Document: WG 14/N1668
Title: Comment on N1663 - TS 17961 - C Secure Coding Rules
Date: 2012-12-10
Author: Willem Wakker

The goal of this comment is to make clear what a conforming analyzer may and/or may not do in terms of grouping or skipping required diagnostics. This issue is touched upon in several paragraphs scattered throughout the Introduction section and the very vague 'For each rule' sentence in the Conformance section.

It is the Dutch position that a conforming analyzer either
- produces all required diagnostics; or
- if diagnostics are skipped or grouped, it should be perfectly clear (documentation required!) on which criteria this grouping or skipping is performed.
A conforming analyzer preferably can operate in both modes.

Proposed changes to N1663.

- Introduction: from the last paragraph of page vi remove the sentences starting with 'Many analyzers...' and 'The implementation of such a mechanism ...'.
Rationale: these words are to be used elsewhere.

- Introduction: last sentence of same paragraph.
Replace the sentence 'This TS assumes that ... ' by a Note:

> Note: For a proper analysis as required by this TS it is obvious that the analyzer's visibility need to extend beyond the boundaries of the current function or translation unit being analyzed (....).

Rationale: this makes it clear that this is not an explicit additional requirement but follows from the general required functionality. Therefore this note can stay in the Introduction section.
Same as DEW #1 in N1666.

- Completeness and soundness (page vii), after the paragraph 'The degree to which conforming analyzers ...' add the following text:

> Analyzers may provide methods to eliminate the need to research each diagnostic on every invocation of the analyzer. This may be done for instance by skipping certain diagnostics (possible examples: 'Omit all diagnostics related to this variable', or 'Omit all diagnostics that follow from the usage of file xyz.c') or by grouping certain diagnostics (possible example: 'Report diagnostic ABC [for this variable] only once'). Such operation of the analyzer should preferably be under user control but should in any case be clearly documented. Details on how such operations might work are outside the scope of this Technical Specification and are merely a matter of Quality of Implementation.

- Conformance section (page 3), replace last paragraph before 2.1 ('For each rule, ...') by

> A conforming analyzer shall either produce all required diagnostics for a given set of C source programs, or,

if diagnostics are skipped or grouped, the criteria
used to group or skip certain diagnostics shall either
be under user control or be documented (or both).