

Guardant[®]

Система защиты от компьютерного пиратства

Guardant **для GNU/Linux**

© 2009 Компания Актив

Современные ключи Guardant, начиная с Guardant Sign, позволяют защищать приложения, запускаемые в ОС GNU/Linux на аппаратных платформах i386 и x86_64. Для этого в комплект разработчика включены статические библиотеки (ELF) — **libgrdapi.a**, соответствующей разрядности, которые реализуют Guardant API.

Кроме того, поддерживается запуск защищенных Windows-приложений с использованием Wine (www.winehq.org) - свободной реализации Windows API. Для этого в комплект разработчика включен проект динамической библиотеки для Wine — **GrdWine**, распространяемый под свободной лицензией GNU Lesser General Public License version 2.1 (поставляется в виде пакета с исходными кодами — **grdwine-0.5.4.tar.gz**).

Ключи работают в ОС GNU/Linux (в том числе, в HID-режима) без установки дополнительных драйверов и демонов, требуя лишь обеспечить имя и разрешение доступа к файлу устройства. Для обращения к ключу используются соответственно Linux USB Device Filesystem или Linux USB HID Device Interface (в случае HID-режима). В комплект разработчика включены наборы правил для систем регистрации устройств и описание требований для случаев нетипичного конфигурирования.

Подготовка к работе с ключами Guardant

Новые модели ключей Guardant, начиная с Guardant Time/Sign, поддерживают работу в среде Linux, в том числе в HID-режиме.

Также поддерживается работа защищенных Windows-приложений под Wine.

Для работы с ключами в ОС GNU/Linux необходимо добавить правило для штатного средства обработки **HotPlugging**. На большинстве современных дистрибутивов, использующих ядро 2.6.x, таким средством является **udev** (<http://kernel.org/pub/linux/utils/kernel/hotplug/udev.html>).

Правило для **udev** добавляется следующим образом:

```
# cp grdnt.udev /etc/udev/rules.d/XX-grdnt.rules
```

Для записи в каталог **/etc/udev/rules.d** потребуются права суперпользователя.

Указанное правило предписывает **udev** установить права на чтение и запись для файла-устройства, представляющего электронный ключ Guardant в системе. Это позволит обращаться к ключу с привилегиями любого пользователя системы.

Защита Native-приложений GNU/Linux

Для сборки защищаемого приложения, необходимо скомпоновать (слинковать) защищаемое приложение со статической библиотекой Guardant API.

Рекомендуется использовать компилятор GCC 4-ой версии, однако, возможно использовать и более ранние версии GCC, и другие компиляторы, например, Intel C++ Compiler (ICC).

Для компиляции с библиотекой Guardant API необходимо выполнить следующее (на примере файла с исходным текстом программы — foobar.c):

```
$ gcc [-I<путь_к_заголовочному_файлу_GrdAPI.h>] -c foobar.c -o foobar.o
$ gcc [-L<путь_к_библиотеке_libgrdapi.a>] foobar.o -o foobar -lpthread
-lgrdapi
```

или

```
$ gcc [-I<путь_к_заголовочному_файлу_GrdAPI.h>]
[-L<путь_к_библиотеке_libgrdapi.a>] foobar.c -o foobar -lgrdapi -lpthread
```

Обратите внимание, что библиотека Guardant API использует библиотеку **pthread** - POSIX Threads, поэтому для компоновки приложений необходимо использовать соответствующую библиотеку.

Подсоедините ключ Guardant к USB-порту компьютера, защищенное приложение готово к работе.

Запуск защищенных Windows-приложений под Wine

Библиотека **grdwine.dll.so**, реализующая работу с ключами Guardant для защищенных Windows-приложений под Wine, поставляется в виде исходных кодов (см. **grdwine-0.5.4.tar.gz**). Это, в принципе, позволяет ее использовать с любой версией Wine, достаточно просто собрать библиотеку из исходных кодов.

Важная информация

Рекомендуемая к использованию версия Wine — 1.x.x. Корректная работа с ранними версиями Wine не гарантируется. Загрузить последнюю версию Wine можно по адресу: <http://www.winehq.org/site/download>

Компиляция библиотеки

```
$ tar xvf grdwine-0.5.4.tar.gz
$ cd grdwine-0.5.4
$ ./configure --with-wineincs=/usr/include/wine
--with-winedlls=/usr/lib/wine
$ make
# make install
```

Важная информация

Указанные пути к заголовочным файлам и библиотекам Wine (**/usr/include/wine** и **/usr/lib/wine**) являются могут меняться в зависимости от версии Wine, используемого дистрибутива или заданного префикса для установки (в случае, если Wine устанавливался из исходных кодов)

Подсоедините ключ Guardant к USB-порту компьютера, защищенное приложение готово к работе.

Удаление библиотеки из системы

```
$ cd grdwine-0.5.4
# make uninstall
```

Имена и доступ к устройствам

Для ключей, работающих в драйверном режиме

Обращение к ключу происходит через Linux USB Device Filesystem.

Подробную информацию см. в `linux/Documentation/usb/proc_usb_info.txt`.

Для успешной работы с ключом в системе нужно разрешить доступ на чтение/запись к файлу устройства.

Для ключей, работающих в HID-режиме

Обращение к ключу происходит через Linux USB HID Device Interface (драйвер `usbhid`).
Подробную информацию см. в `linux/Documentation/usb/hiddev.txt`.

Для успешной работы с ключом в системе нужно изменить имена соответствующих устройств на `/dev/grdnt[N#]` и разрешить доступ на чтение/запись к файлу устройства.

Для hotplug или hotplug-ng

```
# cp etc/grdnt.usermap /etc/hotplug/usb/grdnt.usermap
# cp etc/grdnt /etc/hotplug/usb/grdnt
```

Для udev

Для ключей в драйверном режиме,
и в случае использования файлов-устройств USB Device Filesystem)

```
# cp etc/grdnt.udev /etc/udev/rules.d/95-grdnt.rules
```

Ключи, работающие в HID-режиме

```
# cp etc/grdnt_hid.udev /etc/udev/rules.d/95-grdnt_hid.rules
```

Переменные окружения

Для настройки Guardant API под GNU/Linux следует пользоваться следующими переменными окружения:

GRD_IPC_NAME	директория, в которой процессы будут создавать/открывать для чтения и записи файлы, используемые для синхронизации доступа к ключу. Если переменная не задана, используется значение по умолчанию (<code>/tmp</code>)
USB_DEVFS_PATH	директория Linux USB Device Filesystem (точка монтирования или директория, содержащая дерево соответствующих устройств). Если переменная не задана, будет использоваться <code>/dev/bus/usb</code> (если существует), иначе – <code>/proc/bus/usb</code>

Дополнительные источники информации

При возникновении вопросов, на которые вам не удалось найти ответа в этой инструкции, рекомендуем обратиться к следующим дополнительным источникам информации:

Сайт: <http://www.guardant.ru>

Web-сайт разработчика содержит большой объем справочной информации об электронных ключах Guardant.

Служба технической поддержки:

e-mail: hotline@guardant.ru

тел. +7(495)925-77-90