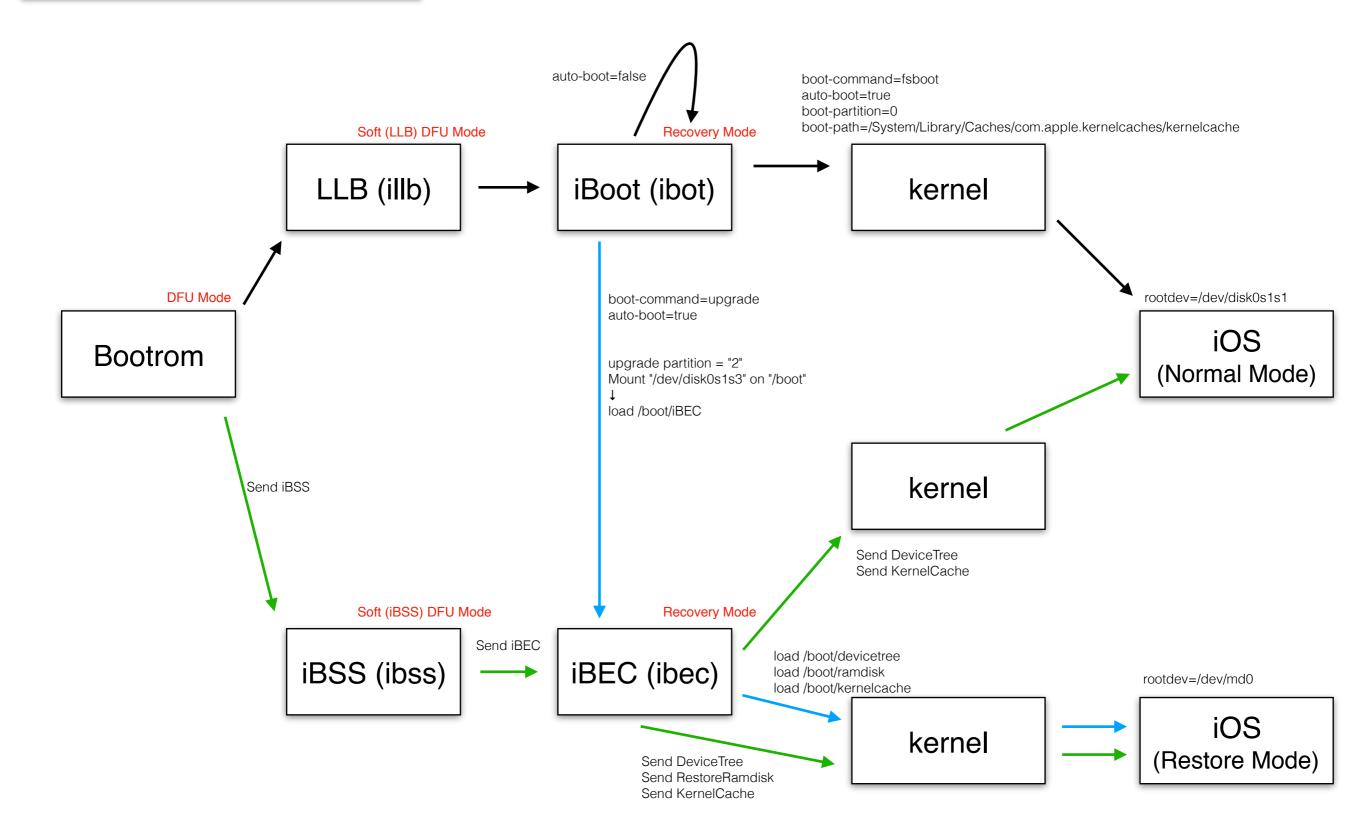
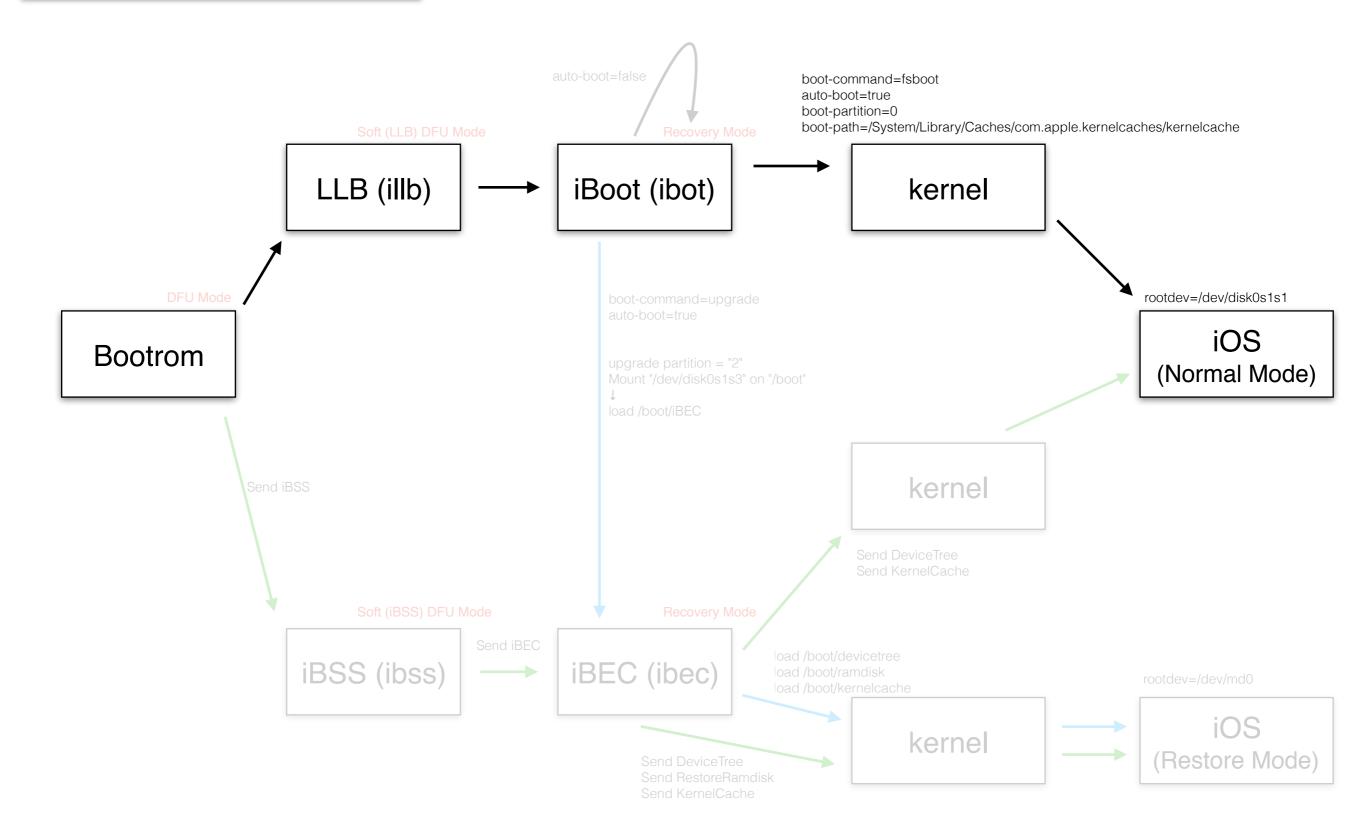
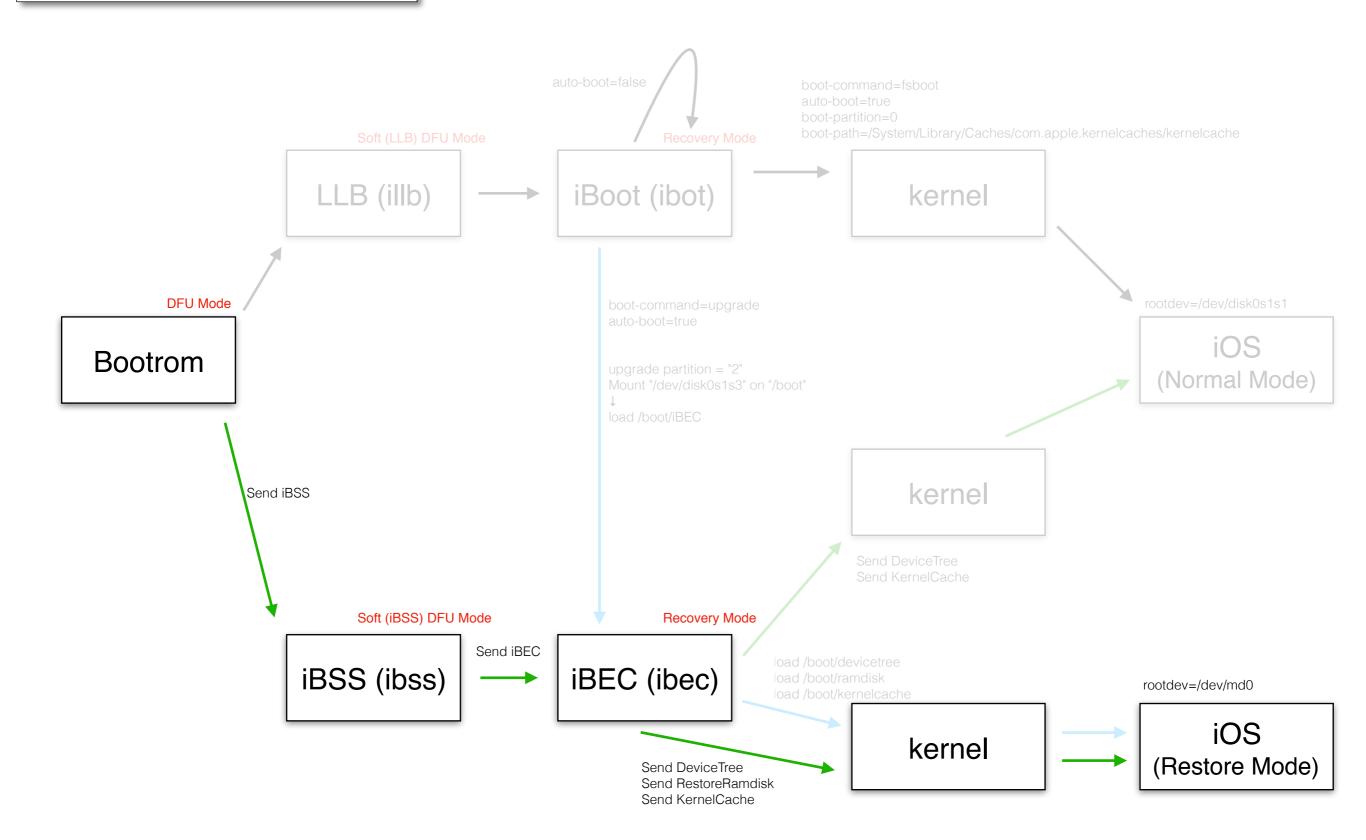
# 32-bit iOS devices boot chain



