

Песочница для безопасного запуска бинарных программ

Назначение

- Запуск бинарных программ, полученных из недоверенного источника, с ограниченными возможностями программы по доступу к ресурсам компьютерной системы

Функциональность

- Ограничение времени выполнения и объема виртуального адресного пространства процесса
- Передача аргументов командной строки и фильтрация переменных окружения
- Ограниченный и конфигурируемый доступ к файловой системе (только текущий каталог, текущий и ограниченное множество других каталогов и т. п.)

Функциональность

- Поддержка создания процессов или нитей в недоверенном процессе с сохранением всех ограничений на созданные процессы (нити)
- Конфигурация ограничений с помощью конфигурационного файла.

Инструментарий

- Язык программирования — C++ или C
- Система сборки — make
- Контроль версий — github
- Библиотека терминального ввода-вывода
ncurses