PHÂN LOẠI MỨC ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN THEO CÁCH TIẾP CẬN CỦA LÝ THUYẾT HỆ THỐNG

Nguyễn Thị Xuân, Hoàng Đăng Hải, Nguyễn Kim Quang

Học viện Công nghệ Bưu chính Viễn thông

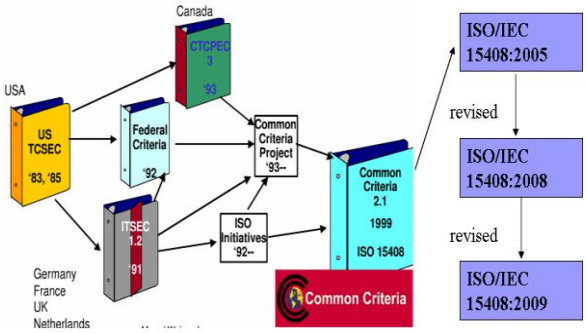
Tóm tắt: Bài báo trình bày về vấn đề phân loại và đánh giá mức độ an toàn hệ thống thông tin. Các phương pháp phân loại tới nay chủ yếu vẫn mang tính định tính. Bài báo trình bày một cách tiếp cận mới trên cơ sở lý thuyết hệ thống và cách thức triển khai áp dụng thực tiễn.

Từ khóa: Phân loại hệ thống thông tin, lý thuyết hệ thống, đánh giá mức độ an toàn thông tin.

I. MỞ ĐẦU

Một nhu cầu thực tế đặt ra là làm thế nào để biết các hệ thống thông tin có tin cậy hay không, có áp dụng các biện pháp và kỹ thuật an toàn phù hợp hay không, mức độ an toàn như thế nào? Phân loại mức độ an toàn hệ thống thông tin là bước quan trọng ban đầu để thực hiện phân tích, đánh giá an toàn cho hệ thống.

Có nhiều phương pháp tiếp cận để phân loại mức độ an toàn hệ thống thông tin. Cách thông thường hay sử dụng tới nay là nhận dạng hệ thống thông tin và chức năng quan trọng nhất của hệ thống, đánh giá mức độ ảnh hưởng do mất an toàn thông tin có thể gây ra. Nhận dạng, phân loại theo chức năng có thể dựa vào ba thuộc tính cơ bản là: tính bí mật, tính toàn vẹn và tính khả dụng của hệ thống. Mức độ tác động do mất an toàn có thể thực hiện thông qua việc xây dựng bộ tiêu chí đánh giá và thực hiện đánh giá theo các tiêu chí. Các tiêu chí đánh giá an toàn thông tin (ATTT) khá đa dạng do tính đa dạng của các hệ thống thông tin (HTTT). Do vậy, một số bộ tiêu chí đã được xây dựng phục vụ cho mục đích này, điển hình là các tiêu chí trong bộ tiêu chuẩn TCSEC của Mỹ, ITSEC của châu Âu, bộ tiêu chí chung (Common Criteria - gọi tắt là CC) quốc tế và bộ tiêu chuẩn ISO/IEC 15408. Hình 1 biểu thị quá trình phát triển của các bộ tiêu chí cho đánh giá an toàn thông tin [1].



Hình 1. Quá trình phát triển các bộ tiêu chí đánh giá an toàn thông tin [1]

Các bộ tiêu chuẩn TCSEC và ITSEC chưa thể hiện đầy đủ yêu cầu cho việc phân loại, đánh giá nên không được sử dụng phổ biến. Xây dựng một bộ tiêu chí chung (CC) là một nhu cầu thực tế. Trên cơ sở đó, bộ tiêu chuẩn ISO/IEC 15408 đã chính thức ra đời từ năm 2005 sau khi rà soát, hiệu chỉnh hoàn thiện cho bộ tiêu chí chung (CC) [2]. Bộ tiêu chuẩn ISO/IEC 15408 [3] bao gồm ba phần. Phần 1 là mô hình chung, phần 2 là bộ tiêu chí chung cho chức năng an toàn, phần 3 là xếp loại mức độ bảo đảm ATTT (theo 7 mức). Đây là bộ tiêu chuẩn toàn diện, chi tiết, có thể dùng để đánh giá ATTT theo các chức năng an toàn để từ đó phân loại mức độ bảo đảm ATTT. Tuy nhiên, bộ tiêu chuẩn này vẫn còn khá phức tạp, rất khó áp dụng trong thực tế cho từng loại hệ thống thông tin cụ thể.

