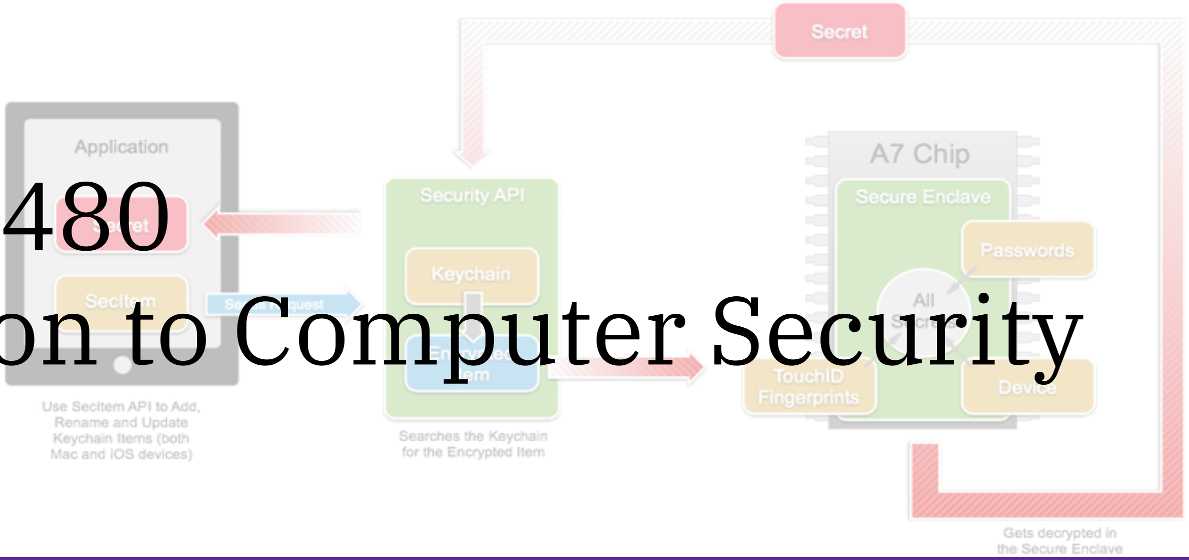
CSCI-UA.9480 Introduction to Computer Security



Use SecItem API to Add, Rename and Update Keychain Items (both Mac and iOS devices)

