TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 14190-1:2024

ISO/IEC 19989-1:2020

Xuất bản lần 1

AN TOÀN THÔNG TIN - TIÊU CHÍ VÀ PHƯƠNG PHÁP LUẬN ĐÁNH GIÁ AN TOÀN HỆ THỐNG SINH TRẮC HỌC - PHẦN 1: KHUNG

Information security - Criteria and methodology for security evaluation of biometric systems - Part 1: Framework

HÀ NỘI – 2024

Mục lục

Lời nói đầu

TCVN 14190-1:2024 hoàn toàn tương đương với ISO/IEC 19989-1:2020.

TCVN 14190-1:2024 do Ban Cơ yếu Chính phủ biên soạn, Bộ Quốc phòng đề nghị, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Bộ tiêu chuẩn TCVN 14190 (ISO/IEC 19989) An toàn thông tin - Tiêu chí và phương pháp luận đánh giá an toàn hệ thống sinh trắc học bao gồm 3 phần:

- TCVN 14190-1 (ISO/IEC 19989-1) An toàn thông tin - Tiêu chí và phương pháp luận đánh giá an toàn hệ thống sinh trắc học - Phần 1: Khung.

- TCVN 14190-2 (ISO/IEC 19989-2) An toàn thông tin - Tiêu chí và phương pháp luận đánh giá an toàn hệ thống sinh trắc học - Phần 2: Hiệu suất nhận dạng sinh trắc học.

- TCVN 14190-3 (ISO/IEC 19989-3) An toàn thông tin - Tiêu chí và phương pháp luận đánh giá an toàn hệ thống sinh trắc học - Phần 3: Phát hiện tấn công trình diện.

Giới thiệu

Các hệ thống sinh trắc học có thể bị tấn công bởi các cuộc tấn công trình diện trong đó những kẻ tấn công cố gắng phá hoại chính sách an toàn hệ thống bằng cách trình diện các đặc trưng sinh trắc học tự nhiên của chúng hoặc các tạo tác sở hữu các đặc điểm đã được sao chép hoặc giả mạo. Các cuộc tấn công trình diện có thể xảy ra trong quá trình đăng ký hoặc các thủ tục định danh/xác minh. Các kỹ thuật được thiết kế để phát hiện những bản trình diện các tạo tác thường khác với các kỹ thuật để chống lại các cuộc tấn công khi sử dụng các đặc điểm tự nhiên. Phòng thủ chống lại các cuộc tấn công trình diện với các đặc điểm tự nhiên thường dựa vào khả năng của hệ thống sinh trắc học để phân biệt giữa những người đăng ký thực và những kẻ tấn công, dựa trên sự khác biệt giữa các đặc trưng sinh trắc học tự nhiên giữa hai thực thể. Khả năng này được thể hiện bởi hiệu suất nhận dạng sinh trắc học của hệ thống. Hiệu suất nhận dạng sinh trắc học và phát hiện tấn công trình diện có ảnh hưởng đến tính an toàn của hệ thống sinh trắc học. Do đó, việc đánh giá các khía cạnh này của hiệu suất từ quan điểm về an toàn sẽ là những cân nhắc quan trọng đối với việc mua sắm các sản phẩm và hệ thống sinh trắc học.

Các sản phẩm và hệ thống sinh trắc học chia sẻ nhiều đặc tính của các sản phẩm và hệ thống CNTT khác có thể đáp ứng được việc đánh giá an toàn bằng cách sử dụng loạt tiêu chuẩn TCVN 8709 và TCVN 11386 theo phương thức tiêu chuẩn. Tuy nhiên, các hệ thống sinh trắc học bao gồm một số chức năng cần các tiêu chí và phương pháp luận đánh giá chuyên biệt mà bộ tiêu chuẩn TCVN 8709 và TCVN 11386 không đề cập đến. Những điều này chủ yếu liên quan đến việc đánh giá nhận dạng sinh trắc học và phát hiện tấn công trình diện. Đây là những chức năng được đề cập trong bộ tiêu chuẩn TCVN 14190.

TCVN 11385 mô tả các khía cạnh cụ thể về sinh trắc học và chỉ rõ các nguyên tắc cần được xem xét trong quá trình đánh giá an toàn của hệ thống sinh trắc học. Tuy nhiên, TCVN 11385 không chỉ rõ các tiêu chí và phương pháp luận cụ thể cần thiết để đánh giá an toàn dựa trên bộ tiêu chuẩn TCVN 8709.

Bộ tiêu chuẩn TCVN 14190 cung cấp cầu nối giữa các nguyên tắc đánh giá cho các sản phẩm và hệ thống sinh trắc học được xác định trong TCVN 11385 và các yêu cầu về tiêu chí và phương pháp luận để đánh giá an toàn dựa trên bộ tiêu chuẩn TCVN 8709. Bộ tiêu chuẩn TCVN 14190 bổ sung cho bộ tiêu chuẩn TCVN 8709 và TCVN 11386 bằng cách cung cấp các thành phần chức năng an toàn mở rộng cùng với các hoạt động bổ sung liên quan đến các yêu cầu này. Các phần mở rộng đối với các yêu cầu và hoạt động bổ sung được tìm thấy trong bộ tiêu chuẩn TCVN 8709 và TCVN 11386 liên quan đến việc đánh giá nhận dạng sinh trắc học và phát hiện tấn công trình diện cụ thể đối với các hệ thống sinh trắc học.

Tiêu chuẩn này bao gồm việc giới thiệu khung để đánh giá an toàn của hệ thống sinh trắc học, bao gồm các thành phần chức năng an toàn mở rộng, các hoạt động đánh giá và phương pháp bổ sung cho kiểm thử viên. Các khuyến nghị chi tiết được phát triển cho các khía cạnh nhận dạng sinh trắc học trong TCVN 14190-2 và cho các khía cạnh phát hiện tấn công trình diện trong TCVN 14190-3.

Trong tiêu chuẩn này, thuật ngữ "người dùng" có nghĩa là thuật ngữ "đối tượng thu thập" được sử dụng trong sinh trắc học.

An toàn thông tin - Tiêu chí và phương pháp luận đánh giá an toàn hệ thống sinh trắc học – Phần 1: Khung.

Information security — Criteria and methodology for security evaluation of biometric systems — Part 1: Framework

1 Phạm vi áp dụng

Để đánh giá an toàn hiệu suất nhận dạng sinh trắc học và phát hiện tấn công trình diện đối với hệ thống xác minh sinh trắc học và hệ thống định danh sinh trắc học, tiêu chuẩn này chỉ rõ:

- Mở rộng các thành phần chức năng an toàn cho các lớp SFR trong TCVN 8709-2 (ISO/IEC 15408-2);

- Các hoạt động bổ sung cho phương pháp luận được quy định trong TCVN 11386 (ISO/IEC 18045) cho các lớp SAR của TCVN 8709-3 (ISO/IEC 15408-3).

Tiêu chuẩn này giới thiệu khung đối với đánh giá an toàn của hệ thống sinh trắc học, bao gồm các thành phần chức năng an toàn mở rộng và các hoạt động bổ sung với phương pháp luận, là các hoạt động đánh giá bổ sung và hướng dẫn/khuyến nghị cho Kiểm thử viên để xử lý các hoạt động đó. Các hoạt động đánh giá bổ sung được phát triển trong tiêu chuẩn này trong khi các khuyến nghị chi tiết được phát triển trong TCVN 14190-2 (ISO/IEC 19989-2) (đối với các khía cạnh nhận dạng sinh trắc học) và trong TCVN 14190-3 (ISO/IEC 19989-3) (đối với các khía cạnh phát hiện tấn công trình diện). Tiêu chuẩn này chỉ có thể áp dụng cho các TOE chứa loại đặc trưng sinh trắc học duy nhất. Tuy nhiên, việc lựa chọn một đặc tính từ nhiều đặc tính trong SFR vẫn được cho phép.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

TCVN 8709-1:2011 (ISO/IEC 15408-1:2009), 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.

TCVN 8709-2:2011 (ISO/IEC 15408-2:2008), 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 8709-3:2011 (ISO/IEC 15408-3:2008) về 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.

TCVN 11386:2016 (ISO/IEC 18045:2008), Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp đánh giá an toàn công nghệ thông tin.

ISO/IEC 2382:2008, Information technology - Vocabulary.

ISO/IEC 2382-37:2017, Information technology - Vocabulary - Part 37: Biometrics.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa nêu trong ISO/IEC 2382:2008, ISO/IEC 2382-37:2017, TCVN 8709-1:2011, TCVN 11386:2016 và tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa sau:

3.1

Tỷ lệ lỗi phân loại tấn công trình diện (attack presentation classification error rate)

APCER

Tỷ lệ các tấn công trình diện sử dụng cùng một loại PAI (3.15) được phân loại không chính xác thành các trình diện trung thực (3.5) trong một tình huống cụ thể

[NGUỒN: ISO/IEC 30107-3: 2017, 3.2.1]

3.2

Kiểu tấn công (attack type)

Yếu tố và đặc điểm của một cuộc tấn công trình diện, bao gồm các loại PAI (3.15), cuộc tấn công che giấu hoặc mạo danh, mức độ giám sát và phương pháp tương tác với thiết bị thu thập.

[NGUỒN: ISO/IEC 30107-3: 2017, 3.1.3]

3.3

Trình diện trung thực (bona fide presentation)

Sự tương tác của chủ thể thu thập sinh trắc học và hệ thống con thu thập dữ liệu sinh trắc học theo cách được dự kiến bởi chính sách của hệ thống sinh trắc học.

CHÚ THÍCH 1: Trung thực tương tự như bình thường hoặc thông thường, khi đề cập đến một trình diện trung thực.

CHÚ THÍCH 2: Các trình diện trung thực có thể bao gồm những trình diện mà người dùng có trình độ đào tạo hoặc kỹ năng thấp. Các trình diện của trung thực bao gồm toàn bộ các trình diện có thiện chí vào một hệ thống con thu thập dữ liệu sinh trắc học.

[NGUỒN: ISO/IEC 30107-3: 2017, 3.1.2]

3.4

Tỷ lệ lỗi phân loại trình diện trung thực (bona fide presentation classification error rate)

BPCER

Tỷ lệ các trình diện trung thực (3.5) được phân loại không chính xác thành các cuộc tấn công trình diện trong một tình huống cụ thể

[NGUỒN: ISO/IEC 30107-3: 2017, 3.2.2]

3.5

Loại PAI (PAI species)

Tập hợp của công cụ công tấn công trình diện được tạo bởi cùng một công thức sản xuất dựa trên các đặc trưng sinh trắc học khác nhau.

VÍ DỤ 1: Một bộ dấu vân tay giả được làm theo cách giống nhau với cùng vật liệu nhưng khác các mô hình vân tay sẽ tạo thành một loại PAI.

VÍ DỤ 2: Một loại thay đổi cụ thể được thực hiện đối với dấu vân tay của một số đối tượng thu thập dữ liệu sẽ tạo thành một loại PAI.

CHÚ THÍCH 1: Thuật ngữ "công thức" thường được sử dụng để chỉ cách tạo ra loại PAI.

CHÚ THÍCH 2: Các công cụ tấn công trình diện của cùng một loại có thể có tỷ lệ thành công khác nhau do sự khác nhau trong quá trình sản xuất.

3.6

Thử nghiệm xâm nhập (penetration testing)

Thử nghiệm được sử dụng trong phân tích lỗ hổng để đánh giá tính dễ bị tổn thương và cố gắng tấn công các lỗ hổng của TOE dựa trên thông tin về TOE được thu thập trong các hoạt động đánh giá liên quan.

CHÚ THÍCH 1: Trong bộ tiêu chuẩn TCVN 8709, thuật ngữ này được sử dụng mà không được định nghĩa.

3.7

Tấn công trình diện (presentation attack)

Trình diện với hệ thống con thu thập dữ liệu sinh trắc học với mục tiêu can thiệp vào hoạt động của hệ thống sinh trắc học.

CHÚ THÍCH 1: Tấn công trình diện có thể được thực hiện thông qua một số phương pháp, ví dụ: tạo tác, cắt xén, phát lại, v.v.

CHÚ THÍCH 2: Các cuộc tấn công trình diện có thể có một số mục tiêu, ví dụ: mạo danh hoặc không được công nhận.

CHÚ THÍCH 3: Hệ thống sinh trắc học có thể không phân biệt được giữa các cuộc tấn công trình diện sinh trắc học với mục tiêu can thiệp vào hoạt động của hệ thống và các trình diện không tuân theo quy định.

[NGUỒN: ISO/IEC 30107-1:2016, 3.5].

3.8

Phát hiện tấn công trình diện (presentation attack detection)

PAD

Tự động xác định một cuộc tấn công trình diện.

CHÚ THÍCH 1: PAD không thể suy ra ý định của đối tượng. Trên thực tế, có thể không thể thu được sự khác biệt đó từ quá trình thu thập dữ liệu hoặc mẫu thu được.

[NGUỒN: ISO/IEC 30107-1:2016, 3.6].

3.9

Công cụ tấn công trình diện (presentation attack instrument)

PAI

Đặc tính hoặc đối tượng sinh trắc học được sử dụng trong cuộc tân công trình diện.

CHÚ THÍCH 1: Bộ PAI bao gồm các tạo tác nhưng cũng sẽ bao gồm các đặc trưng sinh trắc học không có sự sống (tức là từ xác chết) hoặc các đặc trưng sinh trắc học bị thay đổi (ví dụ: dấu vân tay bị thay đổi) được sử dụng trong một cuộc tấn công.

CHÚ THÍCH 2: Ví dụ về các đặc trưng sinh trắc học bị thay đổi là cắt xén, phẫu thuật chuyển dấu vân tay giữa bàn tay và (hoặc) ngón chân (Xem bảng 1 mục 5.2 của ISO/IEC 30107-1: 2016).

[NGUỒN: ISO/IEC 30107-1:2016, 3.7]

4 Ký hiệu và thuật ngữ viết tắt

APCER	attack presentation classification error rate	tỷ lệ lỗi tấn công trình diện được phân loại
BPCER	bona fide presentation classification error rate	tỷ lệ lỗi trình diện trung thực được phân loại
IT	information technology	công nghệ thông tin
FAR	false acceptance rate	tỷ lệ chấp nhận lỗi
FAU	SFR class of audit	Lớp SFR của đánh giá CHÚ THÍCH: Tên lớp được định nghĩa trong TCVN 8709-2. Ở đây, F của FAU là viết tắt của chức năng yêu cầu (functional requirement), AU cho đánh giá (audit). Tên lớp được định nghĩa theo cách này trong loạt tiêu chuẩn TCVN 8709. Để biết chi tiết, xem Phụ lục A.
FMR	false match rate	tỷ lệ trùng khớp lỗi
FNIR	false-negative identification-error rate	tỷ lệ lỗi định danh phủ định sai
FNMR	false non-match rate	tỷ lệ không trùng khớp lỗi
FPIR	false-positive identification-error rate	tỷ lệ lỗi định danh khẳng định sai
FPT	SFR class of protection of the TSF	lớp SFR của bảo vệ bởi TSF Chú ý : xem chú ý tại mục FAU
FRR	false rejection rate	tỷ lệ từ chối lỗi
FTAR	failure-to-acquire rate	tỷ lệ thu thập thất bại
FTER	failure-to-enrol rate	tỷ lệ đăng ký thất bại
PAD	presentation attack detection	phát hiện tấn công trình diện
PAI	presentation attack instrument	công cụ tấn công trình diện
PP	protection profile	hồ sơ bảo vệ
SAR	security assurance requirement	yêu cầu đảm bảo an toàn

SFR	security functional requirement	yêu cầu chức năng an toàn
ST	security target	đích an toàn
TOE	target of evaluation	đích đánh giá
TSF	TOE security functionality	Chức năng an toàn của TOE
TSFI	TSF interface	Giao diện của TSF

5 Nhận xét chung

Ngoài các yêu cầu và khuyến nghị được cung cấp trong mục 7 và mục 8, các yêu cầu và khuyến nghị trong TCVN 8709-2:2011 phải được áp dụng.

Ngoài các yêu cầu và khuyến nghị được cung cấp trong mục 9 đến mục 15, các yêu cầu và khuyến nghị trong TCVN 8709-3:2011 và TCVN 11386:2016 phải được áp dụng.

Phụ lục D cung cấp thông tin cơ bản về các hoạt động bổ sung để đánh giá PAD. Định nghĩa về xác thực có thể xem trong ISO/IEC 2382.

Các định nghĩa của sinh trắc học (tính từ), thu thập sinh trắc học, đảm bảo, thiết bị thu thập sinh trắc học, đặc trưng sinh trắc học, che giấu sinh trắc học, đăng ký sinh trắc học, thực hiện đăng ký sinh trắc học, cơ sở dữ liệu thực hiện đăng ký sinh trắc học, tính năng sinh trắc học, định danh sinh trắc học, giả mạo sinh trắc học, trình diện sinh trắc học, nhân dạng sinh trắc học, sinh trắc học, tham chiếu sinh trắc học, mẫu sinh trắc học, hệ thống sinh trắc học, xác minh sinh trắc học, so sánh, đăng ký, tỷ lệ thu thập thất bại, tỷ lệ đăng ký thất bại, tỷ lệ không trùng khớp lỗi, tỷ lệ lỗi định danh phủ định sai, tỷ lệ không trùng khớp lỗi, tỷ lệ lỗi định danh khẳng định sai, xác định, khớp (danh từ) và ngưỡng (danh từ) có thể được xem trong ISO/IEC 2382-37.

CHÚ THÍCH 1: Trong tiêu chuẩn này, cụm từ "thiết bị thu thập" đôi khi được sử dụng thay cho "thiết bị thu thập sinh trắc học".

CHÚ THÍCH 2: Trong tiêu chuẩn này, cụm từ "che giấu" đôi khi được sử dụng thay cho "che giấu sinh trắc học".

CHÚ THÍCH 3: Trong tiêu chuẩn này, cụm từ "kẻ mạo danh" đôi khi được sử dụng thay cho "kẻ mạo danh sinh trắc học".

Các định nghĩa về quản trị viên, chỉ định, bảo đảm, tiềm năng tấn công, lớp, thành phần, xác nhận, chuyển giao, mô tả, xác định, nhà phát triển, phát triển, phần tử, bảo đảm, đánh giá, mở rộng, họ, tài liệu hướng dẫn, định danh, tương tác, giao diện, vòng đời, đối tượng, hoạt động (trên một thành phần của TCVN 8709), hoạt động, môi trường vận hành, các điểm yếu tiềm ẩn, hồ sơ bảo vệ, đánh giá hồ sơ bảo vệ, yêu cầu an toàn, đích an toàn, Đánh giá ST, chủ thể, đích đánh giá, chức năng an toàn của TOE, dữ liệu TSF, giao diện TSF, tự bảo vệ TSF, thẩm tra và điểm yếu có thể được tìm thấy trong TCVN 8709-1.

CHÚ THÍCH 4: Định nghĩa của "Hoạt động" thứ hai tại mục bên trên liên quan đến lớp AGD.

Các định nghĩa về hành động, hoạt động, thẩm tra, phương pháp luận, báo cáo, lược đồ, hoạt động con và đơn vị công việc có thể được tìm thấy trong TCVN 11386.

6 Các điểm yếu trong hệ thống sinh trắc học và đánh giá an toàn

6.1 Phân loại các điểm yếu phổ biến của hệ thống sinh trắc học

Trong TCVN 11385:2016, 8.3, các điểm yếu phổ biến của hệ thống sinh trắc học được phân loại thành 10 yếu tố sau:

a) Các giới hạn hiệu suất;

b) Tạo tác của đặc trưng sinh trắc học;

c) Điều chỉnh đặc trưng sinh trắc học;

d) Vấn đề của việc che giấu đặc trưng sinh trắc học;

e) Tương đồng do có quan hệ huyết thống;

f) Đặc trưng sinh trắc học đặc biệt;

g) Các mẫu sinh trắc học wolf tổng hợp;

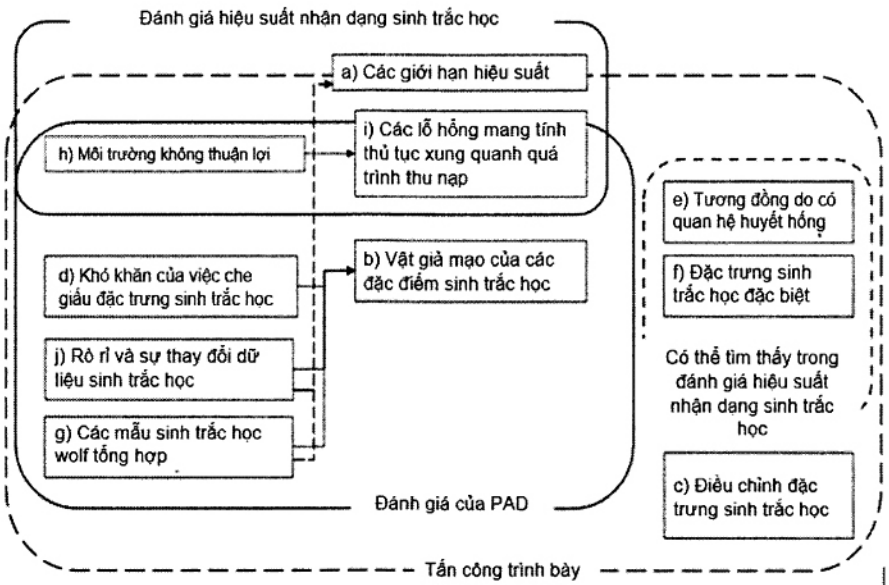
h) Môi trường không thuận lợi;

i) Các lỗ hổng mang tính thủ tục xung quanh quá trình đăng ký;

j) Rò rỉ và sự thay đổi dữ liệu sinh trắc học.

CHÚ THÍCH 1: Tất cả các yếu tố được liệt kê ở trên không phải là điểm yếu của hệ thống sinh trắc học nhưng mỗi yếu tố đều liên quan đến chúng. Trong tiêu chuẩn này, các điểm yếu của các yếu tố trên hoặc những điều liên quan đến các yếu tố và mối quan hệ của chúng với đánh giá an toàn được xem xét.

Hình 1 cho thấy mối quan hệ giữa các điểm yếu với các yếu tố được mô tả trong TCVN 11385 và các loại đánh giá được mô tả trong tiêu chuẩn này.



Hình 1 - Mối quan hệ của các điểm yếu với các yếu tố trong hệ thống sinh trắc học

Yếu tố j) quan trọng liên quan đến việc bảo vệ dữ liệu TSF/dữ liệu đã sử dụng (xem TCVN 11385). Tuy nhiên, trong tiêu chuẩn này, yếu tố j) chỉ được xem xét từ quan điểm bị kẻ tấn công khai thác để tạo điều kiện thuận lợi cho việc xây dựng PAI hoặc gắn kết các cuộc tấn công liên quan đến hiệu suất nhận dạng sinh trắc học. Việc đánh giá các biện pháp để bảo vệ dữ liệu sinh trắc học khỏi bị rò rỉ hoặc thay đổi không được đề cập ở đây.

Yếu tố a), vốn có trong tất cả các hệ thống sinh trắc học, có thể dẫn đến việc chấp nhận sai và từ chối lỗi và được đề cập trong đánh giá hiệu suất nhận dạng sinh trắc học. Tuy nhiên, nó cũng có thể được xem xét liên quan đến cuộc tấn công không có sự đầu tư (trình diện từ các nỗ lực mạo danh theo chính sách về mục đích sử dụng trong tài liệu hướng dẫn TOE). Do đó, đánh giá hiệu suất nhận dạng sinh trắc học và đánh giá PAD có mối quan hệ tương hỗ với nhau. Yếu tố này có liên quan đến việc đăng ký, xác minh và định danh.

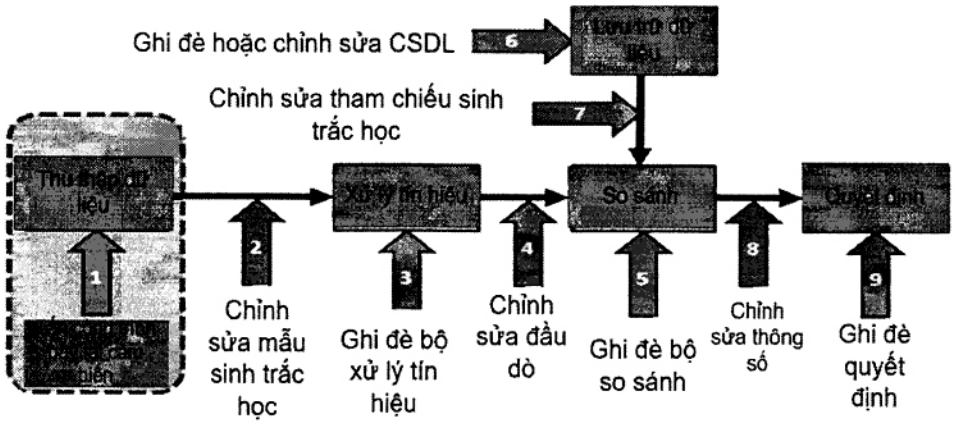
Các yếu tố khác có liên quan đến các cuộc tấn công trình diện. Tuy nhiên, các yếu tố e) và f) nằm ngoài phạm vi đánh giá PAD. Yếu tố f) liên quan đến những cá nhân có các đặc trưng sinh trắc học tự nhiên bất thường khiến họ thường phải tạo ra sự trùng khớp với những người khác. Tuy nhiên, rất khó tìm thấy những cá nhân như vậy cho mục đích kiểm tra trong quá trình đánh giá. Điều này có thể được tìm thấy một cách tình cờ do kết quả của việc đánh giá hiệu suất nhận dạng sinh trắc học. Đối với yếu tố e), rất khó để thu thập các mẫu như vậy để đánh giá an toàn. Có thể gặp các đối tượng ngoại lệ làm tăng hiệu suất nhận dạng sinh trắc học cao bất thường trong quá trình kiểm tra hiệu suất nhận dạng sinh trắc học. Điều này có thể tiết lộ một lỗ hổng tiềm năng trong TOE và thông tin liên quan nên được sử dụng để thông báo cho hoạt động đánh giá AVA.

