Business Plan and Convener's Report
ISO/IEC JTC 1/SC 22/WG 23 N0266

Document:
ISO/IEC JTC 1/SC22 WG 23 N0266

Date:
2010-07-09

PERIOD COVERED:
Sept 2009 – July 2010

SUBMTTED BY:
Convener, ISO/IEC JTC 1/SC 22/WG 23: Vulnerabilities
John Benito
Blue Pilot
P.O. Box 2998
Santa Cruz, CA 95063-2998
USA
+1 (831) 427-0528 (Office)
+1 (831) 600-5547 (Mobile)
John Benito

1. MANAGEMENT SUMMARY

1.1. JTC 1/SC 22/WG 23

Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use

1.2. PROJECT REPORT

1.2.1. COMPLETED PROJECTS

JTC 1 NP 24772, *Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection*. This is a Technical Report type III.

1.2.2. PROJECTS UNDERWAY

JTC 1 NP 24772, *Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection*. This is a revision.

1.2.3. CANCELLED PROJECTS

None over this period.

1.2.4. COOPERATION and COMPETITION

Where appropriate, WG 23 has established active liaisons with other SC22 working groups and other standards organizations. A Category C liaison with MISRA-L has been established.

There is no apparent direct competition with any other current SC22 working group.

2. PERIOD REVIEW

2.1. MARKET REQUIREMENTS

WG 23 feels that it is responding to the needs of the software security community and the software safety community by inclusion. WG 23 will accept input and liaison by any and all appropriate organizations.

2.2. ACHIEVEMENTS

WG 23 has spent the fourth year refining and publishing the first version of TR 24772, successfully balloted the PDTR.2 document, answering all comments from the PDTR.2 ballot. WG 23 developed a DTR document, and answered all comments from the DTR ballot, producing a TR that has been forwarded to ITTF for publication.

2.3. RESOURCES

WG 23 plans to meet three to four times per year. Eight national bodies are currently participating by attending meetings or by being involved in the technical discussions that take place over the email reflector. The national bodies are: Canada, France, Germany, Italy, Japan, Netherlands, UK, and the USA.

Over the last several years WG 23 has made Web conferencing capabilities available for those that are finding it difficult to travel[1].

Liaison with five SC22 Language groups, four groups outside of SC22 has been established, and a Category C liaison has been established with MISRA-L.

Current WG 23 liaisons are:

Group	Name/Type	Person assigned
SC 22/WG4	Cobol	Barry Tauber
SC 22/WG5	Fortran	Dan Nagle
SC 22/WG9	Ada	Erhard Ploedereder
SC 22/ WG14	C	Tom Plum
SC 22/ WG 21	C++	Group (Tom Plum)
SC 7/WG 19	Open Distributed Processing and Modeling Languages	Cesar Gonzalez-Perez
ECMA TC39/TG2	C#	Tom Plum
JSR-282/JSR-302	Real-Time/Safety-Critical Java	Ben Brosgol
Linux Foundation	Linux	Nick Stoughton
MDC	MUMPS	Ed de Moel
MISRA-L	Category C	Clive Pygott

3. FOCUS NEXT WORK PERIOD

WG 23 will focus on:

- JTC 1 NP 24772, *Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection*.
- Work with Language working groups to develop Language independent Annexes.

[1] Furnished by MITRE Corp.

- Work on the New Item if approved, see 4.1 and Attachment 2.

3.1. DELIVERABLES

None.

3.2. STRATEGIES

WG 23 believes that routine handling will suffice to complete the progress desired.

3.3. RISKS

No problems are anticipated.

3.4. OPPORTUNITIES

None.

3.5. WORK PROGRAM PRIORITIES

WG 23 will concentrate on the work item NP 24772.

4. OTHER ITEMS

4.1. POSSIBLE ACTION REQUESTS AT FORTHCOMING PLENARY

WG 23 would like to ask SC 22 to consider, approve and forward the New Work Item that is proposed in WG 23/N0264. Please see Attachment 1.

Now that WG 23 has published TR 24772, WG 23 would like SC 22 to consider a resolution that will ask for TR 24772 to be freely available. Please see Attachment 2 for rationale and proposed wording.

4.2. PROJECT EDITOR

The following individuals have been appointed project editors and backup project editors:

- JTC 1 NP 24772, Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection.

  John Benito (Project Editor)

4.3. ELECTRONIC DOCUMENT DISTRIBUTION

WG 23 has conducted some of its detailed technical discussion using email reflector maintained by James Moore, The MITRE Corporation.

WG 23 also has a Web site provided at http://aitc.aitcnet.org/isai/ and maintained by James Moore, The MITRE Corporation.

