Page vi: [1] Deleted **Stephen Michell** **2017-03-10 12:44 PM**

FOREWORD... VII

INTRODUCTION.. VIII

1. SCOPE 1

2. NORMATIVE REFERENCES...1

3. TERMS AND DEFINITIONS, SYMBOLS AND CONVENTIONS 1

3.1 Terms and definitions 1

3.2 Symbols and conventions.. 5

4. BASIC CONCEPTS 6

4.1 Purpose of this Technical Report 6

4.2 Intended audience 6

4.3 How to use this document... 7

5 VULNERABILITY ISSUES AND GENERAL AVOIDANCE MECHANISMS.............................8

5.1 Predictable execution... 8

5.2 Sources of unpredictability in language specification 9

5.2.1 Incomplete or evolving specification.. 9

5.2.2 Undefined behaviour 10

5.2.3 Unspecified behaviour 10

5.2.4 Implementation-defined behaviour 10

5.2.5 Difficult features.. 10

5.2.6 Inadequate language support 10

5.3 Sources of unpredictability in language usage.. 10

5.3.1 Porting and interoperation 10

5.3.2 Compiler selection and usage 11

5.4 Top avoidance mechanisms (guidance?)... 11

6. PROGRAMMING LANGUAGE VULNERABILITIES 13

6.1 General.. 13

6.2 Type System [IHN] 14

6.3 Bit Representations [STR] 16

6.4 Floating-point Arithmetic [PLF] 18

6.5 Enumerator Issues [CCB] 21

6.6 Conversion Errors [FLC] 23

6.7 String Termination [CJM]... 25

6.8 Buffer Boundary Violation (Buffer Overflow) [HCB] 26

6.9 Unchecked Array Indexing [XYZ]... 28

6.10 Unchecked Array Copying [XYW] 30

6.11 Pointer Type Conversions [HFC] 31

6.12 Pointer Arithmetic [RVG].. 32

6.13 Null Pointer Dereference [XYH] 33

6.14 Dangling Reference to Heap [XYK].. 34

6.15 Arithmetic Wrap-around Error [FIF] 36

6.16 Using Shift Operations for Multiplication and Division [PIK].. 38

6.17 Choice of Clear Names [NAI].. 39

6.18 Dead Store [WXQ].. 41

6.19 Unused Variable [YZS] 42

6.20 Identifier Name Reuse [YOW]... 43

6.21 Namespace Issues [BJL] 45
6.22 Initialization of Variables [LAV] 47
6.23 Operator Precedence and Associativity [JCW] 49
6.24 Side-effects and Order of Evaluation of Operands [SAM] 50
6.25 Likely Incorrect Expression [KOA] 52
6.26 Dead and Deactivated Code [XYQ] 54
6.27 Switch Statements and Static Analysis [CLL] 56
6.28 Demarcation of Control Flow [EOJ] 57
6.29 Loop Control Variables [TEX] 59
6.30 Off-by-one Error [XZH] 60
6.31 Structured Programming [EWD] 61
6.32 Passing Parameters and Return Values [CSJ] 63
6.33 Dangling References to Stack Frames [DCM] 65
6.34 Subprogram Signature Mismatch [OTR] 67
6.35 Recursion [GDL] 69
6.36 Ignored Error Status and Unhandled Exceptions [OYB] 70
6.37 Type-breaking Reinterpretation of Data [AMV] 72
6.38 Deep vs. Shallow Copying [YAN] 74
6.39 Memory Leaks and Heap Fragmentation [XYL] 76
6.40 Templates and Generics [SYM] 77
6.41 Inheritance [RIP] 79
6.42 Violations of the Liskov Substitution Principle or the Contract Model [BLP] 81
6.43 Redispatching [PPH] 83
6.44 Polymorphic variables [BKK] 85
6.45 Extra Intrinsics [LRM] 87
6.46 Argument Passing to Library Functions [TRJ] 88
6.47 Inter-language Calling [DJS] 89
6.48 Dynamically-linked Code and Self-modifying Code [NYY] 91
6.49 Library Signature [NSQ] 92
6.50 Unanticipated Exceptions from Library Routines [HJW] 93
6.51 Pre-processor Directives [NMP] 94
6.52 Suppression of Language-defined Run-time Checking [MXB] 96
6.53 Provision of Inherently Unsafe Operations [SKL] 97
6.54 Obscure Language Features [BRS] 98
6.55 Unspecified Behaviour [BQF] 100
6.56 Undefined Behaviour [EWF] 101
6.57 Implementation-defined Behaviour [FAB] 103
6.58 Deprecated Language Features [MEM] 105
6.59 Concurrency – Activation [CGA] 106
6.60 Concurrency – Directed termination [CGT] 108
6.61 Concurrent Data Access [CGX] 109
6.62 Concurrency – Premature Termination [CGS] 111
6.63 Protocol Lock Errors [CGM] 113
6.64 Reliance on External Format String [SHL] 115