Searches the Keychain for the Encrypted Item

Gets decrypted in the Secure Enclave

Session 3.3
Systems Security and Isolation

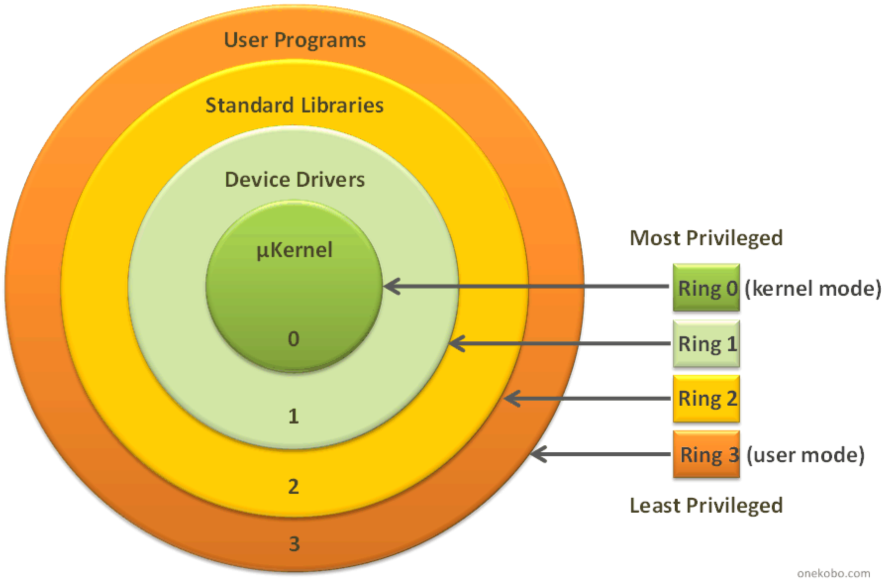
Prof. Nadim Kobeissi

Operating System Security Basics

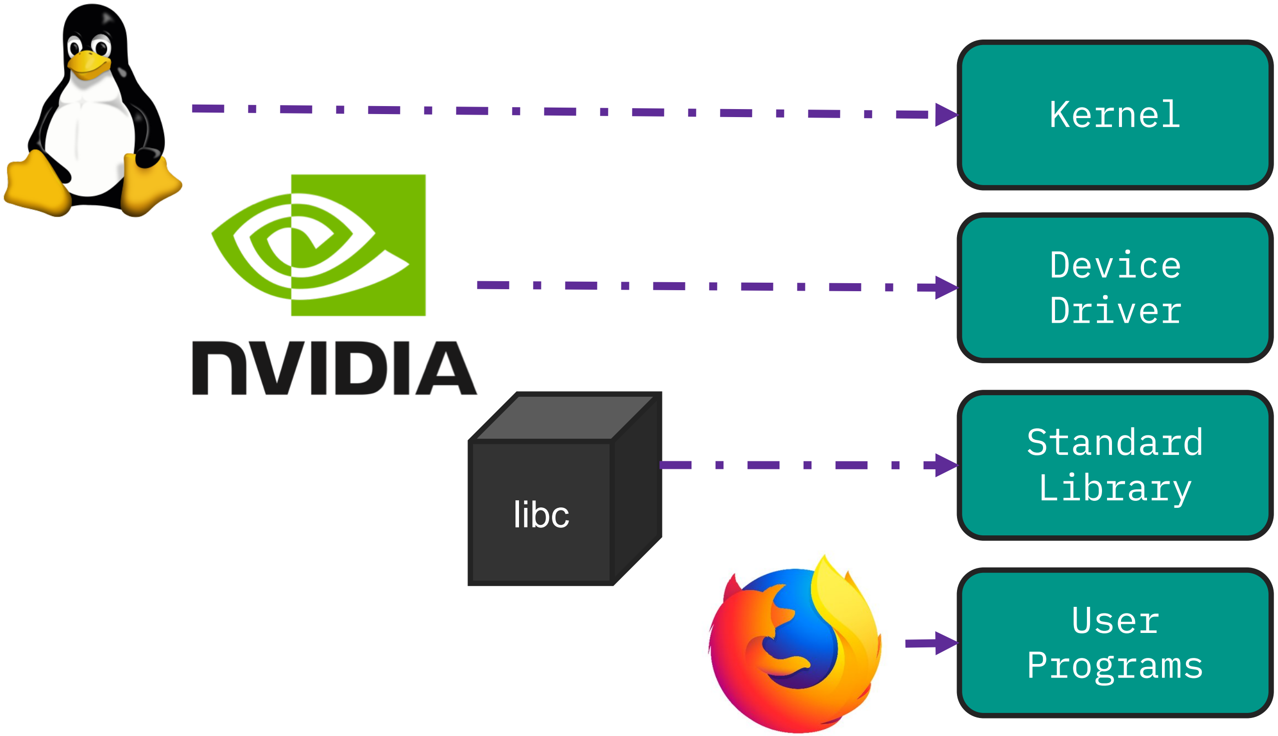
3.3a

Operating systems: protection rings.

- Kernel runs in Ring 0.
- Device drivers run in Ring 1.
- Standard libraries run in Ring 2.
- User programs run in Ring 3.



Examples.



libc

Kernel

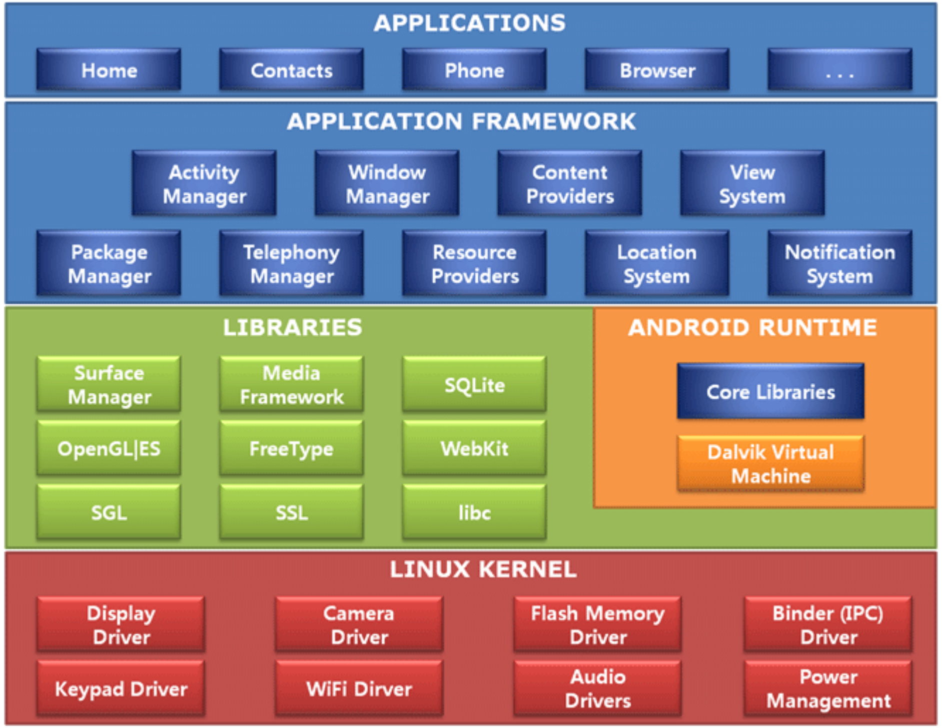
Device Driver

Standard Library

User Programs

What's managed by an operating system?

- *Subjects*: Users and processes.
- *Objects and resources*: Files (system integrity), hardware I/O (devices, private data), scheduling, network access...
- In Linux:
    - /dev: Devices.
    - /etc: Configuration files
    - /usr: Libraries, etc.



