BỘ THÔNG TIN VÀ TRUYỀN THÔNG

TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

BÁO CÁO THUYẾT MINH

NGHIÊN CỨU XÂY DỰNG TCVN VỀ YÊU CẦU KỸ THUẬT AN TOÀN CHO PHẦN MỀM ỨNG DỤNG (Mã số 13-07-NSCL)

Hà Nội - 2017

MỤC LỤC

1 Tên gọi và ký hiệu TCVN

Tên dự thảo tiêu chuẩn quốc gia:

"Công nghệ thông tin – Các kỹ thuật an toàn – Hồ sơ bảo vệ cho phần mềm ứng dụng".

Ký hiệu: TCVN XXXX:YYYY

Mục tiêu của việc xây dựng tiêu chuẩn:

Cung cấp quy định cho việc đảm bảo an toàn cho các phần mềm ứng dụng dựa trên các tiêu chí cụ thể. Tiêu chuẩn này quy định hồ sơ bảo vệ (protection profile) đối với các phần mềm ứng dụng, giúp các nhà phát triển áp dụng khi xây dựng và xây dựng hồ sơ cụ thể cho từng đối tượng/sản phẩm cần được đánh giá, giúp người dùng định hướng vào một nhóm các yêu cầu an toàn và giúp các nhà kiểm định dựa vào đó để đánh giá sản phẩm. Đồng thời, tiêu chuẩn cũng là một thành phần trong Bộ tiêu chuẩn quốc gia về an toàn thông tin.

2 Đặt vấn đề

2.1 Tình hình an toàn thông tin quốc tế và trong nước

An toàn thông tin đang trở thành mối lo và nguy cơ tiềm ẩn, các kẻ tấn công từ bất cứ mọi nơi với nhiều trình độ và kỹ năng chuyên môn từ cao cấp cho đến những người mới bắt đầu, sử dụng các công cụ hoặc các kịch bản có sẵn đều có thể truy cập vào các hệ thống thông tin của các cơ quan, tổ chức từ mọi nơi trên thế giới. Hiểm họa về mất an toàn thông tin cho các hệ thống thông tin ngày càng tăng cao, đa dạng về kiểu tấn công với xu hướng tấn công có mục tiêu, tấn công APT vào tổ chức, cơ quan trong các ngành trọng yếu như: tài chính, ngân hàng, hàng không, cơ quan chính phủ, … Đặc biệt, xu hướng các cuộc tấn công gần đây ngày càng tinh vi và kỹ năng chuyên sâu hơn, bên cạnh các cuộc tấn công vào môi trường mạng – Internet ồn ào trong thời gian qua, các cuộc tấn công lặng lẽ vào hệ thống phần mềm, chuyển hướng dần mục tiêu từ các hệ điều hành sang các phần mềm ứng dụng.

Chúng ta chứng kiến hàng ngày các sự cố liên quan đến mất an toàn, đánh cắp thông tin, thay đổi nội dung, tấn công kiểu từ chối dịch vụ gây đình trệ hoạt động, tấn công dùng mã độc cho các mục đích mã hoá dữ liệu đòi tiền chuộc, đưa các trojan, backdoor vào máy để kiểm soát, phát tán các mã độc bot để các máy chủ điều khiển (c&c server) có thể kiểm soát và ra lệnh thực thi các hành động tấn

công mạng hoặc hành vi độc hại khác, tấn công vào hệ thống email, web để đánh cắp thông tin của tổ chức và của người dùng cá nhân, sử dụng tấn công mạng và các hình thức phishing cho các mục đích chính trị như làm ảnh hưởng đến kết quả … Rất nhiều những tấn công như vậy và sau đây là một số sự cố điển hình trong thời gian qua:

- Tin tặc Nga tấn công bầu cử tổng thống Mỹ

- Các cuộc tấn công DDoS tiếp tục làm tê liệt mạng Internet nhiều lần

- Mã độc mã hoá dữ liệu tống tiền ransomware tiếp tục mở rộng các mục tiêu tấn công

- Công bố các lỗ hổng liên quan đến nhóm ShadowBrokers

- Vault 7 của WikiLeaks công bố 8.761 tài liệu liên quan đến CIA

- CloudBleed (đám mây rỉ máu) vào công ty cung cấp hạ tầng Internet Cloudflare

- 198 triệu hồ sơ bỏ phiếu tại Hoa Kỳ bị lộ

- Chiến dịch Macron Hack nhằm vào cuộc bầu cử của Tổng thống Pháp Emmanuel Macron

Bên cạnh đó, các lỗ hổng của các phần mềm, của hệ điều hành liên tục được công bố với số lượng ngày càng nhiều. Các lỗ hổng công bố chủ yếu chỉ mới các lỗ hổng của các hệ điều hành hoặc các phần mềm ứng dụng phổ biến trong khi các phần mềm dùng riêng chiếu tỷ trọng khá lớn hầu như chưa được công bố khi phát hiện lỗi hoặc chỉ tự cập nhật các bản vá lỗi. Tất cả cho thấy nguy cơ tiềm ẩn đối với các phần mềm, các hệ điều hành là rất cao nếu không có biện pháp đảm bảo an toàn hữu hiệu hoặc giảm thiểu các nguy cơ.

2.2 Tình hình tiêu chuẩn hoá trong nước và quốc tế về tiêu chí, phương pháp đánh giá an toàn công nghệ thông tin

Trên thế giới, đã ban hành nhiều tiêu chuẩn và tài liệu hướng dẫn kỹ thuật liên quan đến các tiêu chí đánh giá và phương pháp đánh giá an toàn công nghệ thông tin gồm các bộ ISO/IEC 15408 (ba phần) về các tiêu chí đánh giá an toàn công nghệ thông tin, ISO/IEC18045 về các phương pháp đánh giá an toàn công nghệ thông tin, và các bộ tài liệu kỹ thuật liên quan đến hồ sơ bảo vệ cho các sản

phẩm công nghệ thông tin gồm các nhóm: bảo vệ dữ liệu, các hệ thống và thiết bị điều khiển truy nhập, các hệ thống và thiết bị liên quan tới mạng, hệ điều hành ..., đặc biệt là tài liệu kỹ thuật về Hồ sơ Bảo vệ cho Phần mềm Ứng dụng của NIAP – Hoa Kỳ, được 17 quốc gia thành viên chính của CCRA gồm Úc, Canada, Pháp, Đức, Ấn Độ, Ý, Nhật, Malaysia, Hà Lan, New Zealand, Na Uy, Hàn Quốc, Tây Ban Nha, Thụy Điển, Thổ Nhĩ Kỳ, Anh, Hoa Kỳ chấp nhận và 11 quốc gia thừa nhận CCRA gồm Áo, Cộng hoà Séc, Đan Mạch, Ethiopia, Phần Lan, Hy Lạp, Hungary, Israel, Pakistan, Quatar, Singapore áp dụng và một số quốc gia khác quan tâm, áp dụng.

Tại Việt Nam đã ban hành một số tiêu chuẩn về các tiêu chí và phương pháp đánh giá an toàn cho các sản phẩm công nghệ thông tin như bộ tiêu chuẩn TCVN 8709:2011 (ISO/IEC 15408) (03 phần) về các tiêu chí đánh giá an toàn công nghệ thông tin và TCVN 11386:2016 về phương pháp đánh giá an toàn công nghệ thông tin, tuy nhiên các tiêu chuẩn này vẫn là tiêu chuẩn chung chưa có tiêu chuẩn đánh giá an toàn cho các phần mềm ứng dụng. Do đó việc xây dựng tiêu chuẩn về các yêu cầu kỹ thuật an toàn cho phần mềm ứng dụng là hết sức cần thiết.