7. APPLICATION VULNERABILITIES 117

7.1 General 117
7.2 Unrestricted File Upload [CBF] 117
7.3 Download of Code Without Integrity Check [DLB] 118
7.4 Inclusion of Functionality from Untrusted Control Sphere [DHU] 119

7.5 URL Redirection to Untrusted Site ('Open Redirect') [PYQ] 120
7.6 Use of unchecked data from an uncontrolled or tainted source [EFS] 121
7.7 Cross-site Scripting [XYT] 122
7.8 Adherence to Least Privilege [XYN] 124
7.9 Privilege Sandbox Issues [XYO] 125
7.10 Executing or Loading Untrusted Code [XYS] 126
7.11 Missing Required Cryptographic Step [XZS] 127
7.12 Insufficiently Protected Credentials [XYM] 128
7.13 Missing or Inconsistent Access Control [XZN] 129
7.14 Authentication Logic Error [XZO] 129
7.15 Hard-coded Password [XYP] 131
7.16 Sensitive Information Uncleared Before Use [XZK] 132
7.17 Improperly Verified Signature [XZR] 133
7.18 Use of a One-Way Hash without a Salt [MVX] 134
7.19 Inadequately Secure Communication of Shared Resources [CGY] 134
7.20 Memory Locking [XZX] 136
7.21 Resource Exhaustion [XZP] 137
7.22 Time Consumption Measurement [CCM] 138
7.23 Incorrect Authorization [BJE] 139
7.24 Improper Restriction of Excessive Authentication Attempts [WPL] 140
7.25 Unspecified Functionality [BVQ] 140
7.26 Fault Tolerance and Failure Strategies [REU] 141
7.27 Distinguished Values in Data Types [KLK] 144
7.28 Resource Names [HTS] 146
7.29 Injection [RST] 147
7.30 Unquoted Search Path or Element [XZQ] 150
7.31 Discrepancy Information Leak [XZL] 151
7.32 Path Traversal [EWR] 152
7.33 Clock Issues [CCI] 154
7.34 Time Drift and Jitter [CDJ] 156

ANNEX A (*INFORMATIVE*) VULNERABILITY TAXONOMY AND LIST 158
A.1 General 158
A.2 Outline of Programming Language Vulnerabilities 158
A.3 Outline of Application Vulnerabilities 160
A.4 Vulnerability List 161

ANNEX B (*INFORMATIVE*) LANGUAGE SPECIFIC VULNERABILITY TEMPLATE 164
~~Bibliography~~ 167

INDEX 170

Page 175: [2] Deleted **Stephen Michell** **2017-03-10 11:50 AM**

~~[1] ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Standards*, 2004~~

~~[2] ISO/IEC TR 10000-1, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework*~~

Page 175: [2] Deleted **Stephen Michell** **2017-03-10 11:50 AM**

~~[1] ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Standards*, 2004~~

~~[2] ISO/IEC TR 10000-1, *Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework*~~

Page 175: [3] Formatted Stephen Michell 2017-03-10 11:54 AM

calibri

Page 175: [4] Formatted Stephen Michell 2017-03-10 11:55 AM

Font:(Default) +Theme Body, 11 pt, Italic, Font color: Auto

Page 175: [5] Formatted Stephen Michell 2017-03-10 11:55 AM

Font:Italic

Page 175: [6] Formatted Stephen Michell 2017-03-10 11:59 AM

Not Strikethrough

Page 175: [6] Formatted Stephen Michell 2017-03-10 11:59 AM

Not Strikethrough

Page 175: [6] Formatted Stephen Michell 2017-03-10 11:59 AM

Not Strikethrough

Page 175: [6] Formatted Stephen Michell 2017-03-10 11:59 AM

Not Strikethrough

Page 175: [7] Deleted Stephen Michell 2017-03-10 12:00 PM

(document RTCA SC167/DO-178B)

