# PV204 Security technologies

## File and disk encryption – lab intro

Milan Brož xbroz@fi.muni.cz
Faculty of Informatics, Masaryk University

CROCS
Centre for Research on Cryptography and Security

# Laboratory – FDE attack examples

**Basic understanding of some tools and hw**

VeraCrypt, LUKS, chip-based encryption

**I. Scanning memory image for encryption key**

ColdBoot attack principle

**II. HW key-logger attack**

**III. Flawed algorithm and watermarking**

Revealing TrueCrypt hidden disk existence (CBC)

# Environment setup

**VirtualBox virtual machine (in IS)**

- note: image is large >4GB (disk-encrypted Linux)
- slightly modified Debian Linux
- Login: pv204
- Password: pv204 (including root/sudo and disk unlock)

VM has all tools prepared.

*You can use own distro, but some tools need to be installed locally:*

- *TrueCrypt 7.1a (last non-crippled version)*
- *VeraCrypt 1.2x*
- *Cryptsetup 2.x (distro provides it)*
- *Patched AesKeyfind – in Exercise2_aeskeyfind.zip or [https://github.com/mbroz/aeskeyfind](https://github.com/mbroz/aeskeyfind)*
- *Small utilities for Exercise 3 – in Exercise3_tc_cbc_hidden_attack.zip*

# Demo

- Storage in Linux
  - lsblk command
  - device-mapper dm-crypt (disk encryption), dmsetup
  - cryptsetup (LUKS: open, dump metadata)
  - CBC benchmark (encryption/decryption speed)

- VeraCrypt intro
  - basic concepts (RNG, key-derivation, encryption, chained ciphers)
  - create AES encrypted container for key search

```
pv204@pv204:~$ lsblk
NAME                  MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
loop0                   7:0    0   16M  0 loop
└─veracrypt1          254:3    0 15.8M  0 dm    /media/veracrypt1
sda                     8:0    0   16G  0 disk
├─sda1                  8:1    0  243M  0 part  /boot
├─sda2                  8:2    0    1K  0 part
└─sda5                  8:5    0 15.8G  0 part
  └─sda5_crypt        254:0    0 15.8G  0 crypt
    ├─pv204--vg-root  254:1    0 15.1G  0 lvm   /
    └─pv204--vg-swap_1 254:2   0  708M  0 lvm   [SWAP]
pv204@pv204:~$ lsblk -f
NAME                  FSTYPE      FSVER    LABEL UUID                                   FSAVAIL FSUSE% MOUNTPOINT
loop0
└─veracrypt1          vfat        FAT16          798C-4D8B                               15.7M     0% /media/veracrypt1
sda
├─sda1                ext2        1.0            324a2572-f2df-4809-93f2-8e2f2b1f04ee    162.7M    26% /boot
├─sda2
└─sda5                crypto_LUKS 1              3bff3b80-20cc-435e-b96f-e0b74807727b
  └─sda5_crypt        LVM2_member LVM2 001       NfxGlz-iWdc-vE3y-JiOV-r4u7-PWmr-ZB7nyy
    ├─pv204--vg-root  ext4        1.0            a7cd1f8a-5e80-400b-b3f3-a863e267578e     11.3G    18% /
    └─pv204--vg-swap_1 swap       1              0270a337-c714-4d91-9150-4a7ad1cf0722                  [SWAP]
pv204@pv204:~$
```

## Display storage stack (with some encryption devices)

```
pv204@pv204:~$ sudo dmsetup table veracrypt1 --showkeys
0 32256 crypt aes-xts-plain64 9fcf190c6aa62be5265739594e0c24b86f12b45beabfcdca1bb4085eaf570e584dcbaa355c119e5212a527ea23de85f47daa9da3c47c
e4e4e6bf8b58e8a3076d 256 7:0 256
pv204@pv204:~$ sudo dmsetup table sda5_crypt --showkeys
0 33046528 crypt aes-xts-plain64 1e0b30621e431358c3cccc5d05cd0a6eb0d6a4562c176ec7a30685d8af91d5ea2b7338b2f081e63eb311d9fee25be242a6011e9c2
5d43973ae58c3f27fbb6156 0 8:5 4096 1 allow_discards
pv204@pv204:~$
```

