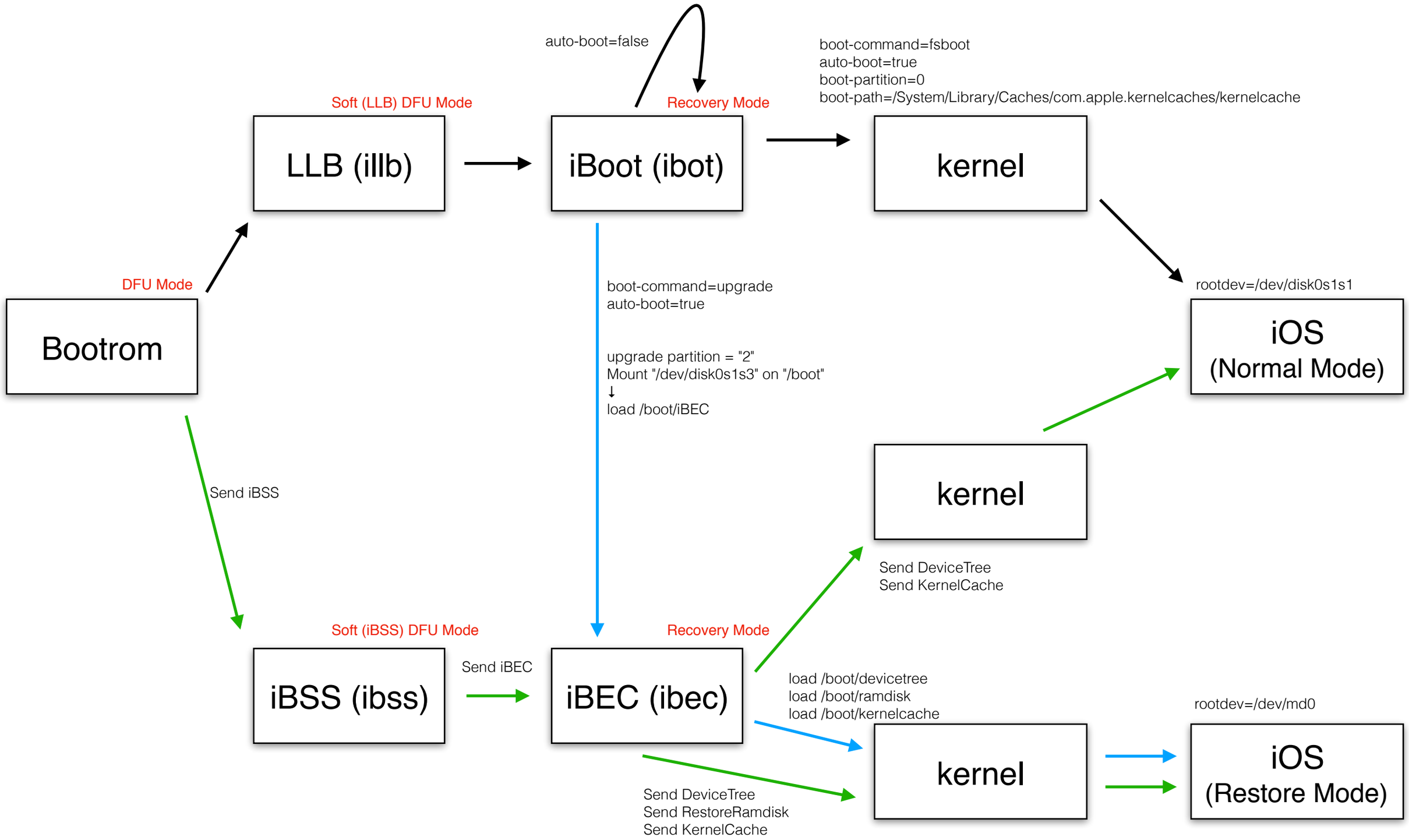
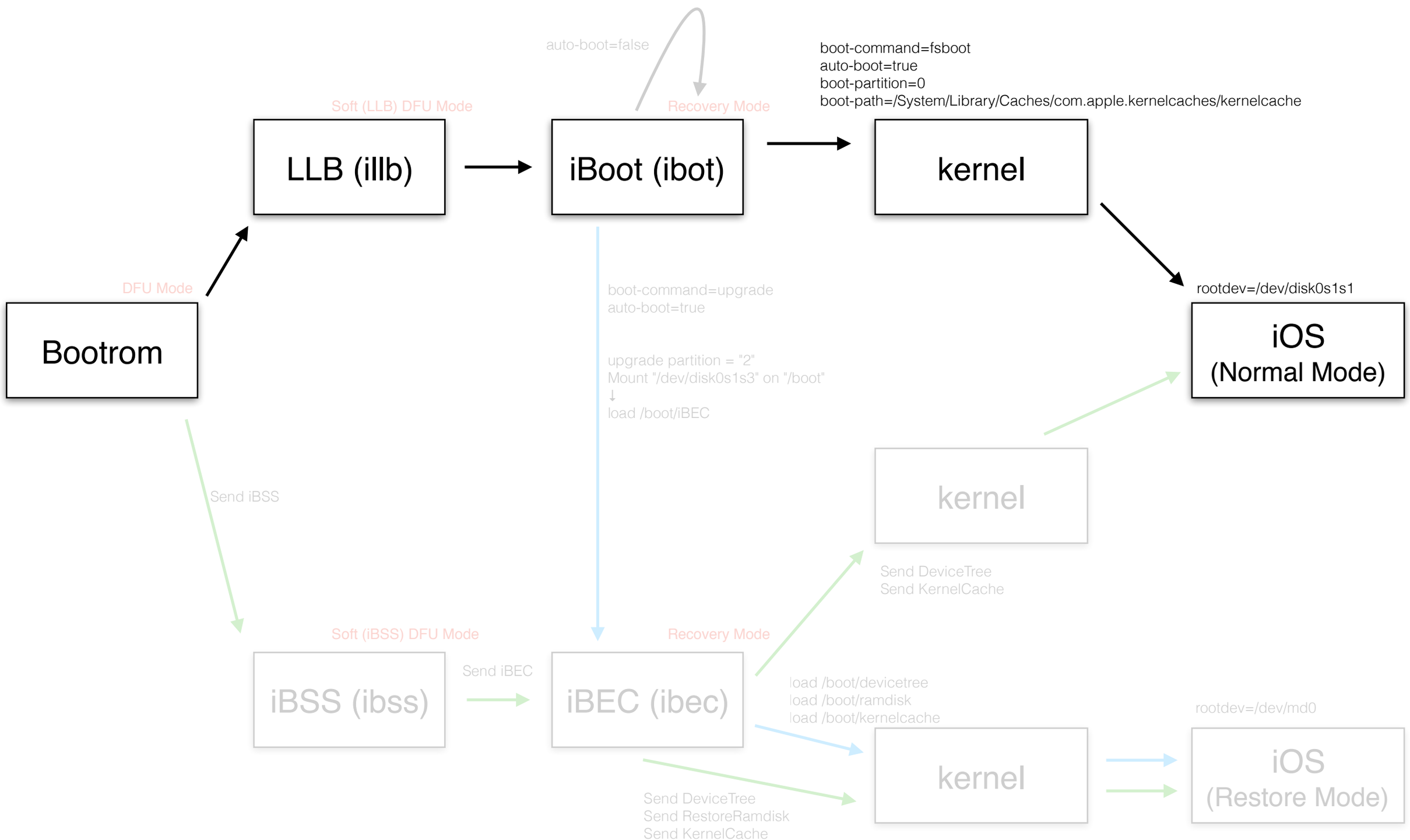
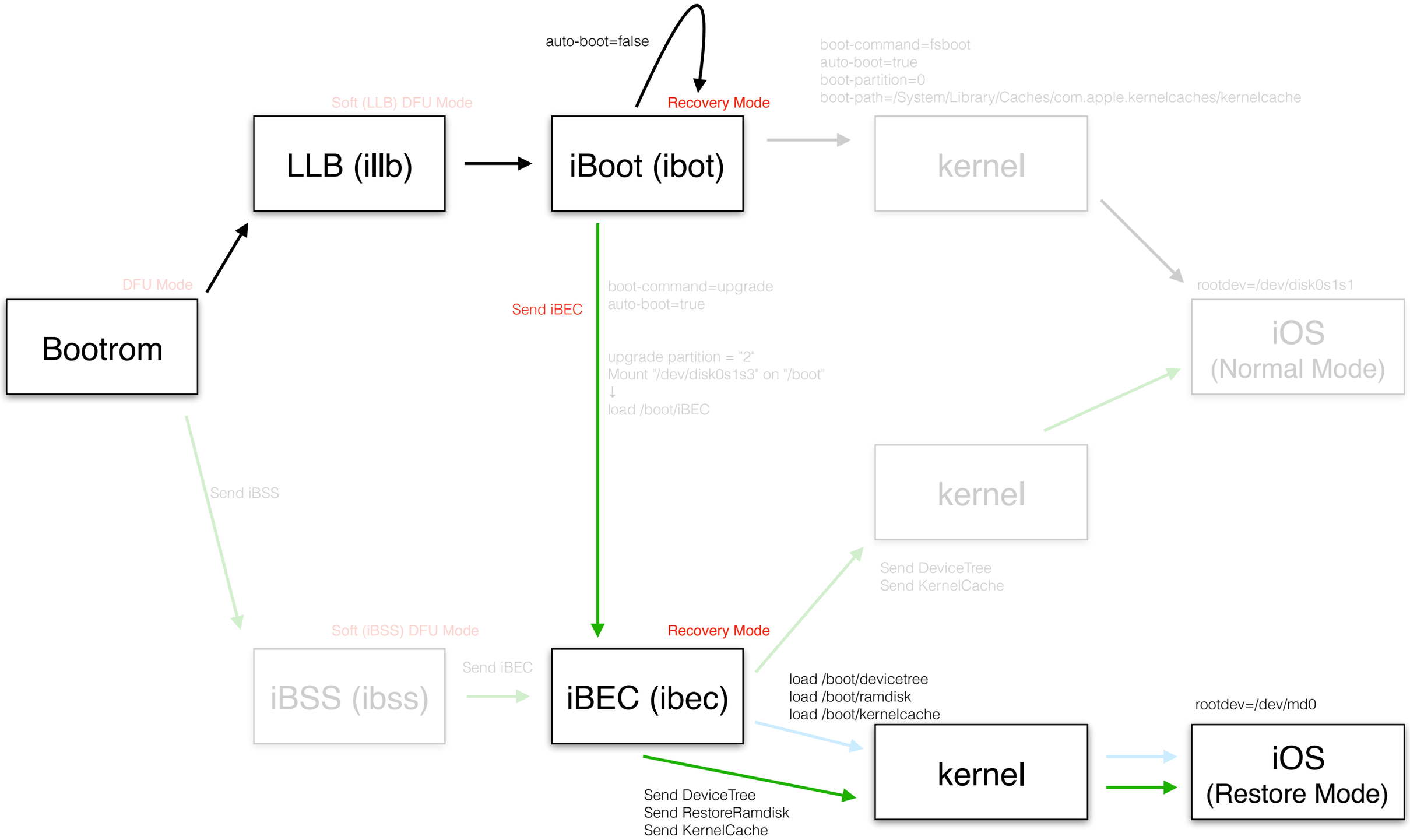
32-bit iOS devices boot chain



