Unconventional use for a BootROM exploit

@1nsane_dev

whoami

Former iDevice HWSW Technician/Consultant,

Internetwork Expert System Engineer, now Technical Project Manager

arm and iOS enthusiast

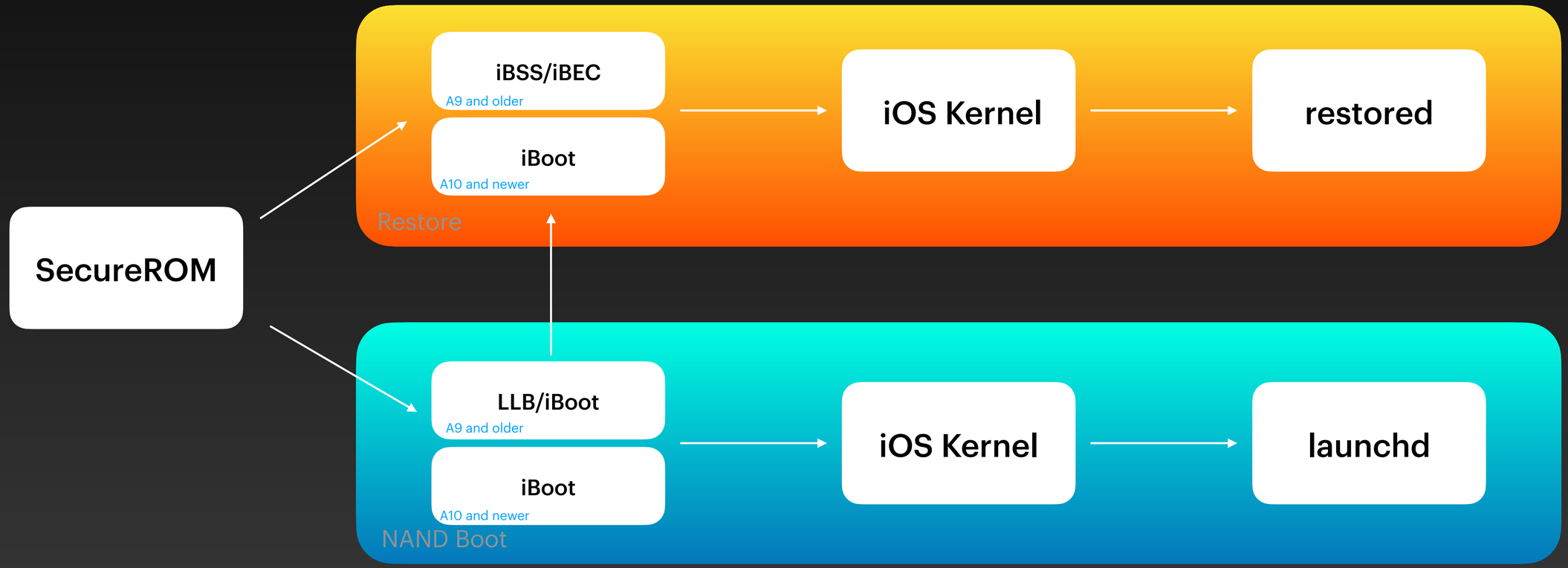
Recently started exploring iOS internals

Agenda

- iOS Security Model
  - Bootchain
  - secure-boot
  - ASN.1 IMG4
- iOS Activation
  - System Config
  - Activation
- Classic servicing procedure
  - Hardware binding
  - Replacing WIFI IC
- A different Approach
  - Attacking secure-boot
  - Booting the Image
  - Control SysCfg
  - Pros
- Automation
  - Purple.app
  - Demo