Page 175: [7] Deleted Stephen Michell 2017-03-10 12:00 PM

(document RTCA SC167/DO-178B)

Page 175: [8] Formatted Stephen Michell 2017-03-10 11:57 AM

Not Strikethrough

Page 175: [9] Deleted Stephen Michell 2017-03-10 11:57 AM

:

Page 175: [9] Deleted Stephen Michell 2017-03-10 11:57 AM

:

Page 175: [10] Formatted Stephen Michell 2017-03-10 11:57 AM

Not Strikethrough

Page 175: [10] Formatted Stephen Michell 2017-03-10 11:57 AM

Not Strikethrough

Page 181: [11] Deleted **Stephen Michell** **2017-03-10 12:39 PM**

Section Break (Continuous)

Ada, 13, 59, 63, 73, 76
AMV – Type-breaking Reinterpretation of Data, 72
API
  Application Programming Interface, 16
APL, 48
Apple
  OS X, 120
application vulnerabilities, 9
Application Vulnerabilities
  Adherence to Least Privilege [XYN], 113
  Authentication Logic Error [XZO], 135
  Cross-site Scripting [XYT], 125
  Discrepancy Information Leak [XZL], 129
  Distinguished Values in Data Types [KLK], 112
  Download of Code Without Integrity Check [DLB], 137
  Executing or Loading Untrusted Code [XYS], 116
  Hard-coded Password [XYP], 136
  Improper Restriction of Excessive Authentication Attempts [WPL], 140
  Improperly Verified Signature [XZR], 128
  Inclusion of Functionality from Untrusted Control Sphere [DHU], 139
  Incorrect Authorization [BJE], 138
  Injection [RST], 122
  Insufficiently Protected Credentials [XYM], 133
  Memory Locking [XZX], 117
  Missing or Inconsistent Access Control [XZN], 134
  Missing Required Cryptographic Step [XZS], 133
  Path Traversal [EWR], 130
  Privilege Sandbox Issues [XYO], 114
  Resource Exhaustion [XZP], 118
  Resource Names [HTS], 120
  Sensitive Information Uncleared Before Use [XZK], 130
  Unquoted Search Path or Element [XZQ], 127
  Unrestricted File Upload [CBF], 119
  Unspecified Functionality [BVQ], 111
  URL Redirection to Untrusted Site ('Open Redirect') [PYQ], 140
  Use of a One-Way Hash without a Salt [MVX], 141
application vulnerability, 5
Ariane 5, 21

bitwise operators, 48
BJE – Incorrect Authorization, 138
BJL – Namespace Issues, 43
black-list, 120, 124
BQF – Unspecified Behaviour, 92, 94, 95
break, 60
BRS – Obscure Language Features, 91
buffer boundary violation, 23
buffer overflow, 23, 26
buffer underwrite, 23
BVQ – Unspecified Functionality, 111

C, 22, 48, 50, 51, 58, 60, 63, 73
C++, 48, 51, 58, 63, 73, 76, 86
C11, 192
call by copy, 61
call by name, 61
call by reference, 61
call by result, 61
call by value, 61
call by value-result, 61
CBF – Unrestricted File Upload, 119
CCB – Enumerator Issues, 18
CGA – Concurrency – Activation, 98
CGM – Protocol Lock Errors, 105
CGS – Concurrency – Premature Termination, 103
CGT - Concurrency – Directed termination, 100
CGX – Concurrent Data Access, 101
CGY – Inadequately Secure Communication of Shared Resources, 107
CJM – String Termination, 22
CLL – Switch Statements and Static Analysis, 54
concurrency, 2
continue, 60
cryptologic, 71, 128
CSJ – Passing Parameters and Return Values, 61, 82

dangling reference, 31
DCM – Dangling References to Stack Frames, 63
Deactivated code, 53
Dead code, 53
deadlock, 106
DHU – Inclusion of Functionality from Untrusted Control Sphere, 139
Diffie-Hellman-style, 136
digital signature, 84
DJS – Inter-language Calling, 81
DLB – Download of Code Without Integrity Check, 137
DoS
  Denial of Service, 118
dynamically linked, 83