APPLICATIONS

Home
Contacts
Phone
Browser
. . .

APPLICATION FRAMEWORK

Activity Manager
Window Manager
Content Providers
View System
Package Manager
Telephony Manager
Resource Providers
Location System
Notification System

LIBRARIES

Surface Manager
Media Framework
SQLite
OpenGL|ES
FreeType
WebKit
SGL
SSL
libc

ANDROID RUNTIME

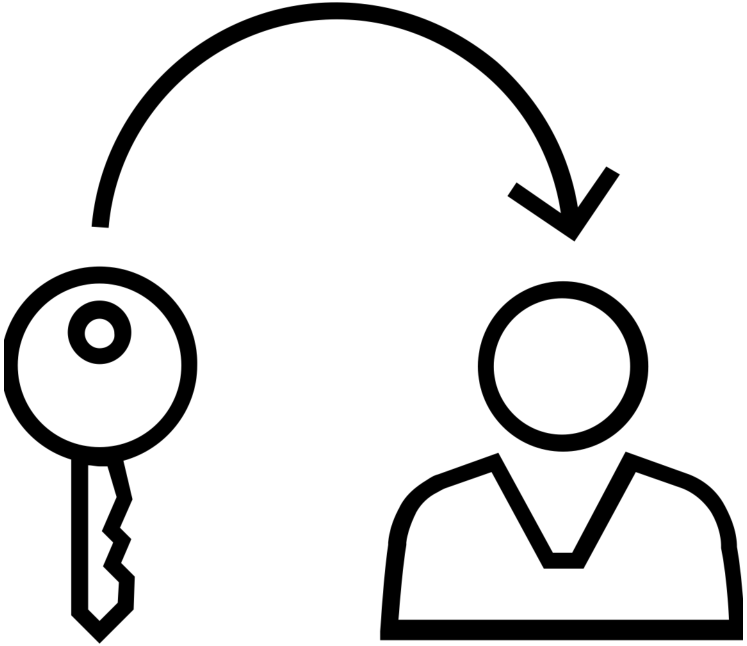
Core Libraries
Dalvik Virtual Machine

LINUX KERNEL

Display Driver
Camera Driver
Flash Memory Driver
Binder (IPC) Driver
Keypad Driver
WiFi Dirver
Audio Drivers
Power Management

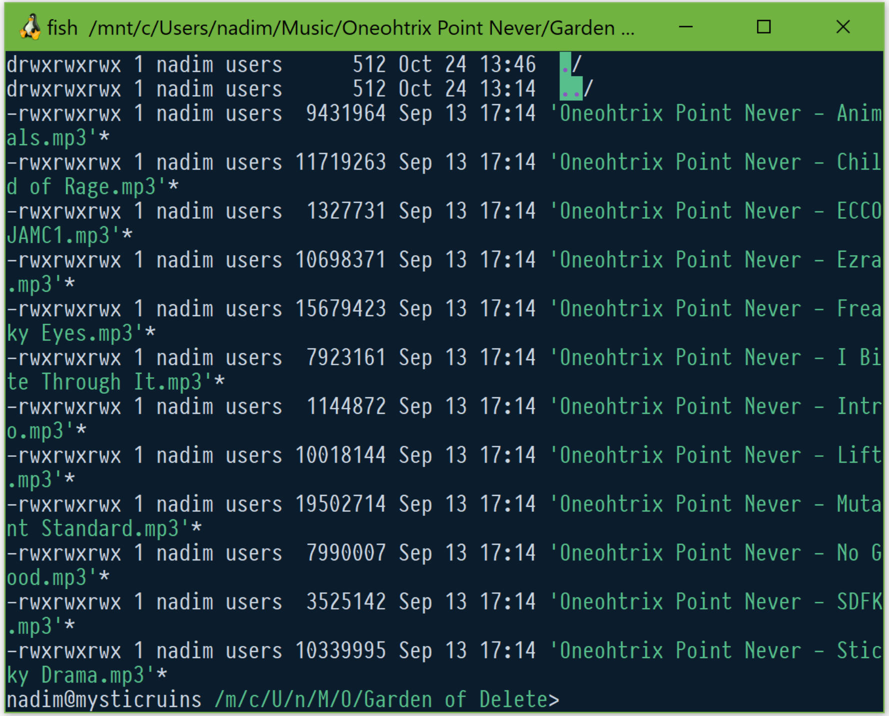
Principle of least-privilege.

- Services may need root access:
    - OpenSSH.
    - Apache, NGINX, Lighttpd…
    - Crond
    - Sendmail, Postfix
- Minesweeper does not.



POSIX permissions model.