Yếu tố c) có thể được coi là một phương tiện tấn công trình diện sẽ khai thác các điểm yếu được nhận dạng như những điểm được tiết lộ với a) và f) nhưng do đó cần được xem xét trong giai đoạn phân tích tính dễ bị tổn thương. Tuy nhiên, nó đòi hỏi các yếu tố phụ nằm ngoài phạm vi đánh giá khách quan. Ví dụ, phẫu thuật để nhúng đặc trưng sinh trắc học của người khác đòi hỏi đối tượng thử nghiệm phải chấp nhận loại bỏ điều gì đó và việc bắt chước đòi hỏi họ phải phát triển các kỹ năng đặc biệt.

Do đó, các yếu tố b), d), g), h) và i) là các yếu tố được đánh giá trong đánh giá TCVN 8709 đối với PAD. Yếu tố i) chỉ cần được xem xét khi đăng ký. Các yếu tố b), g), và h) có liên quan đến sự đăng ký, xác minh và định danh, nhưng lưu ý rằng yếu tố i) bị ảnh hưởng bởi yếu tố h) như được mô tả trong TCVN 11385. Môi trường không thuận lợi có thể gây ra việc đăng ký kém chất lượng. Các tham chiếu sinh trắc tốt sau này có thể được so sánh với các mẫu sinh trắc kém chất lượng (xem TCVN 11385:2016, 8.3.9 và 8.3.10 để biết thêm thông tin). Lưu ý rằng các yếu tố h) và i) phải được đánh giá trong đánh giá TCVN 8709 về hiệu suất nhận dạng sinh trắc học. Yếu tố d) đề cập đến thực tế là nhiều đặc trưng sinh trắc học không bị che giấu và do đó, có khả năng dễ bị thu thập và ghi lại để sử dụng trong việc xây dựng PAI nhằm thực hiện các cuộc tấn công trình diện (ví dụ: hình ảnh dấu vân tay bị ẩn, hình ảnh khuôn mặt, bản ghi âm giọng nói). Do đó, nó sẽ được tính đến khi tính toán tiềm năng tấn công của một cuộc tấn công (xem F.1). Yếu tố g) cũng nên được xem xét trong đánh giá hiệu suất nhận dạng sinh trắc học, vì các mẫu wolf tổng hợp có thể bị khai thác bởi một cuộc tấn công vào hệ thống ở nơi khác chứ không phải trên hệ thống con thu thập dữ liệu (ví dụ: thông qua việc chèn mẫu thích hợp trong quá trình nhận dạng). Điều này liên quan đến các nhiệm vụ phân tích các lỗ hổng trong TCVN 14190-2.

CHÚ THÍCH 2: Yếu tố g) có liên quan gián tiếp đến yếu tố f). Yếu tố f) có thể được coi là một biến thể xuất hiện tự nhiên của yếu tố g) để việc đánh giá khả năng chống chịu của một TOE đối với các mẫu wolf tổng hợp có thể cung cấp cái nhìn chi tiết về khả năng dễ bị tổn thương đối với các đặc trưng sinh trắc học đặc biệt xuất hiện tự nhiên.

Kẻ tấn công có thể có nhiều mục tiêu khác nhau: Kẻ giả mạo sinh trắc học sẽ cố gắng được công nhận là người đăng ký sinh trắc học khác với bản thân kẻ giả mạo. Đối tượng che giấu sinh trắc học sẽ cố gắng tránh bị trùng khớp với tham chiếu sinh trắc học của chính bản thân đối tượng đó.



Hình 2 - Ví dụ về các điểm tấn công trong hệ thống sinh trắc học (theo ISO/IEC 30107-1)

Hình 2 minh họa chung về các cuộc tấn công chống lại hệ thống sinh trắc học. Trong số các cuộc tấn công này, cuộc tấn công được chỉ định bằng mũi tên 1 là cuộc tấn công trình diện và những cuộc tấn công được chỉ định bằng mũi tên 2 và 4 đánh dấu những nơi có thể thực hiện các cuộc tấn công dựa trên dữ liệu mẫu sinh trắc học đã được thu thập và liên quan đến hiệu suất nhận dạng sinh trắc học. Điểm tấn công 2 và 4 chỉ được xem xét trong TCVN 14190-2 khi kịch bản tấn công liên quan đến việc khai thác hành vi cụ thể của hiệu suất nhận dạng sinh trắc học (ví dụ điểm yếu của thuật toán). Các khía cạnh khác được đề cập trong các phương pháp tiếp cận đánh giá an toàn CNTT một cách tổng quan và không dành riêng cho việc đánh giá an toàn của một hệ thống sinh trắc học. Tóm lại, các mục tiêu của TCVN 14190-2 và TCVN 14190-3 là như sau.

Đối với ATE, TCVN 14190-2 đề cập đến việc kiểm tra hiệu suất nhận dạng sinh trắc học để đánh giá các trình diện từ các nỗ lực mạo danh theo chính sách về mục đích sử dụng theo tài liệu hướng dẫn TOE.

TCVN 14190-3 đề cập đến việc thử nghiệm cơ chế phát hiện tấn công trình diện.

Đối với AVA, TCVN 14190-2 dành cho tất cả các điểm yếu cụ thể về sinh trắc học (nghĩa là liên quan đến một mức độ nào đó đối với các hoạt động định danh sinh trắc học), loại trừ những trình diện được thu thập lại bởi hệ thống con, ngược với chính sách sử dụng được mô tả theo tài liệu hướng dẫn TOE; TCVN 14190-3 liên quan đến bất kỳ lỗ hổng nào với một cuộc tấn công trình diện được thu thập lại bởi hệ thống con, ngược với chính sách sử dụng được mô tả theo tài liệu hướng dẫn TOE.

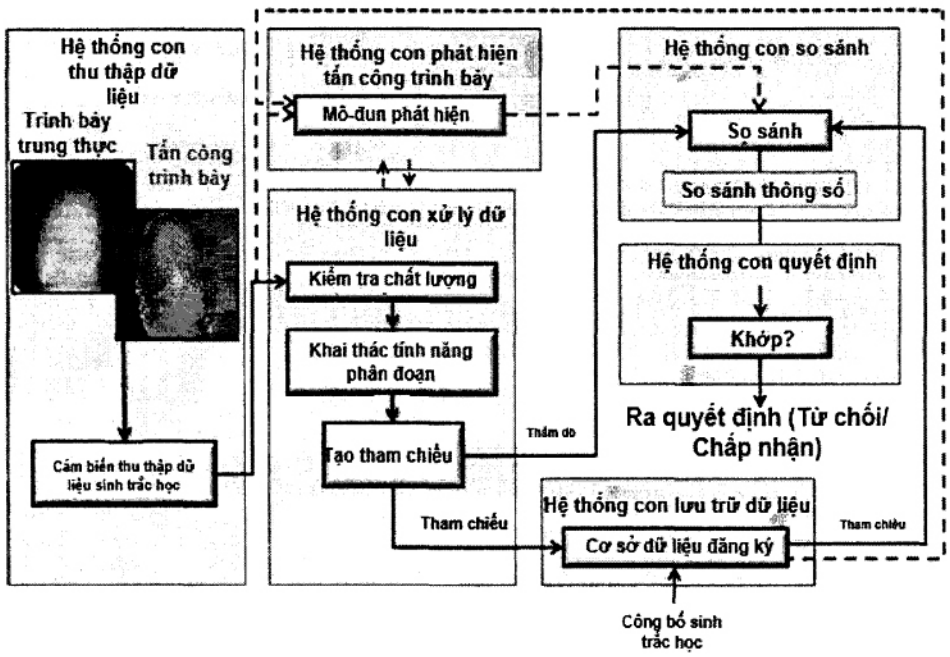
CHÚ THÍCH 3: Các lỗ hổng có thể kết hợp với các lỗ hổng CNTT ảnh hưởng tới các lỗ hổng nêu trên cũng nằm trong phạm vi đánh giá an toàn dựa trên TCVN 8709.

6.2 Hệ thống sinh trắc học và phát hiện tấn công trình diện

Mục đích chung của hệ thống sinh trắc học là nhận biết các cá nhân bằng các đặc trưng sinh trắc học của họ. Một chủ đề dữ liệu trình diện một hoặc nhiều đặc trưng sinh trắc học cho thiết bị thu thập sinh trắc học của hệ thống sinh trắc học để đăng ký, xác minh hoặc định danh. Trong quá

trình thu thập, các mẫu sinh trắc học được thu thập và từ đó các đặc trưng sinh trắc học được trích xuất. Ở giai đoạn đăng ký, các tính năng sinh trắc học đã được trích xuất được sử dụng để tạo tham chiếu sinh trắc học được lưu trữ trong cơ sở dữ liệu đăng ký. Ở giai đoạn xác minh/định danh, các đặc trưng sinh trắc học được sử dụng để tạo một mẫu sinh trắc học để so sánh với (các) tham chiếu sinh trắc học có liên quan. Hình 3 là mô tả khái niệm của hệ thống sinh trắc học có chứa hệ thống con PAD (phát hiện tấn công trình diện). Chức năng của hệ thống con PAD thường không được triển khai như một hệ thống con riêng biệt như được chỉ ra trong Hình 3 nhưng được kết hợp trong một hoặc nhiều hệ thống con bao gồm hệ thống sinh trắc học (ví dụ: hệ thống con thu thập dữ liệu, hệ thống con xử lý tín hiệu).

Hình 3 là mô tả khái niệm của hệ thống sinh trắc học có chứa hệ thống con PAD. Cơ chế hệ thống con PAD thường không được triển khai như một hệ thống con riêng biệt như được chỉ ra trong Hình 3 nhưng được kết hợp trong một hoặc nhiều hệ thống con bao gồm hệ thống sinh trắc học (ví dụ: hệ thống con thu thập dữ liệu, hệ thống con xử lý tín hiệu). Một cuộc tấn công trình diện có thể được thực hiện bằng cách trình diện một công cụ của tấn công trình diện (ví dụ: một vật nhân tạo và những công cụ liên quan khác được sử dụng trong cuộc tấn công) cho một hệ thống sinh trắc học. Hệ thống con PAD được sử dụng ở giai đoạn xác minh/định danh và cả ở giai đoạn đăng ký.

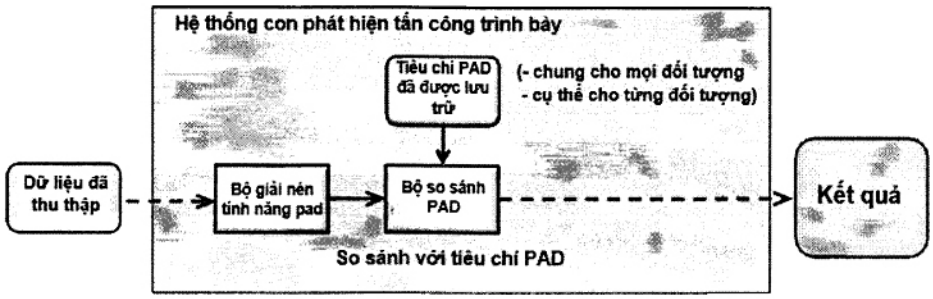


Hình 3 - Khung sinh trắc học chung kết hợp hệ thống con PAD (biểu diễn khái niệm)

Có thể có các cơ chế tại chỗ để bảo vệ thông tin liên lạc giữa khách hàng và dịch vụ nhưng những cơ chế này không được TCVN này đề cập đến. Các biện pháp và giao thức an toàn được mô tả trong TCVN này chỉ quan tâm đến việc xác thực của người dùng đối với dịch vụ sử dụng BHSM. Điều này bao gồm các biện pháp để đảm bảo giao tiếp đầu cuối an toàn giữa BHSM và dịch vụ sao cho, ví dụ, kẻ mạo danh không thể xác thực dịch vụ với tư cách là người dùng được ủy quyền bằng cách đánh cắp hay giả mạo BHSM hoặc khách hàng.

CHÚ THÍCH: Hình 3 được lấy từ ISO/IEC 30107-1 và được sửa đổi để thay thế một thuật ngữ cũ với trình diện trung thực. Một đường đứt nét trong Hình 3 cho thấy sự tương tác giữa hệ thống con PAD và một hệ thống con khác. "Công bố sinh trắc học" trong Hình 3 có nghĩa là công bố tham chiếu sinh trắc học.

Hình 4, cũng được lấy từ ISO/IEC 30107-1, cung cấp các chi tiết bổ sung về hệ thống con PAD được giải thích trong ISO/IEC 30107-1: 2016, 6.4.1, như sau: "Một số hệ thống con PAD có thể không cần tính năng bộ trích xuất tính chất PAD. Bộ so sánh PAD và các tiêu chí PAD được lưu trữ là rất cần thiết trong các hệ thống con ".



Hình 4 - Các thành phần trong hệ thống con PAD chung

ISO/IEC 30107-1: 2016, 6.4.2, mô tả mối quan hệ giữa hệ thống con PAD và các hệ thống con sinh trắc học khác như sau:

"Nên xem xét việc thu thập và xử lý dữ liệu PAD và dữ liệu mẫu sinh trắc học một cách độc lập trong cả thời gian và không gian. Hai dạng dữ liệu có thể cùng tồn tại hoặc có thể tồn tại trong trường hợp không có dữ liệu kia. Quá trình của PAD có thể được xử lý đồng thời, trước hoặc sau bởi một hệ thống sinh trắc học với bất kỳ hệ thống con nào. Các thành phần của hệ thống con PAD thậm chí có thể xuất hiện riêng biệt, giữa và (hoặc) đồng thời với nhiều hệ thống con. Đầu ra PAD có thể phụ thuộc vào nhiều mẫu sinh trắc học được thu thập và không nhất thiết phải là một tín hiệu nhị phân đơn lẻ".

Các kỹ thuật PAD có thể bao gồm cảm biến phần cứng của các cuộc tấn công trình diện và phân tích mẫu sinh trắc học và dữ liệu liên quan khác để tìm kiếm các điều kiện hoặc hoạt động đáng ngờ. Nhiều kỹ thuật có thể được sử dụng với các quyết định dựa trên sự kết hợp các kết quả từ mỗi kỹ thuật riêng lẻ.

Khi đánh giá một cơ chế PAD, tất cả các thành phần phần cứng và phần mềm liên quan đến an toàn phải được xem xét, bao gồm cả các thành phần liên quan đến quá trình thu thập bằng chứng trình diện. Trong một số trường hợp, cảm biến thu thập thông thường được sử dụng trong hệ thống con sinh trắc học có thể cung cấp thông tin này. Trong các trường hợp khác, một cảm biến thu thập chuyên dụng cho PAD có thể được sử dụng. Nếu việc thu thập mẫu nhận dạng và thu thập bằng chứng trình diện bị tách biệt về không gian hoặc thời gian, điều này có thể cho phép các cuộc tấn công trình diện nhắm mục tiêu đến hai quy trình thu thập riêng lẻ và do đó tạo ra các lỗ hổng tiềm năng. Các lỗ hổng này cần được kiểm tra trong quá trình đánh giá (xem TCVN 14190-3).

6.3 Phân loại các TOE liên quan đến loại đánh giá

6.3.1 Đánh giá hiệu suất nhận dạng sinh trắc học

Trong việc đánh giá hiệu suất nhận dạng sinh học, các TOE được phân thành hai loại. Loại đầu tiên là trong đó cơ chế nhận dạng sinh trắc học của TOE chỉ bao gồm các cơ chế phần mềm có thể được phân phối thông qua nhiều hệ thống con nhưng không chứa thiết bị thu thập sinh trắc học. Trong danh mục này, TOE ít nhất chứa hệ thống con so sánh và có thể chứa (các) hệ thống con khác. Loại thứ hai là TOE bao gồm một hệ thống sinh trắc học hoàn chỉnh bao gồm hệ thống con thu thập sinh trắc học (với một thiết bị thu thập sinh trắc học).

Thử nghiệm hiệu suất nhận dạng sinh trắc học phải được thực hiện bằng một thử nghiệm kỹ thuật của thuật toán nhận dạng sinh trắc học sử dụng cơ sở dữ liệu thử nghiệm đã thu được trước đó có chứa các mẫu sinh trắc học và tham chiếu sinh trắc học hoặc bằng thử nghiệm kịch bản cùng nhóm thử nghiệm đã đăng ký với một tổ hợp nhất định của các hệ thống con khác bao gồm hệ thống con thu thập dữ liệu. Với loại đầu tiên, chỉ có thể đánh giá về mặt công nghệ. Trong loại thứ hai, khả năng cao thử nghiệm hiệu suất nhận dạng sinh trắc học được thực hiện dưới hình thức đánh giá kịch bản (theo ISO/IEC 19795-1) với một nhóm thử nghiệm trong khi cả hai đánh giá đều có thể thực hiện được.

CHÚ THÍCH: Trong cả hai loại trên, kết quả thực hiện định danh sinh trắc học liên quan đến một hệ thống hoàn chỉnh. Trong loại đầu tiên, TOE chỉ bao gồm một phần của hệ thống hoàn chỉnh. Trong loại thứ hai, nó bao gồm hệ thống hoàn chỉnh. Trong loại đầu tiên, hệ thống hoàn chỉnh bao gồm TOE và các hệ thống con khác tạo thành môi trường đánh giá được mô tả trong mục tiêu an toàn và kết quả đánh giá chỉ áp dụng cho môi trường đó.

Danh sách sau đây xác định một tập hợp các loại TOE điển hình từ thế giới sinh trắc học và đưa ra một số hướng dẫn về các khía cạnh đặc biệt cần được xem xét của chúng.

- TOE chỉ là phần mềm: TOE chỉ là phần mềm bao gồm một thuật toán chỉ để so sánh hoặc trích xuất và so sánh tính năng. Điều này được quan tâm cụ thể trong các trường hợp của các hệ thống được cấu tạo trong đó một nhà phát triển chỉ cung cấp thuật toán. Trong trường hợp như vậy, có thể hữu ích khi đánh giá các đặc tính an toàn của thuật toán dưới các giả định thích hợp về môi trường của nó. Sau đó, thuật toán có thể được tích hợp vào một phạm vi hệ thống rộng hơn và một đánh giá mới về hệ thống hoàn chỉnh có thể sử dụng lại kết quả đánh giá của thuật toán. Một lĩnh vực khác trong đó TOE chỉ là phần mềm có thể được hướng tới là thẻ thông minh. Ví dụ, một hệ thống so sánh trên thẻ (hoặc so sánh trên thẻ) thường chỉ bao gồm phần mềm để so sánh, được thiết kế chỉ hoạt động trên một chip điện tử an toàn.

- Hệ thống hoàn chỉnh bao gồm thiết bị thu thập sinh trắc học: Một hệ thống sinh trắc học hoàn chỉnh được định nghĩa là TOE bao gồm tất cả các chức năng và đặc điểm an toàn liên quan.

Các thành phần mở rộng của SFR cho hiệu suất nhận dạng sinh trắc học được quy định trong Điều 8.

6.3.2 Đánh giá PAD

Trong trường hợp đánh giá PAD, các TOE được phân loại thành ba trường hợp. Trường hợp đầu tiên là trường hợp chỉ chứa hệ thống con PAD và không cung cấp các chức năng nhận dạng sinh trắc học khác. Trường hợp thứ hai là trường hợp chứa hệ thống con thu thập dữ liệu và chức năng kiểm tra chất lượng bổ sung cho cơ chế PAD nhưng không chứa hệ thống con so sánh. Trường hợp thứ ba là trường hợp chứa ít nhất hệ thống con so sánh và hệ thống con quyết định để xác minh hoặc định danh sinh trắc học ngoài cơ chế PAD. Điều này có thể chứa hệ thống con thu thập dữ liệu hoặc không. Phần mềm xác minh sinh trắc học trên điện thoại thông minh, không được cung cấp từ nhà cung cấp điện thoại thông minh và thẻ IC chỉ cung cấp so sánh sinh trắc học trên thẻ, là hai ví dụ về TOE của trường hợp thứ ba không chứa hệ thống con thu thập dữ

liệu. Khi một PAI bị TOE từ chối trong hai trường hợp sau, Kiểm thử viên có thể biết hoặc không biết liệu việc từ chối có phải là kết quả của việc phát hiện bởi hệ thống con PAD hay vì một số lý do khác như không đạt được, chất lượng mẫu kém, không khớp, thời gian chờ, v.v., tùy thuộc vào thông tin do TOE cung cấp cho Kiểm thử viên.

Các SFR được áp dụng phụ thuộc vào trường hợp một TOE thuộc về. Nếu TOE thuộc trường hợp đầu tiên của hệ thống con PAD, thì các thành phần mở rộng của SFR được quy định trong 7.2 sẽ được áp dụng. Nếu TOE thuộc trường hợp thứ hai, thì các thành phần mở rộng của các SFR quy định trong 7.3 sẽ được áp dụng. Mặt khác, nếu TOE thuộc trường hợp thứ ba, thì các thành phần mở rộng của SFR được quy định trong Điều 8 sẽ được áp dụng.

7 Thành phần chức năng an toàn mở rộng cho Lớp FPT: Bảo vệ TSF

7.1.Tổng quát

Mục này đưa ra định nghĩa về các họ bổ sung FPT_PAD và FPT_BCP của Lớp FPT, được quy định trong TCVN 8709-2, có thể được sử dụng trong các hồ sơ bảo vệ và mục tiêu an toàn để mô hình hóa các cơ chế an toàn của hệ thống con PAD và hệ thống con thu thập dữ liệu với PAD. FPT_BCP và FPT_BCP là các họ được áp dụng tương ứng cho trường hợp thứ nhất và trường hợp thứ hai của TOE được đưa ra trong 6.3.2.

Một số SFR sau đây có các nhiệm vụ cho phép người lập ra ST hoặc PP chỉ định đặc trưng sinh trắc học được sử dụng để triển khai cơ chế (ví dụ: dấu vân tay). Những nhiệm vụ này nhằm tạo điều kiện cho người đọc hiểu được ST cuối cùng.

Phụ lục B cung cấp thông tin giải thích về các thành phần chức năng an toàn mở rộng cho lớp FPT và sẽ một số ý cần tham khảo khi sử dụng các thành phần được xác định trong Điều 7.

CHÚ THÍCH: lớp FPT là lớp "Bảo vệ TSF" được quy định trong TCVN 8709-2 (xem TCVN 8709-2:2008, Điều 14 và Phụ lục A).

7.2. Phát hiện tấn công trình diện

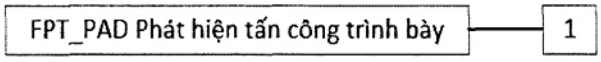
7.2.1 Họ hành vi

Họ này xác định các yêu cầu chức năng an toàn để phát hiện các cuộc tấn công trình diện sinh trắc học.

CHÚ THÍCH: FPT_PAD là họ cho TOE thuộc loại đầu tiên được phân loại trong 6.3.2.

7.2.2 Thành phần nền

Hình 5 cho thấy cấu trúc của họ này.



Hình 5 - Họ phát hiện tấn công trình diện FPT_PAD

FPT_PAD.1 phát hiện tấn công trình diện, phát hiện các cuộc tấn công trình diện cho đáp ứng sinh trắc học hoặc vượt quá các tiêu chí được quy định đối với TOE.

7.2.3 Quản lý của FPT_PAD.1

Hành động sau đây có thể được xem xét đối với các chức năng quản lý trong FMT: quản lý các tham số được sử dụng để phát hiện tấn công trình diện.

7.2.4 Kiểm thử của FPT_PAD.1

Các hành động sau đây có thể được kiểm thử nếu việc tạo dữ liệu kiểm tra an toàn FAU_GEN được bao gồm trong PP/ST:

a) Tối thiểu: Cuộc tấn công trình diện được phát hiện;

b) Cơ bản: Trình diện trung thực được phát hiện.

7.2.5 FPT_PAD.1 Phát hiện tấn công trình diện

Phân cấp thành: Không có các thành phần khác

Phụ thuộc : FMT_MTD.3 bảo vệ dữ liệu TSF

Đặc tả FMT_SMF.1 của các chức năng quản lý

FPT_PAD.1.1

TSF sẽ có thể phân biệt giữa các trình diện trung thực và các tấn công trình diện.

FPT_PAD.1.2

Nếu một cuộc tấn công trình diện được phát hiện, (các) hành động sau sẽ được thực hiện: [gắn với: *danh sách các hành động (list of actions)*].

FPT_PAD.1.3

Nếu phát hiện thấy một trình diện không trung thực, (các) hành động sau sẽ được thực hiện: [gắn với: *danh sách các hành động (list of actions)*].

FPT_PAD.1.4

Cùng với phản hồi về trạng thái tấn công trình diện, được phát hiện hoặc không được phát hiện, TSF sẽ cung cấp thông tin sau: [gắn với: *danh sách thông tin (list of actions)*].

CHÚ THÍCH: Trong TCVN 8709-2, FPT_PAD.1.1, FPT_PAD.1.2, FPT_PAD.1.3 và FPT_PAD.1.4 sẽ được đánh số lần lượt là 7.2.5.1, 7.2.5.2, 7.2.5.3 và 7.2.5.4.

7.3. Thu thập sinh trắc học với phát hiện tấn công trình diện (FPT_BCP)

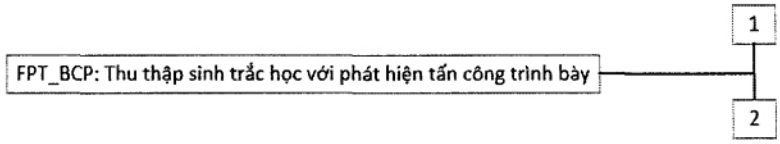
7.3.1 Họ hành vi

Họ này xác định các yêu cầu chức năng an toàn để thu thập sinh trắc học với phát hiện tấn công trình diện được hỗ trợ bởi TSF. Họ này cũng xác định các thuộc tính bắt buộc phải dựa trên cơ chế thu thập sinh trắc học với phát hiện tấn công trình diện.