2.3 Các tiêu chuẩn quốc tế về đánh giá an toàn công nghệ thông tin

Các tổ chức quốc tế đã nghiên cứu và đưa ra nhiều tài liệu, tiêu chuẩn về an toàn công nghệ thông tin như:

1. Bộ tiêu chuẩn về quản lý an toàn thông tin thuộc họ ISO/IEC 27xxx, cung cấp các hướng dẫn và các vấn đề liên quan trong hệ thống quản lý an toàn thông tin. Trong đó, có nhiều tiêu chuẩn được ban hành mới gần đây như ISO/IEC 27033-4:2014, ISO/IEC 27033-5:2014, ISO/IEC 27037:2014 và một số tiêu chuẩn được cập nhật phiên bản mới như ISO/IEC 27001:2013, ISO/IEC 27002:2013, …

- ✓ ISO/IEC 27000:2009 - Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng.
- ✓ ISO/IEC 27001:2005 - Hệ thống quản lý an toàn thông tin - Các yêu cầu.
- ✓ ISO/IEC 27002:2005 - Quy tắc thực hành quản lý an toàn thông tin.
- ✓ ISO/IEC 27003:2010 - Hướng dẫn thực thi hệ thống quản lý an toàn thông tin.
- ✓ ISO/IEC 27004:2009 - Quản lý an toàn thông tin - Đo lường.
- ✓ ISO/IEC 27005:2011 - Quản lý rủi ro an toàn thông tin.

- ✓ ….
- ✓ ISO/IEC 27033:2009 - Tổng quan và các khái niệm về an toàn mạng.
- ✓ ISO/IEC 27034-1:2011 - CNTT - Các kỹ thuật an toàn - An toàn ứng dụng - Tổng quan và các khái niệm.
- ✓ ISO/IEC 27035:2011 - Quản lý sự cố ATTT.
- ✓ ....

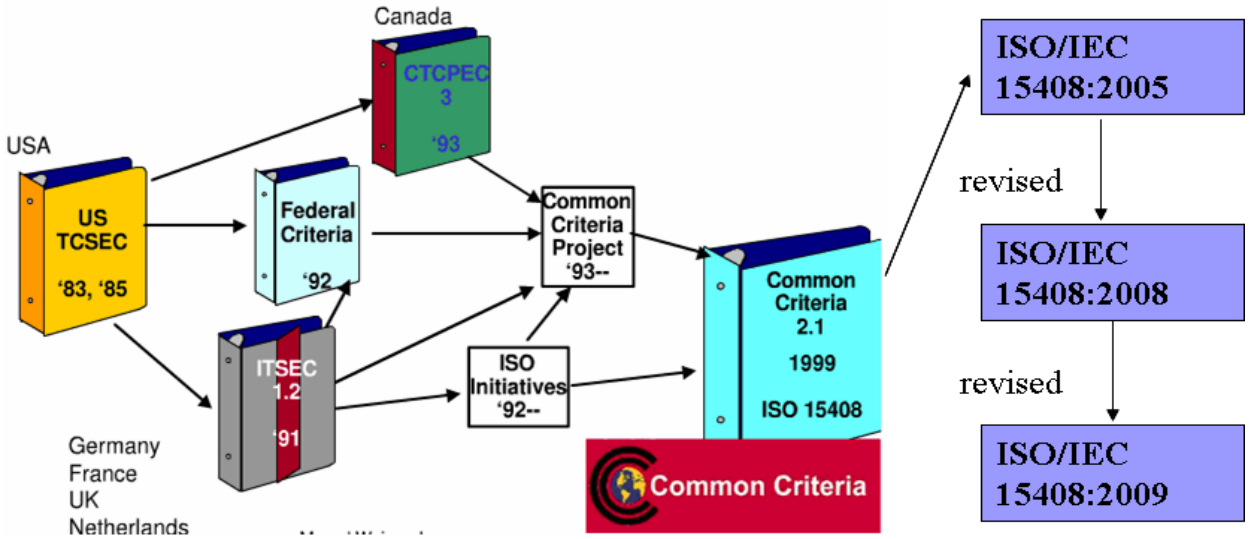
2. Tiêu chuẩn về đánh giá an toàn thông tin

- Bộ tiêu chuẩn ISO/IEC 15408:2009 cung cấp một tập các yêu cầu đảm bảo an toàn của các sản phẩm, hệ thống công nghệ thông tin và các biện pháp đảm bảo áp dụng các yêu cầu trong quá trình đánh giá an toàn. Bộ tiêu chuẩn này gồm có 3 phần:

✓ ISO/IEC 15408-1:2009 - Công nghệ thông tin - Các kỹ thuật an toàn - Tiêu chí đánh giá cho an toàn công nghệ thông tin - Phần 1: Giới thiệu và mô hình chung.

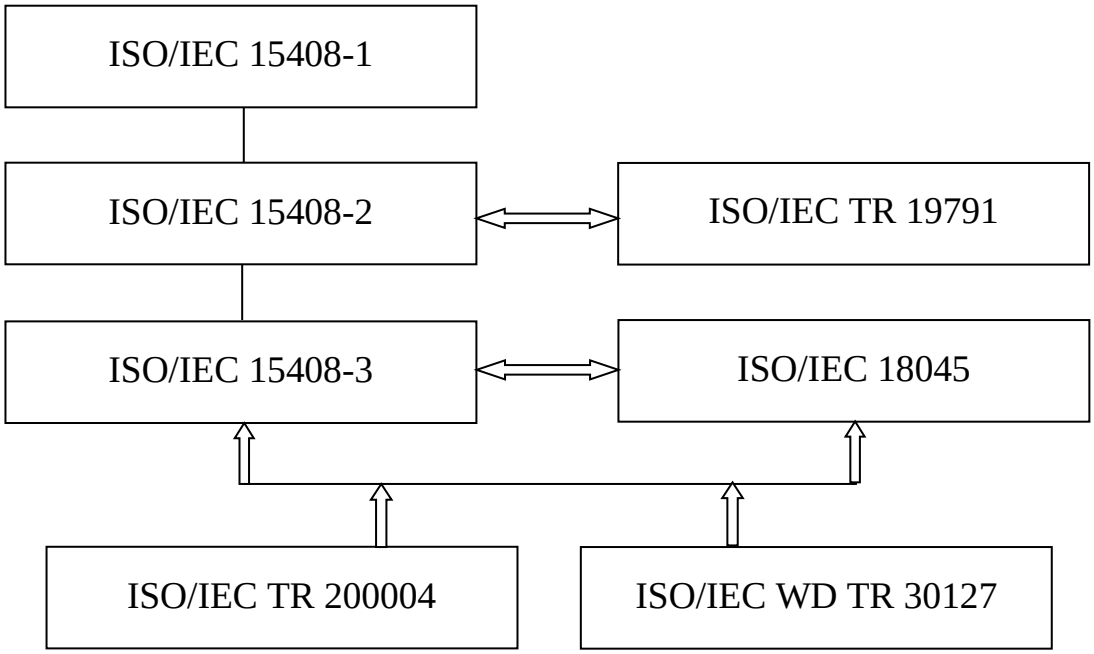
✓ ISO/IEC 15408-2:2009 - Công nghệ thông tin - Các kỹ thuật an toàn - Tiêu chí đánh giá cho an toàn công nghệ thông tin - Phần 2: Các thành phần chức năng an toàn.

✓ ISO/IEC 15408-3:2008 - Công nghệ thông tin - Các kỹ thuật an toàn - Tiêu chí đánh giá cho an toàn công nghệ thông tin - Phần 3: Các thành phần đảm bảo an toàn.