EFS – Use of unchecked data from an uncontrolled or tainted source, 109
encryption, 128, 133
endian
  big, 15
  little, 15
endianness, 14
Enumerations, 18
EOJ – Demarcation of Control Flow, 56
EWD – Structured Programming, 60
EWF – Undefined Behaviour, 92, 94, 95
EWR – Path Traversal, 124, 130

exception handler, 86

FAB – Implementation-defined Behaviour, 92, 94, 95
FIF – Arithmetic Wrap-around Error, 34, 35
FLC – Numeric Conversion Errors, 20
Fortran, 73

GDL – Recursion, 67
generics, 76
GIF, 120
`goto`, 60

HCB – Buffer Boundary Violation (Buffer Overflow), 23, 82
HFC – Pointer Casting and Pointer Type Changes, 28
HJW – Unanticipated Exceptions from Library Routines, 86
HTML
- Hyper Text Markup Language, 124

HTS – Resource Names, 120
HTTP
- Hypertext Transfer Protocol, 127

IEC 60559, 16
IEEE 754, 16
IHN –Type System, 12
inheritance, 78
IP address, 119

Java, 18, 50, 52, 76
JavaScript, 125, 126, 127
JCW – Operator Precedence/Order of Evaluation, 47

KLK – Distinguished Values in Data Types, 112
KOA – Likely Incorrect Expression, 50

language vulnerabilities, 9
Language Vulnerabilities
- Argument Passing to Library Functions [TRJ], 80
- Arithmetic Wrap-around Error [FIF], 34
- Bit Representations [STR], 14
- Buffer Boundary Violation (Buffer Overflow) [HCB], 23
- Choice of Clear Names [NAI], 37
- Concurrency – Activation [CGA], 98
- Concurrency – Directed termination [CGT], 100
- Concurrency – Premature Termination [CGS], 103
- Concurrent Data Access [CGX], 101
- Dangling Reference to Heap [XYK], 31
- Dangling References to Stack Frames [DCM], 63
- Dead and Deactivated Code [XYQ], 52
- Dead Store [WXQ], 39
- Demarcation of Control Flow [EOJ], 56
- Deprecated Language Features [MEM], 97
- Dynamically-linked Code and Self-modifying Code [NYY], 83
- Enumerator Issues [CCB], 18
- Extra Intrinsics [LRM], 79
- *Floating-point Arithmetic [PLF]*, xvii, 16
- Identifier Name Reuse [YOW], 41
- Ignored Error Status and Unhandled Exceptions [OYB], 68
- Implementation-defined Behaviour [FAB], 95
- Inadequately Secure Communication of Shared Resources [CGY], 107
- Inheritance [RIP], 78
- Initialization of Variables [LAV], 45
- Inter-language Calling [DJS], 81
- Library Signature [NSQ], 84
- Likely Incorrect Expression [KOA], 50
- Loop Control Variables [TEX], 57
- Memory Leak [XYL], 74
- Namespace Issues [BJL], 43
- Null Pointer Dereference [XYH], 30
- Numeric Conversion Errors [FLC], 20
- Obscure Language Features [BRS], 91
- Off-by-one Error [XZH], 58
- Operator Precedence/Order of Evaluation [JCW], 47
- Passing Parameters and Return Values [CSJ], 61, 82
- Pointer Arithmetic [RVG], 29
- Pointer Casting and Pointer Type Changes [HFC], 28
- Pre-processor Directives [NMP], 87
- Protocol Lock Errors [CGM], 105
- Provision of Inherently Unsafe Operations [SKL], 90
- Recursion [GDL], 67
- Side-effects and Order of Evaluation [SAM], 49
- Sign Extension Error [XZI], 36
- String Termination [CJM], 22
- Structured Programming [EWD], 60
- Subprogram Signature Mismatch [OTR], 65
- Suppression of Language-defined Run-time Checking [MXB], 89
- Switch Statements and Static Analysis [CLL], 54
- Templates and Generics [SYM], 76
- Termination Strategy [REU], 70
- Type System [IHN], 12
- Type-breaking Reinterpretation of Data [AMV], 72
- Unanticipated Exceptions from Library Routines [HJW], 86
- Unchecked Array Copying [XYW], 27
- Unchecked Array Indexing [XYZ], 25
- Uncontrolled Fromat String [SHL], 110
- Undefined Behaviour [EWF], 94
- Unspecified Behaviour [BFQ], 92
- Unused Variable [YZS], 40
- Use of unchecked data from an uncontrolled or tainted source [EFS], 109
- Using Shift Operations for Multiplication and Division [PIK], 35

language vulnerability, 5

LAV – Initialization of Variables, 45
LHS (left-hand side), 241
Linux, 120
livelock, 106
`longjmp`, 60
LRM – Extra Intrinsics, 79

