TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 8709-1 : 2011
ISO/IEC 15408-1:2009

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – CÁC TIÊU CHÍ ĐÁNH GIÁ AN TOÀN CNTT – PHẦN 1: GIỚI THIỆU VÀ MÔ HÌNH TỔNG QUÁT

Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part1: Introduction and General Model

HÀ NỘI - 2011

Mục lục

Lời nói đầu

TCVN 8709-1:2011 hoàn toàn tương đương ISO/IEC 15408-1:2008

TCVN 8709-1:2011 do Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Tiêu chuẩn này cho phép thực hiện so sánh các kết quả đánh giá an toàn độc lập. Tiêu chuẩn cung cấp một tập các yêu cầu chung về chức năng an toàn cho các sản phẩm công nghệ thông tin (CNTT), và về các biện pháp đảm bảo áp dụng cho các sản phẩm này trong quá trình đánh giá an toàn. Các sản phẩm CNTT này có thể dưới dạng phần cứng, phần sụn hay phần mềm.

Quy trình đánh giá thiết lập một mức tin cậy về việc các chức năng an toàn cho các sản phẩm CNTT và các biện pháp đảm bảo áp dụng cho chúng thỏa mãn các yêu cầu nêu trên. Các kết quả đánh giá có thể giúp người dùng xác định xem sản phẩm hoặc hệ thống CNTT có thỏa mãn yêu cầu đảm bảo an toàn của chúng hay không.

TCVN 8709 là một chỉ dẫn bổ ích cho phát triển, đánh giá và/hoặc đầu tư các sản phẩm CNTT với chức năng an toàn.

TCVN 8709 có tính mềm dẻo, cho phép áp dụng nhiều phương pháp đánh giá cho nhiều đặc tính an toàn của đa dạng sản phẩm CNTT. Chính vì vậy, người dùng tiêu chuẩn này cần thận trọng khi áp dụng để tránh lạm dụng nó. Ví dụ, nếu sử dụng TCVN 8709 kết hợp với các phương pháp đánh giá không phù hợp, các đặc tính an toàn không thích hợp, hoặc các sản phẩm CNTT không phù hợp sẽ dẫn đến các kết quả đánh giá vô nghĩa.

Do vậy, thực tế là một sản phẩm CNTT đã được đánh giá chỉ có ý nghĩa trong phạm vi ngữ cảnh các đặc tính an toàn được đánh giá với các phương pháp đánh giá cụ thể đã sử dụng. Các cơ quan đánh giá cần kiểm tra thận trọng các sản phẩm, đặc tính và các phương pháp để xác định rõ việc đánh giá đem lại kết quả có nghĩa. Ngoài ra, người mua các sản phẩm đã được đánh giá cũng cần xem xét kỹ lưỡng ngữ cảnh này để xác định xem sản phẩm đã đánh giá có hữu ích và áp dụng được cho trường hợp cụ thể của mình và đáp ứng yêu cầu hay không.

TCVN 8709 đề cập đến việc bảo vệ tài sản thông tin chống các truy nhập trái phép, các sửa đổi hoặc mất mát trong sử dụng. Phân loại bảo vệ liên quan đến ba kiểu lỗi an toàn kể trên tương ứng với tính bí mật, tính toàn vẹn và tính sẵn sàng. TCVN 8709 cũng có thể áp dụng cho các đánh giá ngoài ba nhóm trên. TCVN 8709 áp dụng cho các rủi ro phát sinh từ các hành vi của con người (ác ý hoặc lý do khác), và cho các rủi ro không do con người tạo ra. Ngoài an toàn CNTT, TCVN 8709 có thể áp dụng cho các lĩnh vực CNTT khác, song không có ràng buộc nào khi áp dụng cho các lĩnh vực đó.

Một số chủ đề do liên quan đến các kỹ thuật đặc biệt hoặc do chúng nằm ngoài lĩnh vực an toàn CNTT sẽ được coi là nằm ngoài phạm vi TCVN 8709. Một số chủ đề trong số đó như sau:

a) TCVN 8709 không gồm các tiêu chí đánh giá an toàn gắn liền với các biện pháp an toàn quản lý không liên quan trực tiếp tới chức năng an toàn CNTT. Tuy vậy, cũng phải thừa nhận rằng an toàn cơ bản thường đạt được thông qua hoặc được hỗ trợ bởi các biện pháp quản lý ví dụ về mặt tổ chức, nhân sự, vật lý và các thủ tục kiểm soát.

b) Đánh giá các khía cạnh vật lý kỹ thuật của an toàn CNTT ví dụ như kiểm soát dò rỉ thông tin qua điện từ trường không được đề cập riêng biệt, mặc dù nhiều khái niệm đã đề cập có thể áp dụng cho lĩnh vực này.

c) TCVN 8709 không đề cập đến hệ phương pháp đánh giá mà các tiêu chí này sẽ được áp dụng. Hệ phương pháp này được nêu trong ISO/IEC 18045.

d) TCVN 8709 không đề cập đến bộ khung pháp lý và quản lý mà các tiêu chí này sẽ được áp dụng bởi các cơ quan đánh giá. Tuy nhiên, có thể coi là TCVN 8709 sẽ được sử dụng cho các mục đích đánh giá trong ngữ cảnh các bộ khung đó.

e) Các thủ tục sử dụng các kết quả đánh giá để công nhận nằm ngoài phạm vi TCVN 8709. Công nhận là một quy trình quản lý trong đó cho phép quyền khai thác một sản phẩm CNTT (hoặc một tập các sản phẩm) trong mỗi trường hoạt động đầy đủ của nó bao gồm tất cả các phần phi-CNTT. Các kết quả của quy trình đánh giá là đầu vào cho quy trình công nhận. Tuy nhiên, do các kỹ thuật khác thường phù hợp hơn cho việc đánh giá các đặc tính phi- CNTT và mối quan hệ của chúng với các thành phần an toàn CNTT, việc công nhận cần xem xét riêng các khía cạnh này.

f) Chủ đề tiêu chí đánh giá cho chất lượng vốn có của các thuật toán mã hóa không nằm trong TCVN 8709. Nếu cần có đánh giá độc lập cho các đặc tính toán học của mã hóa, lược đồ đánh giá áp dụng TCVN 8709 sẽ phải cung cấp thêm các đánh giá này.

Các thuật ngữ ISO, như "có khả năng", "tham khảo","có thể", "bắt buộc", "cần" và "nên" sử dụng xuyên suốt trong văn bản tiêu chuẩn được định nghĩa trong Các chỉ thị ISO/IEC, phần 2. Lưu ý rằng khái niệm "nên" có nghĩa bổ sung khi áp dụng tiêu chuẩn này. Xem lưu ý dưới đây. Định nghĩa sau đây quy định việc sử dụng từ "nên" trong TCVN 8709.

Nên

Trong văn bản quy chuẩn, từ "nên" dùng để biểu thị "trong một số khả năng, có một khả năng được khuyến nghị là đặc biệt thích hợp mà không cần quan tâm hay loại trừ những khả năng khác, hoặc một diễn biến hành động nào đó được coi là ưa chuộng chứ không cần bắt buộc" (ISO/IEC Directives, Part 2).

CHÚ THÍCH: TCVN 8709 giải thích cụm từ "không cần bắt buộc" nghĩa là việc lựa chọn một khả năng khác đòi hỏi phải giải thích vì sao phương án ưa chuộng hơn không được chọn.

Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn CNTT –

Phần 1: Giới thiệu và mô hình tổng quát

Information Technology – Security Techniques – Evaluation Criteria for IT –

Part 1: Introduction and general model

1 Phạm vi áp dụng

Tiêu chuẩn này thiết lập các khái niệm và nguyên lý chung cho đánh giá an toàn CNTT và đặc tả mô hình đánh giá tổng quát tạo bởi các phần của tiêu chuẩn quốc tế một cách toàn diện, được sử dụng làm cơ sở cho đánh giá các thuộc tính an toàn của các sản phẩm CNTT.

Tiêu chuẩn này trình bày tổng quan về các phần của bộ TCVN 8709. Nó mô tả các phần của chuẩn; định nghĩa các khái niệm và các từ viết tắt sử dụng xuyên suốt trong toàn bộ các phần của tiêu chuẩn; thiết lập khái niệm cốt lõi về Đích đánh giá (TOE); ngữ cảnh đánh giá; mô tả đối tượng độc giả mà các tiêu chí đánh giá hướng đến. Tiêu chuẩn này cũng đưa ra các khái niệm an toàn cơ bản cần thiết cho việc đánh giá các sản phẩm CNTT.

Tiêu chuẩn định nghĩa các thao tác làm cơ sở để đưa ra các thành phần chức năng trong TCVN 8709-2 và các thành phần đảm bảo trong TCVN 8709-3 thông qua việc sử dụng các thao tác cho phép.

Các khái niệm cơ bản về Hồ sơ bảo vệ (PP), các gói yêu cầu an toàn và chủ đề về tính tuân thủ sẽ được nêu; các hệ quả đánh giá và các kết quả đánh giá cũng được mô tả. Phần này của tiêu chuẩn đưa ra hướng dẫn cho việc đặc tả Đích an toàn (ST) và cung cấp bản mô tả về tổ chức các thành phần xuyên suốt mô hình. Thông tin tổng quan về phương pháp luận đánh giá và phạm vi các lược đồ đánh giá được đưa ra trong ISO/IEC 18045.

2 Tài liệu viện dẫn

Tài liệu viện dẫn sau đây không thể thiếu được khi áp dụng tài liệu tiêu chuẩn này:

TCVN 8709 – 2, *"Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn CNTT – Phần 2: Các thành phần chức năng an toàn".*

TCVN 8709 – 3, *"Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn CNTT – Phần 3: Các thành phần đảm bảo an toàn".*

ISO/IEC 18045, *"Công nghệ thông tin – Các kỹ thuật an toàn – Hệ phương pháp cho đánh giá an toàn CNTT"* (ISO/IEC 18045, *"Information Technology – Security Techniques – Methodology for IT security evaluation").*

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa sau đây.

CHÚ THÍCH: Điều khoản này chỉ gồm các thuật ngữ sử dụng riêng trong TCVN 8709. Một số kết hợp của các thuật ngữ chung dùng trong TCVN không có trong điều khoản này sẽ được giải thích rõ trong ngữ cảnh nơi chúng được sử dụng.

3.1 Các thuật ngữ và định nghĩa chung trong TCVN 8709

3.1.1

Các hành động có hại (adverse actions)

Các hành động thực hiện bởi một tác nhân đe dọa vào một tài sản.

3.1.2

Tài sản (assets)

Các thực thể mà chủ sở hữu TOE đặt giá trị vào đó.

3.1.3

Chỉ định (assignment)

Định rõ một tham số định danh trong một thành phần (của TCVN 8709) hoặc một yêu cầu.

3.1.4

Bảo đảm (assurance)

Cơ sở để tin cậy rằng một TOE thỏa mãn các TSF.

3.1.5

Khả năng tấn công (attack potential)

Ước lượng về khả năng tấn công vào TOE biểu thị qua kinh nghiệm, tài nguyên và động cơ của kẻ tấn công.

3.1.6

Gia tăng (augmentation)

Việc thêm một hoặc nhiều yêu cầu vào một gói.

3.1.7

Dữ liệu xác thực (authentication data)

Thông tin được dùng để xác minh định danh đã tuyên bố của một người dùng.

3.1.8

Người dùng có thẩm quyền (authorised user)

Người dùng có thể thực thi một thao tác tương ứng với các SFR.

3.1.9

Lớp (class)

Tập các họ TCVN 8709 cùng chia sẻ một mục tiêu chung.

3.1.10

Tính mạch lạc (coherent)

Sắp sếp thứ tự logic, có nghĩa rõ ràng.

CHÚ THÍCH: Đối với tài liệu, thuật ngữ này dùng cho cả nội dung và cấu trúc của văn bản, biểu thị việc độc giả có hiểu được văn bản đó hay không.

3.1.11

Tính hoàn thiện (complete)

Tính chất thể hiện rằng tất cả các thành phần cần thiết của một thực thể đều được cung cấp.

CHÚ THÍCH: Đối với tài liệu, tính hoàn thiện nghĩa là mọi thông tin liên quan đều có trong tài liệu, ở mức độ chi tiết đến mức không cần có giải thích gì thêm.

3.1.12

Thành phần (component)

Tập nhỏ nhất lựa chọn được của các phần tử mà các yêu cầu có thể dựa vào.

3.1.13

Gói đảm bảo tổng hợp (composed assurance package)

Gói đảm bảo này gồm các yêu cầu rút ra từ TCVN 8709-3 (chủ yêu từ lớp ACO), biểu thị một điểm trong cấp độ đảm bảo tổng hợp đã định nghĩa trước trong TCVN 8709.

3.1.14

Xác nhận (confirm)

Công bố một việc đã được soát xét chi tiết với việc xác định tính đầy đủ một cách độc lập.

CHÚ THÍCH: Mức độ chính xác theo yêu cầu phụ thuộc vào bản chất của sự việc. Khái niệm trên chỉ áp dụng cho các hành động của đánh giá viên.

3.1.15

Tính kết nối (connectivity)

Đặc tính của TOE cho phép tương tác với các thực thể CNTT bên ngoài TOE.

CHÚ THÍCH: đặc tính này bao gồm việc trao đổi dữ liệu qua phương thức hữu tuyến hoặc vô tuyến, qua một khoảng cách bất kỳ trong một môi trường hoặc cấu hình bất kỳ.

3.1.16

Tính nhất quán (consistent)

Mối quan hệ giữa hai hoặc nhiều thực thể trong đó không có sự đối lập rõ rệt nào giữa chúng.

3.1.17

Chống đỡ (counter, verb)

Đối đầu với một tấn công, làm giảm thiểu tác động của mối đe dọa song không nhất thiết phải loại trừ nó.

3.1.18

Tính tuân thủ diễn giải được (demonstrable conformance)

Mối quan hệ giữa một ST và một PP, trong đó ST cung cấp một giải pháp để giải quyết vấn đề an toàn chung nêu trong PP.

CHÚ THÍCH: PP và ST có thể chứa các phát biểu khác nhau hoàn toàn mô tả về các thực thể, khai niệm,... khác nhau. Tính tuân thủ diễn giải được cũng thích hợp với một kiểu TOE khi tồn tại một số PP tương tự nhau, vì thế cho phép tác giả ST tuyên bố tuân thủ đồng thời theo các PP này để giúp tiết kiệm thời gian.

3.1.19

Sự chứng minh (demonstrate)

Đưa ra một kết luận rút ra từ việc phân tích, tuy có kém chặt chẽ hơn một "bằng chứng".

3.1.20

Tính phụ thuộc (dependency)

Mối quan hệ giữa các thành phần mà nếu trong đó một yêu cầu dựa trên thành phần phụ thuộc được đưa vào một PP, ST hoặc một gói thì yêu cầu dựa trên thành phần được phụ thuộc cũng thường phải được đưa vào PP, ST hoặc gói đó.

3.1.21

Mô tả (describe)

Cung cấp các chi tiết đặc trưng của một thực thể.

3.1.22

Xác định (determine)

Khẳng định một kết luận riêng dựa trên một phép phân tích độc lập với mục tiêu đạt được một kết luận cụ thể.

CHÚ THÍCH: Việc sử dụng khái niệm này ngầm chỉ một phép phân tích độc lập tin cậy, thường dùng khi thiếu phân tích trước đó. So sánh với các khái niệm"xác nhận" hay "thẩm tra" ngầm chỉ một phân tích đã thực hiện trước đó cần thiết phải soát xét lại.

3.1.23

Môi trường phát triển (development environment)

Môi trường để phát triển TOE.

3.1.24

Phần tử (element)

Phát biểu cơ bản nhất về một yêu cầu an toàn.

3.1.25

Bảo đảm (ensure)

Sự bảo đảm về mối quan hệ nhân quả chắc chắn giữa một hành động và các hệ quả của nó.

CHÚ THÍCH: Thuật ngữ này với từ „giúp" đặt trước sẽ biểu thị rằng hệ quả không hoàn toàn chắc chắn nếu chỉ có hành động đó.

3.1.26

Đánh giá (evaluation)

Đánh giá một PP, một ST hoặc một TOE theo các tiêu chí đã xác định.

3.1.27

Mức bảo đảm đánh giá (evaluation assurance level - EAL)

Tập các yêu cầu đảm bảo rút ra từ bộ TCVN 8709-3, biểu thị một điểm mốc trên cấp bậc bảo đảm được xác định trước trong TCVN 8709, tạo thành một gói đảm bảo.

3.1.28

Cơ quan đánh giá (evaluation authority)

Cơ quan thiết lập tiêu chuẩn và giám sát chất lượng các đánh giá được thực hiện bởi các đơn vị trong một cộng đồng cụ thể và là đơn vị thực thi TCVN 8709 cho cộng đồng thông qua một lược đồ đánh giá.

3.1.29

Lược đồ đánh giá (evaluation scheme)

Bộ khung quản lý và quy định về việc áp dụng TCVN 8709 cho một cơ quan đánh giá trong một cộng đồng cụ thể.

3.1.30

Thấu đáo (exhaustive)

Đặc trưng của một phương pháp tiếp cận được sử dụng để thực hiện một phân tích hoặc hoạt động theo một kế hoạch rõ ràng.

CHÚ THÍCH: Khái niệm này sử dụng trong TCVN 8709 chú trọng đến việc hướng dẫn phân tích hoặc các hoạt động khác. Nó liên quan đến tính hệ thống song được coi là mạnh hơn. Với nghĩa này, nó không chỉ biểu thị một cách tiếp cận có phương pháp đã được dùng để thực hiện phân tích hay thực hiện công việc theo một kế hoạch rõ ràng, mà còn biểu thị rằng kế hoạch này là đầy đủ để bảo đảm rằng đã thực hiện theo mọi con đường có thể.

3.1.31

Giải thích (explain)

Đưa ra luận cứ về lý do thực hiện một hành động.

3.1.32

Mở rộng (extension)

Bổ sung thêm vào một ST hoặc PP các yêu cầu chức năng không chứa trong TCVN 8709-2 và/hoặc các yêu cầu đảm bảo không chứa trong TCVN 8709-3.

3.1.33

Thực thể bên ngoài (external entity)

Một người dùng hay thiết bị CNTT có thể tương tác với TOE từ bên ngoài ranh giới TOE.

CHÚ THÍCH: Một thực thể bên ngoài có thể được coi là một người dùng.

3.1.34

Họ (family)

Một nhóm các thành phần cùng chia sẻ một mục tiêu giống nhau song khác nhau về tầm quan trọng hay tính chặt chẽ.

3.1.35

Hình thức (formal)

Cách biểu thị bằng một ngôn ngữ cú pháp hạn chế với ngữ nghĩa xác định trên cơ sở các khái niệm toán học được thiết lập rõ ràng.

3.1.36

Tài liệu hướng dẫn (guidance documentation)

Tài liệu mô tả về việc vận chuyển, chuẩn bị, vận hành, quản lý và/hoặc sử dụng cho TOE.

3.1.37

Định danh (identity)

Việc biểu diễn các thực thể (chẳng hạn như người dùng, tiến trình hoặc ổ đĩa) xác định duy nhất trong ngữ cảnh của TOE.

CHÚ THÍCH: Một ví dụ về việc biểu diễn này là một chuỗi ký tự. Đối với người dùng, biểu diễn có thể là tên đầy đủ, hoặc tên viết tắt hoặc một bí danh (duy nhất) của người dùng.

3.1.38

Không hình thức (informal)

Cách diễn tả bằng ngôn ngữ tự nhiên.

3.1.39

Vận chuyển giữa các TSF (inter TSF transfers)

Trao đổi dữ liệu giữa TOE với chức năng an toàn của các sản phẩm CNTT tin cậy khác.

3.1.40

Kênh truyền thông nội bộ (internal communication channel)

Kênh truyền thông giữa các phần tách biệt của TOE.

3.1.41

Vận chuyển nội bộ TOE (internal TOE transfer)

Trao đổi dữ liệu giữa các phần tách biệt của TOE.

3.1.42

Tính nhất quán nội bộ (internally consistent)

Là không có đối lập rõ nét nào trong mọi khía cạnh của một thực thể.

CHÚ THÍCH: Trong tài liệu, điều này có nghĩa là không có phát biểu nào đối lập với phát biểu khác.

3.1.43

Phép lặp (iteration)

Là việc sử dụng lặp lại một thành phần để thể hiện hai hoặc nhiều yêu cầu riêng biệt.

3.1.44

Biện minh (justification)

Là việc phân tích để đi đến một kết luận.

CHÚ THÍCH: Khái niệm "biện minh" chặt chẽ hơn là "diễn giải". Khái niệm này đòi hỏi tính chính xác đáng kể về việc giải thích một cách đặc biệt thận trọng và kỹ lưỡng từng bước cho một luận cứ logic.

3.1.45

Đối tượng (object)

Thực thể thụ động trong TOE có chứa hoặc tiếp nhận thông tin, mà dựa vào đó các chủ thể thực thi các hoạt động.

3.1.46

Hoạt động (operation)

(đối với một thành phần của TCVN 8709) là sự sửa đổi hoặc lặp lại một thành phần.

CHÚ THÍCH: Các hoạt động được phép cho thành phần là chỉ định, phép lặp, bổ sung chi tiết và lựa chọn.

3.1.47

Hoạt động (operation)

(đối với một đối tượng) là kiểu đặc trưng của một hành động do một chủ thể thực hiện trên một đối tượng.

3.1.48

Môi trường vận hành (operational environment)

Môi trường trong đó TOE hoạt động.

3.1.49

Chính sách an toàn của tổ chức (organizational security policy)

Tập các quy tắc, thủ tục, hoặc hướng dẫn an toàn cho một tổ chức.

CHÚ THÍCH: Một chính sách có thể chỉ áp dụng cho một môi trường vận hành cụ thể.

3.1.50

Gói (package)

Tập được đặt tên của các yêu cầu chức năng an toàn hoặc đảm bảo an toàn.

CHÚ THÍCH: Một ví dụ về gói là "EAL 3".

3.1.51

Đánh giá Hồ sơ bảo vệ (Protection Profile evaluation)

Đánh giá một PP theo các tiêu chí định sẵn.

3.1.52

Hồ sơ bảo vệ (Protection Profile - PP)

Phát biểu độc lập về mặt thực thi các yêu cầu cho một kiểu TOE.

3.1.53

Chứng minh (prove)

Chỉ ra sự phù hợp bằng việc phân tích hình thức theo cách tiếp cận toán học.

CHÚ THÍCH : Khái niệm này chính xác toàn diện theo mọi mặt. Điển hình, khái niệm chứng minh được dùng khi mong muốn chỉ ra sự phù hợp giữa 2 biểu diễn TSF ở một mức chính xác cao.

3.1.54

Tinh chỉnh (refinement)

Bổ sung thêm các chi tiết cho một thành phần.

3.1.55

Vai trò (role)

Một tập các quy tắc xác định trước để thiết lập các tương tác được phép giữa một người dùng và TOE.

3.1.56

Bí mật (secret)

Là thông tin chỉ được người có thẩm quyền và / hoặc TSF biết để thực thi một SFP cụ thể.

3.1.57

Trạng thái an toàn (secure state)

Trạng thái mà dữ liệu TSF là nhất quán và TSF tiếp tục thực thi chuẩn xác các SFR.

3.1.58

Thuộc tính an toàn (security attribute)

Các đặc tính của các chủ thể, người dùng (bao gồm các sản phẩm CNTT bên ngoài), đối tượng, thông tin, các phiên và/hoặc các tài nguyên được dùng cho việc xác định các SFR và các giá trị của chúng được dùng trong thực thi các SFR.

3.1.59

Chính sách chức năng an toàn (security function policy)

Tập các quy tắc mô tả hành vi an toàn cụ thể được thực thi bởi TSF và được biểu thị như một tập các SFR.

3.1.60

Mục tiêu an toàn (security objective)

Phát biểu về hướng đối phó với các mối đe dọa xác định và/hoặc hướng thỏa mãn các chính sách an toàn xác định của tổ chức cũng như hướng thỏa mãn các giả định.

3.1.61

Vấn đề an toàn (security problem)

Phát biểu dạng hình thức định nghĩa bản chất và phạm vi an toàn mà TOE chủ ý đề cập đến.

CHÚ THÍCH: Phát biểu là sự kết hợp của:

- Các mối đe dọa mà TOE cần chống trả,
- Các OSP được thực thi bởi TOE, và
- Các giả định đặt ra cho TOE và môi trường vận hành của nó.

3.1.62

Yêu cầu an toàn (security requirement)

Yêu cầu được phát biểu trong ngôn ngữ tiêu chuẩn, dùng để đạt được các mục tiêu an toàn cho một TOE.

3.1.63

Đích an toàn (Security Target - ST)

Phát biểu phụ thuộc thực thi về các yêu cầu cần thiết của một TOE xác định.

3.1.64

Lựa chọn (selection)

Việc định rõ một hoặc nhiều khoản mục từ một danh sách trong một thành phần.

3.1.65

Bán hình thức (semiformal)

Biểu thị bằng một ngôn ngữ cú pháp hạn chế với ngữ nghĩa xác định trước.

3.1.66

Đặc tả (specify)

Là đưa ra chi tiết đặc trưng về một thực thể theo một cách chính xác và chặt chẽ.

3.1.67

Tuân thủ chặt chẽ (strict conformance)

Mối quan hệ có thứ bậc giữa một PP và một ST trong đó mọi yêu cầu có trong PP thì cũng tồn tại trong ST.

CHÚ THÍCH: Mối quan hệ này có thể được xác định như „ST sẽ chứa tất cả các phát biểu có trong PP, nhưng có thể chứa thêm các phát biểu khác". Tuân thủ chặt chẽ dự kiến dùng cho các yêu cầu nghiêm ngặt và đơn giản là chúng cần được giữ gìn triệt để.

3.1.68

Đánh giá ST (ST evaluation)

Đánh giá một ST theo các tiêu chí định sẵn.

3.1.69

Chủ thể (subject)

Một thực thể chủ động thuộc TOE thực thi các thao tác trên đối tượng.

3.1.70

Đích đánh giá (target of evaluation - TOE)

Một tập phần mềm, phần sụn và/hoặc phần cứng cùng với tài liệu hướng dẫn nếu có.

3.1.71

Tác nhân đe dọa (threat agent)

Thực thể có thể gây tác động không mong muốn vào tài sản.

3.1.72

Đánh giá TOE (TOE evaluation)

Đánh giá một TOE theo các tiêu chí định sẵn.

3.1.73

Tài nguyên TOE (TOE resource)

Những gì được dùng hoặc tiêu tốn trong TOE.

3.1.74

Chức năng an toàn của TOE (TSF-TOE security functionality)

Tính năng kết hợp tất cả phần cứng, phần mềm, và phần sụn của TOE mà dựa vào đó TOE mới thực thi được chính xác các SFR.

3.1.75

Theo dấu (trace, verb)

Thực hiện phân tích phù hợp một cách không hình thức giữa hai thực thể chỉ ở mức độ chính xác tối thiểu.

3.1.76

Vận chuyển bên ngoài TOE (transfers outside of the TOE)

Trung chuyển dữ liệu đến các thực thể ngoài tầm kiểm soát của TSF.

3.1.77

Chuyển đổi (translation)

Quá trình mô tả các yêu cầu an toàn sang một ngôn ngữ tiêu chuẩn.

CHÚ THÍCH: Khái niệm chuyển đổi trong ngữ cảnh này không có nghĩa dịch thuật và không ngầm chỉ rằng mọi SFR biểu diễn trong ngôn ngữ chuẩn có thể được dịch ngược lại thành các mục tiêu an toàn.

3.1.78

Kênh tin cậy (trusted channel)

Phương tiện qua đó một TSF và một sản phẩm CNTT tin cậy khác có thể liên lạc với nhau ở độ tin cậy cần thiết.

3.1.79

Sản phẩm CNTT tin cậy (trusted IT product)

Sản phẩm CNTT – không phải là TOE – mà các yêu cầu chức năng an toàn của nó kết hợp về mặt quản trị với TOE và được giả thiết là để thực thi các yêu cầu chức năng an toàn của nó một cách chuẩn xác.

CHÚ THÍCH: Ví dụ về một sản phẩm CNTT tin cậy có thể là một sản phẩm đã được đánh giá tách biệt khác.

3.1.80

Đường dẫn tin cậy (trusted path)

Phương tiện để một người dùng và TSF có thể truyền thông với nhau ở mức tin tưởng cần thiết.

3.1.81

Dữ liệu TSF (TSF data)

Dữ liệu cho việc hoạt động mà TOE dựa vào để thực thi các SFR.

3.1.82

Giao diện TSF (TSF interface)

Phương tiện để một thực thể bên ngoài (hoặc chủ thể thuộc TOE nhưng nằm ngoài TSF) cung cấp dữ liệu cho TSF, nhận dữ liệu từ TSF và thực thi các dịch vụ từ TSF.

3.1.83

Dữ liệu người dùng (user data)

Dữ liệu dùng cho người dùng và không ảnh hưởng đến hoạt động của TSF.

3.1.84

Thẩm tra (verify)

Soát xét kỹ ở mức chi tiết với việc xác định độc lập về tính đầy đủ.

CHÚ THÍCH: Xem khái niệm "Xác nhận" (ở 3.1.14). Khái niệm „thẩm tra" có ý nghĩa chặt chẽ hơn. Nó được dùng trong ngữ cảnh các hành động của đánh giá viên, trong đó đòi hỏi sự nỗ lực độc lập của đánh giá viên.

3.2 Các thuật ngữ và định nghĩa liên quan đến lớp ADV

CHÚ THÍCH: Các khái niệm sau được dùng trong các yêu cầu đối với kiến trúc bên trong phần mềm. Một số khái niệm rút ra từ IEEE Std 610.12-1990 - Tập các khái niệm chuẩn trong công nghệ phần mềm của Viện Công nghệ Điện và Điện tử.

3.2.1

Người quản trị (administrator)

Thực thể có mức độ tin cậy tương ứng với mọi chính sách thực thi bởi TSF.

CHÚ THÍCH: Không phải tất cả PP hoặc ST giả định có cùng mức tin cậy cho người quản trị. Các nhà quản trị điển hình được coi là trung thành mọi lúc với các chính sách trong ST của TOE. Một số chính sách có thể liên quan đến chức năng của TOE, một số khác có thể liên quan đến môi trường vận hành.

3.2.2

Cây truy xuất (call tree)

Xác định các mô đun trong một hệ thống theo dạng biểu đồ, chỉ ra những mô đun nào gọi đến một mô đun khác.

CHÚ THÍCH: Vận dụng theo IEEE Std 610.12-1990.

3.2.3

Tính gắn kết (cohesion)

Cách thức và mức độ chặt chẽ của mô đun liên quan đến một mô đun khác của các tác vụ thực hiện

bởi một mô đun phần mềm đơn lẻ. (Theo IEEE Std 610-12-1990).

CHÚ THÍCH: Các kiểu gắn kết gồm: kiểu trùng hợp, truyền thông, tính năng, logic, tuần tự và tạm thời. Các kiểu gắn kết này được mô tả bởi một khái niệm tương ứng nêu trên.

3.2.4

Gắn kết trùng hợp (coincidental cohesion)

Mô đun với các đặc trưng của việc thực hiện các hành động liên quan hoặc liên quan lỏng lẻo. (Theo IEEE Std 610-12-1990).

CHÚ THÍCH: Xem khái niệm 3.2.3 ở trên.

3.2.5

Gắn kết truyền thông (communicational cohesion)

Mô đun chứa các chức năng tạo ra kết xuất cho hoặc dùng kết xuất lấy từ các chức năng khác trong cùng mô đun.

(Theo IEEE Std 610-12-1990).

CHÚ THÍCH 1: Xem khái niệm 3.2.3 ở trên.

CHÚ THÍCH 2: Ví dụ về một mô đun gắn kết truyền thông là mô đun kiểm tra truy nhập, mô đun này chứa các hàm kiểm tra bắt buộc, tùy biến và kiểm tra năng lực.