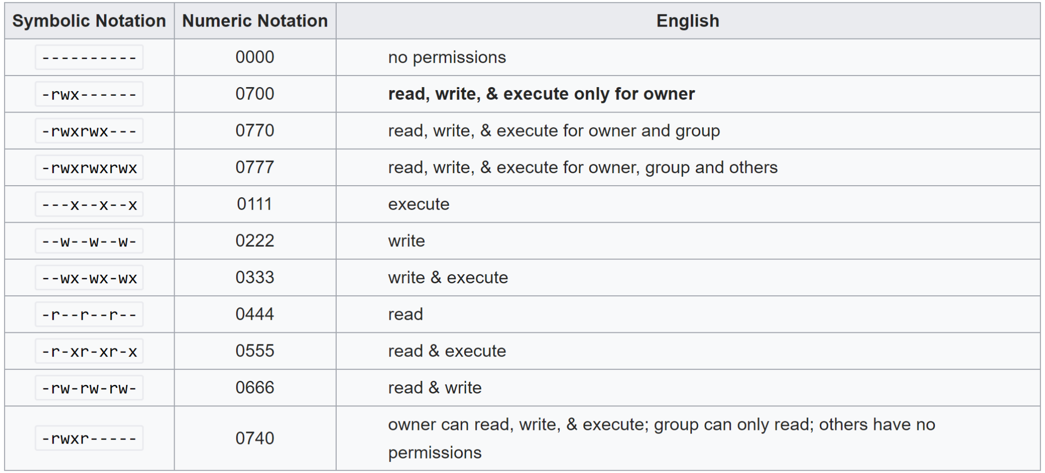
- First letter: special mode operator.
  - d: Directory.
  - l: Symbolic link.
  - s: setuid/setguid.
  - t: sticky bit.


fish /mnt/c/Users/nadim/Music/Oneohtrix Point Never/Garden ...

```
drwxrwxrwx 1 nadim users      512 Oct 24 13:46  ./
drwxrwxrwx 1 nadim users      512 Oct 24 13:14  ../
-rwxrwxrwx 1 nadim users  9431964 Sep 13 17:14 'Oneohtrix Point Never - Anim
als.mp3'*
-rwxrwxrwx 1 nadim users 11719263 Sep 13 17:14 'Oneohtrix Point Never - Chil
d of Rage.mp3'*
-rwxrwxrwx 1 nadim users  1327731 Sep 13 17:14 'Oneohtrix Point Never - ECCO
JAMC1.mp3'*
-rwxrwxrwx 1 nadim users 10698371 Sep 13 17:14 'Oneohtrix Point Never - Ezra
.mp3'*
-rwxrwxrwx 1 nadim users 15679423 Sep 13 17:14 'Oneohtrix Point Never - Frea
ky Eyes.mp3'*
-rwxrwxrwx 1 nadim users  7923161 Sep 13 17:14 'Oneohtrix Point Never - I Bi
te Through It.mp3'*
-rwxrwxrwx 1 nadim users  1144872 Sep 13 17:14 'Oneohtrix Point Never - Intr
o.mp3'*
-rwxrwxrwx 1 nadim users 10018144 Sep 13 17:14 'Oneohtrix Point Never - Lift
.mp3'*
-rwxrwxrwx 1 nadim users 19502714 Sep 13 17:14 'Oneohtrix Point Never - Muta
nt Standard.mp3'*
-rwxrwxrwx 1 nadim users  7990007 Sep 13 17:14 'Oneohtrix Point Never - No G
ood.mp3'*
-rwxrwxrwx 1 nadim users  3525142 Sep 13 17:14 'Oneohtrix Point Never - SDFK
.mp3'*
-rwxrwxrwx 1 nadim users 10339995 Sep 13 17:14 'Oneohtrix Point Never - Stic
ky Drama.mp3'*
nadim@mysticruins /m/c/U/n/M/O/Garden of Delete>
```

POSIX permissions model.

- First three letters: owner permissions.
- Second three letters: group permissions.
- Third three letters: public permissions.
- Also represented using numbers:
    - 4: read.
    - 2: write.
    - 1: execute.
    - -rwxrw-r-- = 764.



Symbolic Notation	Numeric Notation	English
`----------`	0000	no permissions
`-rwx------`	0700	**read, write, & execute only for owner**
`-rwxrwx---`	0770	read, write, & execute for owner and group
`-rwxrwxrwx`	0777	read, write, & execute for owner, group and others
`---x--x--x`	0111	execute
`--w--w--w-`	0222	write
`--wx-wx-wx`	0333	write & execute
`-r--r--r--`	0444	read
`-r-xr-xr-x`	0555	read & execute
`-rw-rw-rw-`	0666	read & write
`-rwxr-----`	0740	owner can read, write, & execute; group can only read; others have no permissions

Test your knowledge!

What does the permission code 600 represent?