Một số bộ tiêu chuẩn của Mỹ như FIPS 199 [4], FIPS 200 [5], NIST SP 800-53 [6] cũng đề cập đến việc xây dựng một bộ tiêu chí cụ thể gắn liền với việc phân loại các hệ thống thông tin và đưa ra các yêu cầu cũng như phương pháp phân loại hệ thống thông tin để có thể đánh giá được mức độ an toàn của từng loại hệ thống. Tuy nhiên, việc đánh giá mức độ tác động do mất ATTT để từ đó phân loại HTTT vẫn còn mang tính định tính là chủ yếu. Bộ tiêu chuẩn chưa chỉ ra cách thức đánh giá cụ thể về mức độ tác động do

mất ATTT cũng như cách thức cụ thể để phân loại HTTT.

Một số công trình nghiên cứu cũng đã đề cập đến vấn đề đánh giá và phân loại mức độ ATTT cho các HTTT, điển hình như [7][8] [9]. Điểm chung của các mô hình đưa ra trong các tài liệu này là cố gắng phân loại các hệ thống thông tin theo các yêu cầu về chức năng an toàn, chia chúng theo các phân lớp và gán các giá trị định lượng cho từng chức năng và từng lớp. Theo mô hình, đánh giá viên thực hiện tác động vào hệ thống (giả lập tấn công) hoặc rà quét lỗ hổng bảo mật, xem phản hồi của hệ thống (hành vi của hệ thống hoặc kết quả rà quét) để phân loại mức độ bảo đảm ATTT của HTTT. Ưu điểm của các mô hình này là đã đưa ra cách thức đánh giá một cách định lượng hơn so với các bộ tiêu chuẩn nêu trên. Tuy nhiên, các mô hình này vẫn chủ yếu dựa vào các bộ tiêu chí chung (CC) hay bộ tiêu chuẩn ISO/IEC 15408 nên vẫn bị hạn chế do tính phức tạp, khó áp dụng cho một HTTT cụ thể. Mặt khác, những mô hình này vẫn chưa xem xét đến tác động ảnh hưởng do mất ATTT khi phân loại, đánh giá HTTT.

Bài báo này đưa ra một cách tiếp cận mới cho phân loại mức độ ATTT của HTTT theo lý thuyết hệ thống. Cách tiếp cận này có ưu điểm là kết hợp được việc xem xét tác động do mất ATTT với việc phân loại HTTT. Theo mô hình này, một tác động từ bên ngoài (ví dụ: tấn công giả lập) vào một HTTT sẽ cho ra một hoặc một chuỗi hành vi (phản ứng của hệ thống). Hành vi chính là thể hiện tác động do mất ATTT. Căn cứ vào hành vi có thể phân loại mức độ an toàn cho HTTT.

Phần còn lại của bài báo được tổ chức như sau. Phần 2 trình bày về nguyên tắc phân loại hệ thống thông tin. Phần 3 trình bày về phân loại mức độ an toàn hệ thống thông tin tiếp cận theo lý thuyết hệ thống. Phần 4 trình bày về cách thức áp dụng mô hình vào việc phân loại mức độ an toàn của hệ thống website. Phần 5 là kết luận của bài.

