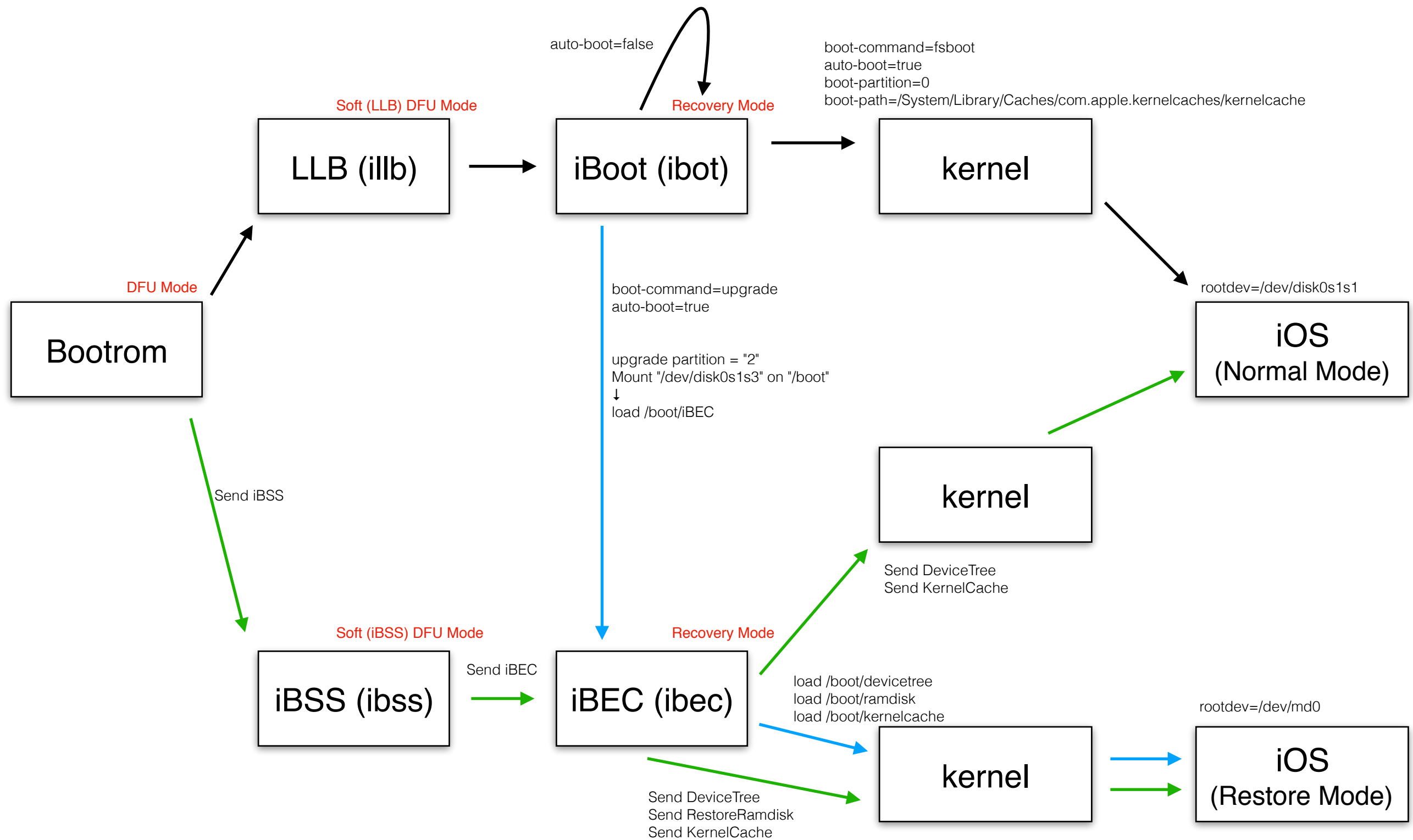
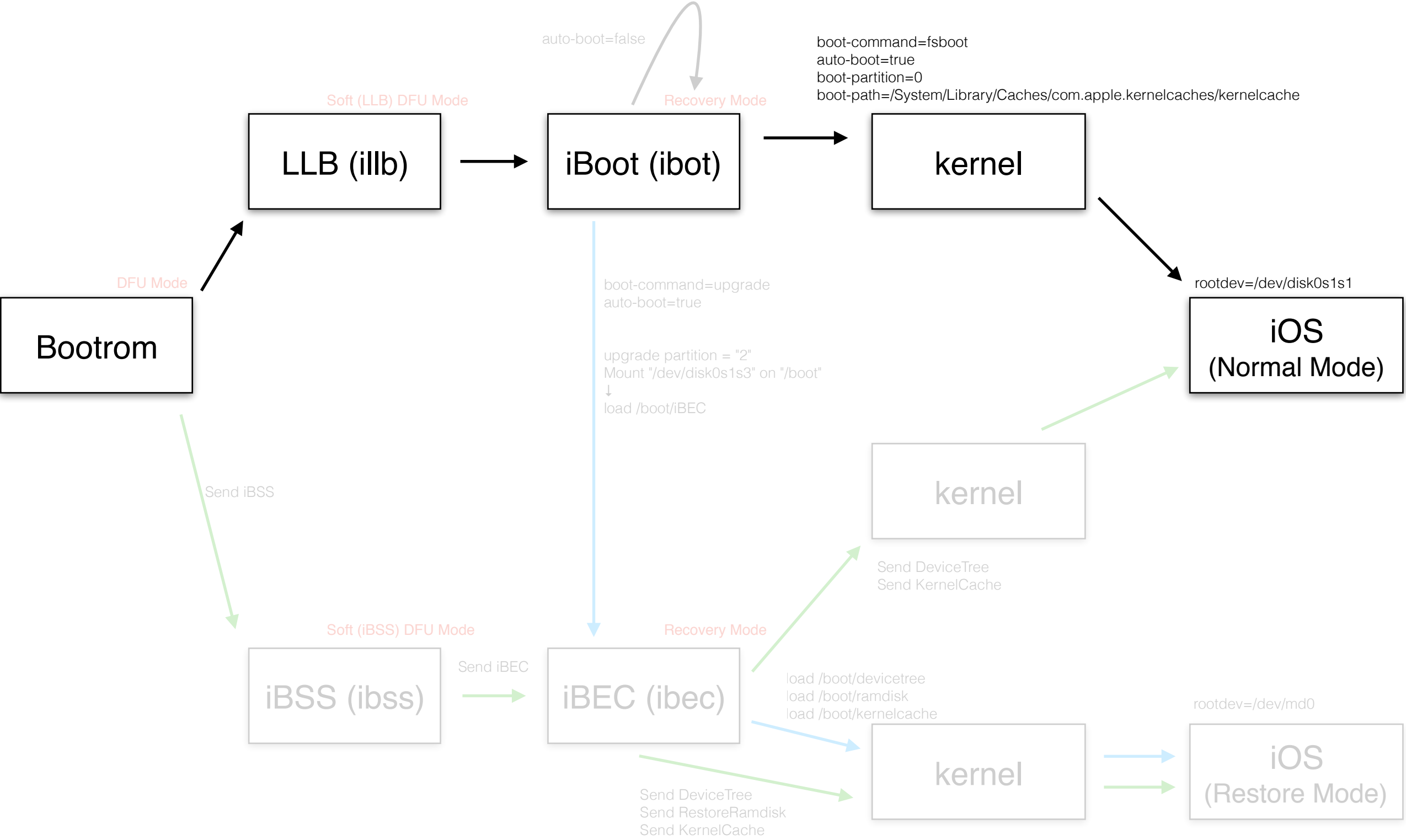