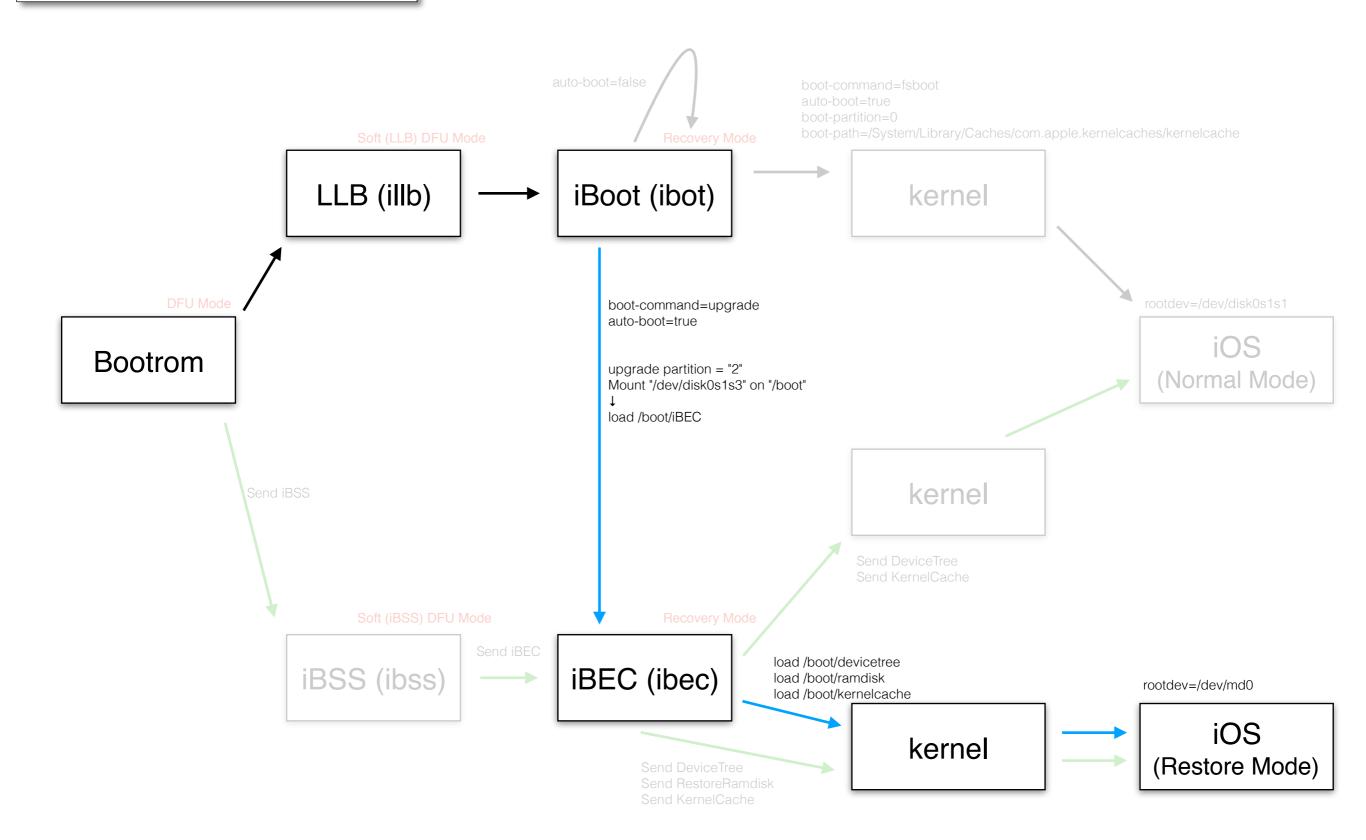
### **Normal Boot**



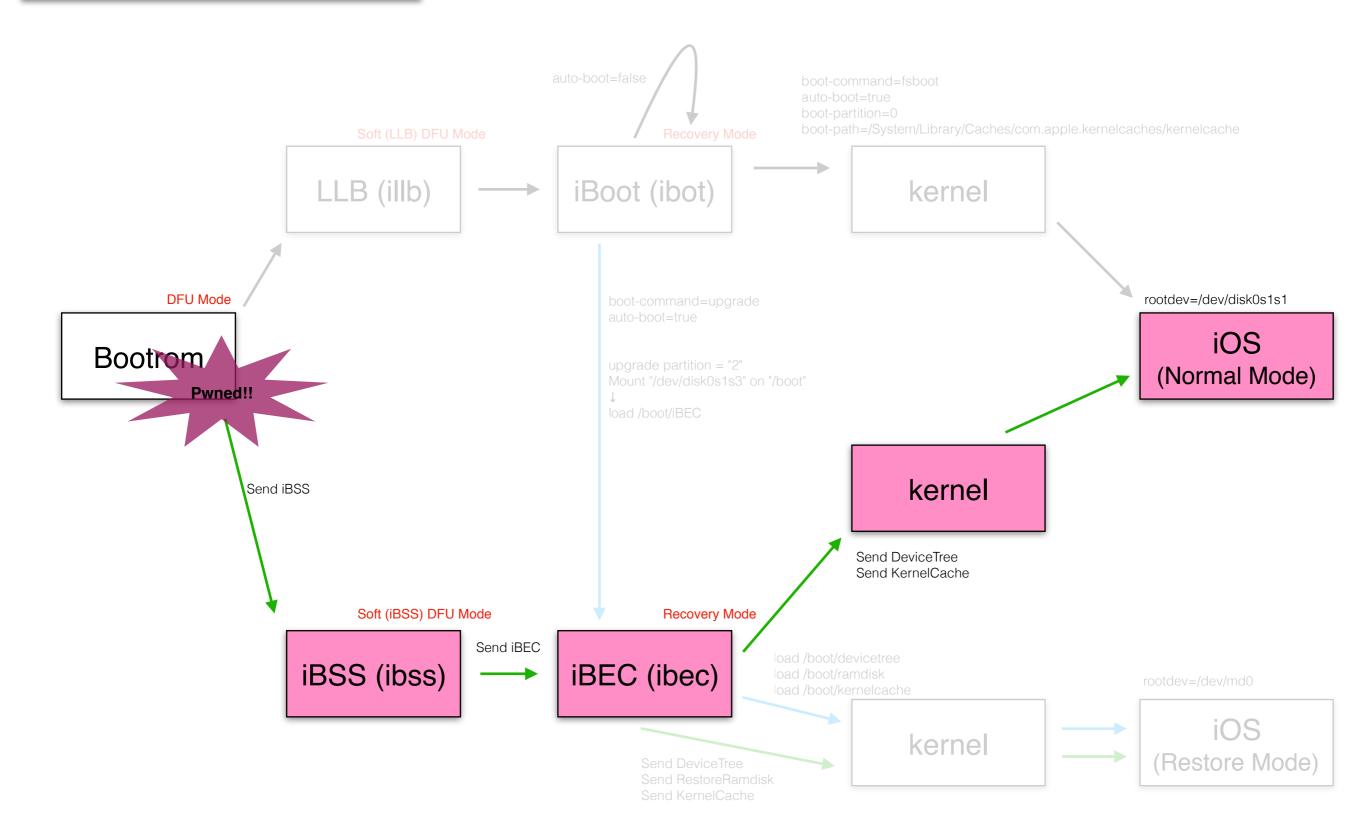
### **Restore/Update**



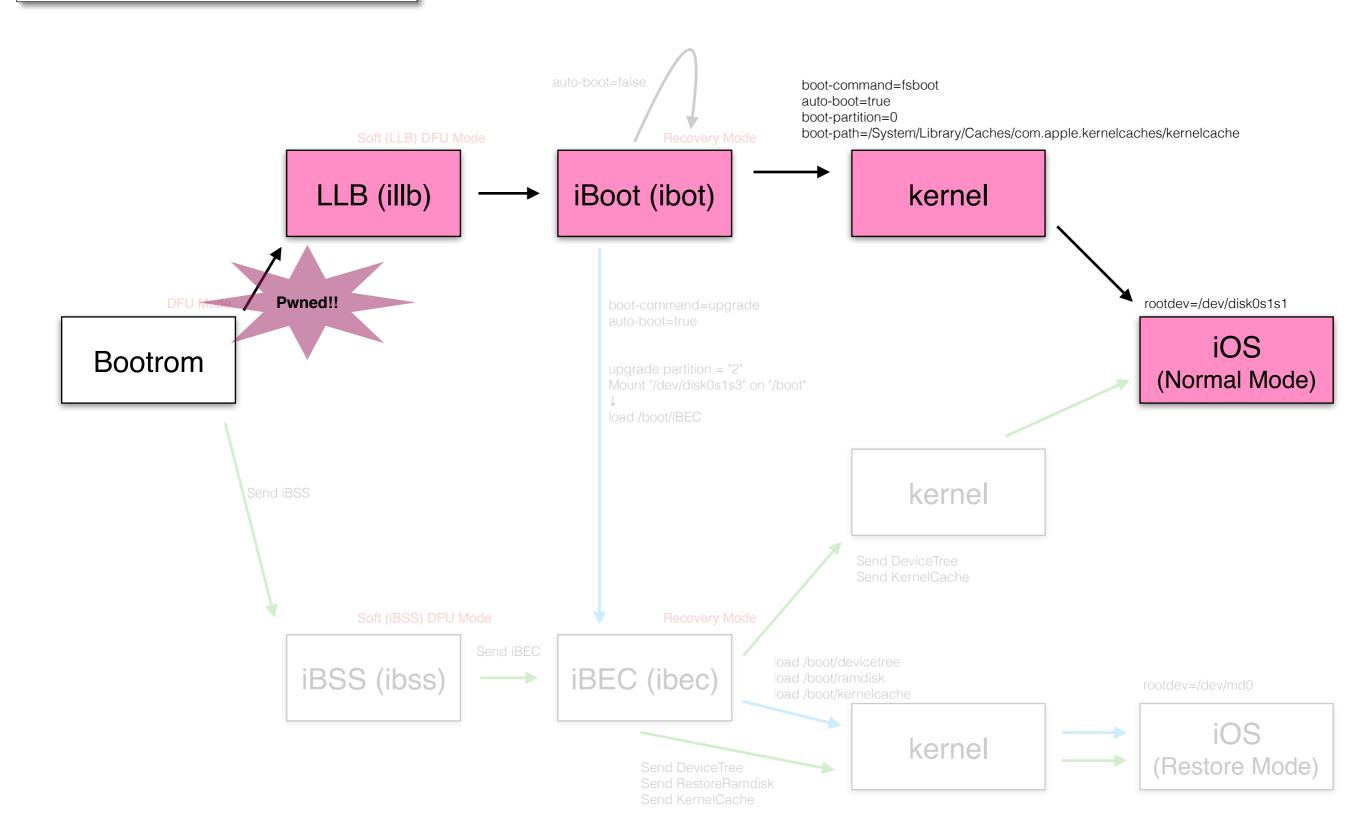