3.2.6

Độ phức tạp (complexity)

Đại lượng đo mức độ khó hiểu của phần mềm, khó để phân tích, kiểm thử và duy trì nó.

(Theo IEEE Std 610-12-1990).

CHÚ THÍCH: Giảm độ phức tạp là đích chung của việc sử dụng phương pháp phân rã mô đun, phân lớp và tối giản hóa. Ghép điều khiển và gắn kết có vai trò quan trọng để đạt mục đích này.

Một nỗ lực trong lĩnh vực công nghệ phần mềm đã thể hiện trong việc cố gắng phát triển các thước đo để đo lường độ phức tạp của mã nguồn. Hầu hết các thước đo này sử dụng các đặc tính dễ tính toán của mã nguồn như số các biểu thức và toán hạng, độ phức tạp của đồ thị luồng điều khiển (độ phức tạp vòng lặp), số các dòng mã nguồn, tỉ lệ chú giải so với mã thực hiện, và các thước đo tương tự khác. Các chuẩn mã hóa cũng đã được tìm ra để có công cụ hữu ích trong việc tạo mã sao cho dễ hiểu hơn.

Họ nội bộ TSF (ADV_INT) gọi đến một hàm phân tích độ phức tạp trong mọi thành phần của chúng. Kết quả dự kiến là nhà phát triển sẽ đưa ra hỗ trợ cho các đòi hỏi về việc đã có giảm đáng kể trong độ phức tạp. Hỗ trợ này có thể gồm các chuẩn lập trình cho nhà phát triển, và một chỉ số về việc mọi mô đun thỏa mãn tiêu chuẩn (hoặc có một số ngoại lệ được biện minh bằng các luận cứ công nghệ phần mềm). Nó có thể chứa các kết quả của các bộ công cụ dùng để đo lượng một số tính chất của mã nguồn, hoặc có thể chứa hỗ trợ khác cho nhà phát triển cần đến.

3.2.7

Ghép nối (coupling)

Cách thức và mức độ của sự không liên thuộc giữa các mô đun phần mềm.

(Theo IEEE Std 610-12-1990).

CHÚ THÍCH: Các kiểu ghép nối gồm ghép nối truy xuất, ghép nối chung và ghép nối nội dung (xem bên dưới).

3.2.8

Ghép nối truy xuất (call coupling)

Quan hệ giữa hai mô đun trao đổi với nhau một cách chặt chẽ qua các lời gọi hàm chức năng được ghi lại tài liệu.

CHÚ THÍCH: Ví dụ về ghép nối truy xuất là dữ liệu, nhãn tem và điều khiển. (Xem phần tiếp theo).

3.2.9

Ghép nối truy xuất (call coupling)

(về dữ liệu). Quan hệ dữ liệu giữa hai mô đun trao đổi chặt chẽ với nhau thông qua việc sử dụng các tham số biểu diễn các biểu thức dữ liệu đơn lẻ.

CHÚ THÍCH: Xem ghép nối truy xuất (3.2.8)

3.2.10

Ghép nối truy xuất (call coupling)

(về nhãn tem). Quan hệ về nhãn tem giữa hai mô đun trao đổi với nhau thông qua việc sử dụng các tham số lời gọi có chứa nhiều trường hoặc có các cấu trúc bên trong có nghĩa.

CHÚ THÍCH: Xem ghép nối truy xuất (3.2.8)

3.2.11

Ghép nối truy xuất (call coupling)

(về điều khiển). Quan hệ về điều khiển giữa hai mô đun nếu một mô đun chuyển thông tin mà nó định gửi để gây ảnh hưởng đến logic bên trong của mô đun kia.

CHÚ THÍCH: Xem ghép nối truy xuất (3.2.8)

3.2.12

Ghép nối chung (common coupling)

Quan hệ giữa hai mô đun cùng chia ser một vùng dữ liệu chung hoặc một tài nguyên hệ thống chung khác.

CHÚ THÍCH: Các biến toàn cục chỉ ra rằng các mô đun sử dụng các biến toàn cục này là các ghép nối chung. Ghép nối chung thông qua các biến toàn cục nhìn chung được phép, song chỉ ở mức độ hạn chế.

Ví dụ: Các biến được đặt trong một vùng toàn cục, song chỉ dùng trong một mô đun, sẽ coi là đặt chỗ sai và cần phải hủy bỏ. Các yếu tố khác cần được xem xét khi đánh giá mức độ phù hợp của các biến toàn cục là:

- Số các mô đun có sửa đổi một biến toàn cục: Nói chung, chỉ một mô đun đơn nên được cấp cho trách nhiệm kiểm soát nội dung của một biến toàn cục. Tuy nhiên có thể có các tình huống trong đó một mô đun thứ hai có thể chia sẻ trách nhiệm này. Trong tình hướng đó, cần có sự biện minh thỏa đáng. Không thể chấp nhận được việc chia sẻ trách nhiệm trên cho nhiều hơn hai mô đun. (Để thực hiện đánh giá này, cần thận trọng khi xác định mô đun thực sự có trách nhiệm đối với nội dung của biến. Ví dụ, nếu có 1 trình đơn lẻ dùng để sửa đổi biến này, song trình này đơn giản chỉ thực hiện việc sửa đổi theo yêu cầu của mô đun gọi đến nó, thì mô đun này là mô đun chịu trách nhiệm và

có thể có nhiều hơn một mô đun như vậy). Tiếp đó, về việc xác định độ phức tạp, nếu 2 mô đun có trách nhiệm đối với nội dung của biến toàn cục, cần có các chỉ số rõ ràng về mức độ phối hợp giữa các sửa đổi này.

- Số các mô đun có tham chiếu đến 1 biến toàn cục: Mặc dù nhìn chung không có hạn chế nào về số lượng các mô đun có tham chiếu đến 1 biến toàn cục, các trường hợp nhiều mô đun có tham chiếu tương tự sẽ cần được kiểm tra về tính hợp lệ và sự cần thiết.

3.2.13

Ghép nối nội dung (content coupling)

Quan hệ giữa hai mô đun trong đó một mô đun tạo tham chiếu trực tiếp đến nội dung bên trong của mô đun kia.

CHÚ THÍCH: Các ví dụ như: sửa đổi mã của - hoặc tham chiếu các nhãn nội bộ tới - mô đun khác. Kết quả là một số hoặc toàn bộ nội dung của một mô đun được ghép hiệu quả vào mô đun kia. Việc ghép nối nội dung có thể liên tưởng giống như việc sử dụng các giao diện mô đun không quảng cáo. Đây là cách đối lập với ghép nối truy xuất chỉ sử dụng các giao diện mô đun quảng cáo.

3.2.14

Phân cách miền (domain separation)

Đặc tính kiến trúc bảo an trong đó TSF định nghĩa các miền an toàn tách biệt cho mỗi người dùng và cho TSF và bảo đảm rằng không có một tiến trình người dùng nào có thể ảnh hưởng đến nội dung của một miền an toàn của người khác hoặc của TSF.

3.2.15

Gắn kết chức năng (functional cohesion)

Đặc tính của một mô đun để thực hiện các hành động liến quan đến một mục đích riêng.

(Theo IEEE Std 610-12-1990).

CHÚ THÍCH: Một mô đun gắn kết chức năng chuyển đổi một kiểu đơn của đầu vào thành một kiểu đơn đầu ra, ví dụ như một khối quản trị tác vụ hoặc quản trị hàng đợi (xem thêm tính gắn kết ở 3.2.3).

3.2.16

Tương tác (interaction)

Hoạt động dựa trên việc truyền thông chung giữa các thực thể.

3.2.17

Giao diện (interface)

Phương tiện tương tác với một thành phần hoặc một mô đun.

3.2.18

Phân lớp (layering)

Kỹ thuật thiết kế trong đó các nhóm mô đun tách biệt (các lớp) được tổ chức phân cấp để có trách nhiệm riêng biệt sao cho một lớp chỉ phụ thuộc vào dịch vụ các lớp bên dưới nó, và cung cấp dịch vụ

chỉ cho các lớp trên nó.

CHÚ THÍCH: Phân lớp chặt chẽ bổ sung điều kiện là mỗi lớp chỉ nhận dịch vụ từ lớp Ingay dưới nó và cung cấp dịch vụ chỉ cho lớp ngay trên nó.

3.2.19

Gắn kết logic, gắn kết thủ tục (logical cohesion, procedural cohesion)

Các đặc trưng của một mô đun thực hiện các động thái giống nhau trên các cấu trúc dữ liệu khác nhau.

CHÚ THÍCH: Một mô đun biểu thị gắn kết logic khi các chức năng của nó thực hiện các hành động liên quan – song khác biệt - ở các đầu ra khác nhau (xem tính gắn kết ở 3.2.3).

3.2.20

Phân tách mô đun (modular decomposition)

Quá trình chia một hệ thống ra nhiều thành phần để thuận tiện cho thiết kế, phát triển và đánh giá. (Theo IEEE Std 610-12-1990).

3.2.21

Khả năng không đi vòng (non-bypassability)

(của TSF) là đặc tính kiến trúc an toàn trong đó mọi hành động liên quan đến SFR được đều được trung chuyển qua TSF.

3.2.22

Miền an toàn (security domain)

Tập hợp tài nguyên mà một thực thể chủ động có đặc quyền truy nhập đến.

3.2.23

Gắn kết tuần tự (sequential cohesion)

Mô đun chứa các chức năng mà kết xuất của mỗi chức năng này là đầu vào cho chức năng tiếp theo trong mô đun.

(Theo IEEE Std 610-12-1990).

CHÚ THÍCH: Một ví dụ về mô đun gắn kết tuần tự là mô đun có chứa các chức năng để ghi các bản ghi kiểm toán và để duy trì một bộ đếm động về số lượng tích lũy các vi phạm kiểm chứng của một kiểu đặc trưng.

3.2.24

Công nghệ phần mềm (software engineering)

Ứng dụng cách tiếp cận định lượng, có hệ thống, có nguyên tắc cho việc phát triển và bảo trì phần mềm, nghĩa là ứng dụng kỹ thuật cho phần mềm.

(Theo IEEE Std 610-12-1990).

CHÚ THÍCH: Như với thực tiễn công nghệ nói chung, cần có một vài suy xét trong khi áp dụng các nguyên tắc kỹ thuật. Nhiều yếu tố ảnh hưởng đến việc chọn lựa, không chỉ việc ứng dụng các thước đo về việc phân tách mô đun, phân lớp và tối giản. Ví dụ, một nhà phát triển có thể thiết kế một hệ thống với các ứng dụng tương lai theo ý tưởng chúng vẫn chưa được triển khai từ khởi điểm. Nhà phát triển có thể chọn đưa vào một vài logic để xử lý các ứng dụng tương lai này mà không cần phải triển khai chúng một cách hoàn thiện. Tiếp đó, nhà phát triển có thể đưa vào một số lời gọi đến các mô đun thực sự vẫn chưa triển khai này, song chỉ là các lời gọi cụt (không thực hiện gì và quay về luôn). Sự biện minh của nhà phát triển về những sai lệch so với các chương trình có kiến trúc hoàn hảo sẽ cần được đánh giá có suy xét, so với việc áp dụng nguyên tắc công nghệ phần mềm.

3.2.25

Gắn kết tạm thời (temporal cohesion)

Các đặc trưng của một mô đun có chứa các chức năng cần thiết để thực hiện tại cùng thời điểm.

CHÚ THÍCH 1: Dựa theo IEEE Std 610-12-1990.

CHÚ THÍCH 2: Các ví dụ về mô đun gắn kết tạm thời gồm các mô đun khởi tạo, khôi phục và ngừng hoạt động.

3.2.26

Tự bảo vệ TSF (TSF self-protection)

Đặc tính kiến trúc an toàn trong đó TSF không thể bị gián đoạn bởi các mã của TSF khác hoặc bởi các thực thể khác.

3.3 Các thuật ngữ và định nghĩa liên quan đến lớp AGD

3.3.1

Cài đặt (installation)

Thủ tục thực hiện bởi người dùng đưa TOE vào môi trường vận hành của nó và đưa nó vào trạng thái hoạt động.

CHÚ THÍCH: Hoạt động này thường chỉ thực hiện một lần, sau khi nhận được và chấp thuận TOE. Dự kiến TOE tiến hành theo cấu hình cho phép bởi ST. Nếu các quá trình tương tự cần được nhà phát triển thực hiện, chúng được biểu thị là "khởi tạo" trong suốt quá trình hỗ trợ vòng đời ALC. Nếu TOE yêu cầu khởi động ban đầu mà không cần nhắc lại định kỳ, quá trình này được phân loại là cài đặt.

3.3.2

Hoạt động (operation)

Giai đoạn sử dụng TOE gồm: "sử dụng bình thường", quản trị và bảo dưỡng TOE sau khi chuyển giao và chuẩn bị.

3.3.3

Chuẩn bị (preparation)

Hoạt động trong giai đoạn vòng đời của một sản phẩm, bao gồm việc chấp thuận của khách hàng đối với TOE đã chuyển giao và cài đặt nó, có thể gồm cả những việc như khởi động, khởi tạo, thiết lập và tiến hành TOE đưa nó vào trạng thái sẵn sàng hoạt động.

3.4 Các thuật ngữ và định nghĩa liên quan đến lớp ALC

3.4.1

Các tiêu chí chấp thuận (acceptance criteria)

Các tiêu chí cần áp dụng khi thực hiện các thủ tục chấp thuận (ví dụ như soát xét thành công tài liệu, kiểm thử thành công về phần mềm, phần sụn hoặc phần cứng).

3.4.2

Các thủ tục chấp thuận (acceptance procedures)

Các thủ tục nối tiếp theo trình tự để chấp nhận các khoản mục cấu hình mới đã tạo lập hoặc đã sửa đổi cho TOE, hoặc để xóa bỏ chúng ở bước tiếp theo trong vòng đời.

CHÚ THÍCH: Các thủ tục này định dạng các vai trò hoặc trách nhiệm riêng đối với việc chấp thuận và các tiêu chí cần áp dụng để quyết định việc chấp thuận.

Có một số loại hình chấp thuận, một số có thể gối lên nhau, đó là:

a) Chấp thuận một khoản mục vào hệ thống quản lý cấu hình cho lần đầu, cụ thể gồm các thành phần phần mềm, phần sụn hay phần cứng từ các nhà sản xuất đưa vào TOE ("tích hợp").

b) Tiến hành các khoản mục cấu hình trong giai đoạn tiếp theo của vòng đời tại mỗi tầng kiến thiết TOE (ví dụ mô đun, hệ thống con, kiểm soát chất lượng của TOE hoàn chỉnh).

c) Kế tiếp với việc chuyển tải các khoản mục cấu hình (ví dụ các phần của TOE hoặc các sản phẩm ban đầu) giữa các địa điểm phát triển khác nhau.

d) Kế tiếp với việc chuyển giao TOE tới người tiêu dùng.

3.4.3

Quản lý cấu hình (Configuration management - CM)

Nguyên tắc áp dụng chỉ đạo và giám sát về mặt kỹ thuật và quản lý để định dạng và tài liệu hóa các đặc tính chức năng và vật lý của một khoản mục cấu hình, kiểm soát những thay đổi về những đặc tính này, ghi nhận và báo cáo sự thay đổi trạng thái xử lý và triển khai, kiểm chứng sự tuân thủ theo các yêu cầu đặc trưng.

CHÚ THÍCH: Dựa theo IEEE Std 610-12-1990.

3.4.4

Tài liệu CM (CM documentation)

Tất cả tài liệu CM bao gồm đầu ra CM, danh sách CM (danh sách cấu hình), các bản ghi hệ thống CM, kế hoạch CM và tài liệu sử dụng CM.

3.4.5

Bằng chứng quản lý cấu hình (configuration management evidence)

Là mọi thứ có thể dùng để thiết lập sự tin cậy trong hoạt động đúng của hệ thống CM.

CHÚ THÍCH: Ví dụ, đầu ra CM, các sở cứ hợp lý cung cấp bởi nhà phát triển, các quan sát, các thí nghiệm hoặc các phỏng

vấn tạo ra bởi đánh giá viên khi có mặt tại cơ sở.

3.4.6

Khoản mục cấu hình (configuration item)

Đối tượng quản lý bởi hệ thống CM trong quá trình phát triển TOE.

CHÚ THÍCH: Các khoản mục này có thể là các phần của TOE hoặc là các đối tượng liên quan đến việc phát triển TOE giống như các tài liệu đánh giá hoặc các công cụ phát triển. Các khoản mục CM có thể được lưu trữ trực tiếp trong hệ thống CM (ví dụ các tệp), hoặc qua tham chiếu (ví dụ các phần cứng) cùng với phiên bản của chúng.

3.4.7

Danh sách cấu hình (configuration list)

Tài liệu đầu ra quản lý cấu hình liệt kê mọi khoản mục cấu hình cho một sản phẩm đặc trưng cùng với phiên bản chính xác của mỗi khoản mục cấu hình tương ứng cho một phiên bản cụ thể của sản phẩm hoàn chỉnh.

CHÚ THÍCH: Danh sách này phân biệt phiên bản đã đánh giá của sản phẩm so với các phiên bản khác. Danh sách quản lý cấu hình là một tài liệu cụ thể cho một phiên bản cụ thể của một sản phẩm cụ thể. (Dĩ nhiên danh sách có thể là một tài liệu điện tử nằm trong một công cụ quản lý cấu hình. Trong trường hợp này, nó có thể coi là là một bản thuyết minh về hệ thống hoặc một phần của hệ thống hơn là phần kết xuất của hệ thống. Tuy nhiên, để sử dụng vào đánh giá, danh sách cấu hình có thể được chuyển giao như một phần của tài liệu đánh giá). Danh sách cấu hình định nghĩa các khoản mục thuộc các yêu cầu quản lý cấu hình của ALC_CMC.

3.4.8

Đầu ra quản lý cấu hình (configuration management output)

Các kết quả liên quan đến quản lý cấu hình, được tạo ra hoặc thực thi bởi hệ thống quản lý cấu hình.

CHÚ THÍCH: Các kết quả liên quan đến quản lý cấu hình này có thể là các tài liệu (ví dụ như các mẫu giấy tờ, các bản ghi hệ thống quản lý cấu hình, dữ liệu ghi nhật ký, các bản giấy sao chụp, dữ liệu kết xuất điện tử) cũng như các hành động (ví dụ các phép đo thủ công để thực hiện các lệnh quản lý cấu hình). Ví dụ về các đầu ra quản lý cấu hình như các danh sách cấu hình, các kế hoạch quản lý cấu hình, và/hoặc các hành vi trong vòng đời sản phẩm.

3.4.9

Kế hoạch quản lý cấu hình (configuration management plan)

Mô tả về việc hệ thống quản lý cấu hình được sử dụng cho TOE như thế nào.

CHÚ THÍCH: Mục tiêu của việc đưa ra một kế hoạch quản lý cấu hình là các nhân viên có thể thấy rõ họ cần làm gì. Từ quan điểm của hệ thống quản lý cấu hình nói chung, kế hoạch này có thể coi như một tài liệu kết xuất (vì nó có thể tạo ra như một phần ứng dụng của hệ thống quản lý cấu hình). Từ quan điểm của một dự án cụ thể, nó là một tài liệu sử dụng vì các thành viên của dự án sử dụng nó để hiểu được các bước cần thực hiện trong dự án. Kế hoạch quản lý cấu hình định nghĩa việc sử dụng hệ thống đối với một sản phẩm cụ thể; hệ thống này có thể mở rộng để dùng cho các sản phẩm khác. Nghĩa là kế hoạch quản lý cấu hình định nghĩa và mô tả đầu ra của một hệ thống quản lý cấu hình chọ một công ty sử dụng trong quá trình phát triển TOE.

3.4.10

Hệ thống quản lý cấu hình (configuration management system)

Tập các thủ tục và công cụ (bao gồm cả tài liệu của chúng) dùng bởi nhà phát triển để phát triển và bảo trì các cấu hình cho sản phẩm của họ trong vòng đời sản phẩm.

CHÚ THÍCH: Các hệ thống quản lý cấu hình có thể khác nhau về mức độ chặt chẽ và chức năng. Ở các mức cao, các hệ thống quản lý cấu hình có thể tự động hóa, với việc sửa chữa khiếm khuyết, kiểm soát thay đổi, và các cơ chế theo dấu khác.

3.4.11

Các bản ghi hệ thống quản lý cấu hình (configuration management system records)

Kết xuất tạo ra trong quá trình hoạt động của hệ thống quản lý cấu hình được tài liệu hóa, ghi lại các động thái quản lý cấu hình.

CHÚ THÍCH: Các ví dụ về bản ghi hệ thống quản lý cấu hình là các khuôn dạng điều khiển thay đổi khoản mục trong quản lý cấu hình hoặc các khuôn dạng phê duyệt truy nhập vào khoản mục quản lý cấu hình.

3.4.12

Các công cụ quản lý cấu hình (configuration management tools)

Các công cụ hoạt động thủ công hoặc tự động nhằm thực hiện hoặc hỗ trợ một hệ thống quản lý cấu hình.

CHÚ THÍCH: Ví dụ các công cụ cho quản lý phiên bản cho các phần của TOE.

3.4.13

Tài liệu sử dụng quản lý cấu hình (configuration management usage documentation)

Phần của hệ thống quản lý cấu hình dùng để mô tả hệ thống quản lý cấu hình được định nghĩa và áp dụng như thế nào. Ví dụ, các sổ tay, các quy định và/hoặc tài liệu về các công cụ và các thủ tục.

3.4.14

Chuyển giao (delivery)

Vận chuyển một TOE hoàn chỉnh từ môi trường sản xuất tới tay khách hàng.

CHÚ THÍCH: Giai đoạn vòng đời sản phẩm này bao gồm cả việc đóng gói và lưu trữ tại địa điểm phát triển, song không bao gồm việc vận chuyển TOE chưa hoàn chỉnh hoặc các phần của TOE giữa các nhà phát triển hoặc giữa các địa điểm phát triển khác nhau.

3.4.15

Nhà phát triển (developer)

Tổ chức có trách nhiệm với việc phát triển TOE.

3.4.16

Phát triển (development)

Giai đoạn trong vòng đời sản phẩm liên quan đến việc biểu thị sự triển khai TOE.

CHÚ THÍCH: Trong mọi yêu cầu ALC, khái niệm phát triển và các khái niệm liên quan (nhà phát triển, phát triển) có ý nghĩa chung bao hàm cả việc phát triển và sản xuất.

3.4.17

Các công cụ phát triển (development tools)

Các công cụ (bao gồm phần mềm kiểm thử nếu có) hỗ trợ việc phát triển và sản xuất TOE.

CHÚ THÍCH: Ví dụ cho một TOE phần mềm, các công cụ phát triển thường là các ngôn ngữ lập trình, các trình biên dịch, các trình liên kết và các công cụ tạo lập.

3.4.18

Mô tả triển khai (implementation representation)

Mô tả trừu tượng tối thiểu cho một TSF, đặc trưng cho việc tạo ra TSF mà không cần bổ sung chi tiết thiết kế nào thêm.

CHÚ THÍCH: Mã nguồn được biên dịch hoặc bản vẽ phần cứng dùng để tạo ra phần cứng cụ thể là các ví dụ về các thành phần của một bản mô tả triển khai.

3.4.19

Vòng đời (life-cycle)

Chuỗi các giai đoạn tồn tại của một đối tượng (ví dụ một sản phẩm hoặc một hệ thống) theo thời gian.

3.4.20

Định nghĩa vòng đời (life-cycle definition)

Định nghĩa cho một mô hình vòng đời.

3.4.21

Mô hình vòng đời (life-cycle model)

Mô tả các giai đoạn và mối quan hệ của chúng với các giai đoạn khác dùng cho việc quản lý vòng đời của một đối tượng nào đó, chỉ ra chuỗi các giai đoạn và các đặc tính mức cao của các giai đoạn cần phải như thế nào.

CHÚ THÍCH: Xem Hình 1.

3.4.22

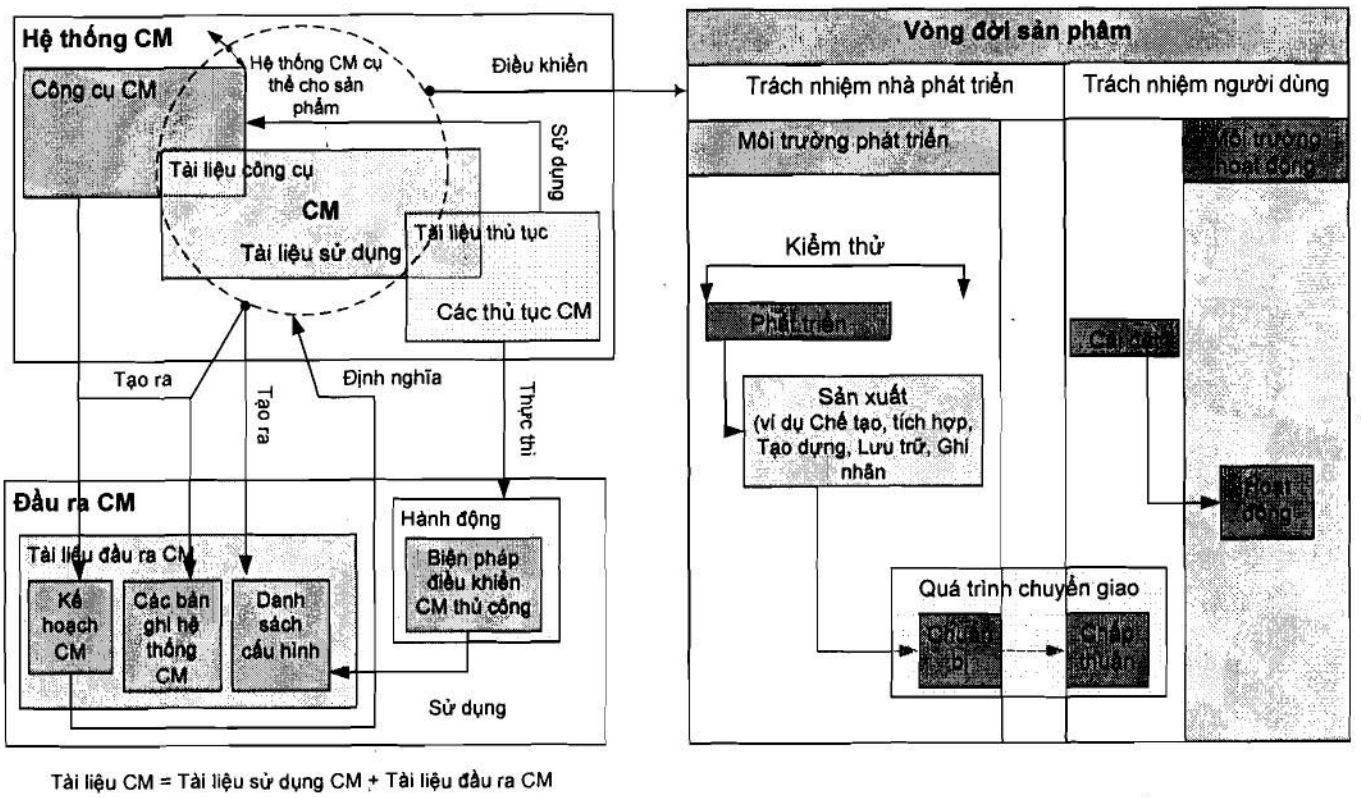
Sản xuất (production)

Giai đoạn vòng đời sản xuất kế tiếp giai đoạn phát triển và bao gồm việc chuyển tải bản mô tả triển khai vào việc triển khai cụ thể cho TOE, nghĩa là đưa nó vào trạng thái chấp nhận được để chuyển

giao cho khách hàng.

CHÚ THÍCH 1: Giai đoạn này gồm sản xuất, tích hợp, tạo lập, vận chuyển nội bộ, lưu trữ và ghi nhãn cho TOE.

CHÚ THÍCH 2: Xem thêm Hình 1.



Hình 1 – Các khái niệm trong CM và vòng đời sản phẩm

3.5 Các thuật ngữ và định nghĩa liên quan đến lớp AVA

3.5.1

Kênh bất hợp pháp (covert channel)

Kênh tín hiệu cưỡng ép trái phép, cho phép một người dùng lén lút vi phạm chính sách riêng biệt đa cấp và vi phạm các yêu cầu không quan sát được của TOE.

3.5.2

Các điểm yếu tiềm ẩn phải đối mặt (encountered potential vulnerabilities)

Các yếu điểm tiềm ẩn trong TOE có thể dùng để vi phạm các SFR được đánh giá viên nhận dạng trong khi thực hiện các hoạt động đánh giá.

3.5.3

Các điểm yếu có thể khai thác (exploitable vulnerability)

Các yếu điểm trong TOE có thể dùng để vi phạm các SFR trong môi trường vận hành của TOE.

3.5.4

Các tấn công giám sát (monitoring attacks)

Phân loại chung của các phương pháp tấn công có sử dụng các kỹ thuật phân tích thụ động nhằm phơi bày dữ liệu nhạy cảm bên trong TOE khi TOE hoạt động theo theo mô tả của các tài liệu hướng dẫn.

3.5.5

Các điểm yếu tiềm ẩn (potential vulnerability)

Các yếu điểm nghi vấn song chưa được khẳng định.

3.5.6

Các điểm yếu còn tồn tại (residual vulnerability)

Các yếu điểm không thể khai thác được trong môi trường vận hành của TOE, song một tin tặc có thể dùng để vi phạm các SFR với tiềm năng tấn công lớn hơn dự đoán trong môi trường vận hành của TOE.

3.5.7

Điểm yếu (vulnerability)

Yếu điểm trong TOE có thể dùng để vi phạm các SFR trong một số môi trường.

3.6 Các thuật ngữ và định nghĩa liên quan đến lớp ACO

3.6.1

Thành phần cơ sở (base component)

Thực thể trong một TOE tổng hợp, bản thân nó là chủ thể của một đánh giá, cung cấp dịch vụ và tài nguyên cho một thành phần phụ thuộc.

3.6.2

Tương thích (compatible)

(Thành phần) Là đặc tính của một thành phần về khả năng cung cấp các dịch vụ đòi hỏi bởi một thành phần khác, thông qua các giao diện phù hợp của mỗi thành phần trong môi trường vận hành nhất quán.

3.6.3

TOE thành phần (component TOE)

TOE đã được đánh giá thành công và là một phần của một TOE tổng hợp khác.

3.6.4

TOE tổng hợp (composed TOE)

TOE bao gồm hai hoặc nhiều thành phần đã được đánh giá thành công trước đó.

3.6.5

Thành phần phụ thuộc (dependent component)

Thực thể trong một TOE tổng hợp, bản thân nó là cơ quan của một đánh giá, dựa trên việc cung cấp dịch vụ bởi một thành phần cơ sở.

3.6.6

Giao diện chức năng (functional interface)

Giao diện với bên ngoài cung cấp cho người dùng khả năng truy xuất đến chức năng của một TOE không trực tiếp liên quan đến việc thực thi các yêu cầu chức năng an toàn.

CHÚ THÍCH: Trong một TOE tổng hợp có các giao diện cung cấp bởi thành phần cơ sở, được đòi hỏi bởi thành phần phụ thuộc để hỗ trợ hoạt động của TOE tổng hợp.

4 Ký hiệu và thuật ngữ viết tắt

Nội dung này liệt kê các thuật ngữ viết tắt trong tiêu chuẩn và các ký hiệu cần thiết để hiểu rõ hơn về tiêu chuẩn.

CHÚ THÍCH: Tiêu chuẩn này đưa ra các thuật ngữ bằng tiếng Việt, các thuật ngữ tiếng Anh tương đương và các thuật ngữ viết tắt tiếng Anh. Tuy chỉ có các thuật ngữ tiếng Việt mới được coi là của tiêu chuẩn, song các viết tắt thuật ngữ tiếng Anh giữ nguyên giúp cho việc tham chiếu tới tiêu chuẩn gốc thuận lợi hơn.