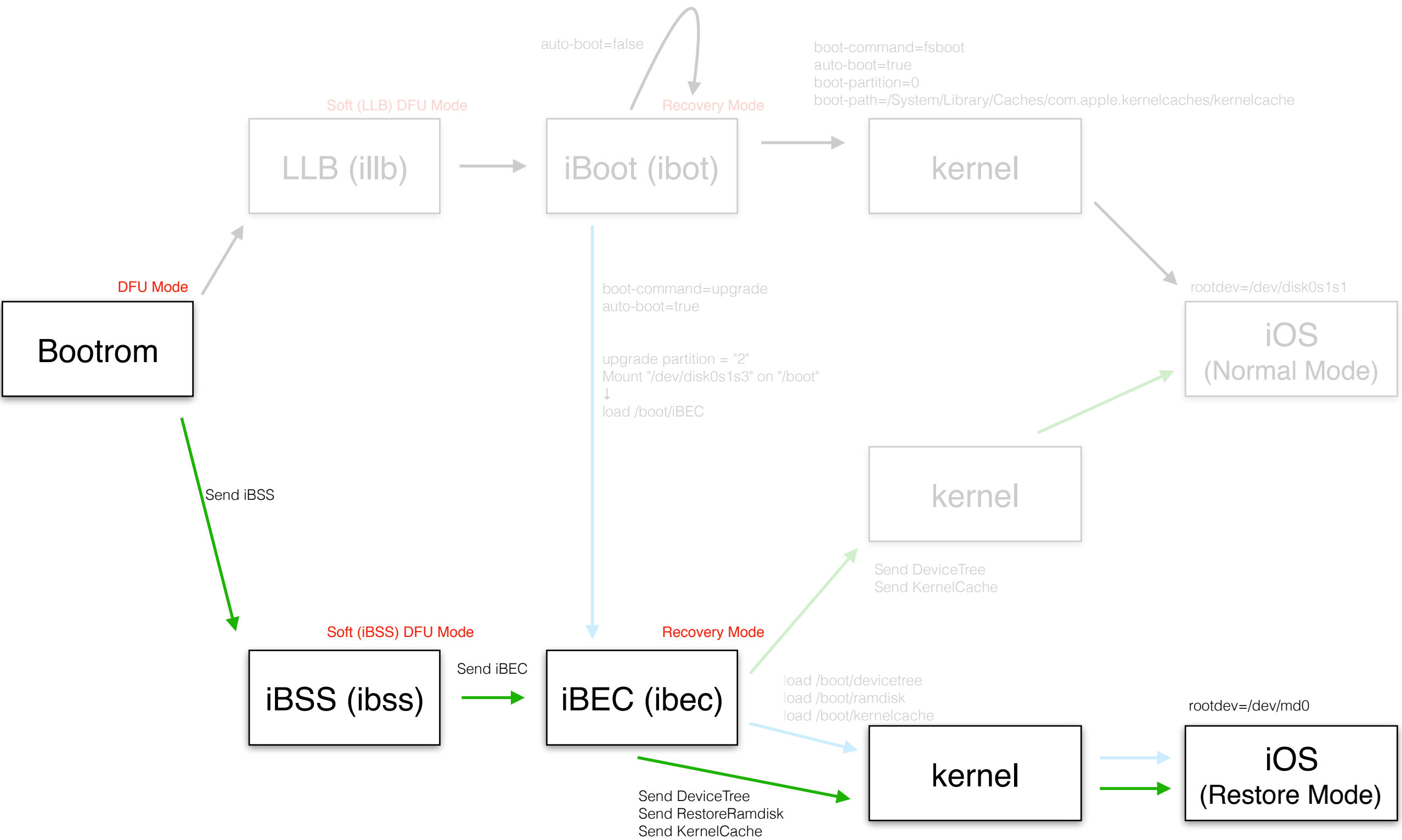
32-bit iOS devices boot chain



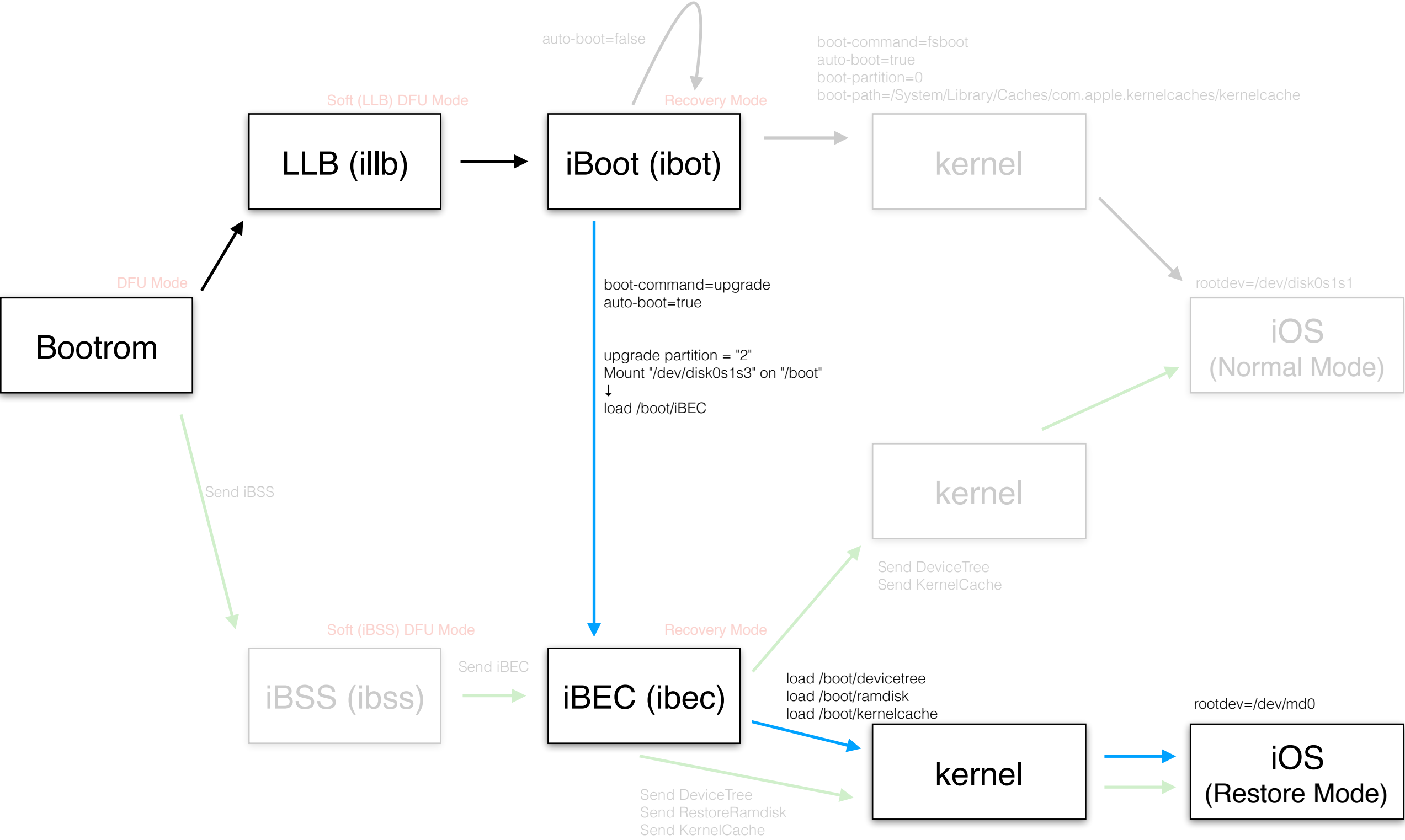
Normal Boot



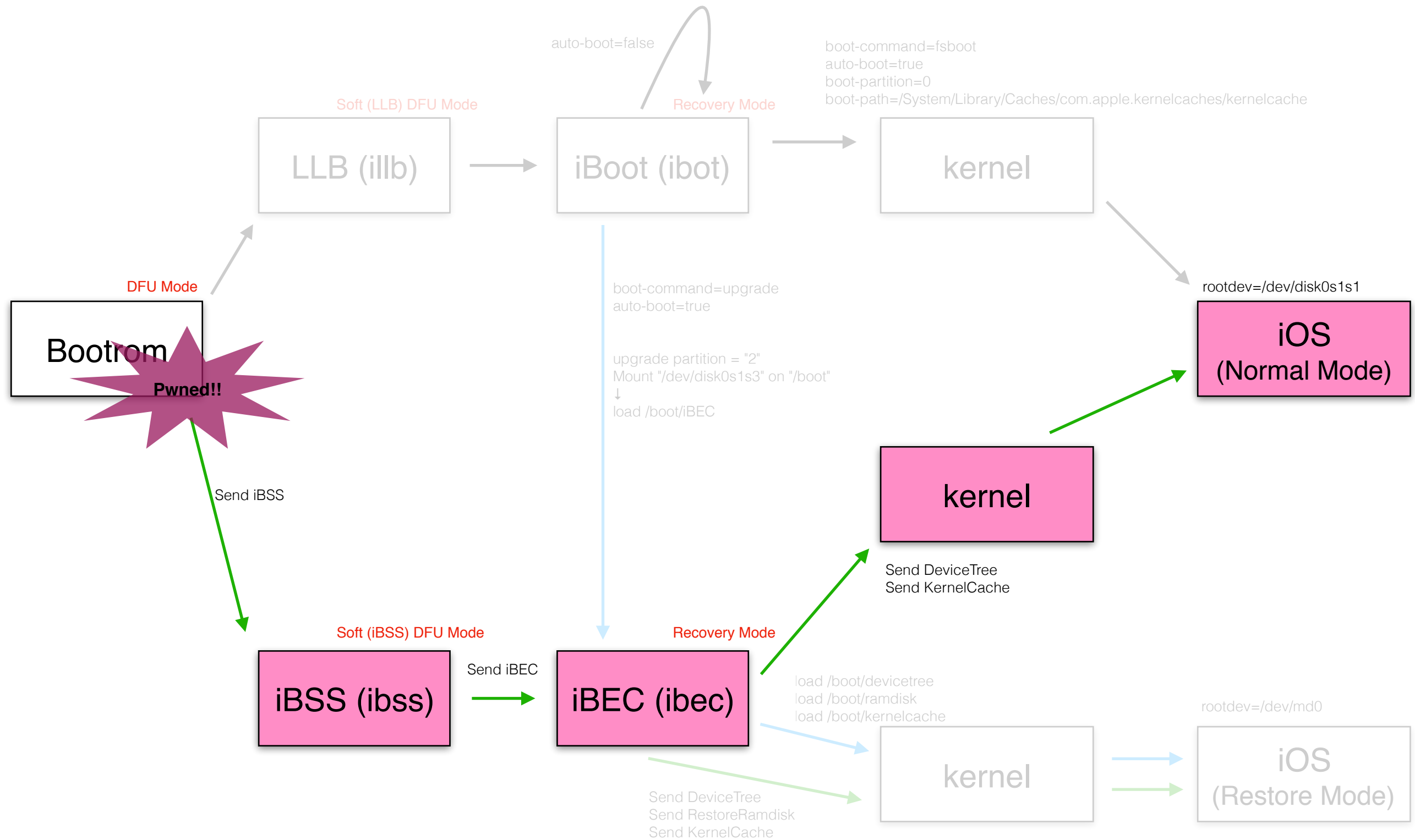
Restore/Update



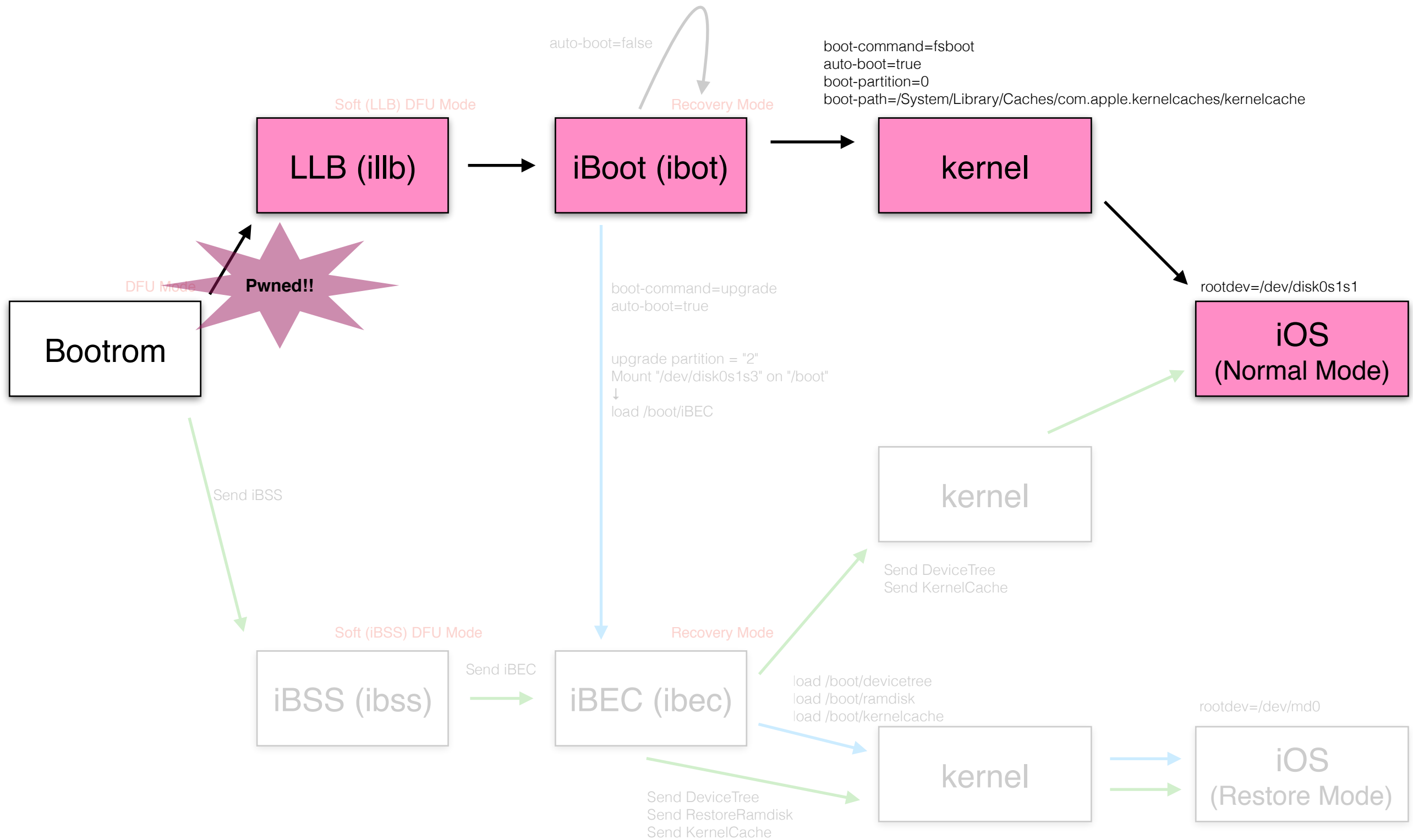
OTA Update