Hình 1 - *Hình thành và tương quan giữa các tiêu chuẩn quốc gia, Tiêu chí Chung (CC) và Bộ tiêu chuẩn ISO/IEC 15408*

Mối quan hệ giữa ISO/IEC 15408 và các tiêu chuẩn khác về đánh giá ATTT:



Hình 2 – *Mối quan hệ giữa ISO/IEC 15408 và các tiêu chuẩn*

- Bộ tiêu chuẩn ISO/IEC 18045:2008 - Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp đánh giá an toàn công nghệ thông tin. Tiêu chuẩn này quy định những hành động mà một người đánh giá cần thực hiện theo một trình tự nhất định để kiểm soát việc đánh giá trong ISO/IEC 15408, sử dụng các tiêu chí đánh giá trong bộ ISO/IEC 15408.
- Bộ tiêu chuẩn ISO/IEC TR 19791:2010 - Công nghệ thông tin - Các kỹ thuật an toàn - Đánh giá an toàn các hệ thống vận hành. Tiêu chuẩn này cung cấp các hướng dẫn và tiêu chí đánh giá an toàn các hệ thống vận hành. Tiêu chuẩn này mở rộng hơn ISO/IEC 15408, nó đề cập các khía cạnh quan trọng trong các hệ thống vận hành mà trong tiêu chuẩn ISO/IEC 15408 không được đề cập.
- Bộ tiêu chuẩn ISO/IEC TR 15443:2012 đề cập đến các khái niệm và tiêu chí cho việc so sánh và phân tích các phương pháp đánh giá sự phù hợp bảo đảm an toàn. Bộ tiêu chuẩn này gồm 2 phần:

✓ ISO/IEC 15443-1:2012 - Công nghệ thông tin - Kỹ thuật an toàn - Khung bảo đảm an toàn công nghệ thông tin - Phần 1: Giới thiệu và khái niệm.

✓ ISO/IEC 15443-2:2012 - Công nghệ thông tin - Kỹ thuật an toàn - Khung bảo đảm an toàn công nghệ thông tin - Phần 2: Các phân tích.

3. Các tiêu chuẩn liên quan đến sản phẩm phần mềm

✓ ISO/IEC 25000:2014 - Kỹ thuật phần mềm và hệ thống - Các yêu cầu và đánh giá chất lượng phần mềm và hệ thống (SQuaRE) - Giới thiệu SQuaRE.

Mục đích của tiêu chuẩn là cung cấp tổng quan về các nội dung của SQuaRE, các mô hình tham khảo chung và các định nghĩa, cũng như mối quan hệ giữa các tài liệu, cho phép người sử dụng hiểu rõ các bộ tiêu chuẩn tùy theo mục đích sử dụng của họ. Nó cũng bao gồm sự lý giải về quá trình chuyển tiếp giữa ISO/IEC 9126, ISO/IEC 14598 và SQuaRE.

✓ ISO/IEC 25010:2011 - Kỹ thuật phần mềm và hệ thống - Các yêu cầu và đánh giá chất lượng phần mềm và hệ thống (SQuaRE) - Các mô hình chất lượng phần mềm và hệ thống.

Phạm vi áp dụng của mô hình bao gồm hỗ trợ xác định, đánh giá phần mềm và các hệ thống máy tính sử dụng phần mềm dựa trên các quan điểm khác nhau của những người có liên quan đến việc mua lại, yêu cầu, phát triển, sử dụng, đánh giá, hỗ trợ, bảo trì, đảm bảo và kiểm soát chất lượng. Việc sử dụng mô hình giúp cho các hoạt động trong quá trình phát triển sản phẩm như: xác định các yêu cầu phần mềm và hệ thống; các mục tiêu thiết kế phần mềm và hệ thống; các mục tiêu kiểm thử phần mềm và hệ thống; tiêu chuẩn kiểm soát chất lượng như một phần của đảm bảo chất lượng; các tiêu chí chấp nhận cho một sản phẩm phần mềm và / hoặc hệ thống máy tính sử dụng phần mềm.

✓ ISO/IEC 25040:2011 - Kỹ thuật phần mềm và hệ thống - Các yêu cầu và đánh giá chất lượng phần mềm và hệ thống (SQuaRE) - Quy trình đánh giá.

Tiêu chuẩn này bao gồm các yêu cầu và khuyến nghị để đánh giá chất lượng sản phẩm phần mềm và làm rõ các khái niệm chung. Nó cung cấp mô tả quá trình đánh giá chất lượng sản phẩm phần mềm và các yêu cầu cho việc áp dụng quy trình này. Quá trình đánh giá có thể được sử dụng cho các mục đích và cách tiếp cận khác nhau, để đánh giá chất lượng phần mềm trước khi phát triển, phần mềm thương mại hoặc phần mềm tùy chỉnh và có thể được sử dụng trong suốt hoặc sau quá trình phát triển.

Tiêu chuẩn này dành cho những người có trách nhiệm đánh giá sản phẩm phần mềm và phù hợp với các nhà phát triển, người sở hữu và người đánh giá độc lập các sản phẩm phần mềm. Nó không dành cho đánh giá các khía cạnh khác của

sản phẩm phần mềm (chẳng hạn như yêu cầu chức năng, yêu cầu quy trình, yêu cầu kinh doanh, v.v ...).

Ngoài ra, bộ tiêu chuẩn quốc tế ISO/IEC còn rất nhiều các tiêu chuẩn liên quan khác, tham khảo tại website: http://www.iso.org/.

2.4 Các tiêu chuẩn trong nước về đánh giá an toàn công nghệ thông tin

1. Bộ TCVN về Hệ thống quản lý an toàn thông tin

✓ TCVN ISO 27001:2009 (ISO/IEC 27001:2005): Công nghệ thông tin - Hệ thống quản lý an toàn thông tin - Các yêu cầu.

✓ TCVN ISO 27002:2011 (ISO/IEC 27002:2005): Công nghệ thông tin - Các kỹ thuật an toàn - Quy tắc thực hành Quản lý an toàn thông tin.

✓ TCVN 10541:2014 (ISO/IEC 27003:2010): Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn triển khai hệ thống quản lý an toàn thông tin.

✓ TCVN 10542:2014 (ISO/IEC 27004:2010): Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý an toàn thông tin - Đo lường.

✓ TCVN 10295:2014 (ISO/IEC 27005:2011): Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý rủi ro an toàn thông tin.

✓ TCVN 10543:2014 (ISO/IEC 27010:2012): Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý an toàn trao đổi thông tin liên tổ chức, liên ngành.

✓ TCVN 11239:2015 (ISO/IEC 27035:2011): Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý sự cố an toàn thông tin.

2. Bộ TCVN về đánh giá an toàn công nghệ thông tin

✓ TCVN 8709-1:2011 (ISO/IEC 15408-1:2009): Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 1: Giới thiệu và mô hình tổng quát.

✓ TCVN 8709-2:2011 (ISO/IEC 15408-2:2008): Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 2: Các thành phần chức năng an toàn.

✓ TCVN 8709-3:2011 (ISO/IEC 15408-3:2008): Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 3: Các thành phần đảm bảo an toàn.

3. Bộ TCVN về phương pháp đánh giá an toàn công nghệ thông tin

✓ TCVN 11386:2016 (ISO/IEC 18045:2008): Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp đánh giá an toàn thông tin. Đây là bộ tiêu chuẩn quốc

gia về hệ thống phương pháp đánh giá an toàn công nghệ thông tin theo các tiêu chí chung về an toàn công nghệ thông tin quy định trong ISO/IEC 15408, phục vụ việc đánh giá an toàn thông tin cho các sản phẩm, hệ thống CNTT.

4. Một số bộ TCVN liên quan đến sản phẩm phần mềm

✓ TCVN 8702:2011 (ISO/IEC 9126): Công nghệ thông tin - Chất lượng sản phẩm phần mềm - Phần 1: Các phép đánh giá ngoài.

