

TCVN

TIÊU CHUẨN QUỐC GIA

**TCVN 14190-3:2024
ISO/IEC 19989-3:2020**

Xuất bản lần 1

**AN TOÀN THÔNG TIN – TIÊU CHÍ VÀ PHƯƠNG PHÁP LUẬN
ĐÁNH GIÁ AN TOÀN HỆ THỐNG SINH TRẮC HỌC – PHẦN
3: PHÁT HIỆN TẤM CÔNG TRÌNH DIỆN**

Information security — Criteria and methodology for security evaluation of biometric systems – Part 3: Presentation attack detection

HÀ NỘI – 2024

Mục lục

Lời nói đầu	4
Giới thiệu	5
1 Phạm vi	7
2 Tài liệu viện dẫn	7
3 Thuật ngữ và định nghĩa	7
4 Thuật ngữ viết tắt	11
5 Nhận xét chung	12
6 Tổng quan về thử nghiệm PAD trong lớp ATE và lớp AVA	12
6.1 Mục tiêu và nguyên tắc	12
6.2. PAI được sử dụng trong các hoạt động thử nghiệm	13
6.3. Các hoạt động thử nghiệm	14
6.4. Tiêu chí đạt / không đạt	15
7. Các hoạt động bổ sung cho TCVN 11386 về thử nghiệm (ATE)	15
7.1. Cách tiếp cận thử nghiệm đối với PAD	15
7.2. Các chỉ số cho thử nghiệm PAD	16
7.3. Quy mô thử nghiệm tối thiểu và tỷ lệ lỗi tối đa	19
8. Các hoạt động bổ sung cho TCVN 11386 về đánh giá lỗi hỏng (AVA)	20
8.1. Thử nghiệm thâm nhập bằng cách sử dụng các biến thể PAI	20
8.2 Các lỗi hỏng tiềm năng	21
8.3. Đánh giá các lỗi hỏng và khả năng chống lại TOE	21
PHỤ LỤC A (tham khảo) Các ví dụ về tính toán giá trị tiềm năng tấn công của cuộc tấn công	22
Thư mục tài liệu tham khảo	28

Lời nói đầu

TCVN 14190-3:2024 hoàn toàn tương đương với ISO/IEC 19989-3:2020.

TCVN 14190-3:2024 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 vật nhân tạo 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 vật nhân tạo 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 cản 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 Công nghệ thông tin 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 cung cấp hướng dẫn và các yêu cầu cho nhà phát triển và kiểm thử viên đối với các hoạt động bổ sung về phát hiện tấn công trình diện được quy định trong TCVN 14190-1. Tiêu chuẩn này được xây dựng dựa trên những cản nhắc chung được mô tả trong TCVN 11385:2016 (ISO/IEC 19792:2009) và phương pháp luận thử nghiệm phát hiện tấn công trình diện được mô tả trong ISO/IEC 30107-3 bằng cách cung cấp thêm hướng dẫn cho kiểm thử viên.

Trong tiêu chuẩn này, thuật ngữ "người dùng" được sử dụng 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 3: Phát hiện tấn công trình diện

Information security — Criteria and methodology for security evaluation of biometric systems – Part 3: Presentation attack detection

1 Phạm vi

Đối với đánh giá an toàn của hệ thống xác minh sinh trắc học và hệ thống định danh sinh trắc học, tiêu chuẩn này dành riêng cho việc đánh giá an toàn phát hiện tấn công trình diện áp dụng bộ tiêu chuẩn TCVN 8709. Nó cung cấp các khuyến nghị và yêu cầu cho nhà phát triển và kiểm thử viên đối với các hoạt động bổ sung về phát hiện tấn công trình diện được quy định trong TCVN 14190-1 (ISO/IEC 19989-1).

Tiêu chuẩn này chỉ có thể áp dụng cho các TOE cho loại đặc tính sinh trắc học đơn lẻ nhưng để lựa chọn một đặc tính từ nhiều đặc tính.

2 Tài liệu viện dẫn

Các tài liệu sau đây được đề cập đến trong văn bản theo cách mà một số hoặc tất cả nội dung của chúng tạo thành các yêu cầu của tiêu chuẩn này. Đối với tài liệu ghi năm chỉ bản được nêu áp dụng. Đối với các tài liệu tham khảo không ghi ngày tháng, phiên bản mới nhất của tài liệu được tham chiếu (bao gồm mọi sửa đổi) sẽ được áp dụng.

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 8709-3:2011 (ISO/ IEC 15408-3:2008), 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 30107-3:2017, Information technology - Biometric presentation attack detection - Part 3: Testing and reporting

3 Thuật ngữ và định nghĩa

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

3.1

Tỷ lệ thu nhận tấn công trình diện (attack presentation acquisition rate)

APRA

Tỷ lệ các tấn công trình diện sử dụng cùng một loại PAI (3.15) mà từ đó hệ thống con thu thập dữ liệu thu được mẫu sinh trắc học có đủ chất lượng.

[NGUỒN: ISO/IEC 30107-3: 2017, 3.2.5]

3.2

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]

3.3

Tỷ lệ không phản hồi tấn công trình diện (attack presentation non-response rate)

APNRR

Tỷ lệ các tấn công trình diện sử dụng cùng một loại PAI (3.15) không gây ra phản hồi tại hệ thống con PAD hoặc hệ thống con thu thập dữ liệu.

Ví Dụ: Hệ thống dấu vân tay có thẻ không đăng ký hoặc phản ứng với việc trình diện PAI do PAI thiếu tính hiện thực.

[NGUỒN: ISO/IEC 30107-3: 2017, 3.2.3]

3.4

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]

3.5

Trình diện trung thực (bona fide presentation)

Sự tương tác của chủ thẻ 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]

3.6

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]

3.7

Tỷ lệ không phản hồi trình diện trung thực (bona fide presentation non-response rate)

BPNRR

Tỷ lệ trình diện trung thực (3.5) không gây ra phản hồi tại hệ thống con PAD hoặc hệ thống con thu thập dữ liệu

[NGUỒN: ISO/IEC 30107-3: 2017, 3.2.4]

3.8

Tỷ lệ không nhận dạng tấn công trình diện che giấu (concealer attack presentation non-identification rate)

CAPNIR

<đánh giá toàn hệ thống của một hệ thống định danh> tỷ lệ các cuộc tấn công trình diện che giấu bằng cách sử dụng cùng một loại PAI (3.15) trong đó tham chiếu định danh của người che giấu không nằm trong số các định danh được trả lại hoặc tùy thuộc vào trường hợp sử dụng dự định, trong đó không có định danh nào được trả lại.

CHÚ THÍCH 1: Trong hệ thống các nhận dạng bị từ chối, chẳng hạn như danh sách đen, người che giấu có thể có ý định rằng không có định danh nào được trả lại để tránh sự giám sát của người điều hành.

[NGUỒN: ISO/IEC 30107-3: 2017, 3.2.9]

3.9

Tỷ lệ không trùng khớp tấn công trình diện che giấu (concealer attack presentation non-match rate)

CAPNMR

<đánh giá toàn hệ thống của một hệ thống xác minh> tỷ lệ các tấn công trình diện che giấu sử dụng cùng một loại PAI (3.15) trong đó tham chiếu của che giấu không trùng khớp

[NGUỒN: ISO/IEC 30107-3: 2017, 3.2.7]

3.10

Tỷ lệ lỗi định danh phù định sai (false-negative identification-error rate)

FNIR

tỷ lệ các giao dịch định danh của người dùng đã đăng ký trong hệ thống trong đó định danh chính xác của người dùng không nằm trong số các giao dịch được trả lại

[NGUỒN: ISO/IEC 19795-1: 2006, 4.6.8]

3.11

Tỷ lệ lỗi định danh khẳng định sai (false-positive identification-error rate)

FPIR

tỷ lệ các giao dịch định danh của người dùng không đăng ký trong hệ thống, trong đó định danh là trả lại.

[NGUỒN: ISO/IEC 19795-1: 2006, 4.6.9]

3.12

Tỷ lệ nhận dạng tấn công trình diện mạo danh (impostor attack presentation identification rate)

IAPIR

<đánh giá toàn hệ thống của một hệ thống định danh> Tỷ lệ tấn công trình diện mạo danh sử dụng cùng một loại PAI (3.15) trong đó định danh tham chiếu được nhắm mục tiêu nằm trong số các định danh được trả về hoặc tùy thuộc vào trường hợp sử dụng dự kiến, ít nhất một định danh được hệ thống trả về.

