ISO/IEC JTC 1/SC 22/WG 23 N 0262

Request for approval of free availability for ISO/IEC TR 24772, Information Technology — Programming Languages — Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use

Date	27 June 2010
Contributed by	James W. Moore
Original file name	
Notes	Draft 1

(It is hoped that this document will be approved at the 2010 plenary meeting of ISO/IEC JTC 1/SC 22 and forwarded to JTC 1 for action.)

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. So the 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, though, 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:

(5) The language-specific annexes of TR 24772 will call out many of the language standards of SC22. Existing freely available material[1] 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 maintainers of programming languages regarding areas that they might address in future revisions. TR 24772 does not contain normative provisions, and it demonstrates the commitment of JTC 1 to meet the challenges of modern Information Technology

(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. We make 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

[1] 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.

	using the standard language, 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.