ISO/IEC JTC 1/SC 22/OWGV N0044

Contribution from Clive Pygott, Vulnerability classifications used in QinetiQ report

19 September 2006

Classification	**Description**
Casting	Issues involving explicit type conversion with cast operators
Constant Objects	Issues involving objects that can not be modified, i.e. objects with a const-qualification
Enumerated Types	Issues involving the value and type of enumeration constants
Evaluation	Issues related to evaluation, but not its order, e.g. whether or how many times expressions are evaluated, rather than in what order, c.f. Initialisation
Evaluation Order	Issues relating to order of evaluation of sub-expression within an expression etc. That is, the elements being ordered are visible in the program, c.f. Initialisation Order
Exceptions	Issues relating to any ‘exceptional’ behaviour. This does not just relate to the explicit C++ exception mechanism
Execution Environment	Issues involving freestanding environments ("execution takes place without the benefit of an operating system") and the **main** function
Function Calls	Issues relating to calling functions
Inheritance	Issues relating to inheritance (excluding virtual functions), both single and multiple
Initialisation	Issues relating to initialisation, excluding the order of initialisation, c.f. Evaluation
Initialisation Order	Order of execution of initialisation actions. That is, where the elements being ordered or the action of concern is implied (e.g. program start) rather than explicit, c.f. Evaluation Order
Layout	Layout of objects in memory, e.g. the order and relative position of sub-objects within an object, c.f. Representation
Lexical Analysis	Issues relating to lexical analysis of the source text
Memory Allocation	Issues relating to if and how memory is allocated and deallocated
Mixed Language Working	Issues relating to the use of multiple language linkages
NameSpace	Issues relating to name-spaces in the general computer science sense of the scope of a name, rather than necessarily to do with C++'s namespace construct
Object Lifetime	Issues relating to the start and end of an object’s lifetime and constructor/destructor calls, e.g. when (or if) an object is created or destroyed
One Definition Rule	Issues relating to the One Definition Rule over multiple translation units, as defined in [3, section 3.2]
Pointers	Issues relating to pointer types
Pre-processor	Issues relating to macros and pre-processing tokens
Representation	The representation of an object in memory (e.g. 2's compliment vs. sign and magnitude), c.f. Layout
String Literal	Issues relating to string literals
Template	Issues relating to templates
Type Info	Issues relating to types, type_info objects and typeid expressions
Value Range	Issues relating to the range of values a type can take
Virtual Functions	Issues relating to virtual functions and calls