jtsec

BEYOND IT SECURITY

secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

Patch Management for ISO/IEC 15408 / Common Criteria

Javier Tallón, jtsec
Sebastian Fritsch, secuvera
ICCC 17.11.2020

- Overview
  - Background
  - Problem description: certification vs. security
  - ISO Project:
    Towards Creating an Extension for Patch Management
    for ISO/IEC 15408 and ISO/IEC 18045
    - Concept
      - ALC_PAM + SPD (for PAM) + (opt.) SFRs (for PAM)
    - Outlook
  - How to apply: practical considerations
  - Conclusions

secuvera

Background

- Background
  - Product time to market
    - Continuous delivery
    - Vulnerabilities are made public and patched everyday
    - But certification is painfully slow
  - Hot topic during first study period at ISO SC27 (2017)
    - Very ambitious
      - Continuous assurance, & all kind of situations
      - A lot of new CC Concepts
    - Conclusions
      - Too difficult
      - Not enough experience
      - But **real-world problem** that needs to be solved

- Background
  - Different approaches to Patch Management
    - Common Criteria
      - Classic: slow / IAR
      - JIL: base of our proposal / smartcards
      - ISCI WG1: same objectives / different approach
    - FIPS 140-2: 3ASUB / priority Q / templates
    - PCI-PTS: evaluated LC / trust by default
    - EMVCo: fast track

jtsec
BEYOND IT SECURITY

secuvera

Problem description

- Problem description
  - Certified TOE with known vulnerabilities
    - risk owners need updates
  - But updates are not certified
    - costs, time for certification
    - only done if required by regulation
  - Problem not limited to Common Criteria/ISO 15408, but any other security product certification
    - relevant to any product certification with defined version

- Problem description
  - CC compliant operation of TOEs often leads to
    - risk owner has to accept known vulnerabilities
    - but those were already fixed in a non-certified TOE update
  - Chances of this proposal
    - risk owner gets possibility to remove existing, known vulnerabilities
    - regulatory body can request risk owners to install updates to remove existing vulnerabilities
    - modernized tool to mandate the use of software which will be secure after certification but also later in the product lifecycle

- Current status
  - Risk owner
    - demand for certificate of product (TOE)
    - but also for
      - security issue handling correction and
      - delivery of security updates
      - often called “support processes”

- Other options

“Perfect the testing so no many patches need to be installed”

ATE_PERFECT.1

secuvera

ISO Project

- Concept
  A. Two (+one) building blocks
     1. ALC_PAM
        – Evaluate the Patch Management Process as part of the standard evaluation (certification)
     2. SPD (for PAM)
        – Common ground for all TOE types: SPD and adaptable Objectives
     3. optional SFRs (for PAM)
        – Technical capabilities for applying patches
        – Generic solution (set of SFRs)
        – Other sets of SFRs might be equivalent, needed to support legacy/existing PPs
  B. Options for Certification Bodies

- New family ALC_PAM
  - ALC_PAM.1 Patch Management Processes
  - key elements:
    - Security Impact Analysis Report (S-IAR)
      - Developer’s self-assessment of security relevance of a planned patch
    - Patch Management Policies
      - describes the mandatory procedures during patch release
      - rules when to re-certify or re-evaluate the TOE
      - end-of-support consideration of TOE
      - assessment and confirmation of the application of Patch Management Policies on a regular basis

- Options for Certification Bodies

  …for optimization

  - Fast-Track Re-Certification
  - Re-Evaluation (without Certification)
  - Provide templates to support the analyse impact of changes of a patch
  - Trust by default developers in order to harmonize security and certification
  - Put penalties if developers do not follow the published rules

- Timeline
  - 2º SP opened in September 2019 - Paris
  - Results of 2ºSP → Creation of a TR - St. Petersburg ISO meeting
  - 1st WD finalized by 19 of June 2020
  - Heavy discussion – Warsaw ISO meeting
  - 2nd WD finalized by 18 of January 2021
  - 2021 balloting of the 3rd WD 

- International support

- Ongoing discussion in ISO for WD2

  will be available January

  - "TOE and patch": analyse the impact on other SARs
    - option 1: modify SARs (like in JIL documents)
    - option 2: add requirements to ALC_PAM
  - Create (adoptable) set of objectives
    - and make set of SFRs only an option
  - Set of SFRs:
    - use CC Part 2, or
    - create new SFRs (use ECD)
  - Terminology: ISO, JIL, GP, … terminology
    - find minimum conflicting terminology for different communities
  - Try to keep ALC_PAM mostly stable
    - but minor changes necessary

How to apply:
practical considerations

- Current Working Draft of ISO Document
  - available here:
    https://www.jtsec.es/papers/Technical/Report_Patch_Management.pdf

- Guide for ST/PP authors:
  - add Extended Component Definition (ALC_PAM.1) to ST
  - add Evaluator Work Unit to ST (or link referenced document)
    - both defined in ISO document
  - add Security Problem Definition (SPD) and Objectives (for Patches) to ST
    - defined in ISO document
  - add SFRs to ST
    - if applicable to TOE
    - otherwise modify SFRs, or take other set of SFRs

- Prepare/Update Patch Management Processes
  - Check degree of implementation of existing Patch Management Processes
    - consider ALC_PAM.1 requirements
  - see also Guidance in ISO Document (→ Annexes)

- Developer perspective – Detailed Requirements
  - provide security patches until estimated end-of-support
  - for each patch/release: Security Impact Analysis Report (S-IAR)
  - update the evidence documentation used in the base evaluation
  - record decisions in the patch management process (transparency)
  - implement Patch Management Policy
    - communicate end-of-support
    - define content of patch release notes
    - mandatory procedures during patch release
    - self-assess and confirm the application of these policies
    - conditions for additional tests by ITSEF/lab before release

- Evaluator perspective
  - What do I have to evaluate / look for?
  - As part of the ´common´ evaluation process
    - The set of SFRs chosen by the vendor solves the PAM SPD
    - The set of SFRs chosen by the vendor are adequately implemented (ATE/AVA)
  - As part of ALC_PAM
    - Content and presentation requirements
      - The process for patch release, including responsibilities
      - The secure use of cryptographic keys involved in patch generation
    - Evidence of application of PAM procedures and self-assessment
      - Through dry run
      - Sampling during a site visit

- Pilot projects
  - secuvera runs first pilot of ALC_PAM evaluation in German CC scheme (BSI) with genua
    - Note: ALC_PAM version from the beginning of 2020

- Conclusions
  - We are trying to solve a real world problem 
  - We are doing it very fast! Balloting of the TR by Autumn'21 
  - International support 
  - Multi community support
  - Accepted for trial use by the new EUCC opening the door to the Critical Update Flow 

jtsec
BEYOND IT SECURITY

secuvera
BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

Thank you!
Vielen Dank!
¡Muchas Gracias!

Javier Tallón
jtallon@jtsec.es
+34-858981999

jtsec Beyond IT Security
Avenida de la Constitución 20, 208
18012 Granada
Spain

Sebastian Fritsch
sfritsch@secuvera.de
+49-7032/9758-24

secuvera GmbH
Siedlerstraße 22-24
71126 Gäufelden/Stuttgart
Germany