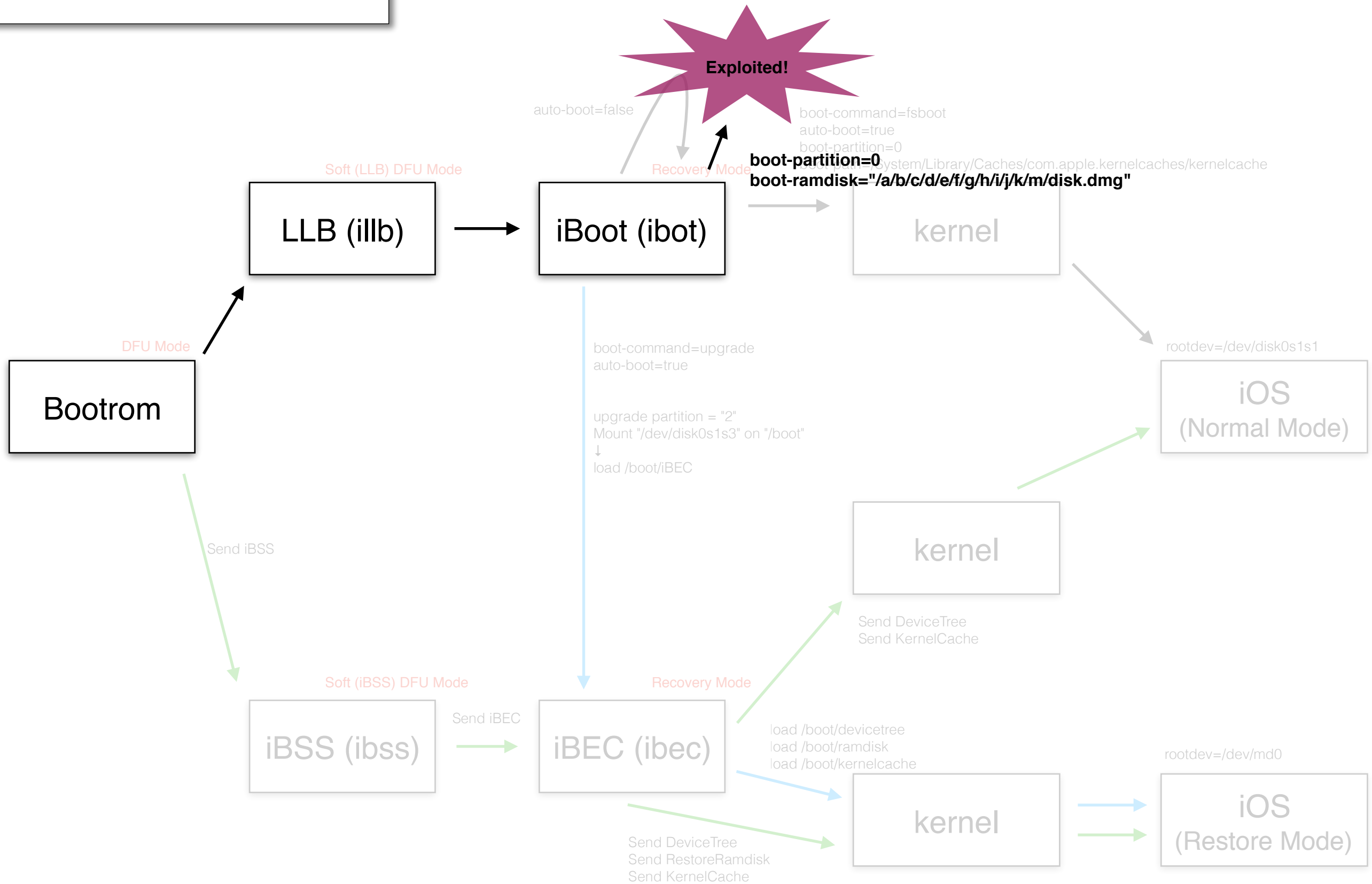
Just Boot (limer1n)



24kpwn



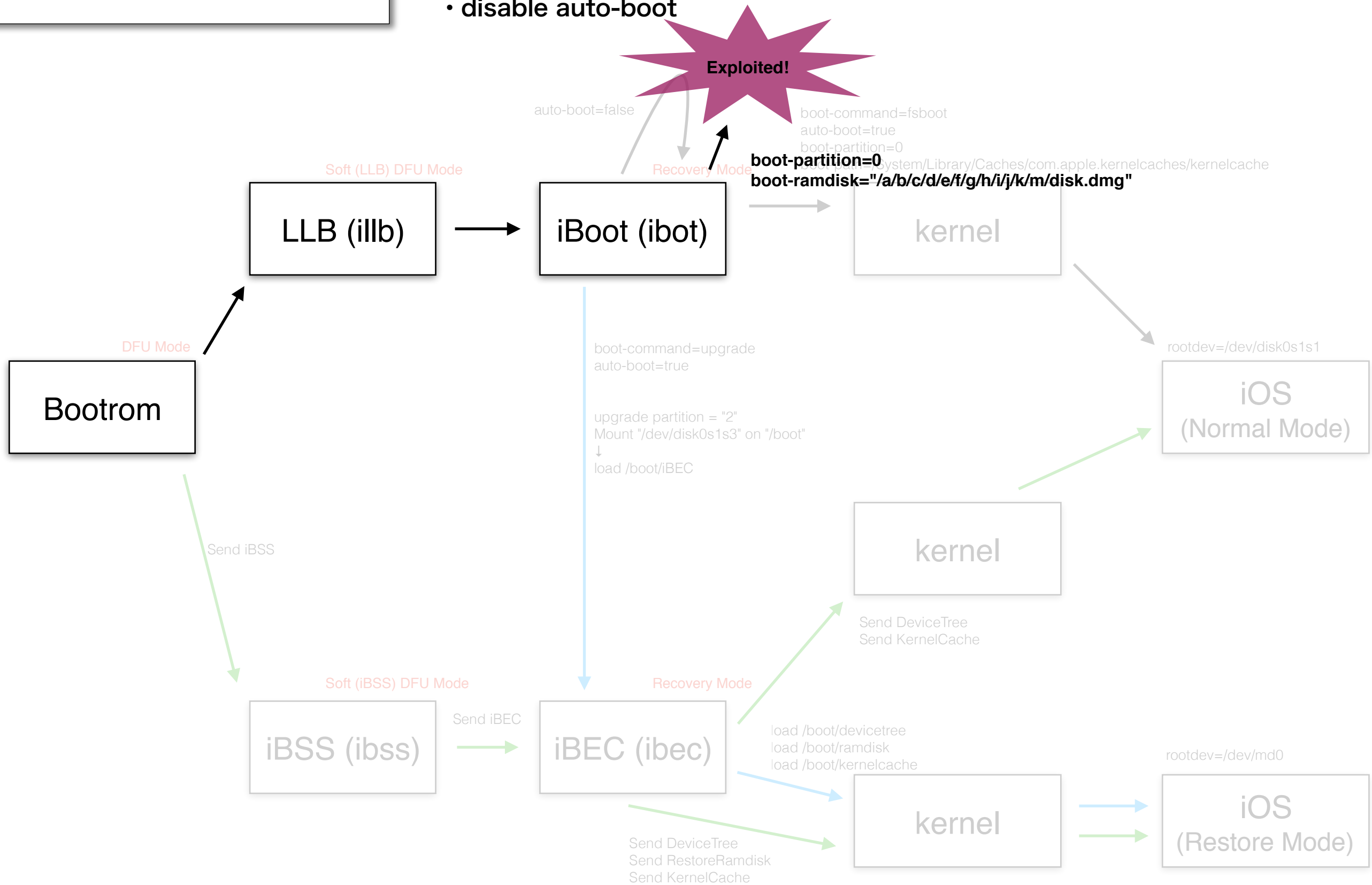
De Rebus Antiquis ramdiskF



De Rebus Antiquis ramdiskF

patching iBoot

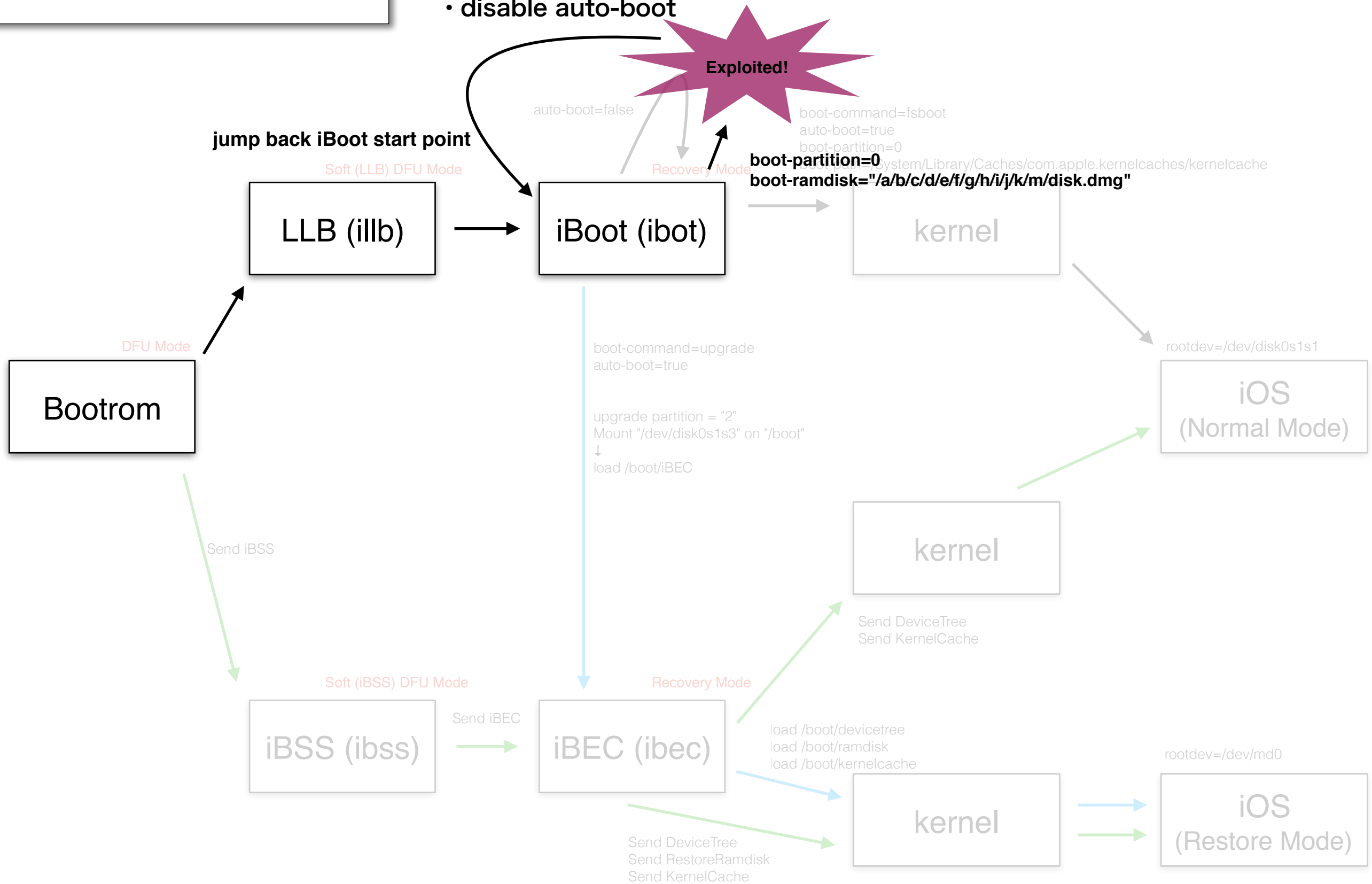
- rsa
- go command handler
- disable auto-boot