II. NGUYÊN TẮC PHÂN LOẠI HỆ THỐNG THÔNG TIN

A. Định nghĩa hệ thống thông tin

Hệ thống thông tin là một nhóm các thành phần có tương tác với nhau nhằm một mục đích chung. Theo định nghĩa trong [10], hệ thống thông tin là một tập hợp phần cứng, phần mềm, cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

Hệ thống thông tin thường không hoạt động hoàn toàn độc lập mà phụ thuộc vào môi trường chứa nó và các hệ thống khác với các trung gian bên ngoài. Phạm vi của hệ thống là đường ranh giới (boundary), bên ngoài ranh giới là môi trường của hệ thống, hệ thống liên hệ với thế giới bên ngoài thông qua giao diện (Interface) với môi trường. Giao diện phục vụ cho việc trao đổi thông tin giữa hệ thống với môi trường và các hệ thống khác. Hệ thống có thể gồm các hệ thống con (subsystem) theo một mô hình phân cấp. Kết nối giữa các hệ thống con là các giao diện cục bộ.

B. Nguyên tắc phân loại thông tin

Việc phân loại một hệ thống thông tin đòi hỏi xem xét đến tất cả các loại thông tin có trong hệ thống. Việc nhận dạng, phân loại thông tin được xử lý trong một hệ thống thông tin là cần thiết nhằm lựa chọn các tiêu chuẩn phù hợp.

Để phân loại, bộ tiêu chuẩn FIPS 199 [4] đưa ra ba mức độ tác động như trong Bảng *I*. Căn cứ vào ba thuộc tính: bí mật, toàn vẹn, khả dụng của thông tin và ba mức độ tác động tương ứng, có thể phân loại thông tin theo 06 cấp độ như trong Bảng *II*.

Bảng I. Mức độ tác động

Mức độ tác động	Tác động do mất tính bí mật, toàn vẹn, khả dụng
Thấp	***Ảnh hưởng bất lợi một phần*** đối với hoạt động, tài sản của tổ chức, cá nhân.
Trung bình	***Ảnh hưởng bất lợi nghiêm trọng*** đối với hoạt động, tài sản của tổ chức, cá nhân.
Cao	***Ảnh hưởng bất lợi nặng nề hay khủng hoảng*** đối với hoạt động, tài sản của tổ chức, cá nhân.

Bảng II. Phân loại thông tin

Phân loại	Tác động khi mất thông tin
Tuyệt mật (Top Secret)	Thiệt hại đáng kể cho mạng sống con người, xung đột ngoại giao quốc tế, hoặc ảnh hưởng nghiêm trọng tới hoạt động tình báo.
Tối mật (Secret)	Đe dọa đến mạng sống con người, phá rối trật tự xã hội, hoặc gây phương hại đến quan hệ ngoại giao quốc tế.

Mật (Confidential)	Xâm phạm quyền con người, gây thiệt hại vật chất, quan hệ ngoại giao quốc tế, ảnh hưởng nghiêm trọng đến đời sống hàng ngày.
Hạn chế (Restrict)	Ảnh hưởng đáng kể đến cá nhân, bất lợi cho các hoạt động quân sự hoặc thực thi pháp luật.
Bảo vệ (Protect)	Gây phiền nhiễu cho các cá nhân, tổn thất tài chính, thanh danh, tiếp tay tội phạm, bất lợi trong thương mại và ngoại giao.
Không phân loại	Không có tác động (không cần thiết phải bảo vệ).

Bộ tiêu chuẩn FIPS 199 [4] đưa ra 27 cấp độ an toàn thông tin theo biểu thức sau đây.

$SC_{\text{Loại thông tin}}$ = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}

Trong đó SC là cấp độ ATTT, *impact* là tác động, có thể có các giá trị thấp, trung bình, cao (hoặc không áp dụng).

Bộ tiêu chuẩn FIPS SP 800-60 [6] đưa ra 26 lĩnh vực dịch vụ với 98 loại thông tin liên quan, điển hình là các lĩnh vực quốc phòng, an ninh quốc gia, an ninh nội địa,…

C. Nguyên tắc phân loại hệ thống thông tin

Việc phân loại hệ thống thông tin cũng dựa vào các thuộc tính và tác động như với thông tin (theo [4,5,6]) như sau:

$SC_{\text{Hệ thống thông tin}}$= {(**confidentiality**, *impact*), (**integrity**,*impact*),(**availability**,*impact*)}

Trong đó SC là mức độ an toàn của hệ thống thông tin. Đối với hệ thống thông tin, *impact* cần được đặt giá trị cao nhất trong số các giá trị đã được xác định cho các loại thông tin có trong hệ thống.

