Unpacking the iOS Sandbox

Yarden Hamami

Presented at OBTS
15/10/2025, Ibiza

Cellebrite labs

Who am I?

I'm an iOS security researcher at

Cellebrite >labs

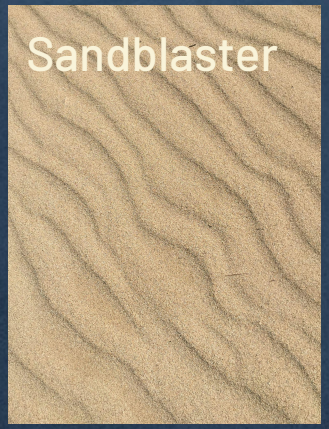
- Working at Cellebrite since 2017
- 4 as digital forensics researcher
- 3 as iOS vulnerability researcher

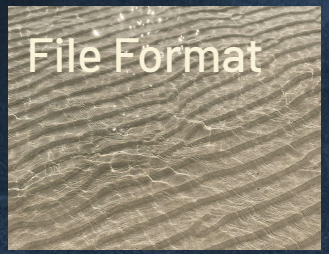


@yarden_ha

Agenda









What is Sandbox?

- Security mechanism
- Protects system resources such as filesystem, xpc services, syscalls
- Implemented in kernel level

Motivation?

- Set of rules
- Aid identifying vulnerabilities
- Quickly determine your strategy
- Different processes different rules

Goal: Decompile Sandbox profiles

Tool: Sandblaster

Sandblaster

"SandBlaster is a tool for decompiling binary Apple Sandbox profiles.

Apple Sandbox profiles are written in SBPL (*Sandbox Profile Language*),

a Scheme-like language, and are then compiled into an undocumented binary format.

SandBlaster is a tool that reverses binary Sandbox profiles

to their original SBPL format and supports up to iOS 11."

Sandblaster

“Sandbox profiles are extracted from the kernel sandbox extension.”

