Накопители со встроенной защитой данных (ATA Security и FDE /SED TCG OPAL)

В данной статье рассматривается использование аппаратной защиты данных на накопителях, "дисков с самошифрованием" и связанные с этим вопросы идентификации пользователей для предоставления доступа к данным.

Описанные в данной статье решения не являются сертифицированными решениями для защиты конфиденциальных данных, подвержены уязвимостям и могут обладать недокументированными возможностями, позволяющими получать несанкционированный доступ к данным.

Чтобы не вводить читателей в заблуждение, в данной статье по возможности не употребляется термин "шифрование", а если исключить этот термин не представляется возможным, то употребляется исключительно в смысле "защитное преобразование данных".

Данная статья применима к:

- ОС ОН Орёл 2.12
- ОС СН Смоленск 1.6
- ОС СН Смоленск 1.5
- ОС СН Ленинград 8.1 (в части ATA Security)

Так как носители автоматически блокируются при отключении электропитания, рассматриваемые в данной статье технологии защиты данных несовместимы с режимами пониженного энергопотребления компьютеров, при которых сохраняется содержимое (электропитание) оперативной (энергозависимой) памяти, но обесточиваются подключенные накопители (режимы S1, S2, S3 («Suspend to RAM» (STR) в BIOS, «Ждущий режим» («Standby»)), так как при выходе системы из режима пониженного энергопотребления данные на накопителях окажутся заблокированными. При использовании рассматриваемых технологий защиты режимы данных эти пониженного энергопотребления следует отключить, однако можно использовать режим S4 («Suspend to disk» (STD)), так как в этом режиме содержимое оперативной памяти сохраняется на накопителе, и может быть восстановлено с него после разблокировки.

Накопители данных с "самошифрованием"

Аппаратное защитное преобразование данных на накопителях данных ("самошифруемый диск", в английской литературе применяются термины Full-Drive Encription (FDE) или Self-Encrypting Drive (SED), являющиеся синонимами) предоставляется сейчас многими производителями накопителей данных, и позиционируется как общее решение для защиты данных от несанкционированного доступа, в том числе и данных, хранящихся на твердотельных накопителях. В таких устройствах защитное преобразование данных выполняется специализированными встроенными в контроллер устройства микросхемами "на лету", и все данные на устройстве хранятся преобразованном виде.
Декларируются следующие возможности таких устройств:

- использование алгоритмов преобразования AES 128 бит / AES 256 бит;
- невозможность извлечение ключей защитного преобразования из устройства;
- возможность мгновенного "удаления" всех хранящихся данных простой заменой внутреннего ключа защитного преобразования, после чего все данные становятся не подлежащими восстановлению;

Наличие всех или некоторых их этих возможностей зависит от производителя и конкретной модели, технические детали обычно не раскрываются, сертификация и проверка недокументированных возможностей не проводится.

Основные методы защиты данных

Для разграничения доступа к данным, хранящимся накопителях, требуется использовать механизмы идентификации пользователей. Для этого применяются два основных решения:

- ATA Security - встроенная блокировка/деблокировка накопителя с помощью задаваемого пользователем пароля, передаваемого через команды интерфейса ATA.
  Этот метод широко распространён, поддерживается большинством накопителей, и никак не привязан к наличию или отсутствию в накопителе встроенного преобразования данных;

- TCG OPAL - решение, предусматривающее установку на накопитель специального ПО, обеспечивающего инициализацию и настройку параметров безопасности, и, далее, при каждом включении устройства, обеспечивающего идентификацию пользователя и разблокировку устройства. При этом доступ защищается паролем, а накопитель после включения и до ввода пароля предоставляет в качестве своего содержимого не реально хранимые данные, а специальный "теневой" (shadow) загрузочный раздел, обеспечивающий загрузку ПО авторизации и перезапуск системы уже с разблокированным реальным содержимым накопителя. При этом спецификации OPAL включают в себя и требования к защитному преобразованию данных, хранящихся в накопителе.