CHÚ THÍCH: FPT_BCP là một họ cho TOE thuộc loại thứ hai được xác định trong 6.3.2.

7.3.2 Thành phần nền

Hình 6 cho thấy cấu trúc của họ này.



Hình 6 - FPT_BCP Họ thu thập sinh trắc học với phát hiện tấn công trình diện

FPT_BCP.1 Kiểm tra các mẫu sinh trắc học cho việc thu thập sinh trắc học với phát hiện tấn công trình diện, yêu cầu TSF ngăn chặn việc tạo các mẫu sinh trắc học hoặc báo cáo việc phát hiện tấn công trình diện nếu công cụ của tấn công trình diện đã được trình diện.

FPT_BCP.2 Tính năng thu thập sinh trắc học với tỷ lệ thất bại thấp, bên cạnh việc yêu cầu TSF tạo ra các mẫu sinh trắc học có chất lượng rất cao để tránh việc chỉ được sử dụng để đăng ký các mẫu sinh trắc học như vậy mà còn nhằm đạt được hiệu quả rõ ràng trong việc xác minh/định danh sinh trắc học sau đó, đồng thời yêu cầu TSF giới hạn FTAR trong một ngưỡng xác định.

7.3.3 Quản lý của FPT_BCP.1

Các hành động sau đây có thể được xem xét đối với các chức năng quản lý trong FMT:

a) Việc quản lý dữ liệu TSF, bao gồm, ví dụ: các giá trị ngưỡng cho điểm chất lượng để tạo ra mẫu sinh trắc học bởi quản trị viên;

b) Việc quản lý dữ liệu TSF, bao gồm, ví dụ: các giá trị để phát hiện các công cụ của tấn công trình diện bởi quản trị viên.

7.3.4 Quản lý của FPT_BCP.2

Hành động sau có thể được xem xét đối với chức năng quản lý trong FMT: quản lý dữ liệu TSF, bao gồm, ví dụ, giá trị ngưỡng cho điểm chất lượng để tạo mẫu sinh trắc học bởi quản trị viên.

7.3.5 Kiểm thử của FPT_BCP.1

Các hành động sau đây có thể được kiểm thử nếu FAU_GEN tạo dữ liệu kiểm thử an toàn được bao gồm trong PP/ST:

a) Tối thiểu: Từ chối bởi TSF của dữ liệu được kiểm tra có chất lượng thấp hoặc được phát hiện là công cụ tấn công trình diện;

b) Cơ bản: Từ chối hoặc chấp nhận bởi TSF của dữ liệu được kiểm tra có chất lượng bình thường hoặc đầu vào cho hệ thống con thu thập sinh trắc học với phát hiện tấn công trình diện;

c) Chi tiết: Các định các thay đổi đối với dữ liệu TSF, bao gồm, ví dụ, các giá trị ngưỡng cho điểm chất lượng và phát hiện các công cụ tấn công trình diện.

CHÚ THÍCH: Lớp FAU là Lớp "Đánh giá an toàn" được quy định trong TCVN 8709-2 (xem TCVN 8709-2: 2008, Điều 14).

7.3.6 Kiểm thử của FPT_BCP.2

Các hành động sau đây có thể được kiểm thử được nếu việc tạo dữ liệu kiểm thử an toàn FAU_GEN được bao gồm trong PP/ST:

a) Tối thiểu: Từ chối bởi TSF của dữ liệu được kiểm tra có chất lượng thấp;

b) Cơ bản: Từ chối hoặc chấp nhận bởi TSF của dữ liệu được kiểm tra có chất lượng bình thường;

c) Chi tiết: Xác định các thay đổi đối với dữ liệu TSF, bao gồm, ví dụ: các giá trị ngưỡng cho điểm chất lượng của dữ liệu sinh trắc học để thu thập.

7.3.7 FPT_BCP.1 Kiểm tra các mẫu sinh trắc học để thu thập

Phân cấp thành: Không có thành phần nào khác.

Phụ thuộc: Không có phụ thuộc.

FPT_BCP.1.1

TSF sẽ ngăn chặn việc sử dụng các công cụ tấn công trình diện không phải nhân tạo để tạo ra các mẫu sinh trắc học từ [gắn với: đặc trưng sinh trắc học] đã được trình diện bởi bất kỳ người dùng TSF nào.

FPT_BCP.1.2

TSF sẽ ngăn chặn việc sử dụng các công cụ tấn công trình diện nhân tạo để tạo ra các mẫu sinh trắc học từ [gắn với: đặc trưng sinh trắc học] đã được trình diện bởi bất kỳ người dùng TSF nào.

CHÚ THÍCH Trong TCVN 8709-2, FPT_BCP.1.1 và FPT_BCP.1.2 sẽ được đánh số lần lượt là 7.3.7.1 và 7.3.7.2.

7.3.8 FPT_BCP.2 Thu thập sinh trắc học với tỷ lệ lỗi thấp

Phân cấp thành: Không có thành phần nào khác.

Phụ thuộc: Không có phụ thuộc.

FPT_BCP.2.1

TSF sẽ cung cấp một cơ chế để thu thập dữ liệu sinh trắc học từ [gắn với: đặc trưng sinh trắc học] với FTAR không vượt quá [gắn với: giá trị xác định].

CHÚ THÍCH: Trong TCVN 8709-2, FPT_BCP.2.1 sẽ được đánh số là 7.3.8.1.

8. Thành phần chức năng an toàn mở rộng cho Lớp FIA: Định danh và Xác thực

8.1 Tổng quát

Mục này cung cấp định nghĩa về các nhóm bổ sung FIA_EBR (xem 8.2), FIA_BVR (xem 8.3) và FIA_BID (xem 8.4) của Lớp FIA, được chỉ định trong TCVN 8709-2, có thể được sử dụng trong các hồ sơ bảo vệ và đích an toàn để mô hình hóa cơ chế an toàn của PAD cho việc đăng ký, xác minh và định danh sinh trắc học. Các nhóm được áp dụng cho các TOE thuộc một trong hai trường hợp trong 6.3.1 của đánh giá hiệu suất nhận dạng sinh trắc học và cho các TOE của trường hợp thứ ba trong 6.3.2 để đánh giá PAD.

Phụ lục C cung cấp thông tin giải thích cho các thành phần chức năng an toàn mở rộng cho Lớp FIA và sẽ được tham khảo tới khi sử dụng các thành phần được xác định trong Mục 8.

CHÚ THÍCH 1: Lớp FIA là lớp "Định danh và xác thực" được quy định trong TCVN 8709-2: 2008 (xem TCVN 8709-2: 2008, Điều 11, và cả Phụ lục A).

CHÚ THÍCH 2: Từ quan điểm đánh giá PAD, các nhóm được cung cấp trong mục này là cho một TOE thuộc loại thứ ba được phân loại trong 6.3.2.

8.2 Đăng ký tham chiếu sinh trắc học (FIA_EBR)

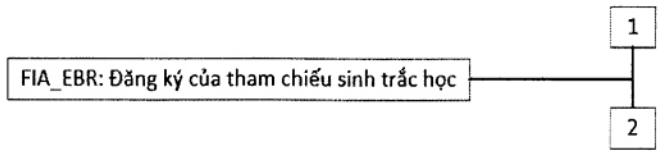
8.2.1 Họ hành vi

CHÚ THÍCH: Trong TCVN 8709-2, tiêu đề là "họ hành vi".

Họ này xác định các cơ chế đăng ký để xác minh/định danh sinh trắc học được hỗ trợ bởi TSF. Họ này cũng xác định các thuộc tính bắt buộc mà các cơ chế đăng ký sinh trắc học phải dựa trên đó.

8.2.2 Thành phần nền

Hình 7 cho thấy cấu trúc của họ này.



Hình 7 – FIA_EBR Họ đăng ký của tham chiếu sinh trắc học

FIA_EBR.1 Kiểm tra các đặc trưng sinh trắc học để đăng ký, yêu cầu TSF ngăn chặn đăng ký nếu các công cụ tấn công trình diện được sử dụng.

FIA_EBR.2 Đăng ký sinh trắc học với tỷ lệ không đăng ký được thấp, yêu cầu TSF chỉ đăng ký các tham chiếu sinh trắc học có chất lượng cực kỳ tốt để đạt được hiệu suất cao trong việc xác minh/định danh sinh trắc học sau đó.

8.2.3 Quản lý của FIA_EBR.1

Các hành động sau đây có thể được xem xét đối với các chức năng quản lý trong FMT:

a) Việc quản lý dữ liệu TSF, bao gồm, ví dụ: các giá trị ngưỡng cho điểm chất lượng để tạo ra tham chiếu sinh trắc học bởi quản trị viên;

b) Việc quản lý dữ liệu TSF, bao gồm, ví dụ: các giá trị để phát hiện các công cụ của tấn công trình diện bởi quản trị viên.

8.2.4 Quản lý của FIA_EBR.2

Hành động sau đây có thể được xem xét đối với các chức năng quản lý trong FMT: quản lý dữ liệu TSF, bao gồm, ví dụ: giá trị ngưỡng cho điểm chất lượng để quản trị viên tạo ra tham chiếu sinh trắc học.

8.2.5 Kiểm thử của FIA_EBR.1

Các hành động sau đây có thể được kiểm thử nếu FAU_GEN tạo dữ liệu kiểm thử an toàn được bao gồm trong PP/ST:

a) Tối thiểu: Từ chối bởi TSF của dữ liệu được kiểm tra có chất lượng thấp hoặc được phát hiện là công cụ tấn công trình diện;

b) Cơ bản: Từ chối hoặc chấp nhận bởi TSF của dữ liệu được kiểm tra có chất lượng bình thường hoặc đầu vào cho hệ thống con phát hiện tấn công trình diện;

c) Chi tiết: Xác định các thay đổi đối với dữ liệu TSF, bao gồm, ví dụ: các giá trị ngưỡng cho điểm chất lượng và phát hiện các công cụ tấn công trình diện.

8.2.6 Kiểm thử của FIA_EBR.2

Các hành động sau đây có thể được kiểm thử được nếu việc tạo dữ liệu kiểm thử an toàn FAU_GEN được bao gồm trong PP/ST:

a) Tối thiểu: Từ chối bởi TSF của dữ liệu được kiểm tra có chất lượng thấp;

b) Cơ bản: Từ chối hoặc chấp nhận bởi TSF của dữ liệu được kiểm tra có chất lượng bình thường;

c) Chi tiết: Xác định các thay đổi đối với dữ liệu TSF, bao gồm, ví dụ: các giá trị ngưỡng cho điểm chất lượng của dữ liệu sinh trắc học để đăng ký.

8.2.7 FPT_BCP.1 Kiểm tra các mẫu sinh trắc học để đăng ký

Phân cấp thành: Không có thành phần nào khác.

Phụ thuộc: Không có phụ thuộc.

FIA_EBR.1.1

TSF sẽ ngăn chặn việc sử dụng các công cụ tấn công trình diện không phải nhân tạo để đăng ký [gắn với: đặc trưng sinh trắc học] đã được trình diện bởi bất kỳ người dùng TSF nào.

FIA_EBR.1.2

TSF sẽ ngăn chặn việc sử dụng các công cụ tấn công trình diện nhân tạo để đăng ký [gắn với: đặc trưng sinh trắc học] đã được trình diện bởi bất kỳ người dùng TSF nào.

CHÚ THÍCH: Trong TCVN 8709-2, FIA_EBR.1.1 và FIA_EBR.1.2 sẽ được đánh số tương ứng là 8.2.7.1 và 8.2.7.2.

8.2.8 FPT_BCP.2 Đăng ký sinh trắc học với tỷ lệ lỗi thấp

Phân cấp thành: Không có thành phần nào khác.

Phụ thuộc: Không có phụ thuộc.

FIA_EBR.2.1

TSF sẽ cung cấp cơ chế đăng ký tham chiếu sinh trắc học cho [gắn với: đặc trưng sinh trắc học] với FTER không vượt quá [gắn với: giá trị xác định].

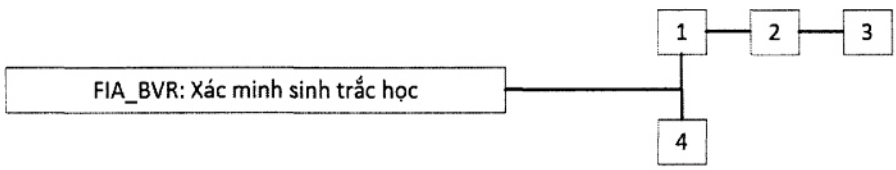
8.3 Xác minh sinh trắc học (FIA_BVR)

8.3.1 Họ hành vi

Họ này xác định các cơ chế xác minh sinh trắc học được TSF hỗ trợ. Họ này cũng xác định các thuộc tính bắt buộc mà các cơ chế xác minh sinh trắc học sẽ dựa trên đó.

8.3.2 Thành phần nền

Hình 8 cho thấy cấu trúc của họ này.



Hình 8 - Xác minh sinh trắc học FIA_BVR

FIA_BVR.1 Xác minh sinh trắc học với hiệu suất cao, yêu cầu TSF giới hạn FMR và FNMR hoặc FAR và FRR tương ứng trong một tỷ lệ được chỉ định.

FIA_BVR.2 Thời gian xác thực người dùng với xác minh sinh trắc học, cho phép người dùng thực hiện các hành động nhất định trước khi xác thực người dùng với xác minh sinh trắc học danh tính của người dùng.

FIA_BVR.3 Xác thực người dùng bằng xác minh sinh trắc học trước bất kỳ hành động nào, yêu cầu người dùng phải xác thực bằng xác minh sinh trắc học trước khi TSF cho phép bất kỳ hành động nào khác.

FIA_BVR.4 Xác minh sinh trắc học không chấp nhận các công cụ tấn công trình diện, yêu cầu cơ chế xác minh sinh trắc học để có thể ngăn chặn việc sử dụng thành công công cụ tấn công trình diện khi cố gắng xác minh.

8.3.3 Quản lý của FIA_BVR.1

Hành động sau đây có thể được xem xét đối với các chức năng quản lý trong FMT: quản lý dữ liệu TSF (bao gồm các giá trị ngưỡng) của quản trị viên.

8.3.4 Quản lý của FIA_BVR.2

Các hành động sau đây có thể được xem xét đối với các chức năng quản lý trong FMT:

a) Quản trị viên quản lý dữ liệu TSF (bao gồm các giá trị ngưỡng);

b) Quản lý danh sách các hành động có thể được thực hiện trước khi người dùng được xác thực.

8.3.5 Quản lý của FIA_BVR.3

Hành động sau đây có thể được xem xét đối với các chức năng quản lý trong FMT: quản lý dữ liệu TSF (bao gồm các giá trị ngưỡng) của quản trị viên.

8.3.6 Quản lý của FIA_BVR.4

Hành động sau đây có thể được xem xét đối với các chức năng quản lý trong FMT: quản lý dữ liệu TSF, bao gồm, ví dụ: các giá trị của quản trị viên để phát hiện các công cụ tấn công trình diện và để kiểm tra chất lượng để tạo ra các mẫu sinh trắc học.

CHÚ THÍCH: Người quản trị là người quản lý hệ thống sinh trắc học.

8.3.7 Kiểm thử của FIA_BVR.1

Các hành động sau đây có thể được kiểm thử nếu FAU_GEN tạo dữ liệu kiểm thử an toàn được bao gồm trong PP/ST:

a) Tối thiểu: Việc sử dụng cơ chế xác minh sinh trắc học không thành công;

b) Cơ bản: Tất cả việc sử dụng cơ chế xác minh sinh trắc học;

c) Chi tiết: Xác định các thay đổi đối với dữ liệu TSF, bao gồm, ví dụ, giá trị ngưỡng cho điểm so sánh sinh trắc học được sử dụng trong xác minh sinh trắc học.

8.3.8 Kiểm thử của FIA_BVR.2

Các hành động sau đây có thể được kiểm thử nếu FAU_GEN tạo dữ liệu kiểm thử an toàn được bao gồm trong PP/ST:

a) Tối thiểu: Sử dụng không thành công cơ chế xác thực người dùng với xác minh sinh trắc học;

b) Cơ bản: Tất cả việc sử dụng cơ chế xác thực người dùng với xác minh sinh trắc học;

c) Chi tiết: Xác định các thay đổi đối với dữ liệu TSF, bao gồm, ví dụ: giá trị ngưỡng cho điểm so sánh sinh trắc học được sử dụng trong xác minh sinh trắc học và tất cả các hành động của người dùng được được thực hiện bởi TSF làm trung gian trước khi xác thực với xác minh sinh trắc học của người dùng.

8.3.9 Kiểm thử của FIA_BVR.3

Các hành động sau đây có thể được kiểm thử nếu FAU_GEN tạo dữ liệu kiểm thử an toàn được bao gồm trong PP/ST:

a) Tối thiểu: Sử dụng không thành công cơ chế xác thực người dùng với xác minh sinh trắc học;

b) Cơ bản: Tất cả việc sử dụng cơ chế xác thực người dùng với xác minh sinh trắc học.

c) Chi tiết: Xác định các thay đổi đối với dữ liệu TSF, bao gồm, ví dụ: giá trị ngưỡng cho điểm so sánh sinh trắc học được sử dụng trong xác minh sinh trắc học.

8.3.10 Kiểm thử của FIA_BVR.4

Các hành động sau đây có thể được kiểm thử nếu FAU_GEN tạo dữ liệu kiểm thử an toàn được bao gồm trong PP/ST:

a) Tối thiểu: Từ chối bởi TSF của dữ liệu được kiểm tra có chất lượng thấp hoặc được phát hiện là công cụ tấn công trình diện;

b) Cơ bản: Từ chối hoặc chấp nhận bởi TSF của dữ liệu được kiểm tra có chất lượng bình thường hoặc đầu vào cho hệ thống con phát hiện tấn công trình diện;

c) Chi tiết: Xác định các thay đổi đối với dữ liệu TSF, bao gồm, ví dụ: các giá trị ngưỡng cho điểm chất lượng và phát hiện các công cụ tấn công trình diện.

8.3.11 FIA_BVR.1 Xác minh sinh trắc học với hiệu suất cao

Phân cấp thành: Không có thành phần nào khác.

Phụ thuộc: FIA_EBR.1 Kiểm tra các mẫu sinh trắc học để đăng ký

FIA_EBR.2 Đăng ký sinh trắc học với tỷ lệ không đăng ký được thấp.

FIA_BVR.1.1

TSF sẽ cung cấp cơ chế xác minh sinh trắc học cho [gắn với: đặc trưng sinh trắc] tới người dùng với [lựa chọn: FMR, FAR] không vượt quá [gắn với: giá trị xác định] và [lựa chọn: FNMR, FRR] không vượt quá [gắn với: giá trị xác định].

CHÚ THÍCH: Trong TCVN 8709-2, FIA_BVR.1.1 sẽ được đánh số là 8.3.11.1.

8.3.12 FIA_BVR.2 Thời gian xác thực người dùng với xác minh sinh trắc học

Phân cấp thành: FIA_BVR.1 Xác minh sinh trắc học với độ chính xác cao

Phụ thuộc: FIA_UID.1 Xác định thời gian

FIA_EBR.1 Kiểm tra các mẫu sinh trắc học để đăng ký

FIA_EBR.2 Đăng ký sinh trắc học với tỷ lệ không đăng ký được thấp.

FIA_BVR.2.1

TSF sẽ cho phép thực hiện [gắn với: danh sách các hành động do TSF làm trung gian] thay cho người dùng trước khi người dùng được xác thực bằng xác minh sinh trắc học dựa trên [gắn với: đặc trưng sinh trắc học].

FIA_BVR.2.2

TSF sẽ cung cấp cơ chế xác thực người dùng với xác minh sinh trắc học dựa trên [gắn với: đặc trưng sinh trắc học] cho người dùng với [lựa chọn: FMR, FAR] không vượt quá [gắn với: giá trị xác định] và [lựa chọn: FNMR, FRR] không vượt quá [gắn với: giá trị được xác định] để yêu cầu từng người dùng phải được xác thực thành công trước khi cho phép bất kỳ hành động nào khác do TSF làm trung gian thay cho người dùng đó.

CHÚ THÍCH: Trong TCVN 8709-2, FIA_BVR.2.1 và FIA_BVR.2.2 sẽ được đánh số tương ứng là 8.3.12.1 và 8.3.12.2.

8.3.13 FIA_BVR.3 Xác thực người dùng với xác minh sinh trắc học trước bất kỳ hành động nào

Phân cấp thành: FIA_BVR.2 thời gian xác thực người dùng với xác minh sinh trắc học

Phụ thuộc: FIA_UID.1 Xác định thời gian

FIA_EBR.1 Kiểm tra các mẫu sinh trắc học để đăng ký

FIA_EBR.2 Đăng ký sinh trắc học với tỷ lệ không đăng ký được thấp.

FIA_BVR.3.1

TSF sẽ cung cấp cơ chế xác thực người dùng với xác minh sinh trắc học dựa trên [gắn với: đặc trưng sinh trắc học] cho người dùng với [lựa chọn: FMR, FAR] không vượt quá [ấn định: giá trị xác định] và [lựa chọn: FNMR, FRR] không vượt quá [gắn với: giá trị được xác định] để yêu cầu từng người dùng được xác thực thành công trước khi cho phép bất kỳ hành động nào khác do TSF làm trung gian thay cho người dùng đó

CHÚ THÍCH: Trong TCVN 8709-2, FIA_BVR.3.1 sẽ được đánh số là 8.3.13.1.

8.3.14 FIA_BVR.4 Xác minh sinh trắc học không chấp nhận các công cụ tấn công trình diện

Phân cấp thành: Không có thành phần nào khác.

Phụ thuộc: FIA_UID.1 Xác định thời gian

FIA_EBR.1 Kiểm tra các mẫu sinh trắc học để đăng ký

FIA_BVR.4.1

TSF sẽ ngăn việc sử dụng các công cụ tấn công trình diện không công cụ nhân tạo để xác minh thành công [gắn với: đặc trưng sinh trắc học].

FIA_BVR.4.2

TSF sẽ ngăn chặn việc sử dụng các công cụ tấn công trình diện nhân tạo để xác minh thành công [gắn với: đặc trưng sinh trắc học].

CHÚ THÍCH: Trong TCVN 8709-2, FIA_BVR.4.1 và FIA_BVR.4.2 sẽ được đánh số tương ứng là 8.3.14.1 và 8.3.14.2.

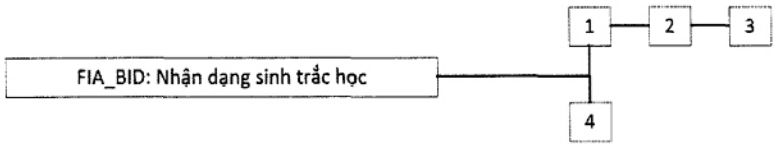
8.4. Định danh sinh trắc học (FIA_BID)

8.4.1 Họ hành vi

Họ này xác định các cơ chế định danh sinh trắc học được TSF hỗ trợ. Họ này cũng xác định các thuộc tính bắt buộc mà các cơ chế định danh sinh trắc học sẽ dựa trên đó.

8.4.2 Thành phần nền

Hình 9 cho thấy cấu trúc của họ này.



Hình 9 - Định danh sinh trắc học FIA_BID

FIA_BID.1 Định danh sinh trắc học với hiệu suất cao, yêu cầu TSF giới hạn FPIR và FNIR tương ứng trong một tỷ lệ quy định.

FIA_BID.2 Thời gian định danh sinh trắc học, cho phép người dùng thực hiện các hành động nhất định trước khi định danh sinh trắc học.

FIA_BID.3 Định danh sinh trắc học trước bất kỳ hành động nào, yêu cầu người dùng phải định danh sinh trắc học trước khi TSF cho phép bất kỳ hành động nào khác.

FIA_BID.4 Định danh sinh trắc học không chấp nhận công cụ tấn công trình diện, yêu cầu cơ chế định danh sinh trắc học để có thể ngăn chặn việc sử dụng thành công công cụ tấn công trình diện trong nỗ lực định danh sinh trắc học.

8.4.3 Quản lý của FIA_BID.1

Hành động sau đây có thể được xem xét đối với các chức năng quản lý trong FMT: quản lý dữ liệu TSF (bao gồm các giá trị ngưỡng) của quản trị viên.

8.4.4 Quản lý của FIA_BID.2

Các hành động sau đây có thể được xem xét đối với các chức năng quản lý trong FMT:

a) Quản trị viên quản lý dữ liệu TSF (bao gồm các giá trị ngưỡng);

b) Quản lý danh sách các hành động có thể được thực hiện trước khi người dùng được định danh sinh trắc học.

8.4.5 Quản lý của FIA_BID.3

Hành động sau đây có thể được xem xét đối với các chức năng quản lý trong FMT: quản lý dữ liệu TSF (bao gồm các giá trị ngưỡng) của quản trị viên.

8.4.6 Quản lý của FIA_BID.4

Hành động sau đây có thể được xem xét đối với các chức năng quản lý trong FMT: quản lý dữ liệu TSF, bao gồm, ví dụ: các giá trị của quản trị viên để phát hiện các công cụ tấn công trình diện và để kiểm tra chất lượng để tạo ra các mẫu sinh trắc học.

CHÚ THÍCH Người quản trị là người quản lý hệ thống sinh trắc học.

8.4.7 Kiểm thử của FIA_BID.1

Các hành động sau đây sẽ có thể được kiểm tra nếu việc tạo dữ liệu kiểm tra an toàn FAU_GEN được bao gồm trong PP/ST:

a) Tối thiểu: Sử dụng không thành công cơ chế định danh sinh trắc học;

b) Cơ bản: Tất cả việc sử dụng cơ chế định danh sinh trắc học;

c) Chi tiết: Xác định các thay đổi đối với dữ liệu TSF, bao gồm, ví dụ: giá trị ngưỡng cho điểm so sánh sinh trắc học được sử dụng trong định danh sinh trắc học.