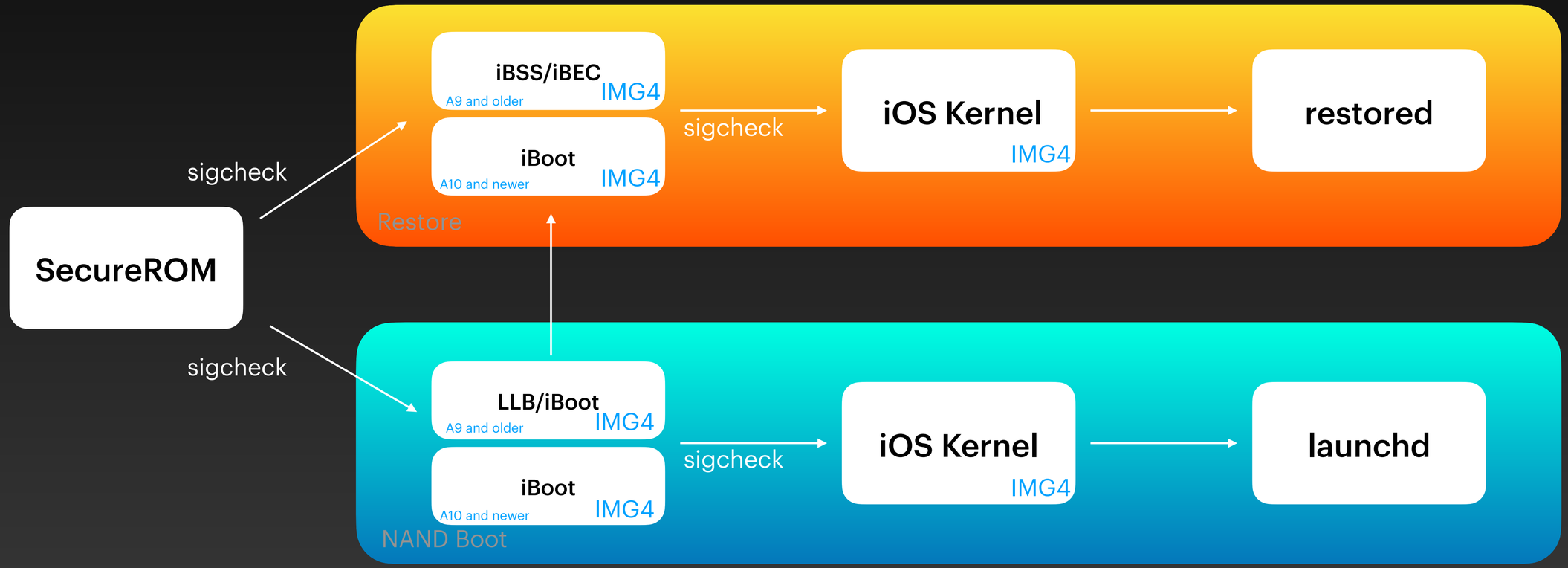
iOS Security Model

- AP bootchain



iOS Security Model

- AP secure-boot: chain of trust



iOS Security Model

- ASN.1 IMG4: IM4P (Payload) + IM4M (Manifest)

```
sequence [
   0: string "IM4P"
   1: string type    - ibot, rdsk, sepi, ...
   2: string description    - 'iBoot-1940.1.75'
   3: octetstring    - the encrypted/raw data
   4: octetstring    - containing DER encoded KBAG values (optional)
         sequence [
            sequence [
                0: int: 01
                1: octetstring: iv
                2: octetstring: key
            ]
            sequence [
                0: int: 02
                1: octetstring: iv
                2: octetstring: key
            ]
         ]
      ]
```

```
sequence [
   0: string "IM4M"
   1: integer version    - currently 0
   2: set [
         tag MANB [   - manifest body
             set [
                 tag MANP [   - manifest properties
                     set [
                         tag <manifest property> [
                             content
                         ]
                         ...   - tags, describing other properties
                     ]
                 ]
                 tag <type> [   - ibot, illb, sepi, krnl, NvMR, bbcl...
                     set [
                         tag <tag property> [
                             content
                         ]
                         ...
                     ]
                 ]
                 ...   - tags for other images
             ]
         ]
      ]
   3: octet string signature
   4: sequence [   - containing certificate chain (arbitrary number of certificates)
         certificates
      ]
```