De Rebus Antiquis ramdiskF

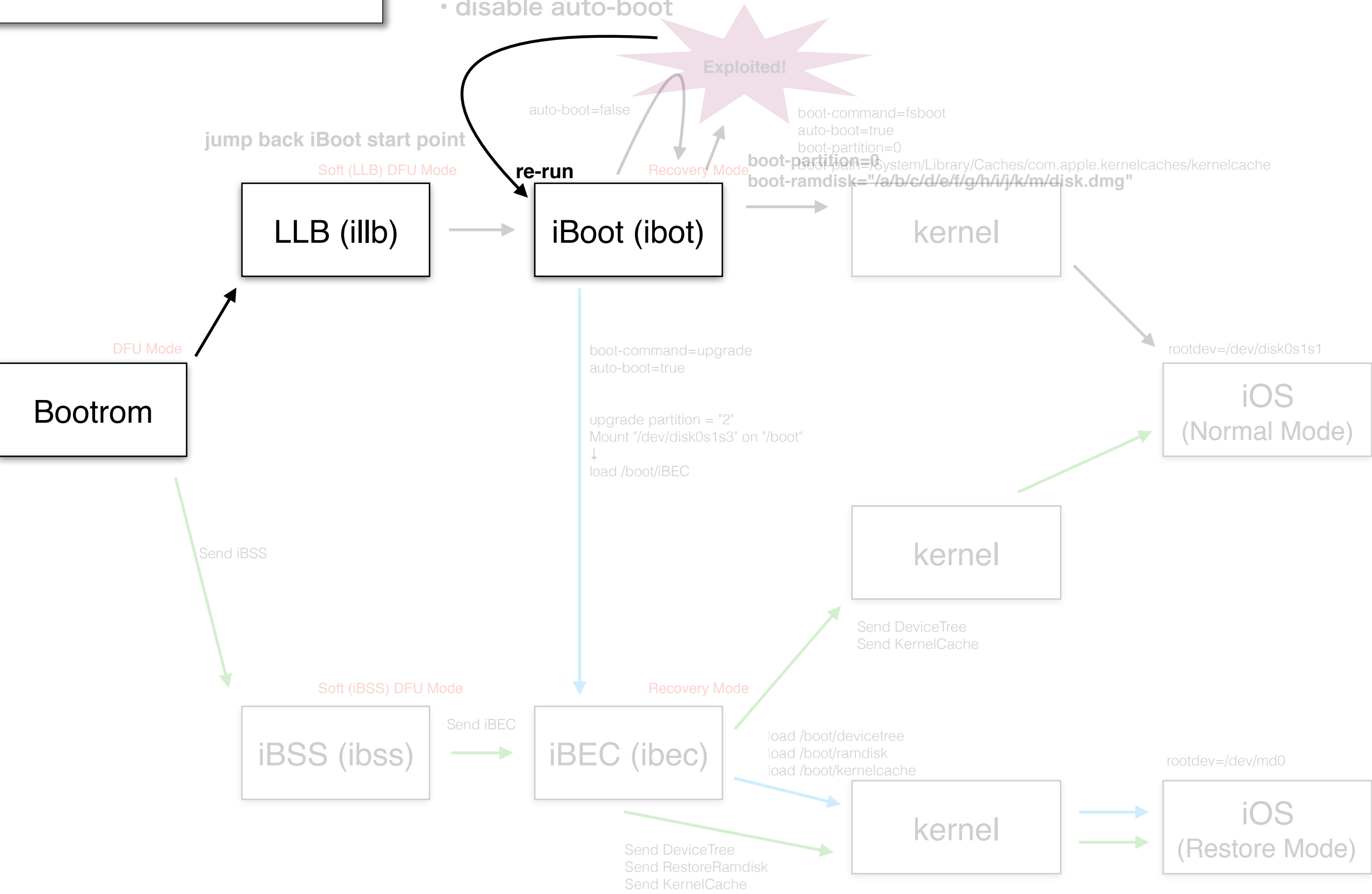
patching iBoot

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



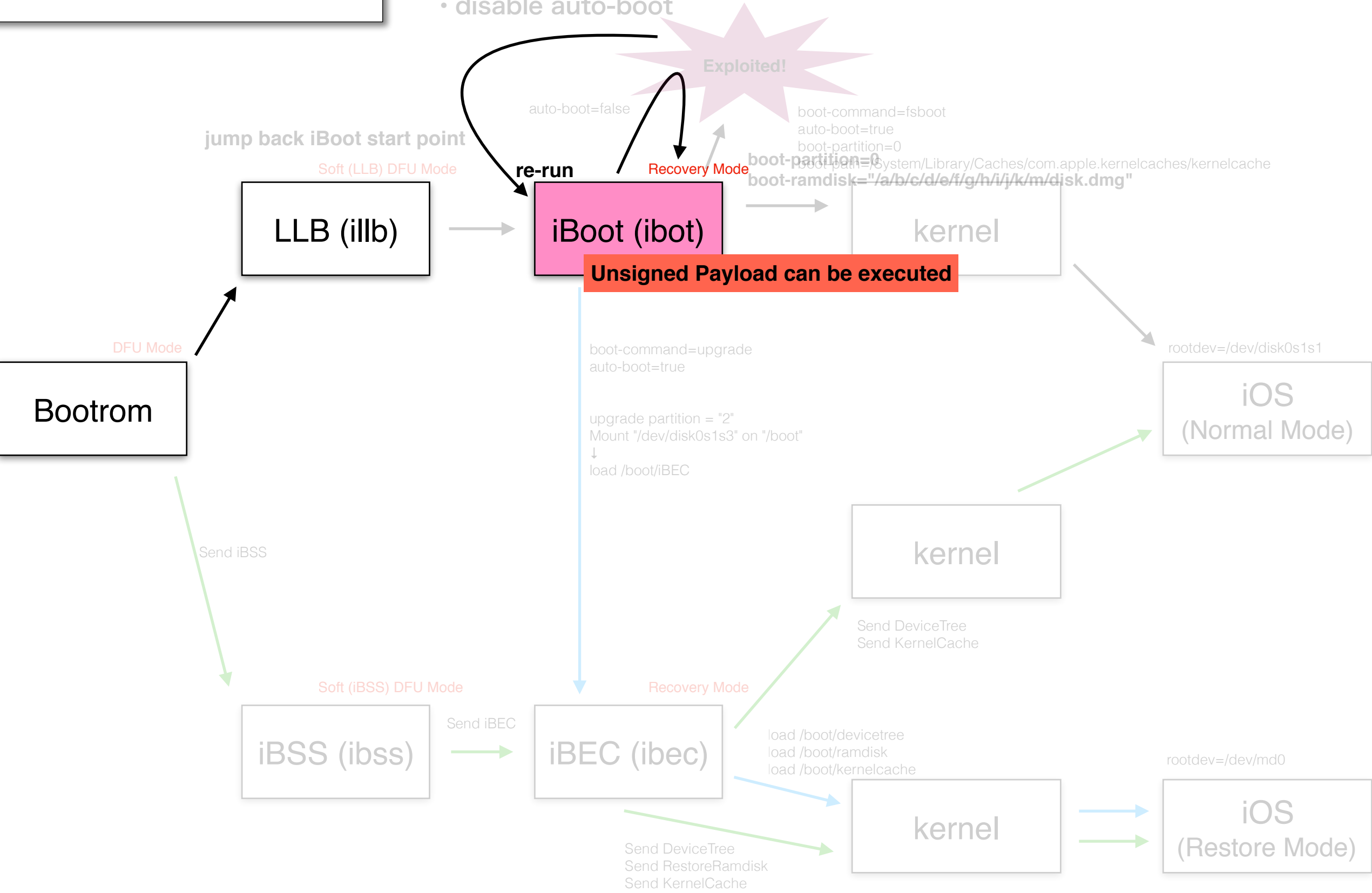
De Rebus Antiquis ramdiskF

- patching iBoot
- rsa
 - go command handler
 - disable auto-boot

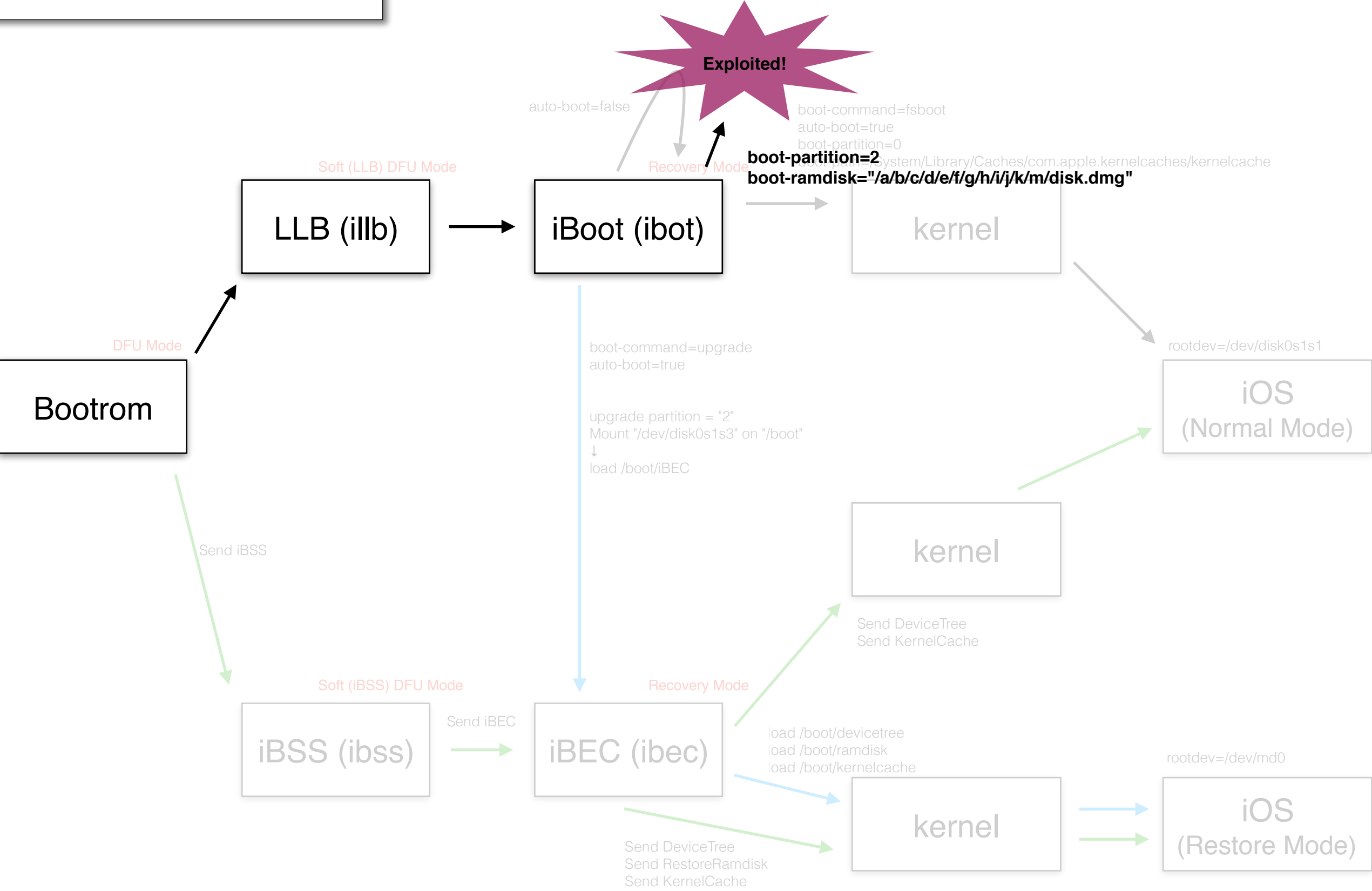


De Rebus Antiquis ramdiskF

- patching iBoot
- rsa
 - go command handler
