CS3281 FINAL PROJECT HIGHLIGHT

SAFE PROGRAMMING TOOL

BUGS DESCRIPTION

Memory Leak	A memory leak usually occurs when a computer program do not release the memory which is not needed anymore.
Dangling Pointer	A dangling pointer is a pointer which does not point to a valid object of the appropriate type.
Access to unauthorized memory memory	Access to unauthorized memory means a pointer try to access the memory which is not authorized by the program.
Concurrency errors	A concurrency error occurs due to the incorrect synchronization safeguards in multi-threaded program.
Deadlock	Deadlock is one kind of concurrency error. It occurs when two or more processes are never able to process because each is waiting for the others to do something.
Race condition	A race condition is another kind of concurrency error. It occurs when concurrent accesses to a shared variable and at least one of the access is a write.

GARBAGE COLLECTION APPROACH VS C/C++ STYLE MEMORY MANAGEMENT APPROACH

Garbage Collection Approach	Garbage collector is an automatic memory management. It attempts to reclaim memory occupied by the objects which are no longer needed. **1. Do not need programmer to manage memoery.**
C/C++ Style Memory Management Approach	Programmer needs to check memory management manually. **1. It does not have overhead since the program does not need extra memory and time to check memory leak.** **2. It can process all kinds of memory leak.**

TOOLS DESCRIPTION

Electric Fence	Electric fence is a memory error detector, which mainly helps to detects two common bugs: 1. access to unauthorized memory 2. dangling pointer (both are described above)
Memcheck from Valgrind	Memcheck is another memory debugger, it can detect the following problems that are common in the C and C++ program: 1. Access memory you shouldn't 2. Use undefined values 3. Incorrect free of heap memory 4. Overlap src and dst pointers in memcpy and related functions. 5. Pass a fishy (presumably negative) value to the size parameter of a memory allocation function 6. Memory leaks
Helgrind from Valgrind	Helgrind is also a Valgrind tool which is for detecting synchronization errors in C, C++ and Fortran programs that use POSIX pthreads thriving primitives. Helgrind can detect three kinds of errors. 1. Misuses of the POSIX pthread API 2. Potential deadlocks arising from ordering problem 3. Data race conditions

TOOLS USAGE SAMPLE

Electric Fence

```
File  Edit  View  Terminal  Tabs  Help
vagrant@Xubuntu-Vagrant:~$ cd /home/vagrant/ClionProjects/project3-examples/src
vagrant@Xubuntu-Vagrant:~/ClionProjects/project3-examples/src$ gcc -g unauthoriz
ed_access.c -o unauthorized_access -lefence
vagrant@Xubuntu-Vagrant:~/ClionProjects/project3-examples/src$ gdb unauthorized_
access
GNU gdb (Ubuntu 7.11-0ubuntu1) 7.11
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from unauthorized_access...done.
(gdb) run
Starting program: /home/vagrant/ClionProjects/project3-examples/src/unauthorized
_access
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

  Electric Fence 2.2 Copyright (C) 1987-1999 Bruce Perens <bruce@perens.com>

Program received signal SIGSEGV, Segmentation fault.
0x00000000004006b7 in main () at unauthorized_access.c:8
8           strcpy(ar,"amee is my name");
(gdb) where
#0  0x00000000004006b7 in main () at unauthorized_access.c:8
```

Memcheck

```
Terminal - vagrant@Xubuntu-Vagrant: ~/ClionProjects/project3-examples/src
File  Edit  View  Terminal  Tabs  Help
vagrant@Xubuntu-Vagrant:~/ClionProjects/project3-examples/src$ gcc -g memory_lea
k.c -o memory_leak
vagrant@Xubuntu-Vagrant:~/ClionProjects/project3-examples/src$ valgrind --tool=m
emcheck ./memory_leak
==25491== Memcheck, a memory error detector
==25491== Copyright (C) 2002-2015, and GNU GPL'd, by Julian Seward et al.
==25491== Using Valgrind-3.11.0 and LibVEX; rerun with -h for copyright info
==25491== Command: ./memory_leak
==25491==
==25491==
==25491== HEAP SUMMARY:
==25491==     in use at exit: 4 bytes in 1 blocks
==25491==   total heap usage: 1 allocs, 0 frees, 4 bytes allocated
==25491==
==25491== LEAK SUMMARY:
==25491==    definitely lost: 4 bytes in 1 blocks
==25491==    indirectly lost: 0 bytes in 0 blocks
==25491==      possibly lost: 0 bytes in 0 blocks
==25491==    still reachable: 0 bytes in 0 blocks
==25491==         suppressed: 0 bytes in 0 blocks
==25491== Rerun with --leak-check=full to see details of leaked memory
==25491==
==25491== For counts of detected and suppressed errors, rerun with: -v
==25491== ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)
vagrant@Xubuntu-Vagrant:~/ClionProjects/project3-examples/src$
```