iOS Activation

- System Config

Stored in NAND,

Set of key-value pairs that holds information describing the hardware of an specific unit.

```
iPhone:~ root# sysconfig read --key FCMS

Key  | Type | Data
FCMS |  STR | G8R817312UZJH842Z

iPhone:~ root#
```

```
iPhone:~ root#
iPhone:~ root#
iPhone:~ root# sysconfig info -a
Bundle Version: 16A93020j
OSDiags Root Version: (null)

Key  | Type | Actual Size | Maximum Size | Station Names                | Erase Spec                                | Description
VbCl | HEX |           0 |           20 |                VibratorPreburn |                          164 (0xA4) | Linear Vibration Calibration
COSC | HEX |           0 |           16 |                            QT1 |                          129 (0x81) | Compass Low Noise Mode Offset Compensation
DTCl | HEX |           0 |          944 |                           FATP |                          128 (0x80) | Temperature Compensation
SPPO | HEX |          56 |           80 |                          PTest |                          150 (0x96) | Single Point Pressure Offset
BTXC | HEX |           0 |         1360 |                     WifiBTCond |                           21 (0x15) | Bluetooth TX Extended Calibration
DBCl | HEX |           0 |          180 |                           FATP |                          166 (0xA6) | Backlight Current Compensation
SwBh | HEX |          16 |            4 |                                |                             None | Software Behavior Values
LSPM | HEX |         420 |          420 |                        Burnin |                          181 (0xB5) | Luna Shape PMIC Calibration
CFG# | STR |          27 |           64 |                            QT0 |                             None | Project + Build + Config
CVCC | HEX |          16 |           16 |                   CompassCal |                          129 (0x81) | Compass VBUS Compensation Coefficient
GSCi | HEX |           0 |           40 |                           IMU |                          151 (0x97) | Gyro Sensitivity calibration inverse matrix
SIFC | HEX |           0 |           28 | OrbInertial OrbCal ButtonTest ButtonCal |                  242 (0xF2) | SSHB Inverse Filter Calibration
W24G | HEX |           0 |           12 |                     WifiBTCond |                           21 (0x15) | 2.4GHz WiFi Calibration data
MiGa | HEX |          16 |           16 |                           FACT |                          162 (0xA2) | Mic Gain
W24R | HEX |           0 |           80 |                                |                             None | 2.4GHz WiFi Receive Calibration data
LFBN | STR |           0 |            4 |                            QT0 |                          128 (0x80) | Luna Functional Bin
MdlC | STR |          88 |          256 |                           FATP | [128 (0x80), 253 (0xFD)] | Module Configuration Information
LSPr | HEX |         420 |          420 |                         OrbCal |                          168 (0xA8) | Luna Shape Pressure Calibration
MLB# | STR |          16 |           17 |                            All |   [0 (0x00), 253 (0xFD)] | Main Logic Board Serial Number
WRxT | HEX |           0 |            1 |                                |                             None | WiFi Receive Temperature Calibration
Regn | STR |           3 |            5 |                           FATP | [128 (0x80), 253 (0xFD)] | Region Code string for the Marketing Part Number
ASCi | HEX |           0 |           40 |                           IMU |                          151 (0x97) | Accelerometer Sensitivity calibration inverse matrix
DClr | HEX |           0 |           16 |                           FATP | [128 (0x80), 253 (0xFD)] | Device Enclosure and Cover Glass Color in RGB.
PxCl | HEX |         144 |          144 |                       ProxCal |                          198 (0xBE) | Prox calibration data
LAFE | HEX |         100 |          100 |                            QT0 |                          128 (0x80) | Luna Analog Front End Calibration
AlsC | HEX |           0 |           80 |          ALSCal DFUNandInit |                          153 (0x99) | ALS Calibration Data
OPTS | STR |           0 |          256 |                           FATP | [128 (0x80), 253 (0xFD)] | HW Configuration Options
LSCI | HEX |           0 |          200 |     ALSAR ALSCal ALSTest |                          153 (0x99) | Light Sensor Calibration
GYTT | HEX |          98 |          256 |                        Burnin |                          181 (0xB5) | Gyro Temperature Table
NSrN | HEX |           0 |           20 |                           FATP | [128 (0x80), 253 (0xFD)] | Finger Print Sensor Serial Number
PRTT | HEX |           0 |          256 |                        Burnin |                          181 (0xB5) | Phosphorus Temperature Compensation Table
PrCL | HEX |         256 |          256 |                                |                          128 (0x80) | Pearl Calibration
VPBR | HEX |           0 |            4 |                            FCT |                            1 (0x01) | Speaker Amp Brownout Voltage
NoCl | HEX |          16 |            2 |                           FATP | [128 (0x80), 253 (0xFD)] | Disable writing calibration data
LFCL | HEX |       37928 |        37928 |                         OrbCal |                          168 (0xA8) | Luna Force Calibration
LSFN | HEX |           0 |          420 |                        Burnin |                          181 (0xB5) | Luna Shape Flex Noise Calibration
LSGC | HEX |           0 |          420 |                        Burnin |                          181 (0xB5) | Luna Shape Graphical Calibration
PSCl | HEX |         592 |          592 |       QT0 VibratorPreburn |                          164 (0xA4) | Hall Effect Position Sensor Calibration
RMd# | STR |           5 |           16 |                                |                             None | Regulatory Model Number
ARot | HEX |          16 |           16 |                           IMU |                          151 (0x97) | Accelerometer Rotation
BTTx | HEX |           0 |           20 |                     WifiBTCond |                           21 (0x15) | Bluetooth Transmit Calibration
SpCl | HEX |           0 |           60 |                        Burnin |                          181 (0xB5) | Speaker Impedance Calibration
PACV | HEX |           0 |          150 |                           FCT |                            1 (0x01) | Power Management Unit Analog-to-Digital Converter Calibration
