ISO/IEC JTC 1 N 9957

2010-01-12

ISO/IEC JTC 1
Information Technology

Document Type:	**New Work Item Proposal**
Document Title:	**New Work Item Proposal on “Secure software development and evaluation under ISO/IEC 15408 and ISO/IEC 18405”**
Document Source:	**SC 27 Secretariat**
Reference:	
Document Status:	**This document is circulated to JTC 1 National Bodies for concurrent review. If the JTC 1 Secretariat receives no objections to this proposal by the due date indicated, we will so inform the SC 27 Secretariat**
Action ID:	**Act**
Due Date:	**2010-04-12**
No. of Pages:	**9**

ISO/IEC JTC 1/SC 27 N8130

ISO/IEC JTC 1/SC 27/WG 3 N38130

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE:	text for Proposed NP Ballot
TITLE:	**New Work Item Proposal on "Secure software development and evaluation under ISO/IEC 15408 and ISO/IEC 18405"**
SOURCE:	Secretariat of JTC 1/SC 27
DATE:	2010-01-11
PROJECT:	**NP**
STATUS:	In accordance with Resolution 7 (contained in SC 27 N8115) of the 39th SC 27/WG 3 meeting held in Redmond, WA, USA, 2nd - 6th November 2009, this document is being circulated to the SC 27 National Bodies for a 3-month NWI letter ballot and to JTC 1 for a concurrent review.
ACTION ID:	**LB**
DUE DATE:	**2010-04-12**
DISTRIBUTION:	P- and L-Members W. Fumy, SC 27 Chairman M. De Soete, SC 27 Vice-Chair E. J. Humphreys, K. Naemura, M. Bañôn, M.-C. Kang, K. Rannenberg, WG-Conveners
MEDIUM:	Livelink-server
NO. OF PAGES:	1+ 8

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1sc27.din.de/en

New Work Item Proposal

NP submitting

PROPOSAL FOR A NEW WORK ITEM

Date of presentation of proposal: 2009-11-03	Proposer: ISO/IEC JTC 1 SC27
Secretariat: National Body	**ISO/IEC JTC 1 N** ISO/IEC JTC 1/SC 27 N 8130

A proposal for a new work item shall be submitted to the secretariat of the ISO/IEC joint technical committee concerned with a copy to the ISO Central Secretariat.

Presentation of the proposal

Title Secure software development and evaluation under ISO/IEC 15408 and ISO/IEC 18405

Scope

In the case where a target of evaluation (TOE) being evaluated, under ISO/IEC 15408 and ISO/IEC 18405, includes specific software portions, the TOE developer may optionally present the developer's technical rationale for mitigating software common attack patterns and related weaknesses as described in the latest revision of the Common Attack Pattern Enumeration and Classification (CAPEC) available from http://capec.mitre.org/. The developer's technical rationale is expected to include a range of mitigation techniques, from architectural properties to design features, coding techniques, use of tools or other means.

This Technical Report (TR) provides guidance for the developer and the evaluator on how to use the CAPEC as a technical reference point during the TOE development life cycle and in an evaluation of the TOE secure software under ISO/IEC 15408 and 18045, by addressing:

a) A refinement of the IS 15408 Attack Potential calculation table for software, taking into account the entries contained in the CAPEC and their characterization.

b) How the information for mitigating software common attack patterns and related weaknesses is used in an IS 15408 evaluation, in particular providing guidance on how to determine which attack patterns and weaknesses are applicable to the TOE, taking into consideration of

   1. the TOE technology;
   2. the TOE security problem definition;
   3. the interfaces the TOE exports that can be used by potential attackers;
   4. the Attack Potential that the TOE needs to provide resistance for.

c) How the technical rationale provided by the developer for mitigating software common attack patterns and related weaknesses is used in the evaluation of the TOE design and the development of test cases.

d) How the CAPEC and related Common Weakness Enumeration (CWE) taxonomies are used by the evaluator, who needs to consider all the applicable attack patterns and be able to exploit specific related software weaknesses while performing the subsequent vulnerability analysis (AVA_VAN) activities on the TOE.

e) How incomplete entries from the CAPEC are resolved during an IS 15408 evaluation.

f) How the evaluator's attack and weakness analysis of the TOE incorporates other attacks and weaknesses not yet documented in the CAPEC.