WG 23 uses a secure wiki setup and maintained by Dinkumware, Ltd.. This secure wiki is used for quick exchange of documents during and between meetings.

WG 23 is providing all the appropriate committee documents on the Committee Web site, eliminating the need for paper mailings.

4.4. RECENT MEETINGS

#1	26-27 Jun 2006	District of Columbia, USA	ANSI/INCITS and Blue Pilot
#2	14-15 Sep 2006	London, UK	BSI
#3	11-13 Dec 2006	District of Columbia, USA	ANSI/INCITS and Blue Pilot
#4	30-2 Apr/May 2007	Padova, Italy	NNI
#5	18-20 July 2007	Ottawa, Ontario Canada	SCC
#6	14-15 Oct 2007	Kona, HI, USA	ANSI/INCITS and Plum Hall
#7	10-10 Dec 2007	Pittsburg, PA, USA	ANSI/INCITS and CERT
#8	09-11 Apr 2008	Amsterdam, NL	NEN, ACE
#9	29-01 Sep/Oct 2008	Stuttgart, DE	Universität Stuttgart
#10	13-15 April 2009	San Diego, CA	ANSI/INCITS and MITRE Corp
#11	13-15 July 2009	Ottawa, Ontario Canada	SCC
#12	01-03 Nov 2009	San Cruz, CA	ANSI/INCITS and Blue Pilot
#13	26-28 Apr 2010	Padova, Italy	UNI
#14	28-30 Jul 2010	Kona, HI, USA	ANSI/INCITS and Plum Hall

4.5. FUTURE MEETINGS

#15	15-17 Sep 2010	Ottawa, Ontario Canada	SCC
#16	14-16 Dec 2010	San Diego, CA	ANSI/INCITS and MITRE Corp
#17	23-25 Mar 2011	Europe (try to co-locate with WG21)	Tentative
#18	18-20 Jun 2011	Edinburgh (co-locate with WG9)	Tentative
#19	Sep 2011	Copenhagen (co-locate with SC 22)	Tentative
#20	Dec 2011	Washington, DC	Tentative

Attachment 1

New Work Item Proposal

February 2004

PROPOSAL FOR A NEW WORK ITEM

Date of presentation of proposal: 2010-04-26	Proposer: SC22 WG23
Secretariat: ANSI (US)	**ISO/IEC JTC 1 N** XXXX ISO/IEC JTC 1/SC 22 N XXX

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 - to be completed by the proposer.

Title (subject to be covered and type of standard, e.g. terminology, method of test, performance requirements, etc.) Information Technology -- Programming languages, their environments and system software interfaces -- Software Code Signing

Scope (and field of application) This new work item encompasses the signing of software code and software executables.

Purpose and justification - attach a separate page as annex, if necessary

Digital signatures for software code are an important technique to ensure trustworthiness and integrity of the software. With a digital signature, there is a reliable way of verifying that what is being used hasn't been modified somewhere in the supply chain. This can have serious consequences for systems that are intended to implement integrity properties such as safety, security or privacy. For less critical systems, the use of a reliable capability to digitally verify software can deny access to attackers or prevent other forms of electronic vandalism.

This project will provide a uniform way to digitally sign software so that the software can be verified at any stage between source and actual use. Code signing can apply to entire software programs, software libraries or to just code segments. Code signing will ultimately provide the needed basis for a widely used infrastructure to lessen the possibility of a supply chain attack.

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 .....2.....

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

- The programming language standards of ISO/IEC JTC 1/SC 22.
- For market reasons, the specifications of popular languages that are not the subject of ISO standards.
- The software engineering standards of ISO/IEC JTC 1/SC 7, as a source of extra-linguistic mitigation methods.
- The crypto standards of ISO/IEC JTC1/SC27
- Java ARchives (JAR) File Specification
- Microsoft Authenticode
- [ITU-T Recommendation X.509] [3] (2005): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 08/05.

Co-operation and liaison

- ISO/IEC/JTC1/SC7/WG7 (Software and Systems Life Cycle Processes)
- ISO/IEC JTC 1/SC7/WG21 (?) (Software Asset Management)
- ISO/IEC/JTC 1/SC27/WG2 (Cryptography and Security Mechanisms)
- ISO/IEC/JTC 1/SC27/WG4 (Security Controls and Services)
- ITU-T

Preparatory work offered with target date(s)

Signature:

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

Are there any known requirements for cultural and linguistic adaptability? No

-If yes, please specify on a separate page

Comments and recommendations of the JTC 1 or SC 22 Secretariat - attach a separate page as an annex, if necessary