Trong thực tế, các thuộc tính bí mật, toàn vẹn, khả dụng thường không đồng thời có cùng mức độ tác động đối với một HTTT cụ thể. Bộ tiêu chuẩn FIPS 200 [5] đưa ra ba phân loại cơ bản như sau:

- Hệ thống có tác động thấp: HTTT có yêu cầu thấp đối với cả ba thuộc tính bí mật, toàn vẹn và khả dụng.

- Hệ thống có tác động trung bình: HTTT có ít nhất một thuộc tính là trung bình, không có thuộc tính nào ở mức cao.

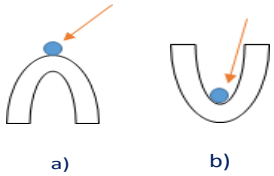
- Hệ thống có tác động cao: HTTT có ít nhất một thuộc tính là mức cao.

FIPS 200 đưa ra các yêu cầu an toàn tối thiểu cho các HTTT về các tiêu chí: 1) Kiểm soát truy nhập, 2) Kiểm thử và gán trách nhiệm, 3) Đánh giá mức độ an toàn, 4) Quản lý cấu hình, 5) Xác định danh tính và xác thực, 5) Phản ứng sự cố, 6) Bảo vệ phương tiện, 7) Bảo vệ truyền tin, 8) Đánh giá rủi ro.

III. ÁP DỤNG LÝ THUYẾT HỆ THỐNG VÀO PHÂN LOẠI MỨC ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN

A. Cách tiếp cận theo lý thuyết hệ thống

Để rõ hơn cách tiếp cận theo lý thuyết hệ thống, ta xét một ví dụ sau (Hình 2). Coi một HTTT như một khối thống nhất đang đứng yên (hình tròn trên Hình 2).



Hình 2. Ví dụ minh họa tác động vào hệ thống

Khi có một tác động từ bên ngoài vào khối đó, sẽ có 2 trường hợp xảy ra:

- Khối sẽ mất cân bằng và dịch chuyển khỏi vị trí ban đầu (hình 2a) và có thể trượt khá xa vị trí cũ.

- Khối có thể bị tác động nhỏ, song vẫn giữ được vị trí cân bằng ban đầu (Hình 2b).

Trong trường hợp 1, tác động từ bên ngoài (ví dụ một tấn công) sẽ gây ra một chuỗi hành vi tác động ảnh hưởng. Hành vi chính là thể hiện tác động do mất ATTT. Nghĩa là hệ thống có mức độ ATTT cao, do tấn công vào hệ thống sẽ gây ra những tác động (thiệt hại) liên hoàn, có thể kéo theo sập cả các hệ thống khác. Trong trường hợp 2, tác động từ bên ngoài ít hoặc không gây thiệt hại gì đáng kể. Hệ thống trong trường hợp này có mức độ ATTT thấp, có thể không cần phải bảo vệ nhiều.

Từ ví dụ nêu trên, ta có thể áp dụng lý thuyết hệ thống vào việc phân tích và phân loại mức độ an toàn HTTT như trong phần sau đây.

B. Mô hình hệ thống theo lý thuyết hệ thống

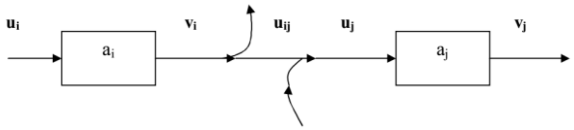
Theo lý thuyết hệ thống, một hệ thống có hai đặc trưng cơ bản đó là cấu trúc và hành vi của hệ thống [11].

1) Cấu trúc hệ thống

Một hệ thống gồm có các phần tử và các liên kết giữa các phần tử. Cấu trúc hệ thống là sự sắp xếp các liên kết giữa các phần tử để tạo nên hệ thống. Có ba loại liên kết cơ bản sau đây:

a) Liên kết nối tiếp

Liên kết nối tiếp giữa hai phần tử a_i và a_j được thể hiện bởi sơ đồ trên hình 3.