## **OTA Update**



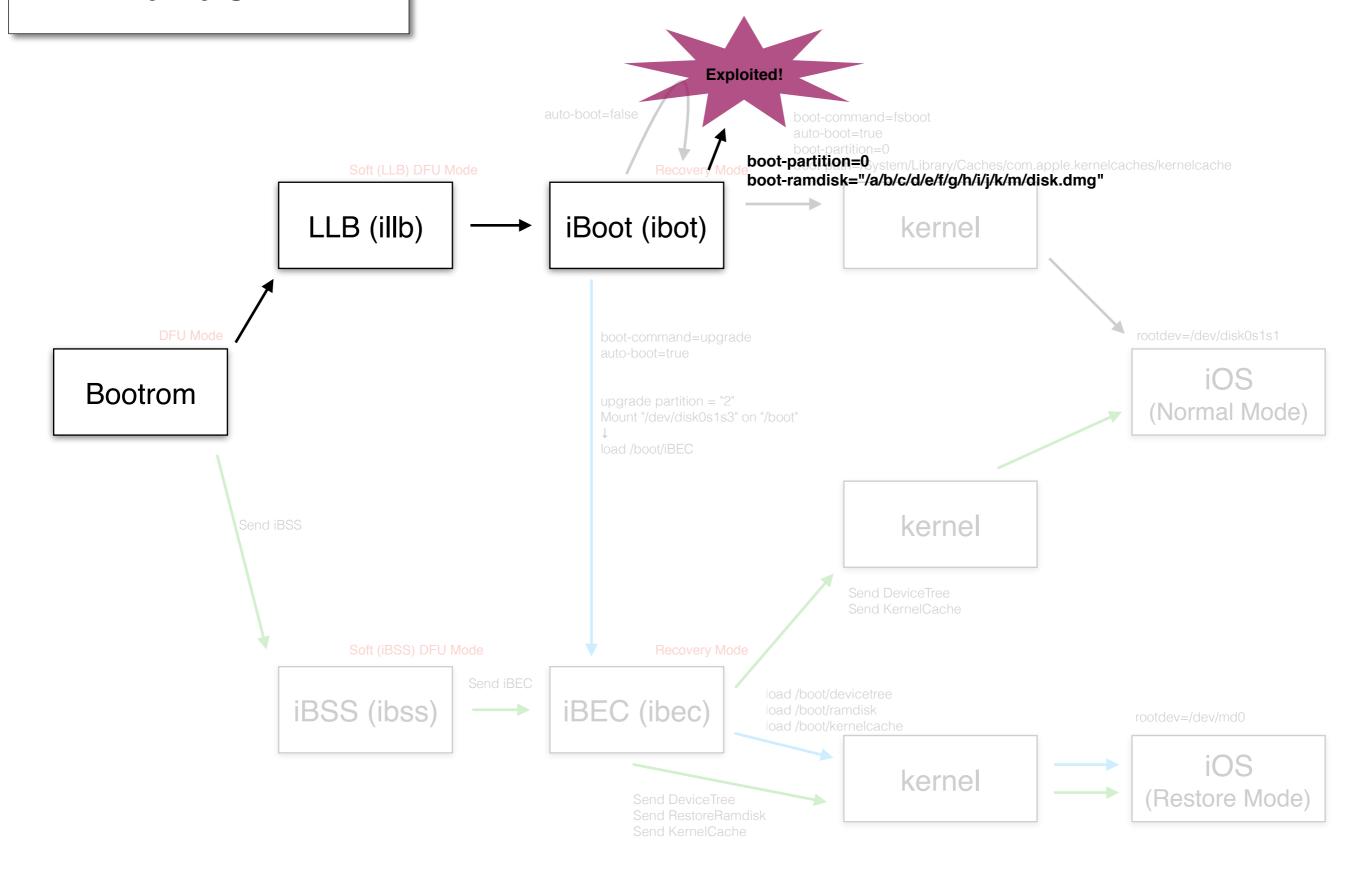
### **Just Boot (limera1n)**



### 24kpwn



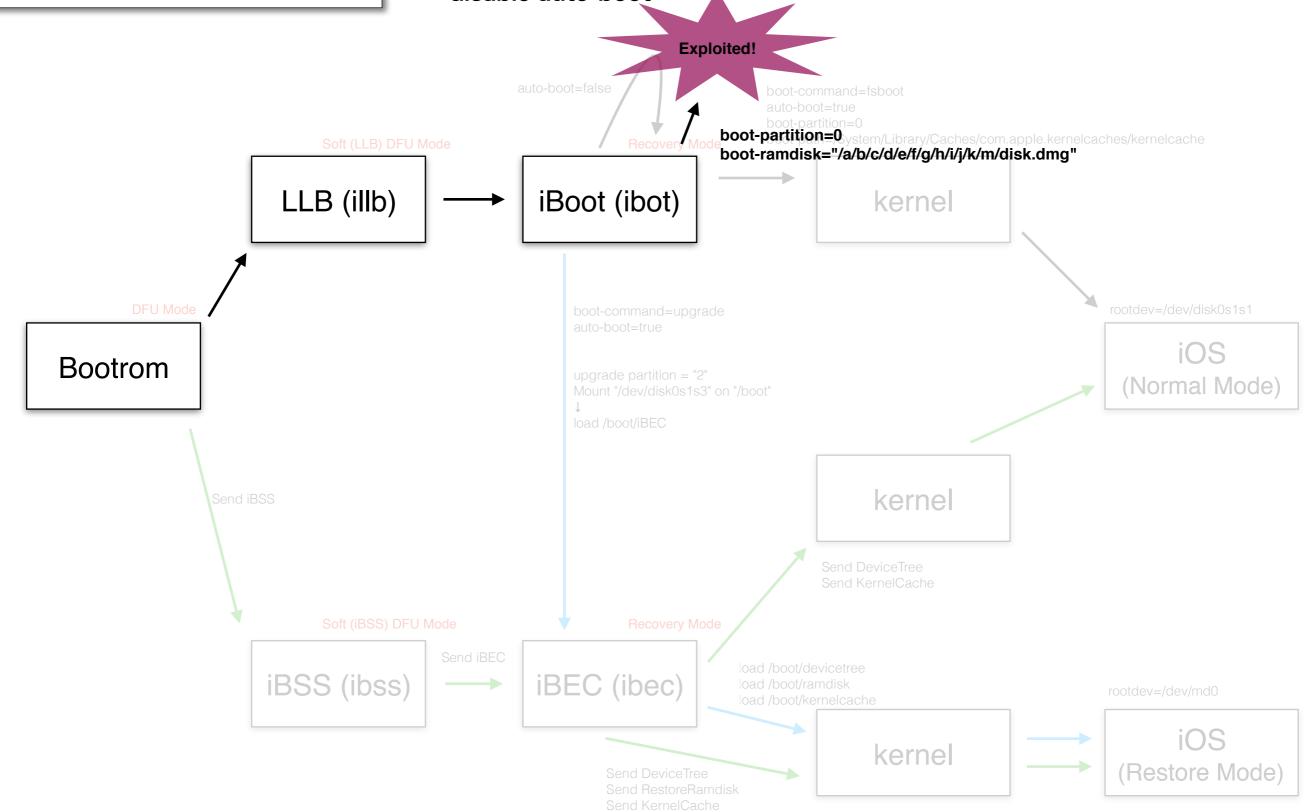
# De Rebus Antiquis ramdiskF

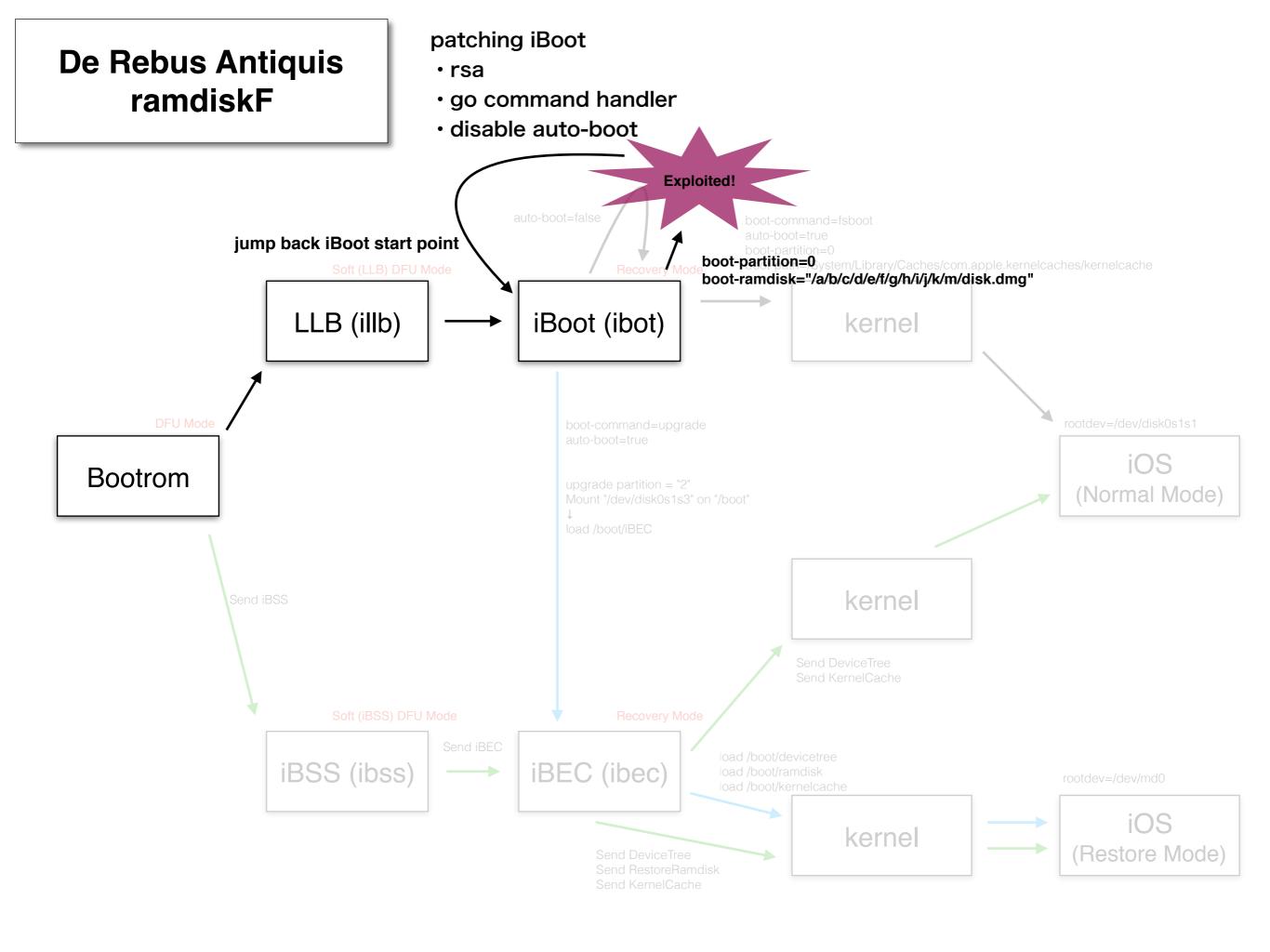