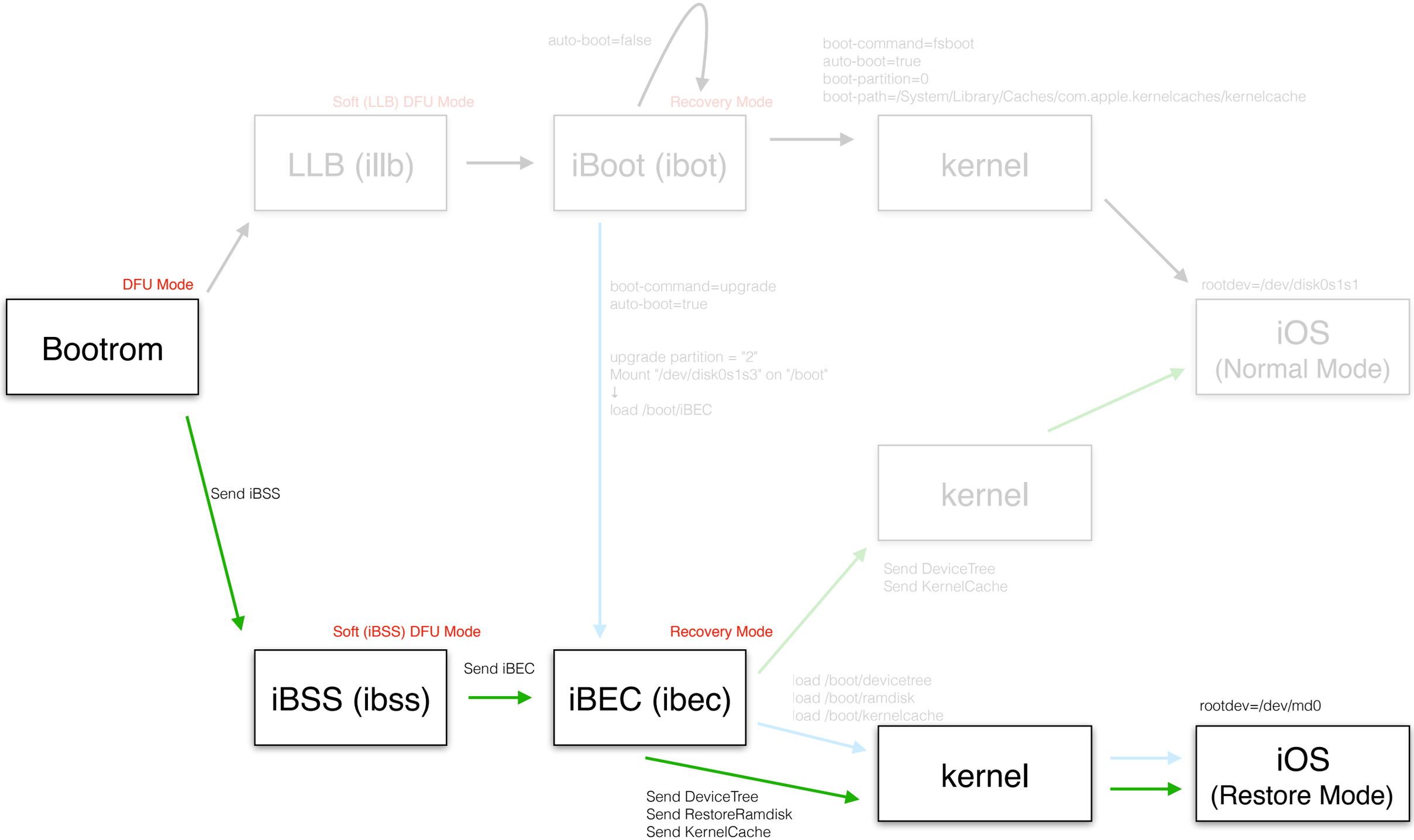
Normal Boot


auto-boot=false
Soft (LLB) DFU Mode
Recovery Mode
boot-command=fsboot
auto-boot=true
boot-partition=0
boot-path=/System/Library/Caches/com.apple.kernelcaches/kernelcache
LLB (illb)
iBoot (ibot)
kernel
DFU Mode
boot-command=upgrade
auto-boot=true
rootdev=/dev/disk0s1s1
upgrade partition = "2"
Mount "/dev/disk0s1s3" on "/boot"
↓
load /boot/iBEC
Bootrom
iOS
(Normal Mode)
kernel
Send iBSS
Send DeviceTree
Send KernelCache
Soft (iBSS) DFU Mode
Recovery Mode
Send iBEC
load /boot/devicetree
load /boot/ramdisk
load /boot/kernelcache
rootdev=/dev/md0
iBSS (ibss)
iBEC (ibec)
kernel
iOS
(Restore Mode)
Send DeviceTree
Send RestoreRamdisk
Send KernelCache