CHÚ THÍCH 1: Kẻ tấn công có thể vừa là kẻ mạo danh (cố gắng so trùng khớp với người đăng ký không phải là bản thân hiện có) vừa là kẻ che khuyết điểm (che giấu mẫu sinh trắc học thực bằng PAI).

[NGUỒN: ISO/IEC 30107-3: 2017, 3.2.8]

3.13

Tỷ lệ trùng khớp tấn công trình diện mạo danh (impostor attack presentation match rate)

IAPMR

<đánh giá toàn hệ thống của một hệ thống xác minh> tỷ lệ các tấn công trình diện mạo danh sử dụng cùng một loại PAI (3.15) trong đó tham chiếu mục tiêu là trùng khớp.

[NGUỒN: ISO/IEC 30107-3: 2017, 3.2.6]

3.14

PAI phi tiêu chuẩn (non-standard PAI)

Công cụ tấn công trình diện (PAI) không tương ứng với loại PAI tiêu chuẩn (3.18).

3.15

Loại PAI (PAI species)

Loại công cụ tấn công trình diện được tạo ra bằng cách sử dụng một phương pháp sản xuất chung và dựa trên các đặc điểm sinh trắc học khác nhau.

VÍ DỤ 1 Một tập hợp các dấu vân tay giả được làm theo cùng một cách với cùng một vật liệu nhưng có các vân ma sát khác nhau sẽ tạo thành một loại PAI.

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

[NGUỒN: ISO/IEC 30107-3: 2017, 3.1.6]

3.16

Thử nghiệm thâm nhập (penetration testing)

Thử nghiệm được sử dụng trong phân tích lỗ hổng để đánh giá tính dễ bị tổn thương, cố gắng phơi bày 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 có định nghĩa.

3.17**PAI tiêu chuẩn (standard PAI)**

PAI nằm trong loại PAI tiêu chuẩn (3.18)

3.18**Loại PAI tiêu chuẩn (standard PAI species)**

Loại PAI (3.15) được tổ chức chứng nhận hoặc cộng đồng kỹ thuật xác định và chỉ định làm tiêu chuẩn cho mục đích thực hiện đánh giá

CHÚ THÍCH 1: Nếu các loại PAI tiêu chuẩn không được chỉ định, nhà phát triển cũng như kiểm thử viên chuẩn bị các PAI phi tiêu chuẩn (3.14) để sử dụng trong các hoạt động đánh giá.

4 Thuật ngữ viết tắt

ADV	security assurance requirement (SAR) class of development	lớp yêu cầu đảm bảo an toàn (SAR) của việc phát triển CHÚ THÍCH: Tên lớp được định nghĩa trong TCVN 8709-3:2011 (TCVN 8709-3). Ở đây A là viết tắt của yêu cầu đảm bảo, DV cho việc phát triển. Tên lớp được định nghĩa theo cách này trong TCVN 8709
ATE	security assurance requirement (SAR) class of tests	lớp các thử nghiệm của yêu cầu đảm bảo an toàn (SAR)
AVA	security assurance requirement (SAR) class of vulnerability assessment	lớp đánh giá lỗ hổng của yêu cầu đảm bảo an toàn (SAR)
AVA_VAN	security assurance requirement (SAR) family for vulnerability analysis in class AVA	họ phân tích lỗ hổng trong lớp AVA của yêu cầu đảm bảo an toàn (SAR)
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
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
SFR	security functional requirement	yêu cầu chức năng an toàn
ST	security target	đích an toàn
TCVN		tiêu chuẩn quốc gia
TOE	target of evaluation	đích đánh giá

5 Nhận xét chung

Ngoài các yêu cầu và khuyến nghị được cung cấp trong tiêu chuẩn này, phải áp dụng các yêu cầu và khuyến nghị trong TCVN 8709-3 (ISO/IEC 15408-3) và TCVN 11386 (ISO/IEC 18045).

Định nghĩa về xác thực có trong ISO/IEC 2382.

Các định nghĩa của sinh trắc học (tính tử), thu thập sinh trắc học, thiết bị thu thập sinh trắc học, đặc điểm sinh trắc học, che giấu sinh trắc học, đăng ký sinh trắc học, định danh sinh trắc học, kẻ giả mạo sinh trắc học, công nhận sinh trắc học, hệ thống sinh trắc học, xác minh sinh trắc học, đối sánh, đăng ký, tỷ lệ thu thập thất bại, tỷ lệ đăng ký thất bại, tỷ lệ trùng khớp sai, tỷ lệ không trùng khớp sai, định danh và ngưỡng (danh từ) có 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 "đăng ký" đôi khi được sử dụng thay cho "đăng ký sinh trắc học".

CHÚ THÍCH 4: Trong tiêu chuẩn này, cụm từ "kẻ mạo danh" đôi khi được sử dụng thay cho "kẻ mạo danh sinh trắc học".

Định nghĩa về đảm bảo, tiềm năng tấn công, lớp, thành phần, xác nhận, phân phối, mô tả, xác định, nhà phát triển, phát triển, đảm bảo, đánh giá, họ, hồ sơ bảo vệ, Đích an toàn, Đích đánh giá và lỗ hổng an toàn có trong TCVN 8709-1.

Các định nghĩa về hoạt động, phương pháp luận và báo cáo có sẵn trong TCVN 11386: 2008.

Các định nghĩa về tấn công trình diện, phát hiện tấn công trình diện và công cụ tấn công trình diện có trong ISO/IEC 30107-1.

6 Tổng quan về thử nghiệm PAD trong lớp ATE và lớp AVA

6.1 Mục tiêu và nguyên tắc

6.1.1. Lớp ATE

Các hoạt động trong Lớp ATE tập trung vào câu hỏi liệu các cơ chế PAD được cung cấp có hoạt động như quy định hay không. Thử nghiệm chức năng có thể chứng minh sự tồn tại của lỗ hổng PAD trong TOE (nghĩa là tỷ lệ lỗi khác 0) nhưng không thể chứng minh rằng không có lỗ hổng nào tồn tại.

Thử nghiệm chức năng về tính hiệu quả đối với tính năng PAD của TOE được thực hiện bằng cách đo lường sự thành công và thất bại của phát hiện bởi TOE với PAI bằng cách sử dụng phương pháp thử nghiệm dựa trên thống kê (tức là đo lường tỷ lệ lỗi và thành công của PAD), để chứng minh rằng tính năng PAD tồn tại và tỷ lệ lỗi PAD đáp ứng đặc điểm kỹ thuật trong tài liệu ATE_FUN. ATE_IND có thể có hoặc không bao gồm thử nghiệm thống kê tùy thuộc vào bối cảnh đánh giá.

Lưu ý rằng thử nghiệm chức năng được mô tả trong tiêu chuẩn này khác với thử nghiệm chức năng về hiệu suất định danh sinh trắc học bằng cách sử dụng các đặc tính sinh trắc học tự nhiên của các đối tượng thử nghiệm được mô tả trong TCVN 14190-2 sau khi sử dụng TOE dự kiến.

6.1.2 Lớp AVA

Đánh giá lớp AVA bao gồm các hoạt động thử nghiệm thâm nhập. Thử nghiệm thâm nhập bao gồm việc điều tra các lỗi hỏng tiềm năng của một TOE đối với các cuộc tấn công trình diện mà có thể chưa được thử nghiệm chức năng trước đó phát hiện (lớp ATE). Điều này có thể bao gồm PAI tiêu chuẩn và các biến thể của PAI tiêu chuẩn được sử dụng trong thử nghiệm chức năng và các PAI mới được tạo ra để tìm hiểu các lỗi hỏng có thể có của PAD trong các thuật toán phần cứng hoặc phần mềm thu được sử dụng, chẳng hạn như trong xử lý tín hiệu và đối sánh sinh trắc học. Thử nghiệm thâm nhập không liên quan đến phương pháp thử nghiệm thống kê được sử dụng để thử nghiệm chức năng (lớp ATE).

Lưu ý rằng thử nghiệm với các PAI có thể tùy thuộc vào sự thay đổi của trình diện và sự thay đổi của quá trình chuẩn bị PAI. Thử nghiệm phải được tiếp tục cho đến khi đạt được mức độ tin cậy thích hợp về kết quả của thử nghiệm tương ứng với mức độ của họ bảo đảm AVA_VAN được chỉ định trong ST của TOE.

