codius-sandbox Documentation

Release 0.1.0

The Codius Team

January 10, 2015

Contents

Codius Sandbox is a small C++ library and node module that uses seccomp to execute untrusted code in a secure sandbox, in the same vein of User Mode Linux, Native Client, and others.

CHAPTER 1

Dependencies

- cppunit
- libuv
- libseccomp
- A compiler that supports C++11, such as GCC 4.8 or Clang.

On Ubuntu, these can be installed with:

```
`apt-get install libuv-dev libseccomp-dev libcppunit-dev`
```

CHAPTER 2

Documentation

Full documentation of codius-sandbox is available on Read The Docs:

http://codius-sandbox.readthedocs.org/

Contents:

2.1 C++ API

2.1.1 The `Sandbox` class

Warning: doxygenclass: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

2.1.2 The `SandboxIPC` class

Warning: doxygenclass: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

2.1.3 The `CallbackIPC` class

Warning: doxygenclass: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

2.1.4 The `VFS` class

Warning: doxygenclass: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

2.1.5 The `Filesystem` class

Warning: doxygenclass: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

2.1.6 The `NativeFilesystem` class

Warning: doxygenclass: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

2.2 Node.js API

2.2.1 The `Sandbox` class

class `Sandbox`()
Construct a new sandbox

`Sandbox.`**`mapFilename`**(*filename*)

Arguments

- **filename** (*string*) – Filename to map

Called when a filename used in open(), stat(), etc should be mapped from a real filename to one within the sandbox's environment.

Should return a string, which is the new filename that will be passed to the underlying syscall.

`Sandbox.`**`onIPC`**(*api_name*, *method_name*, *arguments*, *cookie*)

Arguments

- **api_name** (*string*) – API being called
- **method_name** (*string*) – Method being called
- **arguments** (*object*) – Arguments for the API call
- **cookie** (*object*) – An opaque cookie that must be later passed to Sandbox.finishIPC()

Do not touch the cookie or Very Bad Things could happen including, but not limited to: war, pestilance, spoilage of all the cheese in your home, a strong desire to port Emacs to Node.js.

`Sandbox.`**`onVFS`**(*cookie*, *op*[, ...])

Arguments

- **cookie** (*object*) – An opaque cookie that must be later passed to

Sandbox.finishVFS() :param string op: Method being called

Called when a VFS operation occurs.

Do not touch the cookie. Seriously.

`Sandbox.`**`finishIPC`**(*cookie*, *result*)

Arguments

- **cookie** (*object*) – The opaque cookie from Sandbox.onIPC() that was not

touched. :param object result: API result that is passed to the sandbox

Result should be a structure in the form of:

```
{
  'success': true,
  'result': {foo: {bar: 'baz'}}
}
```

`Sandbox.`**`_init`**`()`
Internal function. Sets up stdio IPC channels upon construction

`Sandbox.`**`onData`**`(`*fd*, *chunk*`)`

Arguments

- **fd** (*number*) – File descriptor inside the sandbox
- **chunk** (*string*) – Data read from the sandbox

Internal function. Called when data from within the sandbox is ready for reading.

`Sandbox.`**`spawn`**`(`*arg0, [...,] [options]*`)`

Arguments

- **arg0** – First argument
- **...** – Further arguments
- **options** – A structure of options

Spawns a binary inside the sandbox

`Sandbox.`**`kill`**`()`
Kills the child process

Attributes

`Sandbox.`**`stdout`**

Type Readable stdio channel that maps to stdout

`Sandbox.`**`stderr`**

Type Readable stdio channel that maps to stderr

`Sandbox.`**`stdio`**

Type Array stdio channels

`Sandbox.`**`debuggerOnCrash`**

Type boolean Launch GDB when the child crashes

Events

`Sandbox.`**`newSocket`**`()`

Arguments

- **path** (*string*) – Path to the unix socket

Emitted when the sandboxed child has called bind() on a socket, which is now mapped to a unix domain socket.

`Sandbox.exit()`

Arguments

- **status** (*number*) – Exit status

Emitted when the sandboxed child has exited

`Sandbox.signal()`

Arguments

- **signal** (*number*) – Signal received

Emitted when the sandboxed child has received a signal

2.3 Codius RPC API

2.3.1 Requests

codius_request_s

Warning: doxygenstruct: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

Warning: doxygenfunction: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

Warning: doxygenfunction: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

Warning: doxygenfunction: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

Warning: doxygenfunction: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

Warning: doxygenfunction: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

Warning: doxygenfunction: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

Warning: doxygenfunction: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

2.3.2 Results

codius_result_s

Warning: doxygenstruct: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

Warning: doxygenfunction: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

Warning: doxygenfunction: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

Warning: doxygenfunction: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

Warning: doxygenfunction: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

Warning: doxygenfunction: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

Warning: doxygenfunction: Cannot find file: /var/build/user_builds/codius-sandbox/checkouts/latest/build/doc/doxygen/xml/index.xml

2.4 Implemented Syscalls

Codius-sandbox handles a number of syscalls that sandboxed processes have access to. Any unhandled syscall results in an instantaneous SIGKILL.

The following syscalls interact with the VFS layer, and their behavior is dependent on any virtual filesystems that are mounted:

- open
- access
- openat
- stat
- read
- close
- ioctl
- fstat
- lstat
- lseek

- write
- getdents
- getdents64
- readdir
- readv
- writev
- getcwd
- fcntl
- chdir
- fchdir
- readlink

Networking emulation layer:

- socket
- connect
- bind
- setsockopt
- getsockname
- getpeername
- getsockopt

Queries about the sandbox system:

- uname
- getrlimit
- getuid
- getgid
- geteuid
- getegid
- getppid
- getpgrp
- getgroups
- getresuid
- getresgid
- capget
- gettid

The following syscalls pass through the sandbox directly to the kernel:

- clone
- fsync

- fdatasync
- sync
- poll
- mmap
- mprotect
- munmap
- madvise
- brk
- rt_sigaction
- rt_sigprocmask
- select
- sched_yield
- getpid
- accept
- listen
- exit
- gettimeofday
- tkill
- epoll_create
- restart_syscall
- clock_gettime
- clock_getres
- clock_nanosleep
- exit_group
- epoll_wait
- epoll_ctl
- tgkill
- pselect6
- ppoll
- arch_prctl
- prctl
- set_robust_list
- get_robust_list
- epoll_pwait
- accept4
- epoll_create1

- pipe2
- futex
- set_tid_address
- set_thread_area

CHAPTER 3

Indices and tables

- *genindex*
- *search*

S