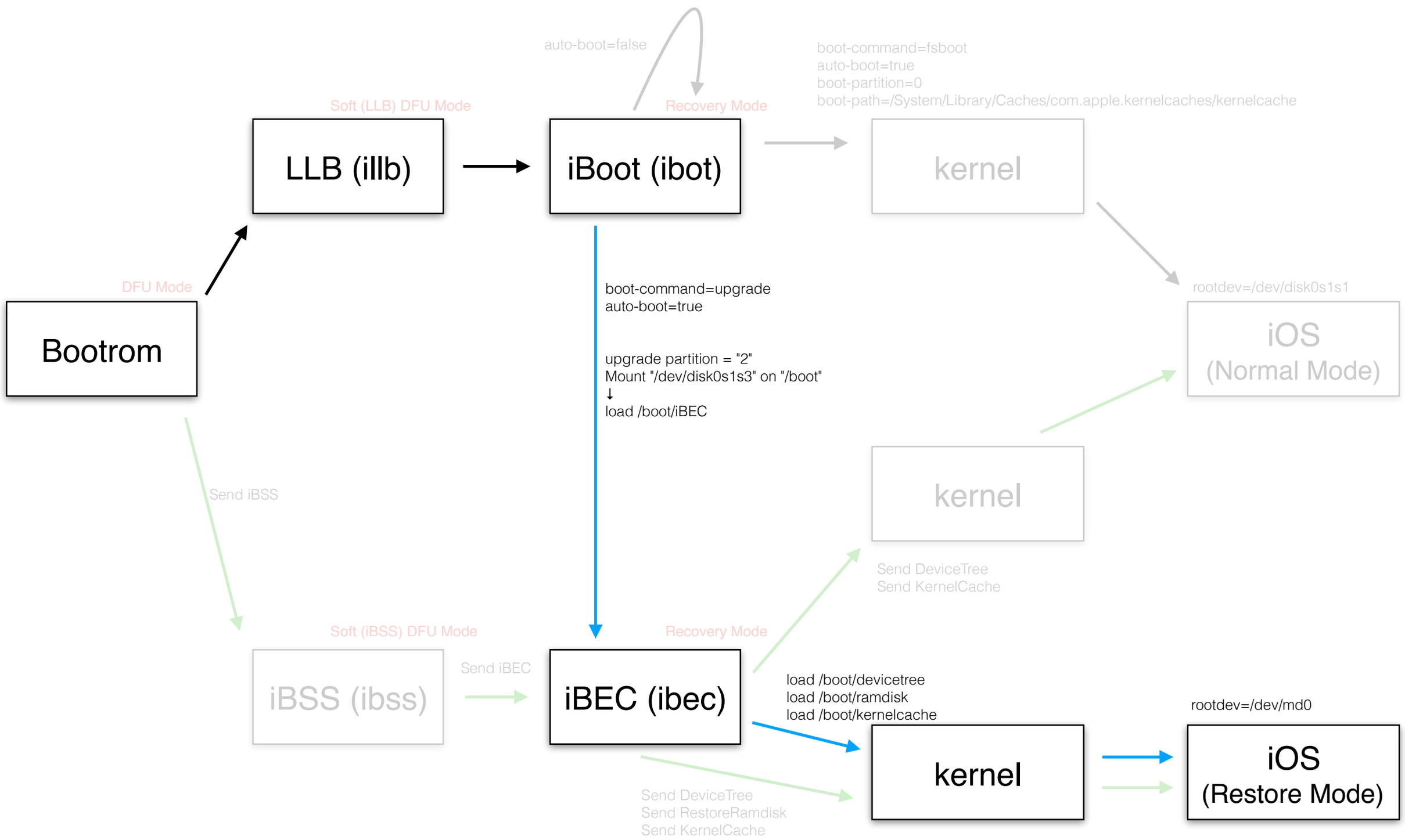
Restore/Update (Recovery)



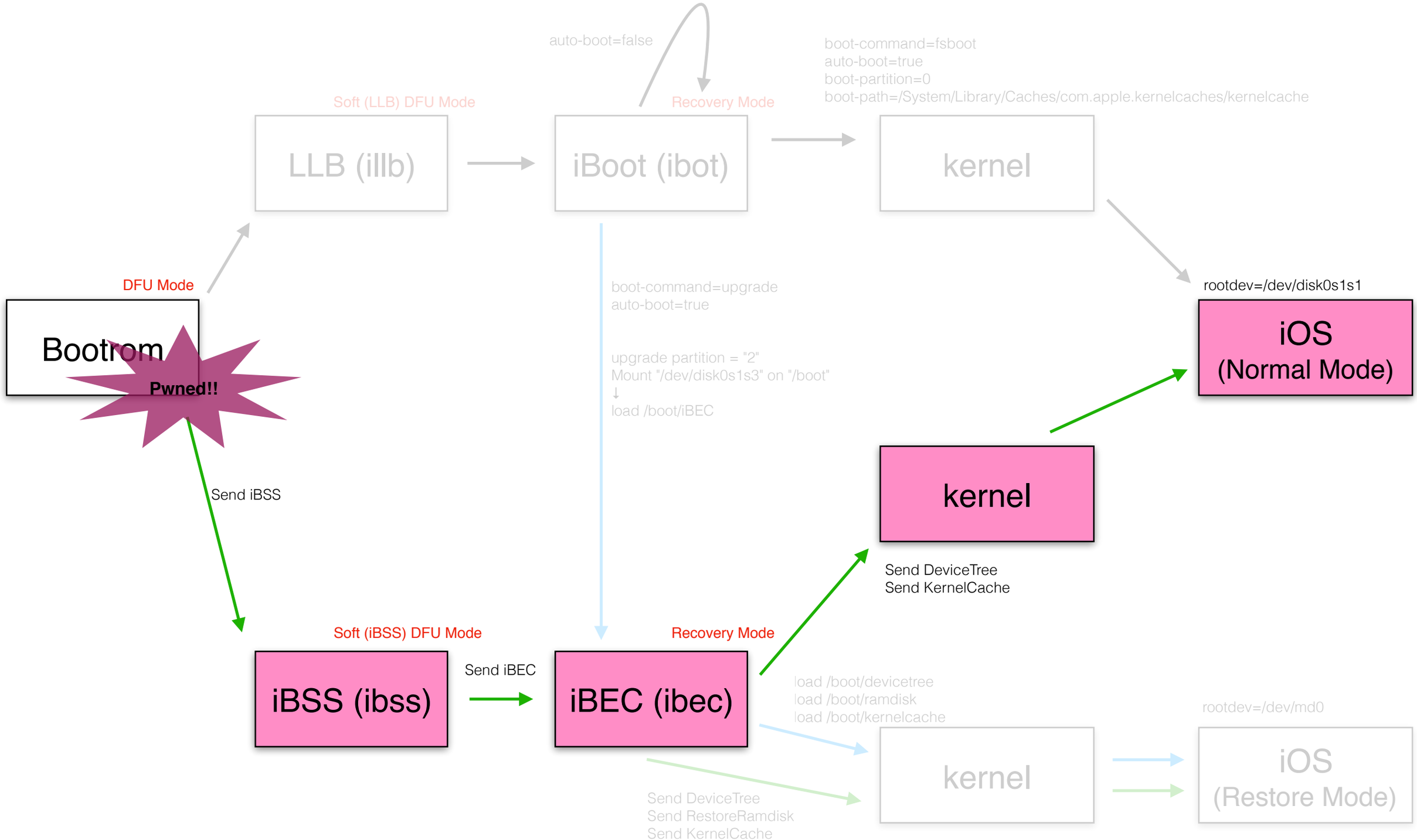
Restore/Update (DFU)