6.2. PAI được sử dụng trong các hoạt động thử nghiệm

6.2.1 Lớp ATE

Các PAI tiêu chuẩn phải được chuẩn bị và sử dụng theo các thông số kỹ thuật và hướng dẫn, nếu được cung cấp. PAI tiêu chuẩn có thể được tổ chức chứng nhận hoặc cộng đồng kỹ thuật cung cấp cho nhà phát triển và kiểm thử viên hoặc do nhà phát triển và kiểm thử viên chuẩn bị theo các thông số kỹ thuật và hướng dẫn của loại PAI tiêu chuẩn. Nếu các PAI tiêu chuẩn không được cung cấp, thì các PAI phi tiêu chuẩn sẽ được xây dựng và sử dụng bởi nhà phát triển và kiểm thử viên.

CHÚ THÍCH Việc sử dụng sinh trắc học tự nhiên như PAI được bao gồm trong các hoạt động thử nghiệm nếu (các) SFR như FPT_BCP.1, FIA_EBR.1, FIA_BVR.4 và FIA_BID.4 quy định trong TCVN 14190-1 được chọn trong ST. Ngay cả khi các SFR đó không được chọn, các PAI sinh trắc học tự nhiên có thể là một phần của các PAI tiêu chuẩn. Như được mô tả trong TCVN 14190-1:2024, 6.4.2.1, 7.5.1.1, 7.5.6.1 và 7.5.10.1, PAI sinh trắc học tự nhiên bao gồm các đặc điểm sinh trắc học tự nhiên được trình diện với các chuyển động, quay hoặc khoảng cách so với thông số kỹ thuật của quá trình thu thập thiết bị. Điều này cũng áp dụng cho Lớp AVA.

Nếu các PAI tiêu chuẩn không được cung cấp, các PAI phi tiêu chuẩn sẽ do nhà phát triển chuẩn bị và nhà phát triển cung cấp cho kiểm thử viên.

Các PAI được kiểm thử viên sử dụng cho ATE thay đổi tùy theo thông tin có sẵn cho kiểm thử viên vì nó là một trong những yếu tố quan trọng để xác định các PAI được kiểm thử viên sử dụng. Theo mặc định, kiểm thử viên phải dựa trên loại PAI tiêu chuẩn. Ngoài ra, kiểm thử viên nên dựa vào thông tin tấn công hiện đại để xác định xem các PAI được sử dụng để thử nghiệm chức năng có phải là đại diện cho các PAI mà kẻ tấn công có thể sử dụng trên TOE hay không.

6.2.2 Lớp AVA

Kiểm thử viên sẽ tạo và sử dụng các PAI phi theo tiêu chuẩn trong thử nghiệm thâm nhập.

6.3. Các hoạt động thử nghiệm

6.3.1. Lớp ATE

Mục tiêu của bất kỳ hoạt động thử nghiệm chức năng nào được thực hiện trong Lớp ATE là để xác định xem cơ chế PAD có thể phát hiện PAI với độ tin cậy đủ hay không. Trong ATE_FUN.1 và ATE_FUN.2, nhà phát triển sẽ tiến hành thử nghiệm chức năng bằng cách sử dụng ít nhất các PAI tiêu chuẩn hoặc các PAI phi tiêu chuẩn tùy thuộc vào việc các loại PAI tiêu chuẩn có được cung cấp hay không. Nhà phát triển có thể chuẩn bị các PAI phi tiêu chuẩn để tiến hành thử nghiệm chức năng bổ sung, cung cấp thông tin về bản chất của các PAI mà kiểm thử viên nên tập trung vào để giảm bớt các hoạt động đánh giá của kiểm thử viên.

Kiểm thử viên sẽ tiến hành thử nghiệm độc lập bằng cách sử dụng các PAI được chọn từ các PAI tiêu chuẩn, nếu các loại PAI tiêu chuẩn được cung cấp hoặc các PAI phi tiêu chuẩn.

Các giá trị cho tỷ lệ lỗi tối đa được xác nhận trong đánh giá được quy định trong tài liệu TOE ATE_FUN và ý nghĩa của các giá trị đối với quy mô thử nghiệm được thảo luận thêm trong 6.3.

Tỷ lệ lỗi phải được báo cáo độc lập cho từng loại PAI được thử nghiệm. Tỷ lệ lỗi tối đa của tất cả các loại PAI được thử nghiệm là chỉ số chính về cách TOE thực hiện trong việc phát hiện các loại PAI nhất định.

CHÚ THÍCH: Các tài liệu ADV chỉ được tiết lộ cho kiểm thử viên và tổ chức chứng nhận khi ST được công khai ở thời điểm TOE được chứng nhận.

6.3.2. Lớp AVA

Thử nghiệm chức năng minh bạch không cung cấp bất kỳ thông tin nào về hiệu quả của PAD đối với các loại PAI chưa được thử nghiệm. Việc đánh giá tính dễ bị tổn thương dựa vào việc đánh giá xem việc sử dụng các PAI bổ sung không phải là một phần của loại PAI tiêu chuẩn hoặc các biến thể của PAI từ loại PAI tiêu chuẩn có thể dẫn đến các lỗ hổng có thể khai thác được hay không.

Trong quá trình phân tích lỗ hổng, kiểm thử viên nên sử dụng thông tin và kiến thức thu được trong quá trình đánh giá các lớp đảm bảo khác để thử nghiệm xâm nhập. Bất kỳ thông tin nào được tìm thấy trong các hoạt động đánh giá trước đó sẽ được cung cấp làm đầu vào cho các hoạt động cho các hoạt động đánh giá AVA được mô tả trong tiêu chuẩn này.

Thử nghiệm thâm nhập phụ thuộc vào chuyên môn, kỹ năng và kiến thức của kiểm thử viên về các lỗ hổng PAD tiềm năng, chẳng hạn như xác định các khu vực có thể có lỗ hổng, thăm dò lặp đi lặp lại các khu vực này bằng cách sử dụng các PAI được chuẩn bị đặc biệt, điều chỉnh các PAI và các kỹ thuật trình diễn để cố gắng tìm ra các lỗ hổng, dựa trên các nguồn thông tin công khai và bí mật có sẵn về các lỗ hổng an toàn và PAI. Thử nghiệm thâm nhập được đặc trưng là một hoạt động dựa trên kiến thức, chuyên môn, kỹ năng và chính sửa để xâm nhập vào TOE bằng cách sử dụng các PAI cụ thể mà tiềm năng tấn công được tính toán từ các thông tin liên quan như chuyên môn, nỗ lực, thời gian, chi phí, v.v., mà kiểm thử viên cần để xác định và khai thác các lỗ hổng.

CHÚ THÍCH: Thử nghiệm xâm nhập không thể chứng minh rằng không có lỗ hổng nào tồn tại ngay cả khi nó không phát hiện ra bất kỳ lỗ hổng PAD nào trong TOE.

6.4. Tiêu chí đạt / không đạt

TOE sẽ chỉ vượt qua đánh giá nếu:

- Thủ nghiệm chức năng cho thấy rằng TOE có thể nhận ra các PAI trong phạm vi tỷ lệ lỗi tối đa được nêu trong tài liệu ATE_FUN của TOE; và
- Phân tích lỗi hỏng cho thấy rằng các biến thể riêng của PAI tiêu chuẩn hoặc bất kỳ PAI phi tiêu chuẩn được tạo ra khác do kiểm thử viên thiết kế không dẫn đến các lỗi hỏng với cuộc tấn công ở dưới mức được xem là tiềm năng tấn công.

7. Các hoạt động bổ sung cho TCVN 11386 về thử nghiệm (ATE)

7.1. Cách tiếp cận thử nghiệm đối với PAD

Mục tiêu chính của hoạt động thử nghiệm đối với hệ thống PAD là chứng minh rằng cơ chế PAD có thể phát hiện các cuộc tấn công trinh diện với đủ độ tin cậy. Để đạt được điều này, nhà phát triển phải xác định tốc độ mà tại đó TOE không phát hiện được PAI của một loại PAI nhất định - tỷ lệ phân loại lỗi tấn công trinh diện (APCER) cho loại PAI đó.

Để xác định APCER của cơ chế PAD, nhà phát triển phải chuẩn bị các PAI tiêu chuẩn nếu được cung cấp.