Описанные ниже способы защиты данных ATA Security и TCG OPAL включаются при обесточивании накопителя. Следует помнить, что, данные, находящиеся на включенном накопителе после разблокировки ничем не защищены пока накопитель включён, а физическая реализация разъёмов SATA (отдельный кабель питания и отдельный кабель данных) при наличии физического доступа к оборудованию предоставляет удобную возможность переподключить накопитель к другой шине данных не отключая его электропитание, и, таким образом, получить полный доступ к данным. Для предотвращения возможности такого рода атак следует обеспечить принудительное полное обесточивание накопителей при вскрытии корпуса.

ATA Security

Режим защиты данных ATA Security не является сертифицированным решением защиты данных.

Установка ПО и проверка соответствия оборудования

Для проверки параметров накопителя выполняется инструментом командной строки hdparm, входящим в пакет hdparm. Пакет доступен в дистрибутиве /репозитории ОС ОН Орёл 2.12 и в дистрибутивах ОС СН Смоленск 1.6 и ОС СН Ленинград 8.1.
Установить пакет можно их графического менеджера пакетов или из командной строки

```
sudo apt install hdparm
```

Подробные параметры накопителя выводятся командой (пример для накопителя /dev/sda):

```
sudo hdparm -I /dev/sda
```

Пример полного вывода команды:

```
$ sudo hdparm -I /dev/sda

/dev/sda:

ATA device, with non-removable media
        Model Number: TOSHIBA HDWD110
        Serial Number: X7HW1XWFS
        Firmware Revision: MS2OA8J0
        Transport: Serial, ATA8-AST, SATA 1.0a, SATA II Extensions, SATA Rev 2.5, SATA Rev 2.6, SATA Rev
3.0; Revision: ATA8-AST T13 Project D1697 Revision 0b
Standards:
        Used: unknown (minor revision code 0x0029)
        Supported: 8 7 6 5
        Likely used: 8
```

```
Configuration:
        Logical max current
        cylinders 16383 16383
        heads 16 16
        sectors/track 63 63
        --
        CHS current addressable sectors: 16514064
        LBA user addressable sectors: 268435455
        LBA48 user addressable sectors: 1953525168
        Logical Sector size: 512 bytes
        Physical Sector size: 4096 bytes
        Logical Sector-0 offset: 0 bytes
        device size with M = 1024*1024: 953869 MBytes
        device size with M = 1000*1000: 1000204 MBytes (1000 GB)
        cache/buffer size = unknown
        Form Factor: 3.5 inch
        Nominal Media Rotation Rate: 7200
Capabilities:
        LBA, IORDY(can be disabled)
        Queue depth: 32
        Standby timer values: spec'd by Standard, no device specific minimum
        R/W multiple sector transfer: Max = 16 Current = 16
        Advanced power management level: disabled
        DMA: mdma0 mdma1 mdma2 udma0 udma1 udma2 udma3 udma4 udma5 *udma6
        Cycle time: min=120ns recommended=120ns
        PIO: pio0 pio1 pio2 pio3 pio4
        Cycle time: no flow control=120ns IORDY flow control=120ns
Commands/features:
        Enabled Supported:
                * SMART feature set
                  Security Mode feature set
                * Power Management feature set
                * Write cache
                * Look-ahead
                * Host Protected Area feature set
                * WRITE_BUFFER command
                * READ_BUFFER command
                * NOP cmd
                * DOWNLOAD_MICROCODE
                  Advanced Power Management feature set
                  Power-Up In Standby feature set
                * SET_FEATURES required to spinup after power up
                  SET_MAX security extension
                * 48-bit Address feature set
                * Device Configuration Overlay feature set
                * Mandatory FLUSH_CACHE
                * FLUSH_CACHE_EXT
                * SMART error logging
                * SMART self-test
                  Media Card Pass-Through
                * General Purpose Logging feature set
                * WRITE_{DMA|MULTIPLE}_FUA_EXT
                * 64-bit World wide name
                * URG for READ_STREAM[_DMA]_EXT
                * URG for WRITE_STREAM[_DMA]_EXT
                * WRITE_UNCORRECTABLE_EXT command
                * {READ,WRITE}_DMA_EXT_GPL commands
                * Segmented DOWNLOAD_MICROCODE
                  unknown 119[7]
                * Gen1 signaling speed (1.5Gb/s)
                * Gen2 signaling speed (3.0Gb/s)
                * Gen3 signaling speed (6.0Gb/s)
                * Native Command Queueing (NCQ)
                * Host-initiated interface power management
                * Phy event counters
                * NCQ priority information
                  Non-Zero buffer offsets in DMA Setup FIS
                * DMA Setup Auto-Activate optimization
                  Device-initiated interface power management
                 In-order data delivery
                * Software settings preservation
                * SMART Command Transport (SCT) feature set
                * SCT Write Same (AC2)
                * SCT Error Recovery Control (AC3)
```

```
                * SCT Features Control (AC4)
                * SCT Data Tables (AC5)
Security:
        Master password revision code = 65534
                  supported
              not enabled
              not locked
                  frozen
              not expired: security count
              not supported: enhanced erase
              156min for SECURITY ERASE UNIT.
Logical Unit WWN Device Identifier: 5000039fd3cc4d45
        NAA : 5
        IEEE OUI : 000039
        Unique ID : fd3cc4d45
Checksum: correct
```