8.4.8 Kiểm thử của FIA_BID.2

Các hành động sau đây sẽ có thể được kiểm tra nếu việc tạo dữ liệu kiểm tra an toàn FAU_GEN được bao gồm trong PP / ST:

a) Tối thiểu: Sử dụng không thành công cơ chế định danh sinh trắc học;

b) Cơ bản: Tất cả việc sử dụng cơ chế định danh sinh trắc học;

c) Chi tiết: Xác định các thay đổi đối với dữ liệu TSF, bao gồm, ví dụ: giá trị ngưỡng cho điểm so sánh sinh trắc học được sử dụng trong định danh sinh trắc học và tất cả các hành động của người dùng qua trung gian TSF được thực hiện trước khi nhận định danh trắc học của người dùng.

8.4.9 Kiểm thử của FIA_BID.3

Các hành động sau đây sẽ có thể được kiểm tra nếu việc tạo dữ liệu kiểm tra an toàn FAU_GEN được bao gồm trong PP/ST:

a) Tối thiểu: Sử dụng không thành công cơ chế định danh sinh trắc học;

b) Cơ bản: Tất cả việc sử dụng cơ chế định danh sinh trắc học;

c) Chi tiết: Xác định các thay đổi đối với dữ liệu TSF, bao gồm, ví dụ: giá trị ngưỡng cho điểm so sánh sinh trắc học được sử dụng trong định danh sinh trắc học.

8.4.10 Kiểm thử của FIA_BID.4

Các hành động sau đây có thể được kiểm thử nếu FAU_GEN tạo dữ liệu kiểm thử an toàn được bao gồm trong PP/ST:

a) Tối thiểu: Từ chối bởi TSF của dữ liệu được kiểm tra có chất lượng thấp hoặc được phát hiện là công cụ tấn công trình diện;

b) Cơ bản: Từ chối hoặc chấp nhận bởi TSF của dữ liệu được kiểm tra có chất lượng bình thường hoặc đầu vào cho hệ thống con phát hiện tấn công trình diện;

c) Chi tiết: Xác định các thay đổi đối với dữ liệu TSF, bao gồm, ví dụ: các giá trị ngưỡng cho điểm chất lượng và phát hiện các công cụ tấn công trình diện.

8.4.11 FIA_BID.1 Định danh sinh trắc học với hiệu suất cao

Phân cấp thành: Không có thành phần nào khác.

Phụ thuộc: FIA_EBR.1 Kiểm tra các mẫu sinh trắc học để đăng ký

FIA_EBR.2 Đăng ký sinh trắc học với tỷ lệ không đăng ký được thấp

FIA_BID.1.1

TSF sẽ cung cấp cơ chế định danh sinh trắc học dựa trên [gắn với: đặc trưng sinh trắc học] cho người dùng với FPIR không vượt quá [gắn với: giá trị xác định] và FNIR không vượt quá [gắn với: giá trị xác định].

CHÚ THÍCH: Trong TCVN 8709-2, FIA_BID.1.1 sẽ được đánh số là 8.4.11.1.

8.4.12 FIA_BID.2 Thời gian định danh sinh trắc học

Phân cấp thành: FIA_BID.1 SSịnh danh sinh trắc học với hiệu suất cao

Phụ thuộc: FIA_EBR.1 Kiểm tra các mẫu sinh trắc học để đăng ký

FIA_EBR.2 Đăng ký sinh trắc học với tỷ lệ không đăng ký được thấp.

FIA_BID.2.1

TSF sẽ cho phép người dùng thực hiện [gắn với: danh sách các hành động do TSF làm trung gian] trước khi người dùng được định danh sinh trắc học dựa trên [gắn với: đặc trưng sinh trắc học].

FIA_BID.2.2

TSF sẽ cung cấp cơ chế định danh sinh trắc học dựa trên [gắn với: đặc trưng sinh trắc học] cho người dùng với FPIR không vượt quá [gắn với: giá trị xác định] và FNIR không vượt quá [gắn với: giá trị xác định] để yêu cầu mỗi người dùng được định danh sinh trắc học trước khi cho phép bất kỳ hành động nào khác do TSF làm trung gian thay cho người dùng đó.

CHÚ THÍCH: Trong TCVN 8709-2, FIA_BID.2.1 và FIA_BID.2.2 sẽ được đánh số tương ứng là 8.4.12.1 và 8.4.12.2.

8.4.13 FIA_BID.3 Định danh sinh trắc học trước bất kỳ hành động nào

Phân cấp thành: FIA_BID.2 thời gian xác thực người dùng với định danh sinh trắc học

Phụ thuộc: FIA_EBR.1 Kiểm tra các mẫu sinh trắc học để đăng ký

FIA_EBR.2 Đăng ký sinh trắc học với tỷ lệ không đăng ký được thấp.

FIA_BID.3.1

TSF sẽ cung cấp cơ chế nhận định danh trắc học dựa trên [gắn với: đặc trưng sinh trắc học] cho người dùng với FPIR không vượt quá [gắn với: giá trị xác định] và FNIR không vượt quá [gắn với: giá trị xác định] để yêu cầu mỗi người dùng được định danh sinh trắc học trước khi cho phép bất kỳ hành động nào khác do TSF làm trung gian thay cho người dùng đó.

CHÚ THÍCH: Trong TCVN 8709-2, FIA_BID.3.1 sẽ được đánh số là 8.4.13.1.

8.3.14 FIA_BID.4 Định danh sinh trắc học không chấp nhận các công cụ tấn công trình diện

Phân cấp thành: Không có thành phần nào khác.

Phụ thuộc: FIA_EBR.1 Kiểm tra các mẫu sinh trắc học để đăng ký

FIA_BID.4.1

TSF sẽ ngăn chặn việc sử dụng các công cụ tấn công trình diện không phải công cụ nhân tạo để [gắn với: đặc trưng sinh trắc học] được xác định thành công.

FIA_BID.4.2

TSF sẽ ngăn chặn việc sử dụng các công cụ tấn công trình diện nhân tạo để [gắn với: đặc trưng sinh trắc học] được xác định thành công.

CHÚ THÍCH: Trong TCVN 8709-2, FIA_BID.4.1 và FIA_BID.4.2 sẽ được đánh số tương ứng là 8.4.14.1 và 8.4.14.2.

9. Các hoạt động bổ sung cho TCVN 11386 về Lớp APE: Đánh giá Hồ sơ bảo vệ

Bảng 1 liệt kê các hoạt động bổ sung cho các đơn vị công việc trong APE_INT sẽ chỉ được áp dụng cho đánh giá an toàn của PAD (xem thêm D.1.1). Không có hoạt động bổ sung nào khác trong Lớp APE.

Bảng 1 - Bổ sung cho APE_INT (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
APE_INT.1.1E	APE_INT.1-1	Không
	APE_INT.1-2	Không
	APE_INT.1-3	Kiểm thử viên ***phải kiểm tra*** tổng quan TOE để xác định rằng TOE cung cấp cơ chế phát hiện tấn công trình diện.
	APE_INT.1-4	Kiểm thử viên ***phải kiểm tra*** tổng quan TOE để xác định rằng không có yêu cầu về tỷ lệ lỗi cho cơ chế phát hiện tấn công trình diện.
	APE_INT.1-5	Không

CHÚ THÍCH: Nó cũng áp dụng cho các TOE không yêu cầu khả năng chống PAD, để kiểm tra xem Kiểm thử viên có cần tính đến tính năng này trong quá trình AVA để thực hiện định danh sinh trắc học hay không.

10. Các hoạt động bổ sung cho TCVN 11386 về Lớp ASE: Đánh giá đích an toàn

Bảng 2 và Bảng 3 liệt kê các hoạt động bổ sung cho các đơn vị công việc trong ASE_INT (xem thêm D.1.1). Không có hoạt động bổ sung nào khác trong Lớp ASE.

Bảng 2 - Bổ sung cho ASE_INT (áp dụng cho hiệu suất nhận dạng sinh trắc học)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ASE_INT.1.1E	ASE_INT.1-1	Không
	ASE_INT.1-2	Không
	ASE_INT.1-3	Không
	ASE_INT.1-4	Kiểm thử viên ***phải kiểm tra*** tham chiếu TOE để xác định rằng xác

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
		định rõ ràng phương thức mà TOE có thể được sử dụng.
	ASE_INT.1-5	Không
	ASE_INT.1-6	Không
	ASE_INT.1-7	Không
	ASE_INT.1-8	Không
	ASE_INT.1-9	Không
	ASE_INT.1-10	Không

Bảng 3 - Bổ sung cho ASE_INT (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ASE_INT.1.1E	ASE_INT.1-1	Không
	ASE_INT.1-2	Không
	ASE_INT.1-3	Không
	ASE_INT.1-4	Kiểm thử viên ***phải kiểm tra*** tham chiếu TOE để xác định rằng xác định rõ ràng phương thức mà TOE có thể được sử dụng.
	ASE_INT.1-5	Kiểm thử viên ***phải kiểm tra*** tổng quan TOE để xác định rằng TOE cung cấp cơ chế phát hiện tấn công trình diện.
	ASE_INT.1-6	Không
	ASE_INT.1-7	Kiểm thử viên ***phải kiểm tra*** tổng quan TOE để xác định rằng nó không yêu cầu tỷ lệ lỗi cho cơ chế phát hiện tấn công trình diện.
	ASE_INT.1-8	Không
	ASE_INT.1-9	Không
	ASE_INT.1-10	Không

11. Các hoạt động bổ sung cho TCVN 11386 về Lớp ADV: Phát triển

11.1 Các hoạt động bổ sung cho cấu trúc an toàn ADV_ARC

Bảng 4 liệt kê các hoạt động bổ sung được bổ sung cho các đơn vị công việc trong hành động hoạt động con ADV_ARC1.1E sẽ chỉ được áp dụng cho việc đánh giá an toàn của PAD. ADV_ARC.1-5 được áp dụng cho TOE cung cấp nhận dạng sinh trắc học cũng như PAD (xem thêm D.2.1).

Bảng 4 - Bổ sung cho ADV_ARC (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ADV_ARC.1.1E	ADV_ARC.1-1	Không
	ADV_ARC.1-2	Không
	ADV_ARC.1-3	Không
	ADV_ARC.1-4	Không
	ADV_ARC.1-5	Kiểm thử viên ***phải kiểm tra*** tài liệu cấu trúc an toàn liên quan đến các cơ chế đảm bảo rằng thiết bị thu thập và PAD đang được trình diện cùng (các) đặc trưng sinh trắc học.

11.2 Các hoạt động bổ sung cho đặc tả chức năng ADV_FSP

11.2.1 Các hoạt động bổ sung để đánh giá hoạt động con ADV_FSP.1

Không có hoạt động bổ sung nào để đánh giá hoạt động con ADV_FSP.1.

11.2.2 Các hoạt động bổ sung để đánh giá hoạt động con ADV_FSP.2

Bảng 5 và Bảng 6 liệt kê các hoạt động bổ sung được bổ sung cho các đơn vị công việc trong hoạt động con ADV_FSP.2.1E (Xem thêm D.2.2). Không có hoạt động bổ sung nào khác được bổ sung cho hành động đánh giá hoạt động con ADV_FSP.2.2E.

Bảng 5 - Bổ sung cho ADV_FSP.2.1E (áp dụng cho hiệu suất nhận định danh sinh trắc học)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ADV_FSP.2.1E	ADV_FSP.2-1	Không
	ADV_FSP.2-2	Không
	ADV_FSP.2-3	Kiểm thử viên ***phải kiểm tra*** đặc tả chức năng để xác định phương thức các thiết bị thu thập được sử dụng khi các đặc trưng sinh trắc học được trình diện là một phần của TOE.
	ADV_FSP.2-4	Kiểm thử viên ***phải kiểm tra*** trình diện của TSFI để xác định rằng nó hoàn toàn khớp với các thông số liên quan đến an toàn cho các thiết bị thu thập.
	ADV_FSP.2-5	Kiểm thử viên ***phải kiểm tra*** trình diện của TSFI để xác định rằng nó mô tả đầy đủ và chính xác các thông số liên quan đến an toàn liên quan đến TSFI cho các thiết bị chụp.

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
	ADV_FSP.2-6	Không
	ADV_FSP.2-7	Không
	ADV_FSP.2-8	Không

Bảng 6 - Bổ sung cho ADV_FSP.2.1E (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ADV_FSP.2.1E	ADV_FSP.2-1	Kiểm thử viên phải kiểm tra đặc tả chức năng để xác định rằng các cơ chế khác nhau được sử dụng để phát hiện tấn công trình diện được mô tả dưới dạng TSFIs.
	ADV_FSP.2-2	Không
	ADV_FSP.2-3	Kiểm thử viên ***phải kiểm tra*** đặc tả chức năng để xác định phương thức các thiết bị thu thập được sử dụng khi các đặc trưng sinh trắc học được trình diện là một phần của TOE.
	ADV_FSP.2-4	Kiểm thử viên ***phải kiểm tra*** trình diện của TSFI để xác định rằng nó hoàn toàn khớp với các thông số liên quan đến an toàn cho các thiết bị thu thập.
	ADV_FSP.2-5	Kiểm thử viên ***phải kiểm tra*** trình diện của TSFI để xác định rằng nó mô tả đầy đủ và chính xác các thông số về mặt an toàn liên quan đến TSFI cho các thiết bị thu thập.
	ADV_FSP.2-6	Không
	ADV_FSP.2-7	Kiểm thử viên ***phải kiểm tra*** trình diện TSFI để xác định rằng không có phản hồi nào về xác định được phát hiện tấn công trình diện cho người dùng nếu như TOE bao gồm nhiều hơn là hệ thống con PAD.
	ADV_FSP.2-8	Không

11.2.3 Các hoạt động bổ sung cho Đánh giá hoạt động con ADV_FSP.3

Bảng 7 và Bảng 8 liệt kê các hoạt động bổ sung được bổ sung cho các đơn vị công việc trong hoạt động con ADV_FSP.3.1E (xem thêm D.2.2). Không có hoạt động bổ sung nào khác được bổ sung cho việc đánh giá hành động của hoạt động con ADV_FSP.3.2E.

Bảng 7 - Bổ sung cho ADV_FSP.3.1E (áp dụng cho hiệu suất nhận dạng sinh trắc học)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ADV_FSP.3.1E	ADV_FSP.3-1	Không
	ADV_FSP.3-2	Không

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
	ADV_FSP.3-3	Kiểm thử viên ***phải kiểm tra*** đặc tả chức năng để xác định phương thức các thiết bị thu thập được sử dụng khi các đặc trưng sinh trắc học được trình diện là một phần của TOE.
	ADV_FSP.3-4	Kiểm thử viên ***phải kiểm tra*** trình diện của TSFI để xác định rằng nó hoàn toàn khớp với các thông số liên quan đến an toàn cho các thiết bị thu thập.
	ADV_FSP.3-5	Kiểm thử viên ***phải kiểm tra*** trình diện của TSFI để xác định rằng nó mô tả đầy đủ và chính xác các thông số về mặt an toàn liên quan đến TSFI cho các thiết bị thu thập.
	ADV_FSP.3-6	Không
	ADV_FSP.3-7	Không
	ADV_FSP.3-8	Không
	ADV_FSP.3-9	Không

Bảng 8 - Bổ sung cho ADV_FSP.3.1E (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ADV_FSP.3.1E	ADV_FSP.3-1	Kiểm thử viên ***phải kiểm tra*** đặc điểm kỹ thuật chức năng để xác định rằng các cơ chế khác nhau được sử dụng để phát hiện tấn công trình diện được mô tả dưới dạng các TSFI.
	ADV_FSP.3-2	Không
	ADV_FSP.3-3	Kiểm thử viên ***phải kiểm tra*** đặc tả chức năng để xác định phương thức các thiết bị thu thập được sử dụng khi các đặc trưng sinh trắc học được trình diện là một phần của TOE.
	ADV_FSP.3-4	Kiểm thử viên ***phải kiểm tra*** trình diện của TSFI để xác định rằng nó hoàn toàn khớp với các thông số liên quan đến an toàn cho các thiết bị thu thập.
	ADV_FSP.3-5	Kiểm thử viên ***phải kiểm tra*** trình diện của TSFI để xác định rằng nó mô tả đầy đủ và chính xác các thông số về mặt an toàn liên quan đến TSFI cho các thiết bị thu thập.
	ADV_FSP.3-6	Không
	ADV_FSP.3-7	Kiểm thử viên ***phải kiểm tra*** trình diện TSFI để xác định rằng không có phản hồi nào về xác định được phát hiện tấn công trình diện cho người dùng nếu như TOE bao gồm nhiều hơn là hệ thống con PAD.
	ADV_FSP.3-8	Không
	ADV_FSP.3-9	Không

11.2.4 Các hoạt động bổ sung cho Đánh giá hoạt động con ADV_FSP.4

Bảng 9 và Bảng 10 liệt kê các hoạt động bổ sung được bổ sung cho các đơn vị công việc trong hoạt động con ADV_FSP.4.1E (xem thêm D.2.2). Không có hoạt động bổ sung nào khác được bổ sung cho việc đánh giá hoạt động con ADV_FSP.4.2E.

Bảng 9 - Bổ sung cho ADV_FSP.4.1E (áp dụng cho hiệu suất nhận dạng sinh trắc học)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ADV_FSP.4.1E	ADV_FSP.4-1	Không
	ADV_FSP.4-2	Không
	ADV_FSP.4-3	Kiểm thử viên ***phải kiểm tra*** đặc tả chức năng để xác định phương thức các thiết bị thu thập được sử dụng khi các đặc trưng sinh trắc học được trình diện là một phần của TOE.
	ADV_FSP.4-4	Không
	ADV_FSP.4-5	Không
	ADV_FSP.4-6	Kiểm thử viên ***phải kiểm tra*** trình diện của TSFI để xác định rằng nó mô tả đầy đủ và chính xác các thông số về mặt an toàn liên quan đến TSFI cho các thiết bị thu thập.
	ADV_FSP.4-7	Không
	ADV_FSP.4-8	Không
	ADV_FSP.4-9	Không
	ADV_FSP.4-10	Không

Bảng 10 - Bổ sung cho ADV_FSP.4.1E (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ADV_FSP.4.1E	ADV_FSP.4-1	Kiểm thử viên ***phải kiểm tra*** đặc điểm kỹ thuật chức năng để xác định rằng các cơ chế khác nhau được sử dụng để phát hiện tấn công trình diện được mô tả dưới dạng các TSFI.
	ADV_FSP.4-2	Không
	ADV_FSP.4-3	Kiểm thử viên ***phải kiểm tra*** đặc tả chức năng để xác định phương thức các thiết bị thu thập được sử dụng khi các đặc trưng sinh trắc học được trình diện là một phần của TOE.
	ADV_FSP.4-4	Không
	ADV_FSP.4-5	Không
	ADV_FSP.4-6	Kiểm thử viên ***phải kiểm tra*** trình diện của TSFI để xác định rằng nó mô tả đầy đủ và chính xác các thông số về mặt an toàn liên quan đến TSFI cho các thiết bị thu thập.
	ADV_FSP.4-7	Không

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
	ADV_FSP.4-8	Kiểm thử viên ***phải kiểm tra*** trình diện TSFI để xác định rằng không có phản hồi nào về xác định được phát hiện tấn công trình diện cho người dùng nếu như TOE bao gồm nhiều hơn là hệ thống con PAD.
	ADV_FSP.4-9	Không
	ADV_FSP.4-10	Không

11.3 Các hoạt động bổ sung cho thiết kế TOE ADV_TDS

11.3.1 Các hoạt động bổ sung để đánh giá hoạt động con ADV_TDS.1

Bảng 11 liệt kê các hoạt động bổ sung được bổ sung cho các đơn vị công việc trong hoạt động con ADV_TDS.1.1E sẽ chỉ được áp dụng cho việc đánh giá an toàn của PAD (xem thêm D.2.4). Không có hoạt động bổ sung nào khác được bổ sung cho việc đánh giá hoạt động con ADV_TDS.1.2E.

Bảng 11 - Bổ sung cho ADV_TDS.1.1E (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ADV_TDS.1.1E	ADV_TDS.1-1	Không
	ADV_TDS.1-2	Không
	ADV_TDS.1-3	Không
	ADV_TDS.1-4	Kiểm thử viên ***phải kiểm tra*** thiết kế của TOE để xác định rằng trong đó có mô tả về các thuộc tính và cơ chế sinh trắc học được sử dụng để phát hiện các tấn công trình diện được mô tả ở cấp hệ thống con, nghĩa là, việc xử lý các tín hiệu thu được bởi các thiết bị thu thập được sử dụng để phát hiện tấn công trình diện và sự chuyển đổi của các tín hiệu này trong việc phân loại tấn công trình diện.
	ADV_TDS.1-5	Kiểm thử viên ***phải kiểm tra*** thiết kế của TOE để xác định rằng các tương tác giữa cơ chế phát hiện tấn công trình diện và chức năng thu thập được mô tả ở cấp hệ thống con.
	ADV_TDS.1-6	Không

11.3.2 Các hoạt động bổ sung để đánh giá hoạt động con ADV_TDS.2

Bảng 12 liệt kê các hoạt động bổ sung được bổ sung cho các đơn vị công việc trong hoạt động con ADV_TDS.2.1E sẽ chỉ được áp dụng cho đánh giá an toàn của PAD (xem thêm D.2.4). Không có hoạt động bổ sung nào khác được bổ sung cho việc đánh giá hoạt động con ADV_TDS.2.2E.

Bảng 12 - Bổ sung cho ADV_TDS.2.1E (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ADV_TDS.2.1E	ADV_TDS.2-1	Không
	ADV_TDS.2-2	Không
	ADV_TDS.2-3	Không
	ADV_TDS.2-4	Kiểm thử viên ***phải kiểm tra*** thiết kế của TOE để xác định rằng trong đó có mô tả về các thuộc tính và cơ chế sinh trắc học được sử dụng để phát hiện các tấn công trình diện được mô tả ở cấp hệ thống con, nghĩa là, việc xử lý các tín hiệu thu được bởi các thiết bị thu thập được sử dụng để phát hiện tấn công trình diện và sự chuyển đổi của các tín hiệu này trong việc phân loại tấn công trình diện.
	ADV_TDS.2-5	Không
	ADV_TDS.2-6	Không
	ADV_TDS.2-7	Kiểm thử viên ***phải kiểm tra*** thiết kế TOE để xác định rằng các tương tác giữa cơ chế phát hiện tấn công trình diện và chức năng thu thập được mô tả ở mức hệ thống con.
	ADV_TDS.2-8	Không

11.3.3 Các hoạt động bổ sung để đánh giá hoạt động con ADV_TDS.3

Bảng 13 liệt kê các hoạt động bổ sung được bổ sung cho các đơn vị công việc trong hành động hoạt động con ADV_TDS.3.1E sẽ chỉ được áp dụng cho đánh giá an toàn của PAD (xem thêm D.2.4). Không có hoạt động bổ sung nào khác được bổ sung cho việc đánh giá hoạt động con ADV_TDS.3.2E.

Bảng 13 - Bổ sung cho ADV_TDS.3.1E (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ADV_TDS.3.1E	ADV_TDS.3-1	Không
	ADV_TDS.3-2	Không
	ADV_TDS.3-3	Không
	ADV_TDS.3-4	Kiểm thử viên **phải kiểm tra** thiết kế của TOE để xác định rằng trong đó có mô tả về các thuộc tính và cơ chế sinh trắc học được sử dụng để phát hiện các tấn công trình diện ở cấp độ mô-đun, nghĩa là, việc xử lý các tín hiệu thu được bởi các thiết bị thu thập được sử dụng để phát hiện tấn công trình diện và sự chuyển đổi của các tín hiệu này trong việc phân loại tấn công trình diện.
	ADV_TDS.3-5	Không
	ADV_TDS.3-6	Kiểm thử viên ***phải kiểm tra*** thiết kế của TOE để xác định rằng các tương tác giữa cơ chế phát hiện tấn công trình diện và chức

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
		năng thu thập được mô tả ở cấp mô-đun.
	ADV_TDS.3-7	Không
	ADV_TDS.3-8	Không
	ADV_TDS.3-9	Không
	ADV_TDS.3-10	Không
	ADV_TDS.3-11	Không
	ADV_TDS.3-12	Không
	ADV_TDS.3-13	Không
	ADV_TDS.3-14	Không

12. Các hoạt động bổ sung cho TCVN 11386 về Lớp AGD: Tài liệu hướng dẫn

12.1 Các hoạt động bổ sung cho hướng dẫn sử dụng vận hành AGD_OPE

Bảng 14 và Bảng 15 liệt kê các hoạt động bổ sung được bổ sung cho các đơn vị công việc trong hoạt động con AGD_OPE.1.1E (xem thêm D.3.1). Không có hoạt động bổ sung nào khác được bổ sung cho đánh giá hoạt động con AGD_OPE.1.2E.