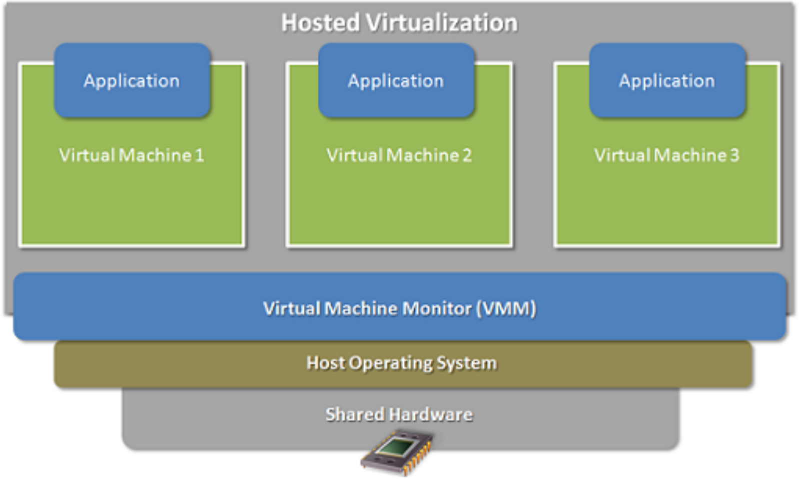
Test your knowledge!

What does the permission code 600 represent?

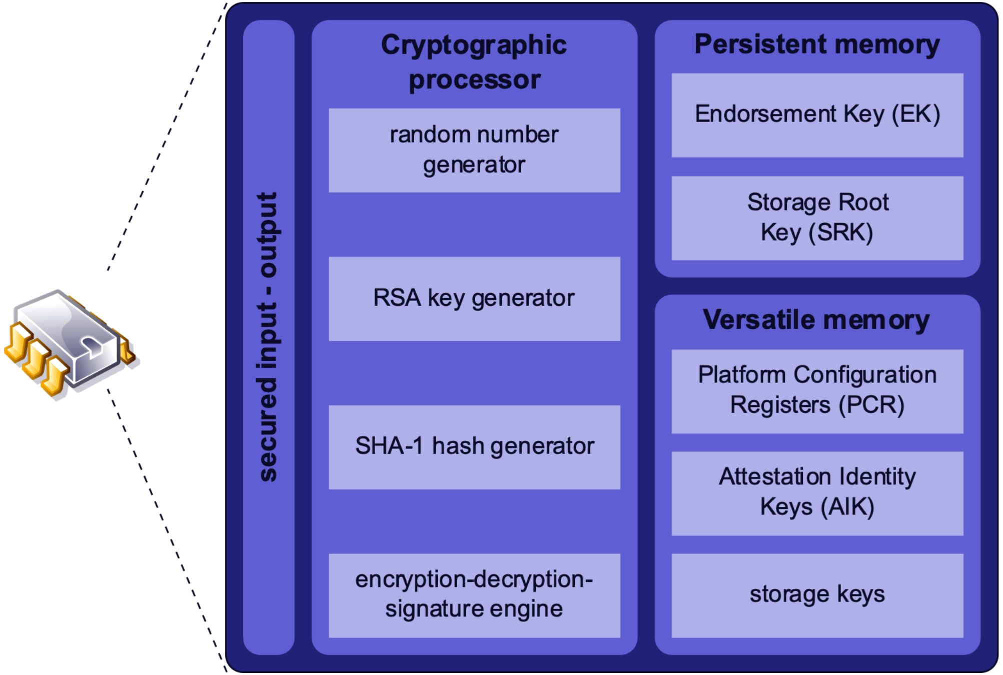
Only the owner may read or write, but not execute. Group and public can do nothing. (-rw-------).

Isolation in operating systems.

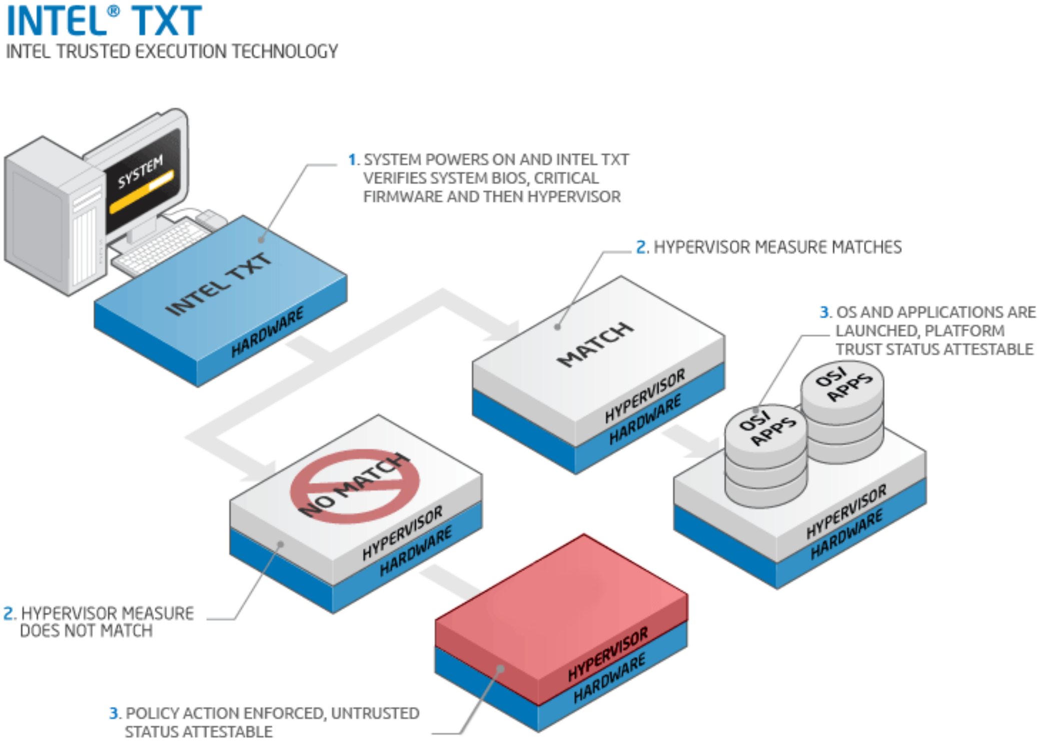
- Chroot: Limits file system view.
- FreeBSD jails, Linux containers:
  - Limit network access.
  - Limit file system, device access…
- Virtualization.