 - disable auto-boot



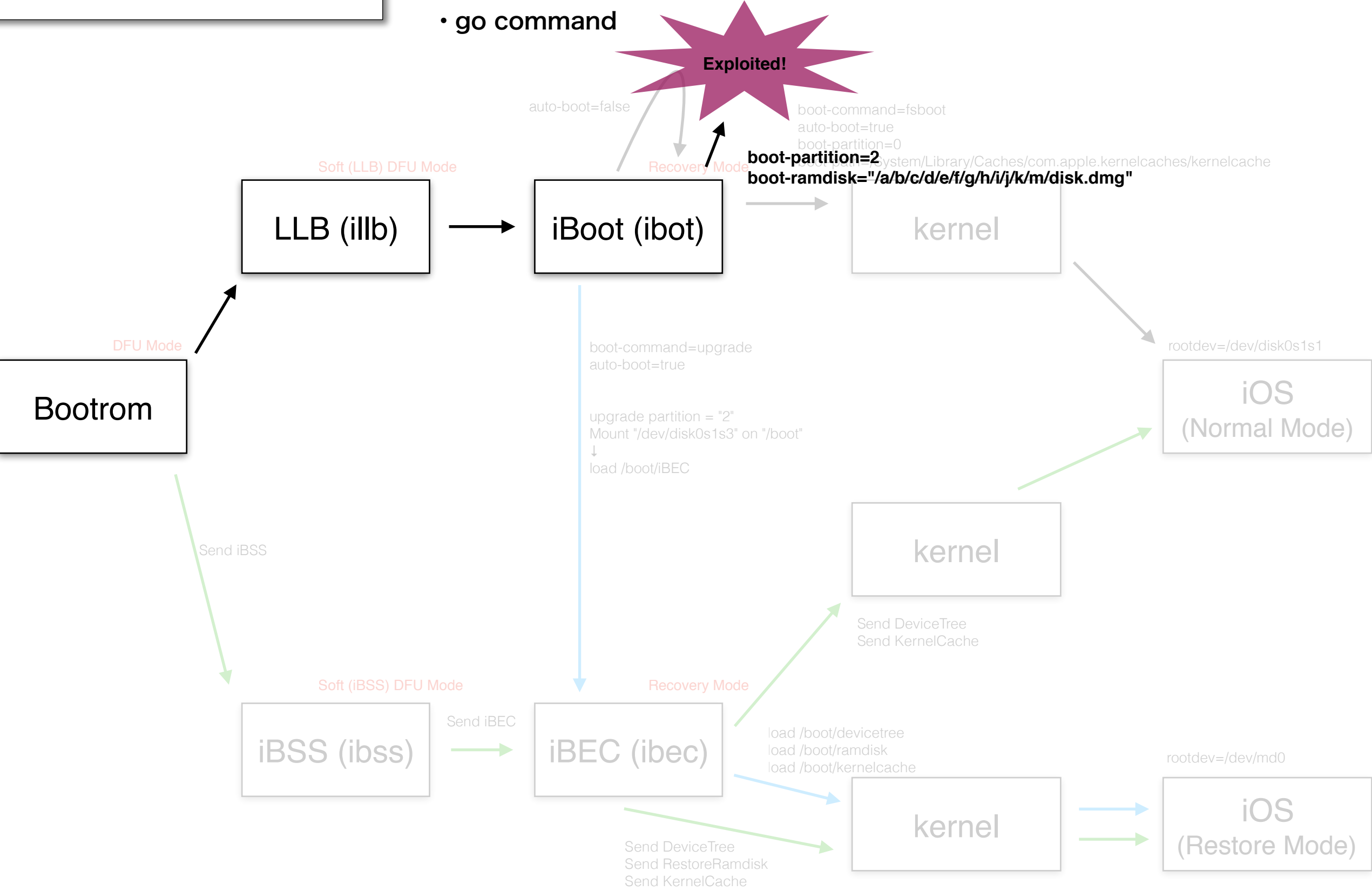
De Rebus Antiquis ramdiskH



De Rebus Antiquis ramdiskH

patching iBoot

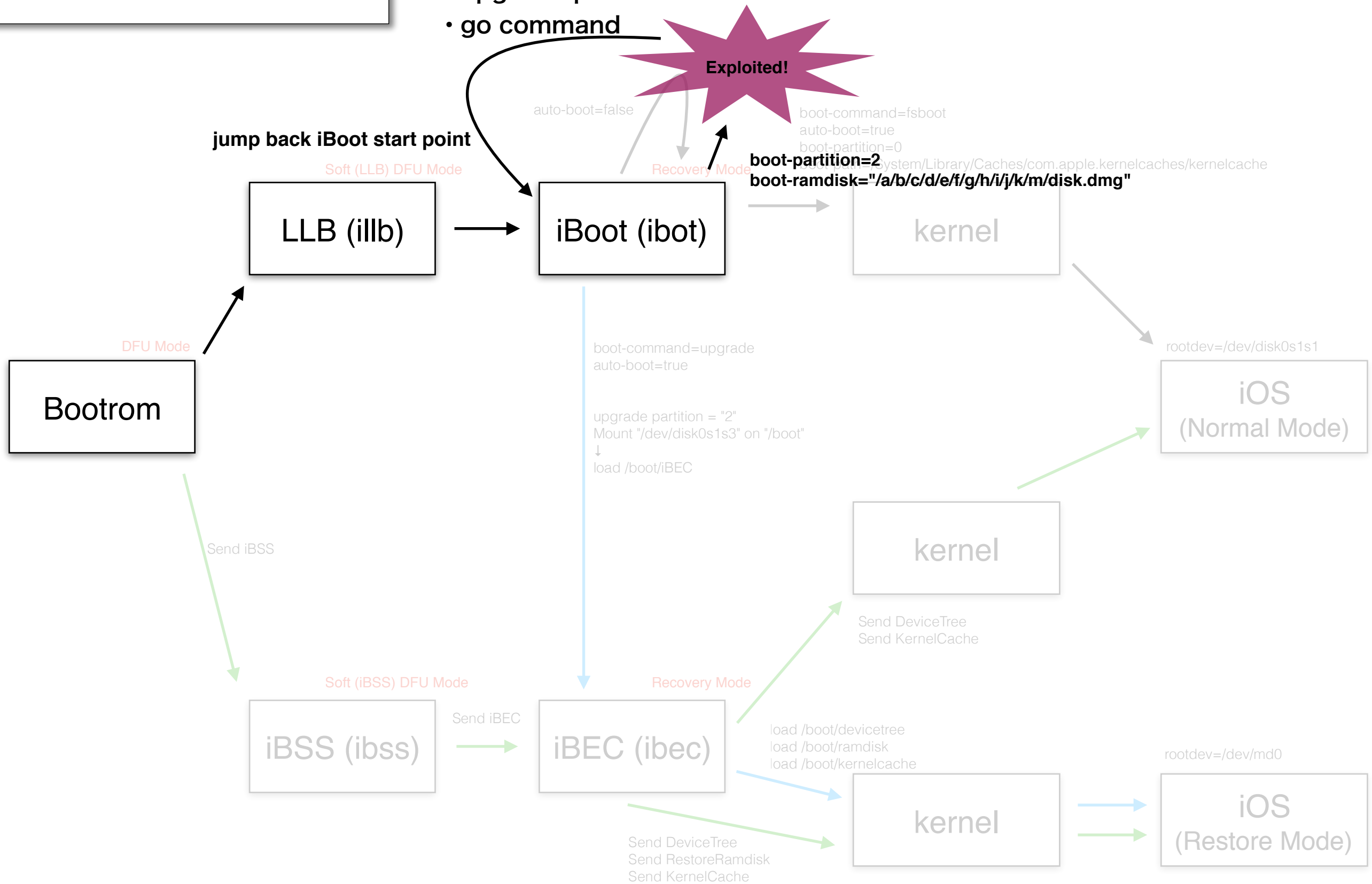
- rsa
- boot-command=fsboot
- upgrade-partition=3
- go command



De Rebus Antiquis ramdiskH

patching iBoot

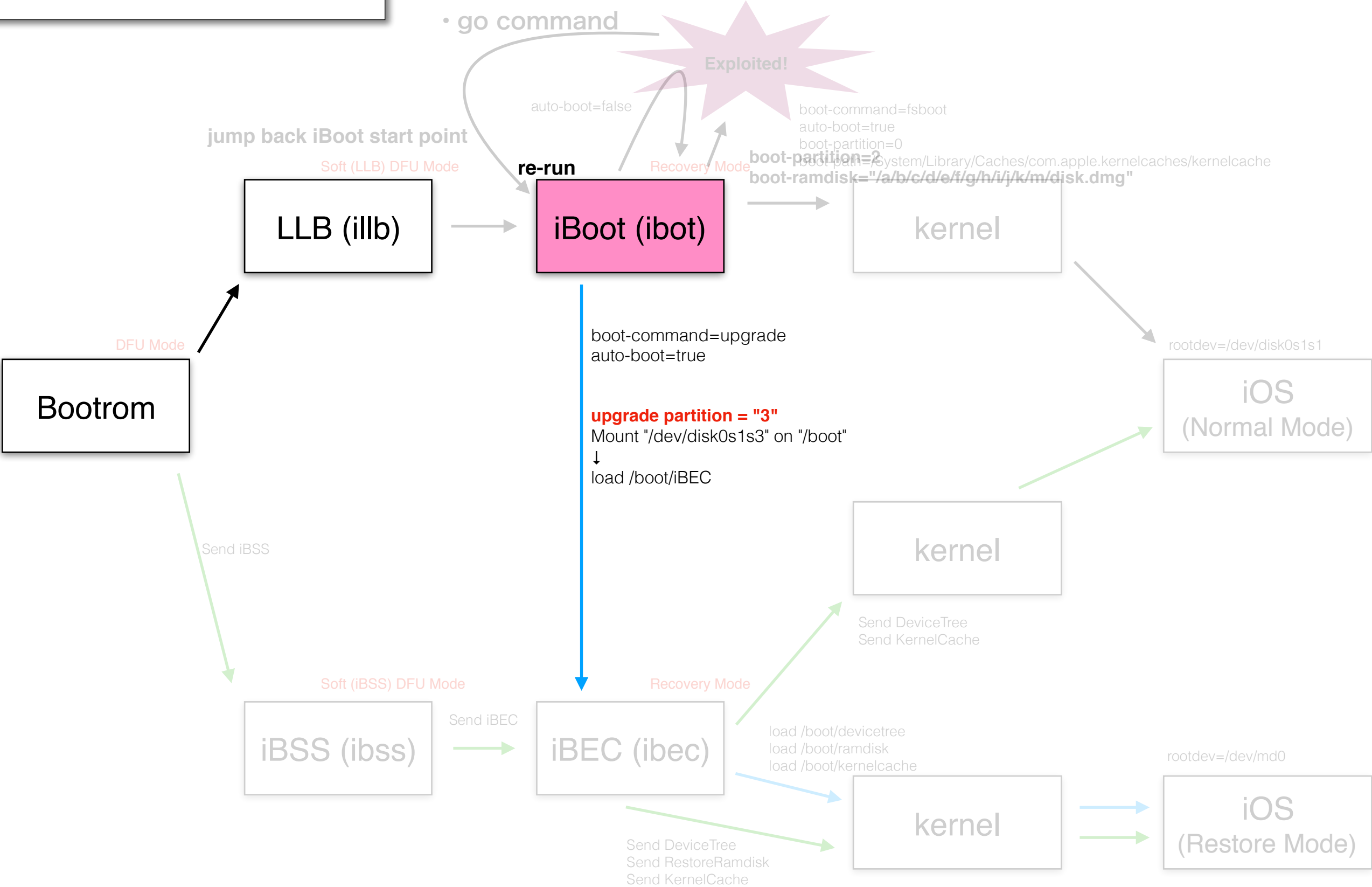
- `rsa`
- `boot-command=fsboot`
- `upgrade-partition=3`
- `go command`



