

TCVN

TIÊU CHUẨN QUỐC GIA

TCVN 14190-2:2024

ISO/IEC 19989-2:2020

Xuất bản lần 1

**AN TOÀN THÔNG TIN - TIÊU CHÍ VÀ PHƯƠNG PHÁP
LUẬN ĐÁNH GIÁ AN TOÀN HỆ THỐNG SINH TRẮC HỌC -
PHẦN 2 : HIỆU SUẤT NHẬN DẠNG SINH TRẮC HỌC**

Information security - Criteria and methodology for assessing the security of biometric systems - Part 2: Biometric recognition performance

HÀ NỘI – 2024

Mục lục

Lời nói đầu	4
Giới thiệu.....	5
1 Phạm vi áp dụng	7
2 Tài liệu viện dẫn	7
3 Thuật ngữ và định nghĩa	8
4 Ký hiệu và thuật ngữ viết tắt.....	10
5 Các hoạt động bổ sung cho TCVN 11386 (ISO/IEC 18045) về các thử nghiệm ATE	10
5.1 Yêu cầu chung	10
5.2 Lập kế hoạch đánh giá	18
5.3 Thu thập dữ liệu	20
5.4 Phân tích	22
5.5 Xem xét các thử nghiệm của nhà phát triển.....	23
5.6 Yêu cầu cụ thể về các thành phần đảm bảo trên ATE_IND	23
5.7 Đánh giá các thử nghiệm của nhà phát triển bằng cách lặp lại một tập con thử nghiệm.....	25
5.8 Tiến hành thử nghiệm độc lập	26
6 Các hoạt động bổ sung cho TCVN 11386 (ISO/IEC 18045) về đánh giá tính dễ bị tổn thương (AVA).....	28
6.1 Các khía cạnh chung.....	28
6.2 TOE để thử nghiệm.....	29
6.3 Các lỗi hỏng tiềm năng.....	29
6.4 Đánh giá khả năng tấn công.....	30
PHỤ LỤC A (tham khảo) Ví dụ về tính toán tiềm năng tấn công cho các hoạt động AVA	31
PHỤ LỤC B (tham khảo) Ví dụ cho các hoạt động ATE	38
PHỤ LỤC C (tham khảo) Ví dụ về tài liệu thử nghiệm hiệu suất của nhà phát triển và chiến lược đánh giá của nó.....	41
Thư mục tài liệu tham khảo.....	46

Lời nói đầu

TCVN 14190-2:2024 hoàn toàn tương đương với ISO/IEC 19989-2:2020.

TCVN 14190-2:2024 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.

TCVN 14190-1 bao gồm việc giới thiệu khuôn khổ chung để đánh giá an toàn của hệ thống sinh trắc học, bao gồm các thành phần chức năng an toàn mở rộng và phương pháp luận bổ sung, là các hoạt động đánh giá bổ sung cho kiểm thử viên. Các khuyến nghị chi tiết được phát triển cho các khía cạnh hiệu suất nhận dạng sinh trắc học trong tiêu chuẩn này và cho các khía cạnh phát hiện tấn công trình diện trong TCVN 14190-3.

Tiêu chuẩn này mô tả các bổ sung cho phương pháp đánh giá để đánh giá hiệu suất nhận dạng sinh trắc học để đánh giá tính an toàn của các sản phẩm sinh trắc học. Nó bổ sung cho loạt TCVN 8709, TCVN 11386 và TCVN 14190-1. Nó được xây dựng dựa trên các cân nhắc chung được mô tả trong TCVN 11385 và phương pháp kiểm tra hiệu suất sinh trắc học được mô tả trong ISO/IEC 19795-1 bằng cách cung cấp hướng dẫn bổ sung cho người đánh giá.

Trong tiêu chuẩn này, thuật ngữ "chủ thể dữ liệu" được sử dụng thay cho thuật ngữ "người dùng" được sử dụng trong TCVN 14190-1, để phù hợp với từ vựng sinh trắc học, vì các chuyên gia về sinh trắc học phải là đọc giả chính của tiêu chuẩn này.

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

Information security – Criteria and methodology for security evaluation of biometric systems – Part 2 : Biometric recognition performance

1 Phạm vi áp dụng

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 hiệu suất nhận dạng sinh trắc học áp dụng bộ tiêu chuẩn TCVN 8709 (ISO/IEC 15408).

Tiêu chuẩn này cung cấp các yêu cầu và khuyến nghị cho nhà phát triển và kiểm thử viên về các hoạt động bổ sung về hiệu suất nhận dạng sinh trắc học được quy định trong TCVN 14190-1 (ISO/IEC 19989-1).

Việc đánh giá các kỹ thuật phát hiện tấn công trình diện nằm ngoài phạm vi của tiêu chuẩn này ngoại trừ đối với trình diện từ các nỗ lực mạo danh theo chính sách về mục đích sử dụng theo tài liệu hướng dẫn TOE.

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 8709-3:2011 (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 bảo đảm 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

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

TCVN 14190-1:2024 (ISO/IEC 19989-1:2020), An toàn thông tin – Tiêu chí và phương pháp luận đánh giá an toàn hệ thống sinh trắc học - Phần 1: Khung

ISO/IEC 2382:2015, Information technology - Vocabulary

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

ISO/IEC 19795-1:2006, Information technology - Biometric performance testing and reporting - Part 1: Principles and framework

ISO/IEC 19795-2:2007, Information technology - Biometric performance testing and reporting - Part 2: Testing methodologies for technology and scenario evaluation

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 nêu trong ISO/IEC 2382-37:2017, ISO/IEC 2382:2015, TCVN 8709-1:2011, TCVN 11386:2016, ISO/IEC 30107-3:2017 và các thuật ngữ, định nghĩa sau:

3.1

trình diện trung thực (bona fide presentation)

Sự tương tác của đối tượng 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 (Bona fide) có tính chất tương tự như thông thường hoặc thường lệ, khi đề cập đến một bản trình diện trung thực.

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

CHÚ THÍCH 3: Khái niệm "theo cách được dự kiến bởi chính sách của hệ thống sinh trắc học" cho sự trung thực được bao gồm trong khái niệm "phù hợp với chính sách về mục đích sử dụng của hệ thống sinh trắc học" được sử dụng trong tiêu chuẩn này

[NGUỒN: ISO/IEC 30107-3:2017, 3.1.2, được sửa đổi - Chú thích 3 đã được bổ sung]

3.2

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

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

[Nguồn: ISO/IEC 30107-3:2017, 3.2.2]

3.3

Đường cong cân bằng lỗi phát hiện (detection error trade-off curve) Đường cong DET

Đường cong ROC đã sửa đổi, biểu thị tỷ lệ lỗi trên cả hai trục (dương tính giả trên trục x và âm tính giả trên trục y)

CHÚ THÍCH 1: Bộ ví dụ về đường cong DET được thể hiện trong ISO/IEC 19795-1: 2006, Hình 3.

[NGUỒN: ISO/IEC 19795-1: 2006, 4.7.1]

3.4

tỷ lệ chấp nhận lỗi (false accept rate) FAR

tỷ lệ giao dịch xác minh với các yêu cầu về danh tính được xác nhận không chính xác
tỷ lệ các giao dịch xác minh với các yêu cầu về danh tính là không đúng nhưng được xác nhận không chính xác.

[NGUỒN: ISO/IEC 19795-1: 2006, 4.6.6]

3.5

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

tỷ lệ các phản hồi về định danh của người dùng đã đăng ký trong hệ thống trong đó định danh đúng của người dùng không nằm trong số các phản hồi được trả lại.

[NGUỒN: ISO/IEC 19795-1: 2006, 4.6.8]

3.6

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

tỷ lệ các phản hồi về định danh của người dùng không đăng ký trong hệ thống, nhưng trong phản hồi lại có định danh.

[NGUỒN: ISO/IEC 19795-1: 2006, 4.6.9]

3.7

tỷ lệ từ chối lỗi (false reject rate)
FRR

Tỷ lệ các giao dịch xác minh với các yêu cầu về danh tính là đúng thực nhưng bị từ chối không đúng.

[NGUỒN : ISO/IEC 19795-1: 2006, 4.6.5]

3.8

tỷ lệ so sánh 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 trong đó tham chiếu đích là trùng khớp.

[NGUỒN: ISO/IEC 30107-3: 2017, 3.2.6]

3.9

diểm hoạt động (operating point)

thiết lập hệ thống sinh trắc học để hoạt động ở ngưỡng quyết định được cố định

CHÚ THÍCH 1: Điểm hoạt động có thể được biểu thị trực tiếp bằng ngưỡng quyết định hoặc có thể được biểu diễn bằng tham số cấu hình xác định trước.

3.10

chính sách về mục đích sử dụng (policy of the intended use)

chính sách nêu rõ cách thức thực hiện các trình diện trung thực

CHÚ THÍCH 1: Mục đích sử dụng là về cách sinh trắc học tự nhiên nên được sử dụng với TOE, tức là các trình diện được thực hiện theo cách mà các trình diện trung thực được thực hiện. Các trình diện bằng tạo tác không được xem xét.

4 Ký hiệu và thuật ngữ viết tắt

ATE	assurance class tests	các thử nghiệm lớp đảm bảo
AVA	assurance class vulnerability assessment	đánh giá lỗ hổng lớp đảm bảo
FAR	false accept rate	tỷ lệ tiếp nhận lỗi
FMR	false match rate	tỷ lệ 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
FRR	false reject 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
IT	information technology	công nghệ thông tin
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
ST	security target	đích an toàn
TCVN		tiêu chuẩn quốc gia
TOE	target of evaluation	đích đánh giá
TSF	TOE security functionality	chức năng an toàn của TOE

5 Các hoạt động bổ sung cho TCVN 11386 (ISO/IEC 18045) về các thử nghiệm ATE

5.1 Yêu cầu chung

5.1.1 Hướng dẫn

Điều 5 bao gồm hướng dẫn, các yêu cầu bổ sung và bổ sung cho các hoạt động đánh giá từ Điều 14 của TCVN 14190-1:2024, dành cho kiểm thử viên.

Định nghĩa về xác thực có thể được tìm thấy trong ISO/IEC 2382.

Các định nghĩa của sinh trắc học (tính từ), thu thập sinh trắc học, thiết bị thu thập sinh trắc học, đặc điểm sinh trắc học, người đăng ký sinh trắc học, đăng ký sinh trắc học, cơ sở dữ liệu đăng ký sinh trắc học, tính năng sinh trắc học, định danh sinh trắc học, kẻ giả mạo sinh trắc học, trình diện sinh trắc học, nhận dạng sinh trắc học, tham chiếu sinh trắc học, mẫu sinh trắc học, sinh trắc học Hệ thống, xác minh sinh trắc học, so sánh, đăng ký, tỷ lệ thu thập thất bại, tỷ lệ đăng ký thất bại, tỷ lệ khớp lỗi, tỷ lệ không khớp lỗi, khớp và ngưỡng có thể được tìm thấy trong ISO/IEC 2382-37.

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

CHÚ THÍCH 2: Trong tiêu chuẩn này, cụm từ thu gọn "người đăng ký" được sử dụng thay cho "người đăng ký sinh trắc học".

CHÚ THÍCH 3: Trong tiêu chuẩn này, cụm từ thu gọn "đăng ký" được sử dụng thay cho "việc đăng ký sinh trắc học".

CHÚ THÍCH 4: Trong tiêu chuẩn này, cụm từ thu gọn gọn "tính năng" thường được sử dụng thay cho "tính năng sinh trắc học".

CHÚ THÍCH 5: Trong tiêu chuẩn này, cụm từ "kẻ mạo danh" đổi khi được sử dụng thay cho "kẻ giả mạo sinh trắc học".

CHÚ THÍCH 6: Trong tiêu chuẩn này, cụm từ thu gọn "trình diện" thường được sử dụng thay cho "trình diện sinh trắc học".

Các định nghĩa về bảo đảm, khả năng tấn công, lối, thành phần, xác nhận, mô tả, xác định, nhà phát triển, phát triển, bảo đảm, đánh giá, tài liệu hướng dẫn, định danh, tương tác, giao diện, đối tượng, hoạt động, môi trường hoạt động, lỗi hỏng tiềm năng, hồ sơ bảo vệ, đích an toàn, đích đánh giá, chức năng an toàn TOE, xác minh và lỗi hỏng an toàn có thể được tìm thấy trong TCVN 8709-1 (ISO/IEC 15408-1).

CHÚ THÍCH 7: Thuật ngữ "hoạt động" có liên quan đến lớp AGD.

Có thể tìm thấy các định nghĩa về thử nghiệm, thử nghiệm, phương pháp luận và báo cáo trong TCVN 11386 (ISO/IEC 18045).

Các định nghĩa về tấn công trình diện, phát hiện tấn công trình diện và tấn công trình diện có thể tìm thấy thiết bị trong ISO/IEC 30107-1.

Hệ thống sinh trắc học sử dụng công nghệ và chức năng đòi hỏi những cân nhắc đặc biệt khi tiến hành đánh giá an toàn, bao gồm đánh giá an toàn dựa trên bộ tiêu chuẩn TCVN 8709 (ISO/IEC 15408). Một trong số đó là tính chất không xác định của các quyết định sinh trắc học, ví dụ khớp; không khớp; và các quyết định khác, và hậu quả là khả năng xảy ra các lỗi quyết định (ví dụ: khớp lỗi, không khớp lỗi) có thể có tác động an toàn đối với hệ thống sinh trắc học.

Thử nghiệm tỷ lệ lỗi nhận dạng sinh trắc học liên quan đến an toàn là một khía cạnh quan trọng của mọi đánh giá an toàn của hệ thống sinh trắc học. Hơn nữa, các yêu cầu trong TCVN 14190-1 đảm bảo rằng nhà phát triển hệ thống sinh trắc học được đánh giá cũng phải thử nghiệm tỷ lệ lỗi của hệ thống theo chính sách về mục đích sử dụng theo tài liệu hướng dẫn TOE.

CHÚ THÍCH 2: Trong tiêu chuẩn này, mục đích sử dụng tuân theo tài liệu hướng dẫn TOE bao gồm cả nỗ lực chính hãng và mạo danh, miễn là việc sử dụng phù hợp với hướng dẫn. Hướng dẫn được cung cấp bởi nhà phát triển TOE.

Điều khoản này bao gồm hướng dẫn và các yêu cầu bổ sung đối với kiểm thử viên và xem xét các thử nghiệm của nhà phát triển cũng như lập kế hoạch, tiến hành và báo cáo thử nghiệm độc lập về tỷ lệ lỗi của hệ thống sinh trắc học. Điều khoản này cũng có thể được nhà phát triển hệ thống sinh trắc học sử dụng để được thông báo về các yêu cầu.

CHÚ THÍCH 3: Trong tiêu chuẩn này, kiểm thử viên được coi là có năng lực theo khuôn khổ đánh giá theo TCVN 8709 (ISO/IEC 15408) (tất cả các phần) và cụ thể là TCVN 8709-1 (ISO/IEC 15408-1).

Các điều phụ 5.1 đến 5.4 có thể áp dụng cho cả ATE_IND và ATE_FUN. Điều 5.5 dành riêng cho ATE_FUN, liên quan đến các thử nghiệm chức năng. Điều 5.6 giới thiệu các khía cạnh cụ thể thu được từ TCVN 14190-1. Điều 5.7 dành cho phần ATE_IND.2 liên quan đến các thử nghiệm của nhà phát triển. Điều 5.8 dành riêng cho thử nghiệm độc lập.

Theo nguyên tắc mặc định, kiểm thử viên phải tuân theo các khuyến nghị được giới thiệu sau đó (ví dụ: về tỷ lệ lỗi, giá trị tối đa, phương pháp thử nghiệm của nhà phát triển, v.v.). Nếu kiểm thử viên nhận

định rằng họ không được lựa chọn thích hợp liên quan đến TOE và ứng dụng, họ có thể sử dụng các giá trị thích hợp hơn để thử nghiệm và phải cung cấp lý do cho việc lựa chọn các giá trị trong báo cáo đánh giá. Các khía cạnh cụ thể về công nghệ trong điều khoản này đã được phát triển dựa trên các yêu cầu trong ISO/IEC 19795-1. Loại thử nghiệm được thực hiện (kích bản, công nghệ hoặc thử nghiệm vận hành) sẽ được xác định bởi kiểm thử viên, dựa trên bản chất của TOE và mục tiêu an toàn TOE (xem 5.1.3 để biết thêm thông tin).

Ngoài các yêu cầu và khuyến nghị được cung cấp trong điều khoản này, kiểm thử viên cũng phải tuân theo các yêu cầu đối với các thành phần đảm bảo được TOE lựa chọn cho lớp ATE trong TCVN 8709-3 (ISO/IEC 15408-3) và phải tuân theo các yêu cầu của các hoạt động tương ứng trong TCVN 11386 (ISO/IEC 18045).