The development of this TR will investigate whether specific elements from ISO/IEC 15026 (and its revision) are applicable to the guidelines being developed in the TR within the context of IS 15408 and 18405.

Purpose and justification –

To implement software with an adequate level of security assurance, it is necessary that the developer uses good software engineering and analytical practices that pay specific attentions to the attacker's perspective. With the public availability of a catalog of attack patterns (to software implementations) along with a comprehensive schema and classification taxonomy from the Common Attack Pattern Enumeration and Classification (CAPEC) organization, the developer and the evaluator have a common mechanism to describe, explain, reason, understand, and investigate the security of the TOE in terms of the TOE's robustness when subject to CAPEC software common attack patterns.

Due to the guidance provided by this TR to the developer and the evaluator, the evaluator's related actions in an ISO/IEC 15408 security evaluation of the TOE can be expected to have a better focus on analysing the resistance of the TOE against common attack methods. The consumer of the corresponding certification report would be able to discover (as a minimum) if a specific CAPEC software common attack pattern has been adequately addressed by the developer and the evaluator for the TOE during the security evaluation.

Because of the established relationship between ISO/IEC JCT1 SC27 WG3 and CCDB on security evaluation, this work is also supported by CCDB. It is expected that the forthcoming Liaison statement from CCDB to SC27 for the Redmond SC27 meeting would include some input materials for supporting this new work item proposal.

Programme of work

If the proposed new work item is approved, which of the following document(s) is (are) expected to be developed?

___a single International Standard

___ more than one International Standard (expected number: ....)

____ a multi-part International Standard consisting of .... parts

____ an amendment or amendments to the following International Standard(s) ....

__X__ a technical report , type ...3........

And which standard development track is recommended for the approved new work item?

__X__a. Default Timeframe

___b. Accelerated Timeframe

____c. Extended Timeframe

Relevant documents to be considered ISO/IEC 15408-3, ISO/IEC 18405, ISO /IEC 15026 (revision)

Co-operation and liaison CCDB

Proposed acting editor: Shaun Gilmore, US NB

Preparatory work offered with target date(s)

WD 2010-05 CD 2011-05 FDIS 2012-10 IS 2013-05

Signature: SC 27/WG 3

Will the service of a maintenance agency or registration authority be required ....No............
- If yes, have you identified a potential candidate? ....
- If yes, indicate name ....

Are there any known requirements for coding? ....No............
-If yes, please specify on a separate page

Does the proposed standard concern known patented items? No
- If yes, please provide full information in an annex

Comments and recommendations of the JTC 1 or SC 27- attach a separate page as an annex, if necessary

{PRIVATE }Comments with respect to the proposal in general, and recommendations thereon:
It is proposed to assign this new item to JTC 1/SC 27

Voting on the proposal - Each P-member of the ISO/IEC joint technical committee has an obligation to vote within the time limits laid down (normally three months after the date of circulation).

Date of circulation: 2010-01-11	**Closing date for voting:** 2010-04-12	**Signature of Secretary:** Krystyna Passia Secretariat SC 27

NEW WORK ITEM PROPOSAL - PROJECT ACCEPTANCE CRITERIA		
Criterion	**Validity**	**Explanation**
A. Business Requirement		
A.1 Market Requirement	Essential _X__ Desirable ___ Supportive ___	
A.2 Regulatory Context	Essential ___ Desirable ___ Supportive ___ Not Relevant _X_	
B. Related Work		
B.1 Completion/Maintenance of current standards	Yes ___ No_X__	
B.2 Commitment to other organisation	Yes _X__ No__	CCDB
B.3 Other Source of standards	Yes ___ No__X_	
C. Technical Status		
C.1 Mature Technology	Yes _X__ No___	
C.2 Prospective Technology	Yes __ No__X_	
C.3 Models/Tools	Yes ___ No_X__	
D. Conformity Assessment and Interoperability		
D.1 Conformity Assessment	Yes __ No_X__	
D.2 Interoperability	Yes __ No__X_	
E. Cultural and Linguistic Adaptability	**Yes____** **No__X___**	
E.1 Cultural and Linguistic Adaptability	Yes __ No__X_	

E.2 Adaptability to Human Functioning and Context of Use	Yes __ No__X_	
F. Other Justification		

Notes to Proforma

A. Business Relevance. That which identifies market place relevance in terms of what problem is being solved and or need being addressed.