Trong quá trình hoạt động thử nghiệm của họ, các PAI do nhà phát triển chuẩn bị sẽ được trình diễn cho hệ thống PAD và kết quả là quyết định của PAD (tấn công trinh diện được phát hiện / tấn công trinh diện không được phát hiện) sẽ được ghi lại. Nhà phát triển phải chuẩn bị và thử nghiệm bằng cách sử dụng các loại PAI tiêu chuẩn áp dụng cho TOE và có thể mở rộng thử nghiệm để bao gồm các PAI phi tiêu chuẩn.

Để đánh giá liệu cơ chế PAD có hoạt động đầy đủ hay không, các giá trị tối đa cho APCER và định nghĩa cho số lượng tối thiểu các kiểu tấn công và các loại PAI sẽ được xác định trong tài liệu TOE ATE_FUN.

Theo yêu cầu của ATE_IND.2 và ATE_IND.3, kiểm thử viên sẽ lặp lại một tập hợp con các thử nghiệm của nhà phát triển và cũng đưa ra các thử nghiệm của riêng họ để có được sự tin tưởng vào hoạt động thử nghiệm của nhà phát triển. Đối với việc lặp lại các thử nghiệm dành cho nhà phát triển, nhà phát triển phải cung cấp mô tả về PAI của họ cho tổ chức đánh giá. Ngoài ra, tổ chức đánh giá sẽ tạo PAI của riêng họ dựa trên thông tin chi tiết hơn từ tài liệu đầy đủ về các loại PAI tiêu chuẩn được cung cấp. Do đó, sự độc lập và mức độ thay đổi đầy đủ được đưa ra.

APCER tối đa và quy mô thử nghiệm tối thiểu như đã giới thiệu ở trên cũng nên được xem xét cho ATE_IND. Giá trị APCER tối đa sẽ được chỉ định riêng cho mỗi loại PAI và không chỉ cho tập hợp tất cả các PAI đã chuẩn bị.

Tóm lại, nhà phát triển và kiểm thử viên sẽ sử dụng các loại PAI tiêu chuẩn, nếu được cung cấp, làm bộ PAI cơ bản cho các hoạt động thử nghiệm của họ. Bằng cách này, có thể đảm bảo rằng một tập hợp các PAI đại diện được sử dụng để thử nghiệm TOE. Tài liệu về các loại PAI tiêu chuẩn xác định một tập hợp tối thiểu các kiểu tấn công mà mọi hệ thống cho PAD đều có thể phát hiện được. Nó không chỉ xác định các loại PAI mà còn xác định cuộc tấn công che giấu hoặc mạo danh, mức độ giám sát và phương pháp tương tác với thiết bị thu thập cho mỗi PAI. Tài liệu cần được duy trì và phát triển để theo dõi các kịch bản về mối đe dọa đang phát triển cùng với nhu cầu của thị trường và sự phát triển hơn nữa của các hệ thống PAD.

Điều quan trọng cần lưu ý là cách tiếp cận thử nghiệm được mô tả ở đây không đủ để khẳng định rằng cơ chế PAD không thể bị phá vỡ bởi bất kỳ PAI nào khác với những cơ chế được sử dụng để thử nghiệm TOE trong quá trình thử nghiệm chức năng. Khía cạnh này là một phần của phân tích lỗi hỏng an toàn (AVA_VAN) được thảo luận trong Điều 7.

7.2. Các chỉ số cho thử nghiệm PAD

7.2.1. Yêu cầu chung

Bộ tiêu chuẩn ISO/IEC 30107 phân loại các kiểu trình diện dựa trên ý định của người trình diện, tức là các trình diện trung thực và tần công trình diện. Tuy nhiên, các hệ thống PAD thường không thể xác định ý định của người trình diện và các kỹ thuật PAD dựa trên việc đo lường các thuộc tính vật lý và/hoặc hành vi liên quan đến trình diện cộng với sơ đồ quyết định phân loại trình diện là trình diện trung thực hoặc tần công trình diện. Quyết định PAD không hoàn toàn mang tính xác định và các lỗi quyết định có thể xảy ra trong các hệ thống sinh trắc học hoạt động nơi các tần công trình diện bị phân loại nhầm là các trình diện trung thực hoặc các trình diện trung thực bị phân loại nhầm là các cuộc tấn công.

Nhận thức được điều này, ISO/IEC 30107-3 chỉ định một tập hợp các chỉ số PAD bao gồm các chỉ số lỗi được xác định cho các kiểu trình diện trung thực và tấn công.

Các số liệu quy định trong ISO/IEC 30107-3 phải được sử dụng trong tài liệu ADV, thử nghiệm chức năng cho PAD và tài liệu của nó. Các số liệu phù hợp phụ thuộc vào chức năng được cung cấp bởi TOE. Tỷ lệ lỗi được đo bằng các số liệu sẽ được báo cáo độc lập cho mỗi PAI được thử nghiệm.

ISO/IEC 30107-3 cung cấp một số thước đo có thể được sử dụng để thử nghiệm hiệu suất của hệ thống PAD. Điều 6.2 quy định các số liệu của ISO/IEC 30107-3 sẽ được sử dụng cho thử nghiệm PAD. Các số liệu phù hợp phụ thuộc vào chức năng được cung cấp bởi TOE.

7.2.2. Các chỉ số được sử dụng cho các TOE của hệ thống con PAD

Thử nghiệm PAD phải bao gồm các chỉ số APCER, BPCER, APNRR và BPNRR, là bắt buộc. Ngoài ra, thời lượng xử lý của hệ thống con PAD (PS-PD) từ hệ thống con PAD có thể được đo lường và báo cáo dưới dạng thời lượng trung bình. Bảng 1 tóm tắt mối quan hệ giữa tỷ lệ lỗi, kiểu trình diện và phân loại tấn công. Lưu ý rằng hai chỉ số APNRR và BPNRR sẽ được đánh giá trong thời gian xử lý của hệ thống con PAD.

BPCER có thể liên quan đến hiệu suất và khả năng sử dụng của hệ thống vì các sự cố xảy ra có thể gây ra các vấn đề về khả năng sử dụng và sự chậm trễ ảnh hưởng đến những người dùng. Mặc dù đánh giá an toàn TCVN 8709 chủ yếu tập trung vào an toàn hơn là các vấn đề về khả năng sử dụng/hiệu suất, việc thử nghiệm BPCER là cần thiết để xác định xem TOE có phù hợp với mục đích của nó hay không. Vì APCER và BPCER là các chỉ số phụ thuộc và thường được điều chỉnh bằng cách sử dụng các thông số cụ thể, nhà phát triển có thể dễ dàng giảm APCER trong khi tăng BPCER. Điều kiện thử nghiệm BPCER phải giống như điều kiện đối với APCER.

Thử nghiệm tỷ lệ lỗi APCER và BPCER thường không yêu cầu quy mô của nhóm thử nghiệm bình thường để thử nghiệm hiệu suất sinh trắc học vì tỷ lệ lỗi APCER và BPCER cho các hệ thống PAD thường lớn hơn đáng kể so với tỷ lệ lỗi FAR và FRR cho các trình diện trung thực và do đó, thống kê về giới hạn độ không đảm bảo đo liên quan đòi hỏi thấp hơn. Lưu ý rằng, nếu việc thử nghiệm hiệu suất định danh sinh trắc học của TOE với trình diện trung thực cũng là một phần của đánh giá, thì số liệu BPCER có thể được rút ra từ kết quả của thử nghiệm đó và được báo cáo dưới dạng thông tin bổ sung trong tài liệu cho hoạt động ATE_FUN.

CHÚ THÍCH: APCER cho một loại PAI nhất định PAIS được định nghĩa và ký hiệu là APCERPAIS trong ISO/IEC 30107-3.

Bảng 1 - Mối liên quan giữa tỷ lệ lỗi, kiểu trình diện và phân loại tấn công cho hệ thống con PAD

Kiểu trình diện (Đầu vào)	Kết quả PAD (Đầu ra)		
	Tấn công	Trung thực	Không phản hồi
Tấn công	—	APCER	APNRR
Trung thực	BPCER	—	BPNRR
— Đang cân nhắc.			

7.2.3 Các số liệu được sử dụng cho các TOE hệ thống con thu thập dữ liệu

Các chỉ số lỗi được sử dụng là APCER, BPCER, APNRR, BPNRR, APNCR, APAR, FTER và FTAR là bắt buộc. Ngoài ra, thời lượng xử lý hệ thống con thu thập dữ liệu có thể được sử dụng. Bảng 2 tóm tắt mối quan hệ giữa tỷ lệ lỗi, kiểu trình diện và phân loại tấn công. Lưu ý rằng các chỉ số trên phải được đánh giá trong khoảng thời gian của thời lượng xử lý của hệ thống con thu thập dữ liệu.