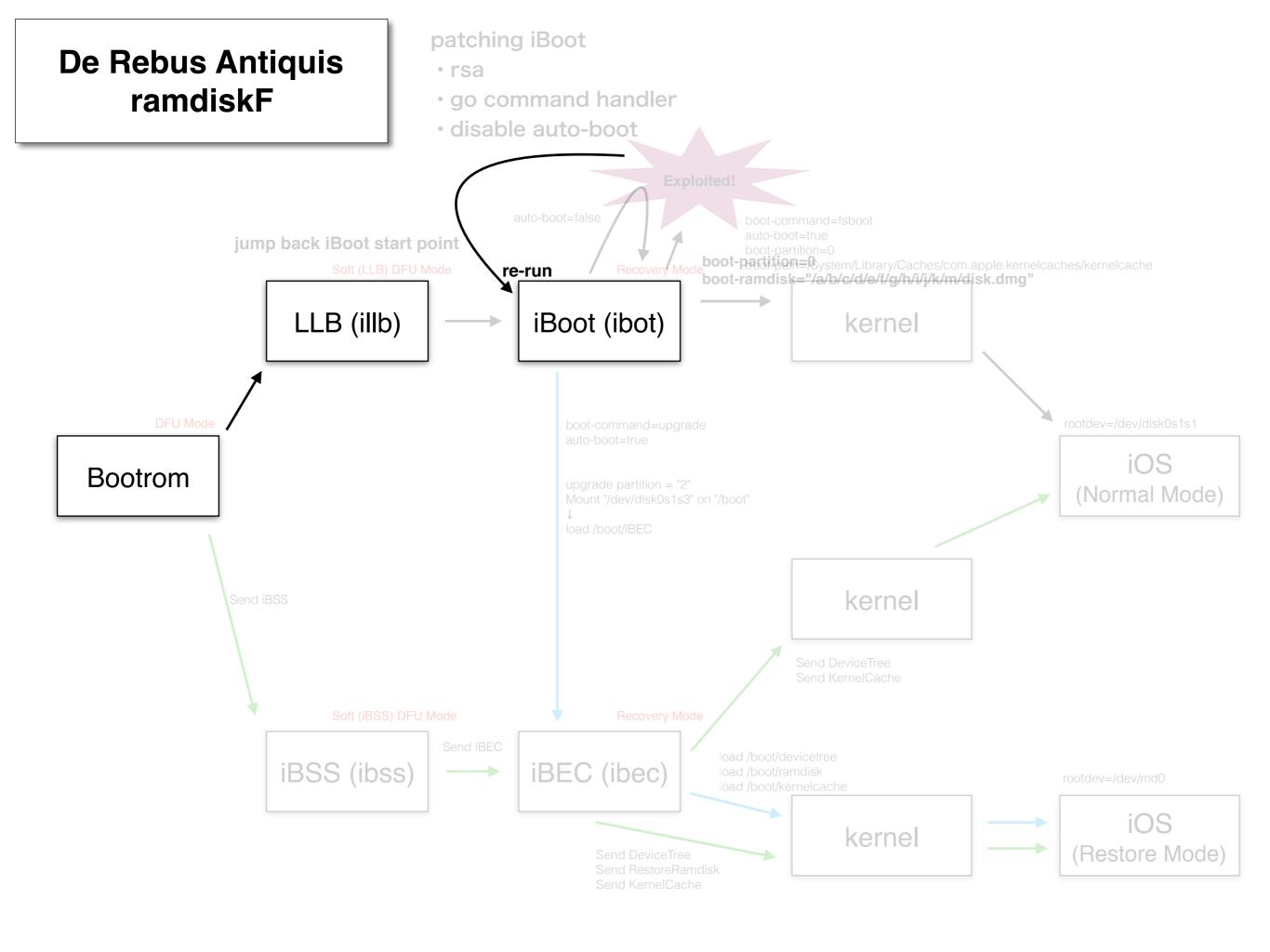
# De Rebus Antiquis ramdiskF

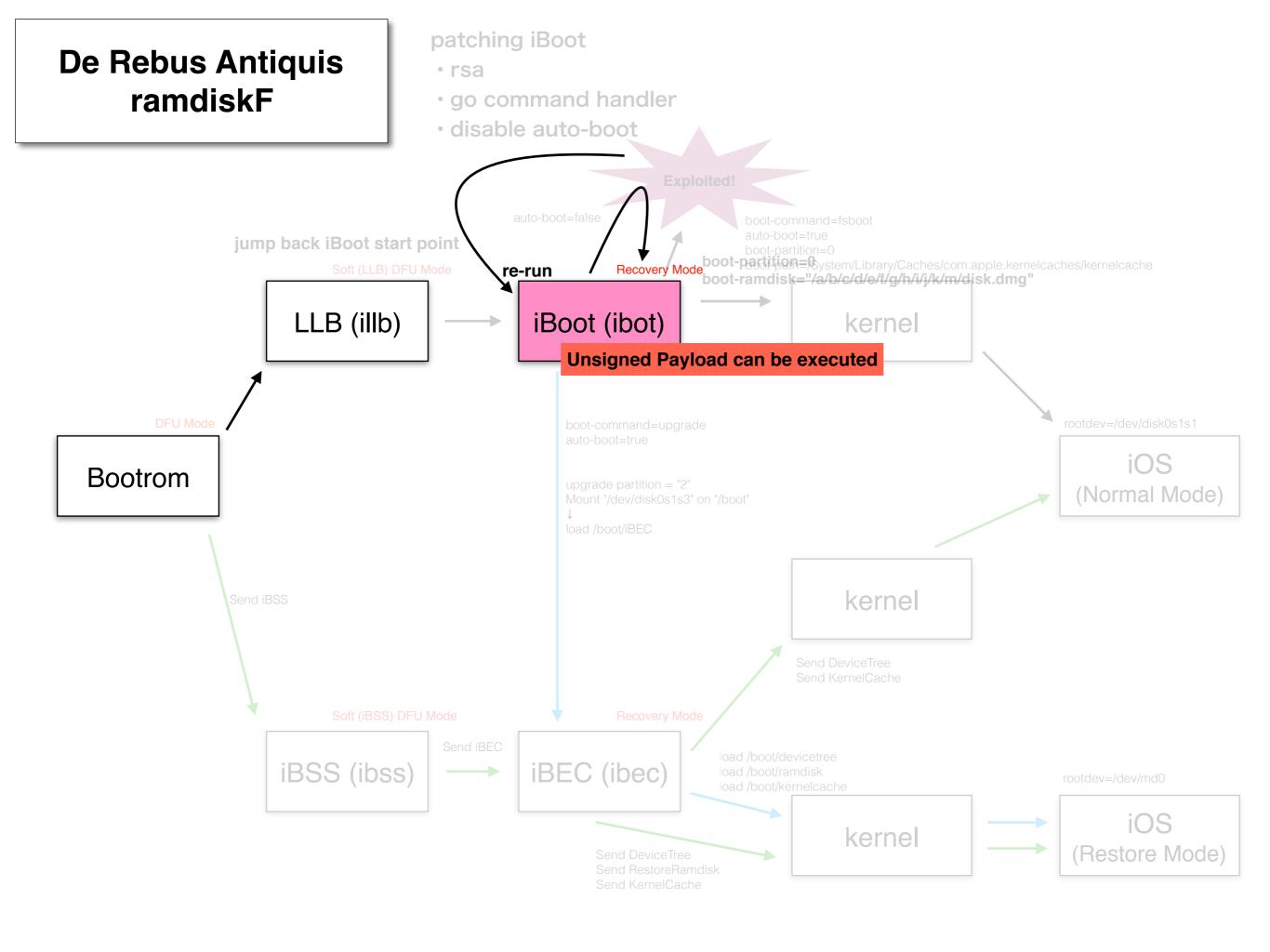
#### patching iBoot

- · rsa
- · go command handler
- disable auto-boot