## Display volume key for active dm-crypt device

```
pv204@pv204:~$ sudo cryptsetup benchmark
# Tests are approximate using memory only (no storage IO).
PBKDF2-sha1       960234 iterations per second for 256-bit key
PBKDF2-sha256    1235071 iterations per second for 256-bit key
PBKDF2-sha512     888623 iterations per second for 256-bit key
PBKDF2-ripemd160  574247 iterations per second for 256-bit key
PBKDF2-whirlpool  330156 iterations per second for 256-bit key
argon2i       4 iterations, 478884 memory, 4 parallel threads (CPUs) for 256-bit key (requested 2000 ms time)
argon2id      4 iterations, 512262 memory, 4 parallel threads (CPUs) for 256-bit key (requested 2000 ms time)
#     Algorithm |       Key |      Encryption |      Decryption
        aes-cbc        128b       415.1 MiB/s      1268.1 MiB/s
    serpent-cbc        128b        59.4 MiB/s       216.4 MiB/s
    twofish-cbc        128b       126.9 MiB/s       236.6 MiB/s
        aes-cbc        256b       335.4 MiB/s      1024.8 MiB/s
    serpent-cbc        256b        65.0 MiB/s       218.4 MiB/s
    twofish-cbc        256b       132.1 MiB/s       236.6 MiB/s
        aes-xts        256b      1047.7 MiB/s      1091.6 MiB/s
    serpent-xts        256b       222.2 MiB/s       211.4 MiB/s
    twofish-xts        256b       232.6 MiB/s       235.5 MiB/s
        aes-xts        512b       880.8 MiB/s       888.3 MiB/s
    serpent-xts        512b       222.9 MiB/s       211.9 MiB/s
    twofish-xts        512b       224.8 MiB/s       232.2 MiB/s
pv204@pv204:~$
```

## cryptsetup benchmark

```
pv204@pv204:~$ /sbin/cryptsetup tcryptDump --veracrypt testimage.img
Enter passphrase for testimage.img:
VERACRYPT header information for testimage.img
Version:        5
Driver req.:    1.b
Sector size:    512
MK offset:      131072
PBKDF2 hash:    sha512
Cipher chain:   aes
Cipher mode:    xts-plain64
MK bits:        512
pv204@pv204:~$
pv204@pv204:~$
pv204@pv204:~$ sudo cryptsetup luksDump /dev/sda5
LUKS header information for /dev/sda5

Version:        1
Cipher name:    aes
Cipher mode:    xts-plain64
Hash spec:      sha1
Payload offset: 4096
MK bits:        512
MK digest:      a7 49 ab bf b0 a3 9e f9 7e 26 8e 0f 4b 9f 32 7e 7e bc f9 38
MK salt:        90 20 c8 1b 27 b9 a4 42 f9 de 80 16 98 d2 b2 09
                4c 7a 79 59 39 23 e3 c2 ad c6 1e ef a4 29 88 6c
MK iterations:  117625
UUID:           3bff3b80-20cc-435e-b96f-e0b74807727b

Key Slot 0: ENABLED
        Iterations:             1024000
        Salt:                   85 a8 40 2e db 73 c5 72 54 a1 06 04 40 0a 34 b0
                                61 77 9d 0d 71 bd 2b 02 bf 3d 71 7b f2 4c 83 1c
        Key material offset:    8
        AF stripes:             4000
Key Slot 1: DISABLED
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
pv204@pv204:~$
```

## cryptsetup metadata dump / VeraCrypt and LUKS1 device

```
pv204@pv204:~$ /sbin/cryptsetup tcryptDump --veracrypt testimage.img --dump-master-key
Enter passphrase for testimage.img:

WARNING!
========
Header dump with volume key is sensitive information
which allows access to encrypted partition without passphrase.
This dump should be always stored encrypted on safe place.

Are you sure? (Type 'yes' in capital letters): YES
TCRYPT header information for testimage.img
Cipher chain:   aes
Cipher mode:    xts-plain64
Payload offset: 256
MK bits:        512
MK dump:        9f cf 19 0c 6a a6 2b e5 26 57 39 59 4e 0c 24 b8
                6f 12 b4 5b ea bf cd ca 1b b4 08 5e af 57 0e 58
                4d cb aa 35 5c 11 9e 52 12 a5 27 ea 23 de 85 f4
                7d aa 9d a3 c4 7c e4 e4 e6 bf 8b 58 e8 a3 07 6d
pv204@pv204:~$
```