“python reverse_sandbox.py -r 9.3 -o ../helpers/iPhone5,1_9.3_13E237.sb_ops -d iPhone5,1_9.3_13E237.reversed_profiles/ ../helpers/sandbox_bundle”

```
platform_profile = (__int64)&platform_profile_data;
profile_size = 0x19389LL;
word_FFFFFFF007D41A8C = 0;
xmmword_FFFFFFF007D41A78 = (__int128)vdupq_n_s64(0x2CuLL);
word_FFFFFFF007D41A90 = 0;
byte_FFFFFFF007D41A93 = 0;
unk_FFFFFFF007D41A60 = xmmword_FFFFFFF0076FFDE0;
qword_FFFFFFF007D41A70 = 0xB958LL;
result = ((__int64 (__fastcall *)(__int64 *))variables_populate)(&platform_profile);
if ( (_DWORD)result
  || (result = re_cache_init(&platform_profile, 9LL), (_DWORD)result)
  || (result = profile_populate_syscall_masks((struct_sandbox_parser *)&platform_profile), (_DWORD)result) )
{
  panic("\"failed to initialize platform sandbox: %d\" @%s:%d", result, "kext.c", 5919LL);
```

```
_operation_names.509 DCQ aDefault_18     ; DATA XREF: ____ZL17iofilter_resolverP4
                                         ; ____ZL17iofilter_resolverP4taskP12IOUs
                                         ; "default"
                     DCQ aAppleeventSend ; "appleevent-send"
                     DCQ aAuthorizationR ; "authorization-right-obtain"
                     DCQ aBootArgSet     ; "boot-arg-set"
                     DCQ aDevice_7       ; "device*"
                     DCQ aDeviceCamera   ; "device-camera"
                     DCQ aDeviceMicropho ; "device-microphone"
                     DCQ aDarwinNotifica ; "darwin-notification-post"
                     DCQ aDistributedNot ; "distributed-notification-post"
                     DCQ aDynamicCodeGen ; "dynamic-code-generation"
                     DCQ aFile_8         ; "file*"
                     DCQ aFileChroot     ; "file-chroot"
                     DCQ aFileClone      ; "file-clone"
                     DCQ aFileIoctl      ; "file-ioctl"
                     DCQ aFileIssueExten ; "file-issue-extension"
                     DCQ aFileLink       ; "file-link"
                     DCQ aFileMapExecuta ; "file-map-executable"
                     DCQ aFileMknod      ; "file-mknod"
                     DCQ aFileMount      ; "file-mount"
                     DCQ aFileMountUpdat ; "file-mount-update"
                     DCQ aFileRead       ; "file-read*"
                     DCQ aFileReadData   ; "file-read-data"
                     DCQ aFileReadMetada ; "file-read-metadata"
                     DCQ aFileReadXattr  ; "file-read-xattr"
                     DCQ aFileRevoke     ; "file-revoke"
                     DCQ aFileSearch     ; "file-search"
                     DCQ aFileTestExiste ; "file-test-existence"
                     DCQ aFileUnmount    ; "file-unmount"
                     DCQ aFileWrite      ; "file-write*"
                     DCQ aFileWriteAcl   ; "file-write-acl"
                     DCQ aFileWriteCreat ; "file-write-create"
                     DCQ aFileWriteData  ; "file-write-data"
                     DCQ aFileWriteFinde ; "file-write-finderinfo"
                     DCQ aFileWriteFlags ; "file-write-flags"
                     DCQ aFileWriteMode  ; "file-write-mode"
                     DCQ aFileWriteOwner ; "file-write-owner"
                     DCQ aFileWriteSetug ; "file-write-setugid"
                     DCQ aFileWriteTimes ; "file-write-times"
```



```
(version 1)
(allow default)
(deny dynamic-code-generation
    (require-not (entitlement-is-bool-true "b'dynamic-codesigning'"))
    (require-not (process-attribute is-sandboxed))
    (process-attribute is-protoboxed))
(deny file-chroot
    (require-all
        (require-not (storage-class-extension 0))
        (require-any
            (file-attribute datavault)
            (process-attribute is-initproc)
            (process-attribute is-installer)
            (process-attribute is-datavault-controller)
            (process-attribute is-initproc)
            (process-attribute is-installer)
            (process-attribute is-datavault-controller)
            (require-all
                (storage-class "b'PassKit'")
                (require-any
                    (process-attribute is-initproc)
                    (process-attribute is-installer)
                    (process-attribute is-datavault-controller)
                    (require-not (entitlement-is-bool-true "b'com.apple.private.secu
            (require-all
                (entitlement-is-bool-true "b'com.apple.private.security.storage.sysd
```