Comments with respect to the proposal in general, and recommendations thereon:
It is proposed to assign this new item to JTC 1/SC 22/WG 23

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: YYYY-MM-DD	**Closing date for voting:** YYYY-MM-DD	**Signature of Secretary:**

NEW WORK ITEM PROPOSAL - PROJECT ACCEPTANCE CRITERIA		
Criterion	Validity	Explanation
A. Business Requirement		
A.1 Market Requirement	Essential _X__ Desirable ___ Supportive ___	Verification of the source of software is an increasingly important problem.
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 ___ No_X__	
B.3 Other Source of standards	Yes ___ No_X__	
C. Technical Status		
C.1 Mature Technology	Yes ___ No_X__	
C.2 Prospective Technology	Yes _X__ No___	
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. Adaptability to Culture, Language, Human Functioning and Context of Use		
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		

Attachment 2

Request

The JTC 1/SC 22 secretariat requests that the JTC 1 secretariat take the necessary action to make ISO/IEC TR 24772, *Information Technology — Programming Languages — Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use*, publicly available and free of charge.

ISO/IEC TR 24772 describes security and safety vulnerabilities that can arise from the undisciplined use of programming languages, including languages maintained by ISO/IEC JTC 1/SC 22. It also describes how improved use of the languages allows one to avoid the vulnerabilities. The free availability of 24772 would promote the use of JTC 1 programming languages by demonstrating how they can be used in a safe and secure manner.

Rationale

Document ISO/IEC JTC 1 N7269 provides the criteria for approving the free availability of a JTC 1 standard or technical report. Three criteria from that document are relevant to the current request:

Items of the proposed criteria	**Justification**	**Ease of consensus**
(5) REFERENCE MODELS A: Standards which explain the relationships between existing standards	Catalogues of standards for sales promotion	++
(6) REFERENCE MODELS B: Architectural descriptions which describe frameworks to guide standards development, including profiles and taxonomies	Not implementable specifications and enhance awareness and influence of JTC 1	+
(8) SUBSETS: Those Type 3 technical reports which describe basic visions and concepts in the technical domains covered by a set of standards	Enhance awareness and influence of JTC 1	+

All of the JTC 1 programming languages were developed in an era prior to the ubiquitous connectivity of today's computers. Their designers paid little attention to the problems of "hacking" by unauthorized users. Therefore these languages contain features that, when improperly used, make the program vulnerable to attack from unauthorized users. Language developers and maintainers, including SC 22 working groups, have paid increasing attention to the problem in recent years and now provide alternative features or alternative ways to use existing features that mitigate the problem. Unfortunately, this is not well known. For example, the C language is commonly accused of having a weakness in its facility for string copying, despite the fact that the standard now provides an alternative library that does not have the weakness.

The purpose of TR 24772 is to survey the subject of vulnerabilities in programming languages and to provide generic descriptions of the vulnerabilities and the ways to mitigate them. The first edition of the report is completely language-independent. Future editions will contain annexes for individual programming languages relating the language-independent descriptions to the specific features of the specific language. The TR can play an important role in bolstering confidence in the SC 22 programming languages.

Therefore, with respect to the criteria cited above:

(5) The language-specific annexes of TR 24772 will call out many of the language standards of SC22. Existing freely available material[2] on similar subjects has the effect of directing persons away from the ISO programming languages. Our material will have the effect of directing users toward the standardized languages because we emphasize adherence to the ISO standards as the most basic step to address the problem.

(6) TR 24772 includes recommendations to the architects of programming languages regarding areas that they might address in future revisions. It demonstrates the commitment of JTC 1 to meet the challenges of modern Information Technology. TR 24772 does not contain normative provisions.

(8) TR 24772 explains how to use standard ISO programming languages in manners that are appropriate to the modern challenges of computing security and safety. The Technical Report makes direct references to the ISO language standards.

In this particular case, it is also useful to describe the situation with respect to the "rules for selection of the criteria," also listed in N7269:

Rules for selection of the criteria	**Comments regarding TR 24772**
(1) Insignificant impact on revenue by free access	TR 24772 cannot be used as a substitute for any of the SC 22 standards. It does not even provide summaries of them.
(2) Promotion of the sales of other JTC 1 documents	TR 24772 helps to improve public awareness of JTC 1 programming languages, the importance of using the standard languages, and the steps that have been taken to improve the standards.
(3) Enhancement of awareness and dominance of JTC 1 work	TR 24772 demonstrates that JTC 1 is the best and most responsible venue for programming language specification.

[2] Examples include cwe.mitre.org, cve.mitre.org, the SANS Institute top 25 list, the CERT website for C and C++, SCAP, nvd.nist.org, and OWASP.