De Rebus Antiquis ramdiskH

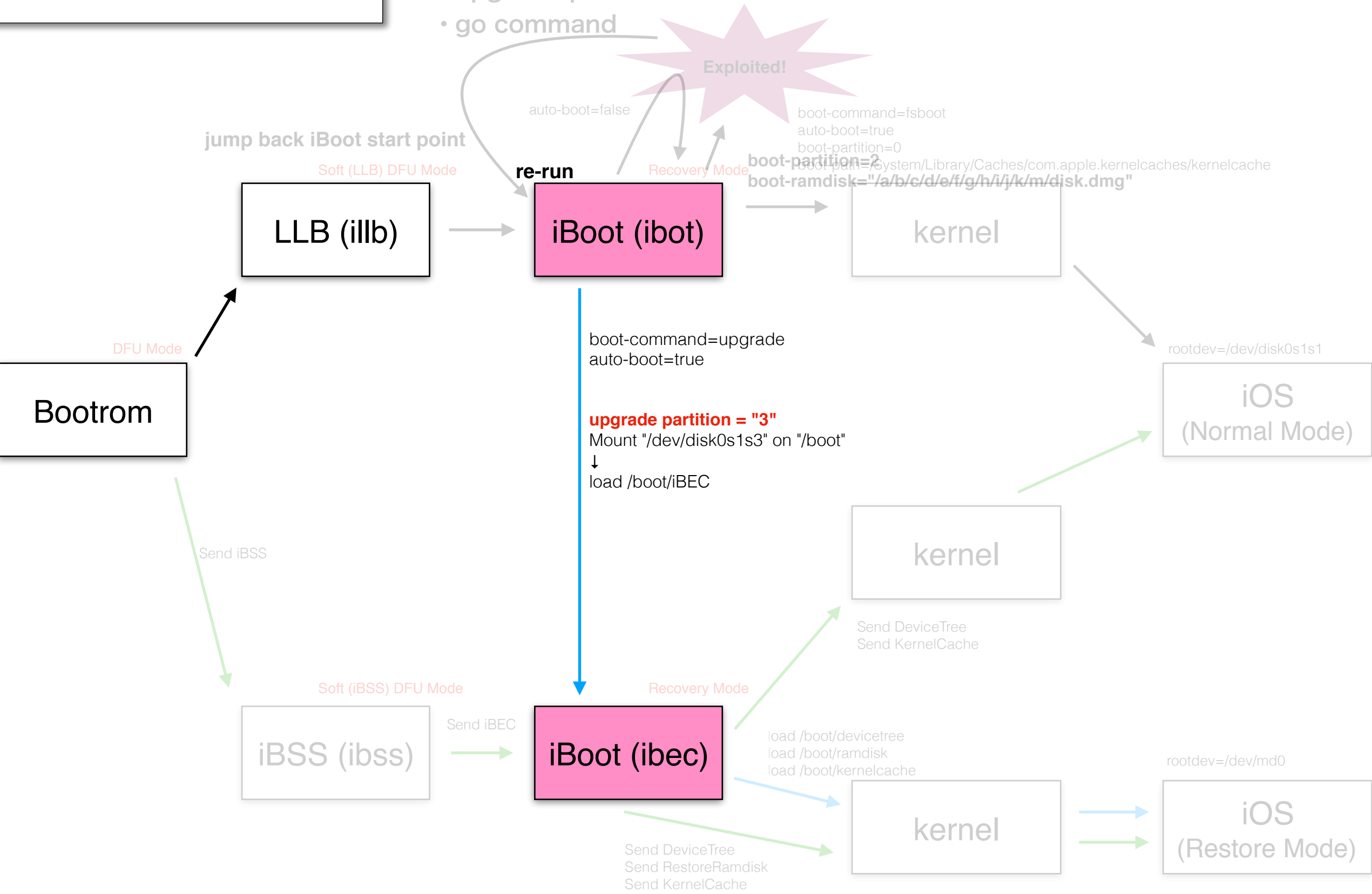
patching iBoot

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



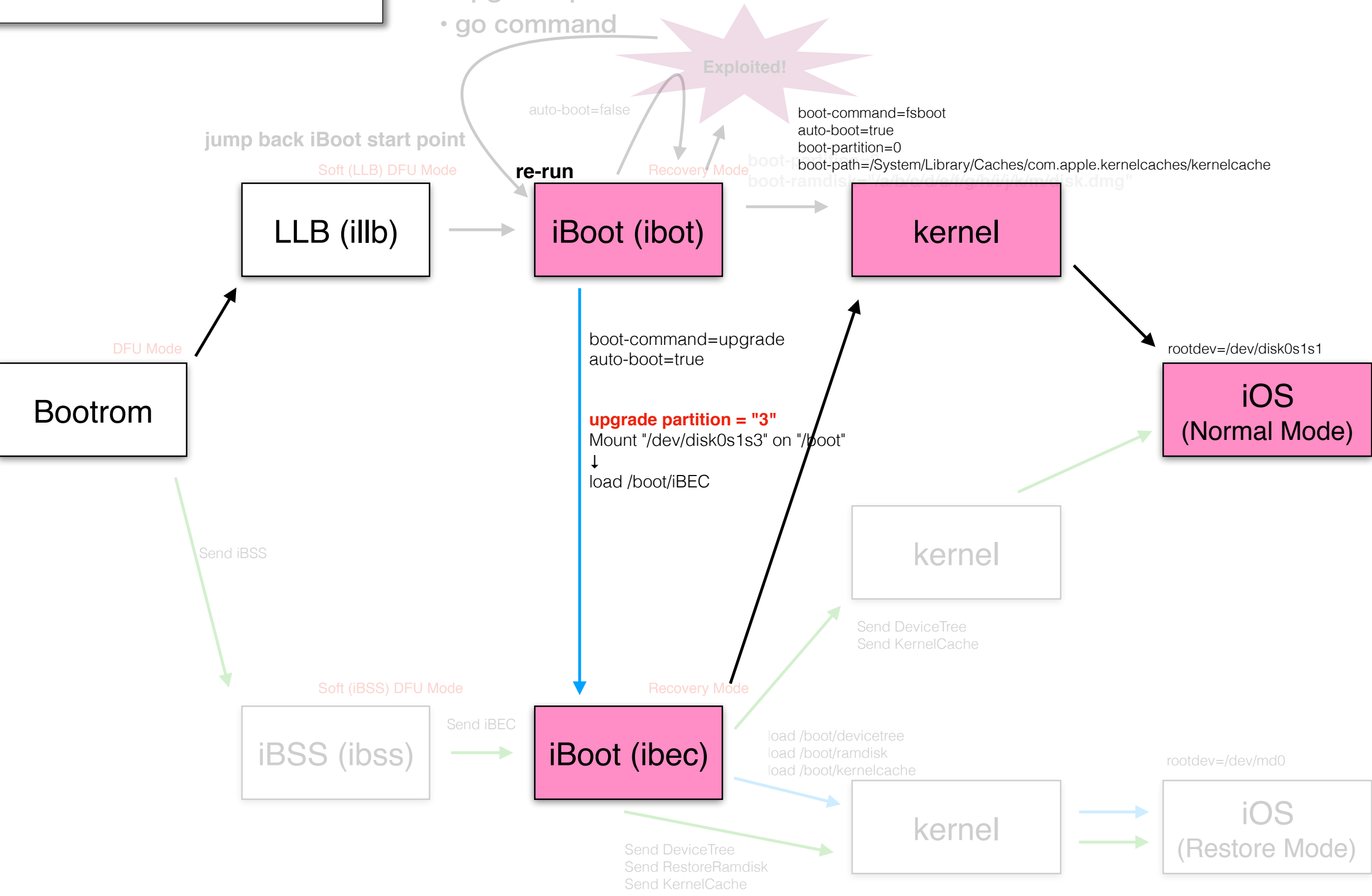
De Rebus Antiquis ramdiskH

- patching iBoot
- rsa
 - boot-command=fsboot
 - upgrade-partition=3
 - go command



De Rebus Antiquis ramdiskH

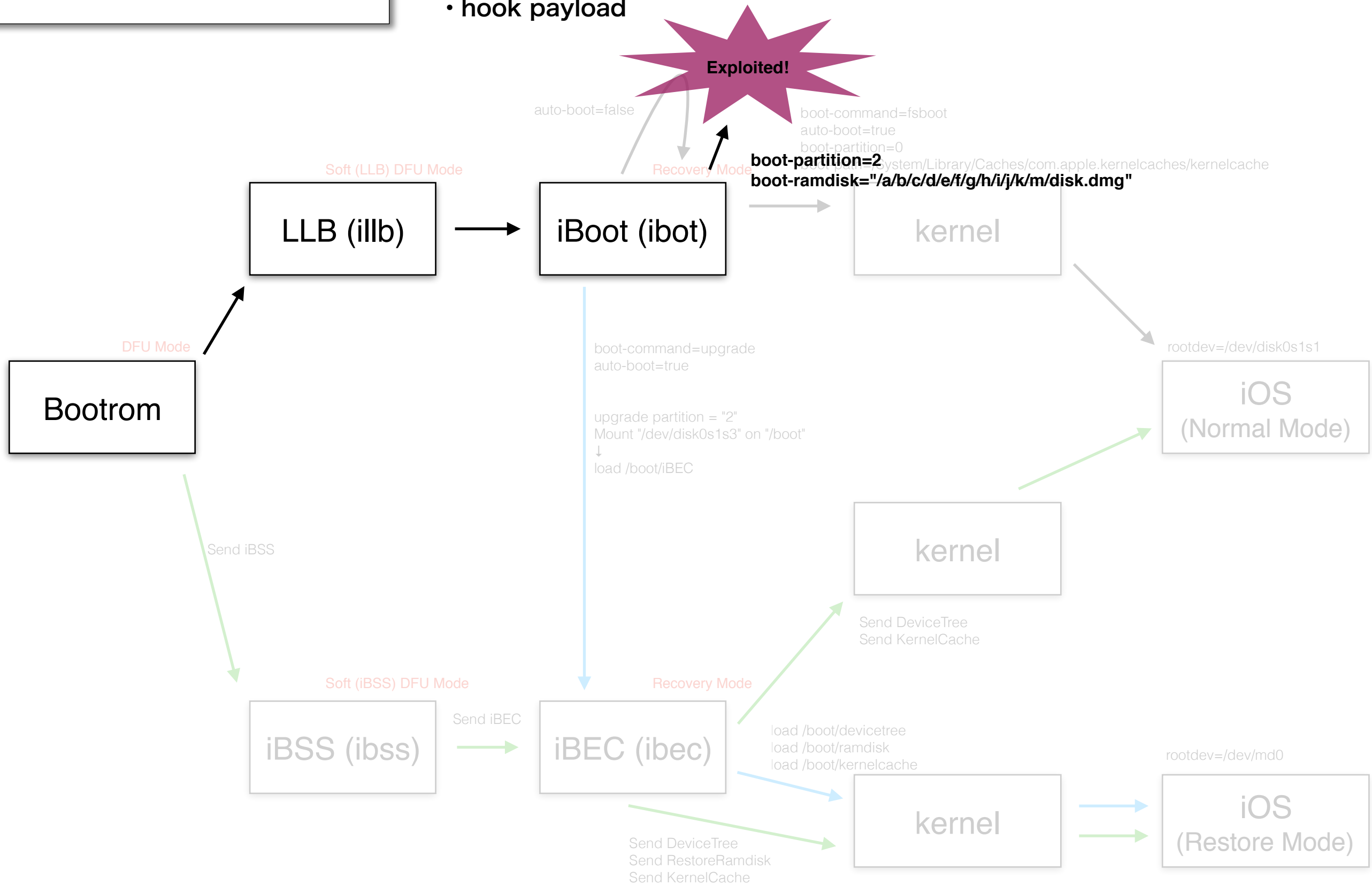
- patching iBoot
- rsa
 - boot-command=fsboot
 - upgrade-partition=3
 - go command