✓ TCVN 8703:2011: Công nghệ thông tin - Chất lượng sản phẩm phần mềm - Phần 2: Các phép đánh giá trong.

✓ TCVN 8704:2011: Công nghệ thông tin - Chất lượng sản phẩm phần mềm - Phần 3: Các phép đánh giá chất lượng người sử dụng.

✓ TCVN 8705:2011 (ISO/IEC 14598): Công nghệ thông tin - Đánh giá sản phẩm phần mềm - Phần 1: Tổng quát.

✓ TCVN 8706:2011: Công nghệ thông tin - Đánh giá sản phẩm phần mềm - Phần 2: Quy trình dành cho bên đánh giá.

✓ TCVN 8707:2011: Công nghệ thông tin - Đánh giá sản phẩm phần mềm - Phần 3: Quy trình dành cho người phát triển.

✓ TCVN 8708:2011: Công nghệ thông tin - Đánh giá sản phẩm phần mềm - Phần 4: Quy trình dành cho người mua sản phẩm.

✓ TCVN 10540:2014 (ISO/IEC 25051:2006): Kỹ thuật phần mềm - Yêu cầu và đánh giá chất lượng sản phẩm phần mềm - Yêu cầu chất lượng và hướng dẫn kiểm tra sản phẩm phần mềm sẵn sàng phổ biến và thương mại hóa (COTS).

✓ TCVN 10607-1:2014 (ISO/IEC 15026-1:2013): Kỹ thuật phần mềm và hệ thống - Đảm bảo phần mềm và hệ thống - Phần 1: Khái niệm và từ vựng.

✓ TCVN 10607-2:2014 (ISO/IEC 15026-2:2011): Kỹ thuật phần mềm và hệ thống - Đảm bảo phần mềm và hệ thống - Phần 2: Trường hợp đảm bảo.

✓ TCVN 10607-3:2014 (ISO/IEC 15026-3:2011): Kỹ thuật phần mềm và hệ thống - Đảm bảo phần mềm và hệ thống - Phần 3: Mức vẹn toàn hệ thống.

✓ TCVN 10607-4:2014 (ISO/IEC 15026-4:2012): Kỹ thuật phần mềm và hệ thống - Đảm bảo phần mềm và hệ thống - Phần 3: Đảm bảo trong vòng đời.

Ngoài các tiêu chuẩn trên còn có các các tiêu chuẩn khác, tham khảo tại website: http://www.tcvn.gov.vn/, http://www.ismq.org.vn/.

2.5 Giới thiệu tài liệu kỹ thuật "Hồ sơ bảo vệ cho phần mềm ứng dụng"

Tài liệu kỹ thuật "Hồ sơ bảo vệ cho phần mềm ứng dụng – Protection Profile for Application Software" là tài liệu của Hiệp hội Đảm bảo Thông tin Quốc gia - NIAP (National Information Assurance Partnership) của Hoa Kỳ, tổ chức giám sát chương trình quốc gia về đánh giá các sản phẩm thương mại về công nghệ thông tin (COTS), dựa trên Tiêu chí Chung về Đánh giá An toàn Công nghệ Thông tin (Common Criteria for Information Technology Security Evaluation) của quốc tế.

Chương trình quốc gia này bao gồm việc Xác nhận và Đánh giá tiêu chí chung (CCEVS) do NIAP quản lý, là một chương trình quốc gia để xây dựng hồ sơ bảo vệ (PP), các phương pháp đánh giá và các chính sách nhằm đảm bảo các yêu cầu bảo mật có thể đạt được, có thể lặp lại và có thể kiểm tra được. CCEVS là sự hợp tác giữa Cơ quan an ninh quốc gia Hoa Kỳ (NSA) và Viện tiêu chuẩn và công nghệ quốc gia Hoa Kỳ (NIST) nhằm thiết lập cơ sở cho việc thực hiện đánh giá và cung cấp các sản phẩm CNTT thương mại (COTS) đáp ứng được các yêu cầu của người dùng và giúp cho các nhà sản xuất các sản phẩm này được chấp nhận trên thị trường toàn cầu. Đánh giá thành công mang lại lợi ích cho các nhà phát triển, nhà cung cấp sản phẩm và các nhà thầu của chính phủ bằng cách xác nhận rằng sản phẩm đáp ứng các yêu cầu bảo mật đối với việc mua sắm, trang bị hệ thống an ninh quốc gia của Mỹ.

Cộng đồng quốc tế thực thi các tiêu chuẩn của CC thông qua Thoả thuận Công nhận Tiêu chí chung (CCRA), trong đó nêu rõ rằng các thành viên tham gia đồng ý chấp nhận kết quả đánh giá Tiêu chí chung CC do các thành viên CCRA khác thực hiện. Do NIAP là thành viên của Thỏa thuận công nhận tiêu chí chung (CCRA) gồm 17 quốc gia chính và 11 quốc gia thừa nhận, nên các sản phẩm của NIAP đã được chứng thực cũng đáp ứng cho các nhà thầu trong các quốc gia thành viên của CCRA.

Việc kiểm tra an toàn CNTT được thực hiện bởi các phòng kiểm nghiệm thương mại đã được NIAP phê chuẩn và được NIST công nhận. Nhà cung cấp sản phẩm chọn một phòng kiểm nghiệm được phê duyệt để hoàn thành việc đánh giá sản phẩm dựa trên một hồ sơ bảo vệ (PP) được lựa chọn. Một hồ sơ bảo vệ là một bộ các yêu cầu an toàn độc lập đối với một công nghệ cụ thể, cho phép thực hiện các hoạt động đánh giá khả thi, có thể lặp lại và có thể kiểm tra được cho mỗi đánh

giá. Tất cả các sản phẩm được đánh giá trong chương trình phải thể hiện sự tuân thủ chính xác theo hồ sơ bảo vệ công nghệ hiện hành.

Tiêu chí Chung (CC) là tiêu chuẩn quốc tế để đánh giá các chức năng bảo mật của các sản phẩm công nghệ thông tin, bao gồm cả phần cứng (hardware) và phần mềm (firmware, software). Tiêu chí chung định nghĩa một bộ khung để giám sát các đánh giá, một cú pháp để xác định các yêu cầu bảo mật cần phải đáp ứng và một phương pháp để đánh giá các yêu cầu đó. Quá trình đánh giá tạo ra mức độ tin tưởng rằng chức năng bảo mật của các sản phẩm CNTT và các biện pháp đảm bảo áp dụng cho các sản phẩm CNTT này đáp ứng được các yêu cầu. Kết quả đánh giá có thể giúp người tiêu dùng xác định liệu những sản phẩm CNTT này có đáp ứng được nhu cầu bảo mật của họ hay không. CC rất hữu ích để hướng dẫn cho việc phát triển, đánh giá hoặc mua sắm các sản phẩm công nghệ thông tin có chức năng bảo mật.

Quan điểm và các nguyên tắc đánh giá tính an toàn của sản phẩm CNTT trong tiêu chí chung (CC) về đánh giá an toàn công nghệ thông tin được thông qua một loạt các khái niệm gồm: đích đánh giá (TOE), đích an toàn (ST), hồ sơ bảo vệ (PP), ...

- Đích đánh giá (TOE): là một hệ thống, ứng dụng hoặc sản phẩm CNTT được chọn để đánh giá. CC đòi hỏi đích đánh giá phải được xem xét trong môi trường bảo mật cụ thể bao gồm môi trường pháp lý (các qui định, các văn bản hướng dẫn liên quan tới TOE); môi trường hành chính, quản trị (các điều khoản của chính sách bảo mật, các chương trình bảo mật có liên quan đến đối tượng); môi trường vật lý và các biện pháp bảo vệ vật lý; môi trường kỹ thuật (mục đích sử dụng của TOE và các lĩnh vực sử dụng, các tài nguyên cần bảo vệ bằng các phương tiện của TOE).

