Petablox Analysis Results

Petablox consists of six checkers for detecting API misuses in C/C++ programs: return value checker, argument checker, causality checker, condition checker, integer overflow checker and format string checker. We ran all checkers except for the argument checker on Drake. The checkers are fully automatic: they do not require specifying correct API usages, or even which functions constitute an API. They automatically mine semantic patterns of API usage across a large codebase like Drake, perform statistical analysis of these patterns, and report infrequent patterns as potential API misuses.

### Return Value Checker

The return value checker semantically analyzes return value checks across different calls to each function and reports unusual ones as potential bugs. For instance, if at least 70% of all calls to the malloc() function check that the return value is non-null, then any of the remaining calls to the malloc() function that do not check for non-nullness are reported.

|  |  |
| --- | --- |
| **Location** | **Description** |
| drake/multibody/parsers/urdf\_parser.cc:1295,  key=Attribute, ctx=((0, 0),) | Should do the null check after return;  this would be a bug if the string constructor cannot initialize with null pointer properly. |
| externals/libbot/bot2-lcm-utils/src/tunnel/introspect.c:107, key=lcm\_subscribe, ctx=((0, 0) | New function should check if subscription fails and do something if it does. |
| externals/libbot/bot2-frames/src/renderer/frame\_modifier\_renderer.c:132, key=fopen, ctx=((0, 0),) | Not sure if this is a genuine bug, but file may not exist. However we create the string that represents the file name, so we may have a guarantee that the file exists. |
| externals/ipopt/ThirdParty/Metis/metis-4.0/Lib/sfm.c:352, key=\_\_PQueueGetMax, ctx=((-2147483648, -2), (0, 2147483647)) | Queue might be empty and should be checked for -1. (Though, the surrounding code might ensure the queue is nonempty) |
| externals/ipopt/ThirdParty/Metis/metis-4.0/Lib/sfm.c:115, key=\_\_PQueueGetMax, ctx=((-2147483648, -2), (0, 2147483647)) | Queue might be empty and should be checked for -1. (Though, the surrounding code might ensure the queue is nonempty) |
| externals/libbot/bot2-lcmgl/src/bot\_lcmgl\_render/lcmgl\_bot\_renderer.c:122, key=g\_hash\_table\_lookup, ctx=((0, 0) | As far as I can tell, the hash table lookup needs to be checked to see if the key is in the table |
| externals/libbot/bot2-lcmgl/src/bot\_lcmgl\_render/lcmgl\_bot\_renderer.c:122, key=g\_hash\_table\_lookup, ctx=((0, 0), | Same as above |
| externals/libbot/bot2-vis/src/bot\_vis/param\_widget.c:166, key=g\_hash\_table\_lookup, ctx=((0, 0), | Same as above |
| externals/libbot/bot2-lcmgl/src/bot\_lcmgl\_render/lcmgl\_bot\_renderer.c:46 | Same as above |
| externals/libbot/bot2-vis/src/bot\_vis/param\_widget.c:76, key=g\_hash\_table\_lookup, ctx=((0, 0), | This is a bug for the same reason as above, depending on whether GNOME does null checks on things passed to its APIs |
| externals/libbot/bot2-procman/src/deputy/procman.c:100, key=getenv, ctx=((0, 0) | Result of getenv should be checked for NULL (though PATH almost certainly exists….) |
| externals/libbot/bot2-vis/src/bot\_vis/viewer.c:352, key=fwrite, ctx=((1, 1) | Result of write not checked for success (so preferences may not be successfully saved) |