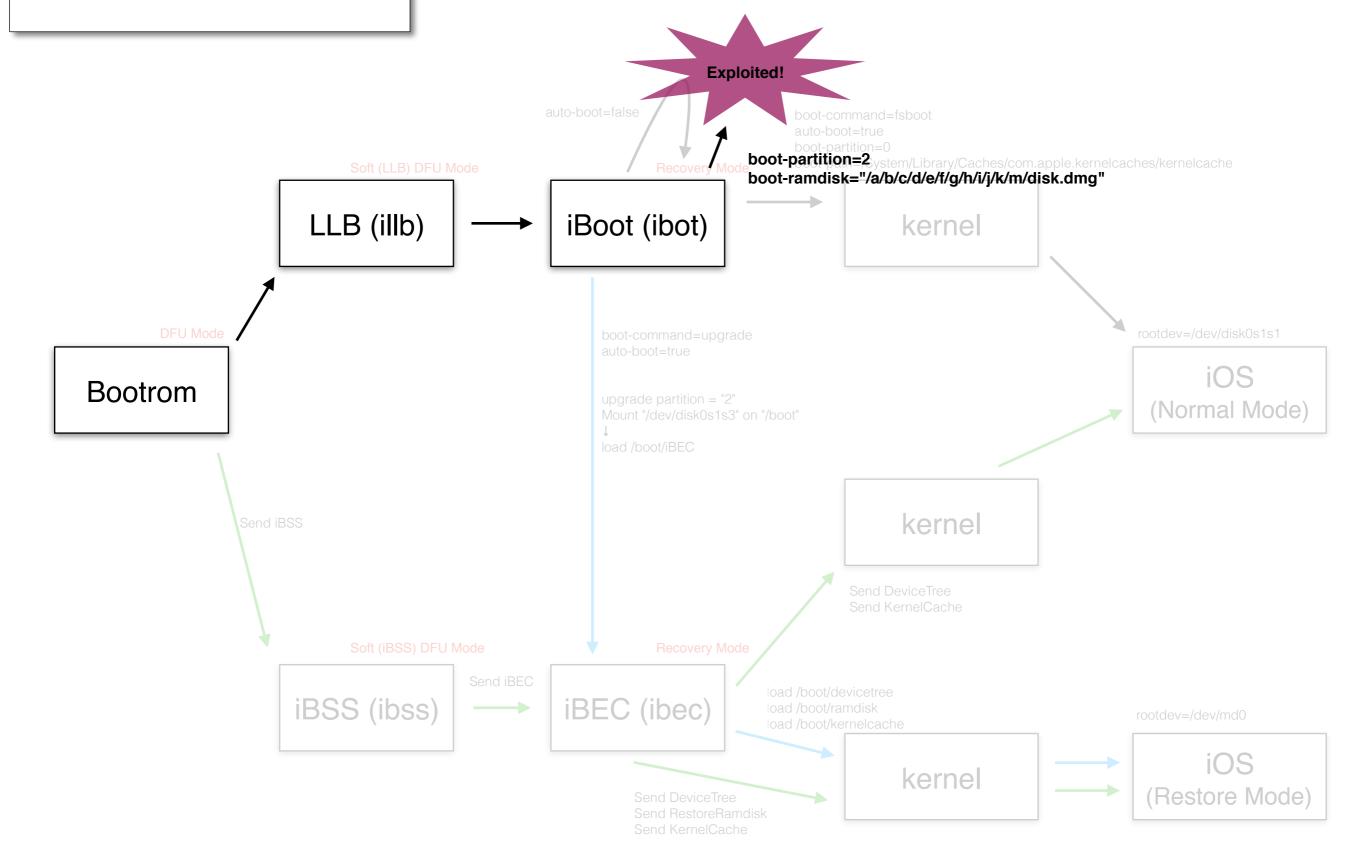








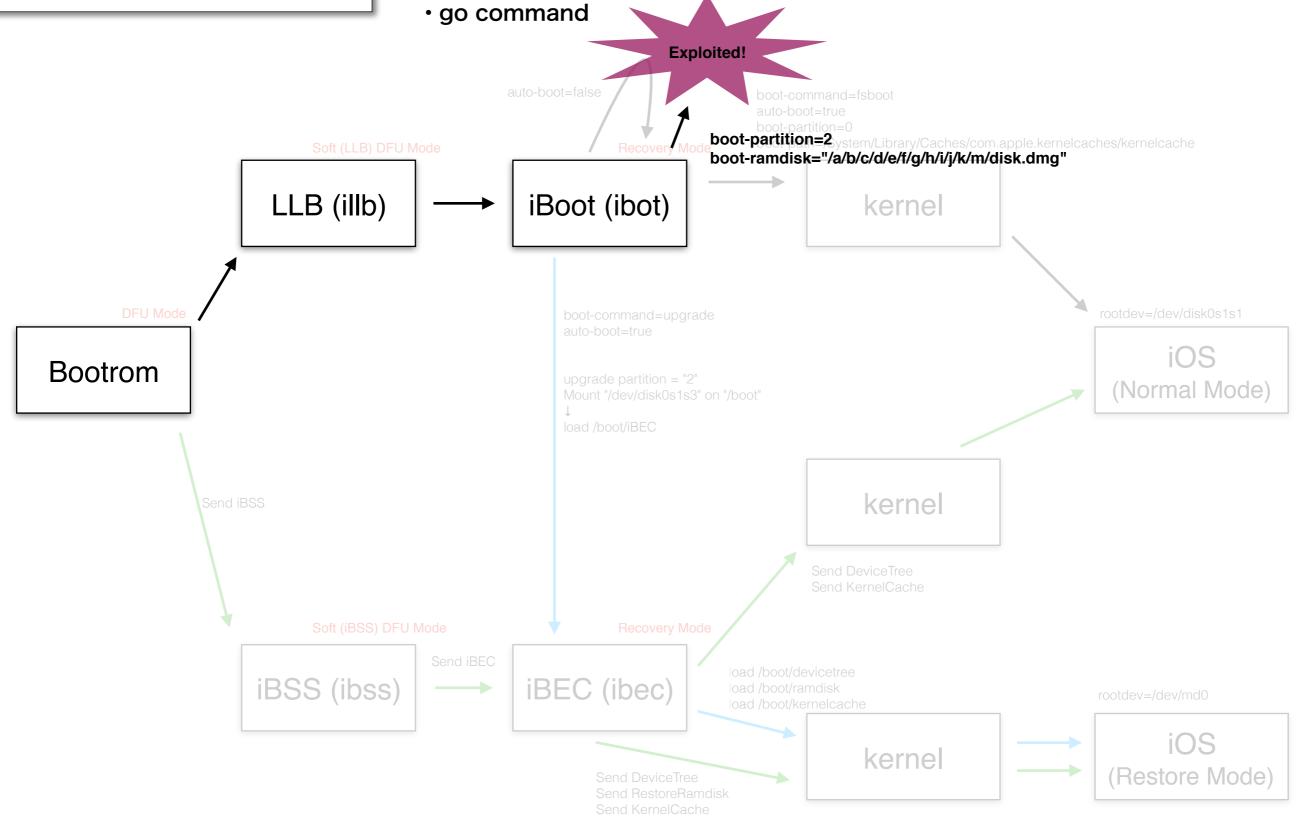
# De Rebus Antiquis ramdiskH

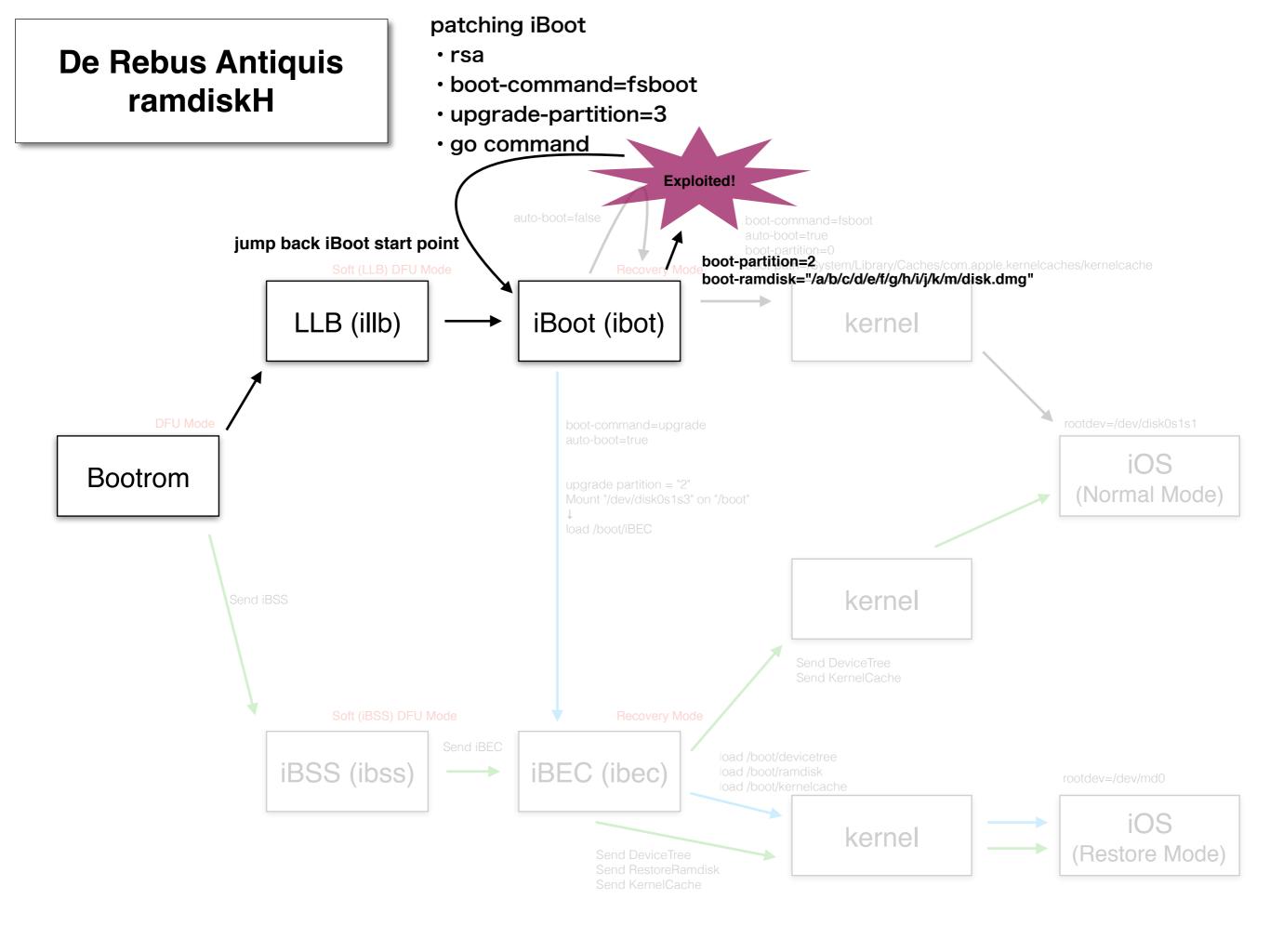


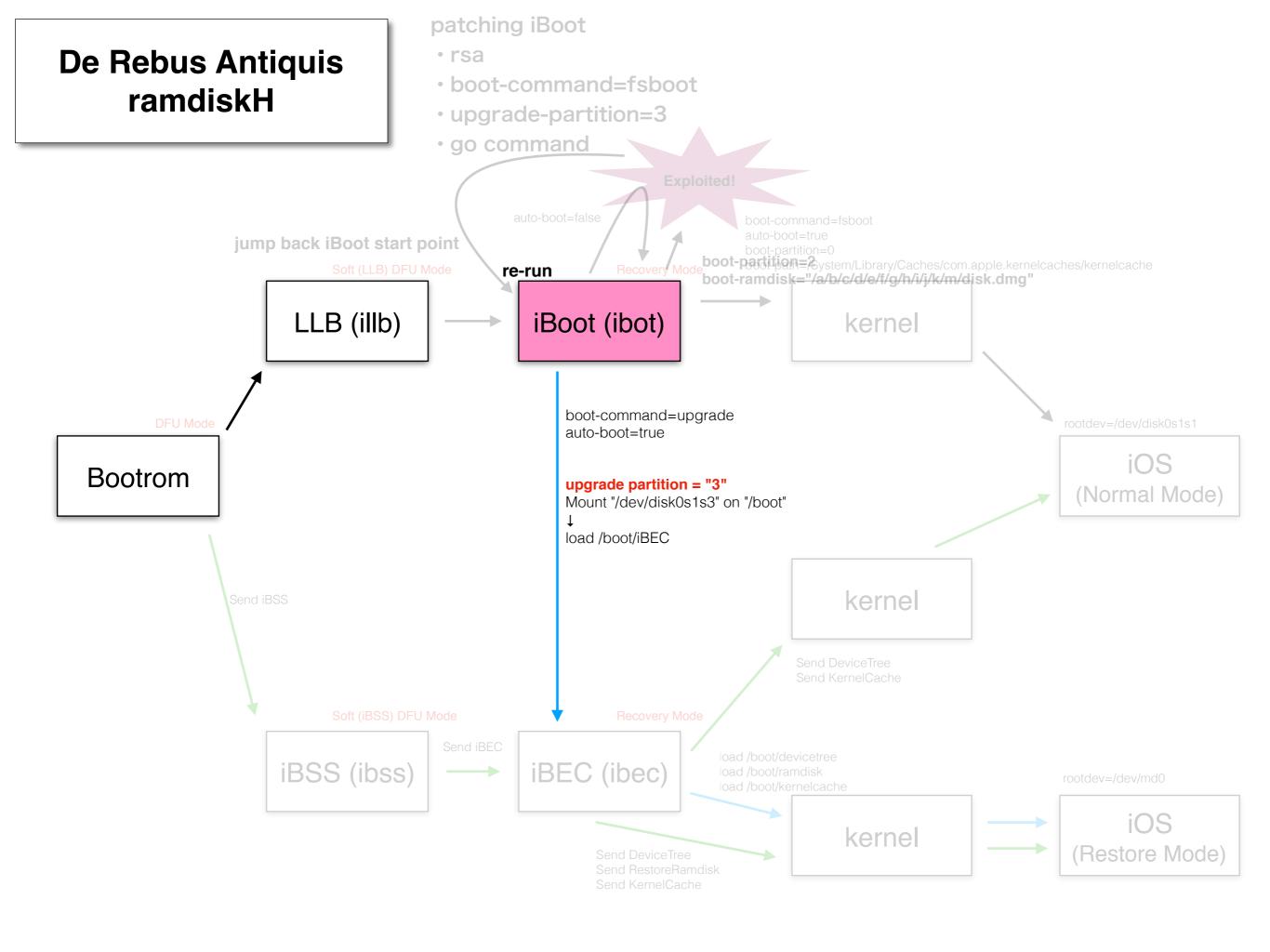