Cấu hình của TOE có thể có ảnh hưởng đến hiệu suất nhận dạng sinh trắc học. Do đó, kiểm thử viên phải đảm bảo rằng cấu hình TOE để thử nghiệm tuân thủ các yêu cầu được chỉ định trong ST hoặc PP. Đặc biệt, khi TOE bao gồm chức năng PAD, kiểm thử viên phải thử nghiệm xem chức năng PAD có được kích hoạt và cấu hình chính xác hay không trong khi tiến hành thử nghiệm hiệu suất nhận dạng sinh trắc học. Nếu cả hiệu suất nhận dạng sinh trắc học và PAD đều được đánh giá cho TOE, thì tỷ lệ lỗi phân loại trình diện trung thực (BPCER) như được xác định trong ISO/IEC 30107-3 phải được tính toán trong thử nghiệm hiệu suất nhận dạng sinh trắc học, bằng cách ghi thêm đầu ra của hệ thống con PAD như một thông tin bổ sung trong tài liệu cho hoạt động ATE_FUN của đánh giá PAD. Tương tự, tỷ lệ trình diện cuộc tấn công mạo danh (IAPMR) như được định nghĩa trong ISO/IEC 30107-3 có thể được truy xuất từ hoạt động ATE_FUN của đánh giá PAD và được tính đến, vì nó liên quan đến hiệu suất sinh trắc học.

CHÚ THÍCH 4: Thông tin về IAPMR từ đánh giá PAD không hữu ích cho kiểm thử viên để ước tính FMR/FAR, vì những số liệu này không liên quan trực tiếp. Tuy nhiên, IAPMR có thể là một thông tin hữu ích cho kiểm thử viên để hiểu các hành vi cụ thể của các thuật toán định danh (và nó cũng có thể hữu ích cho AVA để xác định các điểm yếu tiềm ẩn).

CHÚ THÍCH 5: ATE tập trung vào việc xác nhận hiệu suất của TOE bằng cách thử nghiệm theo chính sách về mục đích sử dụng theo tài liệu hướng dẫn TOE. Do đó, nó bao gồm các nỗ lực trình diện trung thực (trái ngược với các tấn công trình diện được xem xét trong TCVN 14190-3) cho cả các thử nghiệm so sánh theo cặp và các thử nghiệm so sánh không theo cặp (tức là các nỗ lực giả mạo). Trong cả hai thử nghiệm, kiểm thử viên có thể thừa nhận việc sử dụng TOE phù hợp với chính sách của mục đích sử dụng. Tất cả các loại trình diện khác được xem xét trong TCVN 14190-3.

5.1.2 Nhận xét để đánh giá hiệu suất

Mỗi quan hệ giữa hai tỷ lệ lỗi FAR / FRR có thể được minh họa bằng cách sử dụng đường cong cân bằng lỗi phát hiện (DET) cho thấy sự phụ thuộc giữa hai tỷ lệ lỗi sinh trắc học vì ngưỡng quyết định thay đổi trong phạm vi làm việc của nó (xem ISO/IEC 19795-1 để biết thêm thông tin). Các đường cong DET có thể hữu ích để so sánh hiệu suất định danh của các hệ thống sinh trắc học và theo dõi những cải tiến trong hệ thống sinh trắc học trong quá trình phát triển của nó. Trong bối cảnh đánh giá, hệ thống sinh trắc học thường chỉ được xem xét ở một hoặc một bộ ngưỡng quyết định rất hạn chế.

Nhà phát triển phải chỉ định điểm hoạt động hoặc các điểm của TOE trong mục tiêu an toàn, để đảm bảo rằng khách hàng của TOE được thông báo về cấu hình được đánh giá.

Kiểm thử viên phải đảm bảo rằng các cài đặt an toàn liên quan (bao gồm ít nhất các điểm hoạt động) của TOE được sử dụng trong quá trình thử nghiệm hiệu suất được thiết lập và việc đánh giá được thực hiện phù hợp với các giá trị được nêu trong mục tiêu an toàn.

Hơn nữa, cần xem xét rằng việc đánh giá an toàn theo tiêu chuẩn TCVN 8709 (ISO/IEC 15408) là tập trung vào an toàn CNTT. Do đó, tỷ lệ lỗi nhận dạng sinh trắc học liên quan đến an toàn của hệ thống sinh trắc học sẽ được đánh giá trong bối cảnh đánh giá. Tuy nhiên, bởi vì tính an toàn có thể đạt được với chi phí khả năng sử dụng, tỷ lệ lỗi liên quan đến khả năng sử dụng cũng cần được đánh giá. Hướng dẫn xác định tỷ lệ lỗi liên quan được nêu trong 5.1.4.3.

Các điều phụ từ 5.1.3 đến 5.8 cung cấp thông tin chi tiết hơn cho kiểm thử viên về việc xem xét các thử nghiệm của nhà phát triển, lặp lại một tập hợp con thử nghiệm như được nêu trong ATE_IND.2 và về thử nghiệm độc lập theo yêu cầu của ATE_IND.1.

5.1.3 Xác định loại đánh giá hiệu suất

Theo ISO/IEC 19795-1, có thể phân biệt ba loại đánh giá cơ bản đối với tốc độ hoạt động của hệ thống sinh trắc học:

- Đánh giá công nghệ: đánh giá ngoại tuyến một hoặc nhiều thuật toán cho cùng một phương thức sinh trắc học bằng cách sử dụng kho mẫu đã có trước hoặc được thu thập đặc biệt;
- Kịch bản đánh giá: đánh giá trong đó hiệu suất của hệ thống đầu cuối được xác định trong một ứng dụng nguyên mẫu hoặc mô phỏng bằng cách sử dụng các trình diễn sinh trắc học trực tiếp được thực hiện bởi một nhóm thử nghiệm được tuyển dụng cho thử nghiệm;
- Đánh giá hiệu suất: đánh giá trong đó hiệu suất của một hệ thống sinh trắc học hoàn chỉnh được xác định trong môi trường hoạt động của nó với một dân số mục tiêu cụ thể.

Bước đầu tiên đối với kiểm thử viên là xác định loại đánh giá chính xác cho hệ thống sinh trắc học được đánh giá. Loại đánh giá sẽ được xác định bởi thành phần của TOE và những gì được chỉ định trong mục tiêu an toàn. Thành phần của TOE phải có khả năng hỗ trợ (các) loại đánh giá cụ thể.

CHÚ THÍCH: Vì các đánh giá thường đề cập đến một trường hợp của sản phẩm sinh trắc học hơn là một trường hợp cụ thể của việc lắp đặt hệ thống sinh trắc học, nên việc thử nghiệm vận hành của tỷ lệ lỗi nhận dạng sinh trắc học có liên quan thường không được xem xét. Do đó, hầu hết nội dung trong điều khoản này chỉ đề cập cụ thể đến các trường hợp công nghệ và kịch bản.

Loại đánh giá được thực hiện phụ thuộc vào định nghĩa của TOE và phạm vi trong mục tiêu an toàn. Kiểm thử viên phải xác minh rằng thử nghiệm của nhà phát triển phù hợp với loại đánh giá.

ISO/IEC 19795-1 còn phân biệt rõ hơn giữa các thử nghiệm trực tuyến và ngoại tuyến. Trong các thử nghiệm trực tuyến, quá trình ghi danh hoặc so sánh được thực hiện tại thời điểm gửi hình ảnh hoặc tín hiệu trong khi các giai đoạn thử nghiệm đó được giữ riêng trong các thử nghiệm ngoại tuyến. Đánh giá công nghệ được thực hiện bằng cách sử dụng xử lý ngoại tuyến dữ liệu sinh trắc học.

Do các yêu cầu liên quan đến độ lặp lại và độ tái lập áp dụng cho các đánh giá, không nên sử dụng các phép thử trực tuyến thuần túy (trong đó hình ảnh hoặc tín hiệu bị loại bỏ trực tiếp).

5.1.4 Tỷ lệ lỗi nhận dạng sinh trắc học

5.1.4.1 Các chỉ số để xác minh sinh trắc học

Lớp ATE trong tiêu chuẩn này đề cập đến các thử nghiệm sẽ được thực hiện để đánh giá hiệu suất của hệ thống sinh trắc học theo chính sách về mục đích sử dụng theo tài liệu hướng dẫn TOE.

Trong trường hợp của một hệ thống sinh trắc học xác minh, mục đích sử dụng có thể được định nghĩa như sau: "một chủ thẻ dữ liệu có găng được hệ thống công nhận là một chủ thẻ dữ liệu được đăng ký hợp pháp liên quan đến danh tính được xác nhận quyền sở hữu".

Trong trường hợp này, hệ thống có thể dự đoán hai trường hợp sẽ được phân biệt: thử nghiệm so sánh sinh trắc học theo cặp (tức là thử nghiệm so sánh thực) và thử nghiệm so sánh sinh trắc học không theo cặp (tức là giả mạo). Theo hai trường hợp này, tỷ lệ lỗi quyết định sau đây sẽ được báo cáo:

- Đỗ đánh giá thuật toán, FMR và FNMR;
- Đỗ đánh giá hệ thống, FAR và FRR.

Sự khác biệt giữa tỷ lệ lỗi thuật toán (FMR và FNMR) và tỷ lệ lỗi hệ thống (FAR và FRR) là tỷ lệ lỗi phụ thuộc vào số lần xác minh được phép và cũng có thể bao gồm các loại lỗi khác như lỗi không đạt được và không thực hiện được ghi danh.

Tỷ lệ lỗi FAR (tương ứng FMR) và FRR (tương ứng FNMR) của một hệ thống sinh trắc học có liên quan tỷ lệ nghịch, sự cân bằng giữa hai tỷ lệ này được xác định bởi cài đặt ngưỡng quyết định xác minh cho hệ thống.

Lưu ý rằng thử nghiệm tỷ lệ lỗi khác bao gồm giai đoạn thu thập mẫu thường tạo ra các kết quả khác nhau cho các giao dịch được giới hạn trong một lần thử và các giao dịch cho phép thử nhiều lần, ví dụ: không đăng ký được tỷ lệ (FTER) và không đạt được tỷ lệ (FTAR).

5.1.4.2 Các chỉ số để định danh sinh trắc học

Trong một tình huống định danh, một đối tượng cung cấp một mẫu sinh trắc học mà không đưa ra yêu cầu rõ ràng về danh tính. Hệ thống sinh trắc học xác định đối tượng bằng cách so sánh sinh trắc học của mẫu định danh sinh trắc học với tham chiếu sinh trắc học của tất cả các đối tượng đã đăng ký cho đến khi tìm thấy đối tượng phù hợp (hoặc không) dựa trên tiêu chí quyết định định danh được xác định cho hệ thống. Đây được gọi là so sánh 1: nhiều. Tùy thuộc vào tiêu chí, hệ thống có thể tìm thấy và báo cáo không có hoặc nhiều kết quả phù hợp. Khi có nhiều hơn một trận đấu được báo cáo, các danh tính phù hợp có thể được xếp hạng theo điểm so sánh tương ứng.

Trong trường hợp của một hệ thống sinh trắc học định danh, mục đích sử dụng có thể được xác định như sau:

- Kịch bản chấp thuận định dạng: kịch bản trong đó mục đích của hệ thống sinh trắc học là xác minh và xác định bằng cách nhận dạng sinh trắc học rằng chủ thẻ dữ liệu là một đối tượng đăng ký cụ thể trong hệ thống mà không yêu cầu xác nhận trước về danh tính;
- Kịch bản từ chối định dạng: tình huống trong đó mục đích của hệ thống sinh trắc học là xác nhận bằng phương pháp nhận dạng sinh trắc học rằng một chủ thẻ dữ liệu đăng ký không được đăng ký trong hệ thống.

Cũng như kịch bản xác minh, hoạt động ATE cấp trong tiêu chuẩn này đề cập đến các thử nghiệm sẽ được thực hiện để đánh giá hiệu suất của hệ thống định danh sinh trắc học (TOE) theo mục đích sử dụng của nó. Thử nghiệm tính năng phải bao gồm:

- Nếu tình huống chấp thuận định dạng được xem xét: thử nghiệm hiệu suất đối với trường hợp trình diện trung thực, tức là trong đó các thành viên của nhóm thử nghiệm (hoặc dữ liệu thử nghiệm) bao gồm các chủ thẻ dữ liệu đã đăng ký hợp pháp có găng được hệ thống xác định là chính họ và thử

nghiệm hiệu suất cho trường hợp trình diện giả mạo trong đó các thành viên của nhóm thử nghiệm (hoặc dữ liệu thử nghiệm) không đăng ký trong hệ thống cổ gắng bị hệ thống xác định sai là những người đăng ký hợp pháp bằng cách sử dụng các trình diện về các đặc điểm sinh trắc học tự nhiên của họ;

- Nếu tinh huống từ chối định dạng được xem xét: thử nghiệm hiệu suất đối với trường hợp người không đăng ký-các trình diện liên quan trong đó các thành viên của nhóm thử nghiệm (hoặc dữ liệu thử nghiệm) không đăng ký hệ thống cổ gắng không để hệ thống xác định là người đăng ký và thử nghiệm hiệu suất đối với trường hợp thuyết trình liên quan đến người đăng ký, tức là khi các thành viên của nhóm thử nghiệm (hoặc dữ liệu thử nghiệm) bao gồm các chủ thể dữ liệu đã đăng ký cổ gắng bị hệ thống định danh lỗi, sử dụng các trình diện về các đặc điểm sinh trắc học tự nhiên của chúng.

Ngoài các chức năng của hệ thống, các chỉ số chính cần được đánh giá là:

- Nếu kịch bản chấp thuận định dạng được xem xét, tỷ lệ chấp thuận định dạng thực, tỷ lệ lỗi định danh khẳng định sai(FPIR) và xếp hạng định danh;

- Nếu kịch bản từ chối định dạng được xem xét, tỷ lệ từ chối định dạng thực và tỷ lệ lỗi định danh phủ định sai (FNIR).

CHÚ THÍCH Đối với bất kỳ trường hợp nào, tỷ lệ lỗi hệ thống sinh trắc học khác tồn tại có thể trở nên phù hợp đối với các tinh huống. ISO/IEC 19795-1 cung cấp một cái nhìn tổng quan đầy đủ về tất cả các tỷ lệ lỗi nhận dạng sinh trắc học có thể có liên quan.

Tùy các loại tỷ lệ lỗi này, kiểm thử viên sẽ quyết định loại nào phù hợp cho một đánh giá cụ thể (xem 5.1.4.3).

5.1.4.3 Xác định tỷ lệ lỗi liên quan

Không có câu trả lời toàn diện và duy nhất cho câu hỏi tỷ lệ lỗi nào có liên quan đến một hệ thống sinh trắc học cụ thể dưới một đánh giá cụ thể. Kiểm thử viên nên xem xét một số khía cạnh khi xác định tỷ lệ lỗi liên quan như được mô tả dưới đây.

Điều khoản phụ này cung cấp một cái nhìn tổng quan về các khía cạnh quan trọng nhất cần được tính đến để trả lời câu hỏi này. Kiểm thử viên cũng phải tính đến tỷ lệ lỗi được yêu cầu (tuân theo TCVN 14190-1:2024, 8.3, 8.4 và Phụ lục C).

Tỷ lệ lỗi chính được quan tâm là những tỷ lệ có liên quan đến an toàn. Tỷ lệ lỗi có liên quan đến an toàn phụ thuộc vào mục đích của việc nhận dạng sinh trắc học. Để xác minh, chỉ số an toàn chính để thử nghiệm kịch bản là FAR (FMR để thử nghiệm công nghệ). Để chấp thuận định dạng, số liệu an toàn chính để thử nghiệm kịch bản là FPIR (FMR để thử nghiệm công nghệ). Các thông số khác có thể ảnh hưởng đến tỷ lệ lỗi nhận dạng sinh trắc học liên quan đến an toàn, chẳng hạn như việc sử dụng bộ đếm thử lại.

Nếu cả hiệu suất nhận dạng sinh trắc học và PAD đều được đánh giá cho TOE, thì BPCER là một tỷ lệ lỗi có liên quan bổ sung. Nó liên quan đến hiệu suất và khả năng sử dụng của một hệ thống vì nó là thước đo tốc độ mà một hệ thống con PAD xác định rằng một trình diện trung thực là một tấn công trình diện khi nó không đúng. Ngoài các yêu cầu từ TCVN 14190-3, kiểm thử viên cần quan sát đầu ra của hệ thống con PAD trong quá trình thử nghiệm hiệu suất để đo lường các phân loại lỗi của trình diện trung thực như là tấn công trình diện. Tương tự, kiểm thử viên có thể coi IAPMR là một số liệu có liên quan nếu được cung cấp từ hoạt động ATE_FUN của đánh giá PAD, vì nó liên quan đến việc thành công đồng thời để vượt qua PAD và nhận dạng sinh trắc học.

Trong quá trình đánh giá, tỷ lệ lỗi nhận dạng sinh trắc học liên quan đến an toàn sẽ được đánh giá chuyên sâu. Các tỷ lệ lỗi liên quan khác nên được đánh giá.

Để xác định tất cả các tỷ lệ lỗi liên quan, kiểm thử viên phải xem xét tất cả các tỷ lệ lỗi được xác định trong ISO/IEC 19795-1 và trả lời hai câu hỏi cho mỗi tỷ lệ:

- Mức độ an toàn lỗi có liên quan đến TOE không?
- Mức độ liên quan của chúng với ứng dụng là gì?