Bảng 14 - Bổ sung cho AGD_OPE.1.1E (áp dụng cho hiệu suất nhận dạng sinh trắc học)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
AGD_OPE.1.1E	AGD_OPE.1-1	Không
	AGD_OPE.1-2	Kiểm thử viên ***phải kiểm tra*** hướng dẫn vận hành cho người dùng để xác định trong đó có mô tả quá trình trình diện các đặc trưng sinh trắc học trong TOE nếu các thiết bị thu thập là một phần của TOE.
	AGD_OPE.1-3	Kiểm thử viên ***phải kiểm tra*** hướng dẫn vận hành cho người dùng để xác định trong đó có mô tả cấu hình an toàn của các thông số để định nhận dạng trắc học.
	AGD_OPE.1-4	Không
	AGD_OPE.1-5	Không
	AGD_OPE.1-6	Không
	AGD_OPE.1-7	Không
	AGD_OPE.1-8	Không

Bảng 15 - Bổ sung cho AGD_OPE.1.1E (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
AGD_OPE.1.1E	AGD_OPE.1-1	Không
	AGD_OPE.1-2	Kiểm thử viên ***phải kiểm tra*** hướng dẫn vận hành cho người dùng để xác định trong đó có mô tả quá trình trình diện các đặc trưng sinh trắc học trong TOE nếu các thiết bị thu thập là một phần của TOE.
	AGD_OPE.1-3	Kiểm thử viên ***phải kiểm tra*** hướng dẫn vận hành cho người dùng để xác định trong đó có mô tả cấu hình an toàn của các tham số phát hiện tấn công trình diện.
	AGD_OPE.1-4	Kiểm thử viên ***phải kiểm tra*** hướng dẫn vận hành cho người dùng để xác định trong đó có mô tả các thủ tục thay thế cho phép người vận hành ghi đè quyết định của phát hiện tấn công trình diện hoặc của hệ thống con nhận dạng sinh trắc học theo cách thủ công.
	AGD_OPE.1-5	Kiểm thử viên ***phải kiểm tra*** hướng dẫn vận hành cho người dùng để xác định trong đó có mô tả phương thức hoạt động của TOE mà người vận hành có thể ghi đè quyết định phát hiện tấn công trình diện theo cách thủ công.
	AGD_OPE.1-6	Không
	AGD_OPE.1-7	Không
	AGD_OPE.1-8	Không

12.2 Các hoạt động bổ sung cho các quy trình chuẩn bị AGD_PRE

Bảng 16 và Bảng 17 liệt kê các hoạt động bổ sung được bổ sung cho các đơn vị công việc trong hoạt động con AGD_PRE.1.1E sẽ chỉ được áp dụng cho đánh giá an toàn của PAD (xem thêm D.3.2). Không có hoạt động bổ sung nào khác được bổ sung cho việc đánh giá hành động hoạt động con AGD_PRE.1.2E.

Bảng 16 - Bổ sung cho AGD_PRE.1.1E (áp dụng cho hiệu suất nhận dạng sinh trắc học)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
AGD_PRE.1.1E	AGD_PRE.1-1	Không
	AGD_PRE.1-2	Kiểm thử viên ***phải kiểm tra*** quy trình cài đặt được cung cấp để xác định rằng chúng mô tả cụ thể các tham số được sửa đổi đối với cơ chế an toàn của nhận dạng sinh trắc học (ví dụ: một ngưỡng) và sẽ được cấu hình trước khi sử dụng TOE ban đầu.

Bảng 17 - Bổ sung cho AGD_PRE.1.1E (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
AGD_PRE.1.1E	AGD_PRE.1-1	Không
	AGD_PRE.1-2	Kiểm thử viên ***phải kiểm tra*** quy trình cài đặt được cung cấp để xác định rằng trong đó có mô tả cụ thể các tham số được sửa đổi đối với cơ chế an toàn phát hiện tấn công trình diện (ví dụ: một ngưỡng) và sẽ được cấu hình trước khi sử dụng TOE ban đầu.

13 Các hoạt động bổ sung cho TCVN 11386 về Lớp ALC: Hỗ trợ vòng đời

13.1 Các hoạt động bổ sung cho CM hỗ trợ ALC_CMS

Không có hoạt động bổ sung nào được bổ sung để đánh giá các hoạt động con ALC_CMS.1, ALC_CMS.2, ALC_CMS.3 và ALC_CMS.5.

Bảng 18 liệt kê các hoạt động bổ sung được bổ sung cho các đơn vị công việc trong hoạt động con ALC_CMS.4.1E sẽ chỉ được áp dụng cho việc đánh giá an toàn của PAD (xem thêm D.4.1).

Bảng 18 - Bổ sung cho ALC_CMS.4.1E (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ALC_CMS.4.1E	ALC_CMS.4-1	Kiểm thử viên **phải kiểm tra** xem tài liệu được sử dụng để ghi lại chi tiết về các lỗi an toàn được báo cáo liên quan đến việc triển khai có bao gồm những lỗi mà hệ thống phát hiện tấn công trình diện trình diện không phát hiện ra PAI hay không.
	ALC_CMS.4-2	Không
	ALC_CMS.4-3	Không

13.2 Các hoạt động bổ sung cho Phân phối ALC_DEL

Bảng 19 liệt kê các hoạt động bổ sung được bổ sung cho các đơn vị công việc trong hoạt động con ALC_DEL.1.1E sẽ chỉ được áp dụng cho việc đánh giá an toàn của PAD (xem thêm D.4.2).

Bảng 19 - Bổ sung cho ALC_DEL.1.1E (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ALC_DEL.1.1E	ALC_DEL.1-1	Kiểm thử viên ***phải kiểm tra*** tài liệu phân phối để xác định trong đó có mô tả khả năng của TOE có sẵn sàng cho tất cả các loại khách hàng hay chỉ bị thu hẹp bởi những khách hàng đã mua.
	ALC_DEL.1-2	Không

13.3 Các hoạt động bổ sung để khắc phục sai sót ALC_FLR

Những điều sau đây sẽ được áp dụng cho tất cả các đơn vị công việc trong ALC_FLR.

Kiểm thử viên phải xác định rằng các PAI được chấp nhận lỗi bởi hệ thống phát hiện tấn công trình diện được coi là lỗi an toàn trong quy trình của nhà phát triển (xem thêm D.4.3).

14 Các hoạt động bổ sung cho TCVN 11386 về Lớp ATE: Các thử nghiệm

14.1 Các hoạt động bổ sung cho các thử nghiệm chức năng ATE_FUN

Bảng 20 và Bảng 21 liệt kê các hoạt động bổ sung được bổ sung cho các đơn vị công việc trong hoạt động con ATE_FUN.1.1E (xem thêm D.5.1).

Bảng 20 - Bổ sung ATE_FUN.1.1E (áp dụng cho hiệu suất nhận dạng sinh trắc học)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ATE_FUN.1.1E	ATE_FUN.1-1	Kiểm thử viên ***phải kiểm tra*** tài liệu thử nghiệm có đáp ứng các yêu cầu liên quan của ISO/IEC 19795. Kiểm thử viên ***phải giải thích*** về bất kỳ sự sai khác nào so với các quy trình thử nghiệm được quy định trong ISO/IEC 19795 và ***phải mô tả*** bất kỳ ảnh hưởng tiềm năng và tác động đến kết quả thử nghiệm trong tài liệu kiểm tra.
	ATE_FUN.1-2	Kiểm thử viên ***phải kiểm tra*** xem kế hoạch thử nghiệm có cung cấp thông tin về tập dữ liệu hoặc nhóm thử nghiệm được sử dụng cho các thử nghiệm của nhà phát triển về hiệu suất nhận dạng sinh trắc học hay không.
	ATE_FUN.1-3	Không
	ATE_FUN.1-4	Không
	ATE_FUN.1-5	Không
	ATE_FUN.1-6	Không
	ATE_FUN.1-7	Không

Bảng 21 - Bổ sung ATE_FUN.1.1E (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ATE_FUN.1.1E	ATE_FUN.1-1	Không
	ATE_FUN.1-2	Kiểm thử viên ***phải kiểm tra*** kế hoạch thử nghiệm để xác định trong đó có mô tả thông tin về kiểu tấn công được tạo bởi nhà phát triển cho các thử nghiệm bao gồm thông tin chi tiết về loại PAI, như là thông tin về vật liệu và hướng dẫn xây dựng, phương

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
		pháp tương tác với thiết bị thu thập, và có nhằm tới mục tiêu chống lại cuộc tấn công che giấu hay người mạo danh hay không.
	ATE_FUN.1-3	Kiểm thử viên ***phải kiểm tra*** kế hoạch thử nghiệm để xác định rằng các tham số phát hiện tấn công trình diện tiềm năng được cấu hình chính xác theo cấu hình TOE được mô tả trong ST.
	ATE_FUN.1-4	Không
	ATE_FUN.1-5	Kiểm thử viên ***phải kiểm tra*** tài liệu kiểm tra để xác định trong đó có bao gồm tất cả dự kiến về tỷ lệ lỗi trên các kết quả phát hiện tấn công trình diện.
	ATE_FUN.1-6	Kiểm thử viên ***phải xem xét*** xem các kết quả thử nghiệm thực tế về tỷ lệ lỗi trên phát hiện tấn công trình diện trong tài liệu thử nghiệm có phù hợp với kết quả được dự kiến trong tài liệu thử nghiệm hay không.
	ATE_FUN.1-7	Kiểm thử viên ***phải báo cáo*** những cố gắng của nhà phát triển về các thử nghiệm cơ chế phát hiện tấn công bao gồm về số lượng, mô tả về các kiểu tấn công, loại PAI và kích thước thử nghiệm.

Xem thêm TCVN 14190-3.

14.2 Các hoạt động bổ sung cho thử nghiệm độc lập ATE_IND

14.2.1 Tổng quát

Không có hoạt động bổ sung nào được bổ sung để đánh giá hoạt động con ATE_IND.3.

14.2.2 Các hoạt động bổ sung để đánh giá hoạt động con ATE_IND.1

Bảng 22 và Bảng 23 liệt kê các hoạt động bổ sung được bổ sung cho các đơn vị công việc trong ATE_IND.1 (xem thêm D.5.2).

Bảng 22 - Bổ sung cho ATE_IND.1 (áp dụng cho hiệu suất định dạng sinh trắc học)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ATE_IND.1.1E	ATE_IND.1-1	Không
	ATE_IND.1-2	Không
ATE_IND.1.2E	ATE_IND.1-3	Kiểm thử viên ***phải thiết lập*** thử nghiệm độc lập để đánh giá hiệu suất thiết lập của một nhóm thử nghiệm hoặc một bộ dữ liệu thử nghiệm.

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
	ATE_IND.1-4	Kiểm thử viên ***phải đưa ra*** tài liệu thử nghiệm để đánh giá khả năng đáp ứng các yêu cầu liên quan của ISO/IEC 19795. Kiểm thử viên ***phải giải thích*** về bất kỳ sự sai khác nào so với các quy trình thử nghiệm được quy định trong ISO/IEC 19795 và ***phải mô tả*** bất kỳ ảnh hưởng tiềm năng và tác động đến kết quả thử nghiệm trong tài liệu kiểm tra.
	ATE_IND.1-5	Kiểm thử viên ***phải tiến hành*** thử nghiệm bằng cách sử dụng nhóm thử nghiệm mà kiểm thử viên sắp xếp hoặc dữ liệu thử nghiệm mà kiểm thử viên sở hữu.
	ATE_IND.1-6	Kiểm thử viên ***phải ghi lại*** thông tin của nhóm thử nghiệm hoặc dữ liệu thử nghiệm như quy định trong ISO/IEC 19795.
	ATE_IND.1-7	Không
	ATE_IND.1-8	Kiểm thử viên ***phải báo cáo*** trong ETR nỗ lực kiểm tra của kiểm thử viên về hiệu suất nhận dạng sinh trắc học bao gồm kích thước thử nghiệm, thời gian sử dụng và cả các đặc điểm của tập dữ liệu.

Bảng 23 - Bổ sung ATE_IND.1 (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ATE_IND.1.1E	ATE_IND.1-1	Kiểm thử viên ***phải kiểm tra*** TOE để xác định rằng các tham số phát hiện tấn công trình diện tiềm năng được cấu hình chính xác theo cấu hình TOE được mô tả trong ST.
	ATE_IND.1-2	Không
ATE_IND.1.2E	ATE_IND.1-3	Kiểm thử viên ***phải thiết lập*** một tập hợp con thử nghiệm trong đó kiểm thử viên sử dụng hoặc xây dựng lại các PAI do nhà phát triển tạo ra theo cách khác với cách do nhà phát triển thực hiện, chẳng hạn như trình diện PAI theo một phương thức khác. Ngoài ra, kiểm thử viên ***phải thiết lập*** tập con thử nghiệm của riêng họ. Kiểm thử viên ***phải xem xét*** việc sửa đổi các PAI do nhà phát triển tạo để thử nghiệm. Nếu như TOE đó có cơ chế PAD có thể bị vô hiệu hóa để thử nghiệm, Kiểm thử viên ***phải xem xét*** việc vô hiệu hóa cơ chế PAD trong TOE để tinh chỉnh các PAI sao cho chúng có thể được chấp nhận lỗi bởi cơ chế xác minh sinh trắc học của TOE.
	ATE_IND.1-4	Không
	ATE_IND.1-5	Không
	ATE_IND.1-6	Kiểm thử viên ***phải ghi lại*** việc sửa đổi PAI và cách sử dụng.
	ATE_IND.1-7	Không

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
	ATE_IND.1-8	Kiểm thử viên ***phải báo cáo*** trong ETR nỗ lực kiểm tra của kiểm thử viên về cơ chế phát hiện tấn công trình diện về số lượng và mô tả các kiểu tấn công, loài PAI và kích thước thử nghiệm.

14.2.3 Các hoạt động bổ sung cho Đánh giá hoạt động con ATE_IND.2

Bảng 24 và Bảng 25 liệt kê các hoạt động bổ sung được bổ sung cho các đơn vị công việc trong ATE_IND.2 (xem thêm D.5.2).

Bảng 24 - Bổ sung ATE_IND.2 (áp dụng cho hiệu suất nhận dạng sinh trắc học)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ATE_IND.2.1E	ATE_IND.2-1	Không
	ATE_IND.2-2	Không
	ATE_IND.2-3	Không
ATE_IND.2.2E	ATE_IND.2-4	Không
	ATE_IND.2-5	Không
ATE_IND.2.3E	ATE_IND.2-6	Kiểm thử viên ***phải thiết lập*** thử nghiệm độc lập để đánh giá hiệu suất thiết lập của một nhóm thử nghiệm hoặc một bộ dữ liệu thử nghiệm.
	ATE_IND.2-7	Kiểm thử viên ***phải đưa ra*** tài liệu thử nghiệm để đánh giá khả năng đáp ứng các yêu cầu liên quan của ISO/IEC 19795. Kiểm thử viên ***phải giải thích*** về bất kỳ sự sai khác nào so với các quy trình thử nghiệm được quy định trong ISO/IEC 19795 và ***phải mô tả*** bất kỳ ảnh hưởng tiềm năng và tác động đến kết quả thử nghiệm trong tài liệu kiểm tra.
	ATE_IND.2-8	Kiểm thử viên ***phải tiến hành*** thử nghiệm bằng cách sử dụng nhóm thử nghiệm mà kiểm thử viên sắp xếp hoặc dữ liệu thử nghiệm mà kiểm thử viên sở hữu.
	ATE_IND.2-9	Kiểm thử viên ***phải ghi lại*** thông tin của nhóm thử nghiệm hoặc dữ liệu thử nghiệm như quy định trong ISO/IEC 19795.
	ATE_IND.2-10	Không
	ATE_IND.2-11	Kiểm thử viên ***phải báo cáo*** trong ETR nỗ lực kiểm tra của kiểm thử viên về hiệu suất nhận dạng sinh trắc học bao gồm kích thước thử nghiệm, thời gian sử dụng và cả các đặc điểm của tập dữ liệu.

Bảng 25 - Bổ sung ATE_IND.2 (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
ATE_IND.2.1E	ATE_IND.2-1	Kiểm thử viên ***phải kiểm tra*** TOE để xác định rằng các tham số phát hiện tấn công trình diện tiềm năng được cấu hình chính xác theo cấu hình TOE được mô tả trong ST.
	ATE_IND.2-2	Không
	ATE_IND.2-3	Không
ATE_IND.2.2E	ATE_IND.2-4	Kiểm thử viên ***phải tiến hành*** thử nghiệm bằng cách sử dụng hoặc xây dựng lại các PAI do nhà phát triển tạo ra.
	ATE_IND.2-5	Không
	ATE_IND.2-6	Kiểm thử viên ***phải thiết lập*** một tập hợp con thử nghiệm trong đó kiểm thử viên sử dụng hoặc xây dựng lại các PAI do nhà phát triển tạo ra theo cách khác với cách do nhà phát triển thực hiện, chẳng hạn như trình diện PAI theo một phương thức khác. Ngoài ra, kiểm thử viên ***phải thiết lập*** tập con thử nghiệm của riêng họ. Kiểm thử viên ***phải xem xét*** việc sửa đổi các PAI do nhà phát triển tạo để thử nghiệm. Nếu như TOE đó có cơ chế PAD có thể bị vô hiệu hóa để thử nghiệm, Kiểm thử viên ***phải xem xét*** việc vô hiệu hóa cơ chế PAD trong TOE để tinh chỉnh các PAI sao cho chúng có thể được chấp nhận lỗi bởi cơ chế xác minh sinh trắc học của TOE.
	ATE_IND.2-7	Không
	ATE_IND.2-8	Không
	ATE_IND.2-9	Kiểm thử viên ***phải ghi lại*** việc sửa đổi PAI và cách sử dụng.
	ATE_IND.2-10	None
	ATE_IND.2-11	Kiểm thử viên ***phải báo cáo*** trong ETR nỗ lực kiểm tra của kiểm thử viên về cơ chế phát hiện tấn công trình diện về số lượng và mô tả các kiểu tấn công, loài PAI và kích thước thử nghiệm.

Xem thêm TCVN 14190-3.

15 Các hoạt động bổ sung cho TCVN 11386 về Lớp AVA: Đánh giá lỗ hổng

15.1 Tổng quát

Không có hoạt động bổ sung nào được bổ sung cho đánh giá hoạt động con AVA_VAN.1 và đánh giá hoạt động con AVA_VAN.5.

15.2 Các hoạt động bổ sung để phân tích lỗ hổng AVA_VAN

15.2.1 Các hoạt động bổ sung để đánh giá hoạt động con AVA_VAN.2

Bảng 26 và Bảng 27 liệt kê các hoạt động bổ sung được bổ sung cho các đơn vị công việc trong AVA_VAN.2 (xem thêm D.6.1).

Bảng 26 - Bổ sung cho AVA_VAN.2 (áp dụng cho hiệu suất nhận dạng sinh trắc học)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
AVA_VAN.2.1E	AVA_VAN.2-1	Không
	AVA_VAN.2-2	Không
AVA_VAN.2.2E	AVA_VAN.2-3	Không
AVA_VAN.2.3E	AVA_VAN.2-4	Không
	AVA_VAN.2-5	Không
AVA_VAN.2.4E	AVA_VAN.2-6	Kiểm thử viên ***phải thiết lập*** thử nghiệm thâm nhập, đồng thời tham khảo TCVN 14190-2 để xác định các điểm yếu tiềm năng có thể có trong TOE.
	AVA_VAN.2-7	Không
	AVA_VAN.2-8	Không
	AVA_VAN.2-9	Không
	AVA_VAN.2-10	Không
	AVA_VAN.2-11	Kiểm thử viên ***phải tham khảo*** Phụ lục F và các ví dụ trong TCVN 14190-2 để xác định tiềm năng tấn công của các cuộc tấn công chống lại hiệu suất nhận dạng sinh trắc học.
	AVA_VAN.2-12	Kiểm thử viên ***phải tham khảo*** Phụ lục F và các ví dụ trong TCVN 14190-2 để xác định tiềm năng tấn công của các cuộc tấn công chống lại hiệu suất định dạng sinh trắc học.

CHÚ THÍCH: Thử nghiệm thâm nhập là một thuật ngữ được sử dụng trong TCVN 8709-3.

Bảng 27 - Bổ sung cho AVA_VAN.2 (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
AVA_VAN.2.1E	AVA_VAN.2-1	Kiểm thử viên ***phải kiểm tra*** TOE để xác định rằng cấu hình thử nghiệm của các tham số phát hiện tấn công trình diện tiềm năng phù hợp với cấu hình được đánh giá như được mô tả trong ST.

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
	AVA_VAN.2-2	Không
AVA_VAN.2.2E	AVA_VAN.2-3	Không
AVA_VAN.2.3E	AVA_VAN.2-4	Kiểm thử viên ***phải tiến hành*** tham khảo TCVN 14190-3 để xác định các điểm yếu tiềm năng có thể có trong TOE.
	AVA_VAN.2-5	Không
AVA_VAN.2.4E	AVA_VAN.2-6	Kiểm thử viên ***phải thiết lập*** kiểm thử xâm nhập, đồng thời tham khảo TCVN 14190-3 để xác định các điểm yếu tiềm năng có thể có trong TOE.
	AVA_VAN.2-7	Kiểm thử viên ***phải đưa*** các hướng dẫn xây dựng vào tài liệu kiểm thử xâm nhập cho các PAI đã được xây dựng để kiểm thử xâm nhập.
	AVA_VAN.2-8	Không
	AVA_VAN.2-9	Kiểm thử viên ***phải ghi lại*** việc xây dựng và sử dụng PAI.
	AVA_VAN.2-10	Không
	AVA_VAN.2-11	Kiểm thử viên ***phải tham khảo*** Phụ lục F và các ví dụ trong TCVN 14190-3 để xác định tiềm năng tấn công của các tấn công trình diện.
	AVA_VAN.2-12	Kiểm thử viên ***phải tham khảo*** Phụ lục F và các ví dụ trong TCVN 14190-3 để xác định tiềm năng tấn công của các tấn công trình diện.

15.2.2 Các hoạt động bổ sung để đánh giá hoạt động con AVA_VAN.3

Bảng 28 và Bảng 29 liệt kê các hoạt động bổ sung được bổ sung cho các đơn vị công việc trong AVA_VAN.3 (xem thêm D.6.1).

Bảng 28 - Bổ sung cho AVA_VAN.3 (áp dụng cho hiệu suất định dạng sinh trắc học)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
AVA_VAN.3.1E	AVA_VAN.3-1	Không
	AVA_VAN.3-2	Không
AVA_VAN.3.2E	AVA_VAN.3-3	Không
AVA_VAN.3.3E	AVA_VAN.3-4	Không
	AVA_VAN.3-5	Không
AVA_VAN.3.4E	AVA_VAN.3-6	Kiểm thử viên ***phải thiết lập*** thử nghiệm thâm nhập, đồng thời tham khảo TCVN 14190-2 để xác định các lỗ hổng tiềm năng có

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
		thể có trong TOE.
	AVA_VAN.3-7	Không
	AVA_VAN.3-8	Không
	AVA_VAN.3-9	Không
	AVA_VAN.3-10	Không
	AVA_VAN.3-11	Kiểm thử viên ***phải tham khảo*** Phụ lục F và các ví dụ trong TCVN 14190-2 để xác định tiềm năng tấn công của các cuộc tấn công chống lại hiệu suất nhận dạng sinh trắc học.
	AVA_VAN.3-12	Kiểm thử viên ***phải tham khảo*** Phụ lục F và các ví dụ trong TCVN 14190-2 để xác định tiềm năng tấn công của các cuộc tấn công chống lại hiệu suất nhận dạng sinh trắc học.

CHÚ THÍCH: Thử nghiệm thâm nhập là một thuật ngữ được sử dụng trong TCVN 8709-3.

Bảng 29 - Bổ sung cho AVA_VAN.3 (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
AVA_VAN.2.1E	AVA_VAN.2-1	Kiểm thử viên ***phải kiểm tra*** TOE để xác định rằng cấu hình thử nghiệm của các tham số phát hiện tấn công trình diện tiềm năng phù hợp với cấu hình được đánh giá như được mô tả trong ST.
	AVA_VAN.2-2	Không
AVA_VAN.2.2E	AVA_VAN.2-3	Không
AVA_VAN.2.3E	AVA_VAN.2-4	Kiểm thử viên ***phải tiến hành*** tham khảo TCVN 14190-3 để xác định các lỗ hổng tiềm năng có thể có trong TOE.
	AVA_VAN.2-5	Không
AVA_VAN.2.4E	AVA_VAN.2-6	Kiểm thử viên ***phải thiết lập*** thử nghiệm thâm nhập, cũng tham khảo TCVN 14190-3 để xác định các lỗ hổng tiềm năng có thể có trong TOE.
	AVA_VAN.2-7	Kiểm thử viên **phải đưa** các hướng dẫn xây dựng vào tài liệu kiểm tra thâm nhập cho các PAI đã được xây dựng để kiểm tra thâm nhập.
	AVA_VAN.2-8	Không
	AVA_VAN.2-9	Kiểm thử viên ***phải ghi lại*** việc xây dựng và sử dụng PAI.

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
	AVA_VAN.2-10	Không
	AVA_VAN.2-11	Kiểm thử viên ***phải tham khảo*** Phụ lục F và các ví dụ trong TCVN 14190-3 để xác định tiềm năng tấn công của các cuộc tấn công trình diện.
	AVA_VAN.2-12	Kiểm thử viên ***phải tham khảo*** Phụ lục F và các ví dụ trong TCVN 14190-3 để xác định tiềm năng tấn công của các cuộc tấn công trình diện.

15.2.3 Các hoạt động bổ sung để đánh giá hoạt động con AVA_VAN.4

Bảng 30 và Bảng 31 liệt kê các hoạt động bổ sung được bổ sung cho các đơn vị công việc trong AVA_VAN.4 (xem thêm D.6.1).

Bảng 30 - Bổ sung cho AVA_VAN.3 (áp dụng cho hiệu suất nhận dạng sinh trắc học)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
AVA_VAN.4.1E	AVA_VAN.4-1	Không
	AVA_VAN.4-2	Không
AVA_VAN.4.2E	AVA_VAN.4-3	Không
AVA_VAN.4.3E	AVA_VAN.4-4	Không
	AVA_VAN.4-5	Không
AVA_VAN.4.4E	AVA_VAN.4-6	Kiểm thử viên ***phải thiết lập*** thử nghiệm thâm nhập, đồng thời tham khảo TCVN 14190-2 để xác định các lỗ hổng tiềm năng có thể có trong TOE.
	AVA_VAN.4-7	Không
	AVA_VAN.4-8	Không
	AVA_VAN.4-9	Không
	AVA_VAN.4-10	Không
	AVA_VAN.4-11	Kiểm thử viên ***phải tham khảo*** Phụ lục F và các ví dụ trong TCVN 14190-2 để xác định tiềm năng tấn công của các cuộc tấn công chống lại hiệu suất nhận dạng sinh trắc học.
	AVA_VAN.4-12	Kiểm thử viên ***phải tham khảo*** Phụ lục F và các ví dụ trong TCVN 14190-2 để xác định tiềm năng tấn công của các cuộc tấn

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
		công chống lại hiệu suất nhận dạng sinh trắc học.

