DISK ENCRYPTION

Tool: TOMB

MIS311 INFORMATION SECURITY SYSTEMS DESIGN

Instructor: SAFA BURAK GÜRLEYEN

Mücahit AYDIN
16030411022

JUNE 21’

INTRODUCTION

Disk encryption is a technology that transforms the information contained in it into an unreadable code that cannot be easily deciphered to protect it from unauthenticated persons. Disk encryption uses disk encryption software or hardware that encrypts every bit of data going to the disk or any part of the disk. It prevents unauthenticated persons from accessing the data memory.

Full Disk Encryption or Whole Disk Encryption technology is said to encrypt everything except the master boot record or similar space, a boot disk, the operating system boot code. Some hardware-based full disk encryption systems encrypt the entire boot disk, including the master boot record.

SECURITY CONCERNS

- *Most full-disk encryption projects are vulnerable to a cold boot attack, in which the encryption keys are stolen by cold-booting the operating system of the currently running machine and hijacking the data in memory before its contents are lost. This attack is based on the data magnetization feature of computer memory, the magnetization feature is stated as it takes a few minutes for the computer to shred data bits after power is turned off.[3] The Trusted Platform Module is also ineffective against this attack, because the operating system keeps in memory the decryption keys used to access the disk.All software-based encryption systems are vulnerable to various side-channel attacks, such as acoustic cryptoanalysis and hardware keylogger attacks. On the other hand, self-encrypting devices are not vulnerable to such attacks, as the hardware encryption key is never left to the control of the disk.*

INSTALLATION

Install required tools

Tomb needs a few programs to be installed on a system in order to work:

- zsh
- file
- sudo
- gnupg
- cryptsetup
- pinentry-curses (and/or -gtk-2, -x11, -qt)

INSTALLATION

- To install Tomb simply download the source distribution (the tar.gz file) from https://files.dyne.org/tomb and decompress it. From a terminal:

```
cd Downloads tar xvfz Tomb-2.4.tar.gz (correct with actual file name)
```

- Then enter its directory and run 'make install' as root, this will install Tomb into /usr/local:

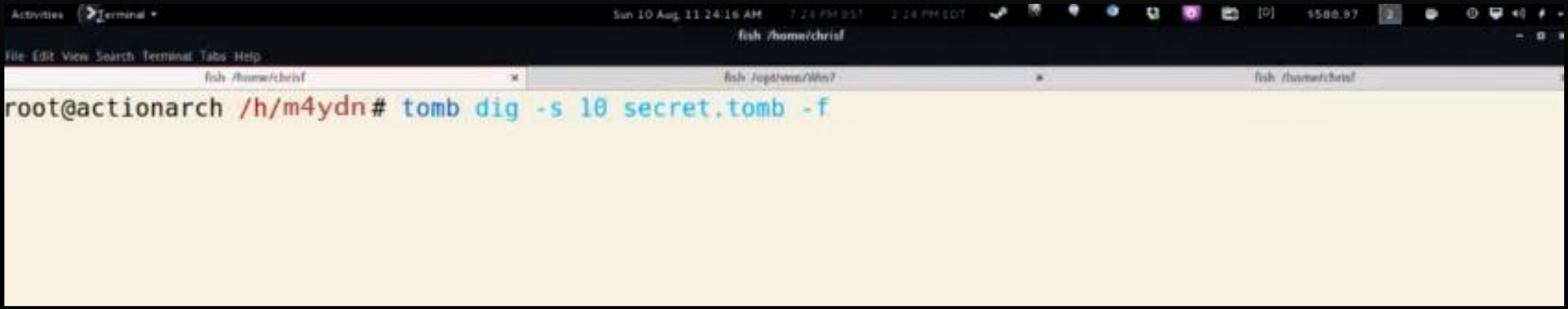
```
cd Tomb-2.4 (correct with actual directory name) sudo make install
```

- After installation one can read the commandline help or read the manual:

```
tomb -h (print a short help on the commandline) man tomb (show the full usage manual)
```

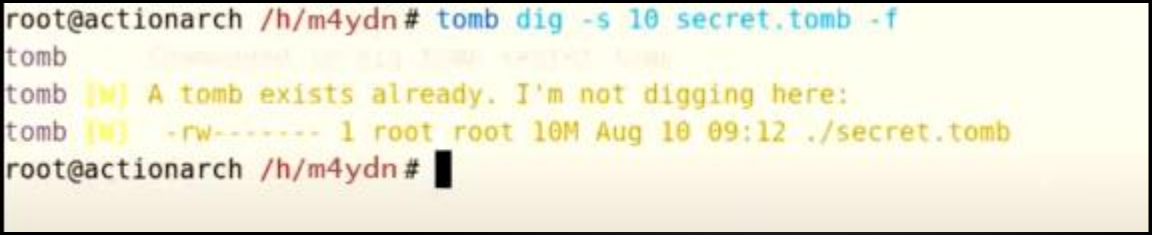
USING

- Once installed one can proceed creating a tomb, for instance:

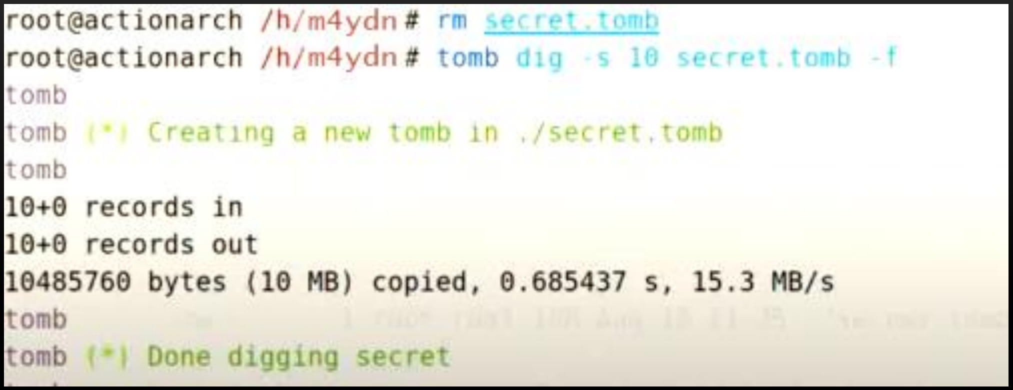


```
root@actionarch /h/m4ydn# tomb dig -s 10 secret.tomb -f
```

- When this is done, the tomb can be opened with

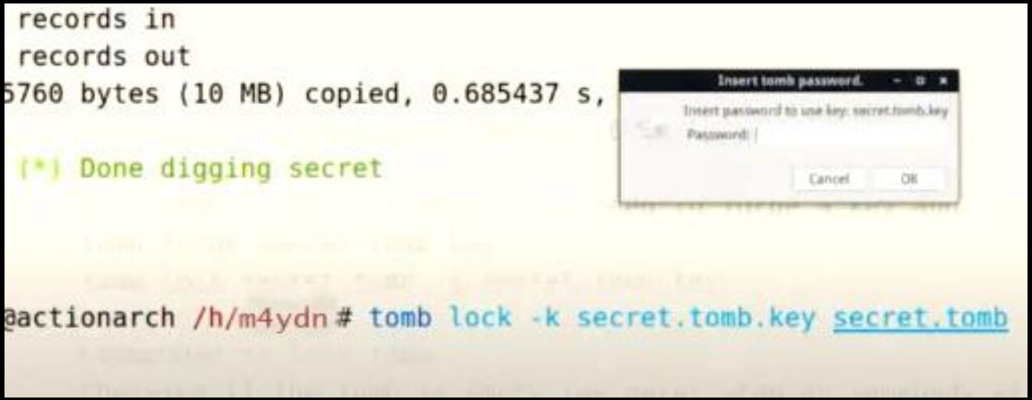


```
root@actionarch /h/m4ydn# tomb dig -s 10 secret.tomb -f
tomb     Commanded to dig tomb secret.tomb
tomb [W] A tomb exists already. I'm not digging here:
tomb [W]  -rw------- 1 root root 10M Aug 10 09:12 ./secret.tomb
root@actionarch /h/m4ydn#
```



```
root@actionarch /h/m4ydn# rm secret.tomb
root@actionarch /h/m4ydn# tomb dig -s 10 secret.tomb -f
tomb
tomb (*) Creating a new tomb in ./secret.tomb
tomb
10+0 records in
10+0 records out
10485760 bytes (10 MB) copied, 0.685437 s, 15.3 MB/s
tomb
tomb (*) Done digging secret
```

- The key can also be hidden in an image, to be used as key later

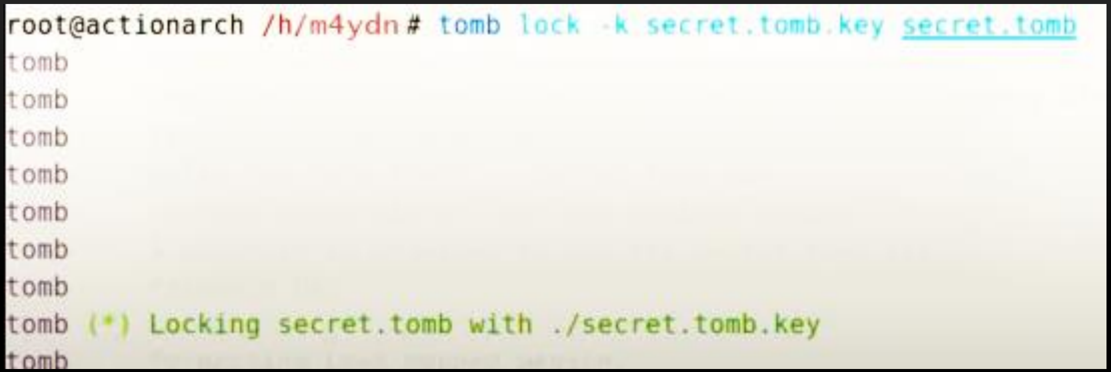


```
 records in
 records out
5760 bytes (10 MB) copied, 0.685437 s,

 (*) Done digging secret



@actionarch /h/m4ydn# tomb lock -k secret.tomb.key secret.tomb
```

Insert tomb password.