Chỉ khi cả hai câu hỏi đều được trả lời tích cực, thì tỷ lệ lỗi mới nên được tính đến đánh giá.

Cần lưu ý rằng một số tỷ lệ lỗi của hệ thống sinh trắc học phụ thuộc vào tỷ lệ lỗi khác thông qua cài đặt cho người quyết định của hệ thống. Một ví dụ là mối quan hệ nghịch đảo giữa tỷ lệ chấp nhận lỗi và tỷ lệ từ chối lỗi. Do đó, tất cả các tỷ lệ lỗi có liên quan đến an toàn liên quan tỷ lệ lỗi nhận dạng sinh trắc học cũng sẽ được báo cáo. Yêu cầu này nhằm đảm bảo rằng khả năng sử dụng của TOE cũng có thể được ước tính từ báo cáo đánh giá.

Kiểm thử viên phải thử nghiệm xem kết quả của phân tích này có phù hợp với thông tin mà nhà phát triển đã cung cấp trong mục tiêu an toàn hay không.

Bảng 1 giới thiệu tổng hợp các lỗi chính và tác động của chúng đối với an toàn và chức năng khác của TOE, trong trường hợp thử nghiệm theo kịch bản.

Bảng 1 - Ảnh hưởng của lỗi sinh trắc học lên các chức năng ứng dụng

Chỉ số lỗi ứng dụng	Chức năng ứng dụng và tác động		
	Đăng ký	Xác minh	Định danh
FTER	Không có khả năng đăng ký các chủ thẻ dữ liệu Cung cấp các quy trình xử lý ngoại lệ	Cung cấp và bảo vệ các quy định xử lý ngoại lệ cho các chủ thẻ dữ liệu không thể đăng ký	Cung cấp và bảo vệ các quy định xử lý ngoại lệ cho các chủ thẻ dữ liệu không thể đăng ký
FAR	N/A	Kẻ mạo danh có thể được xác minh sai là chủ thẻ dữ liệu hợp pháp	N/A
BPCER (if PAD functionality)	Không có khả năng đăng ký các chủ thẻ dữ liệu	Chủ đề dữ liệu hợp pháp có thể không vượt qua được thử nghiệm PAD và do đó cần được xác minh	Chủ đề dữ liệu hợp pháp có thể không vượt qua được thử nghiệm PAD và do đó không được xác định lỗi trong danh sách chủ thẻ dữ liệu
FRR	N/A	Chủ thẻ dữ liệu hợp pháp có thể không được xác minh	N/A
FPIR	N/A	N/A	Kẻ mạo danh có thể bị xác định sai là ứng viên chủ thẻ dữ liệu hợp pháp

Chỉ số lỗi ứng dụng	Chức năng ứng dụng và tác động		
	Đăng ký	Xác minh	Định danh
FNIR	Không có khả năng phát hiện nhiều đăng ký hoặc nỗ lực đăng ký từ một chủ thẻ dữ liệu hợp pháp	N/A	Chủ thẻ dữ liệu hợp pháp có thể không được xác định trong danh sách ứng cử viên

Ví dụ về xác định tỷ lệ lỗi liên quan cho một trường hợp sử dụng cụ thể được thảo luận trong Phụ lục B.

5.1.4.4 Xác định giá trị tối đa cho tỷ lệ lỗi

Giá trị tối đa cho phép đối với tỷ lệ lỗi bị ảnh hưởng bởi các yếu tố chủ yếu do ứng dụng xác định. Điều khoản phụ này cung cấp hướng dẫn cho kiểm thử viên để xác định giá trị nào phù hợp với TOE (xem thêm Phụ lục B để biết ví dụ điển hình). Kiểm thử viên cũng phải tính đến tỷ lệ lỗi được yêu cầu (tuân theo TCVN 14190-1:2024, 8.3, 8.4 và Phụ lục C). Để đảm bảo tính nhất quán với bối cảnh ứng dụng, kiểm thử viên có thể sử dụng Bảng 2 lấy từ ISO/IEC 29115: 2013 để xác định mức độ đảm bảo yêu cầu trên cơ sở đánh giá mức độ nghiêm trọng của tác động có thể có của lỗi xác thực. Việc xác định những gì tạo thành rủi ro tối thiểu, trung bình, đáng kể và cao phụ thuộc vào tiêu chí rủi ro cho từng hậu quả có thể xảy ra.

Bảng 2 - Tác động tiềm ẩn của lỗi xác thực ở mỗi cấp độ đảm bảo

Tác động có thể xảy ra	Mức độ đảm bảo			
	Thấp	Trung bình	Cao	Rất cao
Không thuận tiện, khó khăn hoặc thiệt hại cho vi/tối thiểu thẻ hoặc danh tiếng	vừa phải	đáng kể	cao	
Tốn thất tài chính hoặc trách nhiệm đại lý	tối thiểu	vừa phải	đáng kể	cao
Gây hại cho tổ chức, các chương trình hoặc lợi ích công cộng	N/A	tối thiểu	vừa phải	cao
Phát hành trái phép thông tin nhạy cảm	N/A	vừa phải	đáng kể	cao
An toàn cá nhân	N/A	N/A	tối thiểu đến đáng kể trung bình đến cao	
Vi phạm dân sự hoặc hình sự	N/A	tối thiểu	đáng kể	cao

Ngoài ra, đối với trường hợp hệ thống xác minh sinh trắc học được sử dụng làm yếu tố xác thực duy nhất, ISO/IEC TR 29156: 2015, 6.4, đề xuất chọn các giá trị FAR sau, mà kiểm thử viên có thể sử dụng trong trường hợp thử nghiệm kịch bản để thiết lập FAR hoặc để tính tỷ lệ lỗi khác:

- FAR dưới 0,000 1% để đảm bảo cao;
- FAR dưới 0,01% đối với mức đảm bảo trung bình;
- FAR dưới 1% để đảm bảo cơ bản.

Nếu hệ thống xác minh sinh trắc học được sử dụng cùng với các yếu tố xác thực khác (ví dụ: dựa trên kiến thức), giá trị FAR cao hơn có thể được chấp nhận.

Nếu không có mức cụ thể nào được xác định, kiểm thử viên ít nhất phải tuân theo các hướng dẫn hiện có, chẳng hạn như hướng dẫn FRONTEX [9]. Ví dụ: kiểm thử viên nên đánh giá hệ thống ở ngưỡng tương ứng với mức an toàn về tỷ lệ chấp nhận lỗi (FAR) tối đa là 0,001 (0,1%). Ở cấu hình này, FRR không được cao hơn 0,05 (5%).

Nếu ST tuyên bố sự phù hợp với PP xác định các giá trị tối đa cho tỷ lệ lỗi, để đáp ứng các yêu cầu đánh giá, tỷ lệ lỗi của TOE đo được sẽ thấp hơn giá trị tối đa.

Ví dụ về xác định giá trị lớn nhất cho một trường hợp sử dụng cụ thể được thảo luận trong Phụ lục B.

5.2 Lập kế hoạch đánh giá

5.2.1 Tổng quan

Lập kế hoạch thử nghiệm hiệu suất nhận dạng sinh trắc học nên bao gồm hai cân nhắc quan trọng. Thứ nhất, để đảm bảo rằng các mô hình thiết kế thử nghiệm càng gần với kịch bản trong thế giới thực về mục đích sử dụng của TOE càng tốt. Thứ hai, để đảm bảo rằng các kết quả thử nghiệm có ý nghĩa thống kê trong bối cảnh mục đích sử dụng của TOE.

Ý nghĩa thống kê như vậy về cơ bản được xác định bởi dữ liệu thử nghiệm mà các thử nghiệm được chạy và trên các lần truy cập thực tế được thực hiện với dữ liệu thử nghiệm có sẵn. Kết quả phải được báo cáo theo giá trị tỷ lệ lỗi trung bình và khoảng tin cậy.

Điều khoản phụ này bao gồm các khuyến nghị cho kiểm thử viên để lập kế hoạch và thực hiện thử nghiệm. Nếu thử nghiệm của nhà phát triển được kiểm thử viên coi là đầy đủ và hợp lệ, thì kiểm thử viên có thể giới hạn hoạt động của họ trong các hoạt động thử nghiệm đơn giản hơn và giảm bớt. Sự lựa chọn này phải được chứng minh trong báo cáo đánh giá.

Một kế hoạch thử nghiệm toàn diện phải được lập và lập thành văn bản. Kế hoạch thử nghiệm phải đáp ứng các mục tiêu sau.

- Thiết lập thử nghiệm phải phù hợp với hoạt động dự kiến của hệ thống sinh trắc học càng chặt chẽ càng tốt.

- Kế hoạch thử nghiệm phải xác định chính xác các bước liên quan cần thực hiện trong quá trình thử nghiệm. Cụ thể, khi cần có sự tương tác sâu với nhóm thử nghiệm (ví dụ: trong thử nghiệm theo kịch bản), kế hoạch thử nghiệm phải mô tả rõ ràng quy trình thử nghiệm.

- Kế hoạch thử nghiệm phải bao gồm mô tả rất chi tiết về dữ liệu thử nghiệm mà việc đánh giá sẽ được thực hiện. Điều này bao gồm ví dụ: số lượng chủ thẻ dữ liệu, số lượng mẫu mã chủ đề dữ liệu, số lượng phiên thu nhận có liên quan, môi trường và điều kiện bên ngoài của quá trình thu nhận (ví dụ: nền, ánh sáng, tư thế).

- Kế hoạch thử nghiệm phải bao gồm một giao thức rất rõ ràng về cách dữ liệu thử nghiệm được sử dụng hoặc cách các chủ thẻ dữ liệu thử nghiệm nên tương tác với TOE trong quá trình nắm bắt.

- Kế hoạch thử nghiệm phải bao gồm liệu dữ liệu đã được thu thập cần thiết để đào tạo lại về hệ thống. Trong trường hợp này, dữ liệu thu thập được phải được tách biệt trong dữ liệu đào tạo và thử nghiệm và mục đích của mỗi tập dữ liệu phải được mô tả.

- Tập dữ liệu thử nghiệm phải chứa một số mẫu sinh trắc học cho mỗi chủ thẻ dữ liệu / trường hợp sinh trắc học (ví dụ: từ mỗi ngón tay) và các mẫu từ các chủ thẻ dữ liệu khác nhau để tạo ra cả thử nghiệm so sánh kết hợp và thử nghiệm so sánh không kết hợp.

- Kế hoạch thử nghiệm phải chỉ rõ giai đoạn xác minh trước, bao gồm thu thập (nếu có) và trích xuất đặc điểm để thiết lập danh sách các mẫu được so sánh cùng với thông tin xem cặp so sánh tương ứng với thử nghiệm chính thức hay thử nghiệm giả mạo. Đối với mỗi loại, kiểm thử viên phải lập kế hoạch đo thời gian cho các tiểu phẫu, số lỗi mắc phải (nếu có) và số lỗi để trích xuất các mẫu. Danh sách các mẫu được so sánh phải bao gồm cả các cặp so sánh chính hãng và các cặp so sánh giả mạo, và số lượng các cặp phải được đặt tương ứng với phạm vi tỷ lệ lỗi (ví dụ: FAR và FRR để thử nghiệm kịch bản của hệ thống xác minh) các giá trị cần thử nghiệm bởi kiểm thử viên.

- Kế hoạch thử nghiệm phải chỉ rõ một giai đoạn so sánh để tính toán tất cả các so sánh từ danh sách được chuẩn bị trong giai đoạn trước khi xác minh. Đối với mỗi lần so sánh, kế hoạch đánh giá phải bao gồm thước đo thời gian cho hoạt động, số lỗi để so sánh, lưu trữ điểm đầu ra khi có thể hoặc quyết định. Dựa trên điểm đầu ra và nguồn được quy định bởi TOE (nếu có) hoặc dựa trên quyết định, số lượng chấp nhận lỗi và số lượng từ chối lỗi sẽ được đo lường.

- Kế hoạch thử nghiệm phải xác định các số liệu được báo cáo. Ngoài các giá trị đo được trong quá trình hoạt động, kiểm thử viên phải xác định các chỉ số thử nghiệm được báo cáo và cách lấy chúng từ các lỗi khác nhau mà kiểm thử viên quan sát được. Đối với thử nghiệm kịch bản của hệ thống xác minh sinh trắc học, chúng sẽ bao gồm FTA (nếu có), FTE, FAR và FRR. Nếu có sẵn điểm so sánh, chúng có thể bao gồm tính toán đường cong DET để nhúng đường cong DET vào báo cáo.

- Kế hoạch thử nghiệm cũng phải bao gồm một đặc điểm kỹ thuật đầy đủ của các điểm so sánh được tính toán và cách các số liệu hiệu suất được khấu trừ để hỗ trợ phân tích thống kê và đảm bảo khả năng tái lập đầy đủ.

- Kế hoạch thử nghiệm phải bao gồm việc chuẩn bị báo cáo sẽ báo cáo các giá trị được tính toán cho các chỉ số khác nhau được xác định và tổng hợp các kết quả.

Kế hoạch thử nghiệm phải được thiết kế và thử nghiệm phải được tiến hành phù hợp với ISO/IEC 19795-2.

5.2.2 Ước tính kích thước thử nghiệm

Thu thập và xử lý dữ liệu thử nghiệm là một trong những nhiệm vụ khó khăn nhất và tốn kém nhất trong mỗi thử nghiệm của một hệ thống sinh trắc học. Theo ISO/IEC 19795-1, dữ liệu thử nghiệm càng lớn càng tốt. Lưu ý rằng, để có được kết quả đáng tin cậy về mặt thống kê, cần có kích thước tối thiểu của dữ liệu thử nghiệm. Điều này phụ thuộc vào các yếu tố khác nhau:

- Kích thước của tỷ lệ lỗi cần đo (tỷ lệ lỗi càng nhỏ, số dữ liệu thử nghiệm cần thiết càng lớn);
- Khoảng tin cậy cần thiết.

CHÚ THÍCH: Kích thước của tập dữ liệu thử nghiệm không phải là yếu tố duy nhất ảnh hưởng đến mức độ tin cậy đối với tỷ lệ lỗi được đo. Sự phụ thuộc giữa các cặp so sánh khác nhau cũng ảnh hưởng đến mức độ tin cậy. Có thể so sánh chéo đầy đủ, nhưng sau đó sẽ không có sự độc lập đầy đủ nào nữa và tác động đến mức độ tin cậy sẽ được tính đến.

Vì kích thước yêu cầu của dữ liệu thử nghiệm cũng phụ thuộc vào kết quả của chính thử nghiệm, kích thước thử nghiệm yêu cầu thường chỉ được ước tính gần đúng trong bối cảnh lập kế hoạch thử nghiệm.

Mục đích của thử nghiệm độc lập tại ATE_IND.2 là tìm cách xác thực, ngay cả khi với độ tin cậy hạn chế, nhà phát triển đã xác nhận tỷ lệ lỗi. Điều này có thể được thực hiện với kích thước thử nghiệm nhỏ hơn nhiều so với kích thước dữ liệu thử nghiệm của nhà phát triển.

Số lượng chủ thể dữ liệu thử nghiệm và giao dịch thử nghiệm cần thiết để đảm bảo ý nghĩa thống kê của tỷ lệ lỗi nhận dạng sinh trắc học liên quan đến an toàn được đo lường phải được xác định từ giá trị tối đa cho phép của tỷ lệ lỗi bằng cách sử dụng "quy tắc 3" hoặc "quy tắc 30" (ISO/IEC 19795-1).

Đối với sinh trắc học trên thiết bị di động, hướng dẫn thực tế để tiến hành thử nghiệm hiệu suất được cung cấp trong ISO/IEC 21879. Kiểm thử viên nên tham khảo tài liệu đó để ước tính các kích thước thử nghiệm thích hợp.

5.2.3 Tài liệu thử nghiệm

Điều cần thiết là phải lập kế hoạch tài liệu đầy đủ cho thử nghiệm trước khi bắt đầu bất kỳ hoạt động nào khác.

Như đã giới thiệu trong 5.1.1, theo nguyên tắc mặc định, kiểm thử viên phải tuân theo các khuyến nghị được giới thiệu sau đó (ví dụ: về tỷ lệ lỗi, giá trị tối đa, phương pháp thử nghiệm của nhà phát triển, v.v.). Kiểm thử viên có thể quyết định từ việc xem xét kế hoạch thử nghiệm của nhà phát triển và việc tiến hành thử nghiệm dành cho nhà phát triển, rằng thử nghiệm dành cho nhà phát triển là phù hợp cho mục đích đánh giá và kiểm thử viên không cần lặp lại hoàn toàn quá trình thử nghiệm dành cho nhà phát triển. Nếu không, kiểm thử viên phải tuân theo kế hoạch thử nghiệm của riêng mình và tài liệu phải tuân theo các nguyên tắc tương tự như đối với bất kỳ thử nghiệm nào khác trong bối cảnh đánh giá an toàn theo bộ tiêu chuẩn TCVN 8709 (ISO/IEC 15408) và TCVN 11386 (ISO/IEC 18045). Ngoài ra, các khía cạnh sau sẽ được giải quyết cụ thể:

- Loại chính xác của đánh giá hiệu suất cần được mô tả cẩn trọng;
- Các tỷ lệ lỗi liên quan phải được xác định và các giá trị lớn nhất có thể chấp nhận được của chúng phải được xác định và chứng minh;
- Các đặc tính đặc biệt của dữ liệu thử nghiệm phải được lập thành văn bản;
- Kích thước và đặc điểm của dữ liệu thử nghiệm cần được mô tả đặc biệt chú ý đến số lượng
- Các phiên liên quan đến quá trình thu thập, chủ thể dữ liệu và mẫu cho mỗi chủ thể dữ liệu;
- Cần mô tả rõ ràng các tham số khác nhau của hệ thống được huấn luyện / thiết lập như thế nào (nếu có);
 - Cần được mô tả rõ ràng cách các bộ điểm khác nhau (các thử nghiệm so sánh theo cặp và không theo cặp) được tính toán.

