# Лекция 2. Защита программ от нелегального копирования

Все ломали и ломаем. Как защищать программы?

## Методы защиты

|  |  |  |  |
| --- | --- | --- | --- |
|  | Активные | Пассивные | |
| 1. По методу реализации | | |
| внутренняя самозащита |  | пароль на запуск | |
|  | ограничение времени использования/ ограничение по дате | |
|  | идентификация и аутентификация | |
|  | искажение программы (нарушение штатного функционала) | |
| вирусы (деструктивное действие) |  | |
| идентификация |  | вывод сведений о владельце ПО | |
|  | метка Copyright (авторское право) | |
|  | водяные знаки на документации/ голографические метки на упаковке | |
| предупредительные сообщения (любые сигналы) |  | |
|  | частотный, корреляционный анализ системы/ пользователей | |
| избыточность, внедренные ошибки |  | |
|  | отличительные метки (остатки отладочных процедур) | |
| информационные средства |  | регистрация в официальном регистре программных средств (*Российское агентство по правовой охране программ для ЭВМ, баз данных и топологий интегральных схем при Роспатенте (Федеральном агентстве Российской Федерации по патентам и товарным знакам)*) | |
| внешний контроль лицензий |  | централизоыванный контроль при каждом запуске на сервере лицензий |
| 1. Защита отдельных составляющих в составе системы | | |
| защита носителей информации |  | изменение формата записи | |
|  | специальные методы разметки (нестандартные размеры сектора) | |
|  | уникальные метки (дырка на дискете) | |
| специальная аппаратура |  | специальное HW (например, процессор - на других не заработает) | |
|  | серийные номера устройств | |
|  | аппаратная защита от считывания (закрытых ключей на token, …) | |
|  | электронные ключи (HASP,…) | |
| изменение функций |  | переустановка прерываний | |
|  | переименование устройства | |
| 1. Защита с запросом ключевой информации | | |
| запрос кода |  | пароль | |
|  | персональные данные | |
|  | одноразовый код | |
| шифрование |  | симметричное | |
|  | асимметричное | |
| проверка сигнатур |  | характеристики компьютера (аппаратные, программные) | |
|  | файл в рабочем каталоге | |
|  | записи в реестре | |
|  | уникальный номер электронного ключа | |
| защита от автоматизированного взлома |  | capcha (все цифры, где видишь горы и др.) | |
|  | мониторинг аномально быстрых повторов/ ограничение числа попыток | |
| 1. Собственная защита программного обеспечения | | |
|  |  | обфускация кода (obfuscate-запутывать, сбивать с толку) | |
|  |  | услуги по сопровождению | |
|  |  | заказное проектирование под ключ (вместе с железом) | |

## Схема защиты программы

Internet

Инсталлятор

Программное обеспечение

Образ дистрибутива с процедурой проверки носителя

Программа с идентификатором компьютера

## Определение характеристик компьютера

Виды параметров:

- изменяемые

- постоянные (аппаратные)

Критерии выбора параметров:

- уникальность

- неизменняемость

- стабильность

- доступность

## Получение значений параметров системы

Способы получения:

0) Низкоуровневые обращения к устройствам (на ASM)

Трудоемко, нестабильно, зависит от версий ПО и железа

1) Windows API

GetWindowsDirectory, GetComputerName, GetVolumeInformation, GlobalMemoryStatus, GetDiskFreeSpace, GetSystemInfo (число и тип процессора), GetFileTime (время создания файла), GetSystemTime (текущее время системы), GetCurrentHWProfile ({GUID})

2)Windows Management Instrumentation (универсальный объектно-ориентированный интерфейс мониторинга и управления компонентами Windows)

-- обращения через язык запросов WMI Query Language (WQL) (отличие от ANSI SQL в невозможности изменения данных) для выборки данных с помощью команды SELECT

Пример 1. Запрос информации о процессоре.

Select \* From **Win32\_BIOS**

Пример 2. Запрос информации обо всем.