Intel Trusted Platform Module (TPM).



Intel Trusted Execution.



INTEL® TXT
INTEL TRUSTED EXECUTION TECHNOLOGY

1. SYSTEM POWERS ON AND INTEL TXT VERIFIES SYSTEM BIOS, CRITICAL FIRMWARE AND THEN HYPERVISOR

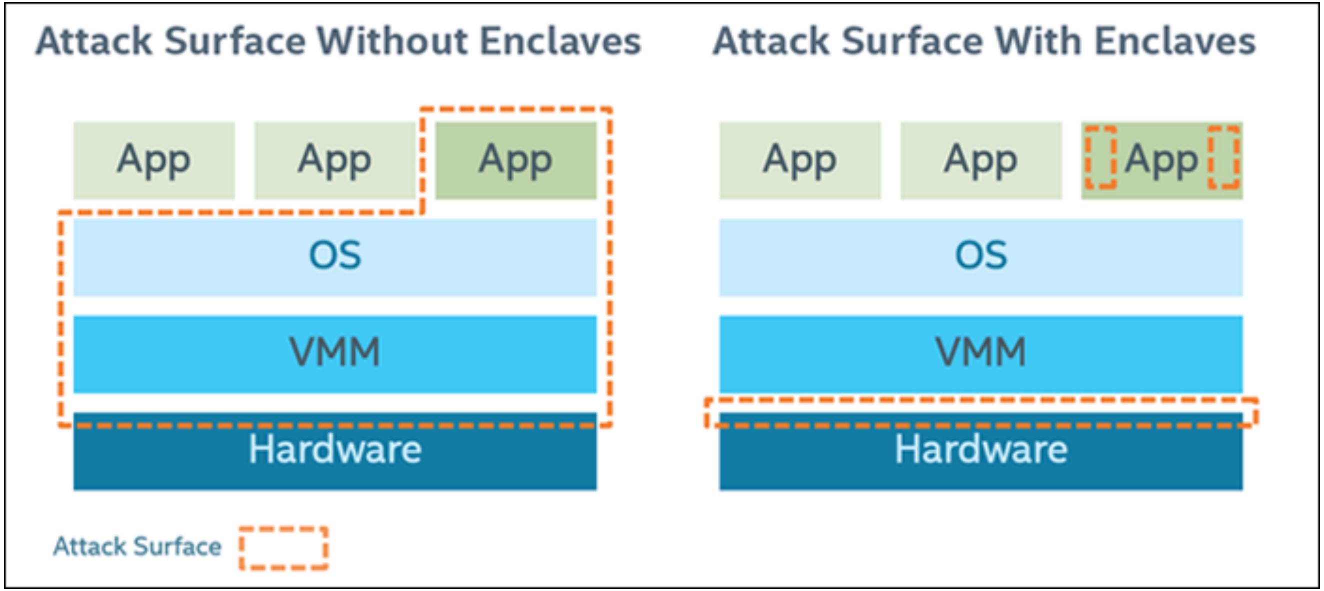
2. HYPERVISOR MEASURE MATCHES

3. OS AND APPLICATIONS ARE LAUNCHED, PLATFORM TRUST STATUS ATTESTABLE

2. HYPERVISOR MEASURE DOES NOT MATCH

3. POLICY ACTION ENFORCED, UNTRUSTED STATUS ATTESTABLE

Intel Software Guard Extensions (SGX).



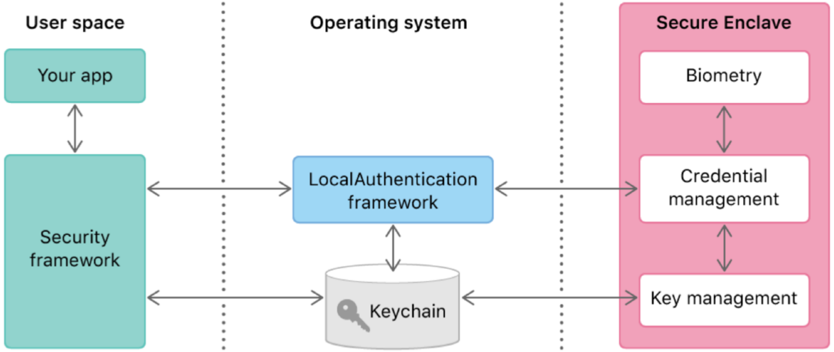
Case Study: Apple T2 Chip

3.3b

Apple T2 Chip: Secure Enclave Component.