5.3 Thu thập dữ liệu

5.3.1 Lựa chọn dữ liệu thử nghiệm hoặc thu thập nhóm thử nghiệm và thiết bị thu thập

Điều khoản phụ này áp dụng cho cả thử nghiệm kịch bản và công nghệ. Một điều quan trọng cần cân nhắc là nguồn dữ liệu mẫu sinh trắc học và nhóm thử nghiệm liên quan. Điều này có thể đạt được bằng nhiều cách khác nhau, ví dụ:

1) thu thập trực tiếp: dữ liệu thử nghiệm được thu thập từ nhóm thử nghiệm đặc biệt cho việc đánh giá TOE (có thể liên quan đến các yêu cầu nắm bắt cụ thể, ví dụ: một số thiết lập chiếu sáng hoặc nền cụ thể trong trường hợp hệ thống định danh khuôn mặt);

2) tái sử dụng cơ sở dữ liệu đã có từ trước, được nhà phát triển và / hoặc kiểm thử viên thu thập trên hệ thống sinh trắc học tương tự trước đó hoặc thu được từ dữ liệu thu được từ các bên thứ ba (chẳng hạn như nhiều cơ sở dữ liệu sinh trắc học công cộng hoặc tư nhân có sẵn ngày nay cho mục đích đo điểm chuẩn).

Trong mọi trường hợp, sự thật cơ bản phải được biết, tức là những mẫu nào trong dữ liệu thu được là những sự thật trùng khớp và cái nào không.

Trường hợp mong muốn nhất sẽ là tùy chọn 1), trong đó cơ sở dữ liệu thu thập trực tiếp được thu thập cho mỗi lần đánh giá. Tuy nhiên, đây cũng là giải pháp tiêu tốn nhiều thời gian và nguồn lực nhất và quyết định cuối cùng nên được thông qua trong từng trường hợp cụ thể. Ví dụ, đối với một công nghệ hoặc kịch bản đánh giá, trường hợp thứ hai có thể đủ nếu không phải đáp ứng các tính năng bên ngoài hoặc bối cảnh cụ thể (ví dụ: cảm biến thu nhận cụ thể). Nếu kiểm thử viên chọn sử dụng lại dữ liệu đã có, họ phải đảm bảo rằng dữ liệu này được tách riêng và nhà phát triển không thể truy cập được. Nhược điểm chính của việc sử dụng lại dữ liệu đã có sẵn mà nhà phát triển có thể có quyền truy cập là nó có thể được sử dụng để điều chỉnh hệ thống của họ. Kiểm thử viên sẽ giảm thiểu nó bằng cách sử dụng nhiều dữ liệu có tính độc lập hơn.

Để có được cơ sở dữ liệu mới hoặc đội thử nghiệm, một số yếu tố quan trọng phải được tính đến để thu được kết quả chính xác nhất có thể. Trong số các yếu tố như vậy, một số đặc điểm lý tưởng cần được đáp ứng bởi cơ sở dữ liệu đánh giá sinh trắc học được nêu bật dưới đây:

- Việc lựa chọn dữ liệu thử nghiệm (quá trình nắm bắt trực tiếp hoặc sử dụng lại dữ liệu đã có từ trước) sẽ thuộc quyền kiểm soát duy nhất của kiểm thử viên. Vì chất lượng của dữ liệu thử nghiệm là yếu tố cần thiết cho kết quả của các thử nghiệm, điều quan trọng là kiểm thử viên phải có kiến thức chi tiết về quá trình thu nhận.

- Một câu hỏi thường có thể nảy sinh là liệu dữ liệu thử nghiệm đã được nhà phát triển thu thập trước đó có thể được sử dụng lại trong quá trình đánh giá độc lập hay không. Mặc dù quyết định cuối cùng về việc sử dụng lại dữ liệu thử nghiệm là quyết định của kiểm thử viên, hướng dẫn này khuyến khích việc sử dụng lại dữ liệu thử nghiệm trong các giới hạn nhất định. Cụ thể, một thử nghiệm không bao giờ được hoàn toàn dựa trên dữ liệu thử nghiệm đã được nhà phát triển thu thập trước đó. Thay vào đó, kiểm thử viên phải thu được một tập nhỏ dữ liệu thử nghiệm và thay thế nó trong tập dữ liệu thử nghiệm ban đầu trước khi sử dụng.

- Nếu hệ thống sinh trắc học được thiết kế để hoạt động với một hồ sơ chủ thẻ dữ liệu cụ thể (ví dụ: nam giới, Châu Á, trên 65 tuổi, thuận tay phải), thì các chủ thẻ dữ liệu trong cơ sở dữ liệu/nhóm đối tượng phải càng gần với hồ sơ đó càng tốt.

- Nếu hệ thống sinh trắc học không được thiết kế để hoạt động với một cảm biến cụ thể, tốt hơn nên thu thập những cá thể giống nhau bằng các thiết bị thu nhận khác nhau để đánh giá cuối cùng được tổng quát hơn. Cũng tốt hơn nếu có thể thu được kết quả về khả năng tương tác (tức là kết quả so sánh giữa các mẫu sinh trắc học đã đăng ký và thử nghiệm được thu thập bằng các thiết bị khác nhau).

- Tập dữ liệu nên được tổ chức để cho phép xác định rõ ràng từng mẫu. Tuy nhiên, để đảm bảo bảo vệ dữ liệu cá nhân, định danh của một mẫu không được chứa bất kỳ thông tin nào liên quan đến danh tính thực của chủ thẻ dữ liệu

- Một số lượng đủ lớn các cá nhân nên được đăng ký vào cơ sở dữ liệu để thu được các kết quả có ý nghĩa thống kê. Những con số như vậy phụ thuộc vào tỷ lệ lỗi tối đa cho phép của hệ thống. Tỷ lệ lỗi càng thấp, số lượng chủ thẻ dữ liệu cần thiết càng lớn để đạt được kết quả đáng tin cậy.

- Ngoài ra, các mẫu khác nhau của cùng một chủ đề dữ liệu không nên được thu thập liên tiếp mà để đủ thời gian giữa chúng để mô phỏng sự thay đổi trong đối tượng của các đặc điểm sinh trắc học. Tốt nhất, cơ sở dữ liệu nên được thu thập trong các phiên khác nhau, cách nhau vài tuần giữa chúng.

- Nếu có liên quan, các siêu dữ liệu khác liên quan đến các chủ thẻ dữ liệu cũng có thể được lấy. Điều này có thể bao gồm giới tính, tuổi tác, sử dụng thiết bị hỗ trợ thị giác (ví dụ: kính) hoặc việc thuận tay. Các siêu dữ liệu này có thể giúp điều chỉnh thêm đánh giá hiệu suất hoặc sử dụng lại dữ liệu sinh trắc học trong các đánh giá trong tương lai.

- Việc thu thập dữ liệu sinh trắc học dễ xảy ra nhiều lỗi khác nhau như thiếu mẫu, mẫu không hợp lệ, mẫu chất lượng thấp và sai số trung thực trong đó mẫu được gán không chính xác cho ID của chủ thẻ. Một số lỗi này có thể là kết quả của sự sai sót của con người và có thể được giảm bớt bằng cách áp dụng các kỹ thuật thu thập và ghi dữ liệu tự động.

- Dữ liệu sinh trắc học là thông tin định danh cá nhân (PII). Do đó, các luật lệ về quyền riêng tư của quốc gia sẽ được xác định trong quá trình mua lại.

CHÚ THÍCH: Luật bảo vệ dữ liệu quốc gia ở quốc gia đánh giá có thể tồn tại và có thể được yêu cầu, trong quá trình thu thập, thông báo cho các chủ thẻ dữ liệu thu được về việc sử dụng sẽ được tạo ra từ dữ liệu của họ và nhận được từ họ một biểu mẫu đồng ý có chữ ký để thu thập những dữ liệu đó.

5.3.2 Thực hiện thử nghiệm

Các điều phụ 5.2.2, 5.2.3 và 5.3.1 xác định tất cả các bước ban đầu cần được thực hiện và được lập thành văn bản trong kế hoạch thử nghiệm trước khi đánh giá, nghĩa là, tỷ lệ lỗi liên quan và giá trị tối đa của chúng, loại đánh giá, cơ sở dữ liệu và đánh giá giao thức liên quan đến nó, thu thập dữ liệu. Khi tất cả các bước đó đã được hoàn thành, việc đánh giá sẽ được thực hiện theo kế hoạch đã thiết kế trước. Trong quá trình đánh giá, một số khía cạnh phải được ghi lại như:

- Bất kỳ sai lệch đáng kể nào so với kế hoạch thử nghiệm ban đầu;

- Thời gian cần thiết để thực hiện mỗi thử nghiệm được xem xét trong đánh giá. Thông tin tạm thời khác, có thể được ghi lại tùy thuộc vào đánh giá, là thời gian phản hồi của hệ thống cho mọi nỗ lực truy cập.

Khi các thử nghiệm được thực hiện, kết quả phải được báo cáo bằng cách sử dụng các thước đo tiêu chuẩn (xem 5.1.4.3 và ISO/IEC 19795-1).

5.4 Phân tích

Việc phân tích kết quả không nên chỉ giới hạn trong việc xác định tỷ lệ lỗi mà còn phải bao gồm điều tra sâu hơn về các trường hợp lỗi và liệu những lỗi đó có tiết lộ vấn đề an toàn nào đó của hệ thống hay không [ví dụ: một sự thay đổi đáng kể trong hiệu suất cho các cấu hình chủ thẻ dữ liệu nhất định (ví dụ:

nam và nữ]). Loại phân tích này có thể giúp xác định các tình huống làm việc có vấn đề tiềm ẩn đối với hệ thống.

Cần lưu ý rằng, nói đúng ra, một phân tích như vậy nên thuộc về lĩnh vực của lớp AVA hơn là lớp ATE vì nó sẽ mở ra hướng đi dẫn đến một lỗ hổng tiềm năng của TOE. Các vấn đề an toàn tiềm ẩn được tìm thấy trong quá trình thử nghiệm ATE nên được báo cáo cho hoạt động đánh giá lỗ hổng AVA để điều tra thêm.

Những sai lệch có thể có này so với hiệu suất dự kiến trung bình của hệ thống phải được báo cáo trong tài liệu cuối cùng để có thể biết rõ trong trường hợp nào hệ thống hoạt động như mong đợi (với tỷ lệ lỗi tối đa cho phép) và trong các tình huống tỷ lệ lỗi có thể tăng lên.

Thử nghiệm hiệu suất của hệ thống sinh trắc học trong quá trình đánh giá an toàn tập trung vào tỷ lệ lỗi nhận dạng sinh trắc học liên quan đến an toàn như FAR. Tỷ lệ lỗi khác, ví dụ: FRR, có liên quan đến các yếu tố khác như khả năng sử dụng. Tỷ lệ lỗi liên quan đến an toàn (chẳng hạn như FAR) đổi khi có thể được đổi với tỷ lệ lỗi phụ thuộc lẫn nhau (trong trường hợp này là FRR) thông qua cài đặt ngưỡng quyết định định danh của hệ thống. Do đó, tỷ lệ lỗi phụ thuộc phải được đánh giá và báo cáo tại mỗi điểm vận hành được chỉ định để đánh giá.

5.5 Xem xét các thử nghiệm của nhà phát triển

Trong quá trình thực hiện các hoạt động đánh giá xung quanh ATE_FUN.1, kiểm thử viên sẽ đánh giá tài liệu và kết quả thử nghiệm do nhà phát triển cung cấp.

Nhà phát triển phải tuân theo các yêu cầu từ ISO/IEC 19795-1 và ISO/IEC 19795-2 đối với thử nghiệm hiệu suất của họ. Bất kỳ sai lệch nào cũng phải được chứng minh trong kế hoạch thử nghiệm.

Tập hợp đầy đủ thông tin về thử nghiệm phải được chuyển giao cho kiểm thử viên trong quá trình đánh giá. Chỉ có cách này mới có thể đảm bảo rằng kiểm thử viên có được cái nhìn tổng quan đầy đủ về tất cả các chi tiết của thử nghiệm. Trong bối cảnh này, nhà phát triển phải cung cấp cho kiểm thử viên quyền truy cập đầy đủ vào thiết bị thử nghiệm và dữ liệu thử nghiệm được sử dụng cho thử nghiệm của nhà phát triển.

Kiểm thử viên sẽ đánh giá tài liệu thử nghiệm của nhà phát triển để xác nhận rằng:

- Kế hoạch thử nghiệm của nhà phát triển, việc tiến hành thử nghiệm của nhà phát triển và tài liệu thử nghiệm phù hợp với các yêu cầu nêu trong ISO/IEC 19795-1 (xem Phụ lục C để làm ví dụ);
- Mọi sai lệch so với các yêu cầu trên đều được chứng minh;
- Kết quả thử nghiệm cho thấy tỷ lệ lỗi nhận dạng sinh trắc học liên quan đến an toàn phù hợp với các tuyên bố trong mục tiêu an toàn TOE.

5.6 Yêu cầu cụ thể về các thành phần đảm bảo trên ATE_IND

5.6.1 Tổng quan

Như được mô tả trong TCVN 14190-1, các yếu tố sau của các thành phần đảm bảo yêu cầu kiểm thử viên để tiến hành thử nghiệm TOE của riêng họ:

- ATE_IND.1.2E: Kiểm thử viên phải thử nghiệm một tập hợp con của TSF khi thích hợp để xác nhận rằng TOE hoạt động như được chỉ định;
- ATE_IND.2.3E: Kiểm thử viên sẽ thiết lập và thực hiện một mẫu các thử nghiệm độc lập và ghi lại chúng để đánh giá kết quả thử nghiệm của nhà phát triển."

Tất cả các đánh giá về TOE sinh trắc học phải bao gồm thành phần đảm bảo ATE_IND.2 như được bổ sung bởi TCVN 14190-1.

Các điều phụ 5.2.2 và 5.2.3 bao gồm hướng dẫn chuyên dụng liên quan đến việc đánh giá hai thành phần đó.

5.6.2 Các yêu cầu cụ thể về ATE_IND.1

Các yêu cầu cụ thể được giới thiệu trong TCVN 14190-1 được trình diện trong Bảng 3. Kiểm thử viên lấy một tập hợp con của TSF để được thử nghiệm độc lập theo hướng dẫn trong TCVN 11386 (ISO/IEC 18045). Vì hiệu suất sinh trắc học là một phần thiết yếu của TOE, kiểm thử viên trong mọi trường hợp phải đảm bảo rằng phần này của TSF thuộc tập hợp con.

Bảng 3 - Các yêu cầu cụ thể về ATE_IND.1 từ TCVN 14190-1

ATE_IND.1-3	Kiểm thử viên cũng phải thiết lập thử nghiệm độc lập để đánh giá hiệu suất thiết lập một nhóm thử nghiệm hoặc một tập dữ liệu thử nghiệm.
ATE_IND.1-4	Kiểm thử viên phải đưa ra tài liệu thử nghiệm để đánh giá hiệu suất đáp ứng các yêu cầu liên quan của ISO/IEC 19795. Kiểm thử viên phải giải thích bất kỳ sai lệch nào so với các quy trình thử nghiệm được nêu trong ISO/IEC 19795 và cũng phải mô tả bất kỳ ảnh hưởng và tác động tiềm ẩn nào đối với kết quả thử nghiệm trong tài liệu thử nghiệm.
ATE_IND.1-5	Kiểm thử viên sẽ 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 có.
ATE_IND.1-6	Kiểm thử viên phải ghi lại thông tin của đội thử nghiệm hoặc dữ liệu thử nghiệm dưới dạng đặc điểm theo tiêu chuẩn ISO/IEC 19795
ATE_IND.1-8	Kiểm thử viên cũng sẽ báo cáo trong ETR nỗ lực thử nghiệm của kiểm thử viên về hiệu suất nhận dạng sinh trắc học về kích thước thử nghiệm, thời gian sử dụng và cả các đặc điểm của tập dữ liệu.

Các thử nghiệm được tiến hành phải tuân theo các yêu cầu và khuyến nghị được liệt kê trong 5.2, 5.3 và 5.4.