Helgrind

```
Terminal - vagrant@Xubuntu-Vagrant: ~/ClionProjects/project3-examples/src
File  Edit  View  Terminal  Tabs  Help
vagrant@Xubuntu-Vagrant:~/ClionProjects/project3-examples/src$ valgrind --tool=helgrind ./ra
ce_condition
==25838== Helgrind, a thread error detector
==25838== Copyright (C) 2007-2015, and GNU GPL'd, by OpenWorks LLP et al.
==25838== Using Valgrind-3.11.0 and LibVEX; rerun with -h for copyright info
==25838== Command: ./race_condition
==25838==
==25838== ---Thread-Announcement------------------------------------------
==25838==
==25838== Thread #1 is the program's root thread
==25838==
==25838== ---Thread-Announcement------------------------------------------
==25838==
==25838== Thread #2 was created
==25838==    at 0x5163B1E: clone (clone.S:74)
==25838==    by 0x4E46189: create_thread (createthread.c:102)
==25838==    by 0x4E47EC3: pthread_create@@GLIBC_2.2.5 (pthread_create.c:679)
==25838==    by 0x4C34BB7: ??? (in /usr/lib/valgrind/vgpreload_helgrind-amd64-linux.so)
==25838==    by 0x400705: main (in /home/vagrant/ClionProjects/project3-examples/src/race_co
ndition)
==25838==
==25838== ----------------------------------------------------------------
==25838==
==25838== Possible data race during read of size 4 at 0x60104C by thread #1
==25838== Locks held: none
==25838==    at 0x400706: main (in /home/vagrant/ClionProjects/project3-examples/src/race_co
ndition)
==25838==
==25838== This conflicts with a previous write of size 4 by thread #2
==25838== Locks held: none
==25838==    at 0x4006C7: child_fn (in /home/vagrant/ClionProjects/project3-examples/src/rac
e_condition)
==25838==    by 0x4C34DB5: ??? (in /usr/lib/valgrind/vgpreload_helgrind-amd64-linux.so)
==25838==    by 0x4E476F9: start_thread (pthread_create.c:333)
==25838==  Address 0x60104c is 0 bytes inside data symbol "var"
==25838==
==25838== ----------------------------------------------------------------
==25838==
==25838== Possible data race during write of size 4 at 0x60104C by thread #1
==25838== Locks held: none
==25838==    at 0x40070F: main (in /home/vagrant/ClionProjects/project3-examples/src/race_co
ndition)
==25838==
==25838== This conflicts with a previous write of size 4 by thread #2
==25838== Locks held: none
==25838==    at 0x4006C7: child_fn (in /home/vagrant/ClionProjects/project3-examples/src/rac
e_condition)
==25838==    by 0x4C34DB5: ??? (in /usr/lib/valgrind/vgpreload_helgrind-amd64-linux.so)
==25838==    by 0x4E476F9: start_thread (pthread_create.c:333)
==25838==  Address 0x60104c is 0 bytes inside data symbol "var"
==25838==
==25838==
==25838== For counts of detected and suppressed errors, rerun with: -v
==25838== Use --history-level=approx or =none to gain increased speed, at
==25838== the cost of reduced accuracy of conflicting-access information
==25838== ERROR SUMMARY: 2 errors from 2 contexts (suppressed: 0 from 0)
vagrant@Xubuntu-Vagrant:~/ClionProjects/project3-examples/src$
```