File Format

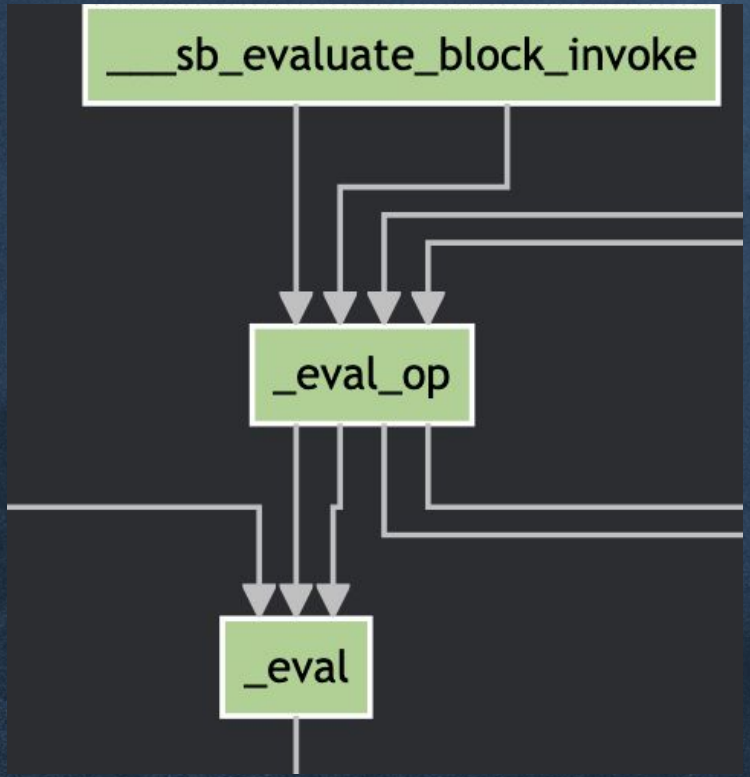
Compile custom profile

Reverse the parsing process done in the Kernel

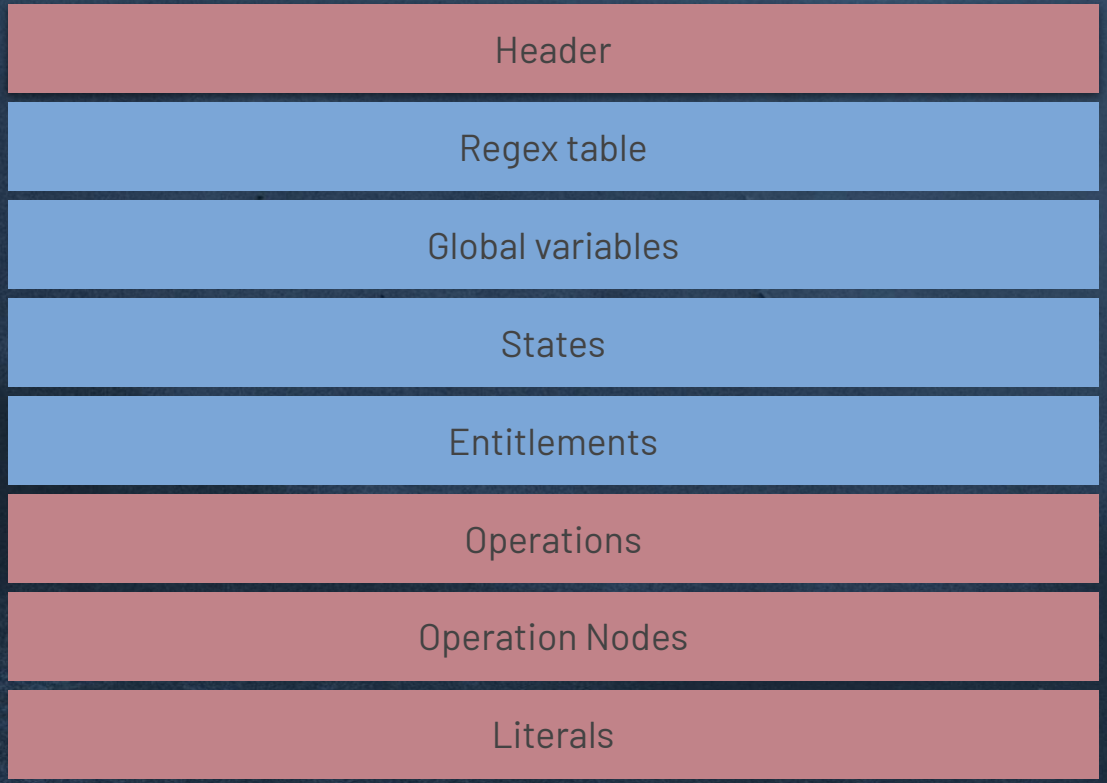
File Format

- Platform Profile
- Built in collection
- Protobox collection

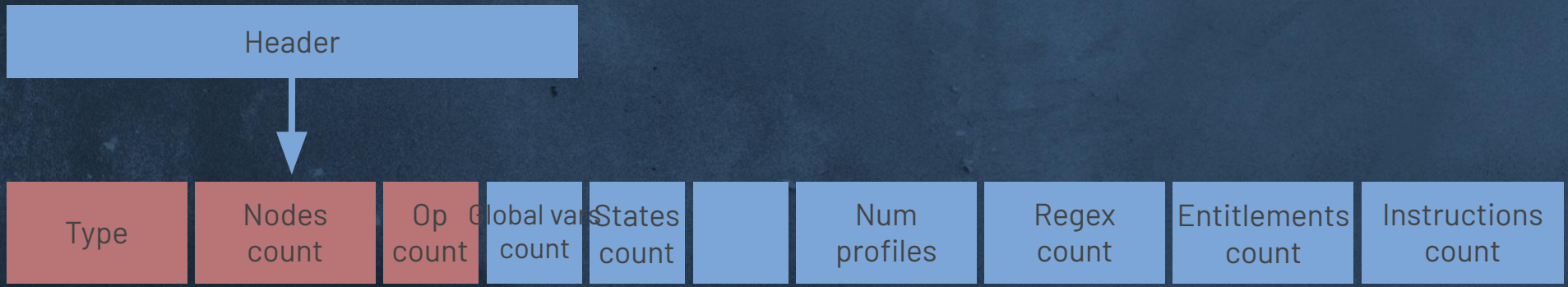
File Format



File Format


Header
Regex table
Global variables
States
Entitlements
Operations
Operation Nodes
Literals

File Format



Operation Nodes:

The actual rules

Operations:

List of syscalls to restrict

File Format

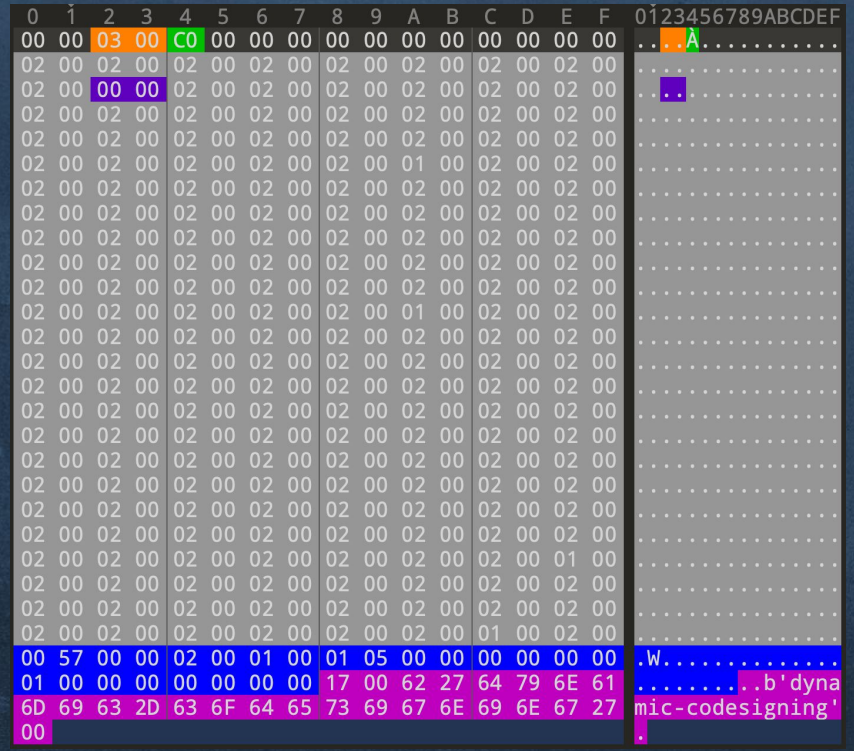
```
1  (version 1)
2  (allow default)
3  (deny dynamic-code-generation
4      (require-not (entitlement-is-bool-true "b'dynamic-codesigning'")))
```

Operation:

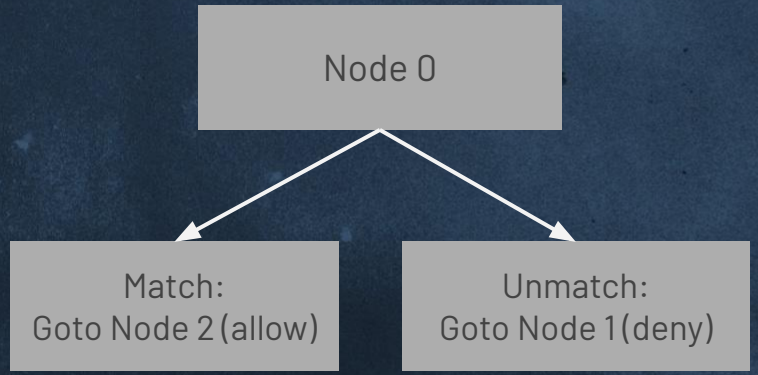
dynamic-code-generation

File Format

- Number of operation nodes
- Number of operations
- Operations table
- Operation nodes
- Literals