De Rebus Antiquis ramdiskl

patching iBoot

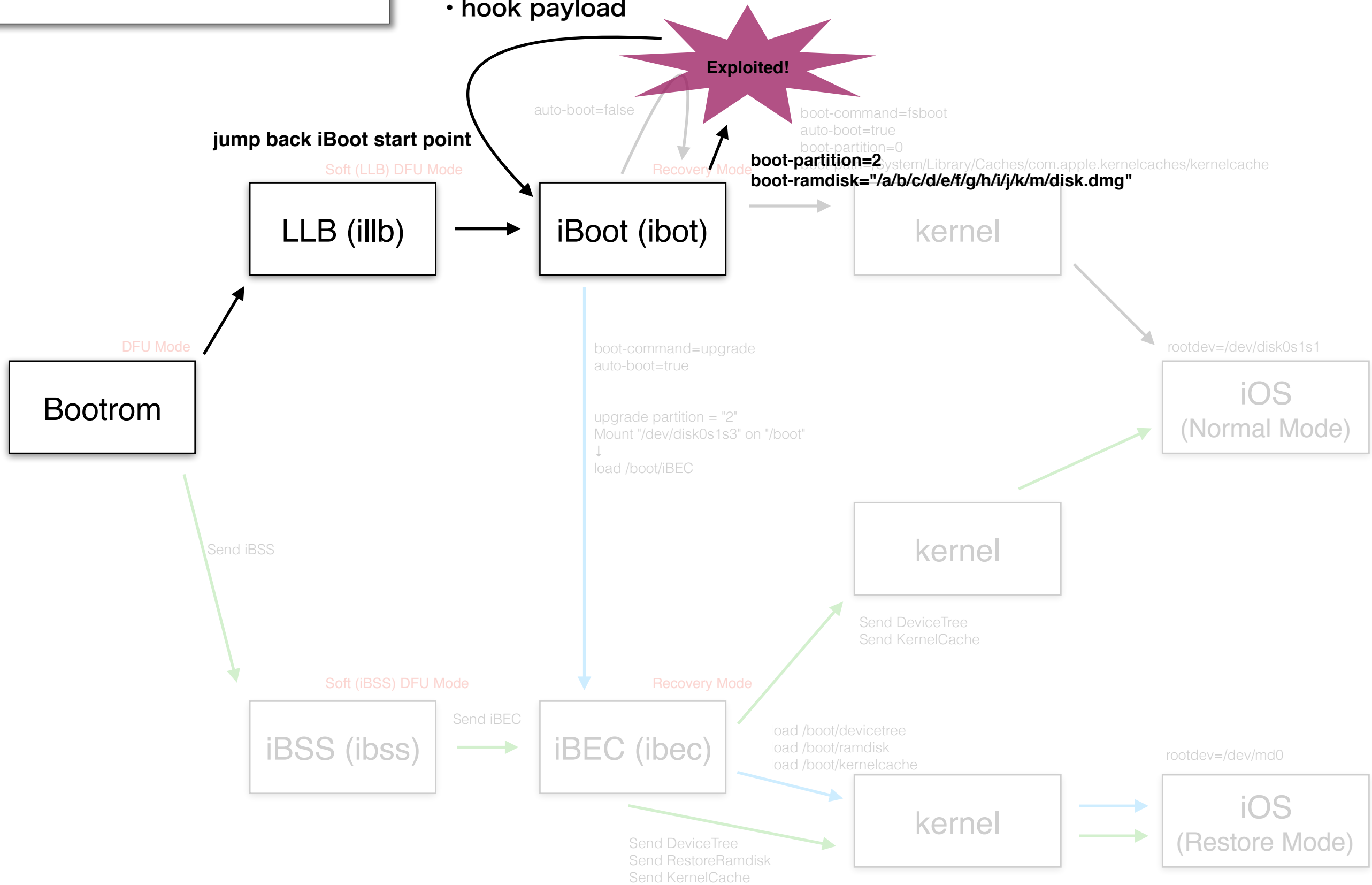
- rsa
- shellcode (image_load_func payload)
- hook payload



De Rebus Antiquis ramdiskl

patching iBoot

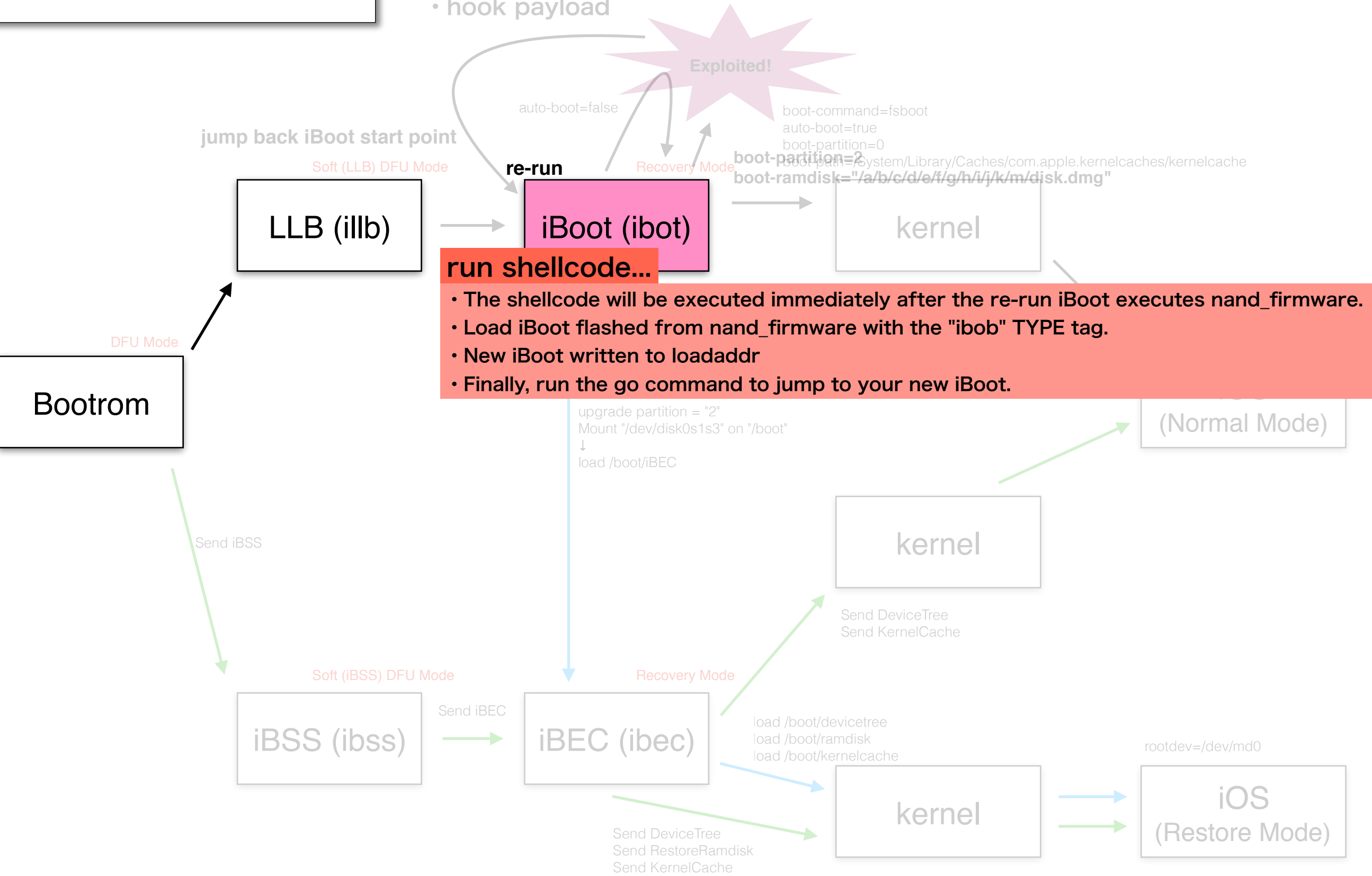
- rsa
- shellcode (image_load_func payload)
- hook payload



De Rebus Antiquis ramdiskl

patching iBoot

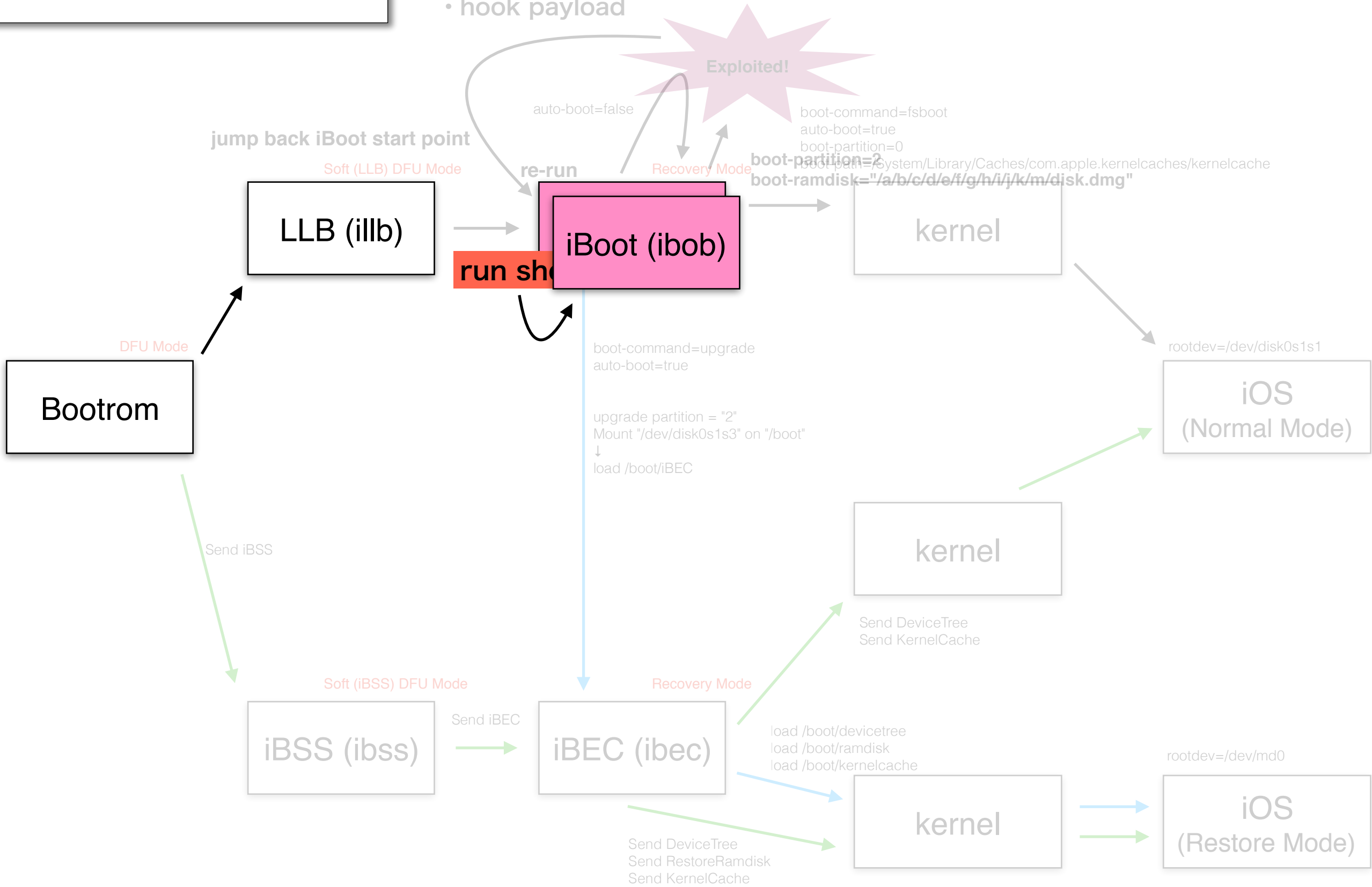
- rsa
- shellcode (image_load_func payload)
- hook payload