- Đích an toàn (ST): là tập hợp các yêu cầu bảo mật và những đặc tả dùng làm cơ sở để đánh giá tính bảo mật của sản phẩm. Đích an toàn được xây dựng sau khi phân tích môi trường bảo mật, tức là phân tích các yếu tố đảm bảo bảo mật như các mối nguy cơ đe dọa bảo mật, các quy định và chính sách bảo mật của tổ chức, kinh nghiệm, kỹ năng và kiến thức. Mục tiêu an toàn bao gồm mục tiêu an toàn cho đối tượng và mục tiêu an toàn cho môi trường. Mục tiêu an toàn cho đối tượng phải có khả năng đối chiếu được với các mối đe dọa bảo mật mà có thể đối

phó bằng các phương tiện kỹ thuật của đích đánh giá hoặc bằng chính sách bảo mật của tổ chức. Mục tiêu an toàn cho môi trường cần đối chiếu được với các mối đe dọa mà các phương tiện kỹ thuật của đối tượng và chính sách bảo mật không hoàn toàn có khả năng chống đỡ.

- Yêu cầu an toàn: là kết quả biến đổi mục tiêu an toàn thành các yêu cầu cụ thể. Các yêu cầu an toàn cũng được xác định riêng cho đối tượng và cho môi trường. CC phân biệt hai loại yêu cầu an toàn gồm các yêu cầu chức năng an toàn và yêu cầu đảm bảo an toàn. Yêu cầu chức năng an toàn được đặt ra cho những chức năng của sản phẩm, có nhiệm vụ duy trì bảo mật CNTT và quyết định sự vận hành an toàn mong muốn của các đối tượng. Ví dụ về yêu cầu chức năng an toàn như các yêu cầu đối với định danh, xác thực, kiểm toán an toàn và không chối bỏ nguồn gốc. Các yêu cầu đảm bảo an toàn lại quy định đối với công nghệ và quá trình thiết kế, chế tạo, khai thác sản phẩm, xác định mức an toàn tối thiểu phù hợp với mục tiêu an toàn đã công bố. Ví dụ về yêu cầu đảm bảo an toàn như các đòi hỏi về tính chặt chẽ của quá trình thiết kế hay xác định những điểm yếu tiềm tàng trong sản phẩm và phân tích ảnh hưởng của nó đến độ an toàn của sản phẩm. Nếu các yêu cầu chức năng an toàn được đặt ra cho các chức năng của sản phẩm thì yêu cầu đảm bảo an toàn lại đặt ra cho hoạt động của nhà thiết kế.

+ Yêu cầu chức năng an toàn (SFR): xác định các chức năng an toàn riêng mà một sản phẩm có thể cung cấp.

+ Yêu cầu đảm bảo an toàn (SAR): mô tả các biện pháp được thực hiện trong quá trình phát triển và đánh giá sản phẩm để đảm bảo tuân thủ chức năng an toàn được yêu cầu. Yêu cầu đối với các mục tiêu cụ thể hoặc các loại sản phẩm được ghi lại trong Đích an toàn (ST) và Hồ sơ bảo vệ (PP) tương ứng.

- Hồ sơ bảo vệ (PP): là tài liệu mẫu để xây dựng mục tiêu an toàn, bao gồm một loạt các yêu cầu chức năng và yêu cầu đảm bảo về an toàn cho một sản phẩm nào đó. Nó giúp nhà phát triển xây dựng hồ sơ cụ thể cho đối tượng cần được đánh giá, giúp người tiêu dùng định hướng vào một nhóm các yêu cầu an toàn và giúp nhà kiểm định dựa vào đó để đánh giá sản phẩm. Nếu mục tiêu an toàn được xây dựng cho một đối tượng cụ thể thì PP lại được xây dựng chung cho một loại đối tượng nào đó. PP mô tả các yêu cầu chung cho các TOE, bởi vậy nó thường do một nhóm người tiêu dùng hoặc một nhóm nhà phát triển sản phẩm viết. Các hồ sơ bảo vệ được sử dụng phổ biến nhất hiện nay được công bố bởi Hiệp hội đảm bảo

thông tin quốc gia Mỹ (NIAP). Ngoài ra, có thể nghiên cứu thêm về các Hồ sơ bảo vệ đã được quốc tế công nhận được công bố trên Cổng thông tin của Tiêu chí Chung.

Nội dung của Hồ sơ bảo vệ cho Phần mềm ứng dụng (phiên bản 1.2) gồm các mục sau:

1. Giới thiệu
    1.1. Tổng quan
    1.2. Thuật ngữ và định nghĩa
    1.3. Ranh giới của mục tiêu đánh giá TOE
    1.4. Các trường hợp áp dụng
2. Các tuyên bố tuân thủ
3. Định nghĩa các vấn đề bảo mật
    3.1. Các mối đe dọa
    3.2. Các giả định
    3.3. Chính sách bảo mật tổ chức
4. Các mục tiêu an toàn
    4.1. Các mục tiêu an toàn cho TOE
    4.2. Các mục tiêu an toàn cho môi trường hoạt động
    4.3. Lý do mục tiêu an toàn
5. Các yêu cầu bảo mật
    5.1. Yêu cầu chức năng bảo mật
    5.2. Yêu cầu đảm bảo bảo mật

Các Phụ lục

2.6 Nhận xét

Hiện nay trên thế giới và trong nước đã có nhiều tiêu chuẩn liên quan đến đảm bảo an toàn thông tin, phổ biến là họ các tiêu chuẩn ISO/ 27xxx về hệ thống quản lý đảm bảo đảm bảo an toàn thông tin, ISO/IEC 15408 (3 phần) – TCVN 8709 về tiêu chí đánh giá an toàn công nghệ thông tin, ISO/IEC 18045 - TCVN 11386 về phương pháp đánh giá an toàn công nghệ thông tin. Tuy nhiên, nhu cầu đánh giá đảm bảo an toàn cho các phần mềm ứng dụng, vấn đề được nêu ra trong mục 2.1 ở trên lại đang còn thiếu và các tiêu chuẩn trong bộ tiêu chuẩn quốc tế ISO/IEC chưa đáp ứng, đòi hỏi phải tìm kiếm các tiêu chí cụ thể đảm bảo an toàn

cho phần mềm ứng dụng trong quá trình thiết kế, xây dựng, đánh giá và kiểm định tính an toàn trước và trong khi sử dụng.

Hồ sơ bảo vệ cho phần mềm ứng dụng của NIAP – Hoa Kỳ thuộc họ các Tiêu chí Chung CC được các quốc gia thành viên và thừa nhận CCRA chấp nhận là hồ sơ hướng dẫn và áp dụng các tiêu chí đảm bảo an toàn trong quá trình thiết kế, xây dựng, đánh giá của các phần mềm ứng dụng. Tài liệu này sẽ phù hợp với quá trình đánh giá, tìm kiếm và xây dựng tiêu chuẩn quốc gia về đảm bảo an toàn cho phần mềm, vừa sẽ là điều kiện thuận lợi khi giao thương, hội nhập với thế giới trong việc cung cấp các phần mềm ứng dụng phát triển trong nước phù hợp với tiêu chuẩn đã được nhiều quốc gia thừa nhận.