W50G | HEX |           0 |           36 |                     WifiBTCond |                           21 (0x15) | 5GHz WiFi Calibration data
FG2G | HEX |           0 |            8 |                                |                             None | Frequency Group 2G WiFi Calibration data
CmCl | HEX |           0 |         2048 |          CameraPostBurn2 |                             None | Camera Banding calibration data
OICo | HEX |           0 |          600 |                           IMU |                             None | Pressure Sensitive Internal Compensation
BMac | HEX |          16 |            6 |                                |                             None | Bluetooth MAC address
FCMS | STR |          17 |           17 |                           FATP | [128 (0x80), 253 (0xFD)] | Front Camera Serial Number
MVCB | HEX |           0 |           84 |                           FCT |                            1 (0x01) | Buck Input Current Limit
GLCl | HEX |           0 |          300 |                      RGBW iSD |                          166 (0xA6) | Gamma Look Up Table Calibration
SpGa | HEX |          16 |           16 |                           FACT |                          162 (0xA2) | Speaker Gain
Batt | STR |          17 |           32 |                           FATP | [128 (0x80), 253 (0xFD)] | Battery Serial Number
W50R | HEX |           0 |           96 |                                |                             None | 5GHz WiFi Receive Calibration data
SpNL | HEX |           0 |           94 |                        Burnin |                          181 (0xB5) | Speaker Nonlinearity Calibration
LTAO | HEX |          20 |           20 |                           IMU |                          151 (0x97) | Low temperature Accelerometer zero offset
BLCl | HEX |           0 |           16 |                      RGBW iSD |                          166 (0xA6) | Display Backlight brightness calibration
FCMB | STR |          64 |           64 |                           FATP | [128 (0x80), 253 (0xFD)] | Front Camera NVRAM configuration
PTPM | STR |           0 |           16 |                          RACK2 |                          144 (0x90) | Pearl Time Zero Performance
AICl | HEX |          16 |           16 |                           IMU |                          151 (0x97) | Accelerometer Interrupt Calibration
LPMp | HEX |         492 |          492 |                            QT0 |                          128 (0x80) | Luna Pixel Map
CDCC | HEX |          16 |           16 |                            QT1 |                          129 (0x81) | System level display compensation coefficient for compass sensor
McCl | HEX |           0 |          512 |                                |                             None | Multitouch chipset calibration
MtCl | HEX |        2696 |         2696 |                      GrapeCal |                          128 (0x80) | Multitouch (Grape) Calibration Data
WSKU | HEX |          16 |           16 |          DFUNandInit All |   [0 (0x00), 253 (0xFD)] | WiFi Driver Power Table SKU Identifier
CLCL | HEX |          80 |           80 |                          CTap |                          164 (0xA4) | Closed Loop Calibration
VBCA | HEX |           0 |            5 |                           FCT |                            1 (0x01) | Speaker Amp and Arc Brownout Voltage
PrAS | HEX |          28 |           28 |                           IMU |                          151 (0x97) | Pressure sensitivity to acceleration
BLCC | HEX |           0 |           56 |                           FCT |                            1 (0x01) | Backlight Current Calibration
SFCl | HEX |           0 |          884 | OrbInertial OrbCal ButtonTest ButtonCal |                  242 (0xF2) | SSHB Force Calbration
Mod# | STR |           9 |           11 |                           FATP | [128 (0x80), 253 (0xFD)] | Main part of the Marketing Part Number
GRSC | HEX |          44 |           44 |                           IMU |                          151 (0x97) | Gyroscope Range and Sensitivity Calibration
LSRx | HEX |         420 |          420 |                        Burnin |                          181 (0xB5) | Luna Shape Receiver Calibration
CLBG | HEX |           0 |           16 |                           FATP |                          128 (0x80) | Color Backing
CGSp | HEX |          16 |            8 |                           FATP | [128 (0x80), 253 (0xFD)] | Cover glass specification
THPC | HEX |           0 |           56 |     HotProbeThermalCal |                          186 (0xBA) | Turtle Hot Probe Temperature Compensation Calibration
ATSc | HEX |           0 |           20 |                          FACT1 |                          162 (0xA2) | Acoustic Transducer Scale
WTxC | HEX |           0 |         1024 |                     WifiBTCond |                           21 (0x15) | 11ac Wifi Tx Power Calibration
ARSC | HEX |          44 |           44 |                           IMU |                          151 (0x97) | Accelerometer Range and Sensitivity Calibration
GTCl | HEX |          60 |           60 |                           IMU |                          151 (0x97) | Carbon component trim calibration
VBST | HEX |           0 |            4 |                           FCT |                            1 (0x01) | Speaker Amp Boost Voltage
PRSq | HEX |          16 |            4 |                                |                             None | Factory Specific - Process Sequence
BCTR | HEX |           0 |           32 |          CameraPostBurn |                          171 (0xAB) | Back camera tilt rotation
RSCl | HEX |           0 |           16 |                                |                             None | Radio and Antenna SKU Calibration
GICl | HEX |          16 |           16 |                           IMU |                          151 (0x97) | Gyro Interrupt Calibration
RxCL | HEX |          16 |           16 |                            QT0 |                          128 (0x80) | Rosaline Calibration Current
GRot | HEX |          16 |           16 |                           IMU |                          151 (0x97) | Gyroscope Rotation
TTCL | HEX |           0 |           92 |                        Burnin |                          181 (0xB5) | Turtle Temperature Compensation
TCal | HEX |          80 |           80 |                           Tap |                          164 (0xA4) | Alert Calibration
NvSn | STR |           0 |           18 |                           QT0 |                          128 (0x80) | Finger Print Sensor Module Number
```