CHÚ THÍCH: Một hệ thống con thu thập dữ liệu, bao gồm phần cứng hoặc/và phần mềm thu thập, kết hợp các cơ chế PAD và thử nghiệm chất lượng có thể không rõ ràng đối với kiểm thử viên. Do đó, kiểm thử viên có thể không phải lúc nào cũng biết lỗi là kết quả của việc phát hiện ra một cuộc tấn công trình diện hoặc chất lượng không đạt của các đặc điểm sinh trắc học.

Bảng 2 - Mối liên quan giữa tỷ lệ lỗi, kiểu trình diện và phân loại tấn công đối với hệ thống con thu thập dữ liệu

Kiểu trình diện (Đầu vào)	Kết quả PAD (Đầu ra)				
	Tấn công	Trung thực	Không phản hồi	Thu thập thất bại	Thu thập thành công
Tấn công	—	APCER	APNRR	—	APAR
Trung thực	BPCER	—	BPNRR	Ghi nhận	FTER
				Xác minh/ định danh	FTAR
— Đang cân nhắc.					

7.2.4. Các thước đo được sử dụng cho các TOE

Các TOE khác tương ứng với trường hợp thứ ba trong TCVN 14190-1:2024, 5.3.2. Một TOE như vậy chứa ít nhất các hệ thống con đối sánh và quyết định để xác minh hoặc định danh sinh trắc học. Loại TOE này bao gồm một hệ thống đầy đủ. Đánh giá PAD đối với một TOE thuộc loại này, ngay cả khi bản thân TOE không phải là một hệ thống đầy đủ, sẽ được thực hiện đối với một hệ thống đầy đủ bổ sung cho các thành phần khác của TOE, nếu có, trong đó các thành phần khác sẽ được chỉ rõ trong ST.

Khi mà TOE dành cho xác minh sinh trắc học, các chỉ số là FNMR, FMR, IAPMR dành cho giả mạo sinh trắc học và CAPNMR dành cho che dấu sinh trắc học. Khi TOE là để từ chối nhận dạng, các số liệu là FPIR và IAPIR. Khi TOE là để chấp thuận nhận dạng, các số liệu là FNIR và CAPNIR. Tất cả các chỉ số này là bắt buộc (xem ISO/IEC 19795-1 về FNMR, FMR, FNIR và FPIR). Ngoài ra, thời lượng xử lý toàn bộ hệ thống được tùy chọn sử dụng. Các chỉ số bắt buộc phải được đánh giá trong khoảng thời gian của thời lượng xử lý toàn bộ hệ thống. Bảng 3 và Bảng 4 tóm tắt mối quan hệ giữa tỷ lệ lỗi, kiểu trình diện và phân loại tấn công.

Nếu che giấu tạo ra sự trùng khớp với một đối tượng khác, nó sẽ được coi là một trùng khớp của kẻ mạo danh.

CHÚ THÍCH 1: Nếu TOE xuất kết quả của PAD ngoài quyết định theo một cách nào đó, APCER và BPCER có thể được sử dụng.

Bảng 3 - Mối liên quan giữa tỷ lệ lỗi, kiểu trình diện và phân loại tấn công cho hệ thống xác minh sinh trắc học đầy đủ

Kiểu trình diện (Đầu vào)		Quyết định (Đầu ra)	
		Phù hợp	Không phù hợp
PAI (đặc điểm sinh trắc học tự nhiên / đồ tạo tác)	Tấn công trình diện	Kẻ giả mạo	IAPMR
		Che giấu	—
		Kẻ mạo danh	FMR
Đặc điểm sinh trắc học tự nhiên	Trình diện trung thực	Thành thật	FNMR
	—	—	—
— Đang cân nhắc.			

CHÚ THÍCH 2: Cột cuối cùng thể hiện quyết định và tỷ lệ lỗi liên quan.

Bảng 4 - Mối liên quan giữa tỷ lệ lỗi, kiểu trình diện và phân loại tấn công cho hệ thống định danh sinh trắc học đầy đủ

Hệ thống	Kiểu trình diện (Đầu vào)	Quyết định (Đầu ra)	
		Ứng viên	Không phải ứng viên
Định danh tích cực	Tấn công	IAPIR	—
	Trung thực	FPIR	—
Định danh tiêu cực	Tấn công	—	CAPNIR
	Trung thực	—	FNIR
— Đang cân nhắc.			

7.3. Quy mô thử nghiệm tối thiểu và tỷ lệ lỗi tối đa

Các yêu cầu về quy mô thử nghiệm đối với thử nghiệm PAD phụ thuộc vào độ lớn của tỷ lệ lỗi được đo và giới hạn lỗi có thể chấp nhận được đối với kết quả thử nghiệm. Khi tỷ lệ lỗi và giới hạn lỗi có thể chấp nhận được giảm xuống, các cân nhắc thống kê yêu cầu quy mô thử nghiệm tăng lên.

Đối với thử nghiệm PAD, các PAI khác nhau đại diện cho các loại PAI và kiểu tấn công phải được thử nghiệm và kết quả sẽ được báo cáo cho từng loại PAI và kiểu tấn công. Quy mô thử nghiệm phải được đánh giá cho từng loại PAI và kiểu tấn công.

Mục đích của thử nghiệm chức năng là để đánh giá rằng PAD đang hoạt động bình thường trên TOE.

Do đó, tất cả các PAI tiêu chuẩn hoặc PAI phi tiêu chuẩn đều không được sử dụng trong thử nghiệm chức năng. Kiểm thử viên nên điều tra các PAI có thể có khác trong AVA. Số lượng loại PAI tối thiểu, quy mô thử nghiệm tối thiểu và tỷ lệ lỗi tối đa để thử nghiệm chức năng có thể được xác định trong các loại PAI tiêu chuẩn hoặc trong hướng dẫn đánh giá của hồ sơ bảo vệ được xem xét. Nếu bất kỳ khuyến nghị nào từ tổ chức chứng nhận được đưa ra, kiểm thử viên nên xem xét các khuyến nghị đó để xác định quy mô thử nghiệm thích hợp cho mỗi loại PAI. Nếu chúng không được xác định, kiểm thử viên sẽ sử dụng ít nhất 10 mẫu khác nhau cho mỗi loại PAI được xem xét. Số lượng loại PAI tối thiểu, quy mô thử nghiệm tối thiểu và tỷ lệ lỗi tối đa cho thử nghiệm chức năng phải được thỏa thuận giữa nhà phát triển và kiểm thử viên. Quy mô thử nghiệm tối thiểu cho mỗi loại PAI phải là 10. Tỷ lệ lỗi tối đa (APCER) cho mỗi loại PAI không được lớn hơn 0,1.

Kiểm thử viên cũng nên xem xét các khuyến nghị từ các tiêu chuẩn quốc tế khác hoặc các tiêu chuẩn phi quốc tế cho các trường hợp sử dụng cụ thể. Ví dụ, trong trường hợp hệ thống sinh trắc học di động, kiểm thử viên nên sử dụng làm cơ sở các khuyến nghị được đưa ra trong ISO/IEC 30107-4 về số lượng các loại PAI khác nhau và quy mô thử nghiệm.

8. Các hoạt động bổ sung cho TCVN 11386 về đánh giá lỗ hổng (AVA)

8.1. Thủ nghiệm thâm nhập bằng cách sử dụng các biến thể PAI

Ngược lại với thủ nghiệm chức năng, kiểm thử viên nên xem xét các khía cạnh cụ thể của TOE trong bối cảnh thử nghiệm thâm nhập. Kiểm thử viên sẽ sử dụng thông tin thu được từ việc đánh giá các lớp đảm bảo khác như ADV để tìm ra các lỗ hổng tiềm năng trong thiết kế hoặc triển khai TOE. Với kết quả của các phân tích, kiểm thử viên phải xác định các kiểu tấn công có khả năng phá vỡ cơ chế PAD của TOE. Kiểm thử viên phải tìm kiếm vật liệu, vật liệu tổng hợp và kỹ thuật có thể được sử dụng để tạo PAI có thể đánh bại các cơ chế PAD của TOE. Kiểm thử viên sẽ thử các PAI ứng viên có liên quan đến mức tiềm năng tấn công được chỉ định đối với TOE đang tìm kiếm các phân loại trình diện sai. Nếu xảy ra phân loại sai, kiểm thử viên phải ghi lại tất cả các chi tiết liên quan của PAI và số lượng phân loại đúng trước đó cho PAI trước khi phân loại sai xảy ra. Các thủ nghiệm sử dụng cùng một PAI sẽ tiếp tục tìm kiếm cho đến khi phát hiện thêm các phân loại sai khác hoặc kiểm thử viên hài lòng rằng các trường hợp phân loại sai không thể lặp lại một cách dễ dàng. Không có quy tắc cố định nào có thể được đưa ra về lượng thời gian nên dành cho một đánh giá điển hình bởi một kiểm thử viên có năng lực. Tuy nhiên, theo hướng dẫn, thời gian dành cho hoạt động này đối với AVA_VAN.1 sẽ là khoảng 1 tuần, trong khi đó phải là khoảng 2 tháng đối với AVA_VAN.5.