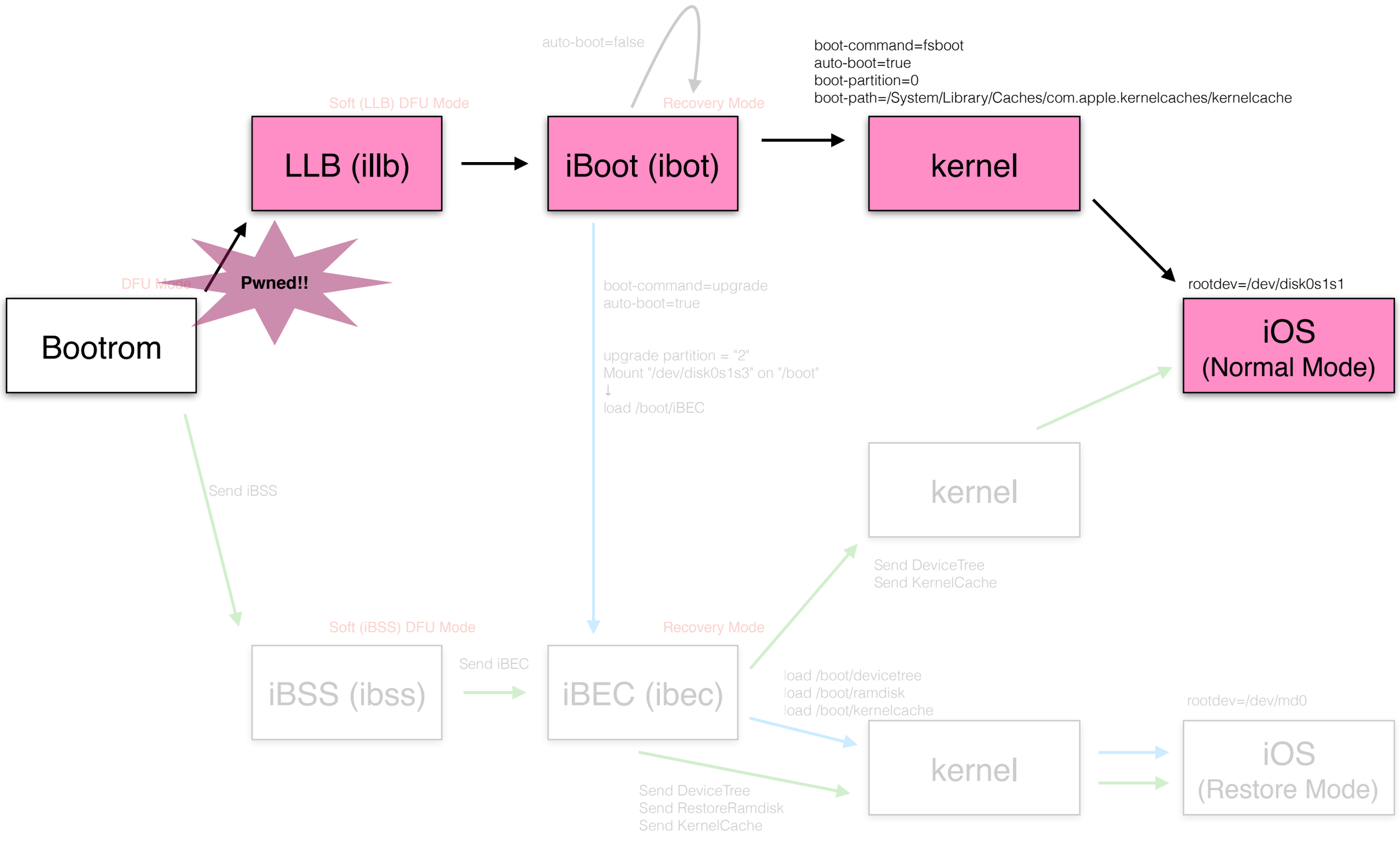
OTA Update


auto-boot=false
boot-command=fsboot
auto-boot=true
boot-partition=0
boot-path=/System/Library/Caches/com.apple.kernelcaches/kernelcache
Soft (LLB) DFU Mode
Recovery Mode
LLB (illb)
iBoot (ibot)
kernel
DFU Mode
rootdev=/dev/disk0s1s1
Bootrom
iOS
(Normal Mode)
boot-command=upgrade
auto-boot=true
upgrade partition = "2"
Mount "/dev/disk0s1s3" on "/boot"
↓
load /boot/iBEC
kernel
Send iBSS
Send DeviceTree
Send KernelCache
Soft (iBSS) DFU Mode
Recovery Mode
iBSS (ibss)
Send iBEC
iBEC (ibec)
load /boot/devicetree
load /boot/ramdisk
load /boot/kernelcache
rootdev=/dev/md0
kernel
iOS
(Restore Mode)
Send DeviceTree
Send RestoreRamdisk
Send KernelCache

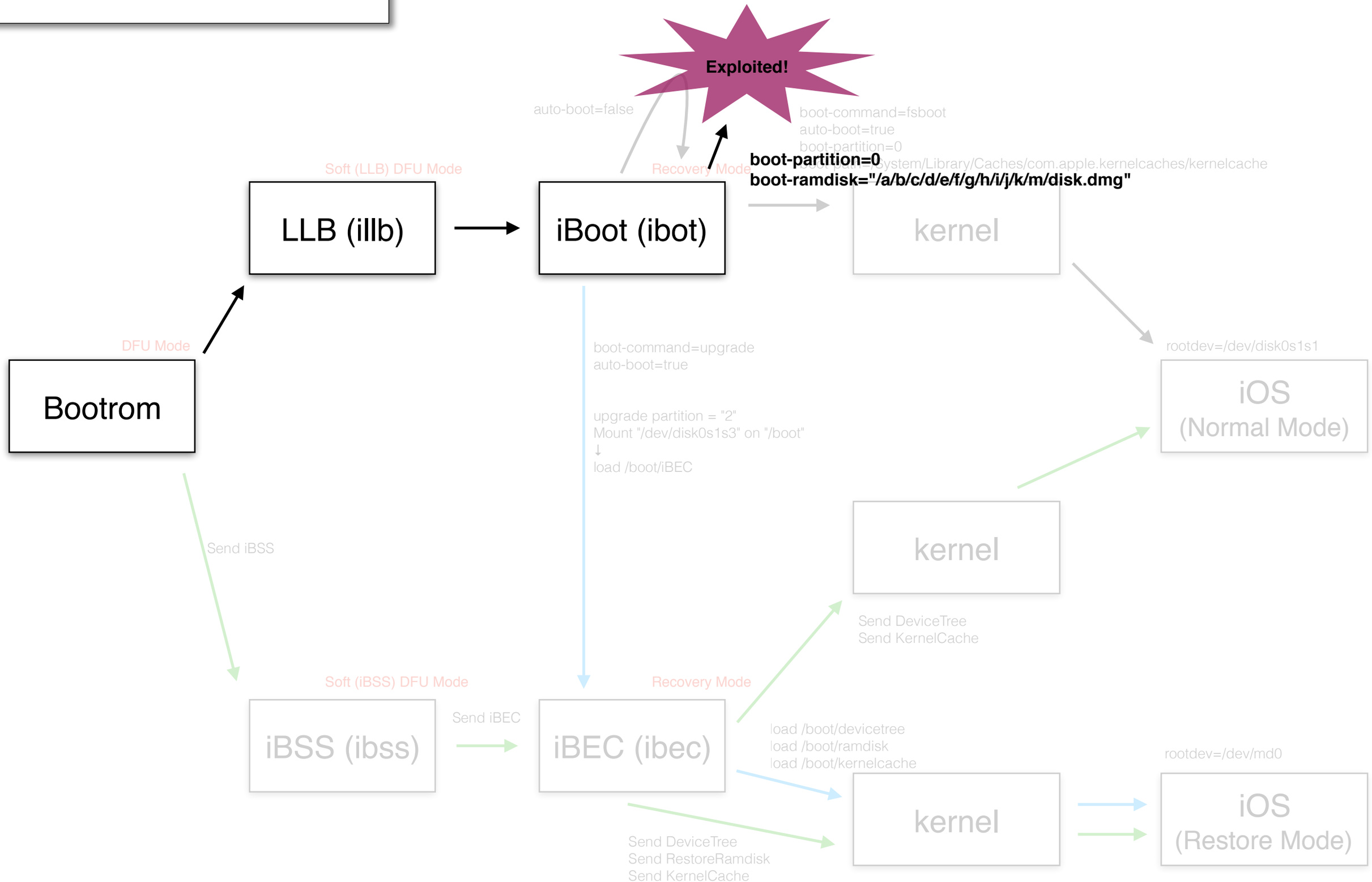
Just Boot (limera1n)