Информация о поддерживаемых параметрах безопасности ATA Security содержится в секции "Security":

```
...

Security:
        Master password revision code = 65534
                  supported
              not enabled
              not locked
                  frozen
              not expired: security count
              not supported: enhanced erase
              156min for SECURITY ERASE UNIT.

....
```

В приведённом примере указано, что поддерживается защита по парольному доступу ("Master password ... suported"), которая на момент регистрации параметров накопителя отключена ("not enabled").
Кроме того в вышеприведённых данных о состоянии накопителя указано, что изменение параметров безопасности заблокировано (строка "frozen"). Эта блокировка автоматически выполняется при загрузке системы большинством современных BIOS-ов и/или операционных систем для того, чтобы в процессе работы ОС вредоносное ПО не смогло несанкционированно установить свои пароли на накопитель, заблокировав доступ ко всем находящимся на нём данные.

Установка пароля

При установке пароля следует помнить, что:

- На устройствах, подключенных через USB, снятие пароля может не работать;
- При загрузке компьютера некоторые BIOS-ы и/или операционные системы выдают всем подключенным дискам команды, запрещающие изменение параметров безопасности (до момента перезапуска по питанию).
  На таких системах для снятия/установки пароля понадобится выполнить "горячее" подключение диска к уже загруженному и работающему компьютеру;

Установка пользовательского пароля выполняется командой (в примере - установка пароля 12345678 на устройство /dev/sdb) :

```
sudo hdparm --user-master u --security-set-pass 12345678 /dev/sdb
```

Блокировка

Блокировка данных включается отключением электропитания диска.
При написании этой статьи было обнаружено, что блокировку можно включить программным удалением диска, однако гарантировать, что это будет так же работать на всех компьютерах не представляется возможным (приведена команда для диска sdb):

```
sudo -i
echo 1 >/sys/block/sdb/device/delete
exit
```

Разблокировка

Горячее подключение

Горячее подключение накопителей SATA корректно поддерживается большинством современных накопителей и контроллеров. Однако, после подключения накопителя для его обнаружения операционной системой необходимо выполнить сканирование дисков.
Это можно сделать из сессии суперпользователя:

```
sudo -i
echo "- - -" > /sys/class/scsi_host/hostX/scan
exit
```

При этом вместо hostX подставить цифру - номер использованного контроллера (при написании этой статьи использовался /sys/class/scsi_host/host3/scan), можно просто последовательно просканировать все контроллеры.