5.6.3 Các yêu cầu cụ thể về ATE_IND.2

Các yêu cầu cụ thể được giới thiệu trong TCVN 14190-1 được trình diện trong Bảng 4. Thử nghiệm sinh trắc học rất phức tạp, tốn thời gian và tốn kém. Cụ thể, việc thu thập đủ dữ liệu thử nghiệm là một thách thức đối với mọi thử nghiệm. Do đó, một câu hỏi quan trọng là liệu dữ liệu thử nghiệm mà nhà phát triển đã sử dụng có thể được sử dụng lại hoàn toàn khi lặp lại thử nghiệm từ tài liệu thử nghiệm của nhà phát triển trong bối cảnh ATE_IND.2 hay không. Hướng dẫn về chủ đề này được cung cấp trong 5.8.

Bảng 4 - Các yêu cầu cụ thể về ATE_IND.2 từ TCVN 14190-1

ATE_IND.2-6	Kiểm thử viên cũng phải thiết lập thử nghiệm độc lập để đánh giá hiệu suất thiết lập một nhóm thử nghiệm hoặc một tập dữ liệu thử nghiệm.
ATE_IND.2-7	Kiểm thử viên phải đưa ra tài liệu thử nghiệm để đánh giá hiệu suất đáp ứng các yêu cầu liên quan của ISO/IEC 19795. Kiểm thử viên phải giải thích bất kỳ sai lệch nào so với các quy trình thử nghiệm được nêu trong ISO/IEC 19795 và cũng phải mô tả bất kỳ ảnh hưởng và tác động tiềm ẩn nào đối với kết quả thử

	nghiệm trong tài liệu thử nghiệm.
ATE_IND.2-8	Kiểm thử viên sẽ 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 có.
ATE_IND.2-9	Kiểm thử viên phải ghi lại thông tin của đội thử nghiệm hoặc dữ liệu thử nghiệm dưới dạng đặc điểm theo tiêu chuẩn ISO/IEC 19795.
ATE_IND.2-11	Kiểm thử viên cũng phải báo cáo trong ETR nỗ lực thử nghiệm của kiểm thử viên về hiệu suất nhận dạng sinh trắc học về kích thước thử nghiệm, thời gian sử dụng và cả các đặc điểm của tập dữ liệu.

Các thử nghiệm được tiến hành phải tuân theo các yêu cầu và khuyến nghị được liệt kê trong 5.2, 5.3, 5.4 và 5.7.

5.7 Đánh giá các thử nghiệm của nhà phát triển bằng cách lặp lại một tập hợp con thử nghiệm

Các yêu cầu của ATE_IND.2 yêu cầu kiểm thử viên lặp lại một tập hợp con các thử nghiệm của nhà phát triển. Các thử nghiệm về tỷ lệ lỗi nhận dạng sinh trắc học liên quan đến an toàn sẽ tạo thành một phần của tập hợp con được lặp lại.

Khi lặp lại thử nghiệm tỷ lệ lỗi nhận dạng sinh trắc học liên quan đến an toàn của hệ thống sinh trắc học, chúng ta thường đặt ra câu hỏi liệu chỉ cần lặp lại thử nghiệm của nhà phát triển là đủ. Điều này có liên quan cụ thể nếu nhà phát triển quản lý để tách việc thu thập dữ liệu thử nghiệm khỏi thử nghiệm thực tế của thuật toán sinh trắc học. Trong những trường hợp đó, kiểm thử viên có thể quyết định chỉ cần lặp lại thử nghiệm.

Các khả năng cho kiểm thử viên cũng phụ thuộc vào loại thử nghiệm sinh trắc học mà nhà phát triển thực hiện:

- Trong trường hợp thử nghiệm công nghệ, kiểm thử viên có khả năng lựa chọn sử dụng cùng một dữ liệu sinh trắc được nhà phát triển sử dụng hoặc lấy một nguồn dữ liệu sinh trắc mới;

- Trong trường hợp thử nghiệm kịch bản, kiểm thử viên có thể sử dụng cùng nhóm thử nghiệm với nhà phát triển. Nếu không, một đội thử nghiệm mới sẽ phải được tuyển dụng. Trong trường hợp kiểm thử viên nhận định rằng việc lặp lại một tập hợp con các thử nghiệm của nhà phát triển có thể bị hạn chế đối với thử nghiệm công nghệ, họ có thể sử dụng lại dữ liệu sinh trắc học thu được từ nhóm thử nghiệm của nhà phát triển (nếu có) hoặc sử dụng nguồn dữ liệu sinh trắc mới.

Khi có thể, kiểm thử viên nên tận dụng những nỗ lực mà nhà phát triển đã bỏ ra để thu thập dữ liệu thử nghiệm bằng cách sử dụng lại dữ liệu này khi thực hiện thử nghiệm. Trên cơ sở này, khi có thể, kiểm thử viên được khuyến khích thực hiện theo chiến lược này: sử dụng lại dữ liệu thử nghiệm của nhà phát triển khi thực hiện một tập hợp con các thử nghiệm của nhà phát triển. Để tránh việc thử nghiệm lặp lại thuận tiện bằng cách sử dụng chính xác cùng một dữ liệu, kiểm thử viên phải xem xét việc thay thế một tập hợp con của dữ liệu thử nghiệm bằng dữ liệu của chính họ (kiểm thử viên phải có được theo 5.3.1). Kiểm thử viên có trách nhiệm quyết định về kích thước của tập hợp con này. Họ sẽ xem xét chất lượng tổng thể của dữ liệu thử nghiệm của nhà phát triển và chất lượng của quá trình thu thập (dựa trên tài liệu của nó). Thay vì thay thế một tập hợp con, kiểm thử viên có thể bổ sung dữ liệu của nhà phát triển bằng dữ liệu của chính họ. Về mặt kỹ thuật, điều cần thiết là tập dữ liệu con được trao

đổi hoặc tập dữ liệu bổ sung phải đủ lớn để đảm bảo rằng nhà phát triển không thể điều chỉnh thuật toán của họ dựa trên cơ sở dữ liệu.

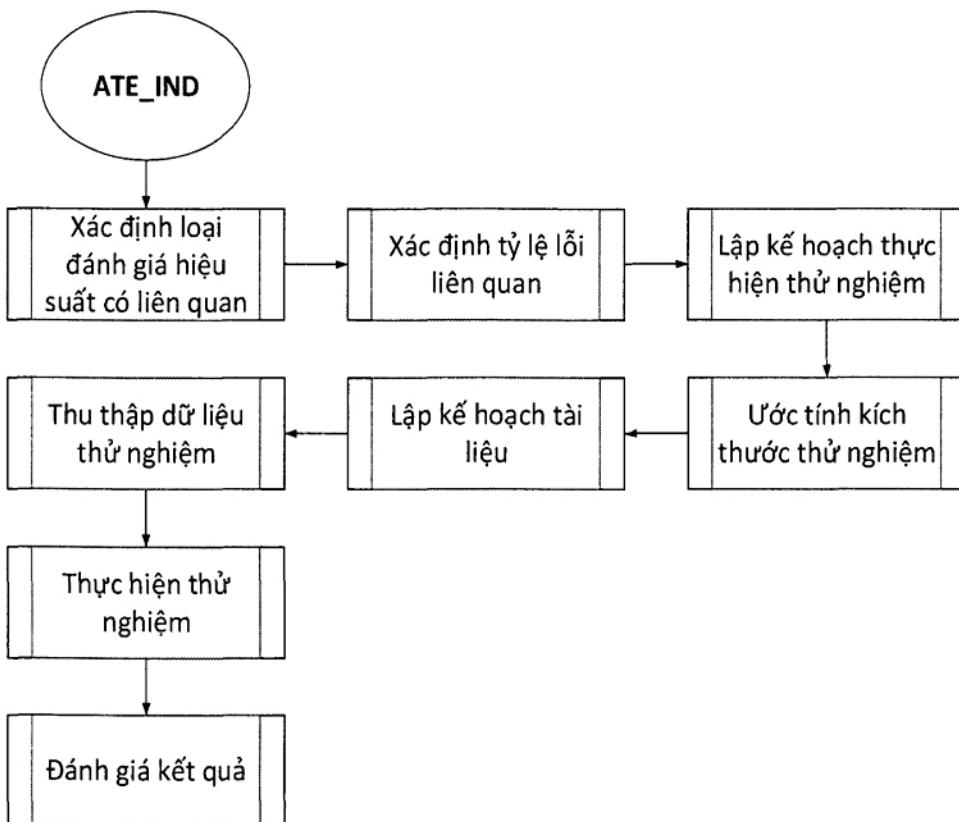
Dữ liệu sinh trắc học là thông tin định danh cá nhân (PII). Do đó, luật pháp về quyền riêng tư của quốc gia sẽ được xác định trong quá trình thử nghiệm, ngay cả khi lặp lại thử nghiệm của nhà phát triển với một số dữ liệu thử nghiệm hiện có.

5.8 Tiến hành thử nghiệm độc lập

5.8.1 Tổng quan

ATE_IND.1 (cũng như ATE_IND.2 và ATE_IND.3) yêu cầu kiểm thử viên tiến hành thử nghiệm riêng của họ về tỷ lệ lỗi nhận dạng sinh trắc học liên quan đến an toàn của TOE. Điều 5.8 cung cấp cho kiểm thử viên hướng dẫn tương ứng. Hình 1 tóm tắt các bước khác nhau mà kiểm thử viên sẽ thực hiện khi lập kế hoạch, tiến hành và báo cáo thử nghiệm độc lập về tỷ lệ lỗi nhận dạng sinh trắc học liên quan đến an toàn của hệ thống sinh trắc học.

Như đã giới thiệu trong 5.1.1, theo nguyên tắc mặc định, kiểm thử viên phải tuân theo các khuyến nghị được giới thiệu trong điều này (ví dụ: về tỷ lệ lỗi, giá trị tối đa, phương pháp thử nghiệm của nhà phát triển, v.v.). Nếu kiểm thử viên nhận định rằng họ không được lựa chọn thích hợp liên quan đến TOE và ứng dụng, thì người đó phải biện minh cho các lựa chọn khác trong báo cáo đánh giá.



Hình 1 - Các quy trình để thử nghiệm độc lập

Quá trình này có thể được chia thành các bước sau được mô tả chi tiết hơn trong các điều từ 5.1 đến 5.4.

- Xác định loại đánh giá hiệu suất có liên quan: Có nhiều loại phương pháp thử nghiệm khác nhau bắt đầu từ thử nghiệm hiệu suất công nghệ của thuật toán sinh trắc học đến đánh giá thử nghiệm hiệu suất hoạt động của hệ thống sinh trắc học. Cách tiếp cận thử nghiệm chính xác phụ thuộc nhiều vào chức năng được cung cấp bởi TOE.

- Xác định tỷ lệ lỗi liên quan: Vì đánh giá an toàn chỉ tập trung vào tỷ lệ lỗi nhận dạng sinh trắc học liên quan đến an toàn, không phải tất cả tỷ lệ lỗi của hệ thống sinh trắc học đều có liên quan. Việc xác định tỷ lệ lỗi liên quan được thực hiện dựa trên loại hệ thống sinh trắc học và trường hợp ứng dụng của nó như được xác định trong mục tiêu an toàn.

- Lập kế hoạch thực hiện thử nghiệm: Việc thực hiện thử nghiệm thực tế phải được lên kế hoạch trước.

- Ước tính kích thước thử nghiệm: Việc thu thập dữ liệu thử nghiệm chiếm một lượng đáng kể nỗ lực của thử nghiệm tổng thể. Điều cần thiết là phát triển ý tưởng về lượng dữ liệu thử nghiệm được yêu cầu trước khi bắt đầu quá trình thu thập dữ liệu thử nghiệm thực tế.

- Lập kế hoạch tài liệu: Điều cần thiết là lập kế hoạch tài liệu cần thiết cho thử nghiệm trước tự thử nghiệm.

- Thu thập dữ liệu thử nghiệm: Dữ liệu thử nghiệm bao gồm các mẫu sinh trắc học phù hợp sẽ được thu thập từ các trình diện trực tiếp của các thành viên trong nhóm thử nghiệm hoặc sử dụng kho mẫu sinh trắc học có sẵn, tùy thuộc vào loại thử nghiệm (kịch bản hoặc công nghệ) và phương pháp thử nghiệm. Trong cả hai trường hợp, dữ liệu thử nghiệm phải bao gồm cái gọi là sự thật cơ bản, tức là kiến thức về nguồn của mỗi mẫu (ví dụ: ID đối tượng) để, với kho tài liệu, cả thử nghiệm so sánh theo cặp và thử nghiệm so sánh không theo cặp có thể được thực hiện. Để đảm bảo chất lượng của các kết quả thử nghiệm, kiểm thử viên phải sử dụng dữ liệu thử nghiệm mà nhà phát triển TOE không biết.

- Thực hiện thử nghiệm: Thử nghiệm phải được thực hiện dưới sự kiểm soát và chịu trách nhiệm duy nhất của kiểm thử viên.

- Đánh giá kết quả: Kết quả thử nghiệm phải được đánh giá và báo cáo bằng cách sử dụng các thước đo tiêu chuẩn.

Kiểm thử viên phải tuân theo các yêu cầu từ ISO/IEC 19795-1 đối với các thử nghiệm vận hành của họ. Mọi sai lệch phải được chứng minh trong kế hoạch thử nghiệm và được ghi lại trong báo cáo thử nghiệm.

Trong trường hợp thử nghiệm công nghệ bằng cách sử dụng kho dữ liệu mẫu sinh trắc học đã có từ trước, kiểm thử viên phải đưa ra lời biện minh rằng kho tài liệu đáp ứng nhu cầu của thử nghiệm và độc lập với dữ liệu thử nghiệm của nhà phát triển.

5.8.2 Xác định loại hình đánh giá hiệu suất

Loại đánh giá được thực hiện chủ yếu phụ thuộc vào định nghĩa của TOE và loại đánh giá hiệu suất của nhà phát triển. Kiểm thử viên nên xác minh rằng loại đánh giá của nhà phát triển là phù hợp. Nếu đúng như vậy, kiểm thử viên cũng nên làm theo. Nếu không phù hợp, kiểm thử viên có thể tự do tiến hành thử nghiệm độc lập sau một loại hình khác. Nếu kiểm thử viên không tuân theo cùng một kiểu đánh giá thì kiểm thử viên phải biện minh cho động cơ trong báo cáo thử nghiệm. Nếu TOE chỉ được

tạo ra từ các chức năng phần mềm, có khả năng nhà phát triển sẽ quyết định thực hiện đánh giá công nghệ và kiểm thử viên, nếu thích hợp, phải thực hiện đánh giá công nghệ tương tự. Nếu TOE là một hệ thống sinh trắc học hoàn chỉnh, đặc biệt là với một bộ cảm biến, thì nhiều khả năng nó sẽ được nhà phát triển thử nghiệm trong kịch bản đánh giá và do đó, kiểm thử viên nên thực hiện kịch bản đánh giá. Lưu ý rằng nếu một TOE không cung cấp các chức năng so sánh và quyết định, thì hiệu suất nhận dạng sinh trắc học của nó không thể được thử nghiệm. Cũng cần lưu ý rằng thử nghiệm kịch bản có thể bao gồm thử nghiệm ngoại tuyến các thuật toán phần mềm nhằm mục đích thử nghiệm so sánh chéo để đo lường tỷ lệ thành tích hiệu suất và tỷ lệ lỗi và để xác định các ô DET.

6 Các hoạt động bổ sung cho TCVN 11386 (ISO/IEC 18045) về đánh giá tính dễ bị tổn thương (AVA)

6.1 Các khía cạnh chung

Điều khoản này đưa ra các điều khoản và bổ sung cho các hoạt động đánh giá từ Điều 15 của TCVN 14190-1:2024, liên quan đến các lỗ hổng do lỗi nhận dạng sinh trắc học có thể xảy ra khi trình diện các đặc điểm sinh trắc học tự nhiên không theo cặp hoặc khi tiêm hoặc thay đổi sinh trắc học không theo cặp đặc điểm sau khi hệ thống con nắm bắt dữ liệu. Các lỗ hổng liên quan đến lỗi phát hiện tấn công trình diện đối với các tấn công trình diện sinh trắc học sử dụng PAI được đề cập đến trong TCVN 14190-3.

Mục đích của điều khoản này là giới thiệu bối cảnh và cung cấp hướng dẫn chung cho kiểm thử viên. Mỗi lỗ hổng an toàn là một trường hợp cụ thể, các ví dụ trong Phụ lục A sẽ cung cấp một số hướng dẫn cụ thể cho kiểm thử viên. Tuy nhiên, kiểm thử viên sẽ đề ra chiến lược của riêng mình dựa trên kiến thức chuyên môn của họ và cá thể TOE được đánh giá.

Ngoài các yêu cầu và khuyến nghị được cung cấp trong Điều 6, kiểm thử viên cũng phải tuân theo các yêu cầu đối với các thành phần đảm bảo được TOE lựa chọn cho lớp AVA trong TCVN 8709-3 (ISO/IEC 15408-3) và phải tuân theo các yêu cầu của các hoạt động tương ứng trong TCVN 11386 (ISO/IEC 18045).