Select \* From **Meta\_Class** Where \_\_Class = **"Win32\_LogicalDisk"**

Win32\_Processor

Win32\_BIOS

Win32\_DiskDrive

Win32\_LogicalDisk

MSFT\_NetAdapter

Утилита командной строки **wmic**: wmic csproduct get name

3) команды Linux

- hddtemp (температура винчестера)

- lsdev (список установленного железа)

- lshal (список устройств HAL (Hardware Abstraction Level - предназначен для сокрытия различий в аппаратном обеспечении от основной части ядра операционной системы))

Вызов:

$ lshal | less

Дает вывод:

scsi.model = 'SAMSUNG HD501LJ' (string)

udi = '/org/freedesktop/Hal/devices/storage\_serial\_SATA\_SAMSUNG\_HD501LJS0MUJ1EPB12062'

block.storage\_device = '/org/freedesktop/Hal/devices/storage\_serial\_SATA\_SAMSUNG\_HD501LJS0MUJ1EPB12062' (string)

info.product = 'SAMSUNG HD501LJ' (string)

info.udi = '/org/freedesktop/Hal/devices/storage\_serial\_SATA\_SAMSUNG\_HD501LJS0MUJ1EPB12062' (string)

storage.model = 'SAMSUNG HD501LJ' (string)

storage.serial = 'SATA\_SAMSUNG\_HD501LJS0MUJ1EPB12062' (string)

Короткий вывод:

$ lshal –s

lspci, lsusb, lsscsi, lshw

**Виртуальная файловая система PROC FS**

- сведения о системе (информация о подключённых устройствах)

- интерфейс управления параметрами ядра (от заряда батарей до скорости вентиляторов)

**ls /proc/ -** выведет список файлов с информацией о состоянии системы:

(i) cat – объединить текст файлов

Пример 1 (процессор):

**cat /proc/cpuinfo**

*processor : 0*

*vendor\_id : AuthenticAMD*

*cpu family : 16*

*model : 6*

*model name : AMD Athlon(tm) II X2 250 Processor*

*stepping : 3*

*microcode : 0x10000c8*

*cpu MHz : 3000.000*

*cache size : 1024 KB*

*physical id : 0*

*siblings : 2*

Пример 2 (логические диски):

**cat /proc/diskstats**

*8 0 sda 382 0 58066 153 7 1 64 10 0 115 163*

*8 1 sda1 346 0 54186 137 7 1 64 10 0 107 147*

*8 32 sdc 2175 0 113696 522 0 0 0 0 0 341 522*

*8 16 sdb 25408 59 1027142 17383 52375 27629 1263624 58618 0 31310 75953*

*11 0 sr0 0 0 0 0 0 0 0 0 0 0 0*

*253 0 dm-0 12591 0 424914 9118 37442 0 453208 39155 0 13609 48273*

*253 1 dm-1 127 0 6472 24 0 0 0 0 0 18 24*

*253 2 dm-2 212 0 7346 47 256 0 2232 219 0 76 266*

*253 3 dm-3 12504 0 585274 8429 42306 0 808184 47543 0 18254 55972*

**cat /proc/partitions**

*major minor #blocks name*

*8 0 1048576 sda*

*8 1 1047552 sda1*

*8 32 31457280 sdc*

*8 16 25165824 sdb*

*11 0 1048575 sr0*

*253 0 8388608 dm-0*

*253 1 4194304 dm-1*

*253 2 4194304 dm-2*

*253 3 8384512 dm-3*

**UDEV**

udevadm info -- query=property

udevadm info -- name=/dev/sda

**MACHINE\_ID**

cat /var/lib/dbus/machne\_id

в MacOS (BSD от FreeBSD) называется Darwin

**SYSCTL** (в BSD и Linux)

Чтение/изменение параметров ядра (на лету) - например: размер сегмента разделяемой памяти, ограничение числа запущенных процессов.

Параметры переопределяются в конфигурационном файле **/etc/sysctl.conf.**

Пример 1 (процессор):

**sysctl hw**

Пример 2 (сетевая карта):

sysctl -w net.ipv4.ip\_forward=1 // включает режим маршрутизатора

(i) аналогично записи в файл /proc/sys/net/ipv4/ip\_forward значения «1».

**IOREG**

Реестр устройств ввода (I/O Kit registry)

**ioreg -l | grep SerialNumber**

**SYSTEM\_PROFILER**

system\_profiler SPHardwareDataType | grep “SerialNumber”

*-------------------------------------------45 минут------------------------------------------------------------*