После подключения и обнаружения накопителя и до его разблокировки данные, находящиеся на этом накопителе,й2 будут недоступны.
Разблокировка данных (действующая до следующего отключения питания) осуществляется командой (для примера используется пароль 12345678):

```
sudo hdparm --user-master u --security-unlock 12345678 /dev/sdb
```

После выполнения разблокировки следует повторно просканировать таблицу дисковых разделов :

```
sudo hdparm -z /dev/sdb
```

Отключение блокировки

Полностью отключить блокировку можно командой:

```
sudo hdparm --user-master u --security-disable 12345678 /dev/sdb
```

Если накопитель был заблокирован, то после выполнения отключения блокировки следует повторно просканировать таблицу дисковых разделов :

```
sudo hdparm -z /dev/sdb
```

TCG OPAL

Программное обеспечение для реализации режима защиты данных TCG Opal не является сертифицированным решением, и не входит в репозитории и дистрибутивы ОС Astra Linux.

При работе ПО используются специальные служебные команды ATA (TPM), использование которых по умолчанию запрещено в параметрах ядра (точнее, в параметрах входящей в ядро библиотеки libata). И, как указано в документации к библиотеке libata, разрешение этих команд

> "... обеспечивает по сути неконтролируемый зашифрованный "черный ход" между при ложениями и диском. Устанавливайте libata.allow_tpm = 1, только если вы имеете для этого реальную причину...".

Список накопителей, поддерживающих OPAL

Данная статья подготовлена на основе инструкций производителя и Wki Archlinux .

Для пользователей с нестандартными клавиатурами

Рассматриваемое ПО предполагает, что всегда используется стандартная клавиатура us_english. Это может привести к проблемам при использовании других раскладок клавиатуры.
Для того, чтобы убедиться, что пароль распознаётся правильно, рекомендуется настраивать диск с использованием загрузки временной системы как описано далее.

Описанная ниже процедура с использованием загрузки с временного диска позволяет установить защиту на загрузочный диск, в том числе на загрузочный диск, на котором уже установлена ОС.
В проведённых экспериментах ранее установленная ОС остаётся работоспособной (естественно, при условии разблокировки диска после включения), однако не забывайте сделать резервную копию.

Защиту незагрузочных дисков можно включать/выключать непосредственно из ОС предварительно разрешив использование команд ATA TPM Соответствующие иструменты командной строки доступны по ссылке https://github.com/Drive-Trust-Alliance/sedutil/wiki/Executable-Distributions.

Для разрешения команд ATA TPM:

1. Установить параметр ядра allow_tpm = 1 в файле /etc/default/grub:

   GRUB_CMDLINE_LINUX_DEFAULT="quiet splash libata.allow_tpm=1"

2. Обновить загрузчик:

   ```
   sudo update-grub
   ```

3. Перезагрузить систему.

Подготовка загрузочной системы

Скачать образ загрузочной системы: для BIOS и для 64bit UEFI.

Это можно сделать командами

```
wget -O RESCUE32.img.gz https://github.com/Drive-Trust-Alliance/exec/blob/master/RESCUE32.img.gz?raw=true
```

или

```
wget -O RESCUE64.img.gz https://github.com/Drive-Trust-Alliance/exec/blob/master/RESCUE64.img.gz?raw=true
```

Для использования UEFI необходимо отключить Secure Boot.

Распаковать скачанные файлы загрузочных образов:

```
gunzip RESCUE32.img.gz
```

или

```
gunzip RESCUE64.img.gz
```

Подключить USB-накопитель и скопировать на него распакованный образ, указав название устройства:

Следующая операция полностью уничтожит данные на накопителе.

```
dd if=RESCUE32.img of=/dev/sd?
```

или

```
dd if=RESCUE64.img of=/dev/sd?
```

Перезагрузить компьютер с созданного накопителя.

После появления приглашения Login ввести "root" без пароля.