## **De Rebus Antiquis** ramdiskH

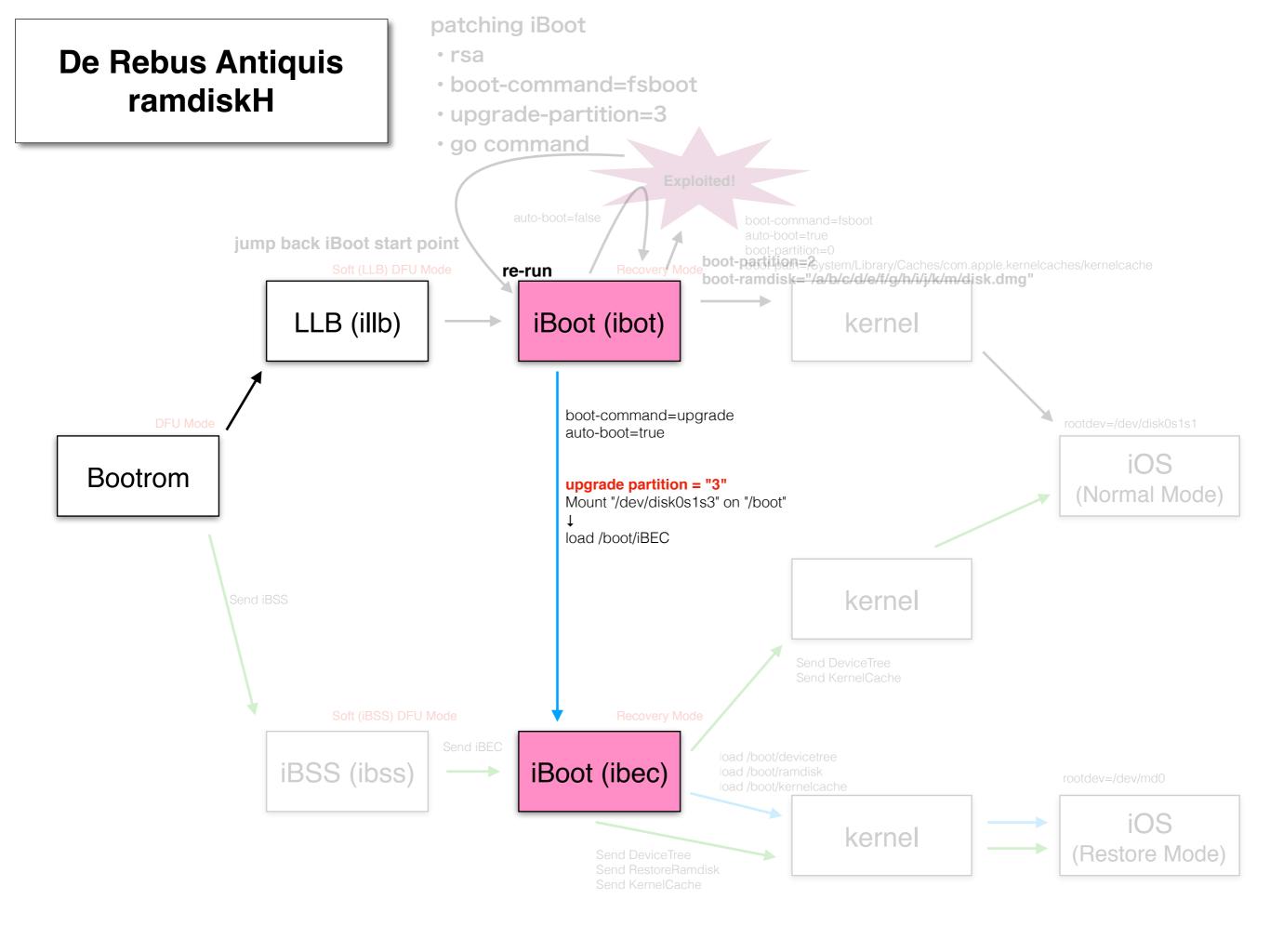
### patching iBoot

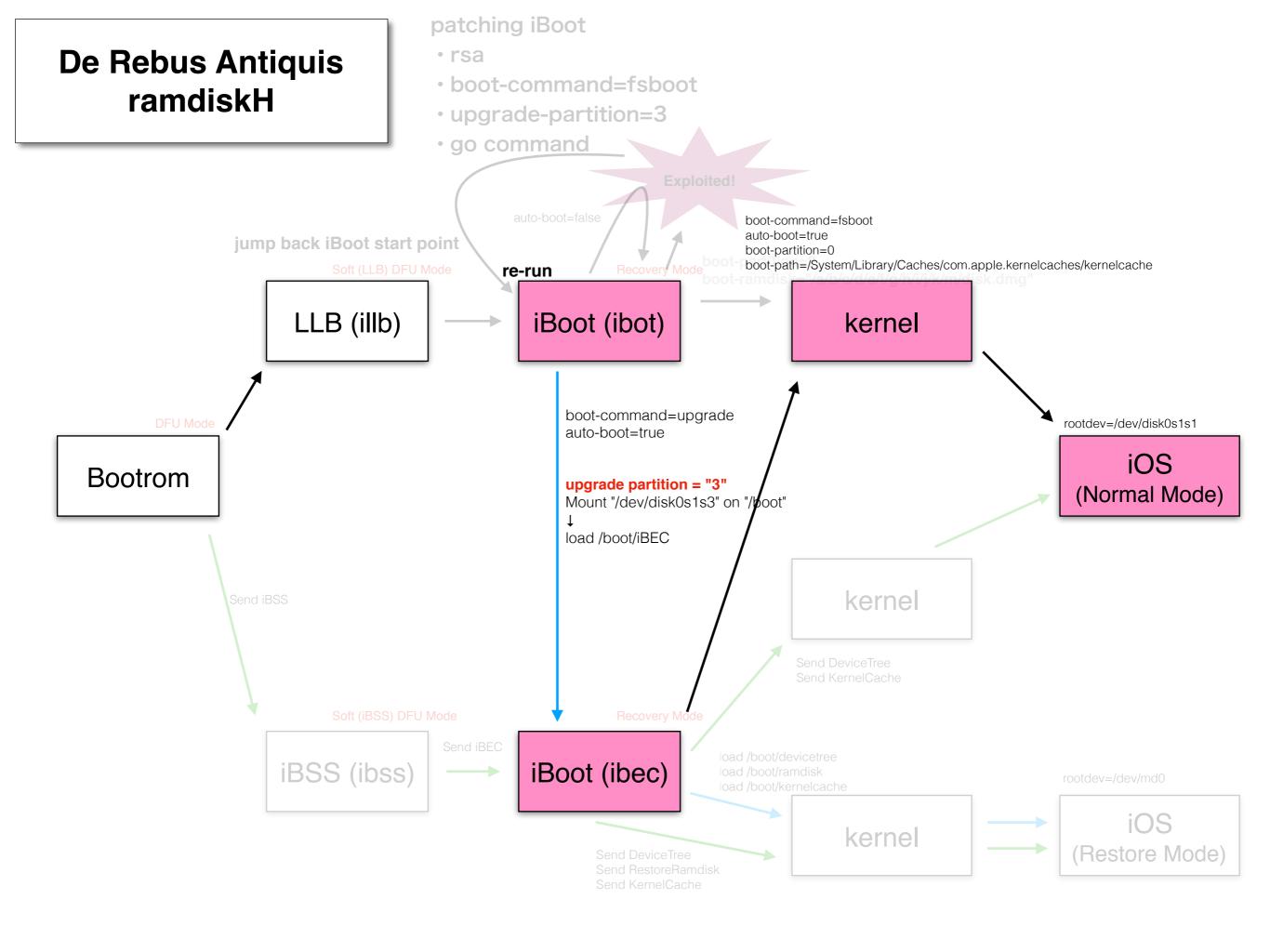
- rsa
- boot-command=fsboot
- upgrade-partition=3



