TÁC GIẢ



TS. Vũ Thị Hương Giang

Đơn vị công tác: Viện Công nghệ Thông tin và Truyền thông, ĐH Bách Khoa Hà Nội.

Email: giangvth@soict.hust.edu.vn

Nhận bằng đại học năm 2001 và nhận bằng thạc sĩ năm 2003 chuyên ngành Công nghệ thông tin tại ĐH Bách Khoa Hà Nội.

Nhận bằng tiến sĩ chuyên ngành Hệ thống và phần mềm tại Đại học Bách Khoa Hà Nội năm 2008.

Hướng nghiên cứu hiện nay: các hệ thống hướng dịch vụ đảm bảo an toàn thông tin, các phương pháp phát triển phần mềm tiên tiến và ứng dụng.



ThS. Nguyễn Mạnh Tuấn

Đơn vị công tác: Viện Công nghệ Thông tin và Truyền thông, ĐH Bách Khoa Hà Nội.

Email: tuannm@soict.hust.edu.vn

Nhận bằng đại học năm 2007 và nhận bằng thạc sĩ năm 2016 chuyên ngành Công nghệ thông tin tại ĐH Bách Khoa Hà Nội.

Hướng nghiên cứu hiện nay: an toàn và bảo mật thông tin, phát triển các hệ thống web tiên tiến.

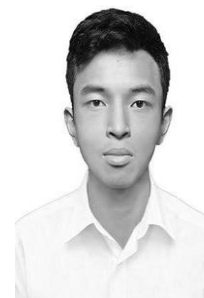


Đặng Bá Tú

Email: dangbatu.hust@gmail.com

Sinh viên năm 5 hệ Kỹ sư, chuyên ngành Công nghệ phần mềm, Viện Công nghệ Thông tin và Truyền thông, ĐH Bách Khoa Hà Nội.

Hướng nghiên cứu hiện nay: an toàn thông tin



Lê Hồng Dương

Email: le.duong6795@gmail.com

Sinh viên năm 5 hệ Kỹ sư, chuyên ngành Công nghệ phần mềm, Viện Công nghệ Thông tin và Truyền thông, ĐH Bách Khoa Hà Nội.

Hướng nghiên cứu hiện nay: an toàn thông tin