Все дальнейшие шаги выполняются во временной системе

Проверка накопителей

Ввести команду

sedutil-cli --scan

Предполагаемый вывод команды:

```
#sedutil-cli --scan
Scanning for Opal compliant disks
/dev/nvme0 2 Samsung SSD 960 EVO 250GB 2B7QCXE7
/dev/sda 2 Crucial_CT250MX200SSD1 MU04
/dev/sdb 12 Samsung SSD 850 EVO 500GB EMT01B6Q
/dev/sdc 2 ST500LT025-1DH142 0001SDM7
/dev/sdd 12 Samsung SSD 850 EVO 250GB EMT01B6Q
No more disks present ending scan
```

Наличие цифры 2 во второй колонке указывает на то, что накопитель поддерживает OPAL 2, и что с ним можно выполнять дальнейшие действия.

Применение дальнейших инструкций к накопителям, не поддерживающим OPAL2, может привести к потере хранящихся на них данных.

Проверка предзагрузочной авторизации (PBA)

Используем команду linuxpba с паролем debug.

При использовании иного пароля система перезагрузится.

Пример вывода команды:

```
#linuxpba
DTA LINUX Pre Boot Authorization
Please enter pass-phrase to unlock OPAL drives: *****
Scanning....
Drive /dev/nvme0 Samsung SSD 960 EVO 250GB is OPAL NOT LOCKED
Drive /dev/sda Crucial_CT250MX200SSD1 is OPAL NOT LOCKED
Drive /dev/sdb Samsung SSD 850 EVO 500GB is OPAL NOT LOCKED
Drive /dev/sdc ST500LT025-1DH142 is OPAL NOT LOCKED
Drive /dev/sdd Samsung SSD 850 EVO 250GB is OPAL NOT LOCKED
```

Убедитесь, что ваш накопитель представлен в списке и отмечен как "is OPAL".

Далее описаны действия по включению блокировки OPAL. В случае возникновения проблем используйте инструкции из раздела "Восстановление информации" для отключения или удаления блокировки.

Далее в примерах предполагается использование накопителя /dev/sdc и архива загрузочного образа /usr/sedutil/UEFI64-1.15.img.gz (архивы образов находятся на загрузочном диске с временной системой).
Для использования в вашей системе укажите правильное устройство /dev/sd? и правильный образ.

Включение блокировки и предзагрузочной авторизации

В установленном загрузочном образе для временной загрузки находится запакованный образ загрузочного сектора.
При первом использовании его следует распаковать:

```
#
gunzip /usr/sedutil/UEFI64-n.nn.img.gz
```

Далее ввести следующие подготовительные команды (для теста используется пароль debug, который будет изменён позднее):

```
sedutil-cli --initialsetup debug /dev/sdc
#
sedutil-cli --loadPBAimage debug /usr/sedutil/UEFI64-n.nn.img /dev/sdc
sedutil-cli --setMBREnable on debug /dev/sdc
```

И включить блокировку следующей командой:

```
sedutil-cli --enableLockingRange 0 password drive
```

Повторная проверка PBA

Повторная проверка позволяет убедиться, что накопитель действительно разблокирован.
Для проверки используется команда и пароль debug. Предполагаемый результат:

```
#linuxpba

DTA LINUX Pre Boot Authorization
Please enter pass-phrase to unlock OPAL drives: *****
Scanning....
Drive /dev/nvme0 Samsung SSD 960 EVO 250GB is OPAL NOT LOCKED
Drive /dev/sda Crucial_CT250MX200SSD1 is OPAL NOT LOCKED
Drive /dev/sdb Samsung SSD 850 EVO 500GB is OPAL NOT LOCKED
Drive /dev/sdc ST500LT025-1DH142 is OPAL Unlocked <---Важно!!!
Drive /dev/sdd Samsung SSD 850 EVO 250GB is OPAL NOT LOCKED
```

Убедитесь, что накопитель действительно разблокирован (помечен как "is OPAL Unlocked").
Если накопитель не разблокирован, то перейдите к процедуре разблокировки и отключения OPAL.