MAC address, 119
macof, 118
MEM – Deprecated Language Features, 97
memory disclosure, 130
Microsoft
- Win16, 121
- Windows, 117
- Windows XP, 120

MIME
- Multipurpose Internet Mail Extensions, 124

MISRA C, 29
MISRA C++, 87
`mlock()`, 117
MVX – Use of a One-Way Hash without a Salt, 141
MXB – Suppression of Language-defined Run-time Checking, 89

NAI – Choice of Clear Names, 37
name type equivalence, 12
NMP – Pre-Processor Directives, 87
NSQ – Library Signature, 84
NTFS
- New Technology File System, 120

`NULL`, 31, 58
`NULL pointer`, 31
null-pointer, 30
NYY – Dynamically-linked Code and Self-modifying Code, 83

OTR – Subprogram Signature Mismatch, 65, 82
OYB – Ignored Error Status and Unhandled Exceptions, 68, 163

Pascal, 82
PHP, 124
PIK – Using Shift Operations for Multiplication and Division, 34, 35, 197
PLF – Floating-point Arithmetic, xvii, 16
POSIX, 99
`pragmas`, 75, 96
predictable execution, 4, 8
PYQ – URL Redirection to Untrusted Site ('Open Redirect'), 140

real numbers, 16
Real-Time Java, 105
resource exhaustion, 118
REU – Termination Strategy, 70
RIP – Inheritance, xvii, 78
`rsize_t`, 22
RST – Injection, 109, 122
runtime-constraint handler, 191
RVG – Pointer Arithmetic, 29

safety hazard, 4
safety-critical software, 5
SAM – Side-effects and Order of Evaluation, 49
security vulnerability, 5
SeImpersonatePrivilege, 115
`setjmp`, 60
SHL – Uncontrolled Format String, 110
`size_t`, 22
SKL – Provision of Inherently Unsafe Operations, 90
software quality, 4
software vulnerabilities, 9
SQL
- Structured Query Language, 112

STR – Bit Representations, 14
`strcpy`, 23
`strncpy`, 23
structure type equivalence, 12
`switch`, 54
SYM – Templates and Generics, 76
symlink, 131

tail-recursion, 68
templates, 76, 77
TEX – Loop Control Variables, 57
thread, 2
TRJ – Argument Passing to Library Functions, 80
type casts, 20
type coercion, 20
type safe, 12
type secure, 12
type system, 12

UNC
- Uniform Naming Convention, 131
- Universal Naming Convention, 131

`Unchecked_Conversion`, 73
UNIX, 83, 114, 120, 131
unspecified functionality, 111
Unspecified functionality, 111
URI
- Uniform Resource Identifier, 127

URL
- Uniform Resource Locator, 127

`VirtualLock()`, 117

white-list, 120, 124, 127
Windows, 99
WPL – Improper Restriction of Excessive Authentication Attempts, 140
WXQ – Dead Store, 39, 40, 41

XSS
  Cross-site scripting, 125
XYH – Null Pointer Deference, 30
XYK – Dangling Reference to Heap, 31
XYL – Memory Leak, 74
XYM – Insufficiently Protected Credentials, 9, 133
XYN –Adherence to Least Privilege, 113
XYO – Privilege Sandbox Issues, 114
XYP – Hard-coded Password, 136
XYQ – Dead and Deactivated Code, 52
XYS – Executing or Loading Untrusted Code, 116
XYT – Cross-site Scripting, 125
XYW – Unchecked Array Copying, 27
XYZ – Unchecked Array Indexing, 25, 28
XZH – Off-by-one Error, 58
XZI – Sign Extension Error, 36
XZK – Senitive Information Uncleared Before Use, 130
XZL – Discrepancy Information Leak, 129
XZN – Missing or Inconsistent Access Control, 134
XZO – Authentication Logic Error, 135
XZP – Resource Exhaustion, 118
XZQ – Unquoted Search Path or Element, 127
XZR – Improperly Verified Signature, 128
XZS – Missing Required Cryptographic Step, 133
XZX – Memory Locking, 117

YOW – Identifier Name Reuse, 41, 44
YZS – Unused Variable, 39, 40

Section Break (Next Page)