Viết tắt	Tiếng Anh tương đương	Tiếng Việt
API	Application Programming Interface	Giao diện lập trình ứng dụng
CAP	Composed Assurance Package	Gói đảm bảo tổng hợp
CM	Configuration Management	Quản lý cấu hình
CNTT	Information Technology (IT)	Công nghệ thông tin (CNTT)
DAC	Discretionary Access Control	Kiểm soát truy nhập tùy ý
EAL	Evaluation Assurance Level	Mức bảo đảm đánh giá
GHz	Gigahertz	Số đo tần số Gigahertz
GUI	Graphical User Interface	Giao diện người dùng dạng đồ họa
IC	Integrated Circuit	Mạch tích hợp
IOCTL	Input Output Control	Kiểm soát vào ra

IP	Internet Protocol	Giao thức Internet
IT	Information Technology	Công nghệ thông tin (CNTT)
MB	Mega Byte	Đơn vị thông tin Mega Byte (MB)
OS	Operating System	Hệ điều hành
OSP	Organizational Security Policy	Chính sách an toàn của tổ chức
PC	Personal Computer	Máy tính cá nhân
PCI	Peripheral Component Interconnect	Liên kết nối các thành phần ngoại vi
PKI	Public Key Infrastructure	Hạ tầng cơ sở khóa công khai
PP	Protection Profile	Hồ sơ bảo vệ
RAM	Random Access Memory	Bộ nhớ truy nhập ngẫu nhiên
RPC	Remote Procedure Call	Lời gọi thủ tục từ xa
SAR	Security Assurance Requirement	Yêu cầu đảm bảo an toàn
SF	Security Function	Chức năng an toàn
SFR	Security Functional Requirement	Yêu cầu chức năng an toàn
SFP	Security Function Policy	Chính sách chức năng an toàn
SPD	Security Problem Definition	Định nghĩa vấn đề an toàn
SOF	Strength of Function	Độ mạnh của chức năng
ST	Security Target	Đích an toàn
TCP	Transmission Control Protocol	Giao thức điều khiển truyền tải
TOE	Target of Evaluation	Đích đánh giá
TSC	TSF Scope of Control	Phạm vi giám sát TSF
TSF	TOE Security Functions	Các chức năng an toàn của TOE
TSFI	TSF Interface	Giao diện TSF
TSP	TOE Security Policy	Chính sách an toàn TOE
VPN	Virtual Private Network	Mạng riêng ảo

5 Tổng quan

5.1 Giới thiệu chung

Mục này giới thiệu các khái niệm chính của tiêu chuẩn TCVN 8709. Nó chỉ ra khái niệm "TOE", các đối tượng sử dụng tiêu chuẩn, và cách thức tiếp cận để trình bày tiêu chuẩn.

5.2 TOE

Tiêu chuẩn TCVN 8709 linh hoạt trong việc đánh giá, do đó không bị bó hẹp trong giới hạn các sản phẩm CNTT như đa số vẫn hiểu. Bởi vậy, trong ngữ cảnh đánh giá, tiêu chuẩn này sử dụng khái niệm "TOE" (Đích đánh giá).

Một TOE được định nghĩa là một tập phần mềm, phần sụn và/hoặc phần cứng có thể kèm theo hướng dẫn.

Trong một số trường hợp TOE gồm có một sản phẩm CNTT, song đó không phải là cần thiết. TOE có thể là một sản phẩm CNTT, một phần của một sản phẩm CNTT, một tập các sản phẩm CNTT, một công nghệ độc nhất có thể chẳng khi nào dùng để sản sinh ra một sản phẩm, hoặc một tổ hợp của các thành phần trên.

Trong liên quan đến TCVN 8709, quan hệ chính xác giữa TOE và bất kỳ sản phẩm CNTT nào chỉ quan trọng ở một khía cạnh: đánh giá cho một TOE chỉ chứa một phần sản phẩm CNTT cần không thể hiện sai là đánh giá cho toàn bộ sản phẩm CNTT đó.

Ví dụ về các TOE là:

- Một ứng dụng phần mềm;
- Một hệ điều hành;
- Một ứng dụng phần mềm kết hợp với một hệ điều hành;
- Một ứng dụng phần mềm kết hợp với một hệ điều hành và một trạm làm việc;
- Một hệ điều hành kết hợp với một trạm làm việc;
- Một mạch tổ hợp thẻ thông minh;
- Một bộ đồng xử lý mật mã của một mạch tổ hợp thẻ thông minh;
- Một mạng cục bộ bao gồm tất cả các đấu nối, máy chủ, thiết bị mạng và phần mềm;
- Một ứng dụng cơ sở dữ liệu ngoại trừ phần mềm máy khách từ xa thường kết hợp với ứng dụng cơ sở dữ liệu.

5.2.1 Các mô tả khác nhau về TOE

Trong TCVN 8709, một TOE có thể xuất hiện theo một số cách thể hiện khác nhau, ví dụ (đối với TOE là phần mềm):

- Một danh sách các tệp trong một hệ thống quản lý cấu hình.
- Một bản sao chính mới được biên dịch;
- Một hộp chứa CD-ROM và sách hướng dẫn để chuyển tới khách hàng;
- Một phiên bản hoạt động đã cài đặt.

Tất cả những thể hiện nêu trên đều được xem là TOE: mỗi khi khái niệm "TOE" được dùng trong phần còn lại của tiêu chuẩn này, ngữ cảnh sẽ xác định cách thể hiện của nó.

5.2.2 Các cấu hình khác nhau của TOE

Nói chung, các sản phẩm CNTT có thể được cấu hình theo nhiều cách: cài đặt theo các cách khác nhau, với các tùy chọn khác nhau hoặc mở hoặc chặn. Vì khi đánh giá với TCVN 8709, TOE sẽ được xác định xem có thỏa mãn các yêu cầu xác định không, sự mềm dẻo trong cấu hình này có thể dẫn đến các vấn đề, do tất cả mọi cấu hình có thể của TOE sẽ phải thỏa mãn các yêu cầu. Vì những lý do này, thông thường phần hướng dẫn TOE phải hạn chế các cấu hình có thể của TOE. Nghĩa là, hướng dẫn TOE có thể khác với hướng dẫn chung cho sản phẩm CNTT.

Một ví dụ là với sản phẩm CNTT là hệ điều hành. Sản phẩm này có thể được cấu hình theo nhiều cách (ví dụ các kiểu người dùng, số người dùng, kiểu các kết nối ra ngoài cho phép/cấm, các tùy chọn mở/chặn ...).

Nếu sản phẩm CNTT cũng chính là một TOE, và được đánh giá theo một tập hợp lý các yêu cầu, cấu hình cần được kiểm soát chặt chẽ hơn, vì nhiều tùy chọn (ví dụ cho phép mọi kiểu kết nối ngoài hoạc quản trị hệ thống không cần phải được xác thực) sẽ dẫn đến vấn đề TOE không thỏa mãn các yêu cầu.

Vì lý do này, thông thường sẽ có sự khác biệt giữa hướng dẫn cho sản phẩm CNTT (cho phép nhiều cấu hình) và hướng dẫn cho TOE (cho phép chỉ một hoặc chỉ những cấu hình không có sự khác biệt về phương thức an toàn thích hợp).

Lưu ý là nếu hướng dẫn cho TOE vẫn cho phép nhiều hơn một cấu hình, các cấu hình này được gọi chung là "cho TOE" và mỗi cấu hình như vậy phải thỏa mãn các yêu cầu tập trung vào TOE.

5.3 Đối tượng sử dụng TCVN 8709

Ba nhóm người có mối quan tâm chung trong đánh giá các thuộc tính an toàn của các sản phẩm và hệ thống CNTT là: Người tiêu dùng TOE, nhà phát triển TOE và đánh giá viên TOE. Các tiêu chí được trình bầy trong tài liệu này được xây dựng để hỗ trợ nhu cầu của cả ba nhóm trên. Họ được xem là người dùng chính của TCVN 8709. Lợi ích mà ba nhóm này có được từ các tiêu chí được liệt kê ra sau đây.

5.3.1 Người tiêu dùng

Tiêu chuẩn này được biên soạn nhằm đảm bảo rằng, việc đánh giá thỏa mãn các nhu cầu của người tiêu dùng vì đó là mục đích cơ bản và là biện minh cho quy trình đánh giá.

Người tiêu dùng có khả năng sử dụng kết quả đánh giá để giúp quyết định xem sản phẩm hoặc hệ thống đã đánh giá có thỏa mãn các nhu cầu an toàn của họ hay không. Những nhu cầu an toàn này thường được xác định qua kết quả của cả việc phân tích rủi ro và định hướng chính sách. Người tiêu dùng cũng có thể sử dụng các kết quả đánh giá để so sánh các TOE khác nhau.

TCVN 8709 mang lại cho người tiêu dùng - đặc biệt cho các nhóm người tiêu dùng và cộng đồng quan tâm - một cấu trúc độc lập với việc triển khai, được gọi là Hồ sơ bảo vệ (Protected Profile - PP), trong đó biểu thị các yêu cầu của họ về an toàn theo một cách rõ ràng.

5.3.2 Các nhà phát triển

TCVN 8709 hỗ trợ các nhà phát triển trong việc chuẩn bị và trợ giúp đánh giá các sản phẩm hoặc hệ thống, trong xác định các yêu cầu an toàn cần thỏa mãn cho các TOE. Các yêu cầu này được chứa trong một kết cấu phụ thuộc vào việc triển khai, được gọi là Đích An toàn (ST). Kết cấu ST này có thể

dựa vào một hoặc nhiều PP để chỉ ra rằng ST tuân thủ các yêu cầu an toàn từ phía người tiêu dùng như đã sắp đặt trong các PP này.

TCVN 8709 có thể dùng để xác định trách nhiệm và các hành động để cung cấp bằng chứng cần thiết cho việc hỗ trợ đánh giá TOE theo các yêu cầu trên. Nó cũng định nghĩa nội dung và cách thể hiện của bằng chứng này.

5.3.3 Đánh giá viên

TCVN 8709 chứa các tiêu chí được đánh giá viên sử dụng khi lập ra các phán xét về sự tuân thủ của các TOE theo các yêu cầu an toàn của chúng. TCVN 8709 mô tả một tập hợp các công việc chung mà đánh giá viên cần thực hiện và các chức năng an toàn, căn cứ theo đó để thực hiện các công việc trên. Lưu ý là TCVN 8709 không chỉ ra các thủ tục hướng dẫn thực hiện các công việc này. Xem thêm thông tin về các thủ tục này ở Mục 5.5.

5.3.4 Các đối tượng khác

TCVN 8709 hướng tới việc định rõ và đánh giá các thuộc tính an toàn CNTT của các TOE, đồng thời nó cũng có thể là một tài liệu tham khảo hữu ích cho tất cả những ai quan tâm đến hoặc có trách nhiệm về an toàn CNTT. Một vài nhóm đối tượng quan tâm khác cũng có khả năng có lợi ích từ các thông tin trong TCVN 8709 bao gồm:

a) Các nhân viên bảo vệ hệ thống và các nhân viên an toàn hệ thống, những người có trách nhiệm trong việc xác định và đáp ứng các chính sách và yêu cầu an toàn CNTT cho tổ chức.

b) Các kiểm toán viên, cả bên trong và bên ngoài, có trách nhiệm lượng giá mức tương xứng về an toàn của một hệ thống.

c) Các nhân viên thiết kế và xây dựng hệ thống, có trách nhiệm định rõ nội dung an toàn cho các sản phẩm và hệ thống CNTT.

d) Những người được ủy quyền, có trách nhiệm chấp thuận việc một giải pháp CNTT đưa vào sử dụng trong một môi trường cụ thể.

e) Những người bảo trợ đánh giá, có trách nhiệm yêu cầu và hỗ trợ việc đánh giá.

f) Các cơ quan đánh giá, có trách nhiệm quản lý và giám sát các chương trình đánh giá an toàn CNTT.

5.4 Các phần khác nhau của bộ tiêu chuẩn

TCVN 8709 được trình bày dưới dạng một tập hợp ba phần riêng biệt song có liên quan như tóm tắt dưới đây. Các thuật ngữ sử dụng để mô tả các phần này được giải thích trong Điều 6.

a) **Phần 1 (TCVN 8709-1): Giới thiệu và mô hình tổng quát**, là phần giới thiệu về TCVN 8709. Trong đó có định nghĩa các khái niệm và nguyên tắc chung cho đánh giá an toàn CNTT, và trình bày một mô hình tổng quát cho đánh giá.

b) **Phần 2 (TCVN 8709-2): Các thành phần chức năng an toàn**, xây dựng một tập các thành phần chức năng an toàn theo cách biểu diễn chuẩn hóa các yêu cầu chức năng cơ bản cho các đích đánh giá (TOE). Phần 2 phân loại tập hợp các thành phần chức năng, các họ và các lớp.

c) **Phần 3 (TCVN 8709-3): Các thành phần đảm bảo an toàn**, xây dựng một tập các thành phần đảm bảo an toàn theo cách biểu diễn chuẩn hóa các yêu cầu đảm bảo cơ bản cho các đích đánh giá (TOE). Phần 3 phân loại tập hợp các thành phần đảm bảo, các họ và các lớp. Phần 3 cũng định nghĩa các tiêu chí đánh giá cho các Hồ sơ bảo vệ (PP) và các Đích An toàn (ST), và trình bày 7 gói đảm bảo định nghĩa trước gọi là các Mức đảm bảo đánh giá (EAL).

Để hỗ trợ ba phần của tiêu chuẩn như nêu ở trên, các tài liệu khác cũng đã được công bố, ví dụ ISO/IEC 18045 cung cấp hệ thống phương pháp cho đánh giá an toàn CNTT sử dụng ISO/IEC 15408 làm cơ sở. Dự đoán là sẽ có thêm các tài liệu khác được công bố, bao gồm các tư liệu sơ cứ kỹ thuật và các tài liệu hướng dẫn.

Bảng dưới đây biểu diễn ba nhóm đối tượng sử dụng tiêu chuẩn chủ chốt, dựa trên mức độ quan tâm đến các phần của tiêu chuẩn TCVN 8709:

	Người tiêu dùng	**Nhà phát triển**	**Đánh giá viên**
Phần 1	Dùng làm thông tin cơ sở và bắt buộc sử dụng để tham chiếu. Cấu trúc hướng dẫn cho các PP.	Dùng làm thông tin cơ sở và tham chiếu. Bắt buộc sử dụng để phát triển các đặc tả an toàn cho các TOE.	Bắt buộc sử dụng để tham chiếu và hướng dẫn trong cấu trúc cho các PP và các ST.
Phần 2	Dùng để hướng dẫn và tham chiếu khi lập các phát biểu về yêu cầu các chức năng an toàn của một TOE	Dùng để tham chiếu khi diễn giải các phát biểu về yêu cầu chức năng, và khi lập các đặc tả chức năng cho các TOE.	Bắt buộc sử dụng để tham chiếu khi diễn giải các phát biểu về các yêu cầu chứç năng.
Phần 3	Dùng để hướng dẫn khi xác định cấp bảo đảm yêu cầu.	Dùng để tham chiếu khi diễn giải các phát biểu về yêu cầu đảm bảo, và khi xác định các cách đảm bảo các TOE.	Dùng để tham chiếu khi diễn giải các phát biểu về các yêu cầu đảm bảo.

Bảng 1 - Cấu trúc "Các tiêu chí đánh giá an toàn CNTT"

5.5 Ngữ cảnh đánh giá

Để đạt được sự so sánh rõ rệt giữa các kết quả đánh giá, các đánh giá cần được thực hiện trong khuôn khổ một lược đồ đánh giá có thẩm quyền. Lưu đồ đó đặt ra các tiêu chuẩn, giám sát chất lượng các đánh giá và quản lý các điều chỉnh mà các nhà đánh giá và các phương tiện đánh giá cần phải tuân thủ theo.

TCVN 8709 không nêu rõ các yêu cầu về bộ khung điều chỉnh. Mặc dù vậy, sự nhất quán giữa các bộ khung điều chỉnh của những người có thẩm quyền đánh giá khác nhau là cần thiết để đạt được mục tiêu công nhận lẫn nhau cho các kết quả đánh giá.

Một cách thứ hai để đạt được tính tương thích nhiều hơn giữa các kết quả đánh giá là sử dụng hệ phương pháp luận chung để đạt các kết quả này. Hệ phương pháp này được công bố trong tiêu chuẩn ISO/IEC 18045 cho tiêu chuẩn TCVN 8709.

Sử dụng một hệ phương pháp đánh giá chung giúp làm tăng khả năng lặp lại và tính khách quan của các kết quả, tuy nhiên như vậy vẫn chưa đủ. Nhiều tiêu chí đánh giá đòi hỏi vận dụng suy xét chuyên gia và kiến thức cơ bản, khi đó sẽ khó khăn hơn để đạt được sự nhất quán. Để nâng cao sự nhất quán của các nhận xét đánh giá, các kết quả đánh giá cuối cùng cần được thông qua một quy trình chứng nhận.

Quy trình chứng nhận là việc thanh tra độc lập các kết quả đánh giá, dẫn đến đưa ra chứng nhận cuối cùng hoặc công nhận. Chứng nhận thường được đưa ra công khai. Điều này chỉ ra rằng quy trình chứng nhận là một cách để đạt được một sự nhất quán hơn khi ứng dụng các tiêu chí an toàn CNTT.

Lược đồ đánh giá và các quy trình chứng nhận là trách nhiệm của những cơ quan đánh giá khi thực hiện các lược đồ đánh giá và không thuộc phạm vi của TCVN 8709.

6 Mô hình tổng quát

6.1 Giới thiệu mô hình tổng quát

Phần này trình bày các khái niệm chung được sử dụng trong TCVN 8709, bao gồm ngữ cảnh trong đó các khái niệm được sử dụng và cách thức TCVN 8709 áp dụng các khái niệm này. TCVN 8709-2 và TCVN 8709-3 là các tài liệu bắt buộc người dùng phần 1 của tiêu chuẩn TCVN 8709 phải tư vấn. Chúng mở rộng việc sử dụng các khái niệm này và giả định cách tiếp cận trên được dùng. Ngoài ra, đối với người dùng tiêu chuẩn TCVN 8709-1 nhằm thực hiện các hoạt động đánh giá, tiêu chuẩn ISO/IEC 18045 có thể áp dụng. Phần này giả thiết một số hiểu biết về an toàn CNTT và không dự định thực hiện vai trò hướng dẫn trong lĩnh vực này.

TCVN 8709 bàn về an toàn dựa trên một tập các khái niệm và thuật ngữ an toàn. Hiểu biết các khái niệm và thuật ngữ này được xem như một điều kiện tiên quyết để sử dụng hiệu quả TCVN 8709. Mặc dù vậy, bản thân các khái niệm này rất tổng quát, không dự kiến hạn chế sử dụng chỉ cho lớp các vấn đề an toàn CNTT mà trong đó TCVN 8709 được áp dụng.

6.2 Tài sản và các biện pháp đối phó

An toàn liên quan đến việc bảo vệ các tài sản. Các tài sản là các thực thể mà ai đó có thể đặt giá trị vào đó. Ví dụ về các tài sản là:

- Các nội dung của một tệp hay một máy chủ;
- Tính xác thực của việc bỏ phiếu trong một cuộc bầu cử;
- Tính khả dụng của một qy trình thương mại điện tử;
- Khả năng sử dụng một máy in đắt tiền;
- Truy nhập vào một tiện nghi đã phân loại tính mật.

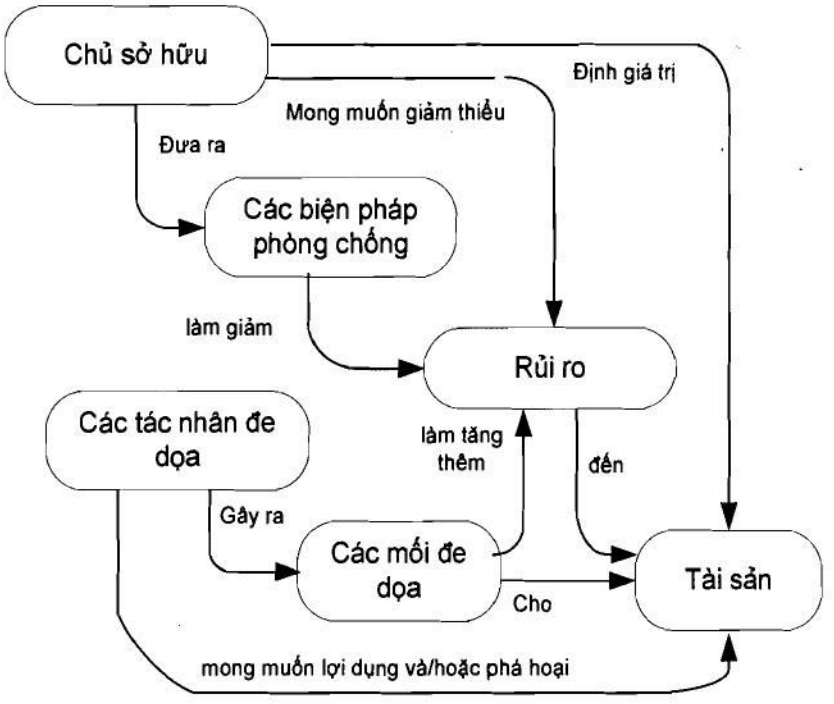
Tuy vậy, do các giá trị có tính chủ quan cao, hầu hết các thứ đều có thể là một tài sản.

(Các) môi trường trong đó các tài sản này được đặt, được gọi là môi trường vận hành. Ví dụ về (các khía cạnh của) môi trường vận hành là:

- Phòng máy tính của một ngân hàng;
- Một mạng máy tính kết nối với Internet;
- Một mạng cục bộ (LAN);

- Một môi trường công sở nói chung.

Rất nhiều tài sản ở dạng thông tin được lưu trữ, xử lý, truyền tải bởi các sản phẩm CNTT để thỏa mãn các yêu cầu đặt ra bởi các chủ sở hữu thông tin. Các chủ sở hữu thông tin có thể yêu cầu là tính khả dụng, phổ biến và sửa đổi của bất kỳ thông tin nào kể trên cần được kiểm soát chặt chẽ và các tài sản cần được bảo vệ chống các mối đe dọa bằng các biện pháp đối phó. Hình 2 minh họa cho các khái niệm và các mối quan hệ mức cao.



Hình 2 - Các khái niệm và quan hệ về an toàn

Đảm bảo an toàn cho tài sản là trách nhiệm của người chủ sở hữu, người đưa các giá trị vào các tài sản đó. Các tác nhân đe dọa hiện hữu hoặc dự đoán cũng có thể đưa các giá trị vào tài sản và tìm cách lạm dụng tài sản theo cách trái ngược với lợi ích của chủ sở hữu. Ví dụ về các tác nhân đe dọa là các tin tặc, kẻ ác ý, những người vô ý (những người đôi lúc gây lỗi), các tiến trình và các tai họa trong máy tính.

Chủ sở hữu sẽ nhận thức được các đe dọa đó là một nguy cơ tổn hại đến các tài sản cũng như làm giảm giá trị các tài sản của họ. Những tổn hại đặc trưng về an toàn nói chung bao gồm, song không chỉ giới hạn ở: mất tính bí mật của tài sản, mất tính toàn vẹn của tài sản và mất tính sẵn sàng của tài sản.

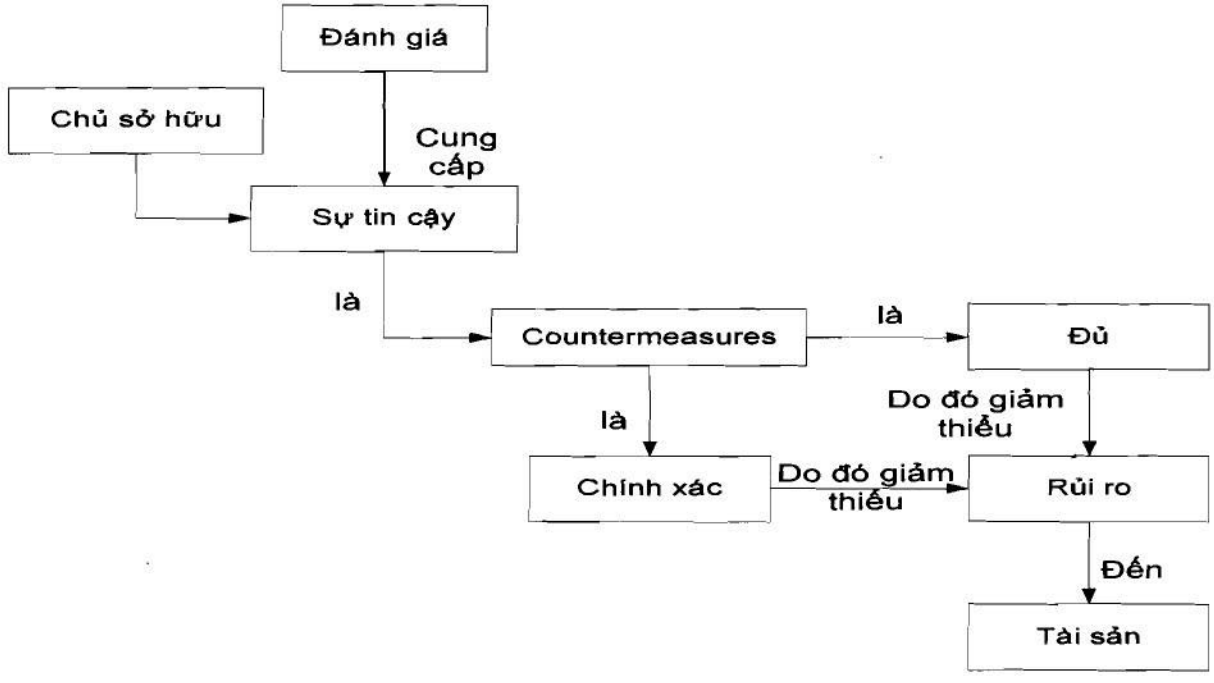
Các mối đe dọa nêu trên sẽ làm gia tăng các rủi ro cho tài sản, dựa trên khả năng một đe dọa đang hình thành và ảnh hưởng vào tài sản khi môi đe dọa được hình thành. Các biện pháp đối phó tiếp theo sẽ được đưa ra nhằm giảm thiểu rủi ro cho các tài sản. Các biện pháp đối phó này có thể gồm các biện pháp đối phó thuộc CNTT (như các tường lửa hay thẻ thông minh) hay các biện pháp đối phó phi-CNTT (như bảo vệ và các quy trình). Có thể xem thêm tiêu chuẩn ISO/IEC 27001 và ISO/IEC 27002 để có thêm thông tin về các biện pháp đối phó an toàn (các điều khiển) và việc triển khai và quản lý chúng như thế nào.

Các chủ sở hữu tài sản có thể chịu trách nhiệm về các tài sản trên và do vậy cần có khả năng bảo vệ quyết định chấp nhận các rủi ro phơi bày tài sản trước các mối đe dọa.

Có hai thành phần quan trong trong việc bảo vệ quyết định này có thể diễn giải, đó là:

- Các biện pháp đối phó là vừa đủ: Nếu các biện pháp đối phó thực hiện theo những gì chúng đặt ra để thực hiện, các mối đe dọa đối với tài sản được ngăn chặn.
- Các biện pháp đối phó là chính xác: Các biện pháp đối phó thực hiện đúng những gì chúng đặt ra để thực hiện.

Nhiều chủ sở hữu tài sản thiếu nhận thức, kinh nghiệm hay tài nguyên cần thiết để suy xét mức độ đầy đủ và chính xác của các biện pháp đối phó, và họ có thể không muốn chỉ đơn thuần dựa vào sự xác nhận của của các nhà phát triển các biện pháp đối phó. Những người tiêu dùng này, do vậy, có thể chọn cách tăng độ tin cậy trong mức độ đủ và chính xác của một số hoặc toàn bộ các biện pháp đối phó thông qua việc đặt hàng đánh giá các biện pháp đối phó này.



Hình 3 - Các khái niệm và quan hệ trong đánh giá

6.2.1 Tính đầy đủ của các biện pháp đối phó

Trong khi đánh giá, tính đầy đủ của các biện pháp đối phó được phân tích thông qua một kết cấu gọi là Đích an toàn (ST). Mục này trình bày một cách sơ lược về kết cấu này, chi tiết và mô tả đầy đủ về ST có thể xem trong Phụ lục A.

Đích an toàn bắt đầu bằng việc mô tả các tài sản và các mối đe dọa tới chúng. Tiếp đó, Đích an toàn mô tả các biện pháp đối phó (dưới dạng các Mục tiêu an toàn) và diễn giải rằng các biện pháp đối phó này là đủ để chống lại các mối đe dọa kể trên: Nếu các biện pháp đối phó thực hiện những gì chúng cần phải thực hiện, các mối đe dọa sẽ được ngăn chặn.

Tiếp theo, Đích an toàn chia các biện pháp đối phó này thành hai nhóm:

a) Các mục tiêu an toàn cho TOE: Đây là mô tả các biện pháp đối phó mà tính chính xác sẽ được xác định trong khi đánh giá;

b) Các mục tiêu an toàn cho môi trường vận hành: Đây là mô tả các biện pháp đối phó mà tính chính xác sẽ không được xác định trong khi đánh giá;

Lý do để chia ra hai nhóm trên như sau:

- TCVN 8709 chỉ thích hợp cho việc đánh giá tính chính xác của các biện pháp đối phó thuộc CNTT. Do đó các biện pháp đối phó phi- CNTT (ví dụ như nhân viên bảo vệ, quy trình) luôn thuộc về môi trường vận hành.
- Việc đánh giá tính chính xác của các biện pháp đối phó tiêu tốn thời gian và tiền bạc, có thể làm nó bất khả thi trong việc đánh giá cho tất cả các biện pháp đối phó thuộc CNTT.
- Tính chính xác của một số biện pháp đối phó thuộc CNTT có thể đã được đánh giá trong một quá trình đánh giá khác. Bởi vậy, để hiệu quả, không cần phải đánh giá lại một lần nữa.

Đối với TOE (các biện pháp đối phó thuộc CNTT với tính chính xác sẽ được đánh giá trong quá trình đánh giá), Đích an toàn đòi hỏi có thêm chi tiết về các mục tiêu an toàn cho TOE trong các yêu cầu chức năng an toàn (SFR). Các SFR này được trình bày trong một ngôn ngữ chuẩn (mô tả trong TCVN 8709-2) để bảo đảm sự chính xác và dễ tương thích.

Tóm lại, Đích an toàn diễn giải:

- Các SFR thỏa mãn các mục tiêu an toàn cho TOE;
- Các mục tiêu an toàn cho TOE và các mục tiêu an toàn cho môi trường vận hành ngăn chặn các mối đe dọa;
- Và do vậy, các SFR cũng như các mục tiêu an toàn cho môi trường vận hành ngăn chặn các mối đe dọa.

Từ đây suy ra rằng, một TOE đúng (thỏa mãn các SFR) trong sự kết hợp với một môi trường vận hành đúng (thỏa mãn các mục tiêu an toàn cho môi trường vận hành) sẽ ngăn chặn các mối đe dọa. Trong hai mục con tiếp theo, tính chính xác của TOE và tính chính xác của môi trường vận hành sẽ được trình bày riêng biệt.

6.2.2 Tính chính xác của TOE

Một Toe có thể được thiết kế và triển khai không chính xác, do đó có thể chứa các lỗi dẫn đến điểm yếu. Qua khai thác các điểm yếu này, tin tặc vẫn có thể phá hoại và/hoặc lạm dụng các tài sản.

Các điểm yếu trên có thể xuất hiện từ các lỗi ngẫu nhiên có trong quá trình phát triển, thiết kế sơ sài, việc cố ý chèn thêm mã độc, kiểm thử sơ sài, v.v.