Hình 3. Liên kết nối tiếp

Trong đó:

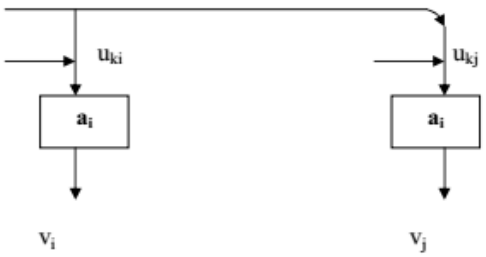
u_i là đầu vào (input) của phần tử i, v_i là đầu ra (output) của phần tử i, u_{ij} là phần đầu ra của phần tử i trở thành đầu vào của phần tử j. u_{ij} thể hiện tác động của phần tử i đối với phần tử j.

Trong liên kết nối tiếp giữa hai phần tử a_i và a_j có thể xảy ra 4 tình huống sau đây:

- Liên kết chặt chẽ nếu $v_i = u_{ij} = u_j$
- Liên kết tự do nếu $u_{ij} \# v_i$ và $u_{ij} \# u_j$
- Liên kết ra tự do nếu $u_{ij} \# v_i$ và $u_{ij} = u_j$
- Liên kết vào tự do nếu $u_{ij} = v_i$ và uij$\# u_j$

b) Liên kết song song

Liên kết song song giữa hai phần tử a_i và a_j thể hiện bởi sơ đồ trên Hình 4 sau:

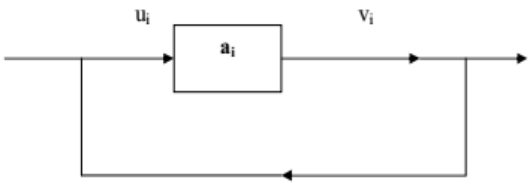


Hình 4. Liên kết song song

Nếu $u_{ki} = u_{kj}$ ta gọi đó là liên kết song song cân xứng; nếu $u_{ki} \# u_{kj}$ thì gọi là liên kết song song không cân xứng.

c)Liên kết ngược

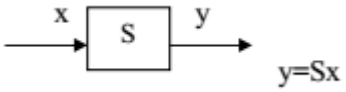
Nếu chỉ xét một phần tử, ta có cấu trúc kiểu liên kết ngược như thể hiện trên sơ đồ Hình 5 như sau:



Hình 5. Liên kết ngược

Điều kiện bắt buộc ở đây là $u_i \# u_{ij} \# v_i$, nếu không thì phần tử a_i không còn khả năng liên kết với bất kỳ phần tử nào của hệ thống.

2) Hành vi hệ thống



Hình 6. Sơ đồ đơn giản của hệ thống

Một hệ thống có thể gồm nhiều phần tử, được minh họa đơn giản hóa bằng khối ***S*** trên Hình 6, với đầu vào ***x*** và đầu ra ***y*** (***x*** và ***y*** có thể là một vectơ chứa nhiều đầu vào và nhiều đầu ra).

Hành vi của phần tử: Xét phần tử a_i của hệ ***S***, khi nó nhận đầu vào $u_i \in U_i$ nó sẽ cho ra một đầu ra $v_i \in V_i$ (U_i là tập các đầu vào và V_i là tập các nhiều đầu ra).

Phép biến đổi $F_i: U_i \rightarrow V_i$ (có thể viết là $v_i = F_i(u_i)$) được coi là hành vi của phần tử a_i. Đầu ra v_i trở thành đầu vào của các phần tử tiếp theo. Tích hợp các phép biến đổi F_i của các phần tử tạo nên hành vi của hệ thống.

Hành vi của hệ thống: Ta gọi ***X*** là tập các đầu vào chấp nhận được trên các phần tử vào của hệ, ***Y*** là tập các đầu ra có thể. Thông qua các phép biến đổi của các phần tử của ***S***, cuối cùng hệ ***S*** sẽ cho ra một đầu ra $\boldsymbol{y \in Y \subset R_m}$. Trong đó $\boldsymbol{R_m}$ là tập trạng thái trong miền hoạt động.