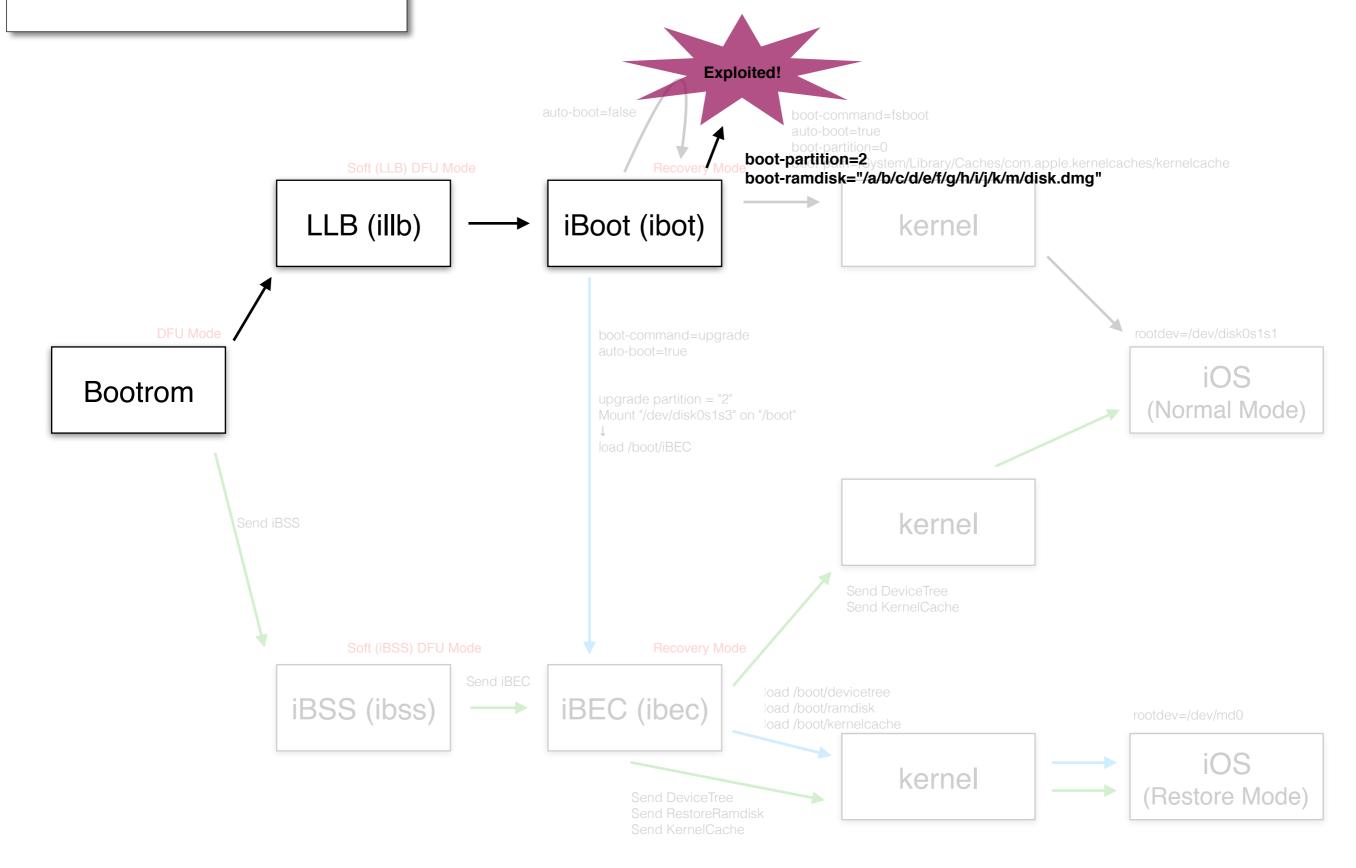








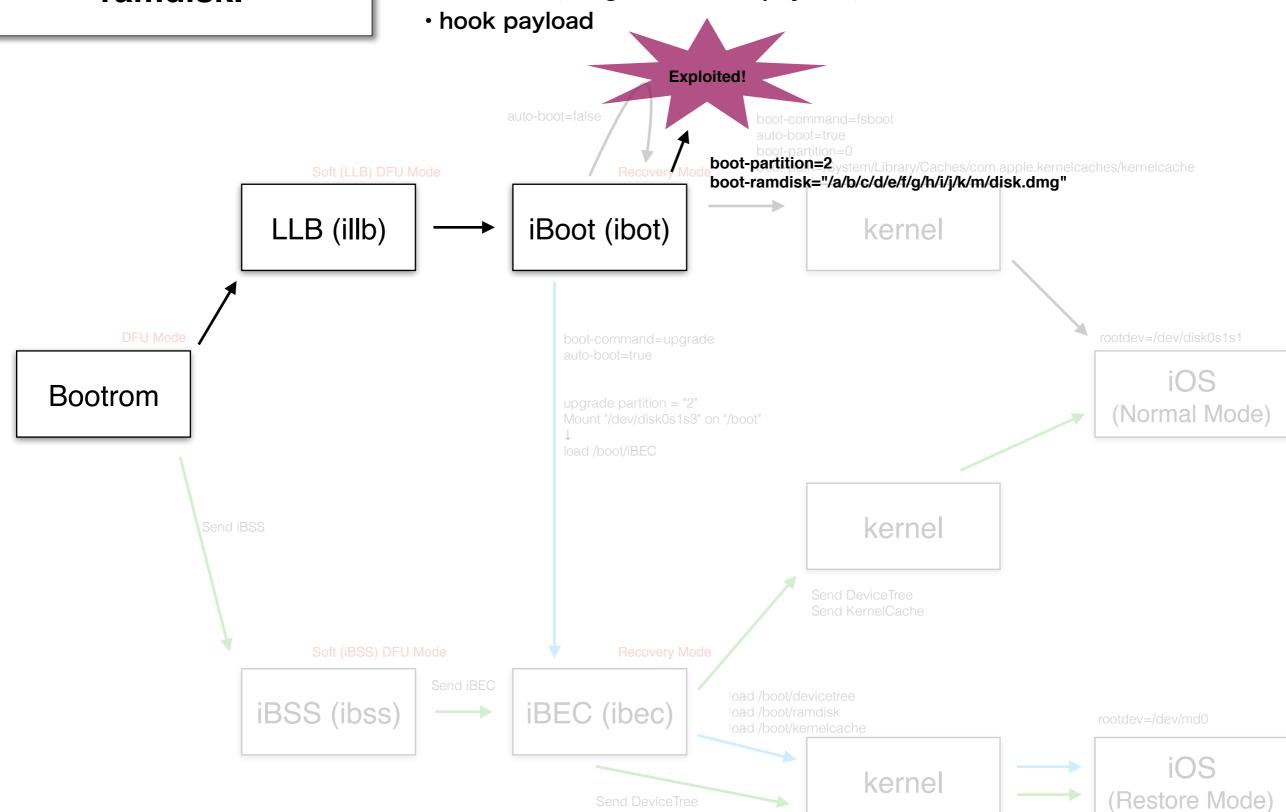
# De Rebus Antiquis ramdiskl



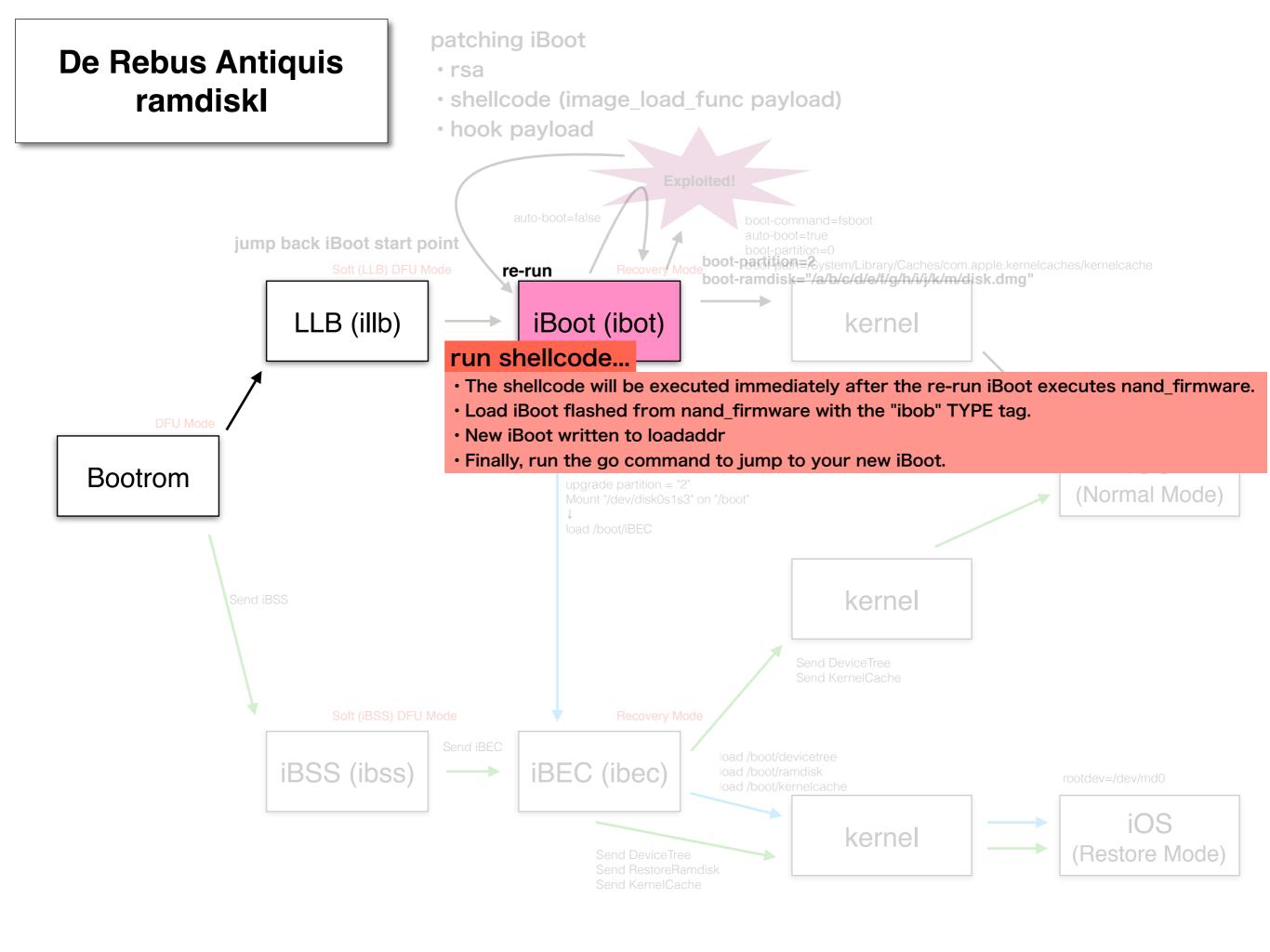
# De Rebus Antiquis ramdiskl

#### patching iBoot

- rsa
- shellcode (image\_load\_func payload)



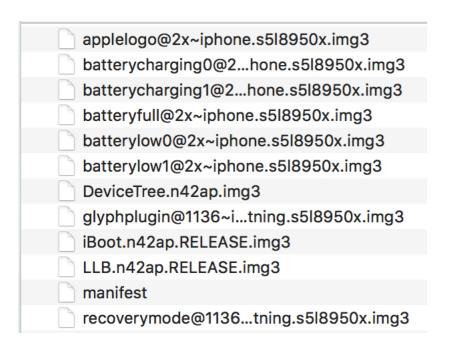
## patching iBoot **De Rebus Antiquis** rsa ramdiskl shellcode (image\_load\_func payload) · hook payload **Exploited!** jump back iBoot start point boot-partition=0 boot-partition=2 boot-ramdisk="/a/b/c/d/e/f/g/h/i/j/k/m/disk.dmg" iBoot (ibot) LLB (illb) kernel iOS **Bootrom** (Normal Mode) kernel iBSS (ibss) iBEC (ibec) iOS kernel (Restore Mode)

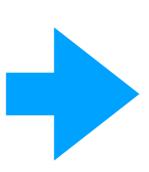


## patching iBoot **De Rebus Antiquis** rsa ramdiskl shellcode (image\_load\_func payload) · hook payload jump back iBoot start point boot-partition=&ystem/Library/Caches/com.apple.kernelcaches/kernelcache re-run boot-ramdisk="<del>/a/b/c/d/e/f/g/h/i/j/k/m/d</del>isk.dmg" LLB (illb) kernel iBoot (ibob) run sh iOS **Bootrom** (Normal Mode) kernel iBSS (ibss) iBEC (ibec) iOS kernel (Restore Mode)

### patching iBoot **De Rebus Antiquis** rsa ramdiskl shellcode (image\_load\_func payload) · hook payload boot-command=fsboot auto-boot=true jump back iBoot start point boot-partition=0 boot-path=/System/Library/Caches/com.apple.kernelcaches/kernelcache re-run LLB (illb) kernel iBoot (ibob) run sh rootdev=/dev/disk0s1s1 iOS **Bootrom** (Normal Mode) kernel iBSS (ibss) iBEC (ibec) iOS kernel (Restore Mode)

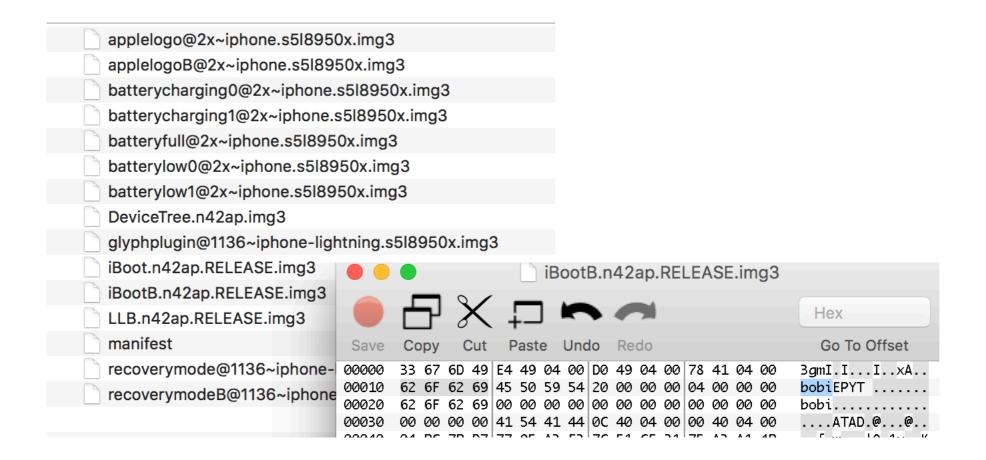
Restore any iBoot that has "ibob" in the TYPE tag allows you get to jump to that iBoot after the DRA has been exploited.





apple	logo@2x~iphone.s5l8950x.img3
apple	logoB@2x~iphone.s5l8950x.img3
batter	rycharging0@2x~iphone.s5l8950x.img3
batter	rycharging1@2x~iphone.s5l8950x.img3
batter	ryfull@2x~iphone.s5l8950x.img3
batter	rylow0@2x~iphone.s5l8950x.img3
batter	rylow1@2x~iphone.s5l8950x.img3
Devic	eTree.n42ap.img3
glyph	plugin@1136~iphone-lightning.s5l8950x.img3
iBoot.	n42ap.RELEASE.img3