24kpwn

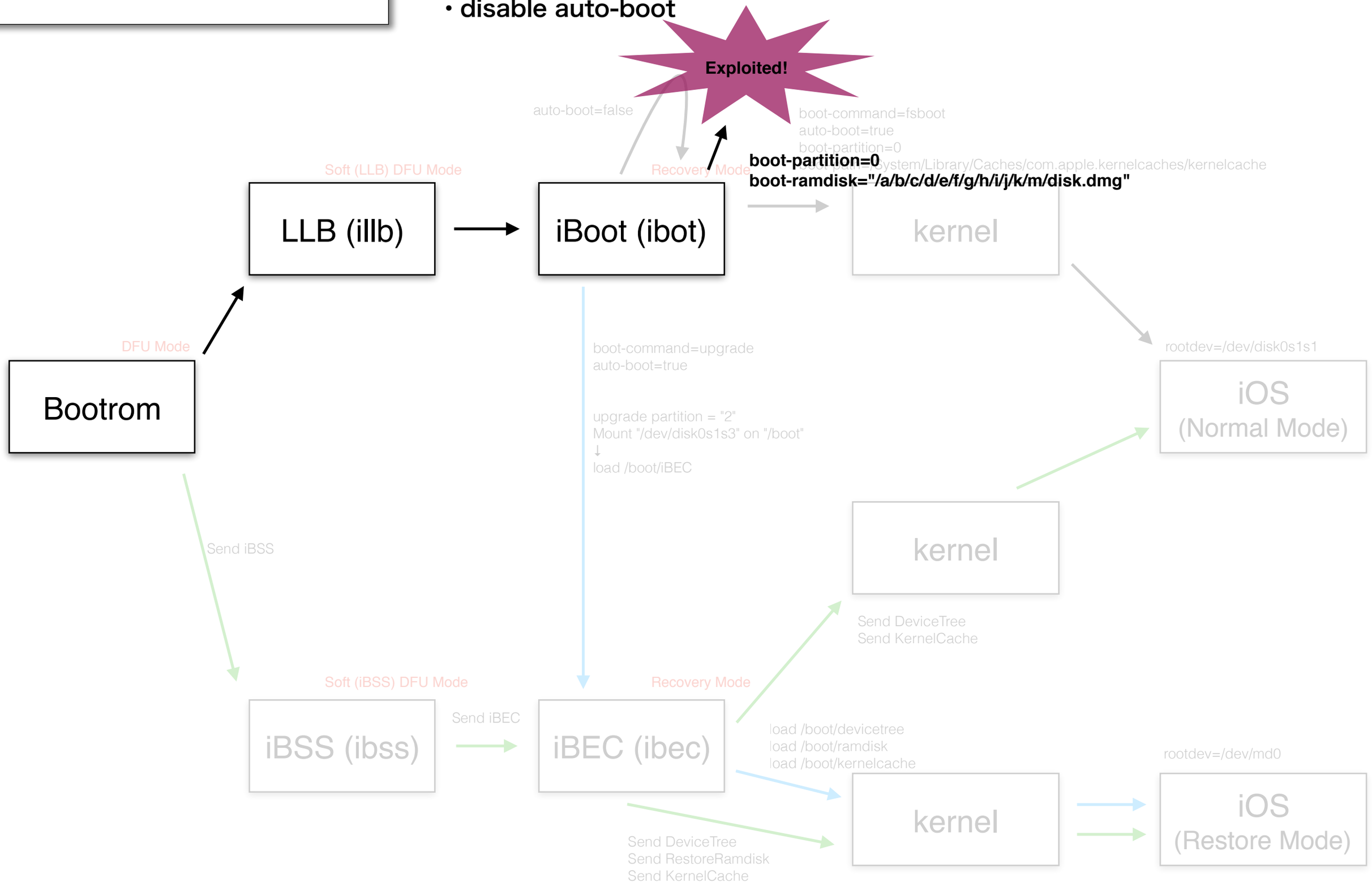

auto-boot=false
Soft (LLB) DFU Mode
Recovery Mode
boot-command=fsboot
auto-boot=true
boot-partition=0
boot-path=/System/Library/Caches/com.apple.kernelcaches/kernelcache
LLB (illb)
iBoot (ibot)
kernel
DFU Mode
Pwned!!
rootdev=/dev/disk0s1s1
Bootrom
boot-command=upgrade
auto-boot=true
iOS
(Normal Mode)
upgrade partition = "2"
Mount "/dev/disk0s1s3" on "/boot"
↓
load /boot/iBEC
kernel
Send DeviceTree
Send KernelCache
Send iBSS
Soft (iBSS) DFU Mode
Recovery Mode
iBSS (ibss)
Send iBEC
iBEC (ibec)
load /boot/devicetree
load /boot/ramdisk
load /boot/kernelcache
rootdev=/dev/md0
kernel
iOS
(Restore Mode)
Send DeviceTree
Send RestoreRamdisk
Send KernelCache