Như vậy hành vi của hệ được thể hiện bởi phép biến đổi **F:X→Y**. Biểu thức này cũng có thể viết thành: $\boldsymbol{y=F(x)}$ với $\boldsymbol{x \in X}$.

$$\text{Hoặc} \begin{cases} y_1 = F(x_1, x_2, \ldots, x_n) \\ y_2 = F_2(x_1, x_2, \ldots, x_n) \\ \ldots \\ y_m = F_m(x_1, x_2, \ldots, x_n) \end{cases}$$

Hành vi của hệ như vừa mô tả, thực ra là một trường hợp đơn giản với giả thiết đó là một hệ tất định và phép biến đổi **F** là đơn trị. Trường hợp tổng quát **F** có thể là ánh xạ đa trị, hoặc **F** là ánh xạ đơn trị, nhưng không chỉ phục thuộc vào đầu vào mà còn phụ thuộc vào trạng thái của hệ khi nhận đầu vào, hoặc một dãy trạng thái của hệ trước khi nhận đầu vào. Ở đây ta cũng bỏ qua yếu tố thời gian. Thường thì sau khi hệ thống nhận đầu vào sẽ không cho ngay ra đầu ra, mà phải sau một khoảng thời gian Δt nào đó hệ thống mới cho

đầu ra. Nếu hệ thống là bất định thì **F** có thể là một đại lượng ngẫu nhiên nhiều chiều, biến thiên theo thời gian.

Do vậy, để đơn giản hóa, ta sẽ chỉ xét với hệ tất định. Một hệ đơn giản hóa như trên gọi là hệ đầu vào – đầu ra mô tả bởi sơ đồ như trên Hình 6.

3) Quan hệ giữa cấu trúc và hành vi

Nếu mỗi phần tử a_i ($i= 1,n$) của hệ thống ***S*** có n phần tử, có hành vi tương ứng với mỗi ánh xạ đơn trị F_i thì cấu trúc của hệ thống quyết định hành vi của hệ thống, cấu trúc nào hành vi nấy; nghĩa là tương ứng với một cấu trúc cho trước thì có một hành vi duy nhất. Nói cách khác mỗi hệ có một hành vi. Ngược lại để đảm bảo một hành vi cho trước thì có thể có nhiều hệ thống, nghĩa là *tương ứng với một hành vi là một tập cấu trúc*.

4) Bài toán phân loại mức độ an toàn HTTT

Để áp dụng lý thuyết hệ thống vào bài toán phân loại mức độ an toàn HTTT ta sử dụng bài toán phân tích hệ thống như sau.

Bài toán phân tích hệ thống là bài toán biết trước cấu trúc của hệ thống và đi tìm hành vi của hệ thống. Có hai vấn đề đặt ra: xác định cấu trúc và sau đó tìm hành vi của hệ thống.

a) Xác định cấu trúc hệ thống

Xác định cấu trúc hệ thống là nhận biết các phần tử trong hệ thống, liên kết giữa chúng, hành vi của tất cả các phần tử có mặt trong cấu trúc. Nghĩa là biết a_i ($i= 1,n$), F_i ($i=1,n$) và biết ma trận cấu trúc:

$W=(w_{ij})$ *với* $i= 0,n$ *và* $j=0,n$

Trong đó a_0 là phần tử đại diện cho môi trường.

b) Tìm hành vi hệ thống

Tìm hành vi của hệ thống tức là tìm phép biến đổi ***F*** mà $\boldsymbol{Y=F(x)}$ với $\boldsymbol{x \in X}$. Trong đó ***x*** là đầu vào của hệ thống, ***X*** là tập các đầu vào chấp nhận được còn ***y*** là đầu ra của hệthống, ***Y*** là tập các đầu ra có thể.

Mặt khác, ta coi: $x= v_0$ là đầu vào của hệ thống là đầu ra của môi trường. $y= u_0$ là đầu ra của hệ thống là đầu vào của môi trường.