Một nguồn thông tin khác về các kiểu tấn công có liên quan được tạo ra để thử nghiệm thâm nhập là thử nghiệm chức năng. Thủ nghiệm chức năng có thể tiết lộ rằng các PAI cụ thể hoặc các kiểu tấn công dẫn đến tỷ lệ lỗi PAD cao hơn bình thường đối với TOE. Các PAI/kiểu tấn công này có thể là ứng viên để khám phá thêm như một phần của thử nghiệm thâm nhập. Ngay cả khi thử nghiệm chức năng không tiết lộ rằng các PAI cụ thể hoặc các kiểu tấn công dẫn đến tỷ lệ lỗi PAD cao hơn bình thường đối với TOE, có thể có các PAI/biến thể/kiểu tấn công khác nhau có thể phá vỡ cơ chế PAD của TOE trong thử nghiệm thâm nhập giai đoạn đánh giá.

Thử nghiệm thâm nhập trong phân tích lỗ hổng có một khía cạnh sáng tạo. Hiệu quả của một cuộc tấn công trình diện phụ thuộc vào việc chuẩn bị các PAI và trình diện của chúng. Trong trường hợp PAI đầu vân tay, vật liệu được sử dụng ảnh hưởng đến sự thành công của một cuộc tấn công cũng như các chi tiết trình diện như nhiệt độ và độ dày của PAI và việc bôi trơn bề mặt của nó bằng nước hoặc dầu. Đối với các phương thức như khuôn mặt, mống mắt và giọng nói, các yếu tố ảnh hưởng khác có thể bao gồm tốc độ lấy mẫu, độ phân giải video, tốc độ khung hình, không gian màu và kích thước vật lý được sử dụng để tạo PAI. Kiểm thử viên nên xây dựng và duy trì mức độ cẩn thận của kỹ năng chuẩn bị và trình diện thông qua sự kết hợp của việc giám sát phạm vi xung quanh và thông tin khác về các cuộc tấn công trình diện chống lại hệ thống sinh trắc học và đào tạo và thử nghiệm thực tế.

Kiểm thử viên phải xác định cách tiếp cận để thử nghiệm xâm nhập, điều tra bất kỳ lỗ hổng tiềm năng nào đã được xác định cho TOE, và thu thập hoặc chuẩn bị các PAI phù hợp. Trong quá trình thử nghiệm xâm nhập, kiểm thử viên phải trình diện tất cả các PAI đã chuẩn bị cho TOE nhiều lần bằng cách sử dụng các biến thể trình diện phù hợp. Nếu không tìm thấy PAI nào có thể phá vỡ hệ thống con PAD, kiểm thử viên có thể kết luận rằng TOE có khả năng chống lại các PAI này.

Nếu một TOE không phát hiện được một PAI được trình diện trong quá trình đánh giá tính dễ bị tổn thương, thì TOE được chứng minh là dễ bị tổn thương đối với PAI/trình diện và do hàm ý đối với PAI/trình diện khác. Kiểm thử viên nên tìm cách tái tạo lỗ hổng để có thể ước tính độ khó của việc tái tạo nó. Các hạn chế thực tế như thời gian và sự thay đổi có thể có nghĩa là độ tái lập chỉ có thể được ước tính trên một mức độ khó bình thường (ví dụ: dễ, khó vừa phải, rất khó). Mức độ khó tái tạo lỗ hổng là một yếu tố để xác định rủi ro liên quan đến việc sử dụng TOE trong một kịch bản ứng dụng và trong việc tính toán tiềm năng tấn công. APCER cho một loại PAI trong thử nghiệm chức năng có thể được sử dụng để thông báo cho thử nghiệm xâm nhập, ví dụ để làm nổi bật các loại PAI mà TOE có thể dễ bị tấn công để điều tra thêm trong tương lai.

Lưu ý rằng một số kịch bản tấn công có thể không cần được thử nghiệm xâm nhập hoàn toàn nếu tiềm năng tấn công được yêu cầu của kịch bản tấn công cao hơn điều được chỉ định bởi thành phần AVA_VAN của TOE. Tiềm năng tấn công đối với một cuộc tấn công sử dụng PAI chống lại cơ chế PAD của TOE sẽ được tính toán theo hướng dẫn trong Phụ lục D. TCVN 14190-1:2024. Các ví dụ được cung cấp trong Phụ lục A.

TCVN 14190-1:2024, C.1, cung cấp thông tin về các lỗ hổng TOE tiềm năng khác và hướng dẫn về thử nghiệm xâm nhập nếu có thể áp dụng cho một TOE cụ thể.

8.2 Các lỗ hổng tiềm năng

Các lỗ hổng mà kiểm thử viên ít nhất phải xem xét đến được mô tả trong TCVN 14190-1:2024, 5.1. Ngoài ra, kiểm thử viên nên xem xét sự kết hợp của các lỗ hổng đó với các lỗ hổng khác liên quan đến CNTT.

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

Đánh giá phải được thực hiện theo TCVN 14190-1:2024, F.1.5, cũng như việc xem xét tiềm năng tấn công (xem TCVN 14190-1:2024, F.1.2). Các ví dụ liên quan đến lỗ hổng PAD được cung cấp trong Phụ lục A.

PHỤ LỤC A

(tham khảo)

Các ví dụ về tính toán tiềm năng tấn công**A.1. Yêu cầu chung**

Phụ lục này cung cấp một số ví dụ bao gồm các hệ thống khác nhau có thể được đánh giá (thiết bị kiểm soát truy cập cho một tòa nhà, văn phòng, v.v., kiểm soát truy cập vào thiết bị cá nhân, v.v.) và các cuộc tấn công "cố ý" có thể được áp dụng. Tham khảo TCVN 14190-1:2024, D.1.2 và TCVN 11386:2008, B.4.

A.2. Ví dụ 1 - Hệ thống đơn giản không có phát hiện tấn công trinh diện

Hai ví dụ được đánh giá ở đây, hệ thống định danh khuôn mặt 2D và dựa trên dấu vân tay, không cần giám sát và không có bất kỳ hạn chế nào để truy cập TOE. Sự khác biệt về các yếu tố chỉ là khả năng tiếp cận các đặc điểm sinh trắc học.

Các vấn đề sau đây được xem xét:

- Thời gian đã trôi qua: 1 ngày là đủ để xác định phương pháp xây dựng kiểu tấn công (định danh) và tạo PAI nhắm vào đối tượng được chọn (khai thác). Đối với hình ảnh 2D, chỉ cần in một bức hình đơn giản là đủ, đối với dấu vân tay, việc đúc bằng vật liệu dễ lấy (keo, silicon, cao su, v.v.) là hiệu quả.

- Chuyên môn: Rất nhiều cách giải thích phương thức thực hiện. Không yêu cầu chuyên môn cụ thể (người bình thường là đủ).

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

- Kiến thức về TOE: Không yêu cầu kiến thức cụ thể về TOE.

- Cơ hội (truy cập vào TOE): Không có vấn đề gì khi truy cập vào TOE cả trong định danh (dễ dàng mua được mà không bị kiểm soát) hoặc khai thác (một dấu vân tay PAI dễ xuất hiện: ví dụ bằng cách "dán" PAI vào ngón tay thật, đối với khuôn mặt 2D, hình ảnh được hiển thị trước máy ảnh).

- Cơ hội (tiếp cận các đặc điểm sinh trắc học): Mức độ là Ngay lập tức cho khuôn mặt 2D và Dễ dàng cho dấu vân tay.

- Thiết bị: Không có yêu cầu cụ thể về thiết bị.