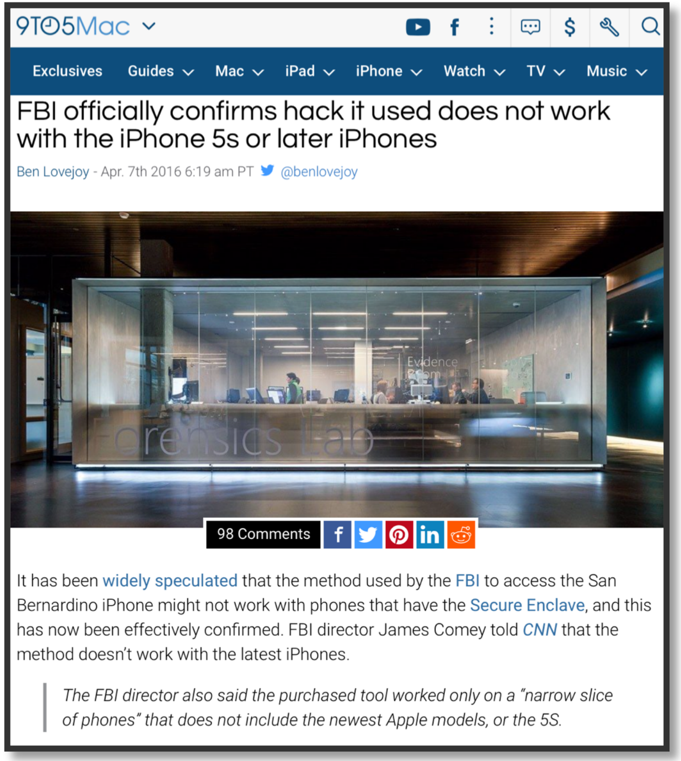
Secure enclave:

- Self-contained, independent computer with its own ”jurisdiction”.
- Encrypted memory.
- Hardware-based *true* random number generator.
- Even of system kernel/CPU is compromised, Secure Enclave maintains integrity.
- Resistant to reverse engineering/forensic analysis.



Apple T2 Chip: Secure Enclave Component.

- Design benefits:
- Hardware lock dependent on user events/password entry.
- Secure key wiping.
- Brute force attack protection.
- Fingerprint data stored inside Secure Enclave, not visible to actual device.
- Can hardware-disconnect microphone.
- Encryption keys never exposed to CPU!



FBI officially confirms hack it used does not work with the iPhone 5s or later iPhones

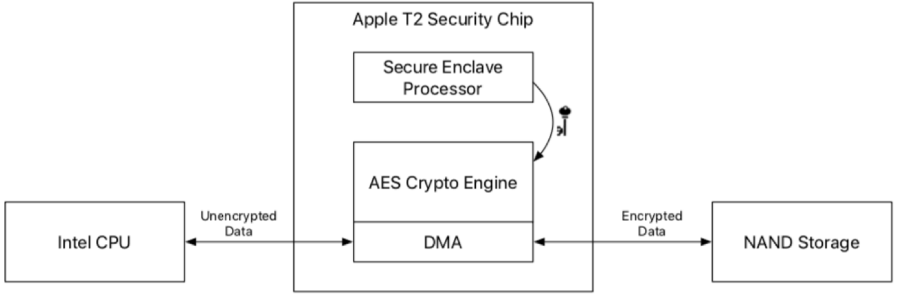
Ben Lovejoy - Apr. 7th 2016 6:19 am PT @benlovejoy

It has been widely speculated that the method used by the FBI to access the San Bernardino iPhone might not work with phones that have the Secure Enclave, and this has now been effectively confirmed. FBI director James Comey told *CNN* that the method doesn't work with the latest iPhones.