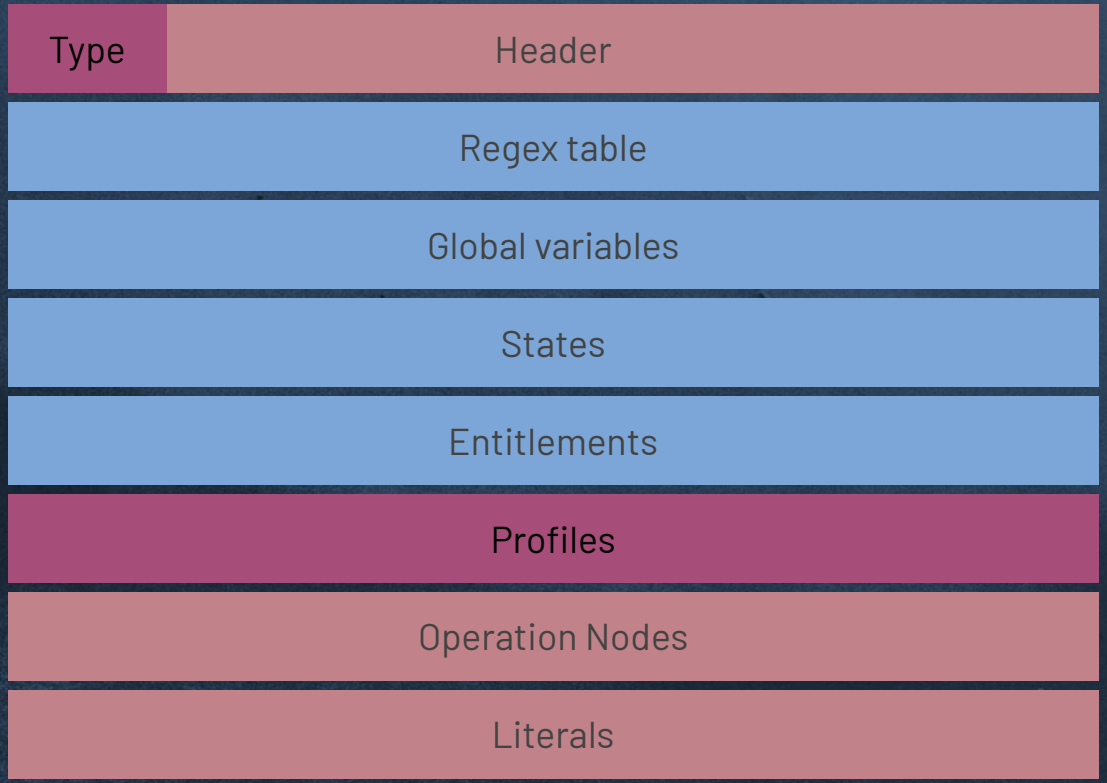

0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
00 00 03 00 C0 00 00 00 00 00 00 00 00 00 00 00
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00
02 00 00 00 02 00 02 00 02 00 02 00 02 00 02 00
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00
02 00 02 00 02 00 02 00 02 00 01 00 02 00 02 00
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00
02 00 02 00 02 00 02 00 02 00 01 00 02 00 02 00
02 00 02 00 02 00 02 00 02 00 02