Bảng 31 - Bổ sung cho AVA_VAN.3 (áp dụng cho PAD)

Thành phần hoạt động của Kiểm thử viên	Đơn vị công việc	Các hoạt động bổ sung
AVA_VAN.4.1E	AVA_VAN.4-1	Kiểm thử viên ***phải kiểm tra*** TOE để xác định rằng cấu hình thử nghiệm của các tham số phát hiện tấn công trình diện tiềm năng phù hợp với cấu hình được đánh giá như được mô tả trong ST.
	AVA_VAN.4-2	Không
AVA_VAN.4.2E	AVA_VAN.4-3	Không
AVA_VAN.4.3E	AVA_VAN.4-4	Kiểm thử viên ***phải tiến hành*** tham khảo TCVN 14190-3 để xác định các lỗ hổng tiềm năng có thể có trong TOE.
	AVA_VAN.4-5	Không
AVA_VAN.4.4E	AVA_VAN.4-6	Kiểm thử viên ***phải thiết lập*** thử nghiệm thâm nhập, đồng thời tham khảo TCVN 14190-3 để xác định các lỗ hổng tiềm năng có thể có trong TOE.
	AVA_VAN.4-7	Kiểm thử viên ***phải đưa*** các hướng dẫn xây dựng vào tài liệu kiểm tra thâm nhập cho các PAI đã được xây dựng để kiểm tra thâm nhập.
	AVA_VAN.4-8	Không
	AVA_VAN.4-9	Kiểm thử viên ***phải ghi lại*** việc xây dựng và sử dụng PAI.
	AVA_VAN.4-10	Không
	AVA_VAN.4-11	Kiểm thử viên ***phải tham khảo*** Phụ lục F và các ví dụ trong TCVN 14190-3 để xác định tiềm năng tấn công của các tấn công trình diện.
	AVA_VAN.4-12	Kiểm thử viên ***phải tham khảo*** Phụ lục F và các ví dụ trong TCVN 14190-3 để xác định tiềm năng tấn công của các tấn công trình diện.

PHỤ LỤC A

(tham khảo)

Giới thiệu các khái niệm cơ bản của TCVN 8709

A.1. Tổng quát

Phụ lục này nhằm cung cấp phần giới thiệu ngắn gọn về các từ ngữ chính được sử dụng trong bộ tiêu chuẩn TCVN 8709 để giúp người đọc chưa biết về bộ tiêu chuẩn TCVN 8709 có thể hiểu được tiêu chuẩn này. Nó không có ý định cung cấp cho người đọc hướng dẫn về cách sử dụng chính của bộ tiêu chuẩn TCVN 8709.

Trong bộ tiêu chuẩn TCVN 8709, đích đánh giá (TOE) là sản phẩm hoặc hệ thống được làm đối tượng của đánh giá. TOE được đặc trưng thông qua đích an toàn (ST), tức là tài liệu xác định các yêu cầu chức năng an toàn (SFR) và các yêu cầu đảm bảo an toàn (SAR) và có thể đề cập đến một hoặc nhiều hồ sơ bảo vệ (PP), tức là tài liệu xác định SFR và SAR cho một loại sản phẩm an toàn. Trong bộ tiêu chuẩn TCVN 8709, cấu hình bảo vệ hoạt động với mục tiêu an toàn cho một sản phẩm cụ thể như một lớp đối với một đối tượng trong ngôn ngữ lập trình hướng đối tượng. Hồ sơ bảo vệ được sử dụng để mô tả một lớp sản phẩm an toàn có chung một phạm vi nhất định và có thể được sử dụng để giải quyết một vấn đề an toàn nhất định. Mặt khác, một mục tiêu an toàn mô tả các đặc điểm an toàn của một sản phẩm cụ thể và cách nó đáp ứng tất cả các yêu cầu.

SFR cũng như SAR được thiết kế theo cấu trúc phân cấp bao gồm một lớp ở đầu phân cấp, tiếp theo là họ và thành phần. Lớp được sử dụng để gán SFR / SAR thành các danh mục được xác định trước và được xác định bằng cách viết tắt gồm ba ký tự; xem Bảng 1 và Bảng 2. Cách viết tắt gồm ba ký tự như vậy cũng được sử dụng để xác định các họ trong SFR và SAR. Các họ là một phần nhỏ hơn nữa của phạm trù lớp để xác định chính xác yêu cầu chức năng hoặc yêu cầu đảm bảo. Cuối cùng, thành phần được xác định bằng số, xác định cho SFR chức năng chuyên dụng cần được cung cấp bởi TOE và cho SAR các phần tử hành động cần được thực hiện trong quá trình đánh giá.

A.2. Yêu cầu chức năng an toàn

Các yêu cầu chức năng trong hồ sơ bảo vệ hoặc đích an toàn được lấy từ TCVN 8709-2. SFR có trong phần đó đóng vai trò như các khối xây dựng để mô hình hóa chức năng an toàn của TOE bằng một ngôn ngữ bán chính thức. Thực tế là chức năng an toàn của TOE không chỉ được mô tả bằng ngôn ngữ tự nhiên tạo điều kiện cho việc xác định chính xác phạm vi chức năng của đánh giá và cũng phục vụ cho việc so sánh các đánh giá khác nhau. Các lớp trong Bảng A.1 được sử dụng trong TCVN 8709-2 để phân loại các yêu cầu chức năng:

Bảng A.1 - Viết tắt của SFR

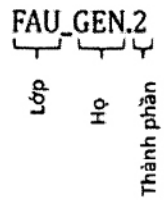
Từ viết tắt	Loại
FAU	Đánh giá an toàn
FCO	Liên lạc
FCS	Hỗ trợ mật mã
FDP	Bảo vệ dữ liệu người dùng
FIA	Định danh và xác thực
FPR	Riêng tư
FTA	Truy nhập TOE

FTP	Tuyến/kênh tin cậy
FRU	Sử dụng tài nguyên
FPT	Bảo vệ TSF
FMT	Quản lý an toàn

Một SFR chỉ định một chức năng liên quan đến việc kiểm tra các sự kiện thuộc về lớp FAU. Một mặt, các phần tử của lớp này được xác định trước trong TCVN 8709-2 và có thể được lựa chọn một cách đơn giản. Mặt khác, nếu không có đủ các họ được xác định trước, người thiết lập ST hoặc PP có thể chỉ định các họ của mình. Để hoàn thành ví dụ về một SFR thuộc lớp FAU, chức năng chịu trách nhiệm tạo kiểm tra được chọn lựa. Họ được xác định trước mô tả chức năng này viết tắt là GEN (tạo dữ liệu kiểm toán an toàn). Trong ST hoặc PP, SFR này sẽ được xác định bằng cách sử dụng ký hiệu FAU_GEN.

Với cùng một ví dụ, việc tạo ngày đánh giá có thể có ở các mức độ chi tiết khác nhau. Các mức này cũng được xác định trước trong TCVN 8709-2 và được chọn bởi số được gắn với mã định danh. Do đó, cả hai mã định danh FAU_GEN.1 cũng như FAU_GEN.2 đều giải quyết việc tạo dữ liệu đánh giá, nhưng ở các mức độ chi tiết khác nhau.

Giải thích của các phần này được tóm tắt trong Hình A.1.



Hình A.1 - Cấu trúc của FAU_GEN.2

Như đã đề cập, điều quan trọng là phải chỉ ra rằng người thiết lập ST hoặc PP có thể xác định các họ của chính họ và chữ viết tắt cần được giải thích trong PP hoặc ST. Tiêu chuẩn này định nghĩa một số SFR bổ sung (được gọi là SFR mở rộng) cho TCVN 8709-2.

A.3 Các yêu cầu đảm bảo an toàn

Các yêu cầu an toàn trong hồ sơ bảo vệ hoặc đích an toàn được lấy từ TCVN 8709-3. SAR có trong TCVN 8709-3 đóng vai trò là các khối xây dựng để xác định các yêu cầu đảm bảo an toàn của TOE sẽ được thực hiện trong quá trình đánh giá. Chúng được chia thành 6 loại trong Bảng A.2.

Bảng A.2 – Viết tắt của SAR

Từ viết tắt	Loại
ASE	Đánh giá an toàn
ADV	Phát triển
AGD	Tài liệu hướng dẫn
ALC	Hỗ trợ vòng đời
ATE	Các kiểm tra
AVA	Đánh giá điểm yếu

Các ký hiệu khác tương tự như ký hiệu được sử dụng cho SFR: các họ cụ thể hóa các yếu tố đánh giá cần được thực hiện và số lượng của thành phần xác định độ sâu cho các hoạt động đánh giá.

PHỤ LỤC B

(quy định)

Lớp FPT: Bảo vệ TSF

B.1 Phát hiện tấn công trình diện

B.1.1 FPT_PAD.1 Phát hiện tấn công trình diện

B.1.1.1 Các ghi chú ứng dụng của người dùng

FPT_PAD.1 yêu cầu TOE cung cấp khả năng phát hiện tấn công trình diện sinh trắc học.

Cơ chế PAD có thể bị ảnh hưởng bởi các tham số PAD có thể cấu hình. Đối với dữ liệu TSF như vậy, chỉ các giá trị an toàn mới được chấp nhận cho các cấu hình hoạt động để cơ chế PAD hoạt động như dự định trong sử dụng vận hành. Do đó, FMT_MTD.3 và FMT_SMF.1 được đưa vào như các phụ thuộc của FPT_PAD.1.

B.1.1.2 Các hoạt động

B.1.1.2.1 Phân công

Trong FPT_PAD.1.2, người thiết lập ST / PP sẽ liệt kê tất cả các hành động được thực hiện khi một tấn công trình diện được phát hiện. Việc phân công ít nhất phải có một hành động.

CHÚ THÍCH: Các ví dụ về hành động là tin nhắn, báo động, ghi âm, v.v. để phát hiện một cuộc tấn công.

Trong FPT_PAD.1.3, người thiết lập ST / PP sẽ liệt kê tất cả các hành động được thực hiện khi phát hiện thấy một trình diện thiếu chính xác.

Trong FPT_PAD.1.4, người thiết lập ST / PP sẽ liệt kê tất cả các thông tin bổ sung được gửi dưới dạng phản hồi với trạng thái tấn công trình diện bằng cơ chế PAD. Thông tin như vậy có thể là một giá trị điểm bổ sung, thể hiện khả năng xảy ra tấn công trình diện. Tuy nhiên, người thiết lập ST / PP nên hiểu mức độ nhạy cảm của thông tin như vậy vì một người dùng độc hại có thể sử dụng nó để xếp hạng các PAI đã tạo. Trong trường hợp đó, việc kiểm soát truy cập đối với những thông tin đó cần được xem xét. Nó có thể được chấp nhận để gán giá trị *none* ở đây.

B.2 Chụp sinh trắc học với phát hiện tấn công trình diện (FPT_BCP)

B.2.1 FPT_BCP.1 Kiểm tra các mẫu sinh trắc học để chụp

B.2.1.1 Các ghi chú ứng dụng của người dùng

Trong FPT_BCP.1.1, công cụ tấn công trình diện không phải nhân tạo bao gồm con người và các công cụ tấn công trình diện tự nhiên khác. Trong khi công cụ tấn công trình diện của con người được phân loại thành không có sự sống, bị thay đổi, không phù hợp, bị ép buộc và phù hợp (xem ISO/IEC 30107-1: 2016, 5.2), tấn công trình diện không phù hợp của con người ngoại trừ bắt chước cần được xem xét (xem 6.1). Các tấn công trình diện không phù hợp như vậy bao gồm trình diện với các chuyển động, quay hoặc khoảng cách chống lại các thông số kỹ thuật của thiết bị chụp (xem ISO/IEC 19795-1: 2006, Phụ lục C). Nó cũng bao gồm một trình diện với một phần của đặc trưng sinh trắc học được che giấu. Tiêu chí quyết định của TOE đối với công cụ tấn công trình diện không phải nhân tạo sẽ được mô tả trong thiết kế TOE.

Trong FPT_BCP.1.2, công cụ tấn công trình diện nhân tạo là một công cụ tấn công trình diện, được xây dựng nhân tạo như thể hiện của một loại PAI đã chọn, mô phỏng đặc trưng sinh trắc học của chủ thể dữ liệu đích mà TOE xử lý. Tiêu chí quyết định của TOE đối với công cụ tấn công trình diện nhân tạo sẽ được xác định trong thiết kế TOE.

B.2.1.2 Các hoạt động – Phân công

Trong FPT_BCP.1.1, người thiết lập ST / PP chỉ nêu rõ một đặc trưng sinh trắc học được sử dụng để thu thập sinh trắc học. Nếu người thiết lập ST / PP chỉ định nhiều đặc trưng sinh trắc học, thì người thiết lập ST / PP sẽ sử dụng thao tác lặp lại và mỗi bản chụp sinh trắc học cần được đánh giá riêng biệt.

B.2.2 FPT_BCP.2 Chụp sinh trắc học với tỷ lệ lỗi thấp

Các hoạt động – Phân công

Trong FPT_BCP.2.1, người thiết lập ST / PP chỉ nêu rõ một đặc trưng sinh trắc học được sử dụng để thu thập sinh trắc học. Nếu người thiết lập ST / PP chỉ định nhiều đặc trưng sinh trắc học, thì người thiết lập ST / PP sẽ sử dụng thao tác lặp lại và mỗi bản chụp sinh trắc học cần được đánh giá riêng biệt.

Trong FPT_BCP.2.1, định nghĩa FTER và FTAR phụ thuộc vào chính sách đăng ký và thu thập dữ liệu của TOE. Người thiết lập ST sẽ mô tả chính sách đó trong ST.

PHỤ LỤC C

(quy định)

Lớp FIA: Định dạng và xác thực

C.1 Đăng ký tham chiếu sinh trắc học (FIA_EBR)

C.1.1 FIA_EBR.1 Kiểm tra mẫu sinh trắc học để đăng ký

C.1.1.1 Các ghi chú ứng dụng của người dùng

Trong FIA_EBR.1.1, công cụ tấn công trình diện không phải công cụ nhân tạo bao gồm: con người và các công cụ tấn công trình diện tự nhiên khác. Trong khi công cụ tấn công trình diện của con người được phân loại thành không có sự sống, bị thay đổi, không phù hợp, bị ép buộc và phù hợp (xem ISO/IEC 30107-1:2016, 5.2), tấn công trình diện không phù hợp của con người ngoại trừ bắt chước, cần được xem xét (xem 6.1). Các tấn công trình diện không phù hợp như vậy bao gồm trình diện với các chuyển động, quay hoặc khoảng cách chống lại các thông số kỹ thuật của thiết bị chụp (xem ISO/IEC 19795-1:2006, Phụ lục C). Nó cũng bao gồm một trình diện với một phần được che giấu. Tiêu chí quyết định của TOE đối với công cụ tấn công trình diện không phải công cụ nhân tạo sẽ được mô tả trong thiết kế TOE.

Trong FIA_EBR.1.2, công cụ tấn công trình diện nhân tạo là một công cụ tấn công trình diện, được xây dựng nhân tạo như thể hiện của một loại PAI đã chọn, mô phỏng đặc trưng sinh trắc học của chủ thể dữ liệu đích mà TOE xử lý. Tiêu chí quyết định của TOE đối với công cụ tấn công trình diện nhân tạo sẽ được xác định trong thiết kế TOE.

C.1.1.2 Các hoạt động – Phân công

Trong FIA_EBR.1.1, người thiết lập ST/PP chỉ xác định một đặc trưng sinh trắc học được sử dụng để đăng ký sinh trắc học. Nếu người thiết lập ST/PP chỉ định nhiều đặc trưng sinh trắc học, người thiết lập ST/PP sẽ sử dụng thao tác lặp lại và mỗi lần đăng ký sinh trắc học cần được đánh giá riêng biệt.

Trong FIA_EBR.1.2, người thiết lập ST/PP sẽ chỉ xác định một đặc trưng sinh trắc học được sử dụng để đăng ký sinh trắc học. Nếu người thiết lập ST/PP chỉ định nhiều đặc trưng sinh trắc học, người thiết lập ST/PP sẽ sử dụng thao tác lặp lại và mỗi lần đăng ký sinh trắc học cần được đánh giá riêng biệt.

C.1.2 FIA_EBR.2 Đăng ký sinh trắc học với tỷ lệ lỗi đăng ký thấp

Các hoạt động – Phân công

Trong FIA_EBR.2.1, người thiết lập ST/PP sẽ chỉ xác định một đặc trưng sinh trắc học được sử dụng để đăng ký sinh trắc học. Nếu người thiết lập ST/PP chỉ định nhiều đặc trưng sinh trắc học, người thiết lập ST/PP sẽ sử dụng thao tác lặp lại và mỗi đăng ký sinh trắc học cần được đánh giá riêng biệt.

Trong FIA_EBR.2.1, định nghĩa của FTER phụ thuộc vào chính sách đăng ký của TOE. Người thiết lập ST sẽ mô tả chính sách đó trong ST.

C.2 Xác minh sinh trắc học (FIA_BVR)

C.2.1 FIA_BVR.1 Xác minh sinh trắc học với hiệu suất cao

C.2.1.1 Các hoạt động – Phân công

Trong FIA_BVR.1.1, người thiết lập ST / PP sẽ chỉ xác định một đặc trưng sinh trắc học được sử dụng để xác minh sinh trắc học. Nếu người thiết lập ST / PP chỉ định nhiều đặc trưng sinh trắc học, người thiết lập ST / PP sẽ sử dụng thao tác lặp lại và mỗi xác minh sinh trắc học cần được đánh giá riêng biệt.

C.2.1.2 Các hoạt động – Lựa chọn

Trong FIA_BVR.1.1, việc lựa chọn cặp tỷ lệ lỗi phụ thuộc vào PP / ST.

C.2.2 FIA_BVR.2 Thời gian xác thực người dùng với xác minh sinh trắc học

C.2.2.1 Các hoạt động – Phân công

Trong FIA_BVR.2.1, người thiết lập ST / PP sẽ chỉ xác định một đặc trưng sinh trắc học được sử dụng để xác minh sinh trắc học. Nếu người thiết lập ST / PP chỉ định nhiều đặc trưng sinh trắc học, người thiết lập ST / PP sẽ sử dụng thao tác lặp lại và mỗi xác minh sinh trắc học cần được đánh giá riêng biệt.

Trong FIA_BVR.2.2, người thiết lập ST / PP sẽ chỉ xác định một đặc trưng sinh trắc học được sử dụng để xác minh sinh trắc học. Nếu người thiết lập ST / PP chỉ định nhiều đặc trưng sinh trắc học, người thiết lập ST / PP sẽ sử dụng thao tác lặp lại và mỗi xác minh sinh trắc học cần được đánh giá riêng biệt.

C.2.2.2 Các hoạt động – Lựa chọn

Trong FIA_BVR.2.2, việc lựa chọn cặp tỷ lệ lỗi phụ thuộc vào PP / ST.

C.2.3 FIA_BVR.3 Xác thực người dùng với xác minh sinh trắc học trước bất kỳ hành động nào

C.2.3.1 Các hoạt động – Phân công

Trong FIA_BVR.3.1, người thiết lập ST / PP sẽ chỉ xác định một đặc trưng sinh trắc học được sử dụng để xác minh sinh trắc học. Nếu người thiết lập ST / PP chỉ định nhiều đặc trưng sinh trắc học, người thiết lập ST / PP sẽ sử dụng thao tác lặp lại và mỗi xác minh sinh trắc học cần được đánh giá riêng biệt.

C.2.3.2 Các hoạt động – Lựa chọn

Trong FIA_BVR.3.1, việc lựa chọn cặp tỷ lệ lỗi phụ thuộc vào PP / ST.

C.2.4 FIA_BVR.4 Xác minh sinh trắc học không chấp nhận các công cụ tấn công trình diện

C.2.4.1 Các ghi chú ứng dụng của người dùng

Trong FIA_EBR.4.1, công cụ tấn công trình diện không phải nhân tạo bao gồm con người và các công cụ tấn công trình diện tự nhiên khác. Trong khi công cụ tấn công trình diện của con người được phân loại thành không có sự sống, bị thay đổi, không phù hợp, bị ép buộc và phù hợp (xem ISO/IEC 30107-1: 2016, 5.2), tấn công trình diện không phù hợp của con người ngoại trừ bắt chước, cần được xem xét (xem 6.1). Các tấn công trình diện không phù hợp như vậy bao gồm trình diện với các chuyển động, quay hoặc khoảng cách chống lại các thông số kỹ thuật của thiết

bị chụp (xem ISO/IEC 19795-1: 2006, Phụ lục C). Nó cũng bao gồm một trình diện với một phần được che giấu. Tiêu chí quyết định của TOE đối với công cụ tấn công trình diện không phải nhân tạo sẽ được mô tả trong thiết kế TOE.

Trong FIA_BVR.4.2, công cụ tấn công trình diện nhân tạo là một công cụ tấn công trình diện, được xây dựng nhân tạo như thể hiện của một loài PAI đã chọn, mô phỏng đặc trưng sinh trắc học của chủ thể dữ liệu đích mà TOE xử lý. Tiêu chí quyết định của TOE đối với công cụ tấn công trình diện nhân tạo sẽ được xác định trong thiết kế TOE.

C.2.4.2 Các hoạt động – Phân công

Trong FIA_BVR.4.1, người thiết lập ST / PP chỉ xác định một đặc trưng sinh trắc học được sử dụng để xác minh sinh trắc học. Nếu người thiết lập ST / PP chỉ định nhiều đặc trưng sinh trắc học, người thiết lập ST / PP sẽ sử dụng thao tác lặp lại và mỗi xác minh sinh trắc học cần được đánh giá riêng biệt.

Trong FIA_BVR.4.2, người thiết lập ST / PP chỉ xác định một đặc trưng sinh trắc học được sử dụng để xác minh sinh trắc học. Nếu người thiết lập ST / PP chỉ định nhiều đặc trưng sinh trắc học, người thiết lập ST / PP sẽ sử dụng thao tác lặp lại và mỗi xác minh sinh trắc học cần được đánh giá riêng biệt.

C.3 Định danh sinh trắc học (FIA_BID)

C.3.1 FIA_BID.1 Định danh sinh trắc học với hiệu suất cao

C.3.1.1 Các hoạt động – Phân công

Trong FIA_BID.1.1, người thiết lập ST / PP sẽ chỉ xác định một đặc trưng sinh trắc học được sử dụng để định danh sinh trắc học. Nếu người thiết lập ST / PP chỉ định nhiều đặc trưng sinh trắc học, người thiết lập ST / PP sẽ sử dụng thao tác lặp lại và mỗi định danh sinh trắc học cần được đánh giá riêng biệt.

C.3.1.2 Các hoạt động – Lựa chọn

Trong FIA_BID.1.1, việc lựa chọn cặp tỷ lệ lỗi phụ thuộc vào PP / ST.

C.3.2 FIA_BID.2 Thời gian định danh sinh trắc học

C.3.2.1 Các hoạt động – Phân công

Trong FIA_BID.2.1, người thiết lập ST / PP sẽ chỉ xác định một đặc trưng sinh trắc học được sử dụng để định danh sinh trắc học. Nếu người thiết lập ST / PP chỉ định nhiều đặc trưng sinh trắc học, người thiết lập ST / PP sẽ sử dụng thao tác lặp lại và mỗi định danh sinh trắc học cần được đánh giá riêng biệt.

Trong FIA_BID.2.2, người thiết lập ST / PP sẽ chỉ xác định một đặc trưng sinh trắc học được sử dụng để định danh sinh trắc học. Nếu người thiết lập ST / PP chỉ định nhiều đặc trưng sinh trắc học, người thiết lập ST / PP sẽ sử dụng thao tác lặp lại và mỗi định danh sinh trắc học cần được đánh giá riêng biệt.

C.3.2.2 Các hoạt động – Lựa chọn

Trong FIA_BID.2.2, việc lựa chọn cặp tỷ lệ lỗi phụ thuộc vào PP / ST.

C.3.3 FIA_BID.3 Định danh sinh trắc học trước bất kỳ hành động nào

C.3.3.1 Các hoạt động – Phân công

Trong FIA_BID.3.1, người thiết lập ST / PP sẽ chỉ xác định một đặc trưng sinh trắc học được sử dụng để định danh sinh trắc học. Nếu người thiết lập ST / PP chỉ định nhiều đặc trưng sinh trắc học, người thiết lập ST / PP sẽ sử dụng thao tác lặp lại và mỗi định danh sinh trắc học cần được đánh giá riêng biệt.

C.3.3.2 Các hoạt động – Lựa chọn

Trong FIA_BID.3.1, việc lựa chọn cặp tỷ lệ lỗi phụ thuộc vào PP / ST.

C.3.4 FIA_BID.4 Định danh sinh trắc học không chấp nhận các công cụ tấn công trình diện

C.3.4.1 Các ghi chú ứng dụng của người dùng

Trong FIA_BID.4.1, công cụ tấn công trình diện không phải nhân tạo bao gồm con người và các công cụ tấn công trình diện tự nhiên khác. Trong khi công cụ tấn công trình diện của con người được phân loại thành không có sự sống, bị thay đổi, không phù hợp, bị ép buộc và phù hợp (xem ISO/IEC 30107-1: 2016, 5.2), tấn công trình diện không phù hợp của con người ngoại trừ bắt chước, cần được xem xét (xem 6.1). Các tấn công trình diện không phù hợp như vậy bao gồm trình diện với các chuyển động, quay hoặc khoảng cách chống lại các thông số kỹ thuật của thiết bị chụp (xem ISO/IEC 19795-1: 2006, Phụ lục C). Nó cũng bao gồm một trình diện với một phần được che giấu. Tiêu chí quyết định của TOE đối với công cụ tấn công trình diện không phải nhân tạo sẽ được mô tả trong thiết kế TOE.

Trong FIA_BID.4.2, công cụ tấn công trình diện nhân tạo là một công cụ tấn công trình diện, được xây dựng nhân tạo như thể hiện của một loài PAI đã chọn, mô phỏng đặc trưng sinh trắc học của chủ thể dữ liệu đích mà TOE xử lý. Tiêu chí quyết định của TOE đối với công cụ tấn công trình diện nhân tạo sẽ được xác định trong thiết kế TOE.