**cryptsetup dump of volume key (VeraCrypt)**

```
# lsblk -f /dev/sda
NAME   FSTYPE  FSVER LABEL     UUID
sda
├─sda1 vfat    FAT32 EFI       67E3-17ED
├─sda2 cs_fvault2              6f353c05-daae-4e76-a0ee-6a9569a22d81
└─sda3 hfsplus       Boot OS X 2c7d08a9-a36f-3a4f-9acb-fe06aed6c524

# cryptsetup fvault2Dump /dev/sda2 --dump-volume-key -q
Enter passphrase for /dev/sda2:
Header information for FVAULT2 device /dev/sda2.
Physical volume UUID:   6f353c05-daae-4e76-a0ee-6a9569a22d81
Family UUID:            f82cceb0-a788-4815-945a-53d57fcd55a8
Logical volume offset:  67108864 [bytes]
Logical volume size:    3288334336 [bytes]
Cipher:                 aes
Cipher mode:            xts-plain64
PBKDF2 iterations:      97962
PBKDF2 salt:            17 3a 4e c7 44 76 62 ec 79 ca 7a 47 df 6c 2a 01
Volume key:             4c 21 13 e9 6e 26 ee 08 09 c7 bd d4 3d 08 10 fc 73 6c 22 1e b0 59 94 cf 1a 2a 35 13 06 a8 db d1
```

**cryptsetup dump of FileVault2 device**

## cryptsetup dump of BitLocker device

```
# cryptsetup bitlkDump /dev/sda
Info for BITLK device /dev/sda.
Version:        2
GUID:           7b9f891c-de39-43f3-a64d-4574aeb62e05
Sector size:    512 [bytes]
Volume size:    3985637376 [bytes]
Created:        Fri May 27 13:41:53 2022
Description:    DESKTOP-71L8959 F: 27.05.2022
Cipher name:    aes
Cipher mode:    xts-plain64
Cipher key:     256 bits

Keyslots:
 0: VMK
        GUID:           38540616-5e99-49fd-b13a-0a5b372a74dc
        Protection:     VMK protected with passphrase
        Salt:           8b54fff189fd5f9a5ff88be6a5e75435
        Key data size:  44 [bytes]
 1: VMK
        GUID:           c0d3fd28-b9ba-4c1f-ae07-c932a4b2c42c
        Protection:     VMK protected with recovery passphrase
        Salt:           f8722c1a1e2146aa03c1fd73e800a95e
        Key data size:  44 [bytes]
 2: FVEK
        Key data size:  44 [bytes]

Metadata segments:
 0: FVE metadata area
        Offset:         34603008 [bytes]
        Size:           65536 [bytes]
 1: FVE metadata area
        Offset:         392519680 [bytes]
        Size:           65536 [bytes]
 2: FVE metadata area
        Offset:         750432256 [bytes]
        Size:           65536 [bytes]
 3: Volume header
        Offset:         34668544 [bytes]
        Size:           8192 [bytes]
        Cipher:         aes-xts-plain64
```

# EXERCISE II
# KEY FROM MEMORY IMAGE

# How to dump VirtualBox memory image

For exercise II. you need to get content (dump) of memory from running VM.

In *Exercise2_aeskeyfind.zip* are scripts for Linux/Windows

- **`Vbox_save_memcore.bat`** *or*
- **`linux/vbox_save_memcore_linux`**

  If you have different paths, it needs some tweaks – script contains only:
  **`vboxmanage debugvm pv204_fde dumpvmcore --filename memcore.img`**

Then use **`memcore.img`** as parameter for **`aeskeyfind`** command.