A.1 Market Requirement. When submitting a NP, the proposer shall identify the nature of the Market Requirement, assessing the extent to which it is essential, desirable or merely supportive of some other project.

A.2 Technical Regulation. If a Regulatory requirement is deemed to exist - e.g. for an area of public concern e.g. Information Security, Data protection, potentially leading to regulatory/public interest action based on the use of this voluntary international standard - the proposer shall identify this here.

B. Related Work. Aspects of the relationship of this NP to other areas of standardisation work shall be identified in this section.

B.1 Competition/Maintenance. If this NP is concerned with completing or maintaining existing standards, those concerned shall be identified here.

B.2 External Commitment. Groups, bodies, or for a external to JTC 1 to which a commitment has been made by JTC for Co-operation and or collaboration on this NP shall be identified here.

B.3 External Std/Specification. If other activities creating standards or specifications in this topic area are known to exist or be planned, and which might be available to JTC 1 as PAS, they shall be identified here.

C. Technical Status. The proposer shall indicate here an assessment of the extent to which the proposed standard is supported by current technology.

C.1 Mature Technology. Indicate here the extent to which the technology is reasonably stable and ripe for standardisation.

C.2 Prospective Technology. If the NP is anticipatory in nature based on expected or forecasted need, this shall be indicated here.

C.3 Models/Tools. If the NP relates to the creation of supportive reference models or tools, this shall be indicated here.

D. Conformity Assessment and Interoperability

D.1 Indicate here if Conformity Assessment is relevant to your project. If so, indicate how it is addressed in your project plan.

D.2 Indicate here if Interoperability is relevant to your project. If so, indicate how it is addressed in your project plan

E. Cultural and Linguistic Adaptability Indicate here if cultural and linguistic adaptability is applicable to your project. If so, indicate how it is addressed in your project plan.

F. Other Justification Any other aspects of background information justifying this NP shall be indicated here

Appendix (Outline Document for the NWIP)

Outline Document for the New Technical Report Work Item “Secure software development and evaluation under ISO/IEC 15408 and ISO/IEC 18405”

To implement software with an adequate level of security assurance, it is necessary that the developer uses good software engineering and analytical practices that pay specific attentions to the attacker’s perspective. For an evaluator to conclude an evaluation assurance level through an evaluation as defined in ISO/IEC 15408 and ISO/IEC 18405 in a more comparable, objective and repeatable manner, a comprehensive catalog of software attack paths, weaknesses and corresponding mitigations is desired as a technical reference point to determine whether the developer practices are effective for the software target of evaluation (TOE). This catalog should be developer independent, and have mechanisms to be updated and improved as it is used in ISO/IEC 15408 evaluations of software TOEs.
This Technical Report (TR) suggests the use of the publicly available catalog of attack patterns (to software implementations) along with its comprehensive schema and classification taxonomy from the Common Attack Pattern Enumeration and Classification (CAPEC) organization (http://capec.mitre.org). Through the guidance provided by the TR, the TR encourages the developer and the evaluator to use this catalog as a common mechanism to describe, explain, reason, understand, and investigate the security of the TOE in terms of the TOE’s resistance when subject to CAPEC software common attack patterns. The TR guidance aims to narrow the focus of the evaluator’s related actions in an ISO/IEC 15408 security evaluation of the TOE to the analysis of the TOE resistance against common attack methods. The consumer of the corresponding certification report would be able to discover (as a minimum) if a specific CAPEC software common attack pattern has been adequately addressed by the developer and the evaluator for the TOE during the security evaluation.