Mục tiêu của nhiệm vụ đánh giá là tìm kiếm các lỗ hổng và chứng minh rằng TOE có khả năng chống lại một khả năng tấn công nhất định và được xác định trước.

CHÚ THÍCH 1: Nếu TOE bao gồm chức năng PAD, kiểm thử viên sẽ đánh giá các lỗ hổng trong bối cảnh của toàn bộ hệ thống để tính đến các tương tác tiềm ẩn giữa các thành phần con.

CHÚ THÍCH 2: Đề cập đến các mối đe dọa được liệt kê trong TCVN 14190-1:2024, 6.1, a) đến j), các mối đe dọa và các hoạt động đánh giá được đề cập trong TCVN 14190-2 đối với việc đánh giá tính dễ bị tổn thương của hệ thống xác minh hoặc nhận dạng sinh trắc học chủ yếu liên quan khai thác tiềm năng của a) Hạn chế về hiệu suất, h) Môi trường thù địch, i) Các lỗ hổng thủ tục xung quanh quá trình đăng ký, để tấn công hệ thống, cùng với các tác động có thể xảy ra của j) Rò rỉ và thay đổi dữ liệu sinh trắc học, e) Tương tự do máu mối quan hệ, f) Các đặc điểm sinh trắc học đặc biệt và g) Các mẫu sinh trắc học Wolf tổng hợp có thể giúp kiểm thử viên xác định các điểm yếu cụ thể và tiến hành tấn công hiệu quả hơn.

Cách tiếp cận được thực hiện ở đây là một minh chứng đối chiếu: để đánh giá một TOE ở mức độ chống an toàn được nhắm mục tiêu, tức là ở một giá trị tiềm năng tấn công tối thiểu được nhắm mục tiêu cho các lỗ hổng được tìm thấy trên TOE, nếu một cuộc tấn công với khả năng tấn công thấp hơn mức được nhắm mục tiêu được tìm thấy, thì chứng minh rằng TOE không chống lại mức này. Vì vậy, việc đánh giá tập trung vào việc tìm ra một cuộc tấn công có thể áp dụng cho TOE trong bối cảnh sử dụng của nó và với mức đánh giá thấp hơn mức được nhắm mục tiêu.

Định nghĩa về một cuộc tấn công thành công sẽ được thực hiện liên quan đến các định nghĩa an toàn của mục tiêu an toàn (ST) và phải tạo ra một thất bại trong các mục tiêu an toàn của TOE (truy cập vào dữ liệu bị cấm, hoạt động trái phép, v.v.).

Kiến thức được kiểm thử viên sử dụng để xác định một cuộc tấn công và một đường dẫn tấn công là tất cả những kiến thức sẵn có, bao gồm kiến thức nền tảng cụ thể trong lĩnh vực (để được công nhận, phòng thí nghiệm phải chứng minh năng lực của mình trong lĩnh vực đó), kiến thức công khai (web, chuyên dụng hội nghị, v.v.) mà còn cả kiến thức về TOE thu được từ các nhiệm vụ đánh giá khác (ví dụ, kiến thức về việc triển khai nếu nhắm mục tiêu AVA_VAN.3 trở lên).

Mục tiêu của thử nghiệm đánh giá là để xác định xem TOE có dễ bị tấn công bởi một cuộc tấn công cụ thể vào tiềm năng tấn công được nhắm mục tiêu hay không (ví dụ lấy cảm hứng từ các mối đe dọa được liệt kê trong CHÚ THÍCH 2). Chuẩn bị để thử nghiệm kiểm thử viên nên thực hiện đánh giá tiềm năng tấn công sơ bộ dựa trên các đặc điểm kỹ thuật của cuộc tấn công (cuộc tấn công là gì, cách thức thử nghiệm cuộc tấn công được tiến hành và kết quả được giải thích như thế nào). Xếp hạng tấn công sơ bộ có thể được sử dụng để ưu tiên thử nghiệm (xếp hạng càng thấp, mức độ ưu tiên càng cao). Kiểm thử viên có thể thử nghiệm các đường tấn công mà đánh giá sơ bộ là trên tiềm năng tấn công mục tiêu.

Khi danh sách thử nghiệm được thiết lập, kiểm thử viên thực hiện các cuộc tấn công tương ứng và trong trường hợp thành công sẽ thực hiện xếp hạng cuối cùng. Xếp hạng này sau đó được sử dụng để xác nhận hoặc bác bỏ mức kháng cự của TOE.

CHÚ THÍCH 3 Nhà phát triển thường mong đợi thêm một số thông tin từ đánh giá: tất cả các điểm yếu của sản phẩm của tôi là gì? Tất cả các cuộc tấn công để chống lại trong một sản phẩm được chứng nhận là gì? Thông tin này là một giá trị gia tăng cho báo cáo đánh giá. Tuy nhiên, việc đánh giá an toàn theo tiêu chuẩn TCVN 8709 (ISO/IEC 15408) và TCVN 11386 (ISO/IEC 18045) không được yêu cầu nghiêm ngặt trong đó một cuộc tấn công thành công duy nhất có thể dừng quá trình đánh giá và không có gì đảm bảo rằng, trong trường hợp tấn công thành công, tất cả điều có thể các cuộc tấn công đã được thử nghiệm và TOE có khả năng chống lại tất cả các cuộc tấn công có thể xảy ra khác.

6.2 TOE để thử nghiệm

Nhà phát triển phải cung cấp TOE để thử nghiệm và TOE phải phù hợp để thử nghiệm.

Định nghĩa chính xác về TOE được chuyển giao phải được thực hiện bằng cách tham chiếu đến các hướng dẫn: bất kỳ tùy chọn, cấu hình, tham số nào được tham chiếu trong các chủ đề hoặc hướng dẫn quản trị phải có sẵn cho kiểm thử viên. Đặc biệt, một hệ thống sinh trắc học nên cho phép kiểm thử viên ghi danh những người cụ thể.

Ngoài ra, khi cần thiết bị bổ sung để sử dụng TOE, nhà phát triển phải cung cấp nó cho kiểm thử viên (ví dụ, nếu TOE được định nghĩa là thiết bị / cảm biến thu thập sinh trắc học, phần cứng và / hoặc phần mềm để kết nối với máy tính và thu nhận, xử lý và khai thác dữ liệu).

Trong một số trường hợp, trình giả lập hoặc trình mô phỏng tồn tại và được nhà phát triển sử dụng để xác thực một phần của TOE (ví dụ, quá trình so sánh và xác nhận nó trên một cơ sở dữ liệu lớn về hình ảnh). Những điều này nên được cung cấp cho kiểm thử viên.

6.3 Các lỗ hổng tiềm năng

Các lỗ hổng mà kiểm thử viên cần phân tích ít nhất phải tinh đến những điểm yếu được giới thiệu trong TCVN 14190-1:2024, 6.1.

Ngoài ra, kiểm thử viên sẽ xem xét sự kết hợp của các lỗ hổng đó với các lỗ hổng khác liên quan đến CNTT. Ví dụ: khi xem xét khả năng thực hiện một cuộc tấn công leo đồi, kiểm thử viên sẽ không hạn chế vòng phản hồi đối với việc đọc điểm mà còn phải ước tính khả năng suy ra thông tin liên quan đến điểm (ví dụ: dựa trên thời gian thực hiện hoặc kênh bên Sự rò rỉ).

CHÚ THÍCH: Như đã nêu rõ trong Điều 6 của TCVN 11385:2016 (ISO/IEC 19792:2009), kiểm thử viên cũng xem xét toàn bộ hệ thống và các tương tác giữa các thành phần con, vì lỗ hổng của một thành phần con có thể được bù đắp bởi một thành phần con khác.

Kiểm thử viên phải tuân theo Điều 8 của TCVN 11385:2016 (ISO/IEC 19792:2009), để đánh giá các lỗ hổng tiềm năng có thể kết hợp với các hạn chế về hiệu suất nhận dạng sinh trắc học.

6.4 Đánh giá khả năng tấn công

Đối với lớp AVA (đánh giá lỗ hổng), việc đánh giá (tức là xếp hạng các yếu tố khác nhau, tính toán khả năng tấn công và so sánh với mức mục tiêu) sẽ được thực hiện theo TCVN 14190-1, cũng như việc xem xét cuộc tấn công, tiềm năng (xem TCVN 14190-1:2024, Phụ lục F).

Các ví dụ xếp hạng liên quan đến các lỗ hổng về hiệu suất nhận dạng sinh trắc học được cung cấp trong Phụ lục A.

PHỤ LỤC A
(tham khảo)

Ví dụ về tính toán tiềm năng tấn công cho các hoạt động AVA

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) và các cuộc tấn công "cỗ điển" có thể được áp dụng. Các tính toán về khả năng tấn công được thực hiện theo TCVN 14190-1:2024, Phụ lục F.

A.2 Leo đồi

VÍ DỤ: Hãy xem xét một hệ thống dựa trên dấu vân tay hoạt động trong một môi trường không được kiểm soát (ví dụ: bảo vệ quyền truy cập vào một hạng mục thiết bị). Giả sử rằng có một cách dễ dàng kết nối máy tính ngay trước quá trình so sánh, cho phép chương trình đưa các mẫu thăm dò ở định dạng phù hợp để so sánh và điểm so sánh có sẵn (ví dụ: thông qua kết nối gõ lỗi). Cuộc tấn công bao gồm tiềm các mẫu thăm dò (ví dụ, bắt đầu với các vị trí ngẫu nhiên của vụn vặt) và dễ tối ưu hóa vị trí bằng cách sử dụng điểm so sánh trong một cuộc tấn công được gọi là "leo đồi".

Kịch bản tấn công này có thể tương ứng với hai mục tiêu khác nhau: Một có thể liên quan đến rò rỉ quyền riêng tư (để tìm hiểu thông tin về dữ liệu đã đăng ký), một có thể liên quan đến giả mạo xác thực (tức là kẻ tấn công tìm cách đạt được xác thực đối với một người đăng ký cụ thể).

Nó được coi là:

- Thời gian cần sử dụng: Giai đoạn định danh tương ứng với việc tìm ra giao diện phù hợp với hệ thống (kết nối máy tính với các tín hiệu được nhắm mục tiêu, cho phép trình diện các mẫu đã xây dựng) và lấy hoặc viết phần mềm tối ưu hóa cho việc tạo mẫu. Nó được coi là dễ dàng trong ví dụ này. Giai đoạn khai thác chỉ là chạy chương trình để có quyền truy cập. 2 tuần để xác định và 1 ngày để khai thác là thực tế;

- Chuyên môn: Ngay cả khi phương pháp tấn công được biết đến và công bố, việc thiết lập các kết nối phù hợp, khai thác các tín hiệu cụ thể và điều chỉnh một phần mềm tối ưu hóa được coi là yêu cầu trình độ chuyên gia để xác định và mức độ thành thạo để khai thác;

- Kiến thức về TOE: Cần có kiến thức sâu về TOE (các định dạng khuôn mẫu, giao thức nội bộ, v.v.) vì vậy cần phải có kiến thức nhạy cảm;

- Cơ hội (truy cập vào TOE): TOE hoạt động trong môi trường không được kiểm soát (được đánh giá là dễ dàng cho giai đoạn khai thác) và nó được coi là hệ thống dễ mua (được đánh giá là dễ dàng cho giai đoạn xác định);

- Cơ hội (truy cập vào các đặc điểm sinh trắc học): Nó được đánh giá là tức thời vì cuộc tấn công không yêu cầu sự sẵn có của dữ liệu thực (mẫu tổng hợp);

- Thiết bị: Cần có thiết bị chuyên dụng (máy tính, kết nối với hệ thống, và chuyên dụng phần lớn là do tạo khuôn mẫu, phần mềm tối ưu hóa) để định danh. Để khai thác, vì phần mềm có sẵn, thiết bị được xếp hạng tiêu chuẩn.

Với các giả định trên, bao tóm tắt tính toán tiềm năng tấn công tương ứng được cung cấp trong Bảng A.1.

Bảng A.1 - Tính toán khả năng tấn công cho tình huống trong A.2

Thời gian cần sử dụng		Chuyên môn		Kiến thức về TOE		Cơ hội				Thiết bị		Tổng số	
						Truy cập vào TOE		Tiếp cận với các đặc tính sinh học				16	
Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp
2	0	4	4	4	-	0	0	-	0	2	0	12	4

Đánh giá cho cuộc tấn công là 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 xếp hạng thấp hơn, sức đề kháng của TOE là cơ bản.

Hệ thống tương thích với thành phần AVA_VAN.2.

A.3 Tấn công kết hợp (nhận điểm so sánh theo cách gián tiếp)

Ví dụ: Giả sử hệ thống tương tự như ví dụ trước, ngoại trừ tín hiệu điểm so sánh không thể được truy cập trực tiếp. Tuy nhiên, một quan sát gián tiếp về quá trình so sánh, ví dụ như thông qua mức tiêu thụ điện năng hoặc thời gian xử lý, có thể cung cấp thông tin về điểm so sánh (phương pháp này được sử dụng rộng rãi trong đánh giá thẻ thông minh và được gọi là tấn công kênh bên).

Tấn công kết hợp được coi là:

- Như trong ví dụ trước, giai đoạn định danh tương ứng với việc tìm ra giao diện phù hợp với hệ thống [thu nhận các tín hiệu nội bộ (tiêu thụ, thời gian), kết nối máy tính với các tín hiệu được nhắm mục tiêu, cho phép trình diễn các mẫu đã xây dựng] và lấy hoặc ghi phần mềm tối ưu hóa cho việc tạo mẫu. Giai đoạn khai thác tương ứng với việc thực hiện thu nhận và xử lý tín hiệu tới TOE thực và chạy chương trình tối ưu hóa để có được quyền truy cập;

- Thời gian cần sử dụng: Trên 1 tháng để xác định và 1 ngày (dưới một tuần) để khai thác là thực tế;

- Chuyên môn: Cần có nhiều chuyên môn [điện tử, thu nhận và xử lý tín hiệu, sinh trắc học (định dạng và tạo mẫu), tối ưu hóa] cho giai đoạn định danh. Ngay cả khi được viết theo kịch bản, cần phải có cấp chuyên gia để khai thác (phần mềm để tạo và tối ưu hóa khuôn mẫu được viết và chỉ cần được sử dụng nhưng phải thực hiện thiết bị vật lý của TOE);

- Kiến thức về TOE: Cần có kiến thức sâu về TOE (các định dạng khuôn mẫu, giao thức nội bộ, v.v.). Cần có kiến thức nhạy bén;

- Cơ hội (Tiếp cận TOE): TOE hoạt động trong một môi trường hoàn toàn không được kiểm soát (được đánh giá là dễ dàng cho giai đoạn khai thác) và nó được coi là hệ thống dễ mua (được đánh giá là dễ dàng cho giai đoạn xác định);

- Cơ hội (truy cập vào các đặc điểm sinh trắc học): Nó được đánh giá là tức thời vì cuộc tấn công không yêu cầu sự sẵn có của dữ liệu thực (mẫu tổng hợp);

- Thiết bị: Cần có nhiều thiết bị chuyên dụng cho giai đoạn định danh (thu nhận và xử lý tín hiệu, máy tính, kết nối với hệ thống, tạo mẫu, phần mềm tối ưu hóa). Đối với việc khai thác, vì phần mềm được coi như đã viết, nên thiết bị chuyên dụng là đủ.

Với các giả định trên, bản tóm tắt tính toán tiềm năng tấn công tương ứng được cung cấp trong Bảng A.2.

Bảng A.2 - Tính toán khả năng tấn công cho kịch bản trong A.3

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				36	
Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp
8	0	8	8	4	-	0	0	-	0	4	4	24	12

Đánh giá cho cuộc tấn công là cao.

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

Hệ thống tương thích với thành phần AVA_VAN.4.

A.4 Tấn công sinh trắc học nghịch đảo

Ví dụ: Giả sử hệ thống này là một hệ thống dựa trên mảng mắt hoạt động trong một môi trường không được kiểm soát (ví dụ: bảo vệ quyền truy cập vào một thiết bị hoặc một thiết bị). Có một cách dễ dàng để kết nối máy tính ngay trước bộ trích xuất tính năng, cho phép chương trình đưa mẫu tổng hợp vào và có tín hiệu tương ứng với điểm so sánh (ví dụ: thông qua kết nối gỡ lỗi). Cuộc tấn công bao gồm tiêm các mẫu tổng hợp được tái tạo lại và tối ưu hóa chúng bằng cách sử dụng điểm so sánh.

Lưu ý sự khác biệt chính giữa cuộc tấn công sinh trắc học nghịch đảo này và cuộc tấn công leo đồi được mô tả trong A.2 là điểm vào của cuộc tấn công, trước bộ so sánh cho việc leo đồi (tức là sau bộ trích xuất đối tượng địa lý) và trước bộ trích xuất đối tượng địa lý cho cuộc tấn công sinh trắc học nghịch đảo. Do đó, cuộc tấn công sinh trắc học nghịch đảo yêu cầu chuyên môn hơn trong việc xác định, vì đầu vào thực tế cho trích xuất tính năng cần được tạo ra trong mỗi lần lặp lại của cuộc tấn công (đây là lý do tại sao cuộc tấn công được gọi là sinh trắc học nghịch đảo) vì vậy xếp hạng kết quả ở đây cao hơn so với đến cuộc tấn công leo đồi ở A.2.