3 Lý do xây dựng tiêu chuẩn

An toàn thông tin đang là mối quan tâm của các quốc gia, các tổ chức trong việc ứng dụng công nghệ thông tin trong các hoạt động quản lý, sản xuất, kinh doanh. Các thông tin liên tục về các vụ tấn công mạng, đánh cắp dữ liệu, thay đổi hệ thống, ngăn cản các hoạt động – kinh doanh, làm sai lệch thông tin, … trở thành mối lo ngại của mọi tổ chức, doanh nghiệp, nhất là khi cuộc cách mạng công nghiệp 4.0 đang liền kề. Hiểm hoạ mất an toàn cho các hệ thống thông tin ngày càng tăng cao, khi xu hướng tấn công nhằm vào các phần mềm ứng dụng tự phát triển hoặc của các bên thứ ba tồn tại nhiều lỗ hổng không được kiểm soát, giúp các kẻ tấn công dễ dàng xâm nhập và điều khiển hệ thống, …

Tại Việt Nam, trong thời gian qua đã ban hành và đang tiếp tục xây dựng nhiều tiêu chuẩn đảm bảo an toàn cho các hệ thống công nghệ thông tin như đã nêu trong phần 2.4 ở trên. Tuy nhiên, các tiêu chuẩn đã ban hành về an toàn thông tin là tiêu chuẩn chung về công nghệ thông tin như bộ tiêu chuẩn TCVN 8709:2011 (ISO/IEC 15408) gồm ba phần về các tiêu chí đánh giá an toàn thông tin, tiêu chuẩn TCVN 11386:2016 về phương pháp đánh giá an toàn công nghệ thông tin và chưa có tiêu chuẩn đánh giá cho phần mềm ứng dụng.

Tuy nhiều cơ quan, tổ chức, doanh nghiệp nhận thức rõ được hậu quả của các sự cố mạng có thể xảy ra, tầm quan trọng của việc đảm bảo an toàn cho các hệ thống và các ứng dụng công nghệ thông tin nhưng do chưa có tiêu chuẩn an toàn – đánh giá cho phần mềm ứng dụng để áp dụng nên việc xây dựng một tiêu chuẩn để

hướng dẫn thực hiện bảo đảm an toàn cho các phần mềm, ứng dụng là hết sức cần thiết.

Bên cạnh đó, một thực tế hiện nay là doanh nghiệp phần mềm trong nước khi phát triển hoặc gia công các phần mềm xuất khẩu ra nước ngoài sẽ gặp nhiều khó khăn nếu không áp dụng các chuẩn đảm bảo an toàn cho phần mềm ứng dụng, không có hướng dẫn hoặc quy định tiêu chuẩn phải áp dụng của bên yêu cầu. Do đó, một tiêu chuẩn an toàn cho phần mềm ứng dụng của quốc gia phù hợp với các tiêu chuẩn quốc tế sẽ giúp các sản phẩm phần mềm ứng dụng trong nước đáp ứng được các yêu cầu nghiêm ngặt về an toàn của quốc tế, tăng khả năng cạnh tranh và mang lại lợi thế cho một ngành kinh tế có nhiều tiềm năng của đất nước.

4 Nhu cầu thực tế và khả năng áp dụng

4.1 Nhu cầu thực tế

Phần cốt lõi của các hệ thống công nghệ thông tin là hoạt động của các phần mềm ứng dụng để cung cấp các tính năng, tiện ích cho các tổ chức và người sử dụng liên quan đến thông tin, dữ liệu truyền đưa và xử lý.

Với ba kiểu chính hiện nay của phần mềm ứng dụng gồm: phần mềm thương mại (có bản quyền, có thể sử dụng cho nhiều người hoặc phát triển theo yêu cầu riêng), phần mềm miễn phí (cả loại đã đóng gói và phần mềm mã nguồn mở) và phần mềm tự phát triển, cả người sử dụng cuối và các nhà quản lý hệ thống thông tin thường gặp rất nhiều khó khăn trong việc nhận biết khả năng đảm bảo an toàn của các ứng dụng đã, đang và sẽ sử dụng.

Ngoài ra, nhu cầu đánh giá định kỳ tính an toàn của các ứng dụng đang sử dụng trong các hệ thống thông tin là một nhu cầu thực tế của các tổ chức, doanh nghiệp nhằm giúp phát hiện sớm các nguy cơ và góp phần ngăn ngừa các sự cố về an toàn thông tin.

Đối với các cơ quan quản lý nhà nước, việc xây dựng một nền tảng an toàn cho các hoạt động ứng dụng công nghệ thông tin là một yêu cầu của quốc gia và của các tổ chức là một yêu cầu cấp thiết và đòi hỏi phải triển khai đồng thời ở tất cả các lĩnh vực liên quan, trong đó có an toàn cho các ứng dụng, phầm mềm.

Các nhu cầu cầu này hiện nay vẫn chưa được đáp ứng nếu chỉ dựa vào các tiêu chuẩn chung về các tiêu chí và phương pháp đánh giá an toàn công nghệ thông tin đã ban hành thành tiêu chuẩn như đã nêu trong phần 4 ở trên.

4.2 Phạm vi và khả năng áp dụng

Tiêu chuẩn này cung cấp hướng dẫn cho việc đảm bảo an toàn cho các phần mềm ứng dụng, do đó sẽ hỗ trợ tốt các cơ quan, tổ chức, doanh nghiệp trong hoạt động sau:

- Hỗ trợ các nhà phát triển ứng dụng, các doanh nghiệp phần mềm trong việc phát triển các phần mềm đáp ứng các tiêu chí và tiêu chuẩn an toàn của quốc gia và quốc tế;

- Hỗ trợ các tổ chức độc lập có thể đánh giá tính an toàn của các phần mềm ứng dụng về các tiêu chí, quy trình đánh giá theo tiêu chuẩn;

- Hỗ trợ các tổ chức, doanh nghiệp và các đối tượng sử dụng phần mềm có cơ sở để nhận khả năng an toàn của sản phẩm phần mềm ứng dụng được đưa vào sử dụng;

- Hỗ trợ các cơ quan quản lý nhà nước trong việc quản lý an toàn, thực thi các hoạt động điều tra hỗ trợ nếu có sự cố mất an toàn,

- Hỗ trợ các đơn vị chuyên trách về an toàn thông tin của các Bộ, các tỉnh-thành phố, các đội ứng cứu sự cố, đơn vị cung cấp dịch vụ an toàn thông tin trong việc điều tra, xác định nguyên nhân trong các trường hợp xảy ra sự cố mất an toàn liên quan đến các phần mềm ứng dụng.

5 Sở cứ xây dựng tiêu chuẩn

5.1 Lựa chọn tài liệu tham chiếu

Hiện tại Việt Nam đã có bộ tiêu chuẩn TCVN 8709 (ISO/IEC 15408) về tiêu chí chung đánh giá an toàn CNTT và TCVN 11386:2016 (ISO/IEC 18045: 2008) về hệ thống phương pháp đánh giá an toàn cho các sản phẩm và hệ thống công nghệ thông tin, nhưng chưa có một tiêu chuẩn cụ thể nào về đánh giá an toàn cho phần mềm ứng dụng.

Nhóm thực hiện nhiệm vụ sau khi nghiên cứu, tìm kiếm tài liệu phù hợp để làm cơ sở cho việc xây dựng tiêu chuẩn quốc gia đã sử dụng tài liệu kỹ thuật "Hồ sơ bảo vệ cho phần mềm ứng dụng" là tài liệu đang được áp dụng cho việc đánh

giá tính an toàn của các sản phẩm phần mềm ứng dụng của 28 quốc gia thành viên CCRA và được nhiều nước khác đang áp dụng để xây dựng tiêu chuẩn quốc gia.

5.2 Phương pháp xây dựng tiêu chuẩn

Trên cơ sở tham khảo các tiêu chuẩn về an toàn thông tin đã ban hành tại Việt Nam, các phương pháp xây dựng các tiêu chuẩn/ quy chuẩn, phương pháp xây dựng tiêu chuẩn này là chấp thuận nguyên vẹn nội dung của tài liệu gốc, có một số chỉnh sửa về thể thức, trình bày theo quy định hiện hành về trình bày Tiêu chuẩn quốc gia.