Bảng A.1 - Tính toán tiềm năng tấn công cho ví dụ 1 (mặt 2D)

Thời gian cần sử dụng		Chuyên môn		Kiến thức về TOE		Cơ hội				Trang thiết bị		Tổng cộng	
						Truy cập vào TOE		Tiếp cận các đặc điểm sinh trắc học				0	
Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp
0	0	0	0	0	—	0	0	—	0	0	0	0	0

Bảng A.2 - Tính toán tiềm năng tấn công cho ví dụ 1 (Vân tay)

Thời gian cần sử dụng	Chuyên môn	Kiến thức về TOE	Cơ hội				Trang thiết bị		Tổng cộng		
			Truy cập vào TOE		Tiếp cận các đặc điểm sinh trắc học		2				
Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp
0	0	0	0	0	—	0	0	—	2	0	0

Như trong Bảng A.1 và Bảng A.2, tiềm năng tấn công của kiều tấn công là cơ bản.

Hệ thống không thành công ở bất kỳ mức độ đánh giá nào giả định rằng cuộc tấn công được mô tả có thể được thực hiện thành công.

A.3 Ví dụ 2 - Dấu vân tay có phát hiện tấn công trình diện

Hệ thống này thường là một hệ thống kiểm soát truy cập trong một môi trường mờ. Có thể trình diện liên tiếp nhưng hành vi "bất thường" của người dùng sẽ bị phát hiện.

Hệ thống bao gồm PAD tìm vật liệu phù hợp để tạo ra kiều tấn công (ví dụ như glycerine, gelatin) và việc áp dụng lên ngón tay thật không phải ngay lập tức (màng mỏng, để lại một phần da tiếp xúc với thiết bị thu thập, in băng mực trực tiếp trên ngón tay thật, v.v.).

Các vấn đề sau đây được xem xét:

- Thời gian cần sử dụng: Việc tìm kiếm tài liệu phù hợp cho kiều tấn công trình diện với hệ thống là không rõ ràng và cần phải trình diện liên tiếp. Theo ví dụ thực tế cần 2 tuần để xác định. Sau khi được xác định, việc sản xuất PAI cho một người được chia và áp dụng phương pháp được xác định trước cho TOE thực là ngay lập tức (1 ngày để khai thác).

- Chuyên môn: Rất nhiều sản phẩm giải thích cách thực hiện. Tuy nhiên, kẻ tấn công phải hiểu (và thậm chí phải tìm) nguyên tắc của PAD là gì, và tìm ra một chiến lược cụ thể cho cả việc tạo PAI và áp dụng nó. Mức độ thành thạo để xác định là thực tiễn, để khai thác một người bình thường là đủ (theo một kịch bản).

- Kiến thức về TOE: Giả định rằng không có kiến thức cụ thể nào được yêu cầu. Sự tồn tại của PAD có thể đã được phổ biến (hoặc bởi nhà phát triển hoặc người dùng). Với một thời gian, kẻ tấn công (có mức độ thành thạo, biết những gì được cung cấp bởi các hệ thống công nghiệp) có thể sẽ tìm thấy dựa trên phương pháp phát hiện này.

- Cơ hội (truy cập vào TOE): Là một hệ thống an toàn, giả định rằng không thể đơn giản mua hệ thống này mà không có bất kỳ sự kiểm soát nào, nhưng việc phân phối được kiểm soát (ví dụ bằng cách yêu cầu xác định người mua và có khả năng ký một thỏa thuận không tiết lộ). Mức độ là vừa phải được điều chỉnh cho giai đoạn định danh và giai đoạn khai thác (phát hiện một hành vi bất thường).

- Cơ hội (tiếp cận các đặc điểm sinh trắc học): Mức độ dễ dàng.

- Trang thiết bị: Không có yêu cầu cụ thể về thiết bị.

Bảng A.3 - Tính toán tiềm năng tấn công cho ví dụ 2

Thời gian trôi qua		Chuyên môn		Kiến thức về TOE		Cơ hội				Trang thiết bị		Tổng cộng	
						Truy cập vào TOE		Tiếp cận các đặc điểm sinh trắc học					
Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp
2	0	0	2	0	—	2	4	—	2	0	0	4	8

Như được trình diện trong Bảng A.3, tiềm năng tấn công của cuộc tấn công đạt nâng cao cơ bản.

Nếu cuộc tấn công có thể được thực hiện thành công và không tìm thấy cuộc tấn công thành công nào khác với tiềm năng tấn công thấp hơn, thì khả năng chống chịu của TOE đạt cơ bản.

Hệ thống tương thích với thành phần AVA VAN.2.

CHÚ THÍCH Tiềm năng tấn công của cuộc tấn công gần với giới hạn giữa cơ bản và cơ bản nâng cao. Điều này có nghĩa là bất kỳ sự cắt giảm nào, ví dụ như ít thời gian hơn trong việc xác định, không có quyền kiểm soát trong việc phân phối hệ thống (chuyển từ trung bình sang dễ dàng trong cơ hội (Truy cập của TOE), trong một môi trường hoàn toàn không được giám sát, có thể làm giảm cuộc tấn công tiềm năng của cuộc tấn công thành cơ bản và sau đó giảm sức phòng chống của hệ thống thành "Không có xếp hạng".

A.4 Ví dụ 3 - Dấu vân tay với tính năng phát hiện tấn công trình diện nâng cao

Hệ thống này thường là một hệ thống kiểm soát truy cập trong một môi trường mở. Có thể thử một số lần nhưng hành vi "bất thường" của người dùng sẽ bị phát hiện.

Hệ thống bao gồm một hệ thống con PAD hiện đại. Nâng cao có nghĩa là nếu không có kiến thức chi tiết, không thể tìm thấy trong một thời gian hợp lý phương pháp để thực hiện các kiểu tấn công không bị phát hiện (nhiều phương pháp phát hiện, cần một chiến lược trình diện cụ thể). Ngoài ra, không có thông tin chi tiết nào có thể được tìm thấy trên phạm vi công cộng, cũng như giải thích cho người mua. Điều này cũng được coi là hệ thống chỉ được bán cho những người dùng được xác định rõ ràng, theo thỏa thuận không tiết lộ.

Các việc sau đây được xem xét.

- Thời gian cần sử dụng: Việc tìm kiếm tài liệu phù hợp cho kiểu tấn công trình diện với hệ thống là không rõ ràng và sẽ cần nhiều lần thử. Theo thực tế cần 1 tháng để xác định. Sau khi được xác định, việc sản xuất PAI cho đối tượng được chọn và áp dụng phương pháp được xác định trước cho TOE thực là ngay lập tức (1 ngày để khai thác).

- Chuyên môn: Chiến lược của PAD không được mô tả trong phạm vi công cộng, các biện pháp chi tiết được giữ bí mật và một chiến lược cụ thể để tạo ra PAI và trình diện nó chắc chắn đã được tạo ra. Trình độ chuyên gia để xác định là thực tiễn, để khai thác cần một người thành thạo là đủ (theo một kịch bản, nhưng áp dụng một chiến lược phức tạp đòi hỏi kiến thức và hiểu biết tốt về cơ chế PAD).

- Kiến thức về TOE: Nếu không có kiến thức chi tiết về các cơ chế PAD, xác định rằng không thể trong một thời gian hợp lý để tạo ra một PAI được chấp nhận. Thông tin này được bảo vệ và cần có sự thỏa hiệp. Vì vậy, cần phải có kiến thức nhạy bén.

- Cơ hội (truy cập vào TOE): Là một hệ thống an toàn, giả định rằng không thể đơn giản mua hệ thống mà không có bất kỳ sự kiểm soát nào, nhưng việc phân phối nó được kiểm soát (ví dụ bằng cách yêu cầu xác định người mua và có khả năng ký một thỏa thuận không tiết lộ). Giả định rằng việc bảo vệ hiệu quả hơn trong ví dụ trước, vì vậy một mức độ khó có thể được điều chỉnh cho giai đoạn định danh. Đối với việc khai thác, quyền truy cập của TOE được đánh giá ở mức trung bình.

- Cơ hội (tiếp cận các đặc điểm sinh trắc học): Mức độ dễ dàng.

- Trang thiết bị: Không có yêu cầu cụ thể về thiết bị.

Bảng A.4 - Tính toán tiềm năng tấn công cho ví dụ 3

Thời gian qua		Chuyên môn	Kiến thức về TOE		Cơ hội				Trang thiết bị		Toàn bộ		
					Truy cập vào TOE		Tiếp cận các đặc điểm sinh trắc học				26		
Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp
4	0	4	4	4	—	4	4	—	2	0	0	16	10

Như được trình diện trong Bảng A.4, tiềm năng tấn công của cuộc tấn công là vừa phải.