Tấn công nghịch đảo được coi là:

- Giai đoạn định danh tương ứng với việc tìm ra giao diện phù hợp với hệ thống (kết nối máy tính với các tín hiệu được nhắm mục tiêu, cho phép trình diện các mẫu tổng hợp) và lấy hoặc viết phần mềm tối ưu hóa cho việc tạo mẫu tổng hợp. Nó được coi là dễ dàng trong ví dụ này. Giai đoạn khai thác chỉ là chạy chương trình để có quyền truy cập;

- Thời gian cần sử dụng: 2 tuần để xác định và 1 ngày để khai thác là thực tế;

- Chuyên môn: Ngay cả khi phương pháp tấn công được biết đến và công bố, việc thiết lập các kết nối phù hợp, khai thác các tín hiệu cụ thể và điều chỉnh một phần mềm tối ưu hóa được coi là yêu cầu trình độ chuyên gia để xác định và mức độ thành thạo để khai thác;

- Kiến thức về TOE: Cần có mức kiến thức hạn chế về TOE;

- Cơ hội (truy cập vào TOE): TOE hoạt động trong một môi trường hoàn toàn không được kiểm soát (được đánh giá là dễ dàng cho giai đoạn khai thác) và nó được coi là hệ thống dễ mua (được đánh giá là dễ dàng cho giai đoạn xác định);

- Cơ hội (truy cập vào các đặc điểm sinh trắc học): Nó được đánh giá là tức thời vì cuộc tấn công không yêu cầu sự sẵn có của dữ liệu thực (mẫu tổng hợp);

- Thiết bị: Cần có thiết bị chuyên dụng (máy tính, kết nối với hệ thống, tạo mẫu tổng hợp, phần mềm tối ưu hóa) để định danh. Đối với khai thác, phần mềm được coi là có sẵn, đánh giá là tiêu chuẩn.

Với các giả định trên, bản tóm tắt tính toán tiềm năng tấn công tương ứng được cung cấp trong Bảng A.3.

Bảng A.3 - Tính toán khả năng tấn công cho kịch bản trong A.4

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				14	
Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp
2	0	4	4	2	-	0	0	-	0	2	0	10	4

Đánh giá cho cuộc tấn công là 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 xếp hạng thấp hơn, khả năng chống chịu của TOE là cơ bản.

Hệ thống tương thích với thành phần AVA_VAN.2.

A.5 Tấn công từ điển

Ví dụ: Giả sử hệ thống là một mảng mắt, một hai tròng đèn hoặc một hệ thống dựa trên khuôn mặt hoạt động trong một môi trường không được kiểm soát (ví dụ, bảo vệ quyền truy cập vào một thiết bị hoặc một thiết bị). Có một cách dễ dàng để kết nối máy tính ngay trước trình giải nén tính năng. Tuy nhiên, bây giờ không cần thiết phải truy cập vào điểm so sánh. Cuộc tấn công bao gồm việc gửi, bằng cách tiêm sau khi hệ thống con thu thập dữ liệu, các mẫu sinh trắc học thực đến hệ thống cho đến khi một mẫu được chấp nhận.

Tấn công từ điển được coi là:

- Giai đoạn định danh tương ứng với giao diện tìm kiếm phải với hệ thống (kết nối máy tính với các tín hiệu được nhắm mục tiêu, cho phép trình diễn các hình ảnh sinh trắc học). Điều này được coi là dễ dàng trong ví dụ này. Giai đoạn khai thác chỉ là nhập hình ảnh để có quyền truy cập;

- Thời gian cần sử dụng: 2 tuần để xác định và khai thác thực tế;

- Chuyên môn: Kẻ tấn công thành thạo sẽ có thể xác định vị trí đầu vào của trình trích xuất tính năng bằng một số thiết bị chuyên dụng, và do đó chèn các hình ảnh mẫu vào hệ thống;

- Kiến thức về TOE: Cần có kiến thức hạn chế về TOE;

- Cơ hội (truy cập vào TOE): TOE hoạt động trong một môi trường không được kiểm soát (được đánh giá là dễ dàng cho giai đoạn khai thác) và nó được coi là hệ thống dễ mua (được đánh giá là dễ dàng cho giai đoạn xác định);

- Cơ hội (tiếp cận các đặc điểm sinh trắc học): Cuộc tấn công từ điển được tiến hành bằng cách sử dụng các mẫu thực. Có được một cơ sở dữ liệu khuôn mặt lớn cho cuộc tấn công là rất dễ dàng (được đánh giá là ngay lập tức) nhưng có được một cơ sở dữ liệu móng mắt đủ lớn có thể rất khó và thậm chí còn nhiều thách thức hơn đối với hai tròng mắt. Xếp hạng trong khai thác đối với khả năng tiếp cận các đặc điểm sinh trắc học phản ánh cả hai thực tế. Mặt khác, lưu ý rằng mặc dù rất khó để có được một cơ sở dữ liệu móng mắt đủ lớn, nhưng một khi có được nó có thể được sử dụng để tấn công các hệ thống khác nhau. Mức độ dễ dàng phản ánh thực tế đó. Đối với hai tròng mắt, vì một lý do tương tự, mức độ vừa phải được chọn;

- Trang thiết bị: Cần có thiết bị chuyên dụng (máy tính, kết nối với hệ thống, cơ sở dữ liệu). Với các giả định trên, bản tóm tắt tính toán tiềm năng tấn công tương ứng được cung cấp

Trong Bảng A.4 đối với trường hợp khuôn mặt, Bảng A.5 đối với trường hợp một móng mắt và Bảng A.6 đối với trường hợp hai móng mắt.

Bảng A.4 - Tính toán khả năng tấn công cho tình huống trong A.5 (mặt)

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					
Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp
2	4	2	0	2	-	0	0	-	0	2	4	8	8

Bảng A.5 - Tính toán khả năng tấn công cho kịch bản trong A.5 (móng mắt)

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					
Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp
2	4	2	0	2	-	0	0	-	2	2	4	8	10

Bảng A.6 - Tính toán khả năng tấn công cho tình huống trong A.5 (hai móng mắt)

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						
Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp
2	4	2	0	2	-	0	0	-	4	2	4
										8	12

Đánh giá cho cuộc tấn công là cơ bản nâng cao (cả khuôn mặt và mồng mắt) và trung bình (đối với trường hợp hai mồng mắt).

Nếu cuộc tấn công có thể được thực hiện thành công và không tìm thấy cuộc tấn công thành công nào khác với xếp hạng thấp hơn, khả năng chống chịu của TOE là cơ bản (cả khuôn mặt và mồng mắt) và cơ sở nâng cao (hai mồng mắt).

Hệ thống tương thích với thành phần AVA_VAN.2 (cả khuôn mặt và mồng mắt) và thành phần AVA_VAN.3 (hai mồng mắt).

CHÚ THÍCH Báo cáo tổng thể của cuộc tấn công về nguyên tắc sẽ phụ thuộc vào FAR của hệ thống, đặc biệt là cho thời gian cần sử dụng và cho các thiết bị cần thiết trong quá trình khai thác. Nếu mắt 1 giây cho mỗi lần thử và nếu một người cần 10 000 lần thử cho FAR 10-3, thì có thể mất ít hơn 2 tuần. Hơn nữa, người ta có thể cần một tập dữ liệu rất lớn cho giai đoạn khai thác. Ví dụ, đối với mồng mắt nếu điểm hoạt động là FAR 10-6, nhu cầu về bộ dữ liệu hơn 1 triệu mồng mắt có thể được coi là một thiết bị chuyên dụng. Ví dụ, đối với hai tròng mắt, với FAR dưới 10-8, kích thước của tập dữ liệu chứng minh việc tăng thiết bị để đặt riêng, do đó tăng tổng số tổng thể cho cuộc tấn công lên 26.

A.6 Tấn công Wolf

VÍ DỤ: Giả sử hệ thống là một hệ thống sinh trắc học theo một phương thức nhất định, hoạt động trong một môi trường không được kiểm soát (ví dụ, bảo vệ quyền truy cập vào một thiết bị hoặc một thiết bị). Giả sử rằng có thể dễ dàng kết nối một máy tính ngay trước trình trích xuất tính năng (ví dụ vì TOE hoàn toàn dựa trên phần mềm) để đưa hình ảnh vào làm đầu vào của giai đoạn trích xuất tính năng. Cũng giả định rằng có một lỗ hổng trong thuật toán so sánh để có một cách tạo ra một hình ảnh (không nhất thiết phải từ các đặc điểm sinh trắc học tự nhiên) mà tỷ lệ chấp nhận lỗi cao hơn đáng kể so với bất kỳ dữ liệu sinh trắc học được rút ra ngẫu nhiên nào. Điều này tương ứng với một hệ thống có tỷ lệ tấn công thành công cao. Cuộc tấn công sẽ bao gồm việc tìm ra (hoặc một trong số) hình ảnh cụ thể dẫn đến cơ hội được chấp nhận cao.

Nó được coi là:

- Giai đoạn định danh tương ứng để tìm ra điểm yếu trong thuật toán so khớp và sau đó tạo ra một hình ảnh khai thác lỗ hổng này. Giai đoạn khai thác chỉ là nhập hình ảnh để có quyền truy cập;
- Thời gian cần sử dụng: Có thể cần hơn một tháng để định danh trong khi việc khai thác là ngay lập tức;

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

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

- Cơ hội (truy cập vào TOE): TOE hoạt động trong môi trường không được kiểm soát (được đánh giá là dễ dàng cho giai đoạn khai thác) và nó được coi là hệ thống dễ mua (được đánh giá là dễ dàng cho giai đoạn xác định);

- Cơ hội (tiếp cận các đặc điểm sinh trắc học): Nó 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 bộ trích xuất tính năng.

Với các giả định trên, bao tóm tắt tính toán tiềm năng tấn công tương ứng được cung cấp trong Bảng A.7.

Bảng A.7 - Tính toán khả năng tấn công cho kịch bản trong A.6

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				
Id	Exp	Id	Exp	Id	Exp	Id	Exp	Id	Exp
8	0	4	0	4	-	0	0	-	0
								2	0
								18	0

Đánh giá cho cuộc tấn công là: 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 xếp hạng thấp hơn, khả năng chống chịu của TOE là cơ bản.

Hệ thống tương thích với thành phần AVA_VAN.2.

PHỤ LỤC B

(tham khảo)

Ví dụ cho các hoạt động ATE**B.1 Yêu cầu chung**

Phụ lục này bao gồm ví dụ về việc áp dụng các yêu cầu và điều khoản từ Điều 5 cho ATE.

B.2 Ví dụ về xác định các lỗi liên quan

Ví dụ: Giả định TOE là một hệ thống kiểm soát biên giới tự động, chỉ xem xét công nghệ xác minh khuôn mặt tức là kiosk xác minh khuôn mặt hoàn toàn tự động như đã thảo luận trong Tài liệu tham khảo số [8]. Do đó, đây là một kịch bản hoạt động đại diện cho một điểm kiểm soát biên giới tự động (BCP) trong sân bay.

Để phân tích lỗi nhận dạng sinh trắc học nào có liên quan đến an toàn đối với hệ thống kiểm soát biên giới tự động, danh sách đầy đủ các lỗi có thể xảy ra (các phép đo hiệu suất trong thuật ngữ tiêu chuẩn) được báo cáo trong ISO/IEC 19795-1. Trong Bảng B.1, tất cả các lỗi được báo cáo trong ISO/IEC 19795-1 được phân tích từng lỗi một.

Bảng B.1 - Ví dụ về xác định các lỗi liên quan đối với hệ thống kiểm soát biên giới tự động

Đo lường hiệu suất	Nhận xét	Liên quan đến an toàn/đánh giá
FTER	Hệ thống sử dụng đăng ký trước chủ thẻ dữ liệu được thực hiện ngoài phạm vi của TOE khi chủ thẻ dữ liệu nhận được ID quốc gia điện tử hoặc hộ chiếu điện tử (eMRTD)	Không tồn tại / Không tồn tại
FTAR	Ứng dụng này là kiểm soát biên giới tự động, trong đó kiến thức chi tiết về FTAR hoặc FMR là không cần thiết liên quan đến đánh giá an toàn. Hoạt động của hệ thống chỉ được đánh giá theo các điều khoản chung do FAR cung cấp và FRR tương ứng của nó (xem 3.2 để làm rõ giữa 4 tỷ lệ lỗi này). FTAR đóng một vai trò trong bối cảnh (FTAR càng cao thì FRR càng cao) nhưng nó không liên quan đến đánh giá	Không / Có

FNMR	Không nhận xét (trong trường hợp này FNMR càng cao thì FRR càng cao, do đó FNMR đóng một vai trò nhưng nó không liên quan đến việc đánh giá)	Không / Có
FMR	Không nhận xét (trong trường hợp này FMR càng cao thì FAR càng cao, do đó FMR đóng một vai trò quan trọng, nhưng việc đánh giá tập trung vào FAR, không phải trong FNMR)	Không / Có
FRR	Tỷ lệ lỗi này đóng một vai trò quan trọng, vì nó quyết định hoạt động của hệ thống. Từ chối lỗi sẽ làm chậm trễ đáng kể quy trình (do chủ thẻ dữ liệu thử lại hoặc do một ngoại lệ được đưa ra để kiểm tra thủ công). Dù sao, tỷ lệ lỗi liên quan ở đây chỉ là FAR, nhưng FRR cũng nên được báo cáo để chứng minh rằng hệ thống có thể sử dụng được	Không / Có
FAR	Đây là tỷ lệ lỗi liên quan đến an toàn duy nhất và do đó là tỷ lệ quan trọng nhất để đánh giá.	Có/Có
Tỷ lệ định danh	Không tồn tại (Hệ thống ở trong chế độ xác minh)	Không tồn tại / Không tồn tại
FNIR	Không nhận xét	Không tồn tại
FPIR	Không nhận xét	Không tồn tại
Thuật toán lựa chọn trước	Không nhận xét	Không tồn tại
Lỗi lựa chọn trước	Không nhận xét	Không tồn tại
Tỷ lệ thâm nhập	Không nhận xét	Không tồn tại
Cấp bậc định danh	Không nhận xét	Không tồn tại

Do đó, tỷ lệ lỗi được xác định duy nhất sẽ được tính đến trong đánh giá là FAR. Ngoài ra, FRR phải được báo cáo để chứng minh rằng hệ thống đang được đánh giá là có thể sử dụng được.

B.3 Ví dụ về xác định giá trị tối đa cho phép đối với tỷ lệ lỗi liên quan

VÍ DỤ Tương tự như B.2, hãy đặt TOE là một hệ thống kiểm soát biên giới tự động (ABC), chỉ xem xét công nghệ xác minh khuôn mặt sử dụng các khuôn mặt đã đăng ký trước được lưu trữ trong bộ chiêu điện tử (eMRTD). Do đó, đây là một kịch bản hoạt động đại diện cho một điểm kiểm soát biên giới trong sân bay.

Kiểm thử viên hiện có thể điều tra các báo cáo hiện đại và cụ thể là các báo cáo thí điểm do các tổ chức đánh giá hoặc nhóm nghiên cứu độc lập thực hiện, ngoài việc quan sát các yếu tố bối cảnh liên quan đến hoạt động của hệ thống được đánh giá. Như đã đề cập ở trên, không có công thức cố định để tính toán tỷ lệ lỗi tối đa mong muốn, nhưng kiến thức từ các công trình trước đây có thể là một trợ giúp quý giá.

Trong ví dụ này, dựa trên kiosk ABC, báo cáo [8] rất toàn diện về các yếu tố được xem xét (có thể tham khảo ở đó) và nghiên cứu sâu về cùng một hệ thống và môi trường hoạt động đang được đánh giá ở đây (trường hợp thử nghiệm số 9 trong Tài liệu tham khảo [số 8]). Từ kinh nghiệm được báo cáo dựa trên việc thí điểm hệ thống xuất nhập cảnh tại Sân bay Schipol và Sân bay Frankfurt (với hơn 6000 khách du lịch tham gia) và sửa kiosk ABC thành $FAR = 0,1\%$, thì FRR quan sát được là khoảng $25\%.$ Do đó, các giá trị tối đa cho tỷ lệ lỗi được xem xét trong ví dụ này có thể được cố định là lớn hơn một chút so với giá trị được quan sát trong báo cáo đó, chẳng hạn, $FAR = 0,2\%$ và đối với thông tin $FRR = 30\%.$ Kiểm thử viên cũng nên ước tính xem các giá trị này có được chấp nhận đối với sự an toàn của các ứng dụng sẽ dựa vào TOE hay không.

PHỤ LỤC C

(tham khảo)

Ví dụ về tài liệu thử nghiệm hiệu suất của nhà phát triển và chiến lược đánh giá của nó**C.1 Yêu cầu chung**

Phụ lục này được cung cấp như một ví dụ để nhà phát triển chuẩn bị tài liệu thử nghiệm hiệu suất của mình và để kiểm thử viên đánh giá nó. Nó được lấy cảm hứng từ Tài liệu tham khảo [10].