iBoot	B.n42ap.RELEASE.img3
LLB.n	42ap.RELEASE.img3
manif	est
recov	erymode@1136~iphone-lightning.s5l8950x.img3
recov	erymodeB@1136~iphone-lightning.s5l8950x.img3

Restore any iBoot that has "ibob" in the TYPE tag allows you get to jump to that iBoot after the DRA has been exploited.



**iBootB** 

Restore any iBoot that has "ibob" in the TYPE tag allows you get to jump to that iBoot after the DRA has been exploited.

```
DeviceTree.n42ap.img3
LLB.n42ap.RELEASE.img3
applelogo@2x~iphone.s5l8950x.img3
batterycharging0@2x~iphone.s5l8950x.img3
batterycharging1@2x~iphone.s5l8950x.img3
batteryfull@2x~iphone.s5l8950x.img3
batterylow0@2x~iphone.s5l8950x.img3
batterylow1@2x~iphone.s5l8950x.img3
glyphplugin@1136~iphone-lightning.s5l8950x.img3
iBoot.n42ap.RELEASE.img3
recoverymode@1136~iphone-lightning.s5l8950x.img3
iBootB.n42ap.RELEASE.img3
applelogoB@2x~iphone.s5l8950x.img3
recoverymodeB@1136~iphone-lightning.s5l8950x.img3
```

### manifest

### iBoot vs iBootB

- · iBoot (original) must be a legitimate image signed by Apple. Do not allow any changes.
- On the other hand, you can put any unsigned image on iBootB. Generally, install pwniBoot for booting target iOS.
- · iBoot displays AppleLogo with 'logo' TYPE tag as the bootlogo, and Recovery Mode Image with 'recm' TYPE tag as the recoverylogo.
- · iBootB displays AppleLogo with 'logb' TYPE tag as the bootlogo, and Recovery Mode Image with 'recb' TYPE tag as the recoverylogo.
- -> You can install custom logos on "ApplelogoB" and "RecoveryModeB"!
  - You need to apply the following patch to iBootB to boot any iOS.
    - · rsa
    - ignore boot-partition
    - ignore boot-ramdisk

### iBoot vs iBootB

iBoot

Do not do anything

iBootB

### Apply patches

- rsa
- ignore boot-partition
- ignore boot-ramdisk

### iBoot vs iBootB

iBoot

Do not do anything

iBootB

Apply patches (complete jailbreaking...)

- rsa
- ignore boot-partition
- ignore boot-ramdisk
- enable setenv
- debug\_enabled
- Injecting BootArgs to disable CS and AMFI
- Kernel patcher payload etc...