Để xác định tính chính xác của TOE, nhiều động thái có thể thực hiện ví dụ như:

- Kiểm thử TOE;
- Kiểm tra các mô tả thiết kế khác nhau của TOE;
- Kiểm tra an toàn vật lý cho môi trường phát triển của TOE.

Đích an toàn cung cấp một mô tả có cấu trúc của các động thái này để xác định tính chính xác dưới dạng Các yêu cầu đảm bảo an toàn (Security Assurance Requirements – SAR). Các SAR này được biểu thị trong một ngôn ngữ chuẩn (mô tả trong TCVN 8709-3) để bảo đảm sự chính xác và dễ tương thích.

Nếu các SAR được thỏa mãn, sẽ có sự bảo đảm về tính chính xác của TOE, và do đó TOE gần như ít chứa các điểm yếu có thể bị tin tặc khai thác hơn. Lượng bảo đảm có trong tính chính xác của TOE

được chính các SAR này xác định: Một vài SAR "yếu" có thể dẫn đến khả năng bảo đảm kém, nhiều SAR "mạnh" sẽ dẫn đến bảo đảm nhiều.

6.2.3 Tính chính xác của môi trường vận hành

Môi trường vận hành có thể được thiết kế và triển khai không đúng, do đó có thể chứa các lỗi dẫn đến điểm yếu. Qua khai thác các điểm yếu này, tin tặc vẫn có thể phá hoại và/hoặc lạm dụng các tài sản.

Tuy nhiên, trong tiêu chuẩn TCVN 8709, không có sự bảo đảm nào đạt được liên quan đến tính chính xác của môi trường vận hành. Hay nói một cách khác, môi trường vận hành không được đánh giá (xem mục 6.3).

Trong liên quan đến đánh giá, môi trường vận hành được giả định là thuyết minh đúng 100% về các mục tiêu an toàn cho môi trường vận hành.

Điều này không cản trở người tiêu dùng một TOE sử dụng các phương pháp khác để xác định tính chính xác của môi trường vận hành đó, ví dụ:

- Nếu đối với một TOE là hệ điều hành, các mục tiêu an toàn cho môi trường vận hành khẳng định "môi trường vận hành cần bảo đảm rằng các thực thể từ một mạng không tin cậy (ví dụ Internet) có thể chỉ truy nhập vào TOE bằng ftp", người tiêu dùng có thể chọn lựa một tường lửa đã đánh giá, và cấu hình nó chỉ để cho phép truy nhập ftp đến TOE;
- Nếu các mục tiêu an toàn cho môi trường vận hành khẳng định "môi trường vận hành cần bảo đảm rằng mọi nhân viên quản trị không có hành vi ác ý", người tiêu dùng có thể điều chỉnh hợp đồng với các nhân viên quản trị để đưa vào các hình phạt đối với hành vi ác ý, song việc xác định này không thuộc phạm vi đánh giá theo TCVN 8709.

Các chủ sở hữu tài sản sẽ phân tích các mối đe dọa có thể xảy ra với tài sản và môi trường của họ, xác định các rủi ro liên quan tới chúng. Phân tích trên có thể hỗ trợ trong việc lựa chọn các biện pháp phòng chống để chống lại các rủi ro và giảm chúng xuống một mức độ chấp nhận được.

Các biện pháp phòng chống được áp đặt để làm giảm các điểm yếu và để đáp ứng các chính sách an toàn của chủ sử hữu tài sản (hoặc trực tiếp hoặc gián tiếp thông qua chỉ dẫn tới các phần khác). Các điểm yếu còn lại có thể vẫn tồn tại sau khi áp đặt các biện pháp phòng chống. Các điểm yếu đó có thể bị khai thác bởi các tác nhân đe dọa thể hiện một mức độ rủi ro tồn đọng cho tài sản. Các chủ sở hữu sẽ tìm cách giảm thiểu rủi ro đó theo những ràng buộc khác.

6.3 Đánh giá

TCVN 8709 thừa nhận hai kiểu đánh giá: đánh giá một ST/TOE như được mô tả sau đây, và đánh giá các PP được định nghĩa trong TCVN 8709-3. Tại nhiều vị trí, TCVN 8709 sử dụng khái niệm đánh giá (không có bổ nghĩa) để chỉ đánh giá ST/TOE.

Trong TCVN 8709, đánh giá ST/TOE được thực hiện theo hai bước sau:

a) Đánh giá ST: xác định tính đầy đủ của TOE và môi trường vận hành.

b) Đánh giá TOE: Xác định tính chính xác của TOE. Như đã nêu ở trên, đánh giá TOE không hàm ý đánh giá tính chính xác của môi trường vận hành.

Đánh giá ST được thực hiện bằng việc áp dụng các tiêu chí đánh giá Đích an toàn (như đã định nghĩa trong TCVN 8709-3 Điều khoản ASE) cho Đích an toàn. Phương pháp chuẩn xác áp dụng các tiêu chí ASE được xác định bởi hệ phương pháp đánh giá được dùng.

Đánh giá TOE phức tạp hơn. Các đầu vào chính của đánh giá TOE là: bằng chứng đánh giá bao gồm TOE và ST, song thường cũng bao gồm cả đầu vào từ môi trường phát triển, ví dụ các tài liệu thiết kế hoặc các kết quả kiểm thử của nhà phát triển.

Đánh giá TOE gồm việc áp dụng các SAR (từ Đích an toàn) vào bằng chứng đánh giá. Phương pháp chuẩn xác để áp dụng một SAR cụ thể được xác định bởi hệ phương pháp đánh giá được dùng.

Việc tài liệu hóa các kết quả áp dụng SAR như thế nào, các báo cáo nào cần tạo ra và đến mức chi tiết nào được xác định bởi cả hệ phương pháp đánh giá được dùng và lược đồ đánh giá theo đó phép đánh giá được thực hiện.

Kết quả của quá trình đánh giá TOE là một trong hai phát biểu sau:

- Một phát biểu về việc không phải mọi SAR đều được thỏa mãn và do đó không có mức đảm bảo đã chỉ ra cho việc TOE thỏa mãn các SFR như đã nêu trong ST;
- Một phát biểu về việc mọi SAR đều được thỏa mãn và do đó có mức đảm bảo đã chỉ ra cho việc TOE thỏa mãn các SFR như đã nêu trong ST;

Đánh giá TOE có thể thực hiện sau khi bước phát triển TOE hoàn tất, hoặc song song với quá trình phát triển TOE.

Phương pháp công bố kết quả đánh giá ST/TOE được mô tả trong Điều 9. Các kết quả này cũng định danh các PP và các gói mà TOE đòi hỏi tuân thủ, các kết cấu này được mô tả trong Điều 7.

7 Biến đổi thích ứng các yêu cầu an toàn

7.1 Các hoạt động

Các thành phần chức năng và đảm bảo của tiêu chuẩn có thể sử dụng chín xác như đã định nghĩa trong TCVN 8709-2 và TCVN 8709-3, hoặc chúng có thể được biến đổi thích ứng qua việc dùng các hoạt động được phép. Khi sử dụng các hoạt động, tác giả PP/ST cần thận trọng là các nhu cầu phụ thuộc vào các yêu cầu khác lệ thuộc vào yêu cầu này cần được thỏa mãn. Các hoạt động được phép được chọn từ tập sau đây:

- Phép lặp: cho phép một thành phần được sử dụng nhiều lần với các hoạt động biến đổi;
- Phép chỉ định: cho phép đặc tả các tham số
- Phép lựa chọn: cho phép đặc tả một hoặc nhiều biểu thức từ một danh sách
- Phép bổ sung chi tiết: cho phép bổ sung các chi tiết

Các hoạt động chỉ định và chọn được cho phép chỉ khi thể hiện một cách rõ rệt trong một thành phần. Các hoạt động lặp và bổ sung chi tiết được phép cho mọi thành phần. Các hoạt động được mô tả chi tiết ở phần sau.

Các phụ lục của TCVN 8709-2 cung cấp hướng dẫn về việc hoàn thiện hợp lệ các lựa chọn và chỉ định. Hướng dẫn này cung cấp các lệnh chuẩn về việc hoàn thành các hoạt động như thế nào, các lệnh đó sẽ kế tiếp ngoại trừ tác giả PP/ST bố trí lại các lệch lạc sau:

a) Từ "Không" chỉ có thể dùng làm một lựa chọn để hoàn tất một phép lựa chọn nếu nó được cung cấp rõ ràng.

Các danh sách đã cung cấp cho việc hoàn thiện các phép lựa chọn cần không được là danh sách trắng. Nếu tùy chọn "Không" được chọn, sẽ không có tùy chọn phép lựa chọn bổ sung nào có thể được chọn. Nếu "Không" đưa ra trong một phép lựa chọn không phải là tùy chọn, nó cho phép kết hợp các chọn lựa trong một phép lựa chọn với "và" và "hoặc", ngoại trừ phép lựa chọn công bố rõ "chọn một trong số ...".

Các hoạt động chọn có thể kết hợp bởi phép lặp khi cần. Trong trường hợp này, khả năng áp dụng được của tùy chọn đã chọn cho mỗi phép lặp cần không chồng lấn lên cơ quan của các phép lựa chọn có lặp khác, vì chúng dự kiến là bị loại trừ.

b) Để hoàn thành các phép gán, các phụ lục của TCVN 8709-2 sẽ được tham khảo để xác định ra khi nào "không" có thể là một hoàn tất hợp lệ.

7.1.1 Hoạt động lặp

Hoạt động lặp có thể được thực hiện ở mọi thành phần. Tác giả PP/ST thực hiện một hoạt động lặp bằng cách đưa vào nhiều yêu cầu dựa trên cùng một thành phần. Mỗi phép lặp của môt thành phần cần khác biệt với mọi phép lặp khác của thành phần đó, điều này được thực hiện bằng việc hoàn thành các phép chỉ định và phép lựa chọn theo một cách khác, hoặc áp dụng phép bổ sung chi tiết cho nó theo một cách khác.

Các phép lặp khác nhau nên định danh duy nhất để cho phép các sở cứ và các dấu vết đến từ và đi từ các yêu cầu này.

Quan trọng là cần lưu ý rằng đôi lúc một hoạt động lặp có thể được dùng với các thành phần, khi đó cũng có thể thực hiện một phép chỉ định với một khoảng giá trị hoặc một danh sách các giá trị thay vì lặp lại chúng. Trong trường hợp này, tác giả có thể chọn ra phương án thích hợp nhất, xem xét xem cs cần cung cấp toàn bộ sở cứ cho một khoảng giá trị hoặc xem có cần có riêng từng sở cứ tách biệt cho mỗi khoảng. Tác giả nên lưu ý nếu việc ghi dấu vết riêng được yêu cầu cho các giá trị này.

7.1.2 Hoạt động chỉ định

Một hoạt động chỉ định xảy ra khi một thành phần cho trước chứa một phần tử với tham số có thể đặt bởi tác giả PP/ST. Tham số có thể là một biến không giới hạn, một quy tắc hạn chế biến trong một khoảng giá trị nhất định.

Mỗi khi một phần tử trong một PP có chứa một phép chỉ định, tác giả của PP cần thực hiện một trong bốn việc sau:

a) Rời bỏ phép chỉ định không hoàn tất. Tác giả PP có thể đưa vào FIA_ASL.1.2 "Khi một số lượng xác định phép thử xác thực không thành công đạt được hoặc vượt qua, TSF cần **[Ấn định: danh sách các hành động]"** trong PP.

b) Hoàn tất phép chỉ định: ví dụ, tác giả PP có thể đưa vào FIA_ASL .1.2 "Khi một số lượng xác định phép thử xác thực không thành công được thỏa mãn hoặc được vượt qua, TSF cần **"ngăn cản thực thể bên ngoài gắn kết với bất kỳ cơ quan nào trong tương lai"** trong PP.

c) Thu hẹp phép chỉ định, tiếp đó giới hạn khoảng giá trị cho phép. Ví dụ, tác giả PP'có thể đưa vào FIA_ÀL.1.1 **"TSF cần phát hiện khi nào [Ấn định: một số nguyên dương giữa 4 và 9] lần thử xác thực không thành công xảy ra..."** trong PP.

d) Chuyển đổi phép chỉ định thành một phép lựa chọn, qua đó thu hẹp phép chỉ định. Ví dụ, tác giả PP có thể đưa vào FIA_ÀL.1.2 **"Khi một số xác định số lần thử xác thực không thành công đã đạt được hoặc vượt quá,TSF cần [Chọn: ngăn cản người dùng này gắn kết với bất kỳ cơ quan nào trong tương lai, thông báo cho người quản trị"** trong PP.

Mỗi khi một phần tử trong một ST chứa một phép chỉ định, tác giả ST cần hoàn tất phép gán này, như đã biểu thị ở mục b) nêu trên. Các tùy chọn a), c) và d) không cho phép đối với ST.

Các giá trị được chọn trong các tùy chọn b), c) và d) cần tuân thủ theo kiểu đã chỉ ra yêu cầu bởi phép chỉ định.

Khi một phép chỉ định cần được hoàn thành với một tập (ví dụ các cơ quan), nó có thể là liệt kê một tập các cơ quan, song cũng một số mô tả của tập có thể được các phần từ của tập dẫn xuất ra, như:

- Toàn bộ các cơ quan
- Toàn bộ các cơ quan của kiểu X
- Toàn bộ các cơ quan ngoại trừ cơ quan a

Chừng nào còn rõ các cơ quan nào được xét tới.

7.1.3 Hoạt động lựa chọn

Một hoạt động lựa chọn xảy ra khi một thành phần cho trước chứa một phần tử và một chọn lựa từ các biểu thức cần được lập bởi tác giả PP/ST.

Mỗi khi một phần tử trong một PP có chứa một phép lựa chọn, tác giả của PP cần thực hiện một trong ba việc sau:

e) Rời bỏ phép lựa chọn không hoàn tất.

f) Hoàn tất phép lựa chọn bằng việc lựa chọn một hoặc nhiều biểu thức.

g) Giới hạn phép lựa chọn qua việc xóa bỏ một số lựa chọn, song để lại 2 hoặc nhiều hơn.

Mỗi khi một phần tử trong 1 ST chứa một phép lựa chọn, tác giả ST cần hoàn tất phép lựa chọn này, như đã biểu thị ở mục b) nêu trên. Các tùy chọn a), c) và d) không cho phép đối với ST.

Biểu thức hoặc các biểu thức được chọn ở b) và c) cần lấy từ các biểu thức đã cung cấp ở phép lựa chọn.

7.1.4 Hoạt động bổ sung chi tiết

Hoạt động bổ sung chi tiết có thể được thực hiện ở mọi yêu cầu. Tác giả PP/ST thực hiện một phép bổ sung chi tiết bằng cách thay đổi yêu cầu này. Quy tắc đầu tiên cho một phép bổ sung chi tiết là một TOE đáp ứng yêu cầu đã chi tiết hóa cũng sẽ đáp ứng các yêu cầu không chi tiết hóa trong ngữ cảnh của PP/ST (nghĩa là yêu cầu chi tiết hóa cần phải "chặt" hơn yêu cầu ban đầu). Nếu một phép bổ sung chi tiết không thỏa mãn quy tắc này, kết qua yêu cầu chi tiết hóa được coi là một yêu cầu mở rộng và cần xử lý như vậy.

Chỉ có một ngoại lệ cho quy tắc này là một tác giả PP/ST được phép bổ sung chi tiết cho SFR để áp dụng cho một số, song không phải là tất cả cơ quan, đối tượng, hoạt động, thuộc tính an toàn và/hoặc các thực thể bên ngoài.

Tuy nhiên, ngoại lệ này không áp dụng cho bổ sung chi tiết SFR lấy từ các PP đang đòi hỏi tuân thủ. Các SFR này có thể không được bổ sung chi tiết để áp dụng to một vài cả cơ quan, đối tượng, hoạt động, thuộc tính an toàn và/hoặc các thực thể bên ngoài so với SFR trong PP.

Quy tắc thứ hai cho một phép bổ sung chi tiết là một phép bổ sung chi tiết cần liên quan đến thành phần chính hiệu.

Một trường hợp đặc biệt của phép bổ sung chi tiết là một bổ sung chi tiết biên soạn, trong đó một thay đổi nhỏ được tạo trong một yêu cầu, nghĩa là làm rõ nghĩa một câu để trung thành với ngữ pháp tiếng Anh đúng, hoặc làm cho nó dễ hiểu hơn cho người đọc. Sự thay đổi này không được phép sửa đổi ý nghĩa của yêu cầu theo bất kỳ cách nào.

7.2 Sự phụ thuộc giữa các thành phần

Giữa các thành phần có thể có các quan hệ phụ thuộc. Các quan hệ phụ thuộc nảy sinh khi một thành phần không đủ và phải tồn tại khi có mặt thành phần khác để cung cấp tính năng an toàn hay đảm bảo.

Các thành phần chức năng trong TCVN 8709-2 điển hình có sự phụ thuộc vào các thành phần chức năng khác như một số thành phần đảm bảo trong TCVN 8709-3 đã có, chúng có thể có sự phụ thuộc vào các thành phần khác của TCVN 8709-3. Sự phụ thuộc của TCVN 8709-2 vào các thành phần TCVN 8709-3 cũng có thể được định nghĩa. Tuy nhiên, điều này không ngăn cản các thành phần chức năng ngoài có sự phụ thuộc vào các thành phần đảm bảo và ngược lại.

Các mô tả sự phụ thuộc của thành phần được xác định qua tham khảo các định nghĩa thành phần trong TCVN 8709-2 và TCVN 8709-3. Để đảm bảo mô tả sự hoàn thiện các yêu cầu an toàn TOE, các phụ thuộc cần được thỏa mãn khi các yêu cầu dựa trên các thành phần với sự phụ thuộc được kết hợp vào PP và ST . Các phụ thuộc nên được xem xét khi cấu trúc các gói.

Nói một cách khác, nếu thành phần A có sự phụ thuộc vào thành phần B, điều đó nghĩa là mỗi khi một PP/ST có chứa một yêu cầu an toàn dựa trên thành phần A, PP/ST cũng cần chứa một trong số:

a) Một yêu cầu an toàn dựa trên thành phần B, hoặc

b) Một yêu cầu an toàn dựa trên một thành phần nằm ở phân cấp cao hơn B, hoặc

c) Một biện minh tại sao PP/ST không chưa một yêu cầu an toàn dựa trên thành phần B.

Trong các trường hợp a) và b), khi một yêu cầu an toàn được bao hàm do tính phụ thuộc, có thể cần thiết phải hoàn thiện các hoạt động (chỉ định, lặp, bổ sung chi tiết, chọn) trên yêu cầu an toàn này theo một cách riêng để đảm bảo rằng nó thực sự thỏa mãn tính phụ thuộc.

Trong trường hợp c), biện minh cho việc không chứa một yêu cầu an toàn nên đề cập đến:

- Tại sao sự phụ thuộc không cần thiết hay không hữu ích, hoặc
- Sự phụ thuộc đã đề cập trong môi trường vận hành của TOE, trong đó việc biện minh cần mô tả cách các mục tiêu an toàn cho môi trường vận hành đề cập đến sự phụ thuộc của nó như thế nào, hoặc

- Sự phụ thuộc đã đề cập đến bởi các SFR khác theo một cách nào đó (các SFR mở rộng, các tổ hợp của các SFR...)

7.3 Các thành phần mở rộng

Trong TCVN 8709, các yêu cầu bắt buộc phải dựa vào các thành phần trong TCVN 8709-2 hoặc TCVN 8709-3 với 2 ngoại lệ sau:

a) Có các mục tiêu an toàn cho TOE không thể chuyển đổi sang các SFR của phần 2, hoặc có các yêu cầu của bên thứ ba (ví dụ luật pháp, tiêu chuẩn) không thể chuyển đổi sang các SAR của phần 3 (ví dụ liên quan đến đánh giá mật mã).

b) Một mục tiêu an toàn có thể được chuyển đổi, song chỉ với mức độ phức tạp cao hoặc/và khó khăn lớn trên cơ sở các thành phần trong TCVN 8709-2 hoặc TCVN 8709-3.

Trong cả hai trường hợp, tác giả PP/ST được đòi hỏi phải định nghĩa các thành phần riêng của họ. Các thành phần mới được định nghĩa này được gọi là các thành phần mở rộng. Một thành phần mở rộng được định nghĩa chính xác là cần thiết để đưa ra ngữ cảnh và ý nghĩa cho các SFR và SAR mở rộng dựa trên thành phần này.

Sau khi các thành phần mới đã được định nghĩa chính xác, tác giả PP/ST có thể đưa ra một hoặc nhiều SFR hoặc SAR trên cơ sở các thành phần mở rọng đã định ngiã này và sử dụng chúng theo cùng cách như với các SFR và SAR khác. Từ đây trở đi, không có sự phân biệt hơn giữa các SAR và SFR dựa theo TCVN 8709 và các SAR, SFR dựa trên các thành phần mở rộng. Xem thêm phần định nghĩa các thành phần mở rộng của TCVN 8709-3 (APE_ECD) và định nghĩa các thành phần mở rộng (ASE_ECD) để rõ hơn các yêu cầu về các thành phần mở rộng.

8 Hồ sơ bảo vệ và gói

8.1 Giới thiệu

Để cho phép các nhóm người tiêu dùng và cộng đồng quan tâm biểu thị các nhu cầu an toàn của họ, và để thuận lợi cho việc viết các ST, phần này của tiêu chuẩn cung cấp hai kết cấu đặc biệt: các gói và các hồ sơ bảo vệ (PPs). Trong các mục 8,.2 và 8.3, các kết cấu này được mô tả chi tiết hơn. Mục nhỏ 8.4 giải thích các kết cầu này có thể được dùng như thế nào.

8.2 Các gói

Một gói là một tập định danh các yêu cầu an toàn. Một gói có thể là:

- Một gói chức năng, chỉ chứa các SFR, hoặc
- Một gói đảm bảo, chỉ chứa các SAR.

Không được phép có các gói hỗn hợp chứa cả SFR và SAR.

Một gói có thể được định nghĩa bởi bất kỳ bên nào và dự kiến là có thể tái sử dụng. Để đạt được mục tiêu này, nó cần chứa các yêu cầu hữu ích và hiệu quả kết hợp với nhau. Các gói có thể được dùng trong kiến thiết các gói lớn hơn, các PP và ST. Hiện tại không có tiêu chí nào cho việc đánh giá các gói, do vậy bất kỳ tập SAR hay SFR có thể là một gói.

Ví dụ về các gói đảm bảo như: các mức đảm bảo đánh giá (EAL) được định nghĩa trong TCVN 8709-3. Hiện tại, chưa có các gói chức năng cho phiên bản tiêu chuẩn này.

8.3 Các hồ sơ bảo vệ

Trong khi một ST luôn mô tả một TOE nhất định (ví dụ thiết bị tường lửa FW MinuteGap v18.5), một PP dự kiến mô tả một kiểu TOE (ví dụ các tường lửa). Cũng PP này do đó có thể sử dụng làm bản mẫu cho nhiều ST khác để sử dụng trong các phép đánh giá khác nhau. Mô tả chi tiết của các PP được đưa ra trong Phụ lục B.

Nói chung, một ST mô tả các yêu cầu cho một TOE, và được viết bởi nhà phát triển TOE này, trong khi đó một PP mô tả các yêu cầu chung co một kiểu TOE, và do đó thường được viết bởi:

- Một cộng đồng người dùng tìm kiếm sự đồng thuận về các yêu cầu cho một kiểu TOE cho trước.
- Một nhà phát triển TOE, hay một nhóm các nhà phát triển của các TOE tương tự mong muốn lập ra một mức tối thiểu cho kiểu TOE này.
- Một chính phủ, hoặc tập đoàn lớn chỉ rõ các yêu cầu của họ là một phần của quá trình thu thập thông tin.

PP xác định kiểu được phép cho tính tuân thủ của ST với PP. Nghĩa là PP công bố (trong phát biểu tuân thủ PP, sem B.5) rằng các kiểu tuân thủ được phép cho ST là:

- Nếu PP công bố là sự tuân thủ chặt chẽ cần có, ST cần tuân thủ với PP theo cách chặt chẽ;
- Nếu PP công bố rằng cần có sự tuân thủ có thể diễn giải được, ST cần tuân thủ với PP theo cách chặt chẽ hoặc cách diễn giải được.

Tường trình lại điều trên theo một cách nói khác, một ST chỉ được phép tuân thủ trong một PP theo cách diễn giải được, nếu PP cho phép một cách rõ ràng điều này.

Nếu một ST đòi hỏi sự tuân thủ với nhiều PP, nó cần tuân thủ (như đã mô tả ở trên) cho mỗi PP theo cách được quy định bởi PP này. Điều này có thể nghĩa là ST tuân thủ chặt chẽ với một số PP và có thể diễn giải tới các PP khác.

Lưu ý rằng hoặc ST tuân thủ theo PP trong yêu cầu hoặc nó không tuân thủ. TCVN 8709 không chấp thuận tính tuân thủ "từng phần". Do đó, trách nhiệm của tác giả PP là đảm bảo PP không phiền hà thái quá, ngăn cấm tác giả PP/ST trong đòi hỏi tuân thủ theo PP.

Một ST tương đương hoặc gới hạn hơn nhiều so với một P nếu:

- Tất cả các TOE thỏa mãn ST cũng thỏa mãn PP, và
- Tất cả các môi trường vận hành thỏa mãn PP cũng thỏa mãn ST.

Hay nói một cách thân thuộc hơn, ST cần tập trung cùng hoặc nhiều hạn chế hơn ở TOE và cùng hoặc ít hạn chế hơn ở môi trường vận hành của TOE.

Phát biểu chung này có thể được tạo ra một cách đặc trưng hơn cho nhiều khoản mục khác nhau của ST như sau:

Định nghĩa vấn đề an toàn: Sở cứ tuân thủ trong ST cần diễn giải rằng định nghĩa vân đề an toàn trong ST tương đương (hoặc nhiều hạn chế hơn) định nghĩa vân đề an toàn trong PP. Điều đó nghĩa là:

- Tất cả các TOE có thể thỏa mãn định nghĩa vân đề an toàn trong ST cũng thỏa mấn định nghĩa vân đề an toàn trong PP;
- Tất cả các môi trường vận hành có thể thỏa mãn định nghĩa vân đề an toàn trong PP cũng sẽ thỏa mãn định nghĩa vân đề an toàn trong ST;

Các mục tiêu an toàn: Sở cứ tuân thủ trong ST cần diễn giải rằng các mục tiêu an toàn trong ST tương đương (hoặc nhiều hạn chế hơn) các mục tiêu an toàn trong PP. Điều đó nghĩa là:

- Tất cả các TOE có thể thỏa mãn các mục tiêu an toàn trong ST cũng thỏa mãn các mục tiêu an toàn cho TOE trong PP;
- Tất cả các môi trường vận hành có thể thỏa mãn các mục tiêu an toàn trong PP cũng sẽ thỏa mãn các mục tiêu an toàn cho môi trường vận hành trong ST;

Nếu tính tuân thủ chặt chẽ cho các hồ sơ bảo vệ được chỉ ra, thì các yêu cầu sau sẽ áp dụng:

a) **Định nghĩa vấn đề an toàn:** ST cần chứa định nghĩa vân đề an toàn của PP, có thể chỉ ra các mối đe dọa bổ sung và các OSPs, song có thể không chỉ ra các giả thiết bổ sung.

b) **Các mục tiêu an toàn:** ST cần:

- Cần chứa tất cả các mục tiêu an toàn cho TOE của PP, song có thể chỉ ra các mục tiêu an toàn bỏ sung cho TOE;
- Cần chứa tất cả các mục tiêu an toàn cho môi trường vận hành (với một ngoại lệ trong mục con tiếp theo), song có thể không chỉ ra các mục tiêu an toàn bổ sung cho môi trường vận hành;
- Có thể chỉ ra các mục tiêu nhất định cho môi trường vận hành trong PP là các mục tiêu an toàn cho TOE trong ST. Điều này gọi là chỉ định lại một mục tiêu an toàn. Nếu một mục tiêu an toàn được chỉ định lại cho TOE, sở cứ cho các mục tiêu an toàn cần làm rõ ràng là giả thiết nào hoặc phần giả thiết nào không cần thiết nữa.

c) **Các yêu cầu an toàn:** ST cần chứa tất cả các SFR và SAR trong PP, song có thể đòi hỏi các SFR và SAR bổ sung hoặc phân cấp mạnh hơn. Sự hoàn tất các hoạt động trong ST cần phải nhất quán với các hoạt động trong PP, hoặc là cùng có sự hoàn tất trong ST như trong PP hoặc một hoạt động nào đó làm cho yêu cầu trở nên hạn chế hơn (áp dụng các quy tắc bổ sung chi tiết).

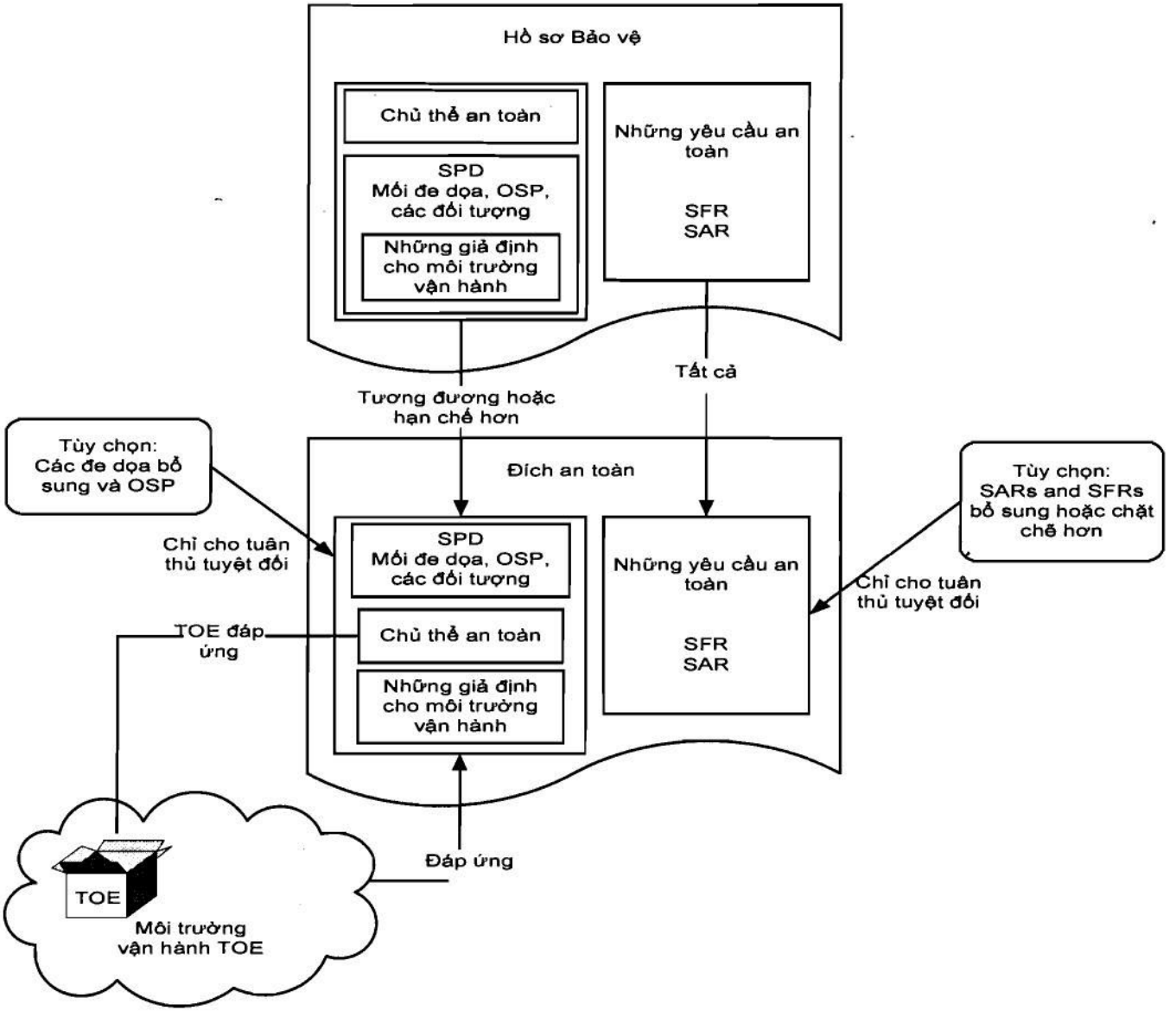
Nếu tính tuân thủ có thể biểu diễn được cho các hồ sơ bảo vệ được chỉ ra, thì các yêu cầu sau sẽ được áp dụng:

- ST cần chứa một sở cứ về việc tại sao ST được xem xét là "tương đương hoặc hạn chế hơn" là so với PP.
- Tính tuân thủ biểu hiện được cho phép một tác giả PP mô tả vân đề an toàn chung cần được giải quyết và cung cấp các hướng dẫn chung cho các yêu cầu cần thiết đối với việc giải quyết nó, với nhận thức rằng có thể có nhiều hơn một cách để chỉ ra lời giải.