iOS Activation

- iOS Activation: from Setup.app to SpringBoard

https://albert.apple.com/deviceservices/deviceActivation

Validatation

Activation Token

Signed Wildcard Ticket

Validatation

lockdownd

SpringBoard

iOS Activation

- iOS Activation: from Setup.app to SpringBoard

Syscfg entries checked here

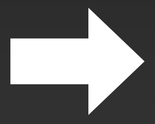
https://albert.apple.com/deviceservices/deviceActivation

Validatation

Activation Token

Signed Wildcard Ticket

Validatation



lockdownd

SpringBoard

iOS Activation

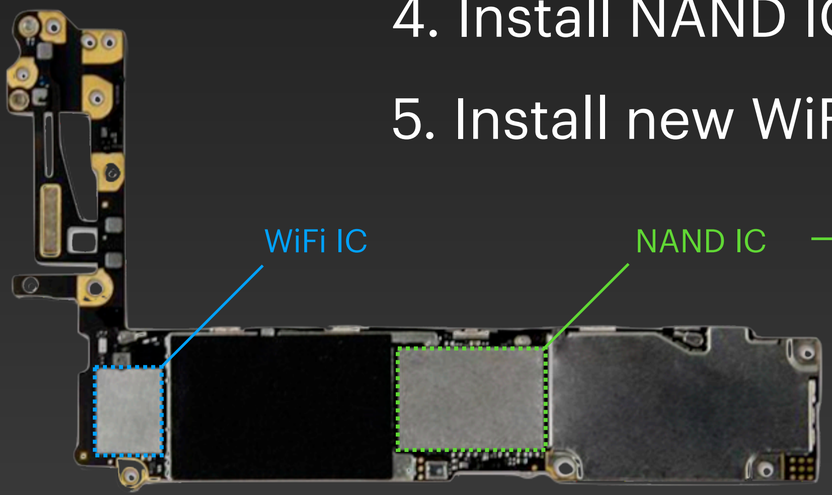
Some hardware components are linked with each other.