6 Nội dung dự thảo tiêu chuẩn

Dự thảo tiêu chuẩn được xây dựng dựa trên tài liệu quốc tế "Protection Profile for Application Software", phiên bản 1.2 ngày 22/4/2016 là phiên bản mới nhất của tài liệu này.

Tuy nhiên cấu trúc của tiêu chuẩn sẽ tuân theo cấu trúc được quy định của Tiêu chuẩn Việt Nam. TCVN "Công nghệ thông tin – Các kỹ thuật an toàn – An toàn cho phần mềm ứng dụng" sẽ chấp thuận các Mục và Phụ lục của tài liệu kỹ thuật "Hồ sơ bảo vệ cho Phần mềm ứng dụng", cụ thể như sau:

1. Phạm vi áp dụng: Đưa ra phạm vi áp dụng của tiêu chuẩn.

2. Tài liệu viện dẫn: Đưa ra các tài liệu mà tiêu chuẩn viện dẫn.

3. Thuật ngữ và định nghĩa: Giới thiệu các thuật ngữ được áp dụng trong tiêu chuẩn này.

4. Ký hiệu và thuật ngữ viết tắt: Giới thiệu các ký hiệu và thuật ngữ viết tắt được sử dụng trong tiêu chuẩn này.

5. Ranh giới của đích đánh giá TOE.

6. Các yêu cầu tuân thủ: bao gồm các báo cáo tuân thủ, các yêu cầu phù hợp với CC, các yêu cầu PP, yêu cầu đóng gói.

7. Định nghĩa các vấn đề an toàn: Các mối đe dọa mà mục tiêu đánh giá TOE sẽ giải quyết, các giả định về môi trường hoạt động.

8. Các mục tiêu an toàn: Định nghĩa các mục tiêu an toàn cho TOE, cho môi trường hoạt động và lý do mục tiêu an toàn.

9. Các yêu cầu an toàn: Yêu cầu chức năng bảo mật và yêu cầu đảm bảo bảo mật.

Phụ lục A: Các yêu cầu không bắt buộc

Phụ lục B: Các yêu cầu dựa trên lựa chọn

Phụ lục C: Các yêu cầu khách quan

Phụ lục D: Tài liệu và đánh giá Entropy

Tài liệu tham khảo

Bảng 1 - Đối chiếu dự thảo tiêu chuẩn với tài liệu viện dẫn

Dự thảo TCVN về đảm bảo an toàn cho phần mềm ứng dụng trong bộ TCVN về Công nghệ thông tin - Các kỹ thuật an toàn		Hồ sơ bảo vệ cho Phần mềm ứng dụng (Protection Profile for Application Software v1.2)	Ghi chú
1	1. Phạm vi áp dụng	1.1. Overview 1.3. Compliant Targets of Evaluation 1.4. Use Cases	Chấp thuận
2	2. Tài liệu viện dẫn		
3	3. Thuật ngữ và định nghĩa	1.2.1. Common Criteria Terms 1.2.2. Technology Terms	Chấp thuận nguyên vẹn
4	4. Ký hiệu và thuật ngữ viết tắt	Appendix F: Acronyms	Chấp thuận nguyên vẹn
5	5. Ranh giới của đích đánh giá TOE	1.3.1. TOE Boundary	Chấp thuận nguyên vẹn
6	6. Các yêu cầu tuân thủ	2. Conformance Claims	Chấp thuận nguyên vẹn
7	7. Định nghĩa các vấn đề an toàn	3. Security Problem Definition	Chấp thuận nguyên vẹn
8	8. Các mục tiêu an toàn	4. Security Objectives	Chấp thuận nguyên vẹn
9	9. Các yêu cầu an toàn	5. Security Requirements	Chấp thuận nguyên vẹn

10	Phụ lục A: Các yêu cầu tuỳ chọn Phụ lục B: Các yêu cầu dựa trên sự lựa chọn Phụ lục C: Các yêu cầu khách quan Phụ lục D: Tài liệu và đánh giá entropy	Appendix A: Optional Requirements Appendix B: Selection-Based Requirements Appendix C: Objective Requirements Appendix D: Entropy Documentation and Assessment	Chấp thuận nguyên vẹn
11	Tài liệu tham khảo	Appendix E: References	Chấp thuận và bổ sung

Bảng 2 - Đối chiếu tài liệu viện dẫn với dự thảo tiêu chuẩn

Hồ sơ bảo vệ cho Phần mềm ứng dụng (Protection Profile for Application Software v1.2)		Dự thảo TCVN về đảm bảo an toàn cho phần mềm ứng dụng trong bộ TCVN về Công nghệ thông tin - Các kỹ thuật an toàn	Ghi chú
1	1.1. Overview	1. Phạm vi áp dụng	Chấp thuận
2		2. Tài liệu viện dẫn	
3	1.2 Terms	3. Thuật ngữ và định nghĩa	Chấp thuận nguyên vẹn
4	1.3. Compliant Targets of Evaluation	1. Phạm vi áp dụng	Chấp thuận nguyên vẹn
5	1.3.1. TOE Boundary	5. Ranh giới của đích đánh giá TOE	Chấp thuận nguyên vẹn
6	1.4. Use Cases	1. Phạm vi áp dụng	
7	2. Conformance Claims	6. Các yêu cầu tuân thủ	Chấp thuận nguyên vẹn
8	3. Security Problem Definition	7. Định nghĩa các vấn đề an toàn	Chấp thuận nguyên vẹn
9	4. Security Objectives	8. Các mục tiêu an toàn	Chấp thuận

			nguyên vẹn
10	5. Security Requirements	9. Các yêu cầu an toàn	Chấp thuận nguyên vẹn
11	Appendix A: Optional Requirements	Phụ lục A: Các yêu cầu tuỳ chọn	Chấp thuận nguyên vẹn
12	Appendix B: Selection-Based Requirements	Phụ lục B: Các yêu cầu dựa trên sự lựa chọn	Chấp thuận nguyên vẹn
13	Appendix C: Objective Requirements Assessment	Phụ lục C: Các yêu cầu khách quan	Chấp thuận nguyên vẹn
14	Appendix D: Entropy Documentation and	Phụ lục D: Tài liệu và đánh giá Entropy	Chấp thuận nguyên vẹn
15	Appendix E: References	Tài liệu tham khảo	Chấp thuận và bổ sung
16	Appendix F: Acronyms	4. Ký hiệu và thuật ngữ viết tắt	Chấp thuận nguyên vẹn

7 Kết luận

Đảm bảo an toàn công nghệ thông tin nói chung và đảm bảo an toàn cho phần mềm ứng dụng nói riêng là một yêu cầu quan trọng trước tình hình các cuộc tấn công nhắm vào các hệ thống phần mềm trong các hệ thống công nghệ thông tin, bao gồm cả các hệ điều hành, các trình điều khiển và các phần mềm ứng dụng. Trong khi các tiêu chuẩn về đảm bảo an toàn cho phần mềm ứng dụng ở Việt Nam vẫn còn thiếu nên việc nghiên cứu xây dựng các tiêu chuẩn, yêu cầu kỹ thuật về đảm bảo an toàn cho phần mềm ứng dụng là rất cần thiết.