Đánh giá PP là tùy ý. Việc đánh giá được thực hiện qua việc áp dung các tiêu chí APE cho chúng như liệt kê trong TCVN 8709-3. Mục đích của việc đánh giá như vậy là đê diễn giải rằng PP là hoàn tất, nhất quán, và và phù hợp về mặt kỹ thuật, thích hợp để dùng làm bản mẫu cho việc tạo ra PP hoặc một ST khác.

Tạo ra một PP/ST dựa trên một PP đã đánh giá có hai ưu điểm:

- Có ít rủi ro hơn về các lỗi, chỗ không rõ ràng, hoặc kẽ hở trong PP. Nếu bất kỳ vấn đề nào với một PP (có thể phát hiện ra khi đánh giá PP) được tìm ra trong quá trình viết hoặc đánh giá một ST mới, một khoảng thời gian đáng kể đã qua đi trước khi PP được sửa lại.
- Đánh giá PP/ST mới thường có thể tái sử dụng các kết quả đánh giá của PP đã được đánh giá, do vậy sẽ giảm bớt công sức đành giá PP/ST mới.



Hình 4 - Các mối quan hệ giữa PP, ST và các nội dung TOE

8.4 Sử dụng PP và các gói

Nếu một ST đòi hỏi được tuân thủ theo một hoặc nhiều gói và/hoặc các Hồ sơ bảo vệ, việc đánh giá ST này sẽ (theo như các đặc tính khác của ST) diễn giải rằng ST thực tế tuân thủ với các gói này và/hoặc các PP mà chúng đòi hỏi tuân thủ theo. Chi tiết về việc xác định tính tuân thủ này được nêu trong Phụ lục A.

Điều trên cho phép tiến trình sau đây:

a) Một tổ chức tìm kiếm thu thập một kiểu cá biệt về sản phẩm an toàn CNTT, thực hiện xây dựng các nhu cầu an toàn của nó trong một PP, tiếp đó đánh giá nó và công bố nó;

b) Một nhà phát triển lấy PP này, viết một ST yêu cầu tuân thủ theo PP và đã đánh giá ST này;

c) Nhà phát triển tiếp đó tạo ra một TOE (hoặc sử dụng một TOE có sẵn) và thực hiện đánh giá theo ST.

Kết quả là nhà phát triển có thể chứng minh rằng TOE của hị tuân thủ theo các nhu cầu an toàn của tổ chức. Do vậy, tổ chức đạt được TOE này. Cách tương tự cũng được áp dụng cho các gói.

8.5 Sử dụng nhiều Hồ sơ bảo vệ

TCVN 8709 cũng cho phép các PP tuân thủ theo các PP khác, cho phép kiến thiết chuỗi các PP, mỗi cái dựa vào một cái (hoặc nhiều cái) trước đó.

Ví dụ, có thể lấy một PP cho một mạch tổ hợp và một PP cho một OS dùng thẻ thông minh, và dùng chúng để kiến thiết ra một PP cho thẻ thông minh (IC và OS) với yêu cầu tuân thủ theo hai PP khác. Có thể viết một PP về các thẻ thông minh cho vận tải công cộng dựa trên PP cho thẻ thông minh và viết một PP cho việc tải Applet. Kế đó, một nhà phát triển có thể kiến thiết một ST dựa theo các thẻ thông minh này cho PP vận tải công cộng.

9 Các kết quả đánh giá

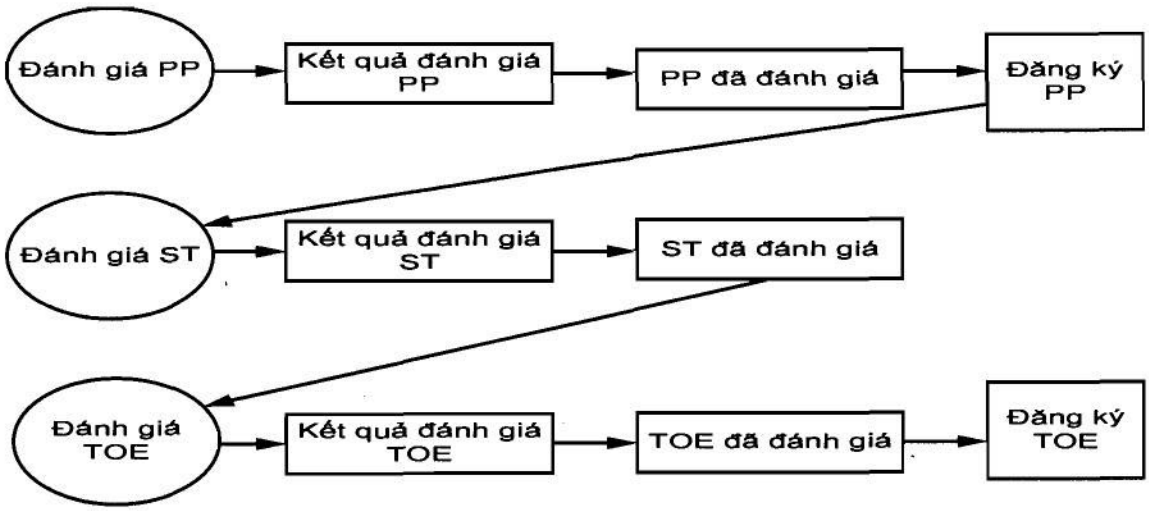
9.1 Giới thiệu

Phần này trình bầy các kết quả mong muốn qua đánh giá PP và ST/TOE thực hiện theo TCVN 8709.

- Các đánh giá PP cho ta được danh mục các PP đã được đánh giá.
- Việc đánh giá ST cho các kết quả trung gian để sử dụng trong khuôn khổ đánh giá TOE.
- Các đánh giá ST/TOE cho ta được danh mục các ST/TOE đã được đánh giá. Trong nhiều trường hợp các danh mục này sẽ tham chiếu tới các sản phẩm CNTT mà các TOE được dẫn xuất ra hơn là TOE xác định. Bởi vậy, sự tồn tại của mọt sản phẩm CNTT trong một danh mục không nên được kiến thiết theo nghĩa là toàn bộ sản phẩm CNTT đã được đánh giá. Thay vào đó việc mở rộng thực tế của đánh giá ST/TOE được định nghĩa qua ST. Tham chiếu đến thư mục cá ví dụ của các danh mục đó.

Các ST có thể dựa trên các gói, các PP đã đánh giá hoặc các PP chưa đánh giá. Tuy nhiên, điều này không bắt buộc vì các ST không cần phải dựa trên một thứ gì cả.

Việc đánh giá nên dẫn tới các kết quả khách quan và nhắc lại được để được coi là bằng chứng, ngay cả khi không có một cấp độ khách quan tuyệt đối nào cho việc biểu diễn các kết quả của một phép đánh giá an toàn. Sự tồn tại của một tập các tiêu chí đánh giá là một điều kiện cần thiết ban đầu cho việc đánh giá để đưa đến một kết quả đánh giá có nghĩa và cung cấp một cơ sửo kỹ thuật cho việc công nhận tương hỗ các kết quả đánh giá giữa các cơ quan đánh giá.



Hình 5 - Các kết quả đánh giá

Một kết quả đánh giá thể hiện việc tìm ra một kiểu xác định cho điều tra các đặc tính an toàn của một TOE. Một kết quả như vậy không tự động bảo đảm tính phù hợp cho sử dụng trong bất kỳ môi tường ứng dụng đặc biệt nào. Quyết định chấp nhận một TOE để sử dụng trong một môi trường ứng dụng đặc trưng dựa trên cơ sở xem xét nhiều vấn đề an toàn, bao gồm cả những kết luận đánh giá.

9.2 Các kết quả đánh giá PP

TCVN 8709-3 chứa các tiêu chí đánh giá mà một đánh giá viên bắt buộc phải tham khảo để xác định xem một PP có hoàn thiện, nhất quán và phù hợp về mặt kỹ thuật và do vậy thích hợp dùng để phát triển một ST hay chưa.

Các kết quả đánh giá PP cần chứa "Tuyên bố tuân thủ" (xem 9.4).

9.3 Các kết quả đánh giá ST/TOE

TCVN 8709-3 chứa các tiêu chí đánh giá mà một đánh giá viên bắt buộc phải tham khảo để xác định xem có tồn tại sự đảm bảo rằng TOE thỏa mãn các SFR trong ST hay không. Do đó, đánh giá TOE cần cho kết quả là một phát biểu đạt/không đạt cho ST. Nếu việc đánh giá cho cả hai ST và TOE cho lại kết quả trong công bố đạt, sản phẩm đang xét có thể sẵn sàng đưa vào bản đăng ký. Các kết quả đánh giá cần chứa một "Tuyên bố tuân thủ" như định nghĩa trong 9.4.

Có thể có trường hợp các kết quả đánh giá được sử dụng tiếp đó trong một tiến trình xác nhận, song tiến trình này nằm ngoài phạm vi của TCVN 8709.

9.4 Tuyên bố tuân thủ

Tuyên bố tuân thủ chỉ ra nguồn tập hợp các yêu cầu được thoả mãn cho một PP hay ST đã vượt qua bước đánh giá. Tuyên bố tuân thủ này chưa một tuyên bố tuân thủ TCVN 8709 như sau:

a) Mô tả phiên bản TCVN 8709 mà PP hay ST tuân thủ theo.

b) Mô tả sự tuân thủ theo TCVN 8709-2 (các yêu cầu chức năng an toàn) là:

- **Tuân thủ TCVN 8709–2 (ISO/IEC 15408–2 conformant):** Một PP hoặc ST là tuân thủ theo TCVN 8709-2 nếu mọi SFR trong PP hay ST này chỉ dựa trên các thành phần chức năng trong TCVN 8709 – 2. **Hoặc**

- **Mở rộng TCVN 8709–2 (ISO/IEC 15408–2 extended):** Một PP hoặc ST là mở rộng của TCVN 8709-2 nếu ít nhất có một SFR trong PP hay ST này không thuộc các thành phần chức năng trong TCVN 8709–2.

c) Mô tả sự tuân thủ theo TCVN 8709-3 (các yêu cầu đảm bảo an toàn) là:

- **Tuân thủ TCVN 8709–3 (ISO/IEC 15408–3 conformant):** Một PP hoặc ST là tuân thủ theo TCVN 8709-3 nếu tất cả các SAR trong PP hay ST này chỉ dựa trên các thành phần đảm bảo trong TCVN 8709 – 3. **Hoặc**
- **Mở rộng TCVN 8709–3 (ISO/IEC 15408–3 extended):** Một PP hoặc ST là mở rộng của TCVN 8709-3 nếu tất cả các SAR trong PP hay ST này không thuộc trên các thành phần đảm bảo trong TCVN 8709–3.

Ngoài ra, Tuyên bố tuân thủ có thể bao gồm cả một phát biểu liên quan đến các gói, trong đó có chứa một trong các điều sau:

- ***Tuân thủ tên gói:*** Một PP hoặc ST là tuân thủ theo một gói xác định trước (ví dụ EAL), nếu
  - Các SFR của PP hay ST này trùng với các SFR trong gói, hoặc
  - Các SAR của PP hay ST này trung với các SAR trong gói.
- ***Gia tăng tên gói:*** Một PP hoặc ST là một phần gia tăng của một gói xác định trước, nếu:
  - Các SFR của PP hay ST này chứa tất cả các SFR trong gói, song có ít nhất một SFR bổ sung hoặc một SFR có phần cấp cao hơn SFR tương ứng trong gói.
  - Các SAR của PP hay ST này chứa tất cả các SAR trong gói, song có ít nhất một SAR bổ sung hoặc một SAR có phần cấp cao hơn SAR tương ứng trong gói.

Lưu ý rằng khi một TOE đã đánh giá thành công theo một ST, bất kỳ một tuyên bố tuân thủ nào của ST cũng sẽ dùng được cho TOE. Một TOE như vậy có thể ví dụ là tuân thủ theo TCVN 8709-2.

Cuối cùng, tuyên bố tuân thủ cũng chứa hai phát biểu sau đây liên quan đến Hồ sở bảo vệ:

a) *Tuân thủ PP:* Một PP hay TOE thoả mãn các PP(s) xác định như đã được liệt kê là một phần của kết quả tuân thủ.

b) *Phát biểu tuân thủ* (chỉ cho PPs): Phát biểu này mô tả cách thức mà các PP hay các ST tuân thủ theo PP này, chặt chẽ hay diễn giải được. Xem Phụ lục B để có thêm thông tin về phát biểu tuân thủ này.

9.5 Sử dụng các kết quả đánh giá ST/TOE

Một khi một ST và một TOE đã được đánh giá, chủ sở hữu tài sản có thể có sự đảm bảo (như đã định nghĩa trong ST) rằng TOE, cùng với môi trường vận hành, chống lại được các mối đe dọa. Các kết quả đánh giá có thể được dùng bởi chủ sở hữu tài sản để ra quyết định về việc có chấp nhận rủi ro phơi bày tài sản trước các mối đe dọa hay không.

Tuy nhiên, chủ sở hữu tài sản nên thận trọng kiểm tra xem:

- Định nghĩa vấn đề an toàn trong ST có phù hợp với vân đề an toàn của mình hay không
- Môi trường vận hành của chủ sở hữu tài sản tuân thủ (hoặc có thể làm cho tuân thủ) theo các mục tiêu an toàn cho môi trường vận hành đã mô tả trong ST hay không.

Nếu không có điều nào trên là đúng, TOE có thể không thích hợp cho các mục đích của chủ sở hữu tài sản.

Ngoài ra, một khi một TOE đã đánh giá đang hoạt đông, vẫn có khả năng các lỗi không biết trước đó, hoặc các điểm yếu trong TOE có thể lộ diện. Trong trường hợp này, nhà phát triển có thể sửa TOE (để sửa chữa các điểm yếu) hoặc thay đổi ST đểloại trừ điểm yếu ra khỏi phạm vi đánh giá. Trong cả hai trường hợp, các kết quả đánh giá cũ có thể không còn hợp lệ nữa.

Nếu như cảm thấy cần thiết phải lấy lại sự tin cậy, việc đánh giá lại là cần thiết. TCVN 8709 có thể được sử dụng để thực hiện đánh giá lại, song các thủ tục chi tiết cho việc đánh giá lại nằm ngoài phạm vi phần này của tiêu chuẩn TCVN 8709.

Phụ lục A

(Tham khảo)

Đặc tả của các đích an toàn

A.1 Mục tiêu và cấu trúc của phụ lục

Phụ lục này giải thích khái niệm Đích an toàn (ST). Phụ lục này không định nghĩa các tiêu chí ASE; định nghĩa này có thể tìm thấy trong TCVN 8709-3 và các tài liệu đã cho trong tài liệu tham khảo.

Phụ lục này gồm bốn phần chính sau:

a) *Một ST phải có những gì.* Điều này được tóm tắt trong A.2, và được mô tả chi tiết hơn trong A.4 đến A.10. Các mục nhỏ này mô tả các nội dung bắt buộc của ST, các mối quan hệ bên trong giữa các nội dung này và đưa ra các ví dụ.

b) *Một ST nên được sử dụng thế nào.* Điều này được tóm tắt trong A.3, và được mô tả chi tiết trong A.11. Mục này mô tả một ST nên được sử dụng như thế nào, và một số câu hỏi có thể được trả lời với một ST.

c) *Các ST mức đảm bảo thấp.* Các ST này là các ST có nội dung được giản bớt. Chúng được mô tả chi tiết trong A.12

d) *Tuyên bố tuân thủ theo tiêu chuẩn.* Điều A.13 mô tả người soạn ST có thể tuyên bố rằng TOE đáp ứng một chuẩn cụ thể như thế nào.

A.2 Những nội dung bắt buộc của một ST

Hình A.1 miêu tả những nội dung bắt buộc của ST được đưa ra trong TCVN 8709-3. Hình A.1 cũng có thể được dùng làm một phác thảo cấu trúc của ST, qua đó cho phép lựa chọn các cấu trúc khác nhau. Ví dụ, nếu sở cứ các yêu cầu an toàn đặc biệt lớn, nó có thể được đưa vào trong một phụ lục của ST thay vì đưa vào trong mục nhỏ về các yêu cầu an toàn. Mỗi mục con riêng biệt của một ST và nội dung của những mục đó được tóm tắt ngắn gọn ở dưới và được giải thích chi tiết hơn trong A.4 tới A.10. Một ST thông thường bao gồm:

a) *Giới thiệu về ST* gồm ba mô tả tường thuật về TOE ở các mức trừu tượng khác nhau;

b) *Định nghĩa vấn đề an toàn,* chỉ ra các mối đe dọa, OSP và những giả định.

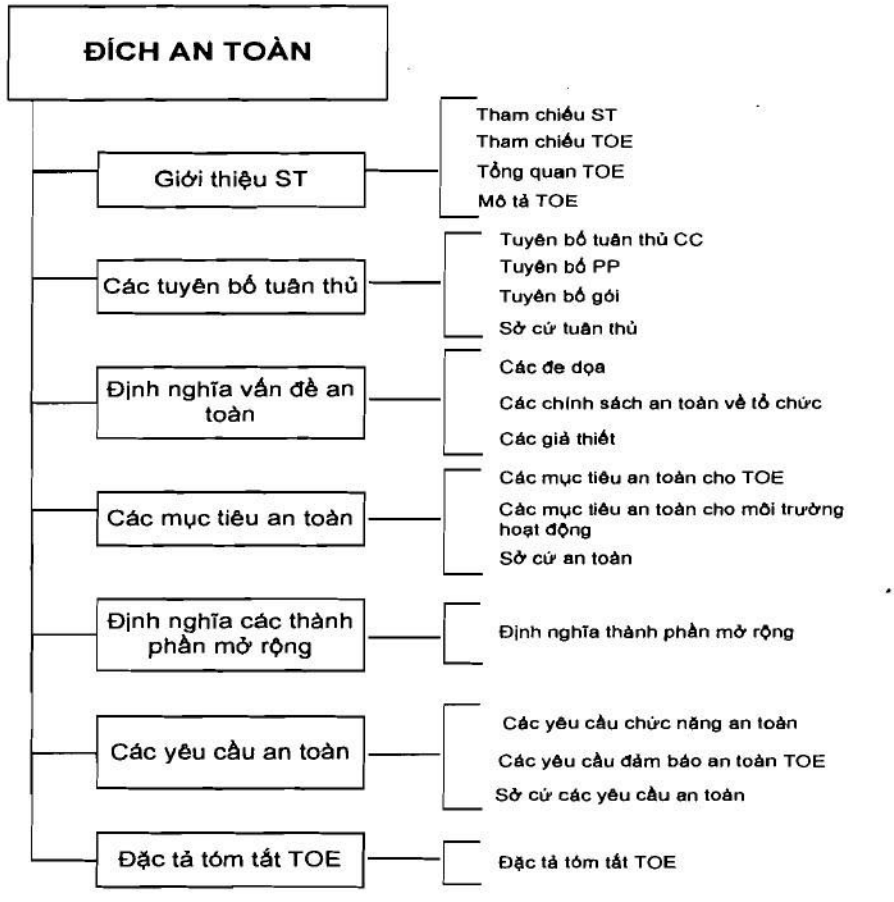
c) *Các mục tiêu an toàn,* chỉ ra giải pháp cho vấn đề an toàn được phân chia giữa các mục tiêu an toàn cho TOE và các mục tiêu an toàn cho môi trường vận hành của TOE thế nào;

d) *Định nghĩa các thành phần mở rộng* (Tùy chọn), ở đây các thành phần mới (nghĩa là các thành phần không có trong TCVN 8709-2 hay TCVN 8709-3) có thể được định nghĩa. Các thành phần mới này cần để định nghĩa các yêu cầu chức năng và các yêu cầu đảm bảo mở rộng;

e) *Những yêu cầu an toàn,* nơi chuyển đổi các mục tiêu an toàn cho TOE sang một ngôn ngữ được chuẩn hóa. Ngôn ngữ chuẩn hóa này dưới dạng các SFR. Thêm vào đó, nó định nghĩa các SAR

f) *Đặc tả tóm tắt TOE,* cho thấy các SFR được thực thi thế nào trong TOE.

Hiện cũng tồn tại các ST đảm bảo thấp đã giảm bớt nội dung, chúng được mô tả chi tiết trong A.12. Tất cả các phần khác của phụ lục này giả định một ST với đầy đủ nội dung.



Hình A.1 - Nội dung đích an toàn

A.3 Sử dụng một ST

A.3.1 Một ST nên được sử dụng thế nào

Một ST điển hình đáp ứng hai vai trò sau:

- Trước và trong suốt khi đánh giá, ST xác định "cái gì được đánh giá". Trong vai trò này, ST phục vụ như nền tảng cơ bản cho việc thỏa thuận giữa nhà phát triển và đánh giá viên trên các đặc tính an toàn chính xác của TOE và phạm vi chính xác của việc đánh giá. Tính đúng đắn và hoàn chỉnh về mặt kỹ thuật là những vấn đề chính trong vai trò này. Điều A.7 mô tả một ST được sử dụng thế nào trong vai trò này.
- Sau khi đánh giá, ST xác định "cái gì đã được đánh giá". Trong vai trò này, ST phục vụ như nền tảng cơ bản cho sự thỏa thuận giữa nhà phát triển hay người bán lại TOE và người tiêu dùng tiềm

năng của TOE. ST mô tả các đặc tính an toàn chính xác của TOE một cách trừu tượng, và người tiêu dùng tiềm năng có thể dựa vào mô tả này vì TOE đã được đánh giá đáp ứng cho ST đó. Dễ sử dụng và dễ hiểu là những vấn đề chính trong vai trò này. Mục A.11 mô tả một ST sẽ được sử dụng thế nào trong vai trò này.

A.3.2 Cách một ST không nên sử dụng

Có hai vai trò (trong số nhiều vai trò) mà một ST không nên đáp ứng là:

- *Một đặc tả chi tiết:* Một ST được thiết kế là một đặc tả an toàn ở một mức cao tương đối về sự trừu tượng. Một ST, nói chung, không chứa các đặc tả giao thức chi tiết, các mô tả chi tiết về thuật toán và/hay cơ chế, không mô tả nhiều về hoạt động chi tiết v.v...
- *Một đặc tả đầy đủ:* Một ST được thiết kế là một đặc tả an toàn và không phải là một đặc tả tổng quát. Ngoại trừ chức năng an toàn liên quan, các đặc tính như khả năng tương tác, kích cỡ và trọng lượng vật lý, điện thế yêu cầu..v.v có thể là một phần của ST. Điều này có nghĩa một ST nói chung có thể là một phần của một đặc tả hoàn chỉnh, nhưng bản thân nó không phải là một đặc tả hoàn chỉnh.

A.4 Giới thiệu ST (ASE_INT)

Giới thiệu về ST mô tả TOE trên ba mức trừu tượng:

a) Tham chiếu ST và tham chiếu TOE: cung cấp tư liệu nhận dạng ST và TOE mà ST tham chiếu tới;

b) Tổng quan về TOE: mô tả tóm tắt về TOE;

c) Mô tả TOE: mô tả chi tiết hơn về TOE;

A.4.1 Tham chiếu ST và tham chiếu TOE

Một ST gồm có phần tham chiếu rõ ràng về ST xác định cho từng ST cụ thể. Một ST điển hình bao gồm tựa đề, phiên bản, các tác giả và ngày phát hành. Ví dụ về một tham chiếu ST như sau "MauveRAM Database ST, phiên bản 1.3, Nhóm MauveCorp Specification, ngày 11 tháng 10 năm 2002".

Một ST cũng bao gồm cả tham chiếu TOE để định danh TOE, đòi hỏi tuân thủ với ST đó. Một tham chiếu TOE điển hình gồm tên nhà phát triển, tên TOE và số phiên bản TOE. Ví dụ như "MauveCorp MauveRAM Database v2.11". Vì một TOE đơn lẻ có thể được đánh giá nhiều lần, ví dụ bởi những người tiêu dùng khác nhau của TOE này, do đó có nhiều ST, nên phần tham chiếu này không phải là cái nhất thiết duy nhất.

Nếu TOE được tạo nên từ một hoặc nhiều sản phẩm nổi tiếng, sẽ được phép thể hiện điều đó trong phần tham chiếu TOE, bằng cách tham chiếu đến tên (các) sản phẩm. Tuy nhiên, điều đó không nên dùng để gây nhầm lẫn cho khách hàng: các trường hợp trong đó những phần chính hay những chức

năng an toàn không được xem xét trong đánh giá, do đó tham chiếu TOE không phản ánh điều này, là không được phép.

Tham chiếu ST và tham chiếu TOE tạo điều kiện cho việc lập chỉ mục, tham chiếu đến ST và TOE và đưa chúng vào tóm tắt danh sách các TOE/ các sản phẩm đã được đánh giá,

A.4.2 Tổng quan về TOE

Tổng quan TOE nhằm hướng tới những khách hàng tiềm năng của TOE, giúp họ lướt nhanh qua danh mục các TOE/các sản phẩm đã đánh giá để tìm kiếm các TOE có khả năng đáp ứng cho nhu cầu an toàn của họ, và được hỗ trợ bởi phần cứng, phần mềm và phần sụn của chúng. Chiều dài thông thường của phần tổng quan TOE khoảng vài đoạn văn bản.

Cuối cùng, phần tổng quan TOE mô tả tóm tắt cách sử dụng TOE và những đặc điểm an toàn chính của nó, chỉ rõ loại TOE và xác định bất kỳ phần cứng/phần mềm/phần sụn chủ yếu nào phi- TOE được yêu cầu bởi TOE.

A.4.2.1 Cách sử dụng và các đặc điểm an toàn chính của một TOE

Việc mô tả cách sử dụng và các đặc điểm an toàn chính của TOE chủ ý đưa ra một ý tưởng chung về việc TOE có khả năng về an toàn thế nào, và nó có thể sử dụng trong một ngữ cảnh an toàn thế nào. Nên biên soạn chúng cho những khách hàng (tiềm năng) của TOE, mô tả cách sử dụng TOE và các đặc điểm an toàn chính theo các hoạt động kinh doanh, sử dụng ngôn ngữ mà khách hàng TOE hiểu được.

Ví dụ "MauveCorp MauveRAM Database v2.11 là một cơ sở dữ liệu nhiều người dùng được hướng đến việc sử dụng trong một môi trường mạng. Nó cho phép 1024 người dùng sử dụng đồng thời. Nó cho phép xác thực mật khẩu/thẻ và sinh trắc học, bảo vệ chống lại việc dữ liệu bị hư hỏng đột ngột, và có thể kéo lại 10 nghìn giao dịch. Các đặc điểm kiểm chứng của nó có khả năng cấu hình cao, do đó cho phép thực hiện kiểm chứng chi tiết cho một số người dùng và giao dịch trong khi bảo vệ quyền riêng tư của những người dùng và giao dịch khác."

A.4.2.2 Kiểu TOE

Phần tổng quan TOE xác định kiểu TOE chung, chẳng hạn như: tường lửa, tường lửa VPN, thẻ thông minh, modem mã hóa, intranet, web server, cơ sở dữ liệu, web server và cơ sở dữ liệu, LAN, LAN với web server và cơ sở dữ liệu, v.v...

Có thể có trường hợp TOE không phải là kiểu sẵn sàng để dùng, trong trường hợp này từ "không" ghi cho kiểu TOE được chấp thuận.

Trong một vài trường hợp , một kiểu TOE có thể làm cho các khách hàng nhầm lẫn. Ví dụ:

- Chức năng nào đó có thể được mong đợi ở TOE do kiểu TOE của nó, nhưng TOE đó không có chức năng này. Ví dụ:

  + Một TOE kiểu thẻ ATM không hỗ trợ bất kỳ chức năng định danh/xác thực nào;

+ Một TOE kiểu firewall không hỗ trợ các giao thức được sử dụng hầu như phổ biến;

+ Một TOE kiểu PKI không có chức năng thu hồi chứng chỉ.

- TOE có thể được mong đợi hoạt động trong những môi trường vận hành nhất định vì kiểu TOE của nó, nhưng nó không thể làm như vậy. Ví dụ:

  + Một TOE kiểu hệ điều hành PC không có khả năng hoạt động an toàn trừ khi PC đó không kết nối mạng, không có ổ đĩa mềm và không có ở đĩa CD/DVD-player;

  + Một tường lửa không có khả năng hoạt động an toàn trừ khi tất cả người dùng có kết nối qua tường lửa này đều là những người không phải là tin tặc.

A.4.2.3 Phần cứng/phần mềm/phần sụn phi- TOE cần thiết

Trong khi một số TOE không dựa vàoCNTTkhác, thì có nhiều TOE (đặc biệt là các TOE phần mềm) dựa trên vào phần cứng, phần mềm và/hoặc phần sụn phi- TOE bổ sung thêm. Trong trường hợp thứ 2, phần tổng quan TOE là cần thiết để xác định phần cứng, phần mềm và/hoặc phần sụn phi- TOE đó. Một định danh chi tiết và thực sự đầy đủ của phần cứng, phần mềm và/hoặc phần sụn bổ sung là không cần thiết, nhưng việc định danh nên đầy đủ và chi tiết đủ để người tiêu dùng tiềm năng xác định được phần cứng, phần mềm và/hoặc phần sụn chính đáp ứng cho nhu cầu sử dụng TOE.

Ví dụ về các định danh phần cứng/phần mềm/phần sụn này là:

- Một PC chuẩn với bộ xử lý 1GHz hoặc nhanh hơn và RAM 512MB hoặc hơn, chạy phiên bản 3.0 Update 6b, c hoặc 7 hoặc phiên bản 4.0 của hệ điều hành Yaiza;
- Một PC chuẩn với bộ xử lý 1GHz hoặc nhanh hơn và RAM 512MB hoặc hơn, chạy phiên bản 3.0 Update 6b, c hoặc 7 hoặc phiên bản 4.0 của hệ điều hành Yaiza và cạc đồ họa WonderMagic 1.0 với bộ Driver WM 1.0;
- Một PC chuẩn với phiên bản 3.0 của Yaiza OS (hoặc cao hơn)
- Một mạch tích hợp CleverCard SB2067;
- Một mạch tích hợp CleverCard SB2067 chạy v2.0 của hệ điều hành thẻ thông minh QuickOS;
- Bản cài đặt cài đặt mạng LAN tháng 12 năm 2002 của Văn phòng Giám Đốc Sở Giao Thông.

A.4.3 Mô tả TOE

Một mô tả TOE là một mô tả tường tận về TOE, có thể dài nhiều trang. Mô tả TOE nên đưa ra cho những đánh giá viên và người tiêu dùng tiềm năng những hiểu biết chung về khả năng an toàn của TOE, chi tiết hơn sẽ được cung cấp trong phần tổng quan về TOE. Mô tả TOE cũng có thể mô tả ngữ cảnh ứng dụng rộng hơn phù hợp với TOE.