You can try another images, or other FS; VMware VM paused images etc.

# AESkeyfind output example

```
milan@merlot:pv204_img$ ./vbox_save_memcore_linux
------------------------------------------------------------
Memory image dumped to memcore.img
------------------------------------------------------------

milan@merlot:pv204_img$ ./aeskeyfind memcore.img
8b3f44d0b632907e31e4c03d91c70bd7e09f7c0bcd2aac4a0c28173059be2090
fe70feccb5f290b1b3869336c5c61f407d99ad6a9c816b34f58aea926a4e12c0
f35b6de1a926a7630f46bd7bebc7ebfde59c5c1cffc43e0f333d724fb95a5f15
72468d800243b97f0aa33e43f2e2a6ad5b05a25001838b9a72e1815eeacc4ba9
4ae9e023ca0e3f4007b2ce0c8a7f8fc1dc3d3dba8333427d82a53e127ab0ad33
0ed2a2074578270c175b106cb93df2d42b3ba34867e51b12fb850acc366687c6
20430658945d785c9365f9c185ceb573deab57b65c6c04516d51e6cb9da84516
0826f7bca941c5b3ebcc1fb67efe1966bf451a0aac30b5b2739bf4f134c89930
2eda34a0bff24dd2881c8196b20384c53a0e2fca6ec75433efe2aa0299327252
085fb1c539d17532b68f8bb215e1acddbb5606aa886de720f064302d1b0c9816
11709afd0becd3ce7d1a4adee2b8dcabf4fd8159605b6587387ed5b9083b0b47
11709afd0becd3ce7d1a4adee2b8dcabf4fd8159605b6587387ed5b9083b0b47
000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f
000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f
085fb1c539d17532b68f8bb215e1acddbb5606aa886de720f064302d1b0c9816
cb1d72180cbc25d6569547353a6efa7f43240c3881dea97330ab31d8a7ebd5d3
000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f
5d288dc273360fe70595c199191b69cd7138a207e50359b8a036c6577315879a
5d288dc273360fe70595c199191b69cd7138a207e50359b8a036c6577315879a
000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f
4ae9e023ca0e3f4007b2ce0c8a7f8fc1dc3d3dba8333427d82a53e127ab0ad33
0ed2a2074578270c175b106cb93df2d42b3ba34867e51b12fb850acc366687c6
fe70feccb5f290b1b3869336c5c61f407d99ad6a9c816b34f58aea926a4e12c0
f35b6de1a926a7630f46bd7bebc7ebfde59c5c1cffc43e0f333d724fb95a5f15
2b7338b2f081e63eb311d9fee25be242a6011e9c25d43973ae58c3f27fbb6156
1e0b30621e431358c3cccc5d05cd0a6eb0d6a4562c176ec7a30685d8af91d5ea
20430658945d785c9365f9c185ceb573deab57b65c6c04516d51e6cb9da84516
Keyfind progress: 100%
```

**Image analysis on host**

*Questions for you:*

- *What are other keys?*
- *Why some keys repeats?*
- *Why is VeraCrypt key printed swapped?*