C.2.4.2 Các hoạt động – Phân công

Trong FIA_BID.4.1, người thiết lập ST / PP chỉ xác định một đặc trưng sinh trắc học được sử dụng để xác minh sinh trắc học. Nếu người thiết lập ST / PP chỉ định nhiều đặc trưng sinh trắc học, người thiết lập ST / PP sẽ sử dụng thao tác lặp lại và mỗi xác minh sinh trắc học cần được đánh giá riêng biệt.

Trong FIA_BID.4.2, người thiết lập ST / PP chỉ xác định một đặc trưng sinh trắc học được sử dụng để xác minh sinh trắc học. Nếu người thiết lập ST / PP chỉ định nhiều đặc trưng sinh trắc học, người thiết lập ST / PP sẽ sử dụng thao tác lặp lại và mỗi xác minh sinh trắc học cần được đánh giá riêng biệt.

PHỤ LỤC D

(tham khảo)

Thông tin cơ bản về các hoạt động bổ sung để đánh giá PAD

D.1 Lớp APE: Đánh giá Hồ sơ Bảo vệ / Lớp ASE: Đích đánh giá an toàn

D.1.1 Giới thiệu APE_INT PP / Giới thiệu ASE_INT ST

Một ST / PP không bao giờ được yêu cầu tỷ lệ lỗi tối đa có thể chấp nhận được đối với PAD (ví dụ: APCER, BPCER như được định nghĩa trong ISO/IEC 30107-3), vì các tỷ lệ này không cần được công bố trong ST / PP sau khi đánh giá. Tính đầy đủ của cơ chế PAD được xác định trong quá trình thử nghiệm (ATE) và đánh giá tính dễ bị tổn thương (AVA) trong bối cảnh mức đảm bảo đã được áp dụng.

Tuyên bố tổng thể liên quan đến cơ chế PAD phải là hệ thống tổng quát, có thể phát hiện các tấn công trình diện với giả định môi trường hoạt động được mô tả và một tiềm năng tấn công cụ thể (ví dụ như được xác định bằng cách sử dụng một thành phần cụ thể của AVA_VAN). Một phần của hoạt động thử nghiệm là xác định xem tỷ lệ lỗi được tạo ra có đủ để đáp ứng mức đảm bảo đã công bố theo các giả định về môi trường hoạt động hay không.

Phần giới thiệu của ST cần xác định rõ ràng các đặc trưng sinh trắc học (ví dụ: dấu vân tay) mà hệ thống con PAD có thể được sử dụng. Thông tin này rất quan trọng đối với những khách hàng tiềm năng đang tìm kiếm một TOE được chứng nhận với cơ chế PAD giống như cơ chế mà họ thường sử dụng sau khi bảo vệ một công nghệ dựa trên một đặc trưng sinh trắc học cụ thể.

Phần giới thiệu cũng phải bao gồm thông tin về hệ thống sinh trắc học được bảo vệ và phải xác định chức năng sinh trắc học (ví dụ: đăng ký, xác minh, định danh) và mục đích sử dụng dự kiến của hệ thống sinh trắc học có tầm quan trọng cụ thể cho kiểm thử viên. Thông tin này được sử dụng để cung cấp thông tin đánh giá liên quan đến các yêu cầu kiểm tra hiệu suất, phân tích lỗ hổng và tính toán tiềm năng tấn công.

Theo yêu cầu của bộ tiêu chuẩn TCVN 8709, ST phải mô tả các thành phần phần cứng bao gồm TOE. ST cần cung cấp tổng quan về cơ chế PAD bao gồm mô tả hoạt động của nó.

D.1.2 APE_SPD Định nghĩa vấn đề an toàn/ ASE_SPD Định nghĩa vấn đề an toàn

ST / PP phải mô tả các chính sách an toàn của tổ chức để bảo vệ quyền riêng tư dữ liệu cá nhân, bao gồm các biện pháp bảo vệ quyền riêng tư của dữ liệu sinh trắc học và dữ liệu đặc biệt nhạy cảm, chẳng hạn như dữ liệu có thể tiết lộ thông tin sức khỏe về người dùng.

CHÚ THÍCH: Khi một PP không thể bao gồm các mô tả chi tiết vì tính chất chung của nó, các mô tả được cung cấp trong ST.

D.2 Lớp ADV: Phát triển

D.2.1 Kiến trúc an toàn ADV_ARC

Trong tài liệu kiến trúc an toàn, nhà phát triển nên mô tả cách thức quá trình thu thập dữ liệu sinh trắc học và quá trình PAD hoạt động cùng nhau. Có một số khả năng, hệ thống con PAD có thể được tích hợp hoàn toàn vào một hệ thống con thu thập sinh trắc học riêng biệt. Ngoài ra, nó có

thể được phân phối trên một trong nhiều hệ thống con (ví dụ: hệ thống con thu thập sinh trắc học và hệ thống con xử lý tín hiệu)

Nhà phát triển nên mô tả cách đảm bảo rằng đặc trưng sinh trắc học được sử dụng để thu thập mẫu sinh trắc học giống với đặc tính được sử dụng cho PAD. Sử dụng thông tin này, kiểm thử viên nên chắc chắn rằng không bỏ qua cơ chế PAD. Ví dụ: trong hệ thống nhận dạng dấu vân tay, nếu cơ chế PAD có trước việc lấy mẫu dấu vân tay, thì có thể thực hiện một cuộc tấn công thành công vào hệ thống bằng cách đưa ra một ngón tay sống để đáp ứng thử nghiệm PAD, sau đó là một tạo tác để cung cấp nhận dạng sinh trắc học vật mẫu. Thông tin thêm về loại lỗ hổng này được cung cấp trong E.2.

D.2.2 Đặc tả chức năng ADV_FSP

Đặc tả chức năng cần đặc biệt mô tả các TSFI cho cơ chế PAD.

Nếu nhiều cơ chế được sử dụng để xác định liệu một trình diện có phải là tấn công trình diện hay không, thì mỗi cơ chế phải được mô tả bằng cách sử dụng các giao diện riêng biệt, các giao diện con riêng biệt hoặc các tham số riêng biệt cho một TSFI.

Nếu một cơ chế PAD chẳng hạn sử dụng cảm biến nhiệt độ và cảm biến điện dung cho PAD của nó, thì nhà phát triển nên mô tả một giao diện được phân tách thành giao diện phụ cho cảm biến nhiệt độ và giao diện phụ cho cảm biến điện dung.

Điều này cần được thực hiện để giúp kiểm thử viên hiểu rõ ràng về từng cơ chế và các khía cạnh vật lý khác nhau của trình diện mà các cơ chế đó dựa trên. Thông tin này là cần thiết trong bối cảnh đánh giá lỗ hổng vì kẻ tấn công có thể sử dụng mọi kênh / cơ chế có sẵn (hoặc kết hợp chúng) để giả mạo TSF.

Nhà phát triển cũng nên xem xét các thông số giao diện cho các cảm biến. Ví dụ, các thông số như vậy có thể là nhiệt độ hoặc độ ẩm của một đặc trưng sinh trắc học được trình diện, cường độ ánh sáng xung quanh hoặc áp lực mà ngón tay tác động lên thiết bị chụp.

Trong quá trình đánh giá đặc tả chức năng, kiểm thử viên nên xem xét liệu TSFI có cung cấp phản hồi về quyết định của cơ chế PAD cho người dùng hay không. Trong một số điều kiện nhất định, kẻ tấn công có thể sử dụng phản hồi đó để thực hiện các cuộc tấn công leo đồi (hill-climbing attacks) vào cơ chế PAD. Ví dụ: nếu TSFI cung cấp các giá trị điểm thể hiện xác suất một cuộc tấn công là một cuộc tấn công, thì những kẻ tấn công có thể sử dụng giá trị này để xếp hạng và cải thiện PAI cho các cuộc tấn công tinh vi hơn.

Nếu các thiết bị cảm biến được sử dụng cho cơ chế PAD là một phần của TOE, nhà phát triển phải mô tả cách TSFI cho cảm biến được dự định sử dụng bởi người dùng. Cụ thể, nhà phát triển nên mô tả quá trình trình diện đặc trưng sinh trắc học cho cảm biến. Lưu ý rằng thông tin này cũng có thể là một phần của tài liệu hướng dẫn trong trường hợp đó FSP có thể tham chiếu hướng dẫn.

D.2.3 Biểu diễn triển khai ADV_IMP

Cơ chế PAD có thể tham chiếu đến một số loại cơ sở dữ liệu để xác định xem liệu một trình diện có phải là một cuộc tấn công hay không (ví dụ: khi các cuộc tấn công trình diện được phát hiện bằng cách sử dụng so sánh mẫu). Trong trường hợp này, cơ sở dữ liệu là an toàn phù hợp với chức năng của PAD. Do đó, nó cũng cần được cung cấp cho kiểm thử viên như một phần của việc trình diện triển khai.

Cơ sở dữ liệu như vậy có thể là một phần rất có tính biến động cao của cơ chế PAD vì cơ sở dữ liệu được cập nhật khi các loại PAI mới xuất hiện. Do đó, nhà phát triển nên quyết định cung cấp thông tin phiên bản dành riêng cho cơ sở dữ liệu này và tách nó khỏi phần còn lại của phần trình diện triển khai (ví dụ: bằng cách chỉ định một hệ thống con hoặc mô-đun chuyên dụng cho nó). Sự tách biệt các khía cạnh động của loại cơ sở dữ liệu này có thể tạo điều kiện thuận lợi cho việc đánh giá lại TOE nếu cơ sở dữ liệu là phần duy nhất đang được cập nhật.

Tuy nhiên, cần phải đề cập rõ ràng rằng chứng nhận một TOE chỉ có giá trị đối với một phiên bản của cơ sở dữ liệu (trừ khi nhiều hơn một cấu hình của một TOE sẽ được đánh giá).

D.2.4 Thiết kế TOE ADV_TDS

Trong thiết kế TOE, nhà phát triển cung cấp thêm thông tin về TSF bằng cách mô tả các hệ thống con và mô-đun TOE. Đối với các hệ thống triển khai PAD, thiết kế TOE cần mô tả bằng chứng tấn công trình diện được kiểm tra cũng như các cơ chế được sử dụng để kiểm tra bằng chứng nhằm phát hiện các cuộc tấn công trình diện. Ví dụ về bằng chứng tấn công trình diện cho dấu vân tay là:

- Độ ẩm ngón tay;

- Điện tích của ngón tay;

- Nhiệt độ ngón tay;

- Lưu thông máu ở ngón tay;

- Oxy máu ở ngón tay;

- Xung;

- Mật độ quang học.

Ví dụ về cơ chế kiểm tra bằng chứng tấn công trình diện là:

- Đo điện tích;

- Phân tích phổ;

- Đo xung oxy để đo lượng oxy trong máu;

- Nhiệt kế;

- Xung siêu âm-echo (siêu âm).

Các cơ chế PAD thường dựa trên việc phát hiện các PAI nhân tạo hoặc cảm nhận sự sống của một trình diện hoặc sự kết hợp của cả hai. Phát hiện PAI nhân tạo cố gắng phân biệt các trình diện PAI nhân tạo với các trình diện đặc trưng sinh trắc học tự nhiên bằng cách đo các đặc tính vật lý của trình diện (có thể bao gồm sự sống). Phát hiện sự sống cố gắng xác định các đặc trưng sinh trắc học còn sống, ví dụ bằng cách đo độ bão hòa oxy trong máu hoặc xung. Thông tin này hữu ích cho kiểm thử viên khi cố gắng xác định các cuộc tấn công tiềm năng vào TOE trong quá trình đánh giá tính dễ bị tổn thương (xem TCVN 14190-3). Nhà phát triển cũng nên mô tả nền tảng lý thuyết cơ bản cho các cơ chế được sử dụng để kiểm thử viên có thể xác định hiệu lực của nó đối với PAD. Đặc biệt, nhà phát triển nên mô tả cách các tín hiệu từ các cảm biến được xử lý và chuyển thành bằng chứng tấn công trình diện.

Thiết kế TOE cần tiết lộ các tương tác giữa cơ chế PAD và chức năng thu thập. Thông tin chi tiết về việc thực hiện các cơ chế PAD của TOE là rất quan trọng đối với kiểm thử viên để giúp họ xác định các khu vực có khả năng bị tổn thương và thông báo cho quá trình đánh giá tính dễ bị tổn thương.

Nếu một hệ thống xác minh sinh trắc học sử dụng TOE của hệ thống con PAD và cho phép người dùng lặp lại các nỗ lực xác thực khi PAD phát hiện ra một tấn công trình diện, thì điều này nên được mô tả trong TDS. Số lần thử lại là rất quan trọng để xác định tỷ lệ lỗi tối đa thích hợp trong ATE. Môi trường mà TOE được dự kiến làm việc cũng có liên quan vì việc thử lại cũng có thể bị giới hạn bởi người điều hành khảo sát hoạt động của TOE.

Trong quá trình đánh giá, kiểm thử viên nên xem xét các vật liệu của PAI nào có thể được phát hiện và vật liệu nào không thể được phát hiện bởi cơ chế PAD. Điều này cũng đưa ra các gợi ý cho việc phân tích tính dễ bị tổn thương (xem TCVN 14190-3). Ví dụ: nếu PAD sử dụng cảm biến điện dung để đo công suất của ngón tay, kiểm thử viên có thể thử sử dụng hỗn hợp keo dán gỗ và bột than chì để sao chép hành vi điện của ngón tay.

D.3 Lớp AGD: Tài liệu hướng dẫn

D.3.1 AGD_OPE Hướng dẫn vận hành cho người dùng

Đối với các giao diện vật lý như thiết bị chụp, tài liệu hướng dẫn phải mô tả cách người dùng trình diện các đặc trưng sinh trắc học của họ cho TOE. Hướng dẫn vận hành cho người dùng phải cung cấp cho người vận hành hướng dẫn cho người dùng cách trình diện các đặc trưng sinh trắc học của họ cho TOE và cũng có trách nhiệm giám sát quá trình nắm bắt để đảm bảo việc sử dụng an toàn của nó. Điều này có thể quan trọng nếu TOE được sử dụng theo một cách cụ thể hoặc nếu hoạt động an toàn của TOE có thể bị đe dọa nếu nó được sử dụng theo một cách khác. Ví dụ: trong trường hợp phương thức vân tay, nếu các trình diện đặt sai vị trí có thể dẫn đến tỷ lệ chấp nhận lỗi gia tăng hoặc tỷ lệ lỗi phân loại trình diện bị tấn công, hướng dẫn sử dụng vận hành phải giải thích điều này và cung cấp lời khuyên cho người vận hành về việc giám sát các trình diện để đảm bảo rằng các trình diện không đúng chỗ không xảy ra.

Hướng dẫn sử dụng vận hành phải mô tả tất cả các tham số có thể cấu hình được sử dụng bởi cơ chế PAD và phạm vi giá trị cho phép của chúng. Các tham số PAD điển hình là các giá trị ngưỡng ví dụ được sử dụng để kiểm soát quyết định PAD. Hướng dẫn cũng phải nêu rõ vai trò nào có thể điều chỉnh các tham số.

Quản trị viên cần nhận được hướng dẫn về cách sửa đổi các tham số này một cách thích hợp và cách các sửa đổi thay đổi hoạt động của TOE. Hướng dẫn cần xác định rõ ràng phạm vi của tất cả các tham số đã được xem xét trong quá trình đánh giá TOE. Ngoài ra, hướng dẫn phải cung cấp thông tin về cách thiết lập các tham số này để TOE vẫn hoạt động trong cấu hình được mô tả trong hướng dẫn vận hành cho người dùng của TOE.

Người quản lý và người vận hành cũng cần được thông báo về các tham số môi trường mà họ chịu trách nhiệm và liệu TOE có không hoạt động trong cấu hình được đánh giá của nó hay không nếu các đặc tính của môi trường bị thay đổi.

Nếu vai trò người vận hành được xem xét trong môi trường hoạt động của TOE, thì hướng dẫn vận hành cho người dùng cũng phải mô tả liệu người vận hành có được phép ghi đè thủ công quyết định của cơ chế PAD hay không. Nếu một vai trò người vận hành được phép làm điều đó, hướng dẫn phải chỉ rõ cách vai trò người điều hành cần thực hiện điều đó. Ví dụ trong trường hợp

vân tay, nếu một đặc trưng sinh trắc học chính hãng không được định danh như vậy vì các trường hợp sau:

- Ngón tay (hoặc thậm chí cả bàn tay) bị mất;

- Dấu vân tay không rõ ràng do khuyết tật bẩm sinh;

- Vết thương như bỏng.

Trong những trường hợp như vậy, có thể có các thủ tục thay thế cần thiết mà người vận hành sẽ xem xét. Các thủ tục thay thế như vậy sau đó phải được mô tả bởi nhà phát triển.

Có thể cần phải tách các tài liệu hướng dẫn cho các vai trò khác nhau, ví dụ: quản trị viên, nhà khai thác và người dùng. Mô tả về cách người dùng nên trình diện đặc trưng sinh trắc học của mình cho thiết bị chụp rất có thể là thông tin công khai. Ngược lại, thông tin chi tiết về các thông số liên quan đến an toàn không nên được người dùng bình thường biết đến (vì khi đó kẻ tấn công cũng có thể dễ dàng truy cập được).

D.3.2 AGD_PRE Quy trình chuẩn bị

Các thủ tục chuẩn bị cho cơ chế PAD phải cung cấp các giá trị cụ thể cho các tham số sửa đổi hành vi của cơ chế PAD và sẽ được cấu hình như một phần của quá trình chuẩn bị TOE (ví dụ: các ngưỡng).

Nếu nhà phát triển cho phép sử dụng nhiều hơn một giá trị ngưỡng liên quan đến an toàn, điều này ngụ ý rằng có nhiều hơn một cấu hình được kiểm tra trong hoạt động thử nghiệm của ATE (xem TCVN 14190-3).

Đối với các TOE cụ thể, có thể cần phải hiệu chỉnh TOE khi nó được chuyển giao cho khách hàng. Ví dụ, nếu các phần vật lý của TOE có thể không được hiệu chuẩn trong quá trình phân phối hoặc cài đặt, thì chúng nên được hiệu chuẩn lại.

Xem xét phần cứng của TOE, các thủ tục chuẩn bị phải mô tả các điều kiện môi trường cần được đáp ứng và lưu giữ để đảm bảo hoạt động an toàn của TOE. Các điều kiện đó có thể là nhiệt độ của môi trường, độ ẩm không khí, áp suất không khí, ánh sáng xung quanh, bức xạ điện từ và các điều kiện khác.

TOE có thể yêu cầu các thành phần phần cứng và / hoặc phần mềm trong môi trường hoạt động của nó. Các thủ tục so sánh phải mô tả cách thức chuẩn bị các thành phần này để được sử dụng với TOE.

D.4 Lớp ALC: Hỗ trợ vòng đời

D.4.1 Phạm vi CM ALC_CMS

Thành phần đảm bảo ALC_CMS.4 đưa ra yêu cầu rằng các báo cáo lỗi an toàn và trạng thái giải quyết phải là một phần của danh sách cấu hình. Các PAI được chấp nhận lỗi bởi cơ chế PAD được coi là lỗi an toàn. Chúng cần được xem xét trong các báo cáo lỗi an toàn và tình trạng giải quyết cho phù hợp.

Tham khảo ALC_FLR trong D.4.3 để biết thêm thông tin về các lỗi an toàn như vậy.

D.4.2 Phân phối ALC_DEL

TOE chỉ có thể được chuyển giao cho các khách hàng được chọn để ngăn chặn các cá nhân không được phép lấy thông tin về TOE. Ví dụ, TOE có thể không có sẵn trong các nhà bán hàng và khách hàng quan tâm có thể cần liên hệ với nhà phát triển để đăng ký. Thực tế này có thể được sử dụng trong các giả định về môi trường hoạt động của TOE vì sẽ khó hơn để tấn công một hệ thống (cụ thể là để chuẩn bị tấn công) sẽ không dễ dàng có được. Tuy nhiên, nhà phát triển sẽ cần cung cấp chi tiết về cách thực hiện phân phối có kiểm soát như vậy để kiểm thử viên có thể xác định hiệu quả của nó đối với tiềm năng tấn công cơ bản.

D.4.3 Khắc phục lỗi ALC_FLR

Trong quá trình đánh giá TOE, các PAI không được phát hiện bởi TOE phải được ghi lại là lỗ hổng an toàn.

Có khả năng các loại PAI mới sẽ xuất hiện mà không phải là đối tượng kiểm tra trong quá trình đánh giá TOE và các PAI mới đó có thể đánh bại cơ chế PAD của TOE. Do đó, cách thức mà nhà phát triển giám sát mối đe dọa đang phát triển và kết hợp các thay đổi trong cơ chế PAD của TOE để chống lại mối đe dọa là một cân nhắc quan trọng đối với việc đánh giá TOE.

Do đó, việc tăng ít nhất ALC_FLR.1 nên được coi là bắt buộc đối với bất kỳ đánh giá TCVN 8709 nào về các TOE có chứa cơ chế PAD.

Nhà phát triển nên mô tả cách họ được thông báo về các PAI mới có khả năng phá vỡ TOE. Nhà phát triển cần đặc biệt mô tả cách thức nhận được thông tin như vậy từ các khách hàng của TOE.

Nhà phát triển nên mô tả cách họ đề xuất để giám sát mối đe dọa đang phát triển đối với TOE do các loại PAI mới gây ra. Giám sát có thể bao gồm:

- Thông tin về các mối đe dọa PAD và các lỗi PAD do khách hàng của TOE báo cáo;

- Tìm kiếm các bài báo và báo cáo có sẵn công khai về các bài kiểm tra khả năng PAD đối với các hệ thống sinh trắc học và công nghệ sử dụng phương thức tương tự như phương thức được sử dụng bởi TOE;

- Thu được các báo cáo về mối đe dọa và lỗ hổng PAD được cung cấp bởi giám sát sự cố an toàn được công nhận bởi các tổ chức như CSIRT và CERT.

Các thủ tục thay thế cho TOE có tầm quan trọng đặc biệt vì các lỗ hổng không thể được giải quyết bằng các bản vá hoặc cách giải quyết được cho là xảy ra đối với hệ thống con PAD thường xuyên hơn đối với các hệ thống CNTT khác. Do đó, nhà phát triển sẽ giải quyết các thủ tục thay thế.

D.4.4 Công cụ và kỹ thuật ALC_TAT

Trong ALC_TAT, nhà phát triển phải ghi lại tất cả các công cụ và kỹ thuật được sử dụng để phát triển, phân tích và triển khai TOE trong các phần phần cứng và phần mềm khác nhau của nó.

Đối với cơ chế PAD, điều này có thể bao gồm các công cụ và kỹ thuật để xây dựng PAI, chẳng hạn như thông tin về vật liệu và hướng dẫn xây dựng cho các loại PAI khác nhau. Tài liệu về các PAI hiện có phải do nhà phát triển cung cấp.

D.5 Lớp ATE: Các kiểm tra

D.5.1 ATE_FUN Các kiểm tra chức năng

Kế hoạch thử nghiệm của nhà phát triển phải cung cấp thông tin như hướng dẫn xây dựng được sử dụng để tạo PAI, vật liệu đã được sử dụng và tỷ lệ hỗn hợp vật liệu nếu có. Nếu các loại PAI tiêu chuẩn được cung cấp, nên sử dụng tập hợp tối thiểu các loại PAI đã xác định và các loại PAI không tiêu chuẩn được bổ sung cũng cần được xem xét trong quá trình thử nghiệm.

Nhà phát triển phải ghi lại các quy trình xây dựng cho tất cả các PAI và mô tả các khía cạnh liên quan như thời gian xây dựng. Ngoài ra, cần mô tả cách sử dụng chính xác của PAI trong quá trình thử nghiệm.

Đối với tất cả hoạt động thử nghiệm, TOE cũng cần thiết phải ở trong cấu hình được mô tả trong ST. Cụ thể, các tham số PAD sửa đổi hành vi của cơ chế PAD do đó phải được thiết lập theo yêu cầu trong ST. Nếu ST cho phép nhiều cài đặt cho các thông số liên quan đến an toàn, tất cả các thử nghiệm phải được tiến hành cho tất cả các cấu hình có thể.

Cuối cùng, kiểm thử viên nên kiểm tra xem số lượng PAI đã xây dựng và kích thước thử nghiệm tổng thể có được lập thành văn bản và đáp ứng các nhu cầu tối thiểu hay không. Xem TCVN 14190-3 để biết thêm thông tin chi tiết.

D.5.2 ATE_IND Kiểm tra độc lập

Đối với tất cả các hoạt động thử nghiệm, điều cần thiết là phải đảm bảo rằng TOE được vận hành trong cấu hình như được mô tả trong ST. Do đó, các tham số PAD sửa đổi hành vi của cơ chế PAD nên được đặt theo yêu cầu trong ST. Nếu ST cho phép nhiều cài đặt cho các thông số liên quan đến an toàn, tất cả các thử nghiệm phải được tiến hành cho tất cả các cấu hình có thể.

Kiểm thử viên phải ghi lại các quy trình xây dựng cho tất cả các PAI và mô tả các khía cạnh liên quan như thời điểm xây dựng. Ngoài ra, cần mô tả cách sử dụng chính xác của PAI trong quá trình thử nghiệm. Đối với các mô tả, kiểm thử viên nên bám sát mức độ chi tiết của các mô tả trong loài PAI tiêu chuẩn nếu được cung cấp.

Cuối cùng, kiểm thử viên phải báo cáo số lượng PAI đã được xây dựng và số lần kiểm tra cho mỗi PAI.

D.6 Lớp AVA: Đánh giá lỗ hổng an toàn

D.6.1 Phân tích lỗ hổng AVA_VAN

Để thực hiện kiểm thử thâm nhập trên TOE, kiểm thử viên cần đảm bảo rằng TOE ở trong cấu hình như được mô tả trong ST. Điều này bao gồm - nhưng không giới hạn ở - các tham số ảnh hưởng đến cơ chế PAD và được xác định trong ST.