Mô tả TOE bàn đến phạm vi vật lý của TOE: danh sách tất cả các phần cứng, phần mềm, phần sụn và các phần hướng dẫn tạo thành TOE. Danh sách này nên được mô tả ở mức độ chị tiết đủ để đưa ra cho người đọc cái nhìn chung nhất về những thành phần đó.

Mô tả TOE cũng nên bàn về phạm vi logic của TOE: các đặc điểm an toàn về mặt logic cung cấp bởi TOE ở một mức độ chi tiết phù hợp để đưa cho người đọc cái nhìn chung về những đặc điểm đó. Mô tả này được đòi hỏi chi tiết hơn so với các đặc điểm an toàn chủ yếu mô tả trong phần tổng quan TOE.

Một đặc tính quan trọng về phạm vi vật lý và logic của TOE là chúng mô tả TOE theo cách mà ở đó không có sự hồ nghi nào về việc một phần hay một đặc điểm nào đó là trong TOE hay không, hoặc phần đó hay đặc điểm đó là bên ngoài TOE hay không. Điều này đặc biệt quan trọng khi TOE được kết hợp với và không thể dễ dàng tách ra khỏi các thực thể phi-TOE.

Các ví dụ về việc TOE được kết hợp với các thực thể phi-TOE là:

- TOE là một bộ đồng xử lý mật mã của IC thẻ thông minh, thay vì toàn bộ IC;
- TOE là một IC thẻ thông minh, ngoại trừ bộ xử lý mật mã;
- TOE là phần chuyển đổi địa chỉ mạng (NAT) của MinuteGap Firewall v18.5.

A.5 Các tuyên bố tuân thủ (ASE_CCL)

Mục này của một ST mô tả cách thức ST tuân thủ với:

- Phần 2 và Phần 3 của Tiêu chuẩn này;
- Hồ sơ bảo vệ (nếu có);
- Các gói (nếu có);

Các mô tả về cách ST tuân thủ với TCVN 8709 bao gồm hai phần: phiên bản của ISO /IEC 15408 đã sử dụng và liệu các ST có chứa các yêu cầu an toàn mở rộng hay không (xem A.8).

Các mô tả về sự tuân thủ của ST với Hồ sơ Bảo vệ, có nghĩa là ST liệt kê các gói đang yêu cầu tuân thủ. Để giải thích về điều này, xem 9.4.

Các mô tả về sự tuân thủ của ST với các gói, có nghĩa là ST liệt kê các gói đang yêu cầu tuân thủ. Để giải thích về điều này, xem 9.4.

A.6 Định nghĩa vấn đề an toàn (ASE_SPD)

A.6.1 Giới thiệu

Định nghĩa vấn đề an toàn xác định vấn đề an toàn cần đề cập đến. Định nghĩa vấn đề an toàn là một điều hiển nhiên trong TCVN 8709. Như vậy, quá trình đi đến định nghĩa vấn đề an toàn nằm ngoài phạm vi của TCVN 8709.

Tuy nhiên, cần lưu ý rằng, tính hữu ích của kết quả đánh giá phụ thuộc rất nhiều vào ST, và tính hữu ích của ST phụ thuộc nhiều vào chất lượng của định nghĩa vấn đề an toàn. Do đó, thật xác đáng khi dành nguồn lực đáng kể và sử dụng những quy trình và phân tích đã biết để đưa ra một định nghĩa tốt về vấn đề an toàn.

Lưu ý rằng theo TCVN 8709-3, không bắt buộc phải có các phát biểu trong tất cả các mục con, một ST với những mối đe dọa không nhất thiết cần có các OSP và ngược lại. Ngoài ra, mọi ST đều có thể bỏ qua các giả định.

Cũng lưu ý rằng tại những nơi TOE được phân phối về mặt vật lý, tốt hơn là nên bàn về các mối đe dọa liên quan, các OSP và các giả định riêng rẽ cho các miền riêng biệt của môi trường vận hành TOE.

A.6.2 Các mối đe dọa

Mục này của định nghĩa vấn đề an toàn chỉ ra các mối đe dọa được tính đến bởi TOE, môi trường vận hành của TOE, hay kết hợp của cả hai.

Một mối đe dọa bao gồm một hành động có hại được thực hiện bởi một tác nhân gây nguy cơ trên một tài sản.

Những hành động có hại là những hành động thực hiện bởi một tác nhân gây nguy cơ trên một tài sản. Những hành động này ảnh hưởng đến một hoặc nhiều đặc tính của một tài sản mà giá trị tài sản xác định từ các đặc tính đó.

Những tác nhân gây nguy cơ có thể được mô tả như những thực thể riêng, nhưng trong một số trường hợp sẽ tốt hơn nếu mô tả chúng theo từng loại thực thể, các nhóm thực thể, v.v...

Ví dụ về các tác nhân gây hại là những tin tặc, người dùng, các tiến trình máy tính, và các tai họa. Những tác nhân gây hại có thể được mô tả hơn nữa về các mặt như kinh nghiệm, nguồn lực, cơ hội và động lực.

Ví dụ về các mối đe dọa là:

- Một tin tặc (có chuyên môn đáng kể, thiết bị chuẩn, và được trả tiền để làm điều đó) sẽ sao chép từ xa các tập tin mật từ một mạng máy tính công ty;
- Một sâu máy tính sẽ làm xuống cấp nghiêm trọng hiệu năng của một mạng máy tính diện rộng;
- Một quản trị viên hệ thống vi phạm quyền riêng tư cá nhân người dùng;
- Một người nào đó trên Internet nghe lén giao tiếp điện tử mật;

A.6.3 Các chính sách an toàn của tổ chức tổ chức (OSPs)

Mục này trong định nghĩa vấn đề an toàn cho thấy OSP cần được thực thi bởi TOE, môi trường vận hành của nó, hoặc sự kết hợp của cả hai.

OSP là những quy tắc, thủ tục, hoặc hướng dẫn an toàn được áp đặt (hoặc coi là sẽ áp đặt) hiện tại và/hoặc trong tương lai bởi một tổ chức thực tế hoặc giả thuyết trong môi trường vận hành. OSP có thể được đặt ra bởi một tổ chức kiểm soát môi trường vận hành của TOE, hoặc chúng có thể được đặt ra bởi các cơ quan lập pháp hay điều tiết. OSP có thể áp dụng cho các TOE và / hoặc môi trường vận hành của các TOE.

Ví dụ về các OSP là:

- Tất cả các sản phẩm được sử dụng bởi Chính phủ phải tuân thủ theo tiêu chuẩn quốc gia trong việc mã hóa và việc phát sinh mật khẩu;
- Chỉ những người dùng có đặc quyền Quản trị Hệ thống và được phép của phòng kiểm tra an ninh mới được phép quản trị máy chủ của cơ quan.

A.6.4 Các giả định

Mục này của định nghĩa vấn đề an toàn chỉ ra các giả định cho môi trường vận hành để có thể cung cấp chức năng an toàn. Nếu TOE được đặt trong một môi trường vận hành không đáp ứng được các giả định này, thì TOE có thể không có khả năng cung cấp tất cả các chức năng an toàn nữa. Những giả định có thể về mặt vật lý, con người và kết nối của môi trường vận hành.

Ví dụ về các giả định là:

- Các giả định về các khía cạnh vật lý của môi trường vận hành:
  - Giả định là TOE sẽ được đặt trong một căn phòng được thiết kế để giảm thiểu phát xạ điện từ;
  - Giả định là các bàn điều khiển quản trị của TOE sẽ được đặt trong một khu vực hạn chế truy cập.
- Các giả định về khía cạnh con người của môi trường vận hành:
  - Giả định là người dùng TOE sẽ được đào tạo đầy đủ để vận hành TOE;
  - Giả định là người dùng TOE chấp thuận những thông tin được phân loại là Bí mật Quốc gia;
  - Giả định là người dùng TOE sẽ không viết ra mật khẩu của họ.
- Giả định các khía cạnh kết nối của môi trường vận hành:
  - Giả định là một máy trạm PC có ít nhất 10GB không gian đĩa sẵn cho việc chạy TOE trên đó;
  - Giả định là TOE là ứng dụng phi-OS duy nhất đang chạy trên máy trạm này;
  - Giả định là TOE sẽ không kết nối với một mạng không tin cậy.

Lưu ý rằng trong quá trình đánh giá, những giả định này được coi là đúng: chúng không được kiểm tra theo bất kỳ cách nào. Vì những lý do này, các giả định chỉ có thể được tạo ra trên môi trường vận hành. Những giả định có thể chưa bao giờ được tạo ra trên hành vi của TOE vì một đánh giá bao gồm các xác nhận đánh giá được tạo ra về TOE và không phải bằng cách giả định là các xác nhận trên TOE là đúng.

A.7 Các mục tiêu an toàn (ASE_OBJ)

Các mục tiêu an toàn là một phát biểu ngắn gọn và trừu tượng về giải pháp dự kiến cho vấn đề được xác định trong định nghĩa vấn đề an toàn. Vai trò của các mục tiêu an toàn là:

- Cung cấp một giải pháp bậc cao, theo ngôn ngữ tự nhiên cho vấn đề;

- Chia giải pháp này thành hai giải pháp từng phần, phản ánh các thực thể khác nhau, mỗi giải pháp đề cập đến một phần của vấn đề;
- Diễn giải rằng các giải pháp từng phần nêu trên hình thành nên một giải pháp hoàn chỉnh cho vấn đề.

A.7.1 Giải pháp mức cao

Các mục tiêu an toàn bao gồm một tập hợp các phát biểu ngắn gọn và rõ ràng mà không quá chi tiết, phối hợp với nhau hình thành một giải pháp mức cao cho vấn đề an toàn. Mức độ trừu tượng của các mục tiêu an toàn nhằm vào tính rõ ràng và dễ hiểu giúp cho người tiêu dùng tiềm năng có thể hiểu được TOE đó. Các mục tiêu an toàn thể hiện theo ngôn ngữ tự nhiên.

A.7.2 Các giải pháp từng phần

Trong một ST, giải pháp an toàn mức cao, như được mô tả với các mục tiêu an toàn, sẽ được chia thành hai giải pháp từng phần. Những giải pháp từng phần này được gọi là các mục tiêu an toàn cho TOE và các mục tiêu an toàn cho môi trường vận hành. Điều này phản ánh rằng các giải pháp từng phần sẽ được cung cấp bởi hai thực thể khác nhau: TOE, và môi trường vận hành.

A.7.2.1 Các mục tiêu an toàn cho TOE

TOE cung cấp chức năng an toàn để giải quyết một phần nhất định của vấn đề được xác định trong định nghĩa vấn đề an toàn. Giải pháp từng phần này được gọi là các mục tiêu an toàn chơ TOE và nó bao gồm một tập các mục tiêu mà TOE nên đạt được để giải quyết phần vấn đề của nó.

Ví dụ về các mục tiêu an toàn cho TOE là:

- TOE phải giữ bí mật nội dung của tất cả các tệp được truyền giữa nó và một máy chủ;
- TOE phải định danh và xác thực tất cả người dùng trước khi cho phép họ truy cập tới Dịch vụ truyền phát cung cấp bởi TOE;
- TOE phải hạn chế người dùng truy cập vào dữ liệu theo chính sách Truy cập Dữ liệu được mô tả trong Phụ lục 3 của ST.

Nếu TOE được phân phối về mặt vật lý, tốt hơn là chia nhỏ điều khoản ST chứa các mục tiêu an toàn cho TOE thành một vài mục con để phản ánh điều này.

A.7.2.2 Các mục tiêu an toàn cho môi trường vận hành

Môi trường vận hành của TOE thực hiện các biện pháp kỹ thuật và thủ tục để hỗ trợ TOE cung cấp đúng chức năng an toàn của nó (được định nghĩa bởi các mục tiêu an toàn cho TOE). Giải pháp từng phần này được gọi là các mục tiêu an toàn cho môi trường vận hành và bao gồm một tập hợp các phát biểu mô tả các mục tiêu mà môi trường vận hành cần đạt được.

Ví dụ về các mục tiêu an toàn đối với môi trường vận hành là:

- Môi trường vận hành phải cung cấp một máy trạm với hệ điều hành Inux OS phiên bản 3.01b để thực thi TOE trên đó;
- Môi trường vận hành phải đảm bảo rằng tất cả người dùng TOE được đào tạo thích hợp trước khi cho phép họ làm việc với TOE;
- Môi trường vận hành của TOE phải giới hạn truy cập vật lý vào TOE cho nhân viên hành chính và cho nhân viên bảo trì có nhân viên hành chính kèm theo;
- Môi trường vận hành phải đảm bảo tính bí mật của các bản ghi kiểm toán tạo ra bởi TOE trước khi gửi chúng tới máy chủ kiểm toán trung tâm.

Nếu môi trường vận hành của TOE bao gồm nhiều địa điểm, mỗi địa điểm có những đặc tính khác nhau, tốt hơn là chia nhỏ điều khoản ST chứa các mục tiêu an toàn cho môi trường vận hành thành các mục nhỏ để phản ánh điều này.

A.7.3 Mối quan hệ giữa các mục tiêu an toàn và định nghĩa vấn đề an toàn

ST cũng chứa một sở cứ cho các mục tiêu an toàn với hai mục con như sau:

- Một dấu vết chỉ ra các mục tiêu an toàn nào nhắm tới các mối đe dọa, các OSP và những giả định nào;
- Một tập các biện minh chỉ ra tất cả các mối đe dọa, các OSP, và các giả định được đề cập đến một cách hiệu quả qua các mục tiêu về an toàn.

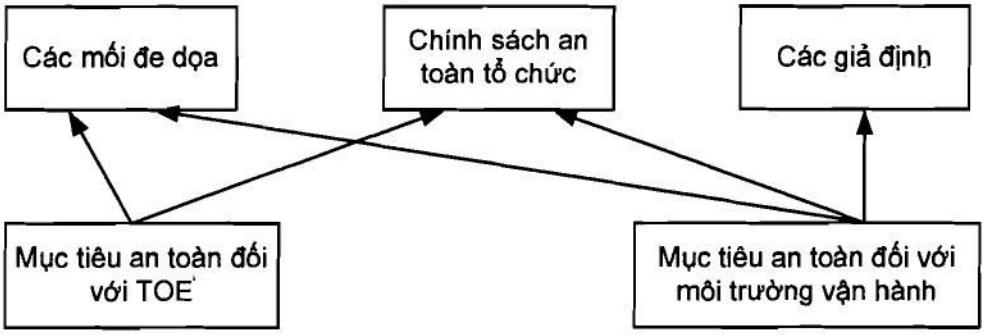
A.7.3.1 Dấu vết giữa các mục tiêu an toàn và định nghĩa vấn đề an toàn

Dấu vết cho thấy cách các mục tiêu toàn truy dấu vết các mối đe dọa, các OSP và các giả định như mô tả trong định nghĩa vấn đề an toàn.

a) *Không mục tiêu giả mạo:* Mỗi mục tiêu an toàn ghi vết theo ít nhất một mối đe dọa, một OSP hoặc một giả định.

b) *Hoàn thành theo định nghĩa vấn đề an toàn:* Mỗi mối đe dọa, OSP và giả định có ít nhất một dấu vết mục tiêu an toàn ghi theo nó.

c) *Ghi vết đúng:* Vì những giả định luôn được tạo bởi TOE trên môi trường vận hành, các mục tiêu an toàn cho TOE không truy vết về những giả định. Các dấu vết được phép trong TCVN 8709-3 được miêu tả trong Hình A.2.



Hình A.2 - Dấu vết giữa các mục tiêu an toàn và định nghĩa vấn đề an toàn

Nhiều mục tiêu an toàn có thể ghi vết theo cùng mối đe dọa, biểu thị rằng sự kết hợp của các mục tiêu an toàn là để chống lại mối đe dọa đó. Một luận cứ tương tự cũng dùng cho các OSP và các giả định.

A.7.3.2 Cung cấp biện minh cho việc ghi vết

Sở cứ cho các mục tiêu an toàn cũng diễn giải rằng lviệc ghi vết có hiệu quả: Tất cả các mối đe dọa, các OSP và các giả định được đề cập đến (nghĩa là được đối phó, thực thi và gìn giữ thích đáng) nếu có được tất cả các dấu vết cho các mục tiêu an toàn đến một mối đe dọa, một OSP hoặc một giả định cụ thể.

Luận cứ này phân tích tác động của việc đạt được các mục tiêu an toàn tương ứng về việc chống lại các mối đe dọa, việc thực thi các OSP và duy trì các giả định để đưa đến kết luận rằng luận cứ trên là đúng.

Trong một số trường hợp, khi các phần của định nghĩa vấn đề an toàn rất giống với một số mục tiêu an toàn, thì luận cứ có thể rất đơn giản. Một ví dụ là: một mối đe dọa "T17: tác nhân gây nguy cơ X đọc được các Thông tin Bí mật truyền qua lại giữa A và B", một mục tiêu an toàn cho TOE: "OT12: TOE phải đảm bảo rằng tất cả các thông tin được truyền giữa A và B được giữ bí mật", và một luận cứ "T17 được đối phó trực tiếp bằng OT12"

A.7.3.3 Chống lại các mối đe dọa

Chống lại một mối đe dọa không cần thiết có nghĩa là loại bỏ mối đe dọa đó, nó có thể cũng nghĩa là giảm thiểu mối đe dọa đó, hoặc giảm nhẹ mối đe dọa.

Ví dụ về loại bỏ một mối đe dọa là:

- Loại bỏ khả năng thực hiện hành động có hại từ tác nhân gây hại;
- Di chuyển, thay đổi hoặc bảo vệ tài sản theo một cách mà hành động có hại không còn áp dụng đối với nó được nữa;
- Loại bỏ các tác nhân gây nguy cơ (ví dụ loại bỏ các máy trong một mạng máy tính thường xuyên làm sập mạng đó).

Ví dụ về làm giảm nhẹ một mối đe dọa là:

- Hạn chế khả năng của tác nhân gây hại thực hiện các hành động có hại;
- Hạn chế cơ hội để thực hiện một hành động có hại của một tác nhân gây hại;
- Giảm khả năng xảy ra của một hành động có hại đang được thực hiện thành công;
- Giảm động lực để thực hiện một hành động có hại của một tác nhân gây hại bằng cách làm nhụt chí;
- Yêu cầu chuyên môn cao hơn hoặc nhiều tài nguyên hơn từ phía tác nhân gây nguy cơ.

Ví dụ về giảm tác động của một mối đe dọa là:

- Tạo back-up thường xuyên của tài sản đó;
- Có được bản sao dự phòng của một tài sản;
- Bảo hiểm tài sản;
- Đảm bảo rằng khi các hành động có hại thành công thì luôn kịp thời phát hiện, từ đó có thể đưa ra hành động thích hợp.

A.7.4 Các mục tiêu an toàn: kết luận

Căn cứ vào các mục tiêu an toàn và sở cứ các mục tiêu an toàn an toàn, kết luận sau đây có thể được rút ra: nếu tất cả các mục tiêu an toàn đạt được thì vấn đề an toàn như đã định nghĩa trong ASE_SPD được giải quyết: tất cả các mối đe dọa sẽ được chống lại; tất cả các OSP được thi hành, và tất cả các giả định được gìn giữ.

A.8 Định nghĩa các thành phần mở rộng (ASE_ECD)

Trong nhiều trường hợp, các yêu cầu an toàn (xem A.9) trong một ST dựa trên các thành phần trong TCVN 8709-2 hoặc TCVN 8709-2. Tuy nhiên, trong một số trường hợp, có thể có các yêu cầu trong một ST không dựa trên các thành phần trong TCVN 8709-2 hoặc TCVN 8709-2. Trong trường hợp này, các thành phần mới (các thành phần mở rộng) cần được định nghĩa, và việc định nghĩa này nên thực hiện trong phần "Định nghĩa các thành phần mở rộng". Để có thêm thông tin, xem Phụ lục C.4.

Lưu ý rằng, mục này chỉ bao gồm các thành phần mở rộng và chứ không gồm những yêu cầu mở rộng (những yêu cầu dựa trên các thành phần mở rộng). Những yêu cầu mở rộng sẽ được đặt trong những yêu cầu an toàn (xem A.9) và cũng là những yêu cầu dựa trên các thành phần trong TCVN 8709-2 hoặc TCVN 8709-3 đối với mọi mục đích.

A.9 Các yêu cầu an toàn (ASE_REQ)

Các yêu cầu an toàn bao gồm hai nhóm sau:

a) *Các yêu cầu về chức năng an toàn (SFR):* Chuyển đổi các mục tiêu an toàn cho TOE sang một ngôn ngữ chuẩn hóa;

b) *Các yêu cầu về đảm bảo an toàn (SAR):* Mô tả cách đạt được sự đảm bảo là TOE đáp ứng các SFR.

Hai nhóm này được thảo luận trong A.9.1 và A.9.2.

A.9.1 Các yêu cầu về chức năng an toàn (SFR)

Các SFR là một bản dịch của các mục tiêu an toàn cho TOE. Chúng thường ở mức độ trừu tượng chi tiết hơn, nhưng chúng phải là một bản dịch hoàn chỉnh (các mục tiêu an toàn phải được đề cập đến một cách đầy đủ) và độc lập với bất kỳ giải pháp kỹ thuật cụ thể nào (sự thực thi). TCVN 8709 yêu cầu chuyển đổi sang một ngôn ngữ chuẩn hóa vì những lý do:

- Để cung cấp một mô tả chính xác về những gì đang được đánh giá. Vì các mục tiêu an toàn cho TOE thường được phát biểu theo ngôn ngữ tự nhiên, nên việc chuyển đổi sang một ngôn ngữ chuẩn hóa cho một mô tả chính xác hơn về chức năng của TOE.
- Để cho phép so sánh giữa hai ST. Vì các tác giả ST khác nhau có thể sử dụng thuật ngữ khác nhau trong việc mô tả các mục tiêu an toàn của họ, nên ngôn ngữ chuẩn hóa ép buộc sử dụng cùng một thuật ngữ và khái niệm. Điều này cho phép dễ dàng so sánh.

Trong TCVN 8709 không yêu cầu có sự chuyển đổi cho các mục tiêu an toàn đối với môi trường vận hành, bởi vì không đánh giá môi trường vận hành và do đó không đòi hỏi việc mô tả nhằm cho việc đánh giá đó. Xem tài liệu tham khảo cho các danh mục liên quan đến đánh giá an toàn cho các hệ thống vận hành.

Có thể có trường hợp, các phần của môi trường vận hành được đánh giá trong một đánh giá khác, nhưng điều này nằm ngoài phạm vi đối với việc đánh giá hiện tại. Ví dụ: một TOE OS có thể yêu cầu một tường lửa hiện diện trong môi trường vận hành của nó. Một đánh giá khác có thể tiếp tục đánh giá bức tường lửa này, song đánh giá này không liên quan gì đến việc đánh giá TOE OS.

A.9.1.1 ISO/IEC 15.408 hỗ trợ việc chuyển đổi này thế nào

TCVN 8709 hỗ trợ việc chuyển đổi trên theo ba cách:

a) Bằng cách cung cấp một "ngôn ngữ" rõ ràng xác định trước, dành cho việc mô tả chính xác những gì sẽ được đánh giá. Ngôn ngữ này cũng được định nghĩa là một tập các thành phần đã được định nghĩa trong TCVN 8709-2. Việc sử dụng ngôn ngữ này để chuyển đổi rành mạch các mục tiêu an toàn cho TOE thành các SFR là bắt buộc, cho dù tồn tại một số ngoại lệ (xem 7.3).

b) Bằng cách cung cấp các hoạt động: các cơ chế cho phép tác giả của ST sửa đổi các SFR để cung cấp một bản dịch chính xác hơn cho các mục tiêu an toàn cho TOE. Phần này của TCVN 8709 định nghĩa bốn hoạt động được phép: Ấn định, lựa chọn, lặp lại, và bổ sung chi tiết. Những điều này sẽ được mô tả rõ hơn trong C.2.

c) Bằng cách đưa ra những phụ thuộc: một cơ chế hỗ trợ một bản dịch hoàn chỉnh hơn tới các SFR. Trong ngôn ngữ TCVN 8709-2, một SFR có thể có một sự phụ thuộc vào các SFR khác. Điều này có ý nghĩa rằng, nếu một ST sử dụng một SFR đó, nó thường cần phải sử dụng cả

những SFR khác đó. Điều này làm cho tác giả của ST không dễ dàng để bỏ qua những SFR cần thiết và do đó cải thiện tính đầy đủ của các ST. Sự phụ thuộc được mô tả rõ hơn trong 7.2.

A.9.1.2 Mối quan hệ giữa SFR và các mục tiêu an toàn

ST cũng chứa một sở cứ về những yêu cầu an toàn, bao gồm hai mục sau về SFR:

- Một dấu vết cho thấy những SFR nào nhắm tới các mục tiêu an toàn nào của TOE;
- Một tập các biện minh chỉ ra tất cả các mục tiêu an toàn cho TOE được đề cập đến một cách hiệu quả nhờ các SFR.

A.9.1.2.1 Dấu vết giữa SFR và các mục tiêu an toàn cho TOE

Dấu vết cho thấy các SFR truy vết các mục tiêu an toàn cho TOE như sau:

a) *Không có SFR giả mạo*: Mỗi dấu vết SFR truy vết tới ít nhất một mục tiêu an toàn .

b) *Hoàn thành theo các mục tiêu an toàn cho TOE*: Mỗi mục tiêu an toàn cho TOE có ít nhất một SFR truy vết đến nó.

Nhiều SFR có thể ghi vết đến cùng một mục tiêu an toàn cho TOE, điều này chỉ ra rằng sự kết hợp của những yêu cầu an toàn an toàn sẽ đáp ứng được mục tiêu an toàn của TOE.

A.9.1.2.2 Cung cấp biện minh cho ghi vết

Sở cứ cho những yêu cầu an toàn diễn giải rằng việc truy vết này có hiệu quả: nếu tất cả SFR truy vết đến một mục tiêu an toàn cụ thể đối với TOE được thỏa mãn, thì mục tiêu an toàn của TOE sẽ đạt được.

Luận cứ trên nên phân tích những ảnh hưởng của việc thỏa mãn SFR có liên quan về việc đạt được các mục tiêu an toàn cho TOE và đưa đến kết luận luận cứ trên là đúng.

Trong các trường hợp SFR rất gần giống các mục tiêu an toàn cho TOE, thì luận cứ có thể rất đơn giản.

A.9.2 Các yêu cầu đảm bảo an toàn (SAR)

Các SAR là mô tả về việc TOE được đánh giá thế nào. Mô tả này sử dụng một ngôn ngữ chuẩn hóa vì hai lý do sau:

- để cung cấp một mô tả chính xác về cách TOE được đánh giá. Sử dụng một ngôn ngữ chuẩn hóa hỗ trợ trong việc tạo ra một mô tả chính xác và tránh sự mơ hồ.
- để cho phép so sánh giữa hai ST. Vì các tác giả ST khác nhau có thể sử dụng thuật ngữ khác nhau khi mô tả việc đánh giá, nên ngôn ngữ chuẩn hóa thực thi bằng cách sử dụng cùng một thuật ngữ và khái niệm. Điều này cho phép dễ dàng so sánh.

Chuẩn hóa ngôn ngữ này được định nghĩa là một tập hợp các thành phần được định nghĩa trong TCVN 8709-3. Việc sử dụng ngôn ngữ này là bắt buộc, mặc dù có một số ngoại lệ tồn tại. TCVN 8709 nâng cao ngôn ngữ này theo hai cách:

a) cung cấp các hoạt động: các cơ chế cho phép tác giả của ST sửa đổi các SAR. TCVN 8709 có bốn hoạt động: chỉ định, lựa chọn, lặp lại, và bổ sung chi tiết. Những điều đó được mô tả rõ hơn trong 7.1.

b) đưa ra những phụ thuộc: một cơ chế hỗ trợ một bản dịch hoàn chỉnh hơn tới SFR. Trong ngôn ngữ TCVN 8709-2, một SFR có thể có một sự phụ thuộc vào các SFR khác. Điều này có ý nghĩa rằng, nếu một ST sử dụng một SFR đó, nó thường cần phải sử dụng cả những SFR khác đó. Điều này làm cho tác giả của ST không dễ dàng để bỏ qua những SFR cần thiết và do đó cải thiện tính đầy đủ của các ST. Sự phụ thuộc được mô tả rõ hơn trong 7.2.

A.9.3 Các SAR và sở cứ những yêu cầu an toàn

ST cũng chứa một sở cứ về các yêu cầu an toàn, giải thích lý do tại sao tập các SAR cụ thể này được coi là thích hợp. Không có yêu cầu đặc trưng nào cho lời giải thích này. Mục tiêu cho lời giải thích này là để cho phép người đọc ST để hiểu lý do tại sao tập đó được chọn.

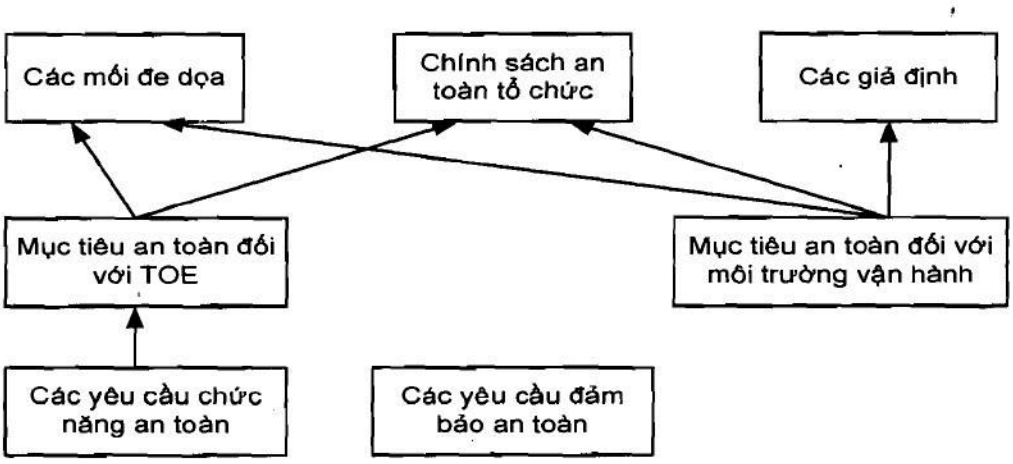
Một ví dụ về sự thiếu nhất quán là nếu mô tả vấn đề an toàn đề cập đến các mối đe dọa mà ở đó tác nhân gây hại là rất có khả năng, thì một ít (hoặc không) AVA_VAN được đưa vào trong SAR.

A.9.4 Những yêu cầu an toàn: kết luận

Trong định nghĩa vấn đề an toàn của ST, vấn đề an toàn được định nghĩa là bao gồm các mối đe dọa, các OSP và các giả định. Trong điều khoản về các mục tiêu an toàn của ST, giải pháp được đưa ra dưới dạng của hai giải pháp con:

- các mục tiêu an toàn cho TOE;
- các mục tiêu an toàn cho môi trường vận hành.

Ngoài ra, một sở cứ các mục tiêu an toàn được đưa ra cho thấy rằng nếu tất cả các mục tiêu an toàn đạt được, thì vấn đề an toàn được giải quyết: tất cả các mối đe dọa sẽ được chống lại, tất cả các OSP được thực thi, và tất cả các giả định được gìn giữ.



Hình A.3 - Quan hệ giữa định nghĩa vấn đề an toàn, các mục tiêu an toàn và các yêu cầu an toàn

Trong mục những yêu cầu an toàn của ST, các mục tiêu an toàn cho TOE được dịch sang SFR và sở cứ các yêu cầu an toàn được đưa ra cho thấy rằng nếu tất cả SFR được thỏa mãn, thì tất cả các mục tiêu an toàn cho TOE là đạt được.

Ngoài ra, một bộ SAR được cung cấp để thể hiện TOE được đánh giá thế nào, cùng với lời giải thích cho việc lựa chọn các SAR đó.