What if any of these components fail and need service?

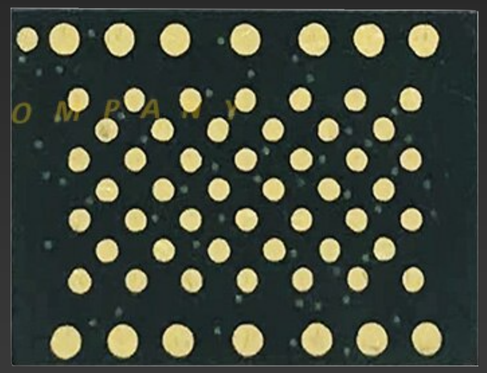
Classic servicing procedure

- Example: Replacing WiFi Integrated Circuit

1. Remove the defective WiFi IC
2. Remove NAND IC
3. Edit Syscfg data in NAND with a NAND IC Programmer tool
4. Install NAND IC back
5. Install new WiFi IC

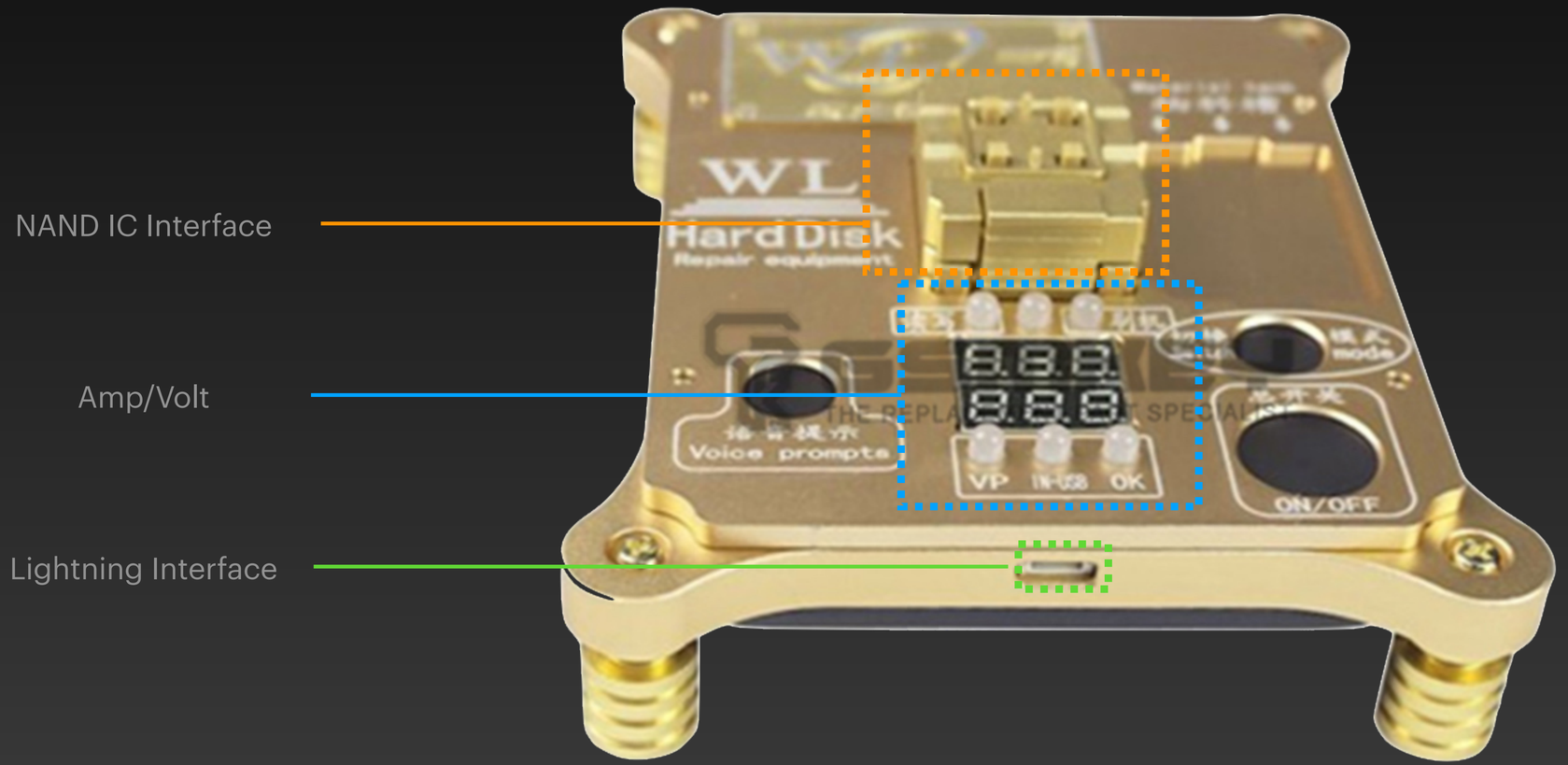


iPhone 6 motherboard



Classic servicing procedure

- NAND IC Programmers



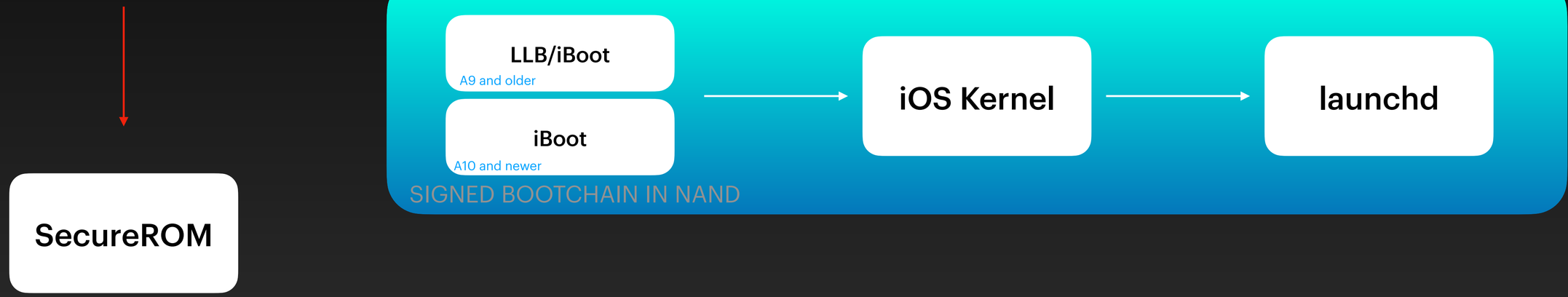
Classic servicing procedure

- Another example, upgrading iPhone storage the old way, VIDEO:

A different approach

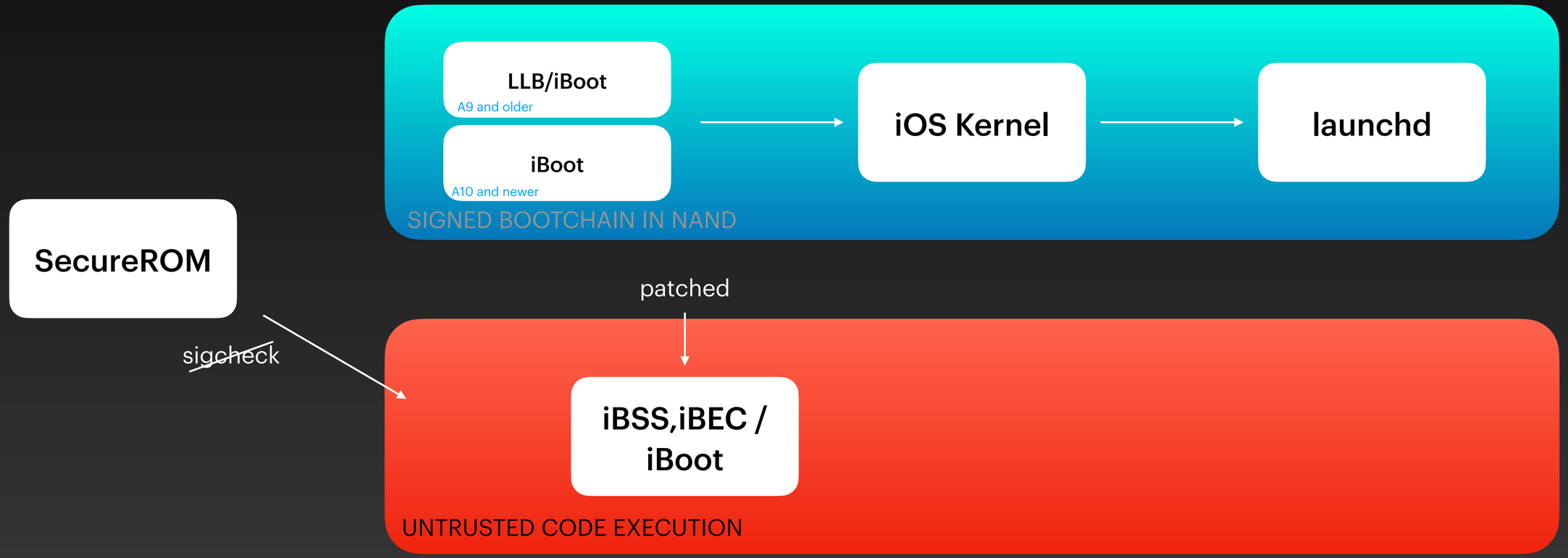
Attacking secure-boot

- checkm8



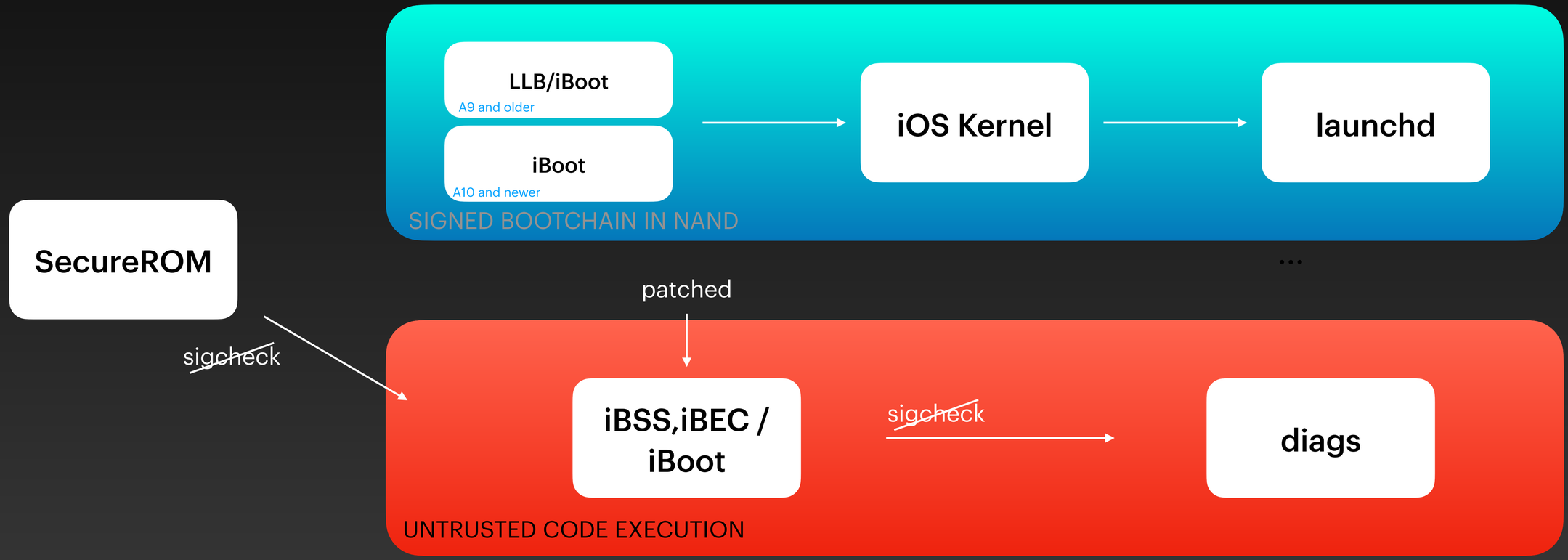
Booting the image

- Loading patched iBoot



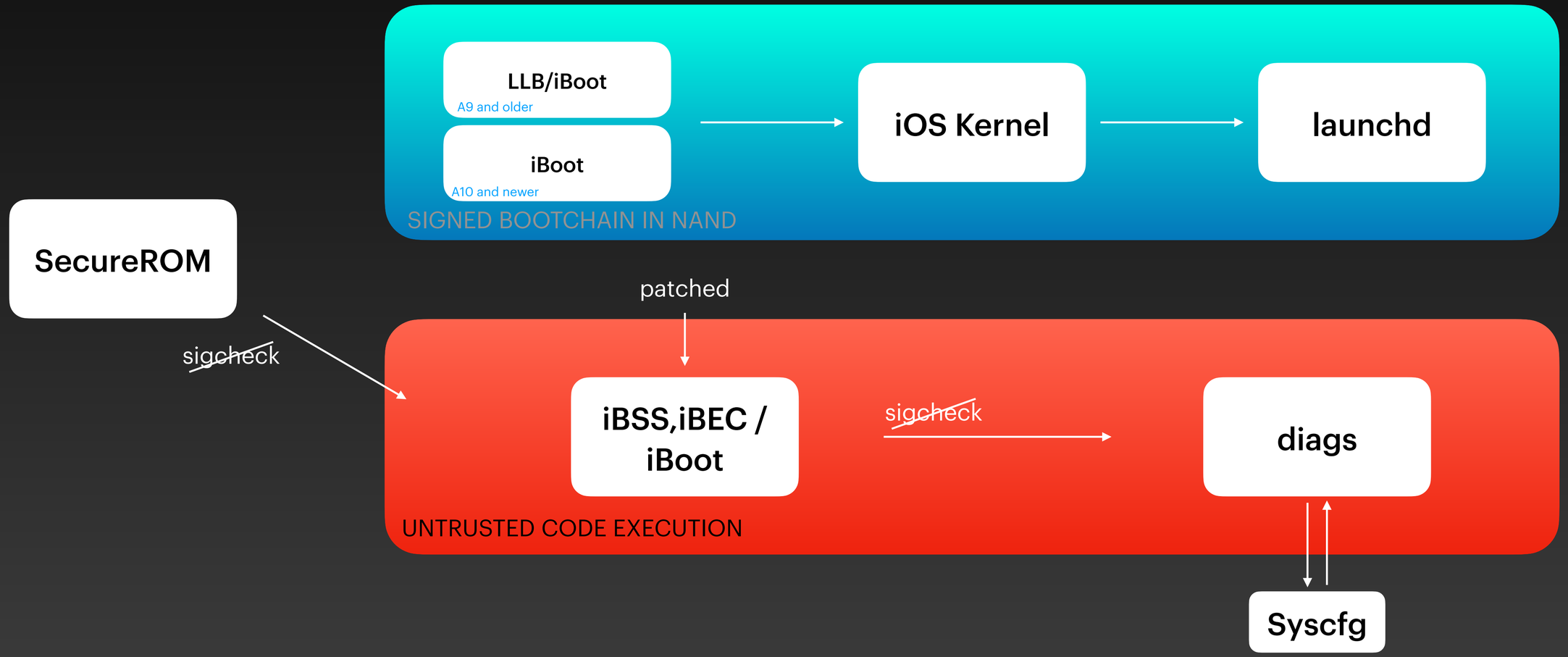
Booting the image

- Loading diags image



Booting the image

- Edit Syscfg



Control SysConfig

```
[001D358E:389A493A] :-)
[001D358E:389A493A] :-)
[001D358E:389A493A] :-) help syscfg
"syscfg" Usage: syscfg [init | add | addbyte | dump | rawdump | print | printbyte | list | type | delete | stats] <Key> <value1> <value2> ...; System Config
        Key and value are optional
[001D358E:389A493A] :-)
[001D358E:389A493A] :-) syscfg print SrNm
Serial: C39XE089KL28