De Rebus Antiquis ramdiskF



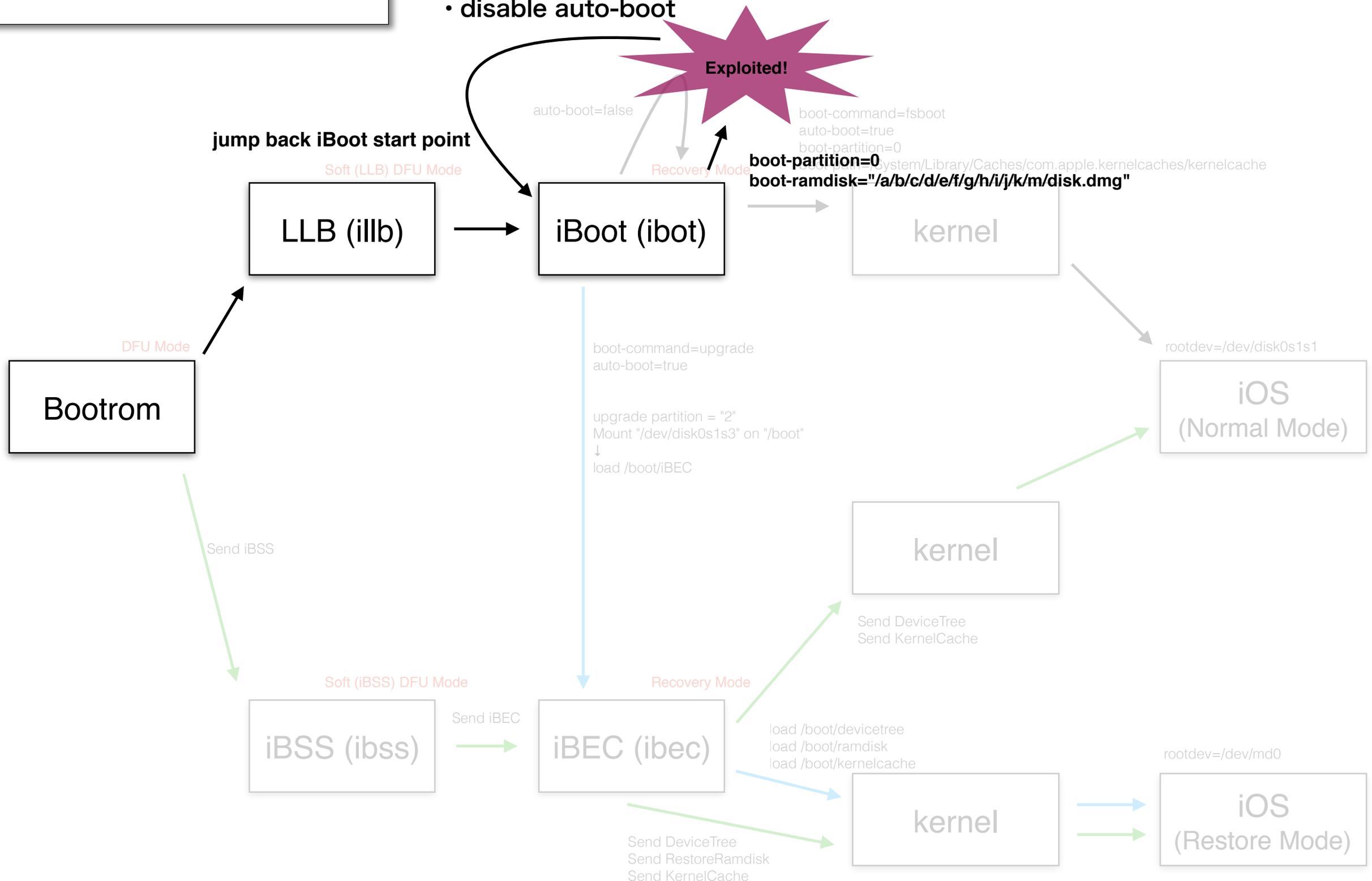
De Rebus Antiquis ramdiskF

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



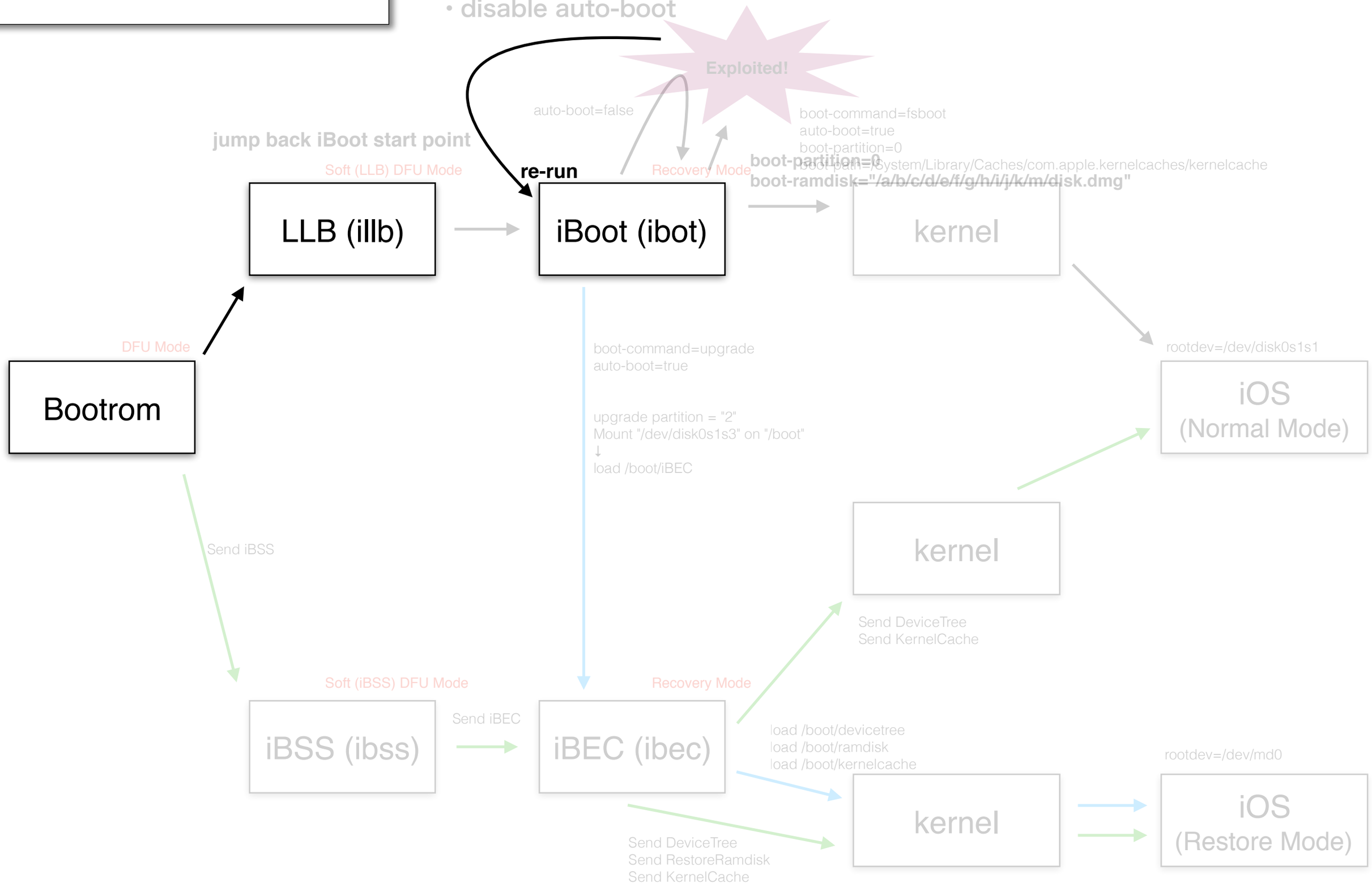
De Rebus Antiquis ramdiskF

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



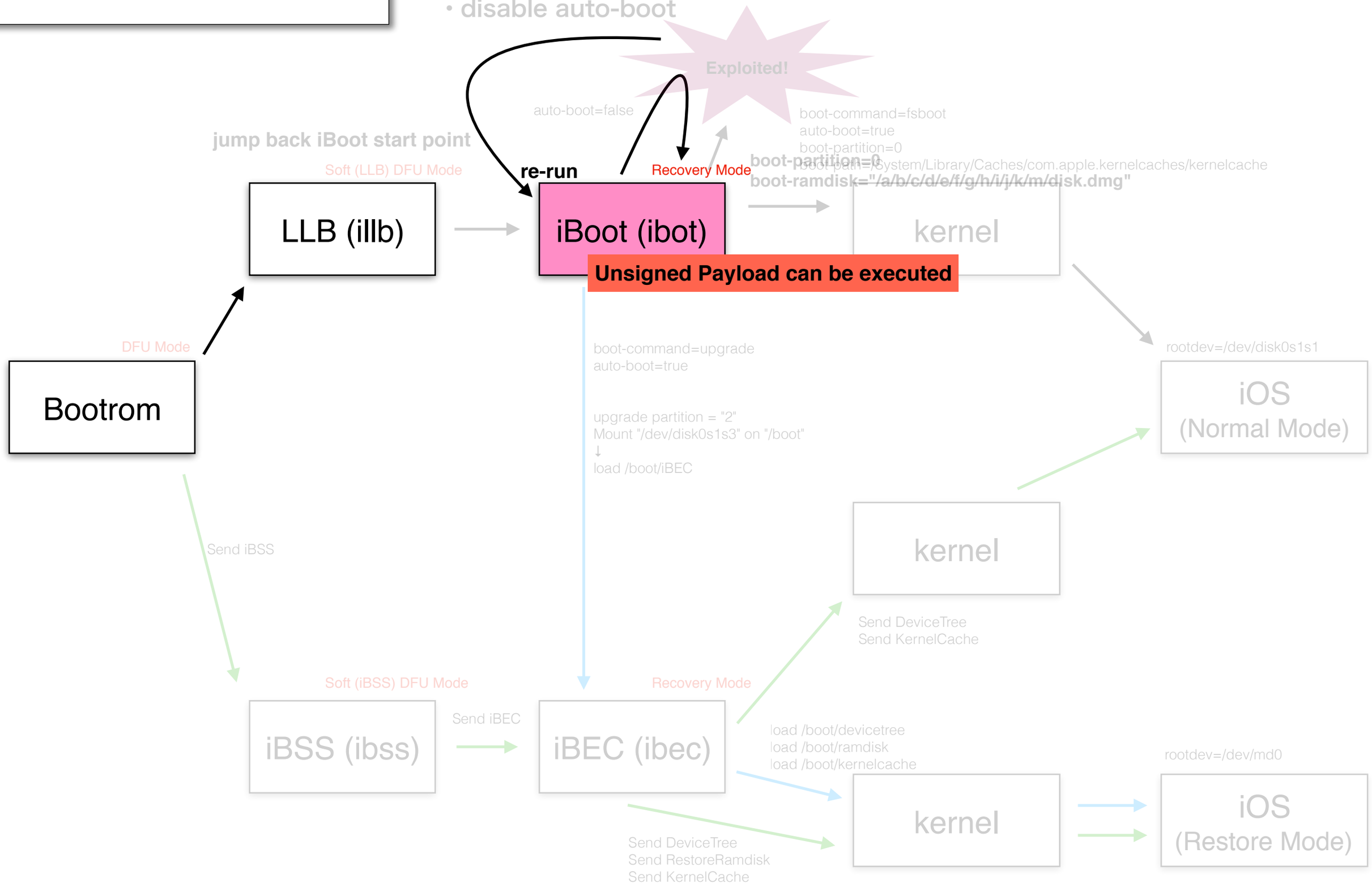
De Rebus Antiquis ramdiskF

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

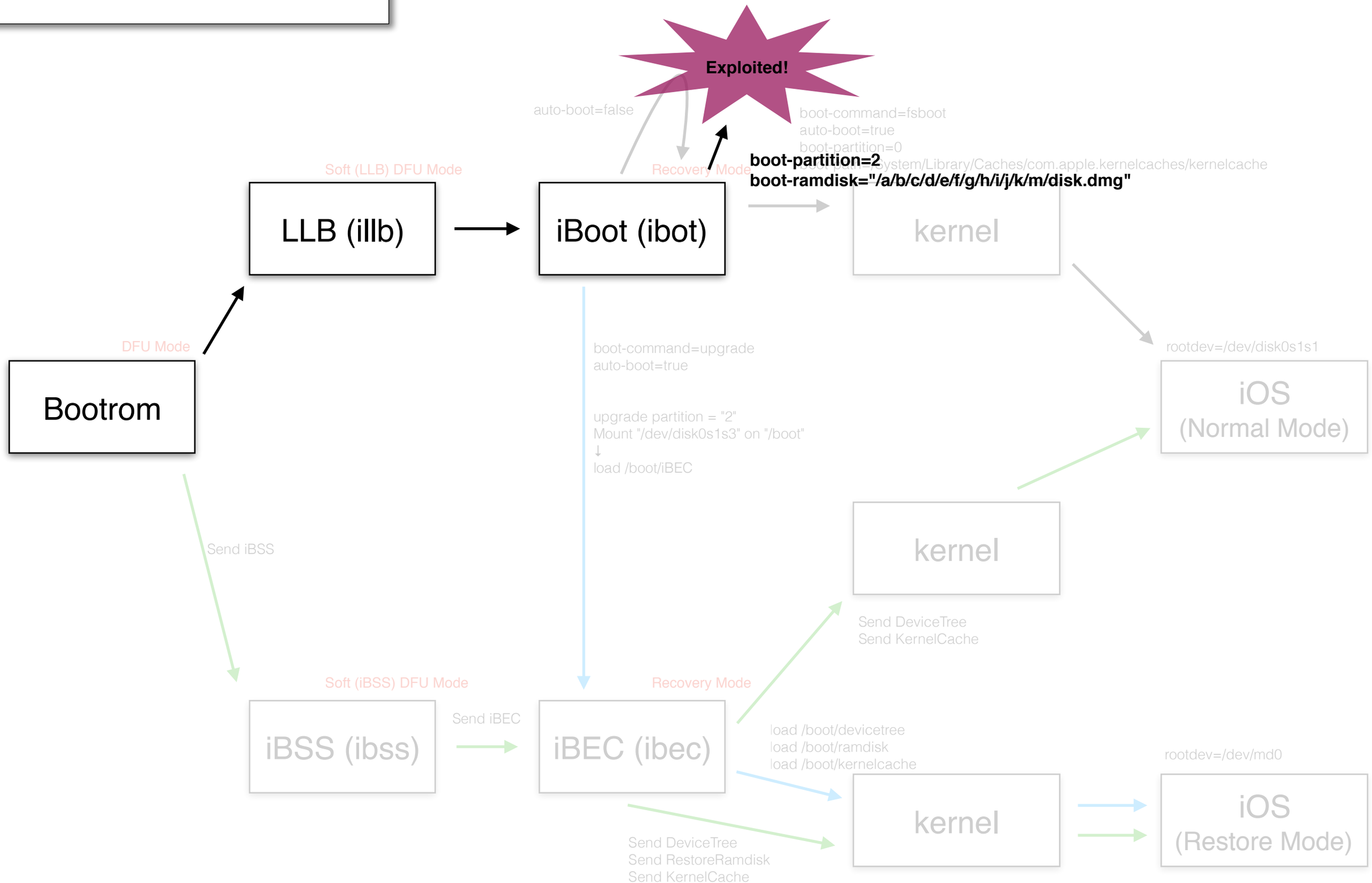