Tất cả điều bên trên có thể được kết hợp thành một phát biểu: Nếu tất cả SFR và SAR được thỏa mãn và tất cả các mục tiêu an toàn đối với các môi trường vận hành đều đạt được, thì sau đó tồn tại đảm bảo rằng vấn đề an toàn theo quy định tại ASE_SPD được giải quyết: tất cả các mối đe dọa sẽ được chống lại, tất cả OSP được thi hành, và tất cả các giả định được tôn trọng. Điều này được minh họa trong Hình A.3.

Lượng bảo đảm đạt được được định nghĩa bởi các SAR, và việc lượng này có đủ hay không được định nghĩa bởi phần giải thích về việc chọn các SAR này.

A.10 Đặc tả tóm tắt TOE (ASE_TSS)

Mục tiêu đối với đặc tả tóm tắt TOE là cung cấp tới người tiêu dùng tiềm năng của TOE một mô tả về TOE thỏa mãn tất cả các SFR như thế nào. Đặc tả tóm tắt TOE nên đưa ra các cơ chế kỹ thuật chung mà TOE sử dụng cho mục đích này. Mức độ chi tiết của mô tả đó nên đủ để cho phép người tiêu dùng tiềm năng hiểu được những dạng và sự thực thi chung của các TOE.

Ví dụ nếu TOE là một PC trên Internet và các SFR chứa FIA_UAU.1 để đặc tả việc xác thực, đặc tả tóm tắt TOE nên chỉ ra làm thế nào xác thực này được thực hiện: mật khẩu, token, quét võng mạc, vv. Các thông tin khác, như các tiêu chuẩn áp dụng mà TOE sử dụng để đáp ứng các SFR, hoặc mô tả chi tiết hơn cũng có thể được đưa ra.

A.11 Những câu hỏi có thể được trả lời với một ST

Sau khi đánh giá, ST quy định "những gì được đánh giá". Trong vai trò này, ST phục vụ như một cơ sở để thỏa thuận giữa các nhà phát triển hoặc người bán lại TOE và người tiêu dùng tiềm năng của các TOE đó. ST do đó có thể trả lời các câu hỏi sau đây (và nhiều hơn):

a) *Làm thế nào tôi có thể tìm thấy ST/TOE mà tôi cần trong vô số những ST/TOE đang hiện tại được đưa ra?* Câu hỏi này được đề cập trong phần tổng quan TOE, trong đó đưa ra một tóm tắt ngắn gọn (khoảng vài đoạn văn bản) cho TOE;

b) *TOE này có phù hợp với cơ sở hạ tầng CNTT hiện tại của tôi không?* Câu hỏi này được đề cập trong phần tổng quan TOE, trong đó xác định các phần tử phần cứng/phần mềm/phần sụn cần thiết để chạy TOE;

c) *TOE này có phù hợp với môi trường vận hành hiện tại của tôi không?* Câu hỏi này được đề cập trong phần các mục tiêu an toàn cho môi trường vận hành, trong đó xác định tất cả các hạn chế mà TOE đặt ra cho môi trường vận hành để hoạt động;

d) *TOE làm gì (những người đọc quan tâm)?* Câu hỏi này được đề cập trong phần tổng quan TOE, nó đưa ra một tóm tắt ngắn gọn (vài đoạn văn bản) về TOE;

e) *TOE làm gì (người tiêu dùng tiềm năng)?* Câu hỏi này được đề cập trong phần tổng quan TOE, nó đưa ra một tóm tắt ngắn gọn (vài trang) về TOE;

f) *TOE làm gì (kỹ thuật viên)?* Câu hỏi này được đề cập trong phần đặc tả tóm tắt TOE, ở đó cung cấp một mô tả mức cao về các cơ chế mà TOE sử dụng;

g) *TOE làm gì (chuyên gia)?* Câu hỏi này được đề cập trong các SFR, ở đó cung cấp một mô tả kỹ thuật trừu tượng mức cao và đặc tả tóm tắt TOE cung cấp chi tiết thông tin bổ sung;

h) *TOE có đề cập đến vấn đề theo quy định của chính phủ /tổ chức của tôi không?* Nếu chính phủ/tổ chức của bạn đã định nghĩa các gói và/hoặc các PP để xác định giải pháp này, thì câu trả lời có thể tìm thấy trong mục Các tuyên bố tuân thủ của ST, trong đó liệt kê tất cả các gói và các PP mà ST tuân thủ theo.

i) *Có TOE có đề cập đến vấn đề an toàn của tôi không (chuyên gia)?* Các mối đe dọa nào mà TOE chống lại được? Nó thực thi các chính sách bảo mật về mặt tổ chức nào? Nó tạo ra các giả định nào về môi trường vận hành? Những câu hỏi này được đề cập trong định nghĩa vấn đề an toàn;

j) *Tôi có thể tin cậy TOE đến mức nào?* Điều này có thể được tìm thấy trong các SAR ở mục những yêu cầu an toàn, ở đó cung cấp các cấp đảm bảo được sử dụng để đánh giá TOE, và do đó độ tin cậy mà việc đánh giá cung cấp trong tính chính xác của TOE.

A.12 Các đích an toàn đảm bảo mức thấp

Biên soạn một ST không phải là một công việc tầm thường, và có thể, đặc biệt là trong đánh giá đảm bảo mức thấp, đây là một phần chính trong toàn bộ nỗ lực bỏ ra của nhà phát triển và đánh giá viên trong toàn bộ quá tình đánh giá. Vì lý do này, cũng có thể viết một ST đảm bảo mức thấp.

TCVN 8709 cho phép sử dụng một ST đảm bảo mức thấp cho một đánh giá EAL 1, nhưng không dùng cho EAL 2 trở lên. Một ST đảm bảo thấp chỉ có thể đòi hỏi phù hợp với một PP đảm bảo thấp (xem Phụ lục B). Một ST thông thường (ví dụ, một ST có nội dung đầy đủ) có thể đòi hỏi phù hợp với một PP đảm bảo thấp.

Một ST đảm bảo thấp có giảm đáng kể nội dung so với một ST thông thường:

- không cần mô tả định nghĩa vấn đề an an toàn;
- không cần mô tả các mục tiêu an toàn cho TOE. Các mục tiêu an toàn cho môi trường vận hành vẫn phải được mô tả;
- không cần mô tả sở cứ các mục tiêu an toàn vì không có định nghĩa vấn đề an toàn trong ST;
- Sở cứ các yêu cầu an toàn chỉ cần để chứng tỏ sự phụ thuộc không được thỏa mãn vì không có những mục tiêu an toàn cho TOE trong ST này.

Tất cả những thứ ST vẫn duy trì là:

a) Các tham chiếu tới TOE và ST;

b) Một tuyên bố tuân thủ;

c) Các mô tả tường tận khác nhau;

1) Tổng quan TOE;

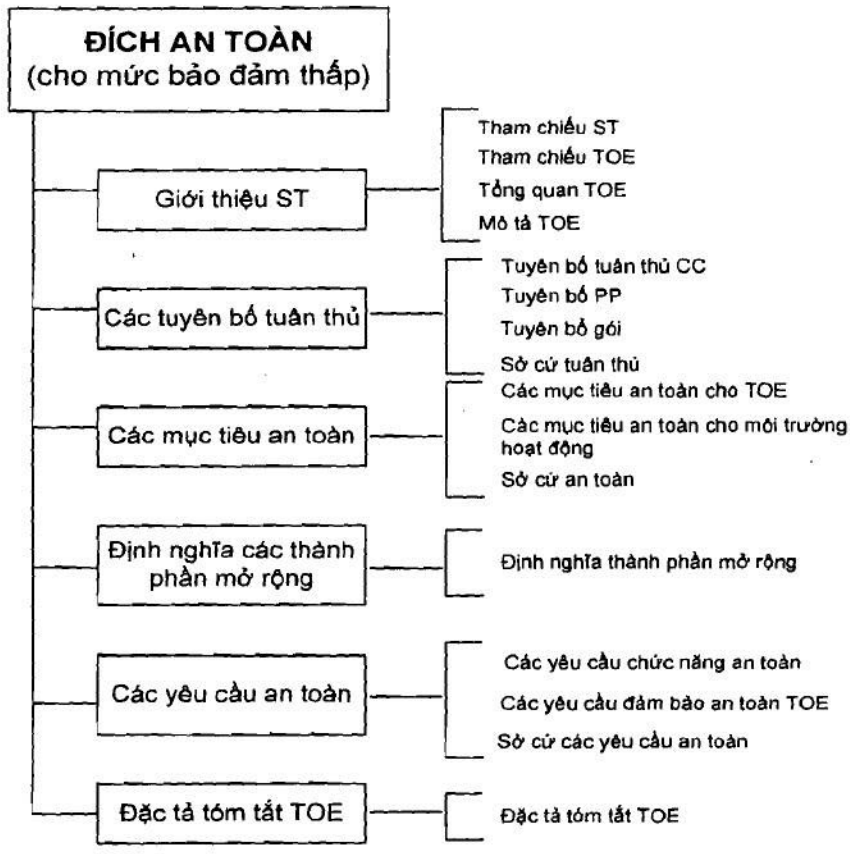
2) Mô tả TOE;

3) Đặc tả tóm tắt TOE.

d) Các mục tiêu an toàn cho môi trường vận hành;

e) Các SFR và SAR (bao gồm cả định nghĩa các thành phần mở rộng) và sở cứ các yêu cầu an toàn (chỉ khi sự phụ thuộc không được thỏa mãn).

Nội dung đã giản lược của một ST đảm bảo thấp được thể hiện trong Hình A.4.



Hình A.4 - Các nội dung của một đích an toàn đảm bảo mức thấp

A.13 Tham chiếu tới tiêu chuẩn khác trong một ST

Trong một số trường hợp, tác giả biên soạn ST có thể muốn tham chiếu tới một tiêu chuẩn bên ngoài, chẳng hạn như một tiêu chuẩn hoặc giao thức mã hóa cụ thể. TCVN 8709 cho phép ba cách thực hiện sau:

a) Như một chính sách an toàn về mặt tổ chức (hoặc một phần của nó).

Nếu, chẳng hạn, tồn tại một tiêu chuẩn chính phủ quy đinh mật khẩu phải được chọn ra sao, điều này có thể được phát biểu như một chính sách an toàn về tổ chức trong một ST. Điều này có thể một đối tượng cho môi trường (ví dụ nếu người sử dụng TOE cần chọn các mật khẩu phù hợp), hoặc nó có thể dẫn đến các mục tiêu an toàn cho TOE và tiếp đó cho các SFR thích hợp (giống như ở lớp FIA), nếu như TOE tạo ra các mật khẩu. Trong cả hai trường hợp, sở cứ mà nhà phát triển cần đưa ra hợp lý là các mục tiêu an toàn cho TOE và các SFR là phù hợp để đáp ứng OSP. Đánh giá viên sẽ kiểm tra nếu điều này thực tế là hợp lý (và có thể quyết định tra cứu tiêu chuẩn cho việc này), nếu OSP được thực thi bởi các SFR như được giải thích dưới đây.

b) Như một tiêu chuẩn kỹ thuật (ví dụ một tiêu chuẩn mật mã) được sử dụng trong một phép bổ sung chi tiết cho một SFR.

Trường hợp này, tuân thủ theo tiêu chuẩn là một phần của việc thỏa mãn các SFR bởi TOE và được xử lý như kiểu một văn bản đầy đủ của tiêu chuẩn là một phần của SFR. Tính tuân thủ tiếp đó được xác định giống như bất kỳ sự tuân thủ khác theo các SFR: trong ADV và ATE, nó được phân tích, qua

phân tích thiết kế và kiểm thử, để chỉ ra SFR là đầy đủ và được triển khai hoàn toàn trong TOE. Nếu chỉ muốn tham chiếu tới một phần nhất định của tiêu chuẩn, thì phần đó cần được nêu rõ ràng trong phần bổ sung chi tiết trong SFR.

c) Như một tiêu chuẩn kỹ thuật (ví dụ như một tiêu chuẩn mật mã) được đề cập trong đặc tả tóm tắt TOE.

Đặc tả tóm tắt TOE chỉ được xem xét đến như một giải thích về cách các SFR được thực hiện, và sử dụng không chặt chẽ như một yêu cầu thực thi chặt chẽ giống như SFR hoặc các tài liệu chuyển giao cho ADV. Như vậy, đánh giá viên có thể phát hiện một sự không nhất quán nếu TSS tham chiếu đến một tiêu chuẩn kỹ thuật và điều này không được phản ánh trong tài liệu ADV, nhưng không có động thái thường kỳ để kiểm thử sự đáp ứng của tiêu chuẩn.

Phụ lục B

(Tham khảo)

Đặc tả của Hồ sơ bảo vệ PP

B.1 Mục tiêu và cấu trúc của phụ lục

Mục tiêu của phụ lục này là giải thích các khái niệm Hồ sơ Bảo vệ (PP). Phụ lục này không định nghĩa các tiêu chí APE, định nghĩa này có thể được tìm thấy trong TCVN 8709-3 và các tài liệu tham khảo.

Vì PP và ST có chồng chéo đáng kể lên nhau, nên phụ lục này tập trung vào sự khác biệt giữa PP và ST . Các tài liệu giống hệt nhau giữa ST và PP được mô tả trong Phụ lục A.

Phụ lục này bao gồm bốn phần chính:

a) *Những gì một PP phải có.* Điều này được tóm tắt trong B.2, và mô tả chi tiết hơn trong B.4 đến B.9. Những điều khoản này mô tả các nội dung bắt buộc của PP, mối tương quan giữa những nội dung này, và đưa ra các ví dụ.

b) *Một PP nên được sử dụng như thế nào.* Điều này được tóm tắt trong B.3.

c) *PP đảm bảo thấp.* PP đảm bảo thấp là PP có nội dung được giản lược. Chúng được mô tả chi tiết trong B.11.

d) *Yêu cầu tuân thủ các tiêu chuẩn.* B.12 mô tả cách một tác giả PP có thể yêu cầu TOE là để đáp ứng một tiêu chuẩn cụ thể.

B.2 Các nội dung bắt buộc của một PP

Hình B.1 miêu tả nội dung bắt buộc đối với một PP mà TCVN 8709-3 đưa ra. Hình B.1 cũng có thể được sử dụng như là một phác thảo cấu trúc của PP, mặc dù cấu trúc thay thế được cho phép. Ví dụ, nếu các lý do những yêu cầu an toàn đặc biệt cồng kềnh, nó có thể được bao gồm trong một phụ lục của PP thay vì trong mục những yêu cầu an toàn. Các mục riêng biệt của một PP và nội dung của những mục đó được tóm tắt ngắn gọn dưới đây và được giải thích chi tiết hơn nữa trong B.4 đến B.9. Một PP chứa:

a) *Giới thiệu PP* chứa đựng một mô tả tường tận loại TOE;

b) *Một tuyên bố tuân thủ,* chỉ ra PP có tuân thủ với bất kỳ các PP và /hoặc các gói hay không, và nếu có, thì với các PP và /hoặc các gói nào.

c) *Một định nghĩa vấn đề an toàn*, chỉ ra các mối đe dọa, OSP và giả định;

d) *Các mục tiêu an toàn,* biểu thị giải pháp cho vấn đề an toàn được chia thành các mục tiêu an toàn cho TOE và mục tiêu an toàn cho môi trường vận hành của TOE;

e) *Định nghĩa các thành phần mở rộng*, ở đó các thành phần mới (tức là những thành phần không có trong TCVN 8709-2 hoặc TCVN 8709-3) có thể được định nghĩa. Các thành phần mới này cần được định nghĩa những yêu cầu chức năng mở rộng và yêu cầu đảm bảo mở rộng;

f) *Những yêu cầu an toàn*, ở đó những mục tiêu an toàn cho TOE được chuyển sang một ngôn ngữ tiêu chuẩn hóa. Ngôn ngữ tiêu chuẩn hóa này là ở dạng các SFR. Ngoài ra mục này còn định nghĩa các SAR;

Cũng tồn tại các PP đảm bảo mức thấp, chúng có các nội dung được giảm bớt; chúng được mô tả chi tiết trong B.11. Ngoài ngoại lệ này, tất cả các phần khác trong phụ lục này giả thiết một PP với đầy đủ các nội dung.

Hình B.1 - Các nội dung hồ sơ bảo vệ

B.3 Sử dụng PP

B.3.1 Một PP nên được sử dụng thế nào

Một PP điển hình là một phát biểu về sự cần thiết, trong đó cộng đồng người dùng, một thực thể pháp lý, hoặc một nhóm các nhà phát triển định nghĩa ra một tập hợp chung của các nhu cầu an toàn. Một PP cung cấp cho người tiêu dùng một phương tiện tham chiếu đến tập này, và tạo điều kiện cho đánh giá tương lai theo những nhu cầu này.

Một PP vì thế thường được sử dụng như:

- một phần của một đặc tả yêu cầu đối với một người tiêu dùng hoặc một nhóm người tiêu dùng xác định, những người sẽ chỉ xem xét việc mua một loại cụ thể của CNTT nếu nó đáp ứng PP;
- một phần của một quy định từ một thực thể pháp lý cụ thể, những người sẽ chỉ cho phép một loại cụ thể của CNTT được sử dụng nếu đáp ứng PP;
- một cơ sở giới hạn xác định bởi một nhóm các nhà phát triển CNTT, những người sẽ đồng ý rằng tất cả các sản phẩm CNTT mà họ sản xuất theo loại này sẽ đáp ứng cơ sở giới hạn này.

mặc dù điều này không ngăn cản các sử dụng khác của PP.

B.3.2 Cách một PP không nên được sử dụng

Ba vai trò (trong số nhiều vai trò) mà một PP không nên thực hiện là:

- *một đặc tả chi tiết*: Một PP được thiết kế để là một đặc tả an toàn trên một mức độ trừu tượng tương đối cao. Một PP nói chung, không nên chứa đặc tả giao thức chi tiết, những mô tả chi tiết về các thuật toán và/hoặc các cơ chế, mô tả dài về các hoạt động chi tiết, vv...
- *một đặc tả hoàn chỉnh*: Một PP được thiết kế để là một đặc tả an toàn và không phải là một đặc tả chung. Ngoại trừ liên quan đến an toàn, các đặc tính chẳng hạn như khả năng tương tác, kích thước và trọng lượng vật lý, điện áp yêu cầu vv... không nên là một phần của PP. Điều này có nghĩa rằng, một PP là một phần của một đặc tả hoàn chỉnh, nhưng không phải là một đặc tả hoàn chỉnh.
- *một đặc tả của một sản phẩm đơn lẻ*: Không giống như một ST, một PP được thiết kế để mô tả một kiểu sản phẩm CNTT, và không phải là một sản phẩm đơn lẻ. Khi chỉ có một sản phẩm được mô tả, sử dụng một ST sẽ tốt hơn cho mục đích này.

B.4 Giới thiệu PP (APE_INT)

Giới thiệu PP mô tả các TOE một cách tường tận theo hai mức độ trừu tượng:

a) tham chiếu PP, cung cấp tài liệu định danh cho PP;

b) tổng quan về TOE, trong đó mô tả ngắn gọn TOE.

B.4.1 Tham chiếu PP

PP chứa đựng một tham chiếu PP rõ ràng, định rõ một PP cụ thể. Một tham chiếu PP điển hình bao gồm tiêu đề, phiên bản, tác giả và ngày xuất bản. Ví dụ về một tham chiếu PP là "Atlantean Navy CablePhone Encryptor PP, phiên bản 2b, Atlantean Navy Procurement Office, 07 tháng 4 năm 2003". Tham chiếu phải là duy nhất để có thể kể đến PP khác và các phiên bản khác của cùng một PP.

Tham chiếu PP giúp lập chỉ mục dễ dàng và tham khảo các PP và đưa nó vào danh sách các PP.

B.4.2 Tổng quan TOE

Tổng quan TOE nhằm hướng tới những khách hàng tiềm năng của TOE, giúp họ lướt nhanh qua danh mục các TOE/sản phẩm đã được đánh giá để tìm kiếm TOE có khả năng đáp ứng cho nhu cầu an toàn của họ, và được hỗ trợ bởi phần cứng, phần mềm và phần sụn của họ.

Tổng quan TOE cũng nhằm hướng đến những nhà phát triển, những người có thể sử dụng PP trong việc thiết kế TOE hoặc trong trong sản phẩm tương thích hiện có.

Thông thường chiều dài của một tổng quan về TOE là một vài đoạn văn bản.

Cuối cùng, phần tổng quan TOE mô tả tóm tắt cách sử dụng của TOE và những đặc điểm an toàn chính của nó, chỉ rõ loại TOE và xác định bất kỳ phần cứng/phần mềm/phần phi-TOE chính nào sẵn dùng cho TOE.

B.4.2.1 Cách sử dụng và các đặc điểm an toàn chính của một TOE

Việc mô tả cách sử dụng và các đặc điểm an toàn chính của TOE được hướng đến để đưa ra một ý tưởng chung về TOE nào có khả năng, và TOE nào nó có thể sử dụng cho một bối cảnh an toàn. Nó có thể được viết cho những khách hàng (tiềm năng) của TOE, mô tả cách sử dụng TOE và các đặc điểm an toàn chính trong nhóm hoạt động kinh doanh, sử dụng ngôn ngữ mà người dùng TOE hiểu được.

Một ví dụ " The Atlantean Navy CablePhone Encryptor là một thiết bị mã hóa cho phép truyền thông tin bảo mật giữa các tàu qua hệ thống Atlantean Navy CablePhone. Nó cho phép ít nhất 32 người dùng khác nhau và hỗ trợ ít nhất là 100 Mbps tốc độ mã hóa. Nó sẽ cho phép cả hai giao tiếp song phương giữa các tàu và quảng bá trên toàn bộ mạng. "

B.4.2.2 Kiểu TOE

Tổng quan TOE xác định loại TOE chung, chẳng hạn như: tường lửa, tưởng lửa VPN, thẻ thông minh, modem mã hóa, intranet, web server, cơ sở dữ liệu, web server và cơ sở dữ liệu, LAN, LAN với web server và cơ sở dữ liệu, v.v...

B.4.2.3 Các phần cứng/phần mềm/phần sụn phi-TOE sẵn dùng

Trong khi một số TOE không dựa vào CNTT khác, nhiều TOE (đặc biệt là TOE phần mềm) dựa vào phi-TOE phần cứng, phần mềm và / hoặc phần sụn bổ sung. Trong trường hợp thứ hai, tổng quan về TOE là cần thiết để xác định các phi-TOE phần cứng / phần mềm / phần sụn.

Vì một hồ sơ bảo vệ không viết cho một sản phẩm cụ thể, nên trong nhiều trường hợp chỉ có một ý tưởng chung có thể là các phần cứng / phần mềm / phần sụn có sẵn được đưa ra. Trong một số trường hợp khác, ví dụ một đặc tả yêu cầu đối với một người tiêu dùng cụ thể như vậy sẽ có thêm (nhiều) thông tin cụ thể có thể được cung cấp.

Ví dụ về sự nhận biết các phần cứng / phần mềm / phần sụn này là:

• Không có. (đối với một TOE hoàn toàn độc lập);

• Hệ điều hành Yaiza 3,0 chạy trên một máy tính nói chung;

• Mạch tích hợp CleverCard SB2067;

• Một CleverCard SB2067 IC chạy v2.0 với hệ điều hành thẻ thông minh QuickOS;

• Bản cài đặt tháng 12 năm 2002 cho các mạng LAN của Văn phòng Giám đốc Sở Giao thông.

B.5 Các tuyên bố tuân thủ (APE_CCL)

Mục này của một PP mô tả cách thức PP tuân thủ với các PP khác và với các gói. Nó giống mục tuyên bố tuân thủ đối với ST (xem A.5), với một ngoại lệ: phát biểu tuân thủ.

Phát biểu tuân thủ trong PP tuyên bố về việc ST và / hoặc PP khác phải tuân thủ với PP đó như thế nào. Tác giả PP lựa chọn xem yêu cầu là tuân thủ "chặt chẽ" hay tuân thủ "biểu hiện". Phụ lục D sẽ cho biết thêm chi tiết về điều này.

B.6 Định nghĩa vấn đề an toàn (APE_SPD)

Mục này giống hệt mục định nghĩa vấn đề an toàn của một ST như được giải thích trong A.6.

B.7 Các mục tiêu an toàn (APE_OBJ)

Mục này giống hệt với các mục mục tiêu an toàn của một ST như được giải thích trong A.7.

B.8 Định nghĩa các thành phần mở rộng (APE_ECD)

Mục này giống hệt với mục định nghĩa các thành phần mở rộng của một ST như được giải thích trong A.8.

B.9 Những yêu cầu an toàn (APE_REQ)

Mục này giống hệt mục những yêu cầu an toàn của một ST như được giải thích trong A.9. Tuy nhiên lưu ý rằng các quy tắc để hoàn thành các hoạt động trong một PP hơi khác các quy tắc để hoàn thành các hoạt động trong một ST. Điều này được giải thích cụ thể hơn trong 7.1.

B.10 Đặc tả tóm tắt TOE

PP không có đặc tả kỹ thuật tóm tắt TOE.

B.11 Hồ sơ Bảo vệ đảm bảo thấp

Một PP đảm bảo thấp có cùng một mối quan hệ với một PP thông thường (PP có nội dung đầy đủ), cũng như một bảo đảm ST thấp có một ST thông thường. Điều này có nghĩa rằng một PP đảm bảo thấp bao gồm

a) Giới thiệu PP, bao gồm phần tham chiếu PP và tổng quan về một TOE;

b) Tuyên bố tuân thủ;

c) Các mục tiêu an toàn cho môi trường vận hành;

d) các SFR và SAR (bao gồm cả định nghĩa các thành phần mở rộng) và sở cứ yêu cầu an toàn (chỉ khi sự phụ thuộc không thỏa mãn).

Một PP đảm bảo thấp chỉ có thể tuyên bố tuân thủ với một PP đảm bảo thấp (xem B.5). Một PP thông thường có thể tuyên bố tuân thủ với một PP đảm bảo thấp.

Nội dung đã giản lược của một PP bảo đảm thấp được thể hiện trong Hình B.2.

Hình B.2 - Các nội dung một hồ sơ bảo vệ mức đảm bảo thấp

B.12 Tham chiếu đến các tiêu chuẩn khác trong PP

Mục này giống hệt mục các tiêu chuẩn cho ST như mô tả trong A.13, ngoại trừ: vì một PP không có đặc tả tóm tắt TOE, nên tùy chọn thứ ba là không hợp lệ cho PP.

Phụ lục C

(Tham khảo)

Hướng dẫn vận hành

C.1 Giới thiệu

Như được mô tả trong phần này của TCVN 8709, Hồ sơ Bảo vệ và Đích an toàn có chứa các yêu cầu an toàn được xác định trước, cũng như cung cấp cho tác giả của PP và ST khả năng mở rộng danh sách thành phần trong một số trường hợp.

C.2 Ví dụ về các hoạt động

Bốn loại hoạt động được đưa ra trong 7.1. Ví dụ về các hoạt động khác nhau được mô tả dưới đây:

C.2.1 Hoạt động lặp

Như được mô tả trong 7.1.1, hoạt động lặp có thể được thực hiện trên mỗi thành phần. Tác giả PP/ST thực hiện một hoạt động lặp lại bằng cách đưa vào nhiều yêu cầu cho cùng một thành phần. Mỗi lần lặp lại của một thành phần đều khác với tất cả các lần lặp lại khác của thành phần đó. Sự khác biệt này có được nhờ thực hiện chỉ định và lựa chọn theo cách khác nhau, hoặc áp dụng các bổ sung chi tiết theo cách khác nhau. Sự lặp lại khác nhau nên được xác định duy nhất để cho phép những sở cứ và dấu vết vào/ra các yêu cầu này được rõ ràng.

Một ví dụ điển hình của phép lặp là FCS_COP.1 được lặp hai lần để yêu cầu thực hiện hai thuật toán mã hóa khác nhau. Ví dụ về mỗi lần lặp lại được xác định duy nhất là:

Mật mã hoạt động (chữ ký RSA và DSA) (FCS_COP.1 (1))

Mật mã hoạt động (TLS / SSL: hoạt động đối xứng) (FCS_COP.1 (2))

C.2.2 Hoạt động chỉ định

Như mô tả trong 7.1.2, một hoạt động chỉ định xảy ra khi thành phần đưa ra chứa một phần tử với một tham số có thể được thiết lập bởi tác giả PP/ST. Tham số có thể là một biến không hạn chế, hay quy luật thu hẹp một biến số thành một dãy các giá trị cụ thể.

Một ví dụ của một phần tử chỉ định là: FIA_AFL.1.2 "Khi số lượng quy định của nỗ lực xác thực không thành công đạt được hoặc vượt qua, thì các TSF cần **[chỉ định: danh sách các hành động]**."

C.2.3 Hoạt động lựa chọn

Như mô tả trong 7.1.3, hoạt động lựa chọn xảy ra khi thành phần đưa ra chứa một phần tử mà ở đó việc lựa chọn một số tiêu chí phải được thực hiện bởi tác giả PP/ ST.

Một ví dụ về một phần tử với lựa chọn là: FPT_TST.1.1 "The TSF phải thực hiện một bộ các kiểm thử [lựa chọn: trong suốt thời gian khởi tạo ban đầu, định kỳ trong quá trình hoạt động bình thường, theo

yêu cầu của người sử dụng được cấp quyền, tại các điều kiện [chỉ định : điều kiện theo đó tự kiểm thử nên xảy ra]] để diễn giải các hoạt động chính xác của ... "

C.2.4 Các hoạt động bổ sung chi tiết

Như mô tả trong 7.1.4, hoạt động bổ sung chi tiết có thể được thực hiện trên mọi yêu cầu. Tác giả PP / ST thực hiện một bổ sung chi tiết bằng cách thay đổi yêu cầu đó.

Một ví dụ về một bổ sung chi tiết hợp lệ là FIA_UAU.2.1 "The TSF cần yêu cầu mỗi người dùng phải xác thực thành công trước khi cho phép bất kỳ hành động trung gian TSF nào thay mặt cho người dùng đó." được bổ sung chi tiết để trở thành "TSF cần yêu cầu mỗi người sử dụng xác thực thành công **bằng tên người dùng / mật khẩu** trước khi cho phép bất kỳ hành động trung gian TSF nào thay mặt cho người dùng đó. "

Quy tắc đầu tiên để bổ sung chi tiết là một TOE đáp ứng yêu cầu đã tinh lọc cũng cần đáp ứng các yêu cầu chưa tinh lọc trong ngữ cảnh của PP/ST (tức là một yêu cầu đã tinh lọc phải "chặt chẽ" hơn so với yêu cầu ban đầu). Ngoại lệ duy nhất cho quy tắc này là một tác giả PP/ST được phép tinh lọc một SFR để áp dụng cho một số nhưng không phải tất cả các chủ thể, đối tượng, các hoạt động, các thuộc tính an toàn và / hoặc các thực thể bên ngoài.

Một ví dụ về một trường hợp ngoại lệ như vậy là FIA_UAU.2.1 "The TSF cần yêu cầu mỗi người dùng phải xác thực thành công trước khi cho phép bất kỳ hành động trung gian TSF nào thay mặt cho người dùng đó" được bổ sung chi tiết để trở thành "TSF cần yêu cầu mỗi người sử dụng **có nguồn gốc từ Internet** phải xác thực thành công trước khi cho phép bất kỳ hành động trung gian TSF nào thay mặt cho người dùng đó. "

Quy tắc thứ hai cho một bổ sung chi tiết được đưa ra là bổ sung chi tiết phải liên quan đến các thành phần gốc. Ví dụ, tinh lọc một thành phần kiểm toán với một phần tử bổ sung chống bức xạ điện từ là không được phép.