De Rebus Antiquis ramdiskl

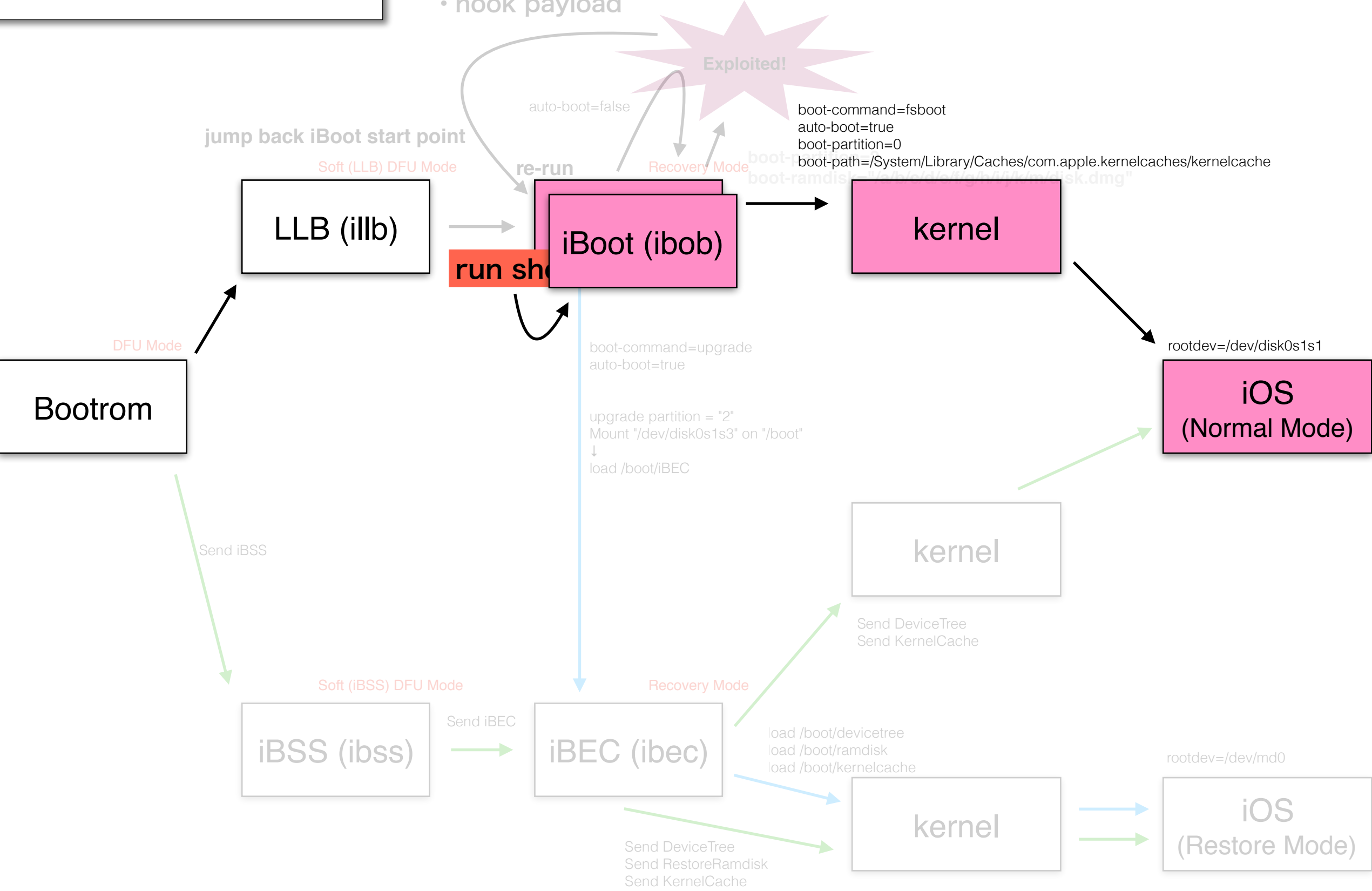
patching iBoot

- rsa
- shellcode (image_load_func payload)
- hook payload



De Rebus Antiquis ramdiskl

- patching iBoot
- rsa
 - shellcode (image_load_func payload)
 - hook payload

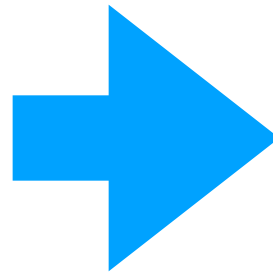


De Rebus Antiquis

How to use ramdisk1?

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

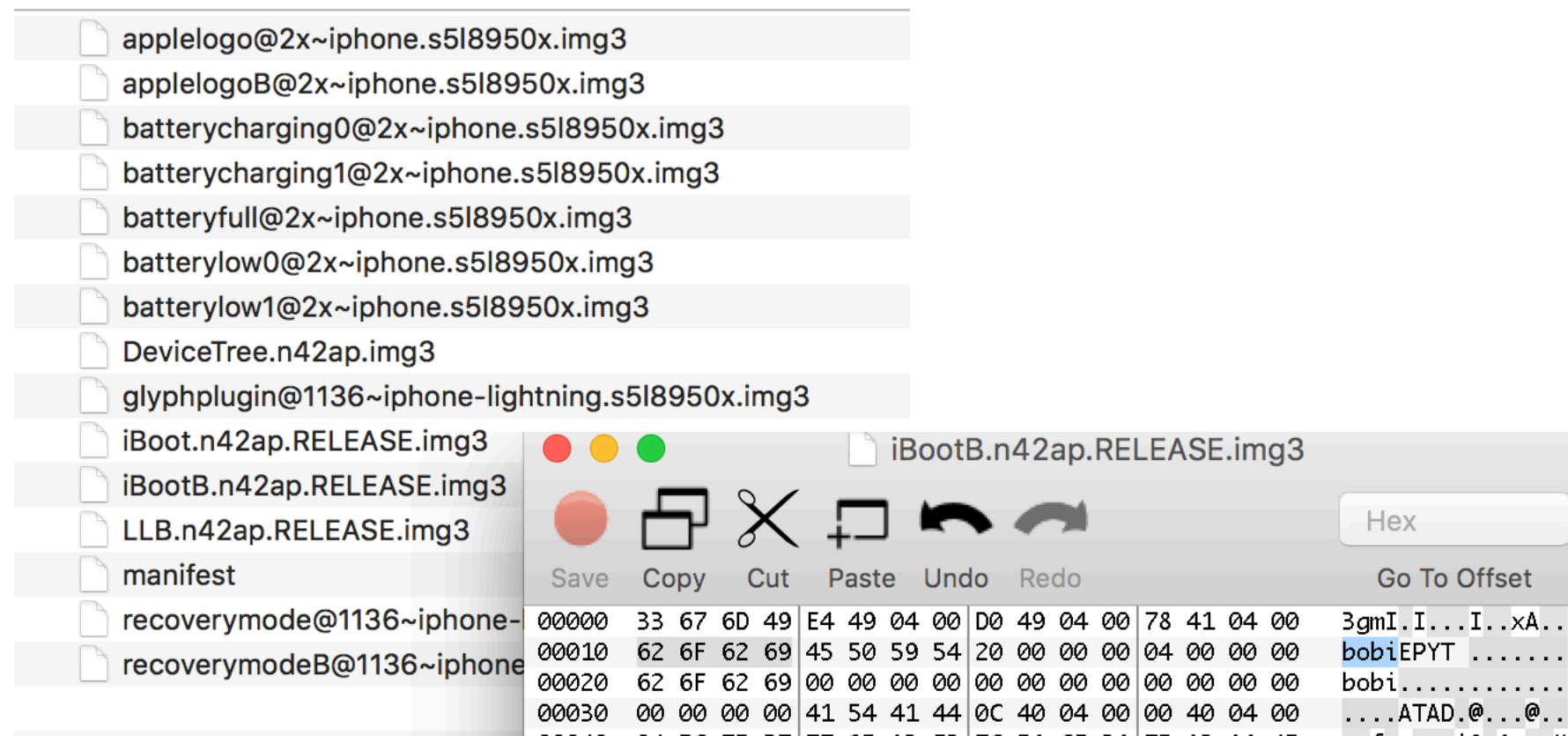
applelogo@2x~iphone.s5l8950x.img3
batterycharging0@2...hone.s5l8950x.img3
batterycharging1@2...hone.s5l8950x.img3
batteryfull@2x~iphone.s5l8950x.img3
batterylow0@2x~iphone.s5l8950x.img3
batterylow1@2x~iphone.s5l8950x.img3
DeviceTree.n42ap.img3
glyphplugin@1136~i...tning.s5l8950x.img3
iBoot.n42ap.RELEASE.img3
LLB.n42ap.RELEASE.img3
manifest
recoverymode@1136...tning.s5l8950x.img3



applelogo@2x~iphone.s5l8950x.img3
applelogoB@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
DeviceTree.n42ap.img3
glyphplugin@1136~iphone-lightning.s5l8950x.img3
iBoot.n42ap.RELEASE.img3
iBootB.n42ap.RELEASE.img3
LLB.n42ap.RELEASE.img3
manifest
recoverymode@1136~iphone-lightning.s5l8950x.img3
recoverymodeB@1136~iphone-lightning.s5l8950x.img3

De Rebus Antiquis How to use ramdiskl?

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

De Rebus Antiquis How to use ramdiskl?

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

De Rebus Antiquis

How to use ramdiskl?

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

De Rebus Antiquis

How to use ramdiskl?

iBoot vs iBootB

iBoot

Do not do anything

iBootB

Apply patches

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

De Rebus Antiquis How to use ramdiskl?

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...**