Index

alias-locs, 50, 51  
array-descriptor domain, 59  
assignment graph, 126  
assignment operator, 107  
atexit table, 14  
buffer overrun, 4, 15  
cast  
  conversion, 110  
  copy, 110  
CCured, 27, 84, 109, 149  
\text{Checked}^\text{in}, \text{Checked}^\text{out}, 46, 142  
\text{checked-derefs}  
  EPT, 40  
  MSE, 31  
  naive, 32  
  range analysis, 76  
  redundant checks, 47  
  SLC, 94  
  write-only, 33  
chunk, malloc, 18  
classification, MSE, 31  
continuation bit, 112  
conversion cast, 110  
copy cast, 110  
\text{CopyTag}, 115  
coverage, 33  
  tracked, 80  
Cyclone, 84, 149  
data bits, 112  
demand-zero paging, 28, 95  
dereference, 24  
  checked, 31  
  definitely safe, 34  
  potentially unsafe, 34  
  unchecked, 31  
derefs, 30  
descriptor-offset domain, 60  
\text{DO} (\text{Descriptor-Offset}), 60  
\text{.dtors} table, 14  
\text{Env}, 61  
EPT (Extended Points-To) analysis, 38  
\text{Eval}, 62  
\text{exec}, 14, 94  
fat pointer, 26  
format string vulnerability, 16  
function pointers, 14
Gen/Kill, 47, 142

global offset table, 14, 19

GOT (global offset table), 14, 19

Hobbes, 109, 151

init, 112

instrumentation, MSE, 31

integer interval domain, 56

INTEGRAL, 111

intended target, 23

intersect, 69

invalid access, 23

invalid read, 23

invalid write, 23

Kill, 47, 142

Killval, Killtype, 142

LO (Location-Offset), 57

location, 123

location-offset domain, 57

locs, 30, 57, 123

locs_s, 74

locs_u, 60

longjmp buffers, 14, 94

lvalue, 47

lvalue expression, 49, 107

lvalue-affecting-locs, 50, 51

malloc chunk, 18

malloc_t, 30

may-be-uninitialized analysis

flow-insensitive, 41

flow-sensitive, 137

may-points-to analysis, 36

MayFree, 47

MayMod, 47, 138

MBU (may-be-uninitialized) analysis, 139

MBU-lite, 140

mem-unsafe expression, 123

mirror

MSE, 28

RTC, 112

MSE (Memory-Safety Enforcer), 23

narrowing/widening, 71

open array, 26, 28

open-max, 70

open-min, 70

outer, 75

outermost object, 25, 31

pointer, 112

points-to analysis, 36

popen, 14

possible-type, 128, 129

produce, 107

pt-set, 36, 50, 51

Purify, 101, 151
REAL, 111
redundant checks analysis, 46, 141
required-type, 128, 129
return address, 14
RTC (Runtime Type Checker), 101
runtime type, 108, 111
rvalue, 47
rvalue-affecting-locs, 50, 51
safe expression, 123
sensitive location, 13, 82, 90
SetTag, 115
shadow process, 149, 156
shellcode, 13
SLC (Sensitive Location Checker), 90
spatial access error, 23
stack smashing, 4, 14
STRLITi, 30
system, 14
T#, 127
lattice, 128
tag
bit value, 28, 95
runtime type, 112
valid/invalid, 28, 90
temporal access error, 23
traceroute vulnerability, 18
tracked coverage, 80
tracked location
MSE, 31
RTC, 123
SLC, 94
tracked-locs
MSE, 31
naive, 32
points-to analysis, 37
SLC, 94
type class, 112
type-unsafe expression, 123
unalloc, 109, 112
uninit, 108, 112
Uninit\textsuperscript{in}, Uninit\textsuperscript{out}, 137
unsafe location, 123
untracked location
MSE, 31
RTC, 123
use, 107
VALUE\textsubscript{r}, 127
Var, 61
VerifyDeref, 115
VerifyType\_assign, 115
VerifyType\_use, 115
widening/narrowing, 71
write-derefs, 33