Tiêu chuẩn này được xây dựng dựa trên tài liệu kỹ thuật Hồ sơ bảo vệ cho phần mềm ứng dụng, phiên bản 1.2 được nhiều quốc gia thừa nhận và áp dụng. Vì vậy, tiêu chuẩn này khi được ban hành sẽ giúp các cơ quan, tổ chức có thể sử dụng để thực hiện các đánh giá mức độ đảm bảo an toàn cho các phần mềm ứng dụng đang và sẽ sử dụng, hoặc dựa vào đó để xây dựng, phát triển các sản phẩm phần mềm đảm bảo các yêu cầu về an toàn. Ngoài ra, nó cũng là cơ sở đánh giá tính an

toàn của các phần mềm ứng dụng của các nhà phát triển ngoài nước khi đưa vào áp dụng trong nước và ngược lại, đưa các phần mềm phát triển trong nước đáp ứng các yêu cầu đảm bảo an toàn khi cung cấp sang các nước trên thế giới.

Khi ban hành, tiêu chuẩn cũng giúp cho các cơ quan quản lý nhà nước trong lĩnh vực an toàn thông tin kiểm định tính an toàn của sản phẩm phần mềm phục vụ cho việc cấp phép hay cấp chứng nhận sử dụng, tăng cường quản lý, thực thi đảm bảo an toàn thông tin.

Bên cạnh đó, tiêu chuẩn này cũng hỗ trợ Trung tâm Ứng cứu Khẩn cấp Máy tính Việt Nam và các tổ chức cung cấp dịch vụ đánh giá an toàn thông tin trong việc đánh giá an toàn cho các phần mềm ứng dụng được sử dụng trong các tổ chức, cơ quan, doanh nghiệp hoặc được cung cấp cho các cá nhân.

8 Kiến nghị

- Để phù hợp với Bộ tiêu chuẩn quốc gia về an toàn thông tin, kiến nghị đặt tên của Tiêu chuẩn là Hồ sơ bảo vệ cho phần mềm ứng dụng:

CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN – HỒ SƠ BẢO VỆ CHO PHẦN MỀM ỨNG DỤNG

Information Technology - Security Techniques – Protection Profile for Application Software

- Ngoài ra, để tiêu chuẩn khi ban hành ngoài việc áp dụng trong nước mà còn thuận lợi cho các doanh nghiệp, tổ chức phát triển phần mềm trong nước khi xuất ra thị trường nước ngoài đáp ứng tiêu chuẩn được chấp nhận của nhiều nước, đề nghị ban hành tiêu chuẩn theo hình thức song ngữ Việt – Anh.

9 Tài liệu tham khảo

[1] NIAP *Protection Profile for Application Software (Hồ sơ bảo vệ cho các Phần mềm ứng dụng)*, phiên bản 1.2, ngày 22/4/2016.

[2] CCMB-2012-09-001 *Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and General Model (Tiêu chí chung dùng đánh giá an toàn về công nghệ thông tin – Phần 1: Giới thiệu và các Mô hình chung)*, phiên bản 3.1 – sửa đổi lần 4, tháng 9/2012.

[3] CCMB-2012-09-002 *Common Criteria for Information Technology Security Evaluation - Part 2: Security Functional Components (Tiêu chí chung dùng đánh giá an toàn về công nghệ thông tin – Phần 2: Các thành phần chức năng an toàn)*, phiên bản 3.1 – sửa đổi lần 4, tháng 9/2012.

[4] CCMB-2012-09-003 *Common Criteria for Information Technology Security Evaluation - Part 3: Security Assuarance Components (Tiêu chí chung dùng đánh giá an toàn về công nghệ thông tin – Phần 3: Các thành phần đảm bảo an toàn)*, phiên bản 3.1 – sửa đổi lần 4, tháng 9/2012.

[5] CCMB-2012-09-004 *Common Evaluation Methodology for Information Technology Security - Evaluation Methodology (Phương pháp Đánh giá Chung dùng cho an toàn công nghệ thông tin – Phương pháp đánh giá)*, phiên bản 3.1 – sửa đổi lần 4, tháng 9/2012.

[6] NIAP *Application Software Protection Profile (ASPP) Extended Package: File Encryption: Mitigating the Risk of Disclosure of Sensitive Data on a System (Gói mới rộng của Hồ sơ Bảo vệ Phần mềm Ứng dụng (ASPP): mã hoá tập tin: Giảm thiểu Rủi ro Công bố Dữ liệu Nhạy cảm trên Hệ thống)*, phiên bản 1.0, ngày 10/11/2014.

[7] NIAP *Extended Package for Secure Shell (SSH) (Gói mở rộng cho Shell an toàn SSH)*, phiên bản 1.0, ngày 19/02/2016

[8] *Clarification to the Entropy Documentation and Assessment Annex* (*Làm rõ Phụ lục Tài liệu và Đánh giá Entropy*), địa chỉ tham khảo: *https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/Entropy%20Documentation%20and%20Assessment%20Clarification.pdf*

[9] SP 800-38A của NIST, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques (Khuyến nghị cho các Phương thức Hoạt động của Mã Khối: Phương pháp và Kỹ thuật*), tháng 12/2001.

[10] SP 800-38D của NIST, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC (Khuyến nghị cho các Phương thức Mã Khối của Hoạt động: Phương thức Galois/Counter (GCM) và GMAC*), tháng 11/2007.

[11] SP 800-56A của NIST, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Khuyến nghị cho các Lược đồ Thiết lập Khoá Cặp bằng cách sử dụng mật mã Lô-ga-rít rời rạc*), Rev. 2, tháng 5/2013.

[12] SP 800-56B của NIST, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography (Khuyến nghị cho các Lược đồ Thiết lập Khoá Cặp bằng cách sử dụng mật mã phần tử số nguyên*), Rev. 1, tháng 9/2014.

[13] SP 800-57 part 1 của NIST, *Recommendation for Key Management, Part 1: General (Khuyến nghị cho Quản lý Khoá, Phần 1: Tổng quát)*, Rev. 4, tháng 01/2016.

[14] SP 800-90A của NIST, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Khuyến nghị cho việc tạo số ngẫu nhiên bằng cách sử dụng các Bộ tạo Bit Ngẫu nhiên Xác định)*, Rev. 1, tháng 6/2015.

[15] SP 800-90B của NIST, *Recommendation for Entropy Sources Used for Random Bit Generation (Khuyến nghị cho các nguồn Entropy được dùng để Tạo Bit Ngẫu nhiên)*, bản dự thảo lần 2, tháng 1/2011.

[16] SP 800-131A của NIST, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths (Chuyển đổi: Khuyến nghị cho việc chuyển đổi sử dụng của các thuật toán mật mã và độ dài khoá)*, Rev. 1, tháng 11/2015.

[17] FIPS 140-2 của NIST, *Security Requirements for Cryptographic Modules*

(Các Yêu cầu Bảo mật cho các Thành phần Mật mã), 25/5/2001, Change Notice 2, 12/03/2002

[18] FIPS 180-4 của NIST, *Secure Hash Standard (SHS) (Tiêu chuẩn Hàm Băm An toàn)*, tháng 8/2015

[19] FIPS 186-4 của NIST, *Digital Signature Standard (DSS) (Tiêu chuẩn Chữ ký Số)*, tháng 7/2013

[20] FIPS 198-1 của NIST, *The Keyed-Hash Message Authentication Code (HMAC) (Mã xác thực thông điệp Khoá Băm HMAC)*, tháng 7/2008

[21] ANSI X9.31-1998, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA) (Các chữ ký số sử dụng mật mã khoá công khai có thể đảo ngược cho Công nghệ các Dịch vụ Tài chính)*, 01/01/1998

[22] NIST, *The Secure Hash Algorithm Validation System (SHAVS) (Hệ thống Xác thực Thuật toán Băm An toàn)*, cập nhật ngày 21/5/2014

[23] TCVN 8709-1:2011 *Công nghệ thông tin – Các kỹ thuật an toàn – Các tiêu chí đánh giá an toàn công nghệ thông tin - Phần 1: Giới thiệu và mô hình tổng quát,* 2011