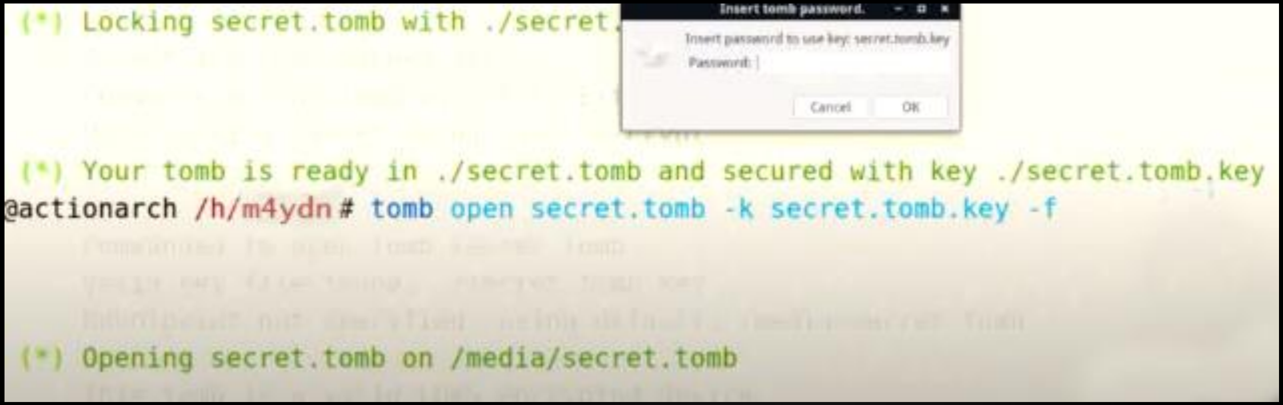
Insert password to use key: secret.tomb.key

Password:



```
root@actionarch /h/m4ydn# tomb lock -k secret.tomb.key secret.tomb
tomb
tomb
tomb
tomb
tomb
tomb
tomb
tomb (*) Locking secret.tomb with ./secret.tomb.key
tomb
```

- Type the password you created

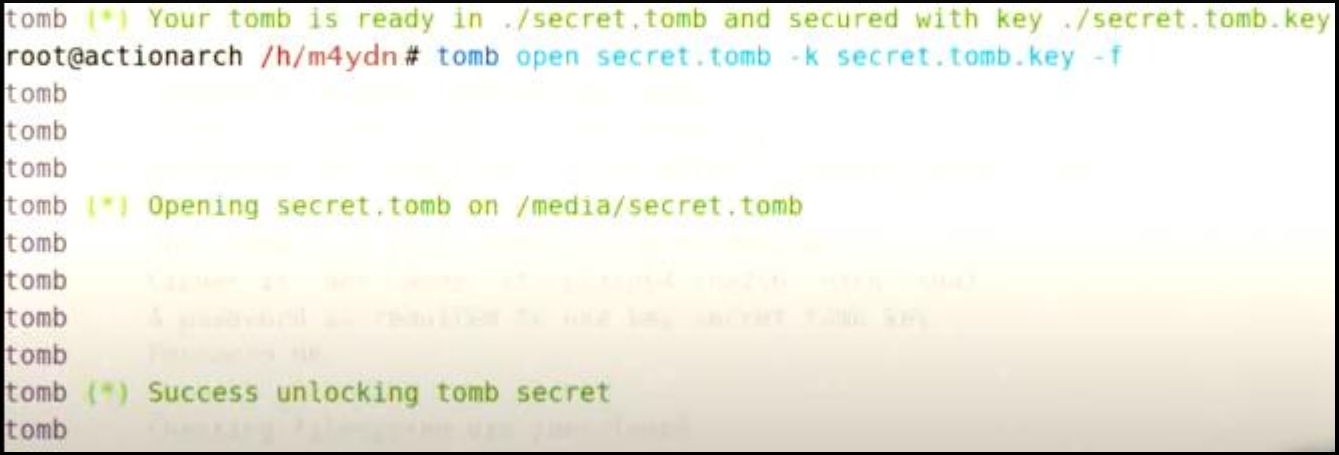


```
 (*) Locking secret.tomb with ./secret.

 (*) Your tomb is ready in ./secret.tomb and secured with key ./secret.tomb.key
@actionarch /h/m4ydn# tomb open secret.tomb -k secret.tomb.key -f

 (*) Opening secret.tomb on /media/secret.tomb
```

Insert tomb password.

Insert password to use key: secret.tomb.key

Password:



```
tomb (*) Your tomb is ready in ./secret.tomb and secured with key ./secret.tomb.key
root@actionarch /h/m4ydn# tomb open secret.tomb -k secret.tomb.key -f
tomb     [illegible]
tomb     [illegible]
tomb     [illegible]
tomb (*) Opening secret.tomb on /media/secret.tomb
tomb     [illegible]
tomb     Cipher is [illegible]
tomb     A password is required to use key secret.tomb.key
tomb     Password OK
tomb (*) Success unlocking tomb secret
tomb     Checking filesystem via [illegible]
```

Thank You

THE END