Việc phân tích tính dễ bị tổn thương nên xem xét các gợi ý về các lỗ hổng đã được tìm thấy trong quá trình đánh giá ST, tài liệu phát triển, tài liệu hướng dẫn và các nguồn công khai. Thông tin thêm về các gợi ý về các lỗ hổng tiềm năng đối với PAD được tổng hợp trong Phụ lục E.

Kiểm thử viên phải ghi lại các kỹ thuật xây dựng cho các loại PAI khác nhau được sử dụng để thử nghiệm thâm nhập. Thông tin liên quan cần có trong đó ít nhất là vật liệu PAI đã sử dụng và mô tả quá trình xây dựng. Kiểm thử viên nên bám sát mức độ chi tiết của các mô tả trong các loài PAI tiêu chuẩn nếu được cung cấp.

Kiểm thử viên nên tính toán tiềm năng tấn công của các cuộc tấn công khai thác các lỗ hổng cụ thể của TOE. Đối với các cuộc tấn công vào cơ chế PAD sử dụng PAI, kiểm thử viên nên sử dụng phương pháp tính toán tiềm năng tấn công được thảo luận trong Phụ lục F.

PHỤ LỤC E

(tham khảo)

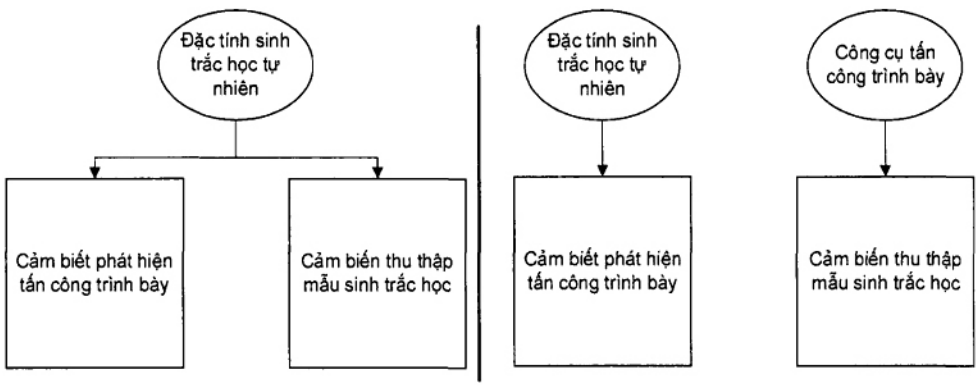
Các lỗ hổng tổng quát khác

E.1 Tổng quát

Phụ lục này cung cấp thêm hướng dẫn về một số lỗ hổng tổng quát tiềm năng có thể ảnh hưởng đến PAD hoặc các hệ thống con nhận dạng sinh trắc học. Kiểm thử viên nên xem xét chúng trong quá trình phân tích lỗ hổng. Nếu hai loại dữ liệu được thu thập bởi các cảm biến riêng biệt trong thiết bị thu thập sinh trắc học, thì có thể thực hiện một cuộc tấn công thành công bằng cách tấn công từng cảm biến riêng lẻ.

E.2 Tấn công hai kênh

Một cuộc tấn công hai kênh cố gắng khai thác bất kỳ sự tách biệt nào trong không gian hoặc thời gian có thể tồn tại giữa quá trình thu thập chính đặc trưng sinh trắc học và việc thu thập bằng chứng tấn công trình diện cho đặc tính đó. Nếu hai loại dữ liệu được thu thập bởi các cảm biến riêng biệt trong thiết bị thu thập sinh trắc học, thì có thể thực hiện một cuộc tấn công thành công bằng cách tấn công từng cảm biến riêng lẻ. Ví dụ: trong hệ thống sinh trắc học dấu vân tay, nếu phát hiện PAI thu thập dữ liệu từ một phần khác của thiết bị thu thập sinh trắc học với dữ liệu thu thập mẫu sinh trắc học được sử dụng để nhận dạng, kẻ tấn công có thể đưa ra một phần của ngón tay thật để vùng phát hiện PAI của thiết bị thu thập sinh trắc học và PAI cho vùng thu mẫu sinh trắc học. Trong trường hợp này, TOE có thể dễ bị tấn công hai kênh. Điều này được minh họa trong Hình E.1.



a) Người dùng thông thường **b) Tấn công hai kênh**

Hình E.1 - Tấn công hai kênh

Cuộc tấn công này cũng có thể khai thác các khía cạnh thời gian của quá trình thu thập khi việc phát hiện và thu thập cuộc tấn công trình diện được thực hiện theo trình tự. Các kiểm thử viên nên cảnh giác với khả năng phá vỡ các kỹ thuật PAD bằng các cuộc tấn công hai kênh.

Trong quá trình đánh giá tài liệu phát triển, kiểm thử viên phải đạt được sự tin tưởng rằng các cuộc tấn công hai kênh là không thể. Thông tin thu thập được trong quá trình đánh giá các khía cạnh ADV và AGD có thể là điểm khởi đầu cho phần đánh giá này.

Nếu việc kiểm tra thiết kế TOE chỉ ra rằng có khả năng một cuộc tấn công hai kênh có thể thành công, kiểm thử viên nên tiến hành kiểm tra thâm nhập để xác định liệu lỗ hổng có tồn tại trong thực tế hay không.

E.3 Phản hồi do TOE cung cấp

Phản hồi do TOE cung cấp về kết quả của các nỗ lực trình diện có thể hữu ích cho kiểm thử viên đang tiến hành đánh giá an toàn. Những thông tin đó có thể bao gồm: thu thập kết quả (thành công / thất bại và lý do), thu thập thông tin chất lượng mẫu, điểm số từ hệ thống con PAD, quyết định PAD, v.v.

Tuy nhiên, điều quan trọng là phải ngăn chặn thông tin phản hồi rơi vào tay người dùng thông thường, những người có thể là kẻ tấn công. Những kẻ tấn công có thể sử dụng thông tin phản hồi để hỗ trợ một cuộc tấn công và tăng khả năng nó thành công. Việc bảo vệ thông tin phản hồi là một vấn đề an toàn thông tin tạo thành một phần của đánh giá an toàn của TOE.

Kiểm thử viên nên xem xét liệu những thông tin đó có thể được kẻ tấn công sử dụng để hỗ trợ các cuộc tấn công trình diện hay không. Ví dụ: nếu có thể xác định các thuộc tính PAI dẫn đến giá trị điểm thấp hơn (hoặc cao hơn), thì có thể cải thiện PAI hiệu quả hơn bằng cách sử dụng phương pháp leo đồi.

Thông tin thu được từ việc đánh giá ADV_FSP có thể có giá trị cho phần đánh giá này.

Nếu việc kiểm tra đặc tả chức năng của TOE không xác nhận rằng về việc không có phản hồi ảnh hưởng đến an toàn nào được tạo ra, thì kiểm thử viên nên tiến hành kiểm tra thâm nhập để xác định xem liệu phản hồi có thể bị kẻ tấn công khai thác hay không.

Trong giai đoạn định danh, thời gian cần sử dụng tương ứng với thời gian cần thiết để tạo ra cuộc tấn công và để chứng minh rằng nó có thể được áp dụng thành công cho TOE (bao gồm thiết lập hoặc xây dựng bất kỳ thiết bị phần cứng hoặc phần mềm cần thiết nào). Việc chứng minh rằng cuộc tấn công có thể được áp dụng thành công cần phải xem xét bất kỳ khó khăn nào trong việc mở rộng một kết quả được tiến hành trong phòng thử nghiệm để tạo ra một cuộc tấn công hữu ích. Ví dụ, một trong những kết quả đầu ra từ định danh là một tập lệnh đưa ra mô tả từng bước về cách thực hiện cuộc tấn công. Tập lệnh này được giả định sử dụng trong phần khai thác.

Trong giai đoạn khai thác, thời gian cần sử dụng tương ứng với thời gian cần thiết để áp dụng "kịch bản" cho các đặc điểm sinh trắc học cụ thể. Ví dụ: đối với một cuộc tấn công bản trình diện vào thiết bị chụp dấu vân tay, nó tương ứng với thời gian cần thiết để tạo PAI từ một hình ảnh của một bản in (chứ không phải việc thu được hình ảnh này được tính đến trong yếu tố cơ hội (truy cập vào các đặc trưng sinh trắc học)).

Những khó khăn tiềm năng để có thể truy cập vào TOE trong môi trường khai thác được tính đến trong yếu tố cơ hội (truy cập vào TOE).

Chuyên môn đề cập đến mức độ thông thạo của kẻ tấn công đối với yêu cầu và kiến thức chung mà người đó sở hữu, không cụ thể về hệ thống bị tấn công. Các cấp độ như sau:

a) Công dân bình thường là trình độ không cần tới chuyên môn và bất kỳ người nào có trình độ học vấn phổ thông đều có thể thực hiện cuộc tấn công. Ví dụ: việc tạo PAI theo cách đã biết (đã được công bố) mà không có khó khăn cụ thể được xem xét ở cấp độ chuyên môn này.

CHÚ THÍCH: Thuật ngữ "công dân bình thường" được sử dụng cho sự trung lập về giới.

b) Thành thạo là mức độ yêu cầu một số kiến thức nâng cao trong các chủ đề cụ thể nhất định (sinh trắc học) cũng như kiến thức về các cuộc tấn công hiện đại. Kẻ tấn công ở cấp độ này có khả năng điều chỉnh các phương pháp tấn công đã biết theo nhu cầu. Ví dụ: điều chỉnh một cuộc tấn công đã biết (đã được phát hành) và tạo PAI bằng cách lựa chọn các tài liệu cụ thể (không được phát hành và đôi khi khó tìm) để vượt qua cơ chế phát hiện tấn công trình diện và/hoặc tìm một cách không rõ ràng để trình diện PAI này đối với hệ thống hoàn toàn có thể được xảy ra ở cấp độ chuyên môn này.

c) Chuyên ngành là cấp độ cần có sự chuẩn bị cụ thể trong nhiều lĩnh vực như nhận dạng mẫu, thị giác máy tính hoặc tối ưu hóa để thực hiện cuộc tấn công. Kẻ tấn công ở cấp độ này có khả năng tạo ra các thuật toán tấn công mới của riêng mình. Ví dụ: tìm một cách mới (chưa được phát hành) để tạo PAI bằng cách sử dụng các vật liệu mới và cụ thể ở cấp độ này có thể xem xét (chưa được phát hành) để chống lại cơ chế phát hiện tấn công trình diện nâng cao,. Ngoài ra, cấp độ này có thể được kết hợp với các trang bị cụ thể (thiết kế riêng).

d) Đa chuyên ngành là cấp độ mà cuộc tấn công cần sự hợp tác của một số người có chuyên môn cấp cao trong các lĩnh vực khác nhau (ví dụ: điện tử, phân tích mật mã, vật lý, v.v.). Cần lưu ý rằng một năng lực cụ thể trong sinh trắc học không được coi là "đa chuyên ngành". Ví dụ, xây dựng một cuộc tấn công "leo đồi" bằng cách đạt được quyền truy cập vào các điểm so sánh yêu cầu chuyên môn bổ sung để tấn công điện và thâm nhập TOE, có thể được coi là tạo thành một cấp độ "đa chuyên ngành".

CHÚ THÍCH 1: Như đã lưu ý ở phần trước, chuyên ngành khai thác thường thấp hơn chuyên ngành nhận dạng. Công dân bình thường hoặc thành thạo có thể được coi là giá trị tiêu biểu cho chuyên ngành trong giai đoạn khai thác. Vì lý do tương tự, nhiều cấp chuyên ngành bị loại khỏi giai đoạn khai thác.

CHÚ THÍCH 2: Như tất cả các yếu tố, tiềm năng tấn công cao hơn sẽ yêu cầu kiểm thử viên giải thích cụ thể.

Kiến thức về TOE đề cập đến lượng kiến thức về hệ thống cần thiết để thực hiện cuộc tấn công.

Ví dụ: định dạng của các mẫu thu được, kích thước và độ phân giải của hệ thống thu thập, định dạng cụ thể của các mẫu, nhưng cũng như các thông số kỹ thuật và thực hiện các biện pháp đối phó là những kiến thức có thể cần để thiết lập một cuộc tấn công.

Thông tin này có thể được công bố công khai trên trang web của nhà sản xuất thiết bị thu thập hoặc được bảo vệ (phân phối cho các bên liên quan theo thỏa thuận không tiết lộ hoặc thậm chí được phân loại trong nội bộ công ty). Các cấp độ như sau:

a) Thông tin công khai khá dễ lấy (ví dụ: trên web).

b) Thông tin hạn chế chỉ được chia sẻ bởi nhà phát triển và các tổ chức đang sử dụng hệ thống, thường là theo một thỏa thuận không tiết lộ.

c) Thông tin bí mật chỉ có sẵn trong tổ chức phát triển hệ thống và không có trường hợp nào được chia sẻ bên ngoài nó.

d) Thông tin quan trọng chỉ có sẵn cho những người hoặc nhóm nhất định trong tổ chức phát triển hệ thống.

Trong điểm này, cần đặc biệt chú ý đến các biện pháp đối phó có thể được thực hiện trong hệ thống và liệu có cần thiết hay không biết về sự tồn tại của các biện pháp đó để thực hiện thành công trong một cuộc tấn công nhất định.

Giả định rằng tất cả các kiến thức cần thiết để thực hiện cuộc tấn công được thu thập trong giai đoạn định danh và được "lên kịch bản" cho việc khai thác. Do đó, hệ số này không được sử dụng cho giai đoạn khai thác.

Cơ hội (Truy cập vào TOE) đề cập đến việc đo lường mức độ khó khăn trong việc truy cập vào TOE để chuẩn bị tấn công hoặc để thực hiện nó trên hệ thống đích.

Đối với giai đoạn xác định, các yếu tố cần được tính đến bao gồm sự dễ dàng để mua cùng một thiết bị sinh trắc học (có và không có biện pháp đối phó).

Đối với giai đoạn khai thác, cả các biện pháp kỹ thuật (điều chỉnh đã biết / chưa biết) và các biện pháp tổ chức (sự hiện diện của người bảo vệ, khả năng sửa đổi vật lý mục tiêu, số lần thử hạn chế, v.v.) cần được tính đến.

Số lượng và cấp độ thiết bị được yêu cầu để xây dựng cuộc tấn công cũng được tính đến trong yếu tố này.

Yếu tố này không được tính bằng thời gian. Các cấp độ như sau:

a) Dễ dàng: Đối với giai đoạn xác định, không có ràng buộc mạnh mẽ nào đối với kẻ tấn công phải mua TOE (giá hợp lý) để chuẩn bị tấn công. Đối với giai đoạn khai thác, không có giới hạn về số lần thử.

b) Trung bình: Đối với giai đoạn xác định, tồn tại các sơ đồ phân phối chuyên biệt (không áp dụng cho các cá nhân). Đối với giai đoạn khai thác, cần phải điều chỉnh cuộc tấn công đối với hệ thống cuối cùng (ví dụ: tham số không xác định của các biện pháp đối phó) hoặc có sự giám sát

của hệ thống sinh trắc học phát ra, ví dụ, một cảnh báo trong trường hợp trình diện không thành công.

c) Khó khăn: Đối với giai đoạn nhận dạng, hệ thống không khả dụng ngoại trừ những người dùng đã được xác định và việc truy cập đòi hỏi sự thỏa hiệp của một trong các tác nhân. Đối với giai đoạn khai thác, ví dụ PAI được điều chỉnh để điều chỉnh cụ thể (không xác định) hoặc có sự giám sát chặt chẽ (ví dụ như người bảo vệ) hoặc hệ thống cần sửa đổi vật lý (ví dụ: truy cập vật lý vào một tín hiệu ẩn quan trọng của điểm so sánh). Thường phải thỏa hiệp với một tác nhân tham gia vào việc sử dụng hệ thống (bảo vệ, quản trị viên và bảo trì).

Cơ hội (tiếp cận các đặc điểm sinh trắc học)

Các đánh giá an toàn của ISO / IEC 15408 được dành riêng để đánh giá khả năng phòng chống nội bộ của hệ thống. Do số lượng đường tấn công tiềm năng (ví dụ có hoặc không có sự hợp tác của đối tượng đã đăng ký), việc đánh giá không tính đến cách thu thập được đặc điểm sinh trắc học thực. Đối với phát hiện tấn công trình diện, phân tích lỗ hổng dựa trên giả thuyết rằng một "hình ảnh" thực có sẵn và tiềm năng tấn công chỉ liên quan đến việc tạo và trình diện PAI.

Tuy nhiên, điều quan trọng là có thể so sánh khả năng chống chịu của các hệ thống khác nhau, thậm chí dựa trên các sinh trắc học khác nhau. Ngoài ra, việc có được một "hình ảnh" thực để xây dựng PAI hoàn chỉnh là một phần của cuộc tấn công và được quan tâm, đối với người dùng cuối cùng của TOE và sự phù hợp của chứng chỉ để thêm yếu tố liên quan đến khía cạnh n. Các cấp độ như sau:

a) Ngay lập tức dành cho khuôn mặt 2D, hình ảnh chữ ký và giọng nói. Các mẫu của các phương thức này có thể được thu thập mà không gặp khó khăn, thậm chí không cần tiếp xúc trực tiếp với chủ thể dữ liệu đã đăng ký (khám phá qua web và mạng xã hội, v.v.).

b) Dễ dàng là đối với dấu vân tay. Dấu vân tay tiềm năng thường để lại trên các đối tượng mà chủ thể dữ liệu đã đăng ký có trong tay, nhưng cần được tiết lộ, thu thập và các hình ảnh tương ứng cần được xử lý trước.

c) Trung bình dành cho khuôn mặt 3D, chữ ký động và vân tay 3D. Hình ảnh 3D yêu cầu nhiều lần thu thập, có thể là theo cách có kiểm soát, mà không có sự cộng tác của chủ thể dữ liệu đã đăng ký nhưng có thể có liên hệ trực tiếp với chúng.

d) Khó là đối với mống mắt và tĩnh mạch. Có thể thu được hình ảnh mống mắt bằng máy ảnh độ phân giải cao, nhưng có một số khó khăn để có được hình ảnh chất lượng cao hoàn chỉnh mà không có sự hợp tác của chủ thể dữ liệu đã đăng ký. Tĩnh mạch là một đặc điểm ẩn, nhưng các camera hồng ngoại, ở gần chúng, có thể thu được hình ảnh để sử dụng.

CHÚ THÍCH 1: Việc phân phối các phương thức trên mỗi cấp có thể được sửa đổi tùy thuộc vào sự phát triển của công nghệ và cách sử dụng. Phân phối hiện tại được coi là hướng dẫn cho kiểm thử viên, người sẽ điều chỉnh tiềm năng tấn công thành hiện đại nhất.

CHÚ THÍCH 2: Đánh giá khả năng chống chịu của hệ thống dựa trên tiềm năng tấn công của các cuộc tấn công thành công và xác minh rằng không có cuộc tấn công thành công nào được tìm thấy ở cấp được nhắm mục tiêu. Một số cuộc tấn công không cần có sẵn dữ liệu sinh trắc học thực, ví dụ, các cuộc tấn công dựa trên hình ảnh tổng hợp hoặc tạo mẫu. Trong trường hợp như vậy, yếu tố này cần được xem xét ngay lập tức.

Trang thiết bị đề cập đến loại thiết bị cần thiết để thực hiện cuộc tấn công. Điều này bao gồm các cơ sở dữ liệu sinh trắc học được sử dụng (nếu có). Các cấp độ như sau:

- Thiết bị tiêu chuẩn là thiết bị có thể đặt hàng, dễ lấy và vận hành đơn giản (ví dụ: máy tính, máy quay video, điện thoại di động, vật liệu "tự làm" và các vật liệu nghệ thuật).

- Thiết bị chuyên dụng đề cập đến thiết bị khá đắt tiền, không có sẵn trên thị trường tiêu chuẩn và đòi hỏi phải có một số cấu tạo cụ thể để sử dụng (ví dụ: thiết bị phòng thí nghiệm, vật liệu và mực in cao cấp được xác định cụ thể và máy dò sóng tiên tiến).

- Thiết bị thiết kế riêng đề cập đến thiết bị rất đắt tiền với khả năng truy cập khó khăn và được kiểm soát; ví dụ, nghiên cứu hệ thống in ấn với loại mực cụ thể và thích ứng hỗ trợ linh hoạt. Ngoài ra, nếu cần nhiều hơn một thiết bị chuyên dụng để thực hiện các phần khác nhau của cuộc tấn công, thì cấp độ này nên được sử dụng. Trước khi sử dụng cấp độ này, phải kiểm tra cẩn thận để đảm bảo không có dịch vụ nào khả dụng (cho thuê, truy cập có thời hạn, v.v.). Nếu dịch vụ đó tồn tại, cấp độ sẽ được chuyển xuống cấp độ chuyên dụng.

F.1.4 Tính toán tiềm năng tấn công

Bảng F.1 xác định các yếu tố được thảo luận trong F.1.3 và kết hợp các giá trị số với tổng giá trị của mỗi yếu tố.

Bảng F.1 - Tính toán tiềm năng tấn công

Yếu tố	Giá trị	
	Định danh	Khai thác
Thời gian cần sử dụng		
≤ một ngày	0	0
≤ một tuần	1	2
≤ hai tuần	2	4
≤ một tháng	4	8
> một tháng	8	16
Chuyên môn		
Công dân bình thường	0	0
Thành thạo	2	4
Chuyên ngành	4	8
Đa chuyên ngành	8	Không áp dụng
Kiến thức về TOE		
Công khai	0	Không áp dụng

Yếu tố	Giá trị	
	Định danh	Khai thác
Hạn chế	2	Không áp dụng
Nhạy cảm	4	Không áp dụng
Quan trọng	8	Không áp dụng
Cơ hội (truy cập vào TOE)		
Dễ	0	0
Trung bình	2	4
Khó	4	8
Cơ hội (tiếp cận các đặc điểm sinh trắc học)		
Ngay lập tức	Không áp dụng	0
Dễ	Không áp dụng	2
Trung bình	Không áp dụng	4
Khó	Không áp dụng	8
Trang thiết bị		
Tiêu chuẩn	0	0
Chuyên dụng	2	4
Thiết kế riêng	4	8

Để tính toán giá trị tiềm năng tấn công của toàn bộ cuộc tấn công, kiểm thử viên phải thêm tất cả các giá trị của tất cả các yếu tố trong giai đoạn xác định và giai đoạn khai thác. Bảng F.1 được sử dụng như một hướng dẫn. Kiểm thử viên có thể sửa đổi bảng với một lý do phù hợp.

F.1.5 Đánh giá các lỗ hổng và khả năng chống lại TOE

Cột "Giá trị" của Bảng F.2 cho biết phạm vi của các giá trị tiềm năng tấn công (được tính bằng cách sử dụng Bảng A.1) của một tình huống tấn công dẫn đến các SFR bị phá hủy.

Bảng F.2 - Xếp hạng các lỗ hổng và khả năng chống lại TOE

Giá trị	Tiềm năng tấn công cần thiết để khai thác kịch bản:	TOE có khả năng chống lại những kẻ tấn công với tiềm năng tấn công là:	Đáp ứng các thành phần đảm bảo:	Lỗi của các thành phần:
<10	Cơ bản	Không xếp hạng	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
10–19	Nâng cao– Cơ bản	Cơ bản	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA_VAN.5
20–29	Trung bình	Nâng cao– Cơ bản	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3	AVA_VAN.4, AVA_VAN.5
30–39	Cao	Trung bình	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4	AVA_VAN.5
≥40	Vượt ngưỡng – Cao	Cao	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA_VAN.5	-

Thư mục tài liệu tham khảo

[1]. TCVN 11385:2016 (ISO/IEC 19792:2009) về Công nghệ thông tin - Các kỹ thuật an toàn - Đánh giá an toàn sinh trắc học

[2]. ISO/IEC 19795-1, Information technology — Biometric performance testing and reporting —Part 1: Principles and framework

[3]. ISO/IEC 29794-1:2016, Information technology — Biometric sample quality — Part 1: Framework

[4]. ISO/IEC 30107-1:2016, Information technology — Biometric presentation attack detection —Part 1: Framework

[5]. ISO/IEC 30107-3:2017, Information technology — Biometric presentation attack detection —Part 3: Testing and reporting

[6]. Bundesamt für Sicherheit in der Informationstechnik, Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies FSDPP_OSP v1.7, November 2009

[7]. Ellingsgaard J., Sousedik C., Busch C., Detecting Fingerprint Alterations by Orientation Field and Minutiae Orientation Analysis, in Proceedings of the 2nd International Workshop on Biometrics and Forensics 2014 (IWBF 2014), 27-28th March 2014, Valletta, Malta, (2014)

[8]. Gomez-Barrero M., Galbally J., Morales A., Ferrer M., Fierrez J., Ortega-Garcia J., A novel hand reconstruction approach and its application to vulnerability assessment. Information Sciences, 268:103–121, 2014

[9]. Gottschlich C., Mikaelyan A., Olsen M., Bigun J., Busch C., Improving Fingerprint Alteration Detection, in Proceedings 9th International Symposium on Image and Signal Processing and Analysis (ISPA 2015), 7-9 September, Zagreb, Croatia, (2015)

[10]. Haraksim R., Anthonioz A., Champod C., Olsen M., Ellingsgaard J., Busch C., Altered fingerprint detection - Algorithm performance evaluation, in Proceedings of the 4th International Workshop on Biometrics and Forensics 2016 (IWBF 2016), 3-4th March 2016, Limassol, Cyprus, (2016)

[11]. Martinez-Diaz M., Fierrez J., Galbally J., Ortega-Garcia J., An evaluation of indirect attacks and countermeasures in fingerprint verification systems. Pattern Recognition Letters, 32(12):1643–1651, 2011

[12]. Yoon S., Feng J., Jain A. K., Altered Fingerprints: Analysis and Detection, IEEE Trans. Pattern Anal. Mach. Intell., vol. 34, no. 3, pp. 451–464, (2012)