Như vậy bài toán tìm hành vi của hệ thống chính là tìm phép biến đổi ***F*** sao cho $\boldsymbol{U_0 = F(v_0)}$ với $\boldsymbol{v_0 \in X}$.

Ở đây ***X*** là tập các tập các đầu vào chấp nhận được của hệ thống được coi là dữ liệu cho trước của bài toán.

Để tìm ***F*** ta tiến hành tích hợp các phép biến đổi F_i $(i=1,n)$ theo vết của ma trận cấu trúc $W=(w_{ij})$ bắt đầu từ các phần tử vào của hệ, qua các phần tử trung gian bên trong hệ và cuối cùng đến các phần tử ra của hệ. Sự phụ thuộc của đầu ra của các phần tử ra của hệ, vào các đầu vào của các phần tử vào của hệ, chính là phép biến đổi ***F***. Thuật toán cho các bài toán này nói chung không phải là vấn đề quá khó. Khi tìm được ***F*** thì với mỗi $\boldsymbol{x \in X}$ ta tìm được $\boldsymbol{y=F(x)}$ tức là tìm được đầu ra tương ứng. Từ đó ta cũng sẽ tìm được tập các đầu ra $\boldsymbol{Y=F(X)}$. Tập đầu ra ***Y*** thể hiện hành vi của hệ đó.

IV. ÁP DỤNG MÔ HÌNH VÀO PHÂN LOẠI MỨC ĐỘ AN TOÀN HỆ THỐNG WEBSITE

Trong phần sau đây, bài báo trình bày cách thức áp dụng mô hình theo lý thuyết hệ thống vào việc phân loại mức độ an toàn HTTT, nghĩa là bài toán "biết cấu trúc hệ thống, cần xác định hành vi hệ thống".

Hệ thống được xem xét là một Website. Đầu vào để xác định hành vi Website được giả thiết là các tấn công giả định theo 10 tiêu chí do OSWAP [12] đưa ra. Website được xếp vào loại HTTT có mức độ an toàn thấp nếu khi có tác động tấn công giả định nêu trên, hệ thống cho ra các đầu ra (hành vi phản ứng) gây ra những hậu quả nghiêm trọng, ảnh hưởng đến hoạt động của tổ chức có Website đó, và ảnh hưởng dây chuyền đến các dịch vụ Website đó cung cấp cho các hệ thống khác. Một Website điển hình có thể là Website quản trị thông tin cho điều hành công tác của một tổ chức, cung cấp thông tin điều hành cho các đơn vị khác trong tổ chức (các hệ thống thông tin con trong tổ chức đó). Nếu tác động tấn công vào Website không gây ra hành vi gì thì Website đó được xếp vào loại HTTT có mức độ an toàn cao, nghĩa là không gây ảnh hưởng gì (hoặc rất ít) đến hoạt động của tổ chức có Website.

Gọi $\boldsymbol{X}=x_i$ $(i=1…10)$ với x_i là các đầu vào tác động, i là một trong 10 tiêu chí được liệt kê trong [12].

Với mỗi i ta sẽ xác định được F_i . Nghĩa là

thực hiện việc đưa từng tham số đầu vào hệ thống để xác định hành vi tác động mà chúng gây ra như thế nào đối với hệ thống. Từ đó sẽ xác định được tập hành vi (đầu ra) của hệ thống.

Ví dụ với x_1 là tác động tấn công SQL Injection, khi đó cách thức thực hiện áp dụng mô hình lý thuyết hệ thống vào phân tích, phân loại Website sẽ như sau.

Tác động đầu vào: thực hiện thêm một ký tự ' vào sau đường dẫn URL của Website. Nếu xuất hiện thông báo lỗi thì xác định được hệ thống dính lỗi SQL Injection. Đây chính là một hành vi (đầu ra cho lại của hệ thống Website).

Các bước thực hiện đưa một tác động bên ngoài (giả lập tấn công SQL Injection) vào hệ thống Website và kiểm tra hành vi hệ thống (đầu ra phản ứng của Website) như sau:

- Xác định lỗ hổng SQL Injection trên Website.