Scope

In the case where a target of evaluation (TOE) being evaluated, under ISO/IEC 15408 and ISO/IEC 18405, includes specific software portions, the TOE developer may optionally present the developer’s technical rationale for mitigating software common attack patterns and related weaknesses as described in the latest revision of the Common Attack Pattern Enumeration and Classification (CAPEC) available from http://capec.mitre.org/. The developer’s technical rationale is expected to include a range of mitigation techniques, from architectural properties to design features, coding techniques, use of tools or other means.
This Technical Report (TR) provides guidance for the developer and the evaluator on how to use the CAPEC as a technical reference point during the TOE development life cycle and in an evaluation of the TOE under ISO/IEC 15408 and 18045, by addressing:
a) A refinement of the ISO/IEC 15408 Attack Potential calculation table for software, taking into account the entries contained in the CAPEC and their characterization.
b) How the information for mitigating software common attack patterns and related weaknesses is used in an ISO/IEC 15408 evaluation, in particular providing

guidance on how to determine which attack patterns and weaknesses are applicable to the TOE, taking into consideration of

1. the TOE technology;
2. the TOE security problem definition;
3. the interfaces the TOE exports that can be used by potential attackers;
4. the Attack Potential that the TOE needs to provide resistance for.

c) How the technical rationale provided by the developer for mitigating software common attack patterns and related weaknesses is used in the evaluation of the TOE design and the development of test cases.

d) How the CAPEC and related Common Weakness Enumeration (CWE) taxonomies are used by the evaluator, who needs to consider all the applicable attack patterns and be able to exploit specific related software weaknesses while performing the subsequent vulnerability analysis (AVA_VAN) activities on the TOE.

e) How incomplete entries from the CAPEC are resolved during an ISO/IEC 15408 evaluation.

f) How the evaluator's attack and weakness analysis of the TOE incorporates other attacks and weaknesses not yet documented in the CAPEC.

Modifications to ISO/IEC 15408 or 18045 are outside the scope of this TR.

Similar Efforts

In the Common Criteria evaluation terminology, this TR may also be viewed as a "Supporting Document". In field of smart-cards and similar devices, a comprehensive set of Supporting Documents are published and maintained by the CCRA Development Broad (http://www.commoncriteriaportal.org/supdocs.html). These documents have been developed with the support from the user community, the product vendors, and the Certification Bodies that have historically been involved in the Common Criteria evaluation of such devices, thus bringing into their content not only technical value and know-how, but more importantly, the agreement of the technology specific eco-system on how secure to develop and how to evaluate the type of products that they refer to.

This TR intends to achieve a similar effect for software TOEs. As it is developed within ISO/IEC JTC 1 SC27, the TR should enjoy a similar support from the user community, the product vendors, and the Certification Bodies.

Table of Content Suggestion

In alignment with the proposed scope, this TR includes the following sections/clauses.

- A refinement of the ISO/IEC 15408 Attack Potential calculation table for software, taking into account the entries contained in the CAPEC and their characterization.
- The way how the CAPEC information is applied on an ISO/IEC 15408 evaluation, in particular providing guidance on how to determine which entries are applicable to a product functionality type of the TOE, taking into consideration
    - the TOE technology;
    - the TOE security problem definition;
    - the interfaces the TOE exports that can be used by potential attackers;
    - the Attack Potential that the TOE needs to provide resistance for.

- How the technical rationale provided by the developer for mitigating software common attack patterns and related weaknesses is used in the evaluation of the TOE design and the development of test cases.
- How the CAPEC and related Common Weakness Enumeration (CWE) taxonomies are used by the evaluator, who needs to consider all the applicable attack patterns and be able to exploit specific related software weaknesses while performing the subsequent vulnerability analysis (AVA_VAN) activities on the TOE.
- How incomplete entries from the CAPEC are resolved during an ISO/IEC 15408 evaluation.
- How the evaluator's attack and weakness analysis of the TOE incorporates other attacks and weaknesses not yet documented in the CAPEC.