File Format

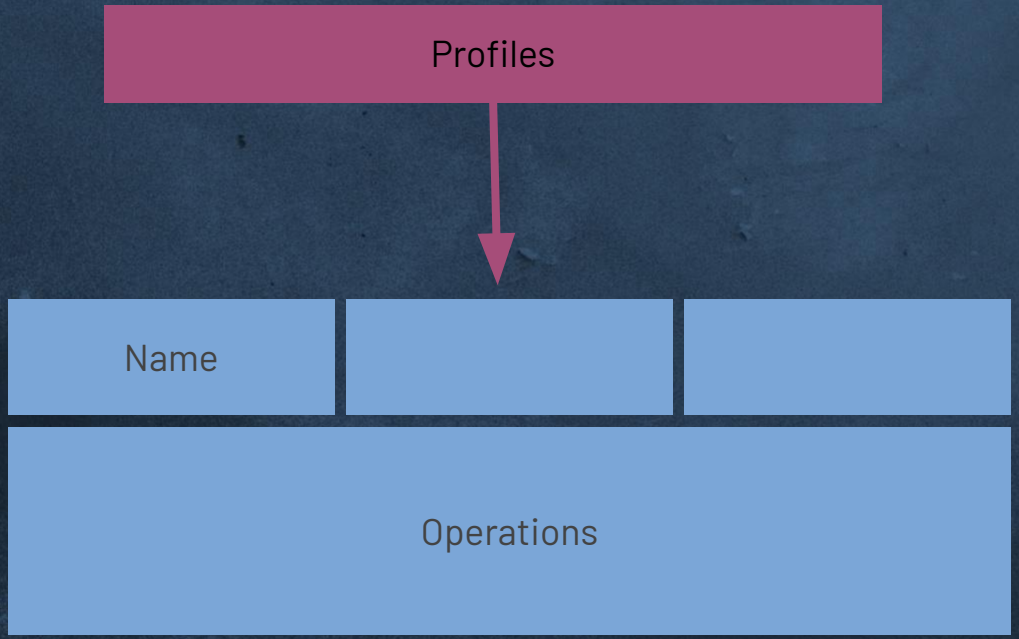



```
 0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
00 00 03 00 C0 00 00 00 00 00 00 00 00 00 00 00 ....A...........
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 00 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 01 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 01 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 02 00 01 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 02 00 02 00 ................
02 00 02 00 02 00 02 00 02 00 02 00 01 00 02 00 ................
00 57 00 00 02 00 01 00 01 05 00 00 00 00 00 00 .W..............
01 00 00 00 00 00 00 00 17 00 62 27 64 79 6E 61 ..........b'dyna
6D 69 63 2D 63 6F 64 65 73 69 67 6E 69 6E 67 27 mic-codesigning'
00 |                                             .
```

File Format


Type
Header
Regex table
Global variables
States
Entitlements
Profiles
Operation Nodes
Literals

File Format



The Output Challenge

```
(deny file-chroot
    (require-all
        (require-not (storage-class-extension 0))
        (require-any
            (file-attribute datavault)
            (process-attribute is-initproc)
            (process-attribute is-installer)
            (process-attribute is-datavault-controller)
            (process-attribute is-initproc)
            (process-attribute is-installer)
            (process-attribute is-datavault-controller)
            (require-all
                (storage-class "b'PassKit'")
                (require-any
                    (process-attribute is-initproc)
                    (process-attribute is-installer)
                    (process-attribute is-datavault-controller)
                    (require-not (entitlement-is-bool-true "b'com.apple.private.security.storage.PassKit'"))))
            (require-all
                (entitlement-is-bool-true "b'com.apple.private.security.storage.sysdiagnose'")
                (require-not (subpath "/private/var/db/sysdiagnose")))
            (require-all
                (storage-class "b'DiagnosticReports'")
                (require-any
                    (process-attribute is-initproc)
                    (process-attribute is-installer)
                    (process-attribute is-datavault-controller)
                    (entitlement-is-bool-true "b'com.apple.private.security.storage.DiagnosticReports'")
                    (require-not (entitlement-is-bool-true "b'com.apple.private.security.storage.DiagnosticReports.read-write'"))))
            (require-all
                (storage-class "b'DoNotDisturb'")
                (require-any
                    (process-attribute is-initproc)
                    (process-attribute is-installer)
                    (process-attribute is-datavault-controller)
                    (entitlement-is-bool-true "b'com.apple.rootless.storage.DoNotDisturb'")
                    (require-not (entitlement-is-bool-true "b'com.apple.private.security.storage.DoNotDisturb'"))))
            (require-all
                (storage-class "b'sysdiagnose.sysdiagnose'")
                (require-any
                    (process-attribute is-initproc)
                    (process-attribute is-installer)
                    (process-attribute is-datavault-controller)
                    (entitlement-is-bool-true "b'com.apple.private.security.storage.sysdiagnose.sysdiagnose'")
                    (require-not (entitlement-is-bool-true "b'com.apple.rootless.storage.sysdiagnose.sysdiagnose'"))))
            (require-all
                (storage-class "b'Weather'")
                (require-any
                    (process-attribute is-initproc)
                    (process-attribute is-installer)
```