- Sau khi đã xác định được lỗ hổng SQL Injection, tiến hành tìm tên cơ sở dữ liệu.

- Xác định được tên cơ sở dữ liệu, tìm tiếp tên các bảng có trong cơ sở dữ liệu.

- Xác định tên các cột trong bảng.

- Lấy thông tin dữ liệu từ bảng và cột.

- Tìm trang đăng nhập của admin hay trang quản lý CSDL và tiến hành đăng nhập.

Sau khi thực hiện từng bước như trên, ta quan sát kết quả đầu ra.

Kết quả đầu ra: Nếu lấy được tài khoản quản trị và chiếm quyền điều khiển hệ thống website thì mức an toàn của hệ thống được xem là mức thấp ($y_1 = 0$).

Nếu kết quả là không tồn tại lỗ hổng SQL thì mức độ an toàn của hệ thống Website được đánh giá mức cao ($y_1 = 1$).

Tương tự như vậy thực hiện với 10 lỗ hổng mà trong Top 10 OWASP đưa ra sẽ xác định được các đầu ra hành vi y_i. Khi đó $\boldsymbol{Y}$ sẽ là tổng của các y_i. Tùy vào mức độ an toàn Y, ta có thể dễ dàng phân chia giải giá trị và phân loại được mức độ an toàn của hệ thống theo các mức độ cao, trung bình, thấp.

V. KẾT LUẬN

Bài báo đã trình bày về vấn đề phân loại và đánh giá mức độ an toàn hệ thống thông tin. Bài báo đã nêu các cách phân loại thông tin và hệ thống thông tin phổ biến hiện nay dựa trên các bộ tiêu chí chung và các tiêu chuẩn. Các phương pháp phân loại truyền thống vẫn chủ yếu dựa vào định tính và có một số hạn chế trong áp dụng thực tế.

Từ quan điểm lý thuyết hệ thống, Bài báo này đưa ra một cách tiếp cận mới cho phân loại mức độ an toàn của hệ thống thông tin. Cách tiếp cận này có ưu điểm là kết hợp được việc xem xét tác động do mất an toàn thông tin với việc phân loại hệ thống thông tin. Tiếp đó, bài báo đã trình bày một ví dụ minh họa cách thức áp dụng bài toán phân tích hệ thống vào việc phân loại mức độ an toàn của một hệ thống Website.

TÀI LIỆU THAM KHẢO

[1] Common Methodology for Information Technology Security Evaluation, www.ssi.gov.fr/site_documents/CC/CEMv2.2.pdf

[2] CCWAPSS (Common Criteria Web Application Security Scoring)

[3] ISO 15408: Information Technology – Security Techniques–Evaluation Criteria for IT Security, Part 1, 2 and 3.

[4] NIST. Standards for Security Categorization of Federal Information and Information Systems. National Institute of Standards and Tęchnology, FIPS Publication 199

[5] NIST. Standards for Security Categorization of Federal Information and Information Systems. National Institute of Standards and Tęchnology, FIPS Publication 200.

[6] NIST Special Publication 800-60 Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories

[7] Andersson, Richard (2003), Evaluation of the Security of Components in Distributed Information Systems, LITH-ISY-EX-3430-2003, Linköping University, Sweden

[8] Hallberg, J., Hunstad, A,, Bond, A,, Peterson, M., Pihlsson, N., (2004). System IT Securiry Assessment, FOI-R-- 146&SE, Linkoping, Sweden

[9] Peterson, M. (2004). CAESAR - A proposed method for evaluating security in component-based distributed information systems. Master's Thesis. LITH-ISY-EX-3581-2004. Linkopings universitet

[10] R.M.Losee, A Discipline Independent Definition of Information, Journal of the American Society for Information Science, Vol.48(3), Nov.1998, p.1-31

[11] Nguyễn Văn Huân, Vũ Xuân Nam, Nguyễn Thu Hằng, Bài giảng lý thuyết hệ thống và điều khiển học, Trường ĐH CNTT và Truyền thông, 2012.

[12] https://www.owasp.org/