Nếu cuộc tấn công có thể được thực hiện thành công và không tìm thấy cuộc tấn công thành công nào khác với tiềm năng tấn công thấp hơn, thì khả năng chống chịu của TOE đạt nâng cao cơ bản.

Hệ thống tương thích với thành phần AVA VAN.3.

CHÚ THÍCH: Một phần đáng kể của tiềm năng tấn công được tính toán là do các biện pháp phi kỹ thuật [kiến thức về TOE, cơ hội (truy cập vào TOE)]. Điều này có nghĩa, nếu các biện pháp như vậy không được thực hiện, thì khả năng chống chịu của TOE cần được chuyển xuống mức cơ bản.

A.5 Ví dụ 4 - Khuôn mặt 3D với tính năng phát hiện tấn công trình diện và bộ đếm số lần thử

Ví dụ này dành cho hệ thống dựa trên khuôn mặt 3D với PAD (tương đối đơn giản), nhưng hệ thống này khó phát hiện với cơ hội lớn hơn 10% và bộ đếm số lần thử làm tăng cảnh báo (và kích hoạt một số hành động khác phục tiếp theo) khi hơn 3 cuộc tấn công trình diện đã được phát hiện trong một loạt các lần thử mà không có bất kỳ sự chấp nhận thành công nào. Hệ thống này thường là một hệ thống kiểm soát truy cập trong một môi trường mở. Hệ thống bao gồm PAD tìm vật liệu phù hợp để chế tạo khuôn mặt.

Các việc sau đây được xem xét.

- Thời gian cần sử dụng: Việc tìm kiếm tài liệu phù hợp cho khuôn mặt và cách trình diện nó với hệ thống là không rõ ràng và cần nhiều lần thử. Theo ví dụ thực tế cần 1 tháng để xác định. Sau khi được xác định, việc sản xuất PAI cho người được chọn và áp dụng phương pháp được xác định trước cho TOE thực là ngay lập tức (1 ngày để khai thác).

- Chuyên môn: Một số sản phẩm có thể giải thích cách thực hiện. Tuy nhiên, để xác định phải hiểu (và thậm chí phải tìm) nguyên tắc của PAD là gì, và tìm ra một chiến lược cụ thể cho cả việc tạo PAI và áp dụng nó. Định danh thành thạo là mức độ cần thiết tối thiểu, để khai thác người bình thường là đủ (theo một tập lệnh).

- Kiến thức về TOE: Giả định rằng cần phải có kiến thức bị giới hạn về TOE để hiểu những gì được sử dụng cho PAD trong trường hợp hệ thống 3D.

- Cơ hội (truy cập vào TOE): Là một hệ thống an toàn, giả định rằng không thể đơn giản mua hệ thống mà không có bất kỳ sự kiểm soát nào, nhưng việc phân phối nó được kiểm soát (ví dụ bằng cách yêu cầu xác định người mua và có khả năng ký một thỏa thuận không tiết lộ). Mức độ vừa phải có thể được điều chỉnh cho giai đoạn xác định. Để khai thác, việc truy cập vào TOE được đánh giá là khó khăn do bộ đếm số lần thử.

- Cơ hội (tiếp cận các đặc điểm sinh trắc học): Mức độ vừa phải.
- Thiết bị: Có thể có thiết bị cụ thể cần thiết để sản xuất 3D PAI trong quá trình xác định và khai thác.

Bảng A.5 - Tính toán tiềm năng tấn công cho ví dụ 4

Thời gian qua		Chuyên môn		Kiến thức về TOE		Cơ hội				Trang thiết bị		Toàn bộ	
						Truy cập vào TOE		Tiếp cận các đặc điểm sinh trắc học					
Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp
4	0	2	0	2	—	2	8	—	4	2	4	12	16

Như được trình diện trong Bảng A.5, tiềm năng tấn công của cuộc tấn công là vừa phải.

Nếu cuộc tấn công có thể được thực hiện thành công và không tìm thấy cuộc tấn công thành công nào khác với tiềm năng tấn công thấp hơn, thì khả năng chống chịu của TOE được nâng cao cơ bản.

Hệ thống tương thích với thành phần AVA VAN.3.

A.6 Ví dụ 5 - tấn công Wolf

VÍ DỤ đối với một hệ thống sinh trắc học cho một phương thức nhất định, hoạt động trong một môi trường hoàn toàn không được kiểm soát (ví dụ: bảo vệ quyền truy cập vào một thiết bị hoặc một dụng cụ). Giả sử rằng nó là một hệ thống hoàn toàn dựa trên phần mềm, do đó nó dễ dàng kết nối máy tính ngay trước trình giải nén tính năng. Cũng giả định rằng có một lỗ hổng trong thuật toán đối sánh để có một cách tạo ra một hình ảnh (không nhất thiết phải đại diện cho việc thu thập sinh trắc học) mà tỷ lệ chấp nhận cao hơn đáng kể so với bất kỳ dữ liệu sinh trắc học được chọn ngẫu nhiên nào, bất kể dữ liệu được đăng ký là gì. Điều này tương ứng với một hệ thống có tỷ lệ tấn công thành công cao. Cuộc tấn công bao gồm việc tìm ra (hoặc một trong số) hình ảnh cụ thể dẫn đến cơ hội được chấp nhận cao.

Các việc sau đây được xem xét:

Giai đoạn định danh tương ứng với việc tìm ra lỗ hổng trong thuật toán đối sánh và do đó để tạo ra một hình ảnh khai thác lỗ hổng này. Giai đoạn khai thác chỉ là nhập hình ảnh để có quyền truy cập.

CHÚ THÍCH Có rất ít người có đặc điểm sinh trắc học đặc biệt hiếm có với các đặc điểm trên. Những đặc điểm sinh trắc học đặc biệt như vậy được gọi là Human Wolves.

- Thời gian cần sử dụng: Có thể cần hơn một tháng để định danh trong khi khai thác là ngay lập tức.

- Chuyên môn: Cần có chuyên gia tấn công để tìm ra lỗ hổng trong thuật toán. Một người bình thường có thể nhập hình ảnh sau khi được tạo.

- Kiến thức về TOE: Cần phải có kiến thức nhạy cảm của TOE để tìm hiểu chi tiết về thuật toán so trùng khớp.

- Cơ hội (truy cập vào TOE): TOE hoạt động trong một môi trường hoàn toàn không được kiểm soát.

- Cơ hội (tiếp cận các đặc điểm sinh trắc học): Được đánh giá là ngay lập tức vì không cần truy cập cho cuộc tấn công.

- Thiết bị: Có thể cần một thiết bị cụ thể để tạo ra hình ảnh, có thể chấp nhận được đổi với tính năng trích xuất.

Bảng A.6 - Tính toán tiềm năng tấn công cho ví dụ 5

Thời gian qua		Chuyên Môn		Kiến thức về TOE		Cơ hội				Trang thiết bị		Toàn bộ	
						Truy cập vào TOE		Tiếp cận các đặc điểm sinh trắc học				18	
Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp
8	0	4	0	4	—	0	0	—	0	2	0	18	0

Như thể hiện trong Bảng A.6, tiềm năng tấn công của cuộc tấn công là: tăng cường-cơ bản.

Nếu cuộc tấn công có thể được thực hiện thành công và không tìm thấy cuộc tấn công thành công nào khác với tiềm năng tấn công thấp hơn, thì khả năng chống chịu của TOE là cơ bản.

Hệ thống tương thích với thành phần AVA VAN.2.

Thư mục tài liệu tham khảo

- [1] ISO/IEC 2382-37:2017, Information technology — Vocabulary — Part 37: Biometrics
- [2] TCVN 8709-1:2011, 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
- [3] TCVN 11385:2016 (ISO/IEC 19792:2009) về Công nghệ thông tin - Các kỹ thuật an toàn - Đánh giá an toàn sinh trắc học
- [4] ISO/IEC 19795-1:2006, Information technology — Biometric performance testing and reporting — Part 1: Principles and framework
- [5] ISO/IEC 30107-1:2016, Information technology — Biometric presentation attack detection — Part 1: Framework
- [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] Tekampe N., Merle A., Bringer J., Gomez-Barrero M., Fierrez J., Galbally J., D6.5: Towards the Common Criteria evaluations of biometric systems, March 2016
- [13] 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)