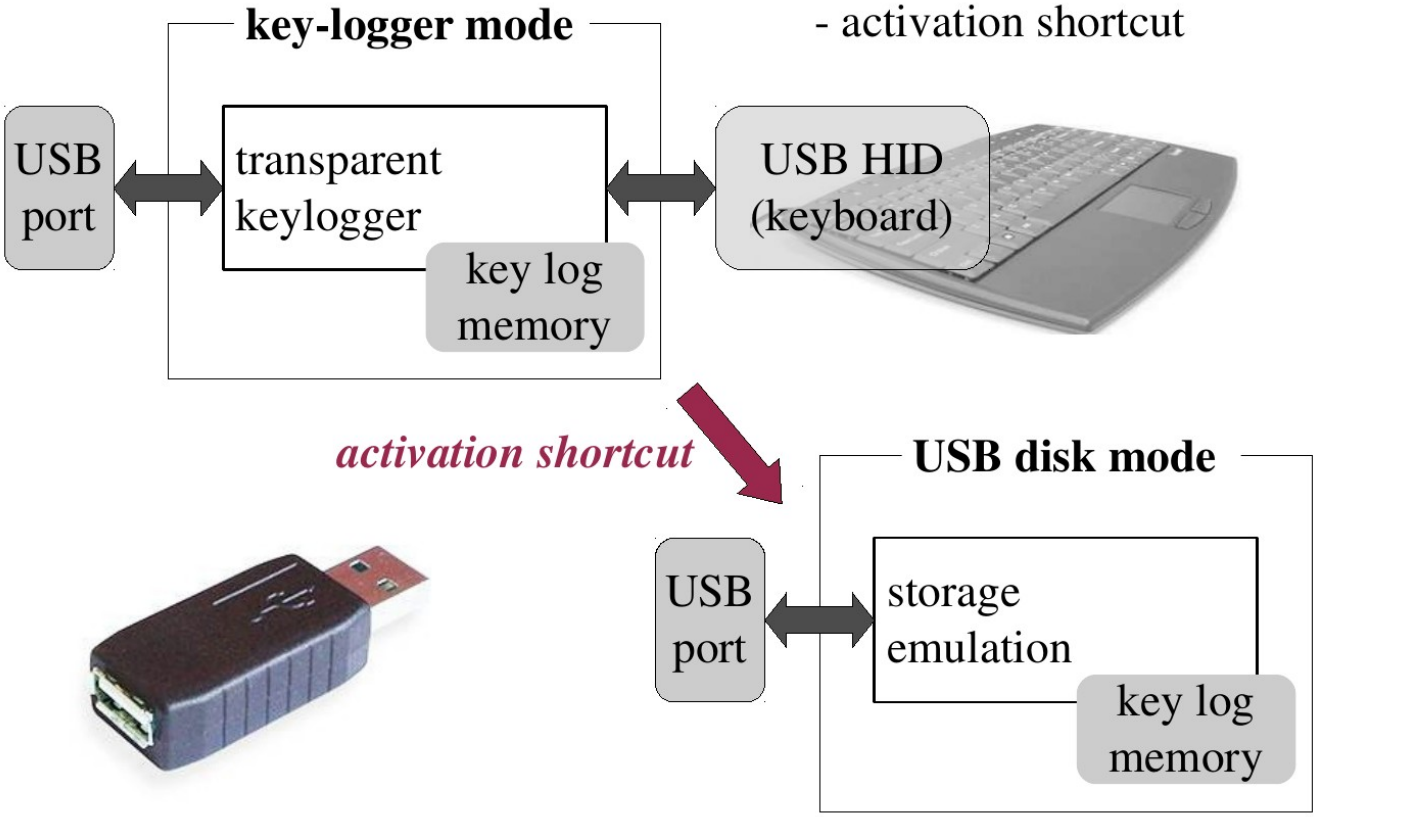
**dm-crypt key (from VeraCrypt container)**

```
pv204@pv204:~$ lsblk
NAME                  MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINT
loop0                   7:0    0   16M  0 loop
└─veracrypt1          254:3    0 15.8M  0 dm    /media/veracrypt1
sda                     8:0    0   16G  0 disk
├─sda1                  8:1    0  243M  0 part  /boot
├─sda2                  8:2    0    1K  0 part
└─sda5                  8:5    0 15.8G  0 part
  └─sda5_crypt        254:0    0 15.8G  0 crypt
    ├─pv204--vg-root  254:1    0 15.1G  0 lvm   /
    └─pv204--vg-swap_1 254:2   0  708M  0 lvm   [SWAP]
pv204@pv204:~$ sudo dmsetup table veracrypt1 --showkeys
0 32256 crypt aes-xts-plain64 0826f7bca941c5b3ebcc1fb67efe1966bf451a0a
ac30b5b2739bf4f134c89930204306589 45d785c9365f9c185ceb573deab57b65c6c04
516d51e6cb9da84516 256 7:0 256
```

# EXERCISE I
# HW KEYLOGGER

# Simple HW Keylogger Demo

- uses USB capabilities
- retrieve log – virtual USB disk
- activation shortcut



# HW Keylogger – KeyDaemon module