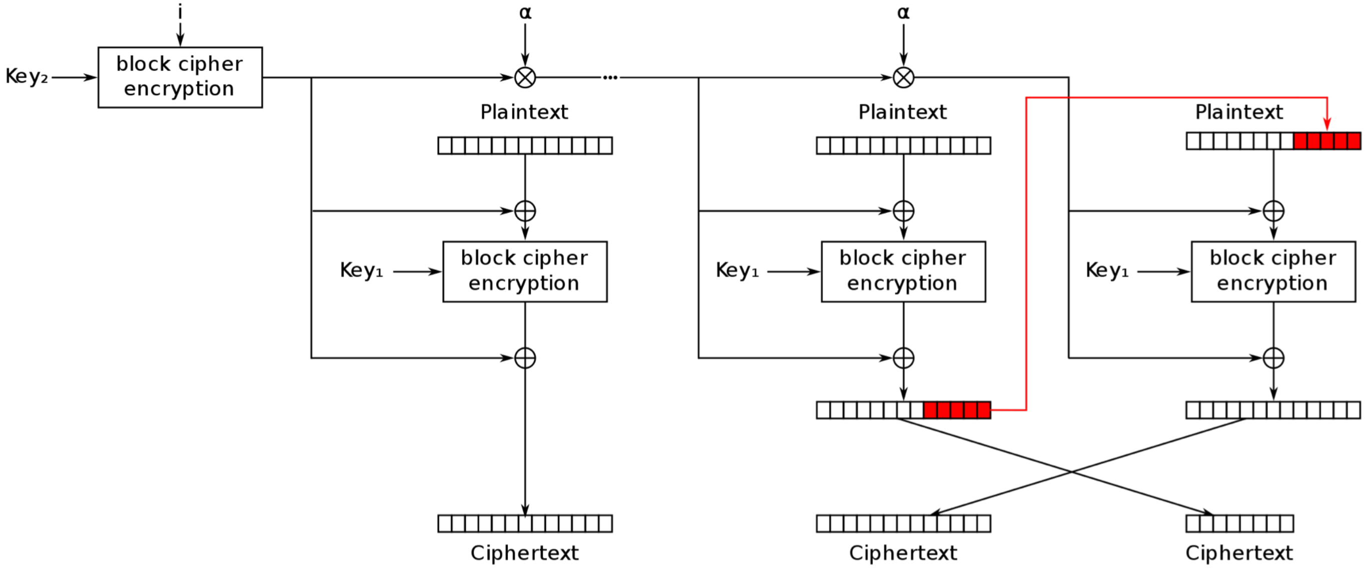
> *The FBI director also said the purchased tool worked only on a "narrow slice of phones" that does not include the newest Apple models, or the 5S.*

Apple T2 Chip: Core Concepts.

- File encryption engine built into the DMA path between flash storage and main system memory.
  - *DMA: Direct Memory Access (access RAM without going through CPU.)*
- Each Mac has a unique UID and AES keys baked in at the factory.
  - Secure enclave design prohibits key extraction.
  - Keys generated *within* secure enclave.



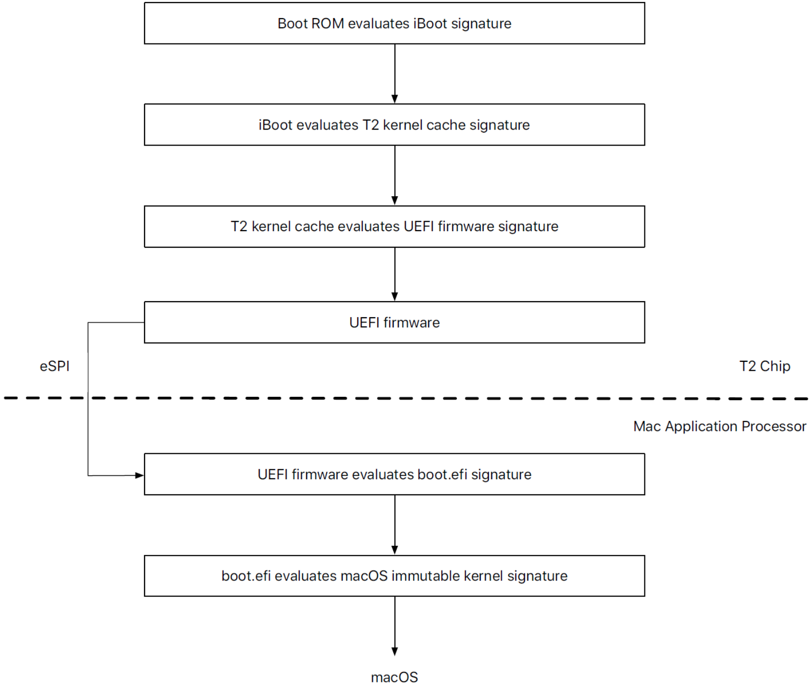
AES-XTS: Used only for disk encryption.



XEX with tweak and ciphertext stealing (XTS) mode encryption

Goal: prevent targeted malleability (easier in other modes such as CBC, CTR.)

Apple Secure Boot.



Boot ROM evaluates iBoot signature
iBoot evaluates T2 kernel cache signature
T2 kernel cache evaluates UEFI firmware signature
UEFI firmware
eSPI
T2 Chip
Mac Application Processor
UEFI firmware evaluates boot.efi signature
boot.efi evaluates macOS immutable kernel signature
macOS

Test your knowledge!

Can you think of any daily use applications with keys that macOS would benefit from storing inside T2/Secure Enclave?

Test your knowledge!

Can you think of any daily use applications with keys that macOS would benefit from storing inside T2/Secure Enclave?

Test your knowledge!

Can you think of any daily use applications with keys that macOS would benefit from storing inside T2/Secure Enclave?

File encryption
with APFS

Long-term keys
for encrypted calls

Long-term keys
For secure messaging

Code signing keys

Next time: Mobile Security

3.4