Установка реальных паролей

В примере используются одинаковые пароли SID и Admin1, хотя они не обязательно должны совпадать.
Команды для установки паролей:

```
sedutil-cli --setsidpassword debug yourrealpassword /dev/sdc
sedutil-cli --setadmin1pwd debug yourrealpassword /dev/sdc
```

Примерный диалог:

```
#sedutil-cli --setsidpassword debug yourrealpassword /dev/sdc
#sedutil-cli --setadmin1pwd debug yourrealpassword /dev/sdc
- 14:20:53.352 INFO: Admin1 password changed
```

Проверьте правильность паролей командой:

```
sedutil-cli --setmbrdone on yourrealpassword /dev/sdc
```

Примерный диалог

#sedutil-cli --setmbrdone on yourrealpassword /dev/sdc
- 14:22:21.590 INFO: MBRDone set on Your drive in now using OPAL locking.

Следующим шагом следует отключить и полностью обесточить систему.
После отключения питания накопитель будет заблокирован и переведён в режим загрузки предзагрузочной авторизации с запросом пароля (PBA) при следующих включениях.

На некоторых компьютерах понадобится в явном виде указать в BIOS в настройках загрузки сектор PBE для загрузки.

Восстановление информации

В случае возникновения проблем с помощью загрузочного накопителя можно отключить блокировку или полностью удалить OPAL для дальнейшего использования накопителя без блокировки.

Отключение блокировки и предзагрузочной авторизации

```
sedutil-cli --disableLockingRange 0 <password> <drive>
sedutil-cli --setMBREnable off <password> <drive>
```

Примерный диалог:

#sedutil-cli --disablelockingrange 0 debug /dev/sdc
- 14:07:24.914 INFO: LockingRange0 disabled
#sedutil-cli --setmbrenable off debug /dev/sdc
- 14:08:21.999 INFO: MBREnable set off

Восстановление блокировки и предзагрузочной авторизации

```
sedutil-cli --enableLockingRange 0 <password> <drive>
sedutil-cli --setMBREnable on <password> <drive>
```

Примерный диалог:

#sedutil-cli --enablelockingrange 0 debug /dev/sdc
- 14:07:24.914 INFO: LockingRange0 enabled ReadLocking,WriteLocking
#sedutil-cli --setmbrenable on debug /dev/sdc
- 14:08:21.999 INFO: MBREnable set on

Полное удаление OPAL

Некоторые накопители OPALимеют ошибку во встроенном ПО, ведущую к уничтожению данных при выполненнии следующих команд.
Список проверенных накопителей, не подверженных этой ошибке доступен по ссылке.

```
sedutil-cli --revertnoerase <password> <drive>
sedutil-cli --reverttper <password> <drive>
```

Примерный диалог:

#sedutil-cli --revertnoerase debug /dev/sdc
- 14:22:47.060 INFO: Revert LockingSP complete
#sedutil-cli --reverttper debug /dev/sdc
- 14:23:13.968 INFO: revertTper completed successfully
#

Уязвимости

Уязвимость "сохранение питания"

Типичный самозащищенный накопитель, будучи однажды разблокированным, остаётся разблокированным пока на него подается электропитание. Таким образом, при условии сохранении питания, накопитель может быть перенесен куда угодно, оставаясь в разблокированном состоянии. Например, было показано, что при некоторых условиях компьютер может быть перезагружен с запуском другой операционной системы, также демонстрировался перенос накопителя на другой компьютер без отключения питания.

Скомпрометированное встроенное ПО

Встроенное программное обеспечение накопителя может иметь недокументированные возможности, позволяющие получать несанкционированный доступ к данным, а применяемые алгоритмы защитного преобразования остаются на усмотрение производителей.
См. например исследование уязвимостей накопителей.