**TIÊU CHUẨN QUỐC GIA**

**TCVN 14190-2:2024  
ISO/IEC 19989-2:2020**

**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*

**Mục lục**

**Lời nói đầu**

**Giới thiệu**

**1 Phạm vi áp dụng**

**2 Tài liệu viện dẫn**

**3 Thuật ngữ và định nghĩa**

**4 Ký hiệu và thuật ngữ viết tắt**

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

5.1 Yêu cầu chung

5.2 Lập kế hoạch đánh giá

5.3 Thu thập dữ liệu

5.4 Phân tích

5.5 Xem xét các thử nghiệm của nhà phát triển

5.6 Yêu cầu cụ thể về các thành phần đảm bảo trên ATE\_IND

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

5.8 Tiến hành thử nghiệm độc lập

**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

6.2 TOE để thử nghiệm

6.3 Các lỗ hổng tiềm năng

6.4 Đánh giá khả năng tấn công

**PHỤ LỤC A (tham khảo) Ví dụ về tính toán tiềm năng tấn công cho các hoạt động AVA**

**PHỤ LỤC B (tham khảo) Ví dụ cho các hoạt động ATE**

**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**

**Thư mục tài liệu tham khảo**

**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 điện tử 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 thi 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

*…………………*

*Nội dung Tiêu chuẩn bằng File Word (đang tiếp tục cập nhật)*