

Study Period on Introduction  
of new assurance requirements in ISO/IEC 15408-3 and evaluation  
methodology in ISO/IEC 18045 covering patch management and deployment

## Final Report

Francois Guerin, Sebastian Fritsch, Tyrone Stodart

ISO JTC 1/SC 27/WG 3

Gjøvik, 30/09 to 04/10/2018



- 1st Call for Contributions in Berlin
- 2nd Call for Contributions in Wuhan
  - We asked for:
    - [..]
    - Assurance requirements to give assurance on patch management process
    - [..]
    - Product type / technology domain specific information
      - e.g. patch periods, types of patches

- Initial idea
    - benefit of standardized patch management evaluation
    - add some patch (or software update) related vocabulary to CC
    - for PP/ST writers: have a set of predefined SFR covering patch management (technical update functionality)
    - for PP/ST writers: have set of predefined SAR covering patch management (TOE updates)
    - similar Evaluation methodology, maybe derived for different technologies
- consistency and flexibility

- Contributions

- 1st CfC

- 4 contributions received from US, DE and FR delegations.

- 2nd CfC

- 1 contribution received from JP delegation.
    - Plus input from liaison channel IEC/TC 65/WG 10:  
IEC TR 62443-2-3:2015 Annex B

- Summary

- few contribution received between meetings
  - few contributing people during meetings and confcalls

- Not so sure we have a real-world problem?
  - unsure if WG3 members would like to standardize?
- Process evaluation vs Product evaluation
  - some WG3 members required explicitly to perform a process evaluation instead of product evaluation
  - not in line with CC framework (ISO 15408) based on product evaluation

- IEC TR 62443-2-3:2015 Annex B
  - documents reflects the perspective of the asset owner (end user) of industrial components (products) and not of product developer
  - previous certification (or qualification) of products is assumed to be already done
    - but this is the focus of our work

2. SFR-Packages	8
2.1. Introduction	8
2.2. Package 1: Update initiation	8
2.3. Package 2: Secure loading	11
2.4. Package 3: Patch identification and verification	12
2.5. Package 4: Activation and installation	13
2.6. Package 5: Failure handling	14
2.7. Overview	16
2.7.1. Rational (Mapping of the SFRs to Objectives)	16
2.7.2. Examples by different categories of Technologies	16
3. SAR-Packages	17
3.1. Introduction	17
3.2. SARs from ISO/IEC 15408-3	18
3.2.1. Flaw remediation (ALC_FLR)	18
3.3. Extended SARs	19
3.3.1. TEMPLATE (Axx_vyy)	19
3.3.2. Patch Management-Process (ADV_PMP)	19
3.3.2.1. ADV_PMP.1	19
3.3.3. Patch Development Process (ALC_PDP)	19
3.3.3.1. ALC_PDP.1	19
3.3.4. Actual Flaw Remediation (ALC_AFR)	20
3.3.4.1. ALC_AFR.1	20
3.3.5. Patch Delivery Process (ALC_PYP)	20
3.3.5.1. ALC_PYP.1	20
3.3.6. Update Deployment (AGD_UPD)	21
3.3.6.1. AGD_UPD.1	21
3.3.7. Source Code Difference Analysis (ADV_DIF)	21
3.3.7.1. ADV_DIF.1 Basic Source Code Difference Analysis	21
3.3.8. Patch Verification Analysis (AVA_PVA)	21
3.3.8.1. ADV_PVA.1	21
3.4. EAL-Mapping	22
3.4.1. Assurance Continuity concept	22
3.4.2. TOE Assurance concept	22

## • Work of rapporteurs group after Wuhan

- worked on document to collect SFRs and SARs
- definition of packages
- good progress defining SFR packages
- but had trouble to identify and describe sufficient generic evaluation actions for assurance requirements

- Another outcome of discussion
  - Several solutions per Technical Domain (TD)
    - i.e. no simple way to standardize
  - Different security objectives
  - some TD have already solved the problem for their own situation
    - yearly re-certification (no time for patch certification)
      - e.g. Multi-Function Printer (MFP)
    - those have no need to standardize Patch Management



- Identified solutions for SARs based on current practices
  - Reuse of principles from assurance continuity based on IAR document
    - e.g. standardize IAR process and extend those
  - Reuse of principles found in supporting documents
    - e.g. composite evaluation in SOG-IS
  - But need for broader discussion of universally applicable evaluation actions for patch management
    - at the moment not enough experience

- Conclusion

- We have a real world problem which needs to be solved!
  - work has to be continued
- Standardize SFRs is possible
  - e.g. with packages
  - but different objectives for different technical domains
  - but SFRs are the easier part of the problem, first focus on SARs
- Standardize SAR is much more complex
  - we produced ideas
    - e.g. ALC\_PMP, ... vs. {ALC,ADV,ATE}\_DIF
  - but at the moment we do not have enough experience

- Final conclusion
  - we suspend the work in ISO
  - need more experience on this topic between vendors, labs and CBs before standardize
  - next steps:
    - run pilot projects in one or two schemes involving labs
    - possible future activity in ISO
      - create Technical Report (TR) to be used as supporting document including new vocabulary, SFRs and SARs
      - reflect differences in Technical Domains
  - Please contact us, if you want to collaborate on this topic!

# secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

## Thank you!

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

secuvera GmbH  
Siedlerstraße 22-24  
71126 Gäufelden/Stuttgart  
Germany