Nhà phát triển có thể tạo tài liệu thử nghiệm để báo cáo kết quả thử nghiệm hiệu suất (ví dụ: FRR / FAR hoặc FNMR / FMR).

Kiểm thử viên có thể thử nghiệm tài liệu thử nghiệm theo chiến lược đánh giá được mô tả trong phụ lục này để xác minh rằng thử nghiệm hiệu suất của nhà phát triển đã được thực hiện theo cách khách quan và có thể lặp lại để thử nghiệm độ tin cậy của tỷ lệ lỗi đo được.

Các hướng dẫn xác định trong phụ lục này được tạo ra dựa trên ISO/IEC 19795-1 và ISO/IEC 19795-2.

C.2 Cung cấp tài liệu thử nghiệm

Nhà phát triển có thể cung cấp tài liệu thử nghiệm cho các đánh giá sau tiêu chuẩn này. Mệnh đề C.4 xác định nội dung của tài liệu thử nghiệm.

C.3 Tóm tắt

Bảng C.1 trình diện các mục có thể được báo cáo trong tài liệu thử nghiệm. Tên hoặc cấu trúc của tài liệu thử nghiệm không cần tuân theo Bảng C.1. Tuy nhiên, tất cả các mục trong bảng đều được quan tâm đối với tài liệu thử nghiệm. Ngoài ra, nếu một số mục không được bao gồm trong tài liệu thử nghiệm, nhà phát triển có thể cung cấp lý do cho việc loại trừ đó cho kiểm thử viên.

Bảng C.1 - Các mục báo cáo

Mục phụ	Nội dung
C.4.2	Tổng quan về thử nghiệm hiệu suất (bao gồm cả kết quả thử nghiệm)
C.4.3	Đích ứng dụng và các yếu tố ảnh hưởng
C.4.4	Lựa chọn chủ đề thử nghiệm
C.4.5	Hướng dẫn thử nghiệm và đào tạo
C.4.6	Quản lý đổi tượng thử nghiệm
C.4.7	Quy trình thử nghiệm

C.4 Mô tả các mục báo cáo

C.4.1 Yêu cầu chung

Điều khoản này mô tả chi tiết từng mục trong Bảng C.1. Tất cả các mục được tạo dựa trên ISO/IEC 19795-1 và ISO/IEC 19795-2. Tuy nhiên, một số trong số chúng được sửa đổi để điều chỉnh cho phù hợp với các đánh giá theo TCVN 8709 (ISO/IEC 15408) (tất cả các phần).

C.4.2 Tổng quan về thử nghiệm hiệu suất

C.4.2.1 Nguyên tắc chung

Nhà phát triển có thể báo cáo thông tin chung sau đây về thử nghiệm hiệu suất.

C.4.2.2 Cấu hình thử nghiệm hiệu suất

Tài liệu thử nghiệm có thể báo cáo thông tin sau, phù hợp với thông tin trong ST, để xác định duy nhất cấu hình thử nghiệm của thử nghiệm hiệu suất.

- Tham chiếu TOE: Thông tin xác định duy nhất TOE. Sửa đổi TOE để thử nghiệm hiệu suất, nếu có (ví dụ: TOE được sửa đổi để xuất dữ liệu sinh trắc học cho thử nghiệm ngoại tuyến). Cơ sở lý luận rằng việc sửa đổi đó không ảnh hưởng đến việc thực hiện TOE. Ví dụ: nhà phát triển có thể tuyên bố rằng hiệu suất không bị ảnh hưởng vì mã sửa đổi không được thực thi trong quá trình xác minh sinh trắc học trên thiết bị di động hoặc nhà phát triển có thể chạy thử nghiệm hồi quy để xác minh rằng sửa đổi không thay đổi kết quả xác minh (ví dụ: điểm tương tự).

- Cấu hình TOE: Bất kỳ tham số hoặc thiết lập có thể cấu hình của TOE có thể ảnh hưởng đến việc thực hiện. Giá trị của mỗi tham số được đặt cho thử nghiệm. Ví dụ: nếu người dùng (ví dụ: người quyết định và người chất lượng hình ảnh) có thể được định cấu hình bởi người dùng, thì giá trị của người dùng được đặt cho thử nghiệm.

- Công cụ thử nghiệm hiệu suất: Thông tin xác định duy nhất tất cả các công cụ thử nghiệm (ví dụ: SDK) được sử dụng cho thử nghiệm hiệu suất.

C.4.2.3 Kết quả của thử nghiệm tính năng

Tài liệu thử nghiệm có thể báo cáo các mục sau đây để cung cấp kết quả thử nghiệm.

- Thời gian và địa điểm thử nghiệm: Tiến trình cho việc thử nghiệm hiệu suất (mẫu hoặc mẫu có thể được thu thập qua nhiều phiên) và vị trí thử nghiệm.

- Kết quả thử nghiệm cho từng phương thức được báo cáo riêng.

- Định nghĩa giao dịch chính hãng và giao dịch mạo danh: Nếu có liên quan đến FAR / FRR, hãy xác định rõ ràng những gì cấu thành giao dịch dựa trên tình huống xấu nhất để tuân theo cùng một quy tắc nhất quán trong suốt quá trình thử nghiệm hiệu suất.

- Số lượng đối tượng thử nghiệm, mẫu và mẫu: các số sau được sử dụng để tính FMR / FNMR hoặc FAR / FRR (phụ lục này giả định rằng ít nhất FMR hoặc FAR được đo thông qua thử nghiệm ngoại tuyến, tức là so sánh chéo, để đạt được con số tối đa các lần thử hoặc giao dịch. FNMR hoặc FRR có thể được đo lường thông qua thử nghiệm trực tuyến hoặc ngoại tuyến).

a) Đối tượng thử nghiệm: Số lượng đối tượng thử nghiệm đã tham gia thử nghiệm.

b) Mẫu đăng ký: Số lượng mẫu đăng ký dùng để thử nghiệm. Tất cả các đối tượng thử nghiệm có thể không tạo thành công các mẫu và tổng số mẫu có thể ít hơn phép nhân số đối tượng thử nghiệm với số bộ phận cơ thể của đối tượng thử nghiệm.

c) Mẫu: Số lượng mẫu lấy của từng bộ phận cơ thể và tổng số mẫu thu được của tất cả các đối tượng thử nghiệm. Tất cả các đối tượng thử nghiệm có thể không tạo ra các mẫu thành công và tổng số mẫu có thể ít hơn nhân của số đối tượng thử nghiệm, với số bộ phận cơ thể của đối tượng thử nghiệm và số lượng mẫu được thu thập cho từng bộ phận cơ thể.

- Kết quả của thử nghiệm: Tỷ lệ lỗi được đo lường bởi thử nghiệm hiệu suất. Nếu có liên quan đến FAR và FRR, số lượng giao dịch chính hãng và mạo danh. Nếu có liên quan đến FNMR, số lần thử chính hãng và mạo danh.

C.4.3 Ứng dụng mục tiêu và các yếu tố ảnh hưởng

Tài liệu thử nghiệm có thể chỉ định một ứng dụng mục tiêu được mô hình hóa trong thử nghiệm, chẳng hạn như xác minh sinh trắc học trên thiết bị di động trong môi trường văn phòng trong nhà với nhóm đối tượng thường xuyên.

Tài liệu thử nghiệm cũng có thể báo cáo các yếu tố ảnh hưởng có thể ảnh hưởng đến hoạt động, các biện pháp để kiểm soát các yếu tố đó và thử nghiệm hiệu suất được tiến hành dưới những yếu tố nào.

Các yếu tố ảnh hưởng, phù hợp với ứng dụng mục tiêu, có thể được xác định bằng cách giới thiệu phù hợp các tài liệu (ví dụ: ISO/IEC TR 19795-3) hoặc tham khảo biểu dữ liệu sản phẩm (ví dụ: nhiệt độ hoạt động).

Các yếu tố sau đây là ví dụ về các yếu tố kiểm soát để xác minh tĩnh mạch ngón tay / bàn tay. Nhà phát triển có thể xác định đúng các yếu tố này, ví dụ, dựa trên ISO/IEC TR 19795-3. Bất kỳ thông tin nào hữu ích trong bối cảnh của phương thức sinh trắc học đã sử dụng đều có thể được nhà phát triển xem xét để xác định các yếu tố.

Tất cả các yếu tố ảnh hưởng có thể được kiểm soát một cách thích hợp vì các tỷ lệ lỗi khác nhau có thể được đo lường dưới các yếu tố ảnh hưởng khác nhau.

- Nhân khẩu học của đối tượng thử nghiệm: tỷ lệ phân bố tuổi theo các nhóm tuổi tùy ý (ví dụ: 1 tuổi, 5 tuổi, 10 tuổi), phân bố theo giới tính, tỷ lệ phân bố theo nguồn gốc dân tộc. Danh mục nguồn gốc dân tộc có thể được xác định tùy ý bởi nhà phát triển.

- Tư thế và vị trí: tư thế của đối tượng thử nghiệm hoặc vị trí của bàn tay / ngón tay của họ (ví dụ: hướng của bàn tay / ngón tay liên quan đến cảm biến hoặc khoảng cách tới cảm biến), phù hợp với hướng dẫn vận hành TOE hoặc phản hồi tự động do TOE cung cấp.

- Môi trường trong nhà hoặc ngoài trời nơi thử nghiệm sẽ được tiến hành. Trong trường hợp môi trường ngoài trời, các yếu tố khác ảnh hưởng đến hiệu suất (ví dụ: ánh sáng môi trường).

- Nhiệt độ: phạm vi nhiệt độ mà thử nghiệm sẽ được tiến hành (ví dụ: "Thử nghiệm được tiến hành trong môi trường điều hòa nhiệt độ, nơi nhiệt độ được giữ giữa độ X và độ Y").

- Khoảng thời gian (ví dụ: thời gian tối thiểu, tối đa và trung bình) giữa đăng ký và xác minh.

- Thói quen: Mức độ mà đối tượng thử nghiệm đã quen thuộc với TOE (ví dụ: tần suất sử dụng của TOE).

- Điều chỉnh tiêu bản: mức độ thích ứng tiêu bản xảy ra trước khi đo FNMR hoặc FRR nếu TOE có thể điều chỉnh các mẫu theo thời gian với mục đích giảm tỷ lệ từ chối lỗi.

C.4.4 Lựa chọn đối tượng thử nghiệm

Phương pháp lựa chọn đối tượng thử nghiệm có thể được báo cáo (ví dụ: thu thập đối tượng thử nghiệm từ nhân viên của nhà phát triển hoặc tuyển dụng chúng từ công chúng). Nhân khẩu học của các đối tượng thử nghiệm có thể theo ứng dụng mục tiêu.

C.4.5 Hướng dẫn thử nghiệm và đào tạo

Các hướng dẫn và đào tạo cho các đối tượng thử nghiệm có thể được báo cáo. Tất cả các đối tượng thử nghiệm có thể được hướng dẫn và đào tạo giống nhau.

- Thông tin thử nghiệm và các hướng dẫn thử nghiệm chung được cung cấp cho đối tượng thử nghiệm trước hoặc sau khi thu thập dữ liệu sinh trắc học, phù hợp với hướng dẫn hoặc phản hồi tự động do TOE đưa ra hoặc các hướng dẫn được mô tả trong hướng dẫn vận hành TOE. Kiểm thử có thể không được điều chỉnh theo đặc tả TOE không được mô tả trong hướng dẫn vận hành TOE.

- Xác nhận nơi ở: phương pháp xác nhận mức độ thường trú của đối tượng trước khi thu thập dữ liệu sinh trắc học. Nếu thói quen đã được xác nhận thông qua đào tạo, phương pháp để đảm bảo tính nhất quán của đào tạo giữa các đối tượng thử nghiệm và các công cụ được sử dụng để đào tạo (ví dụ: nhà phát triển có thể chuẩn bị trước kịch bản cho đào tạo và áp dụng nó cho tất cả các đối tượng thử nghiệm để đảm bảo tính nhất quán).

C.4.6 Quản lý đối tượng thử nghiệm

Thông tin sau về quản lý đối tượng thử nghiệm có thể được báo cáo. Quản lý thích hợp là cần thiết để tránh các sai sót của con người có thể xảy ra trong quá trình thử nghiệm.

Quy trình quản lý: Dữ liệu sinh trắc học có thể bị hỏng do lỗi của con người trong quá trình thu thập (ví dụ: sử dụng ngón giữa khi ngón trỏ được yêu cầu). Báo cáo các quy trình quản lý đối tượng thử nghiệm để tránh các lỗi như vậy và quy trình quản lý để bao gồm các quy trình sau.

- a) Phương thức đăng ký đối tượng thử nghiệm ban đầu;
- b) Phương pháp đảm bảo tính duy nhất của đối tượng thử nghiệm;
- c) Số lượng và loại dữ liệu cá nhân được thu thập;
- d) Phương pháp tránh các lỗi thu thập dữ liệu (ví dụ: sử dụng phần mềm thu thập dữ liệu giảm thiểu lượng dữ liệu yêu cầu nhập bàn phím).

C.4.7 Quy trình thử nghiệm

Một giao thức thử nghiệm cho thử nghiệm có thể được báo cáo. Các mục sau đây có thể được bao gồm.

- Loại nỗ lực hoặc giao dịch: cho dù nỗ lực hoặc giao dịch được thực hiện trực tuyến hay ngoại tuyến. Trực tuyến có nghĩa là đăng ký và xác minh được thực hiện tại thời điểm gửi hình ảnh. Ngoại tuyến có nghĩa là đăng ký và xác minh được thực hiện riêng biệt với việc gửi hình ảnh.

- Luồng thử nghiệm: chi tiết về luồng thử nghiệm hoặc giao dịch giả mạo và chính hãng để đo tỷ lệ lỗi, với cùng một luồng áp dụng cho tất cả các đối tượng thử nghiệm. Nhà phát triển có thể duy trì một tệp nhật ký trong đó mỗi tương tác với TOE được ghi lại. Nhật ký có thể bao gồm tất cả các lần thử, các lần chuẩn bị hoặc thực hành, quy trình thiết lập (ví dụ: đặt ngưỡng) và các hoạt động bảo trì (ví dụ: làm sạch cảm biến). Một tệp nhật ký như vậy có thể rất hữu ích để đảm bảo quá trình thử nghiệm được tiến hành theo quy trình thử nghiệm.

- Tiêu chí loại trừ mẫu: tiêu chí loại trừ mẫu. Người vận hành thử nghiệm không được loại bỏ theo cách thủ công hoặc sử dụng cơ chế tự động để loại bỏ các mẫu đã thu thập trừ khi các mẫu phù hợp với các tiêu chí loại trừ đã được lập thành văn bản. Báo cáo số lượng mẫu bị loại trừ. Nếu các giao dịch không thành công do các mẫu bị loại trừ như vậy, hãy báo cáo số lượng các giao dịch không thành công đó. Các giao dịch không thành công này có thể được tính là giao dịch không thành công để tính tỷ lệ lỗi.

- Khuyến cáo hoặc hành động khắc phục: Các thiết bị hoặc hành động khắc phục để thử nghiệm đối tượng không hoàn thành giao dịch hoặc bộ sưu tập mẫu. Những khuyến cáo hoặc hành động khắc phục như vậy có thể được giới hạn ở mức tối thiểu cần thiết đối với ứng dụng đích. Những khuyến cáo hoặc hành động khắc phục tương tự có thể được đưa ra cho đối tượng thử nghiệm ở cùng điều kiện.

Thư mục tài liệu tham khảo

- [1] ISO/IEC 2382:2015, Information technology — Vocabulary
- [2] ISO/IEC 2382-37:2017, Information technology — Vocabulary — Part 37: Biometrics
- [3] ISO/IEC 15408-1:2009, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model
- [4] ISO/IEC 29115:2013, Information technology — Security techniques — Entity authentication assurance framework
- [5] ISO/IEC TR 29156:2015, Information technology — Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics
- [6] ISO/IEC 30107-1:2016, Information technology — Biometric presentation attack detection — Part 1: Framework
- [7] ISO/IEC 30107-3:2017, Information technology — Biometric presentation attack detection — Part 3: Testing and reporting
- [8] Smart borders pilot project: Report on the technical conclusions of the pilot. Technical report, eu-LISA, December 2015. doi: 10.2857/086263, <https://www.eulisa.europa.eu/Publications/Reports/Smart%20Borders%20-%20Technical%20Report.pdf>
- [9] Best Practice Operational Guidelines for Automated Border Control (ABC) Systems. FRONTEX, September 2015. doi: 10.2819/39041, https://frontex.europa.eu/assets/Publications/Research/Best_Practice_Operational_Guide_lines_ABC.pdf
- [10] Evaluation Activities for collaborative Protection Profile for Mobile biometric enrolment and verification – for unlocking the device – cPP, Supporting Document Mandatory Technical Document, Version 0.2 17-AUG-2018, <https://github.com/biometricITC/cPP-biometrics>