Document ISO/IEC/JTC 1/SC 22/WG 23 N0680

Draft Agenda Meeting #47
ISO/IEC JTC 1/SC 22/WG 23: Programming Language Vulnerabilities
23-24 January 2017

Meeting Location :

Holiday Club Vacations at Orange Lake – North Village
8505 W. Irlo Bronson Parkway (Hwy 192)
Kissimmee, Fl

Meeting Times:

23-24 January 2017: 0900-1700 Eastern Standard Time (1400-2200 UTC)

Local Arrangements:

Hotel and local arrangement information can be found in the local arrangements document.

Local Contacts:

Stephen Michell (stephen.michell@maurya.on.ca), mobile +1 613 299 9047

IMPORTANT:

Agenda

1 Opening activities

1.1 Opening Comments

1.2 Introduction of Participants/Roll Call

1.3 Procedures for this Meeting

1.4 Approval of previous Minutes (meeting 46, document N674)

1.5 Review of actions items and resolutions, Action Item and Decision Logs

1.6 Approval of Agenda [N 0680]

1.7 Future Meeting Schedule

2018

Pre-mtg 55	01/11/18	
#54	01/09/18	Ottawa Canada
#53	15-16/06/18	With WG 9 and Ada Europe
Pre-mtg-53	Teleconference	
#52	TBD April 2018	
Pre-mtg 52	TBD March 2018	
#51	22-23 January 2018	Orlando, FL, or Atlanta GA at CSA

2017

pre-mtg-51	20/11/17	Teleconference (UTC 2000, 2 hr)
post-mtg-50	16/10/17	Teleconference (UTC 2000, 2 hr)
#50	17-18 August 2017	BSI London (with SC 22 Plenary)
#49	12-13 June 2017	Vienna, Austria with Ada Europe(2 day)

post-mtg-48	15/05/17	Teleconference (UTC 2000, 2 hr)
#48	6-7 April 2017	IBM Markham, Canada (2 day)
pre-mtg-48	06/03/17	Teleconference (UTC 2100, 2 hr)
#47	23-24 January 2017	In-person (2 day) (this meeting)

---

2. Liaison Activities

2.1 SC 22

2.2 PL 22 (Open)

2.3 PL22.3/WG5 (Fortran)

2.4 WG4 (COBOL)

2.5 WG9 (Ada)

2.6 PL22.11/WG14 (C)

2.7 PL22.16/WG21 (C++)

2.8 Ecma International, TC49/TG2 (C#)

2.9 Ecma International, TC39 (ECMAScript)

2.10 MISRA (C)

2.11 MISRA (C++)

2.12 SPARK

2.13 SC7/WG19 (UML)

2.14 SC27/WG3, WG4 Security

2.15 Other Liaison Activities or National body reports

3. Document Review

We have a major decision to make about the class of documentation that we create. ISO is treating Technical Reports with distain, insistung that they only contain data that was used in the creation of standards. JTC 1 at its last plenary assigned TR 10000-1 to SC 7 to update and republish as an IS. A key point here is that SC 7 is republishing it as an IS without a New Work Item Proposal.

For discussion: It is likely time that WG 23 made TR 24772 (all parts) into standards vice TR's. If we do this, do we want to repackage, or essentially send forward the current documents? Repackaging could see the .5 (Guidance) portions become normative and the other subclauses supporting informative material.

3.1 TR 24772-1 Vulnerabilities, language independent

Document N0677,

3.2 TR 24772-2 Ada language specific part

Document N0681. The Ada Part has been delivered by WG 9. Joyce Tokar assumes the role of editor. This version is missing 4 sections that we added in clause 6, plus the accumulated guidance in section 5. We also need to update a couple of titles, and Erhard is proposing new wording for failure modes.

3.3 TR 24772-3 C language specific part

Document N0676.

Notes from Paul Preney (Canada)

It seems to me that in N0665 (TR 24772-3 C), 6.15 Arithmetic Wrap-around Error there should also be some mention of:
Emphasize that signed integer over/underflows might trap on some systems.
i.e., It is imperative to ensure that all operations on signed integers will never over- or underflow.
Remind the reader that one cannot assume the underlying representation of signed integers.
Also in 6.24 Side-effects and Order of Evaluation of Operands in N0665, there is no mention of Annex C: Sequence Points --which IMHO should be added to the 2nd paragraph. Annex C nicely refers to the appropriate sections of the C standard where additional details are provided for the specific items.

6.39 Deep vs. Shallow Copying... Stephen's note. I agree --but I would add that in C one should write a function to perform the correct and desired copying of a data structure. This is the best way, in C, to avoid issues when copying data. Thus, I would suggest the guidance should be to write a function to perform the copying of a data structure to avoid accidental incorrect copying of the data structure.

3.4 TR 24772-4 Python language specific part

Document N0592.

3.5 TR 24772-8 Fortran

Document [N0560] needs review.

3.6 TR 24772-X C++

Consider document [N0582]

3.7 Bibliography for each TR24772 Part

3.8 Dirty Dozen Rules for C, generic, and other languages

Review how the rules are incorporated into Part 1 and Part 3. Consider the generic rules for other Parts.

4 Strategy (Face to face meetings only)

5 Publicity (Face to face meetings only)

6 Other Business

6.1 Review of Assignment of responsibilities

7. Resolutions and Action Items

8. Adjournment