Một trường hợp đặc biệt của bổ sung chi tiết là một bổ sung chi tiết biên tập, ở đó, một sự thay đổi nhỏ sẽ được tạo ra trong một yêu cầu, nghĩa là diễn tả lại một câu để giữ đúng ngữ pháp tiếng Anh, hoặc để làm cho nó dễ hiểu hơn đối với người đọc. Sự thay đổi này không được phép sửa đổi ý nghĩa của yêu cầu. Ví dụ về bổ sung chi tiết biên tập bao gồm:

• SFR FPT_FLS.1 "TSF cần tiếp tục duy trì một trạng thái an toàn khi các lỗi sau đây xảy ra: **sự cố của một CPU**" có thể được bổ sung chi tiết thành FPT_FLS.1 "TSF cần tiếp tục duy trì một trạng thái an toàn khi xảy ra **lỗi** sau đây: **sự cố của một CPU**" hoặc thậm chí FPT_FLS.1 "TSF cần tiếp tục duy trì một trạng thái an toàn khi **một CPU bị hỏng**".

C.3 Tổ chức của các thành phần

TCVN 8709 tổ chức các thành phần trong TCVN 8709-2 và TCVN 8709-3 thành các cấu trúc có thứ bậc:

• Các lớp, bao gồm

• Các họ, bao gồm

• Các thành phần, bao gồm

• Các phần tử.

Tổ chức thành một hệ thống các lớp - họ - thành phần – phần tử được cung cấp để trợ giúp người tiêu dùng, nhà phát triển và đánh giá viên trong xác định các thành phần cụ thể.

TCVN 8709 trình bày các thành phần chức năng và đảm bảo theo cùng kiểu phân cấp, sử dụng mô hình tổ chức và các khái niệm như nhau.

C.3.1 Lớp

Ví dụ về một lớp là lớp FIA, lớp này tập trung vào việc định danh người dùng, xác thực người dùng và ràng buộc các người dùng với các chủ thể.

C.3.2 Họ

Ví dụ về một họ là họ Xác thực người dùng (FIA_UAU), họ này là một phần của lớp FIA. Họ này tập trung vào việc xác thực người sử dụng.

C.3.3 Thành phần

Một ví dụ về một thành phần là FIA_UAU.3 Xác thực chống giả mạo, thành phần này tập trung vào xác thực chống giả mạo.

C.3.4 Phần tử

Một ví dụ về một phần tử là FIA_UAU.3.2, phần tử này tập trung vào việc ngăn chặn việc sử dụng dữ liệu chứng thực đã sao chép.

C.4 Các thành phần mở rộng

C.4.1 Cách xác định thành phần mở rộng

Mỗi khi tác giả PP/ST định nghĩa một thành phần mở rộng, việc đó cần thực hiện theo phương thức tương tự như các thành phần đã có trong TCVN 8709: rõ ràng, không mơ hồ và có thể đánh giá được (có thể diễn giải một cách hệ thống về việc liệu một yêu cầu dựa trên thành phần đó có áp dụng được cho một TOE hay không). Các thành phần mở rộng phải sử dụng ghi nhãn, cách thức thể hiện, mức độ chi tiết tương tự như các thành phần đã có trong TCVN 8709.

Tác giả PP / ST cũng cần phải chắc chắn rằng mọi sự phụ thuộc áp dụng cho một thành phần mở rộng đã được đưa vào trong định nghĩa thành phần mở rộng đó. Ví dụ về sự phụ thuộc có thể là:

a) nếu một thành phần mở rộng tham chiếu đến kiểm toán, thì sự phụ thuộc đến các thành phần của lớp Fau có thể phải được đưa vào;

b) nếu một thành phần mở rộng sửa đổi hoặc truy xuất dữ liệu, sự phụ thuộc đến các thành phần của họ FDP_ACC có thể phải được đưa vào;

c) nếu một thành phần mở rộng sử dụng một mô tả thiết kế cụ thể, sự phụ thuộc vào họ ADV tương ứng (ví dụ Đặc tả chức năng) có thể phải được đưa vào.

Trong trường hợp một thành phần chức năng mở rộng, tác giả PP / ST cũng cần phải đưa vào mọi kiểm toán phù hợp và thông tin về các hoạt động liên quan trong định nghĩa của thành phần đó, tương tự như các thành phần sẵn có trong tiêu chuẩn TCVN 8709-2. Trong trường hợp một thành phần đảm bảo mở rộng, tác giả PP/ST cần phải cung cấp phương pháp luận đánh giá thích hợp cho thành phần, tương tự như phương pháp luận đã có trong ISO/IEC 18045.

Các thành phần mở rộng có thể được đặt trong các họ hiện có, trong đó người biên soạn PP/ST phải chỉ ra sự thay đổi các họ như thế nào. Nếu chúng không phù hợp với một họ hiện có, chúng sẽ được đặt trong một họ mới. Họ mới phải được định nghĩa tương tự theo TCVN 8709.

Các họ mới có thể được đặt trong các lớp hiện tại, trong đó người biên soạn PP / ST phải chỉ ra các lớp này thay đổi như thế nào. Nếu chúng không phù hợp với một lớp hiện có, chúng sẽ được đặt trong một lớp mới. Lớp mới này phải được định nghĩa tương tự theo TCVN 8709.

Phụ lục D

(Tham khảo)

Tuân thủ PP

D.1 Giới thiệu

Một PP được hướng đến sử dụng như là một "mẫu" cho một ST. Nghĩa là: PP mô tả một tập hợp các nhu cầu của người sử dụng, trong khi một ST tuân thủ với PP đó mô tả một TOE thỏa mãn những nhu cầu đó.

Lưu ý rằng cũng có thể một PP được sử dụng như một mẫu cho một PP khác. Đó là các PP có thể tuyên bố tuân thủ với các PP khác. Trường hợp này là hoàn toàn tương tự như của một ST so với một PP. Phụ lục này chỉ mô tả trường hợp ST/PP, còn nó được tổ chức như đối với trường hợp PP/ PP.

TCVN 8709 không cho phép bất kỳ hình thức tuân thủ từng phần nào, vì vậy nếu một PP được yêu cầu, các PP hoặc ST phải tuân thủ đầy đủ với PP hoặc các PP tham chiếu. Tuy nhiên, có hai kiểu tuân thủ ("hoàn toàn" và "có thể diễn giải") và kiểu tuân thủ cho phép được xác định bởi PP. Như vậy, PP tuyên bố (trong phát biểu tuân thủ PP, xem B.5) về những kiểu tuân thủ được phép cho ST. Sự phân biệt giữa tuân thủ chặt chẽ và tuân thủ có thể diễn giải có thể áp dụng cho mỗi PP mà một ST có thể yêu cầu tuân thủ theo cách riêng. Điều này có thể nghĩa là ST tuân thủ chặt chẽ với một số PP và tuân thủ có diễn giải với một số PP khác. Một ST chỉ được phép tuân thủ với một PP theo phương thức diễn giải, nếu PP cho phép một cách rõ ràng điều này, trong khi đó một ST luôn có thể tuân thủ chặt chẽ với mọi PP.

Phát biểu điều trên bằng một cách khác là, một ST chỉ được phép tuân thủ với một PP theo phương thức diễn giải, nếu PP cho phép một cách rõ ràng điều này.

Tuân thủ với một PP nghĩa là PP hoặc ST (và nếu một ST là một sản phẩm đã được đánh giá, cũng như một sản phẩm) đáp ứng mọi yêu cầu của PP này.

Các PP được công bố sẽ thường yêu cầu tuân thủ có thể diễn giải. Điều đó nghĩa là các ST đòi hỏi tuân thủ với PP sẽ phải đưa ra một giải pháp cho vấn đề an toàn chung đã nêu trong PP, song có thể thực hiện điều đó theo bất kỳ cách nào tương đương hoặc chặt chẽ hơn cách đã mô tả trong PP. "Tương đương song chặt chẽ hơn" được định nghĩa về độ dài trong TCVN 8709, song về nguyên tắc, điều đó nghĩa là PP và ST có thể chứa toàn bộ các phát biểu khác nhau về các thực thể khác nhau, sử dụng các khái niệm khác nhau.., với điều kiện tổng quát là ST thu được cùng hoặc nhiều hạn chế hơn về TOE, và cùng hoặc ít hạn chế hơn về môi trường hoạt động của TOE.

D.2 Tuân thủ chặt chẽ

Tuân thủ chặt chẽ hướng đến tác giả PP, người đòi hỏi bằng chứng về việc các yêu cầu trong PP được đáp ứng, về việc ST là một bản sao của PP, mặc dù ST có thể là rộng hơn so với PP. Về bản

chất, ST quy định TOE đạt ít nhất tương tự như trong PP, trong khi môi trường vận hành hầu như giống trong PP.

Một ví dụ điển hình của việc sử dụng tuân thủ chặt chẽ là việc lựa chọn dựa trên mua sắm, trong đó các yêu cầu an toàn của sản phẩm được kỳ vọng trùng hợp chính xác với những quy định trong PP.

Tuân thủ chặt chẽ với một PP cho một bản sao của một ST có thể vẫn có một số hạn chế bổ sung so với những gì đã có trong PP.

D.3 Tuân thủ có thể diễn giải

Tuân thủ có thể diễn giải hướng tới tác giả PP, người yêu cầu bằng chứng về việc ST là một giải pháp thích hợp cho vấn đề an toàn chung được mô tả trong PP.

Khi có một mối quan hệ kiểu tập con – tập lớn rõ rệt giữa PP và ST trong trường hợp tuân thủ chặt chẽ, mối quan hệ này sẽ bị giảm tính rõ ràng trong trường hợp tuân thủ có thể diễn giải. Các ST yêu cầu tuân thủ với PP phải đưa ra một giải pháp cho vấn đề an toàn chung được mô tả trong PP.

Tuy nhiên, việc đòi hỏi tuân thủ chỉ được phép trong trường hợp ST áp đặt tương tự hoặc nhiều hơn các hạn chế trên TOE, và tương tự hoặc ít hơn các hạn chế về môi trường vận hành của TOE.

Thư mục tài liệu tham khảo

Các tiêu chuẩn ISO/IEC và hướng dẫn

[1] ISO/IEC 15292, Information technology — Security techniques — Protection Profile registration procedures

[2] ISO/IEC 15443 (all parts), Information technology — Security techniques — A framework for IT security assurance

[3] ISO/IEC 15446, Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets

[4] ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules

[5] ISO/IEC 19791, Information technology — Security techniques — Security assessment of operational systems

[6] ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements

[7] ISO/IEC 27002:2005, Information technology — Security techniques — Code of practice for information security management

[8] ISO/IEC 15408 – 1 : 2005, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and general model.

[9] ISO/IEC 15408 – 2 : 2005, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 2: Security functional requirements.

[10] ISO/IEC 15408 – 3 : 2005, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 3: Security assurance requirements.

[11] ISO/IEC 15408 – 1 : 2009, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and general model.

[12] ISO/IEC 15408 – 2 : 2008, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 2: Security functional requirements.

[13] ISO/IEC 15408 – 3 : 2008, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 3: Security assurance requirements.

Các tiêu chuẩn và hướng dẫn khác

[14] IEEE Std 610.12-1990, Institute of Electrical and Electronics Engineers, Standard Glossary of Software Engineering Terminology

[15] Common Criteria portal, February 2009. CCRA, www.commoncriteriaportal.org.

[16] TCVN 27001: 2009, Công nghệ thông tin – Các kỹ thuật an toàn – Các hệ thống quản lý an toàn thông tin — Các yêu cầu

CÁC THUẬT NGỮ SỬ DỤNG TRONG TIÊU CHUẨN

CHÚ THÍCH: Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa trong bảng sau đây. Lưu ý là các thuật ngữ này được sử dụng riêng trong TCVN 8709 và ý nghĩa của chúng được hiểu trong ngữ cảnh của tiêu chuẩn TCVN 8709nơi chúng được sử dụng.

1	Acceptance criteria	Các tiêu chí chấp thuận
2	Acceptance procedures	Các thủ tục chấp thuận
3	Administrator	Người quản trị
4	adverse actions	Các hành động có hại
5	Assets	Tài sản
6	Assignment	Chỉ định
7	Assurance	Bảo đảm
8	Attack potential	Khả năng tấn công
9	Augmentation	Gia tăng
10	Authentication data	Dữ liệu xác thực
11	Authorized user	Người dùng có thẩm quyền
12	Base component	Thành phần cơ sở
13	Call coupling	Ghép nối truy xuất
14	Call tree	Cây truy xuất
15	Class	Lớp
16	CM documentation	Tài liệu CM
17	Coherent	Tính mạch lạc
18	Cohesion	Tính gắn kết
19	Coincidental cohesion	Gắn kết trùng hợp
20	Common coupling	Ghép nối chung
21	Communication cohesion	Gắn kết truyền thông
22	Compatible	Tương thích
23	Complete	Tính hoàn thiện
24	Complexity	Độ phức tạp
25	Component	Thành phần
26	Component TOE	TOE thành phần
27	Composed Assurance package	Gói đảm bảo tổng hợp
28	Composed TOE	TOE tổng hợp
29	Configuration management (CM)	Quản lý cấu hình (CM)
30	Configuration management evidence	Bằng chứng quản lý cấu hình
31	Configuration management plan	Kế hoạch quản lý cấu hình
32	Configuration management output	Đầu ra quản lý cấu hình
33	Configuration management system	Hệ thống quản lý cấu hình
34	Configuration management system records	Các bản ghi hệ thống quản lý cấu hình

35	Configuration management tools	Các công cụ quản lý cấu hình
36	Configuration management usage documentation	Tài liệu sử dụng quản lý cấu hình
37	Configuration item	Khoản mục cấu hình
38	Configuration list	Danh sách cấu hình
39	Confirm	Xác nhận
40	Connectivity	Tính kết nối
41	Consistent	Tính nhất quán
42	Content coupling	Ghép nối nội dung
43	Counter (verb)	Chống trả
44	Coupling	Ghép nối
45	Covert channel	Kênh bất hợp pháp
46	Delivery	Chuyển giao
47	Demonstable conformance	Tính tuân thủ diễn giải được
48	Demontrate	Diễn giải
49	Dependency	Tính phụ thuộc
50	Dependent component	Thành phần phụ thuộc
51	Describe	Mô tả
52	Determine	Xác định
53	Developer	Nhà phát triển
54	Development	Phát triển
55	Development environment	Môi trường phát triển
56	Development tools	Các công cụ phát triển
57	Domain separation	Phân cách miền
58	Element	Phần tử
59	Encountered potential vulnerabilities	Các điểm yếu tiềm ẩn phải đối mặt
60	Ensure	Bảo đảm
61	Evaluation	Đánh giá
62	Evaluation assurance level (EAL)	Mức bảo đảm đánh giá (EAL)
63	Evaluation authority	Cơ quan đánh giá
64	Evaluation scheme	Lược đồ đánh giá
65	Exhaustive	Thấu đáo
66	Explain	Giải thích
67	Exploitable vulnerability	Các điểm yếu có thể khai thác
68	Extension	Mở rộng
69	External entity	Thực thể bên ngoài
70	Family	Họ
71	Formal	Hình thức
72	Functional cohesion	Gắn kết chức năng

73	Functional interface	Giao diện chức năng
74	Guidance documentation	Tài liệu hướng dẫn
75	Identity	Định danh
76	Implementation representation	Mô tả triển khai
77	Informal	Không hình thức
78	Installation	Cài đặt
79	Inter TSF transfer	Vận chuyển giữa các TSF
80	Interaction	Tương tác
81	Interface	Giao diện
82	Internal communication channel	Kênh truyền thông nội bộ
83	Internal TOE transfer	Vận chuyển nội bộ TOE
84	Internally consistent	Tính nhất quán nội bộ
85	iteration	Phép lặp
86	Justification	Biện minh
87	Layering	Phân lớp
88	Life-cycle	Vòng đời
89	Life-cycle definition	Định nghĩa vòng đời
90	Life-cycle model	Mô hình vòng đời
91	Logical cohesion, procedural cohesion	Gắn kết logic, gắn kết thủ tục
92	Modular decomposition	Phân tách mô đun
93	Monitoring attacks	Các tấn công (kiểu) giám sát
94	Non-bypassability	Khả năng không đi vòng
95	Object	Đối tượng
96	Operation	Hoạt động
97	Operational environment	Môi trường vận hành
98	Organizational security policy	Chính sách an toàn của tổ chức
99	Package	Gói
100	Potential vulnerability	Các điểm yếu tiềm ẩn
101	Preparation	Chuẩn bị
102	Production	Sản xuất
103	Protection profile	Hồ sơ bảo vệ (PP)
104	Protection profile evaluation	Đánh giá Hồ sơ bảo vệ
105	Prove	Chứng minh
106	Refinement	Bổ sung chi tiết
107	Residual vulnerability	Các điểm yếu còn tồn tại
108	Role	Tập phân vai
109	Secret	Bí mật
110	Secure state	Trạng thái an toàn
111	Security attribute	Thuộc tính an toàn

112	Security domain	Miền an toàn
113	Security function policy	Chính sách chức năng an toàn
114	Security objective	Mục tiêu an toàn
115	Security problem	Vấn đề an toàn
116	Security requirement	Yêu cầu an toàn
117	Security Target	Đích an toàn (ST)
118	Selection	Lựa chọn
119	Semiformal	Bán hình thức
120	Sequential cohesion	Gắn kết tuần tự
121	Software engineering	Công nghệ phần mềm
122	Specify	Đặc tả
123	Strict conformance	Tuân thủ chặt chẽ
124	ST evaluation	Đánh giá ST
125	Subject	Chủ thể
126	Target of Evaluation (TOE)	Đích đánh giá (TOE)
127	Temporal cohesion	Gắn kết tạm thời
128	Threat agent	Tác nhân đe dọa
129	TOE Evaluation	Đánh giá TOE
130	TOE resource	Tài nguyên TOE
131	TOE security functionality	Chức năng an toàn của TOE (TSF)
132	Trace (verb)	Theo dấu
133	Transfers outside of the TOE	Vận chuyển bên ngoài TOE
134	Translation	Chuyển đổi
135	Trusted channel	Kênh tin cậy
136	Trusted IT product	Sản phẩm CNTT tin cậy
137	Trusted path	Đường dẫn tin cậy
138	TSF self-protection	Tự bảo vệ TSF
139	TSF data	Dữ liệu TSF
140	TSF interface	Giao diện TSF
141	User data	Dữ liệu người dùng
142	Verify	Thẩm tra
143	Vulnerability	Điểm yếu

CÁC KÝ HIỆU VÀ TỪ VIẾT TẮT TRONG TIÊU CHUẨN

Viết tắt	Tiếng Anh tương đương	Tiếng Việt
ADV	**ADV:Development**	**Lớp ADV: Phát triển**
ADV_ARC	ADV_ARC:Security architecture Description	ADV_FSP: Đặc tả kiến trúc an toàn
ADV_FSP	ADV_FSP:Basic functional specification	ADV_FSP: Đặc tả chức năng cơ bản
ADV_TDS	ADV_TDS: Basic design	ADV_TDS: Thiết kế cơ bản
AGD	**AGD:Guidance documents**	**Lớp AGD: Tài liệu hướng** dẫn
AGD_OPE	AGD_OPE:Operational user guidance	AGD_OPE: Hướng dẫn người dùng vận hành
AGD_PRE	AGD_PRE:Preparative procedures	AGD_PRE: Các thủ tục chuẩn bị
ALC	**ALC:Life-cycle support**	**Lớp ALC: Hỗ trợ vòng đời**
ALC_CMC	ALC_CMC: Labelling of the TOE	ALC_CMC: Dán nhãn TOE
ALC_CMC	ALC_CMS: TOE CM Coverage	ALC_CMS: Tổng quát TOE CM
ALC_DEL	ALC_DEL: Delivery procedures	ALC_DEL: Các thủ tục chuyển giao
ALC_DVS	ALC_DVS: Identification of security measures	ALC_DVS: Định danh các biện pháp an toàn
ASE	**ASE:Security Target evaluation**	**Lớp ASE: Đánh giá đích an toàn**
ASE_CCL	ASE_CCL: Conformance claims	ASE_CCL: Các yêu cầu tuân thủ
ASE_ECD	ASE_ECD: extended components definition	ASE_ECD: Định nghĩa các thành phần mở rộng
ASE_INT	ASE_INT: ST introduction	ASE_INT: Giới thiệu ST
ASE_OBJ	ASE_OBJ: Security objectives for the operational environment	ASE_OBJ: Các mục tiêu an toàn cho môi trường vận hành
ASE_REQ	ASE_REQ: Stated security requirements	ASE_REQ: Các yêu cầu an toàn đã công bố
ASE_SPD	ASE_SPD: Security problem definition	ASE_SPD: Định nghĩa vấn đề an toàn
ASE_TSS	ASE_TSS: TOE summary specification	ASE_TSS: Đặc tả tóm tắt TOE
ATE	**ATE:Tests**	**Lớp ATE: Kiểm thử**
ATE_COV	ATE_COV:Evidence of coverage	ATE_COV: Chứng cứ về tính tổng quát
ATE_DPT	ATE_DPT: Testing: basic design	ATE_DPT: Kiểm thử: thiết kế cơ bản
ATE_FUN	ATE_FUN:Functional Testing	ATE_FUN: Kiểm thử chức năng
ATE_IND	ATE_IND:Independent testing - conformance	ATE_IND: Kiểm thử độc lập – Tuân thủ
AVA	**AVA:Vulnerability assessment**	**Lớp AVA:.Đánh giá điểm yếu**
AVA_VAN	AVA_VAN:Vulnerability survey	AVA_VAN: Khảo sát điểm yếu
API	Application Programming Interface	Giao diện lập trình ứng dụng
CAP	Composed Assurance Package	Gói đảm bảo tổng hợp
CM	Configuration Management	Quản lý cấu hình

CNTT	Information Technology (IT)	Công nghệ thông tin (CNTT)
DAC	Discretionary Access Control	Kiểm soát truy nhập tùy ý
EAL	Evaluation Assurance Level	Mức bảo đảm đánh giá
FAU	Function Security Audit Class	Lớp kiểm toán an toàn (FAU)
FAU_ARP	FAU: Security audit automatic response	FAU: Phản hồi tự động kiểm toán an toàn
FAU_GEN	FAU: Security audit data generation	FAU: Tạo dữ liệu kiểm toán an toàn
FAU_SAA	FAU: Security audit analysis	FAU: Phân tích kiểm toán an toàn
FAU_SAR	FAU: Security audit review	FAU: Soát xét kiểm toán an toàn
FAU_SEL	FAU: Security audit event selection	FAU: Lựa chọn sự kiện kiểm toán an toàn
FAU_STG	FAU: Security audit event storage	FAU: Lưu trữ sự kiện kiểm toán an toàn
FCO	Function Communication	Lớp FCO:truyền thông
FCO_NRO	FCO_NRO: Non-repudiation of origin	FCO_NRO: Không từ chối nguồn gốc
FCO_NRR	FCO_NRR: Non-repudiation of receipt	FCO_NRR: Không từ chối khi nhận
FCS	Function Cryptographic support	Lớp FCS: Hỗ trợ mật mã
FCS_CKM	FCS_CKM: Cryptographic key management	FCS_CKM: Quản lý khóa mật mã
FCS_COP	FCS_COP: Cryptographic operation	FCS_COP: Hoạt động mật mã
FDP	Function User Data Protection	Lớp FDP: Bảo vệ dữ liệu người dùng
FDP_ACC	FDP:Access control policy	FDP: Chính sách kiểm soát truy nhập
FDP_ACF	FDP:Access control functions	FDP: Các chức năng kiểm soát truy nhập
FDP_DAU	FDP:Data authentication	FDP_DAU: Xác thực dữ liệu
FDP_ETC	FDP:Export from TOE	FDP_ETC: Xuất dữ liệu ra khỏi TOE
FDP_IFC	FDP:Information flow control policy	FDP_IFC: Chính sách kiểm soát luồng tin
FDP_IFF	FDP:Information flow control functions	FDP_IFF: Các chức năng kiểm soát luồng tin
FDP_ITC	FDP:Import from outside of the TOE	FDP_ITC: Nhập dữ liệu từ bên ngoài TOE
FDP_ITT	FDP:Internal TOE transfer	FDP_ITT: Vận chuyển nội bộ TOE
FDP_RIP	FDP:Residual information protection	FDP_RIP: Bảo vệ thông tin còn sót lại
FDP_ROL	FDP:Rollback	FDP_ROL: Khôi phục lại
FDP_SDI	FDP:Stored data integrity	FDP_SDI: Toàn vẹn dữ liệu đã lưu trữ
FDP_UCT	FDP:Inter-TSF user data confidentiality	FDP_UCT: Bảo vệ truyền bí mật dữ

	transfer protection	liệu người dùng liên – TSF'
FDP_UIT	FDP:Inter-TSF user data integrity transfer protection	FDP_UIT: Bảo vệ truyền vẹn toàn dữ liệu người dùng liên -TSF
FIA	Function Identification and Authentication	Lớp FIA: Định danh và xác thực
FIA_AFL	FIA_AFL: Authentication failures	FIA_AFL: Các lỗi xác thực
FIA_ATD	FIA_ATD: User attribute definition	FIA_ATD: Định nghĩa thuộc tính người dùng
FIA_SOS	FIA_SOS: Specification of secrets	FIA_SOS: Đặc tả các bí mật
FIA_UAU	FIA_UAU: User Authentication	FIA_UAU: Xác thực người dùng
FIA_UID	FIA_UID: User identification	FIA_UID: Định danh người dùng
FIA_USB	FIA_USB: User-subject binding	FIA_USB: Liên kết người dùng-chủ thể
FMT	Function Security Management	Lớp FMT: Quản lý an toàn
FMT_MOF	FMT_MOF: Management of functions in TSF	FMT_MOF: Quản lý các chức năng trong TSF
FMT_MSA	FMT_MSA: Management of Security attributes	FMT_MSA: Quản lý các thuộc tính an toàn
FMT_MTD	FMT_MTD: Management of TSF data	FMT_MTD: Quản lý dữ liệu TSF
FMT_REV	FMT_REV: Revocation	FMT_REV: Hủy bỏ
FMT_SAE	FMT_SAE: Security attribute expiration	FMT_SAE: Các thuộc tính an toàn quá hạn
FMT_SMF	FMT_SMF: Specification of Management functions	FMT_SMF: Đặc tả các chức năng quản lý
FMT_SMR	FMT_SMR: Security Management roles	FMT_SMR: Các vai trò quản lý an toàn
FPR	Function Privacy	Lớp FPR: Riêng tư
FPR_ANO	FPR_ANO: Anonymity	FPR_ANO: Nặc danh
FPR_PSE	FPR_PSE: Pseudonymity	FPR_PSE: Biệt danh
FPR_UNL	FPR_UNL: Unlinkability	FPR_UNL: Không thể liên kết
FPR_UNO	FPR_UNO: Unobservability	FPR_UNO: Không thể quan sát
FPT	Function Protection of the TSF	Lớp FPT: Bảo vệ TSF
FPT_FLS	FPT_FLS:Fail secure	FPT_FLS: An toàn khi có lỗi
FPT_ITA	FPT_ITA:Availability of exported TSF data	FPT_ITA:Tính sẵn sàng của dữ liệu TSF xuất ra
FPT_ITC	FPT_ITC:Confidentiality of exported TSF data	FPT_ITC: Tính bí mật của dữ liệu TSF xuất ra
FPT_ITL	FPT_ITL:Integrity of exported TSF data	FPT_ITL: Tính toàn vẹn của dữ liệu TSF xuất ra
FPT_ITT	FPT_ITT: Internal TOE TSF data transfer	FPT_ITT: Vận chuyển dữ liệu nội bộ TOE TSF
FPT_PHP	FPT_PHP: TSF physical protection	FPT_PHP: Bảo vệ vật lý cho TSF
FPT_RCV	FPT_RCV:Trusted recovery	FPT_RCV: Khôi phục tin cậy
FPT_RPL	FPT_RPL: Replay detection	FPT_RPL: Phát hiện chạy lại

FPT_SSP	FPT_SSP:State synchrony protocol	FPT_SSP: Giao thức đồng bộ trạng thái
FPT_STM	FPT_STM: Time stamps	FPT_STM: Các nhãn thời gian
FPT_TDC	FPT_TDC: Inter-TSF TSF data consistency	FPT_TDC: Sự nhất quán dữ liệu TSF liên TSF
FPT_TEE	FPT_TEE: Testing of external entitites	FPT_TEE: Kiểm thử các thực thể bên ngoài
FPT_TRC	FPT_TRC: Internal TOE TSF data replication consistency	FPT_TRC:Tính nhất quán của bản sao dữ liệu nội bộ của TOE TSF
FPT_TST	FPT_TST: TSF selftest	FPT_TST: Tự kiểm tra TSF
FRU	Function Resource Utilisation	Lớp FRU: Sử dụng tài nguyên
FRU_FLT	FRU_FLT: Fault tolerance	FRU_FLT: Khả năng chịu lỗi
FRU_PRS	FRU_PRS: Priority of service	FRU_PRS: Ưu tiên dịch vụ
FRU_RSA	FRU_RSA: Resource allocation	FRU_RSA: Cấp phát tài nguyên
FTA	Function TOE Access	Lớp FTA: Truy nhập TOE
FTA_LSA	FTA_LSA:Limitation on scope of selectable attributes	FTA_LSA:Giới hạn phạm vi các thuộc tính có thể chọn lựa
FTA_MCS	FTA_MCS: Limitation on multiple concurrent sessions	FTA_MCS: Giới hạn số lượng phiên đồng thời
FTA_SSL	FTA_SSL: Session locking and termination	FTA_SSL: Khoa phiên và kết thúc
FTA_TAB	FTA_TAB: TOE access banners	FTA_TAB: Các tiêu đề truy nhập TOE
FTA_TAH	FTA_TAH: TOE access history	FTA_TAH: Lịch sử truy cập TOE
FTA_TSE	FTA_TSE: TOE session establishment	FTA_TSE: Thiết lập phiên TOE
FTP	Function Trusted Path/Channel	Lớp FTP: Tuyến/Kênh tin cậy
FTP_ITC	FTP_ITC: Inter-TSF trusted channel	FTP_ITC: Kênh tin cậy liên TSF
FTP_TRP	FTP_TRP: Trusted path	FTP_TRP: Đường dẫn tin cậy
GHz	Gigahertz	Số đo tần số Gigahertz
GUI	Graphical User Interface	Giao diện người dùng dạng đồ họa
IC	Integrated Circuit	Mạch tổ hợp
IOCTL	Input Output Control	Kiểm soát vào ra
IP	Internet Protocol	Giao thức Internet
IT	Information Technology	Công nghệ thông tin (CNTT)
MB	Mega Byte	Đơn vị thông tin Mega Byte (MB)
OS	Operating System	Hệ điều hành
OSP	Organizational Security Policy	Chính sách an toàn của tổ chức
PC	Personal Computer	Máy tính cá nhân
PCI	Peripheral Component Interconnect	Liên kết nối các thành phần ngoại vi

PKI	Public Key Infrastructure	Hạ tầng cơ sở khóa công khai
PP	Protection Profile	Hồ sơ bảo vệ
RAM	Random Access Memory	Bộ nhớ truy nhập ngẫu nhiên
RPC	Remote Procedure Call	Lời gọi thủ tục từ xa
SAR	Security Assurance Requirement	Yêu cầu đảm bảo an toàn
SF	Security Function	Chức năng an toàn
SFR	Security Functional Requirement	Yêu cầu chức năng an toàn
SFP	Security Function Policy	Chính sách chức năng an toàn
SPD	Security Problem Definition	Định nghĩa vấn đề an toàn
SOF	Strength of Function	Độ mạnh của chức năng
ST	Security Target	Đích an toàn
TCP	Transmission Control Protocol	Giao thức điều khiển truyền tải
TOE	Target of Evaluation	Đích đánh giá
TSC	TSF Scope of Control	Phạm vi giám sát TSF
TSF	TOE Security Functions	Các chức năng an toàn của TOE
TSFI	TSF Interface	Giao diện TSF
TSP	TOE Security Policy	Chính sách an toàn TOE
VPN	Virtual Private Network	Mạng riêng ảo