The Output Challenge

@LIJI32

“It’s only a set of If else if else”

We will use C code

```
_int64 file_chroot()

bool v262; // w8
bool v299; // w8
bool v440; // w8
bool v472; // w8
bool v474; // w8
bool v475; // w8

if ( storage_class_extension("0") )
  return allow("");
if ( file_attribute("datavault") != 0 )
  return deny("sip-override");
if ( file_attribute("sip-protected") != 0 )
  return allow("");
if ( storage_class("os_eligibility") )
{
  if ( process_attribute("is-initproc") == 0
    && process_attribute("is-installer") == 0
    && process_attribute("is-datavault-controller") == 0
    && entitlement_is_bool_true("com.apple.private.security.storage.os_eligibility") == 0
    && entitlement_is_bool_true("com.apple.private.security.storage.os_eligibility.readwrite") == 0 )
  {
    return deny("sip-override");
  }
}
else if ( storage_class("PassKit") == 0 )
{
  if ( storage_class("DiagnosticReports") == 0 )
  {
    if ( storage_class("DoNotDisturb") == 0 )
    {
      if ( storage_class("Weather") == 0 )
      {
        if ( storage_class("SoundProfileAsset") == 0 )
        {
          if ( storage_class("fpsd") == 0 )
          {
            if ( storage_class("SiriSELF") == 0 )
            {
```

The Output Challenge

@LIJI32

“It’s only a set of If else if else”

We will use C code

@cjori - Automated parsing helper

iOS 18 Changes

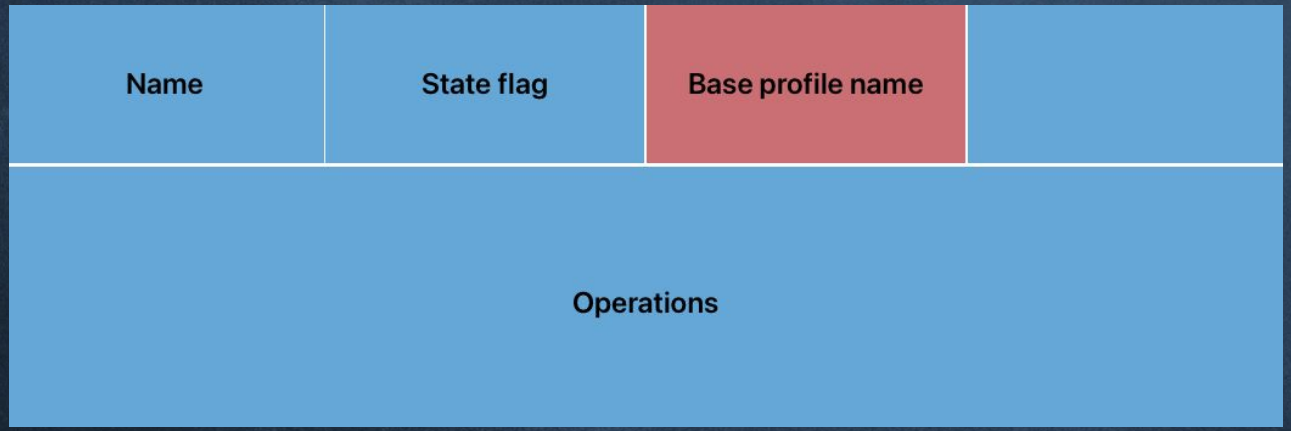
```
collection_init(&autobox_collection, aAutoboxCollect, &autobox_data, 0xB4B49LL, sub_
_DWORD)v54 )

4:
= sub_FFFFFFF008524B38("\"failed to initialize autobox collection: %d\" @%s:%d", v54
```

```
actions         DCQ aDeny


                DCQ aAllow
                DCQ aDelegate
                DCQ aAutobox
```

iOS 18 Changes



Future Goals

- Sandbox extensions
- States layer
- Unknown file format data

Thank you!

@yarden_ha



Cellebrite

Cellebrite >labs