[001D358E:389A493A] :-) syscfg add SrNm AB123CDE4567
Finish!
[001D358E:389A493A] :-) syscfg print SrNm
Serial: AB123CDE4567
[001D358E:389A493A] :-)
```

Pros

- Saving time on NAND removal/installation
- Saving money on hardware IC programmers
- Avoiding risks of damaging NAND by hardware working on it
- Enhance possibilities: diags offers a set of tests that can be very useful for diagnosis

DEMO

- Purple.app

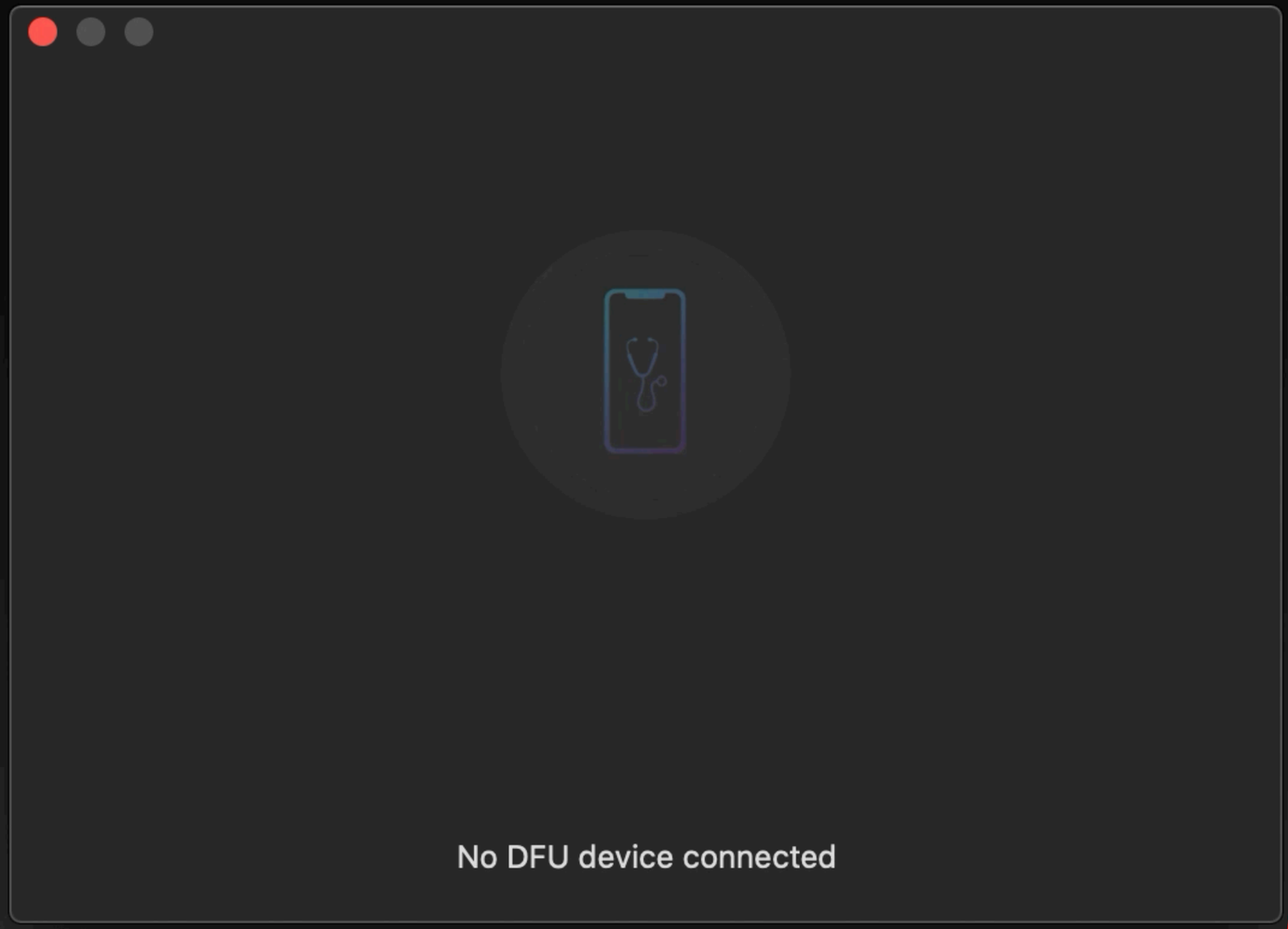
Automated process that

patches SecureROM sigchecks,

loads the first and second stage

bootloaders, and sends diags

image to the target device



Thanks for your time

https://twitter.com/1nsane_dev

https://1nsane.dev

@1nsane_dev