De Rebus Antiquis ramdiskF

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



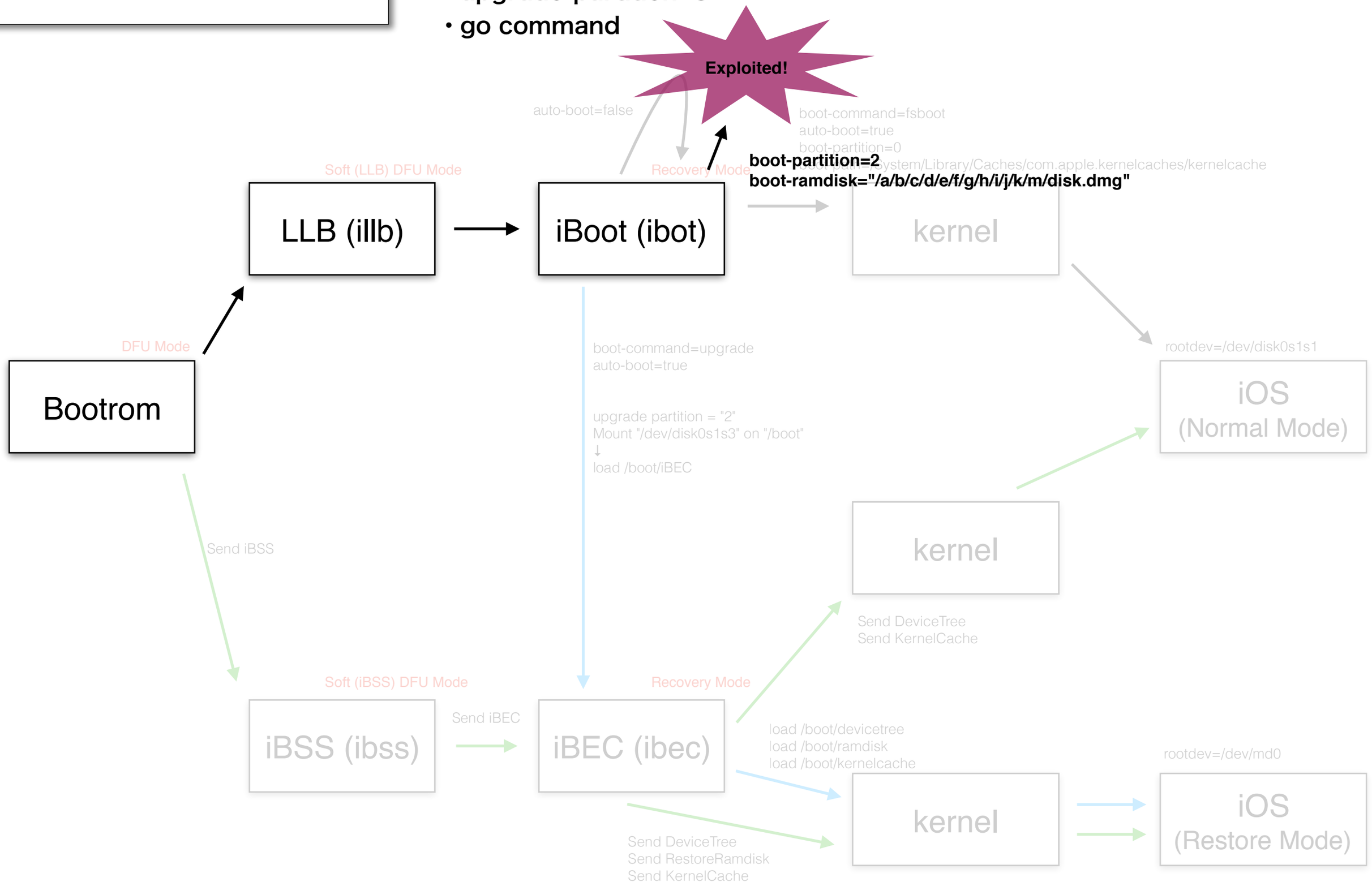
De Rebus Antiquis ramdiskH



De Rebus Antiquis ramdiskH

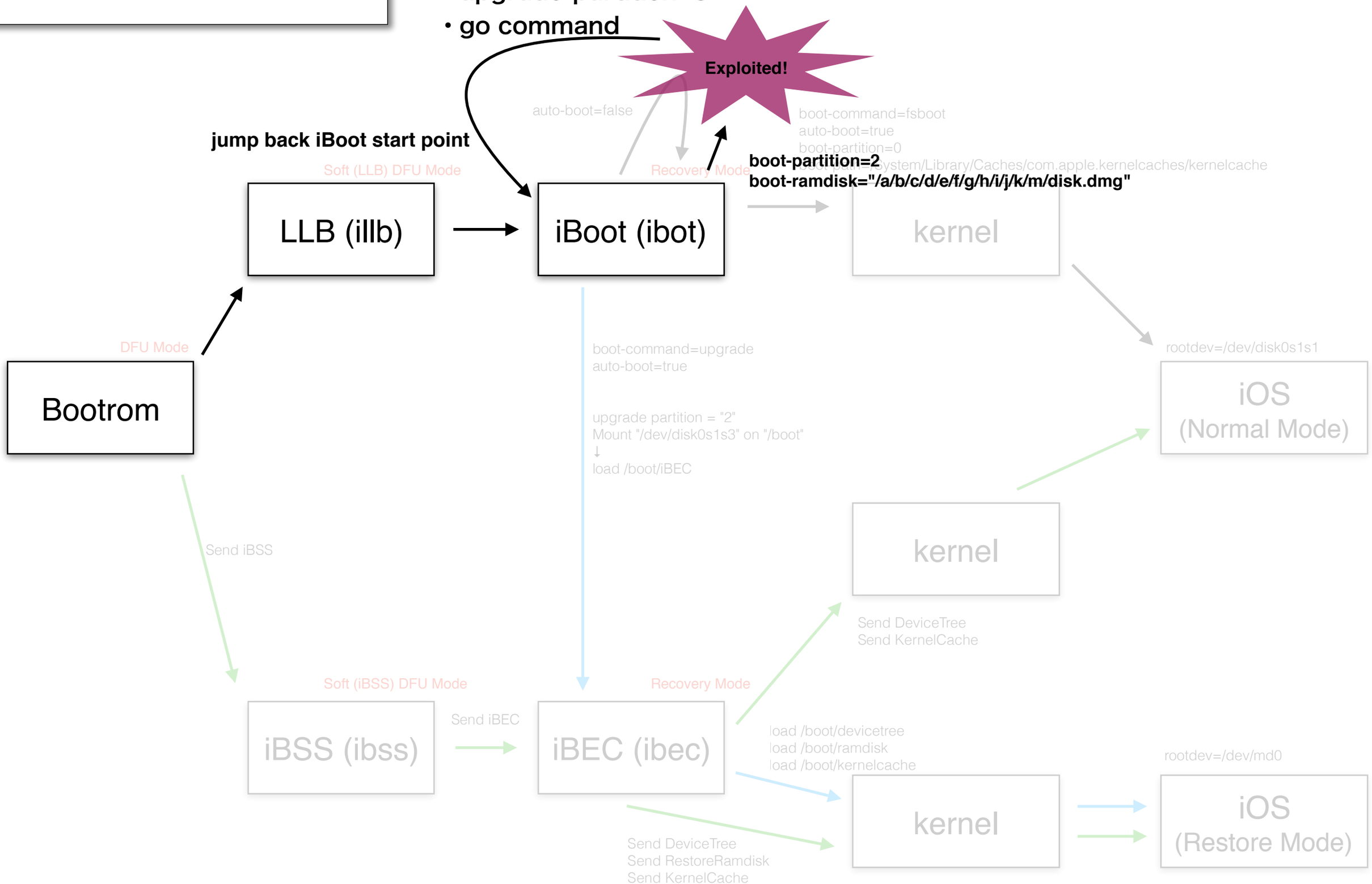
patching iBoot

- 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

Exploited!

auto-boot=false

jump back iBoot start point

Soft (LLB) DFU Mode

re-run

Recovery Mode

boot-command=fsboot
auto-boot=true
boot-partition=0
boot-path=/System/Library/Caches/com.apple.kernelcaches/kernelcache

boot-partition=2
boot-ramdisk="/a/b/c/d/e/f/g/h/i/j/k/m/disk.dmg"

LLB (illb)

iBoot (ibot)

kernel

DFU Mode

Bootrom

boot-command=upgrade
auto-boot=true

upgrade partition = "3"
Mount "/dev/disk0s1s3" on "/boot"
↓
load /boot/iBEC

rootdev=/dev/disk0s1s1

iOS
(Normal Mode)

kernel

Send iBSS

Send DeviceTree
Send KernelCache

Soft (iBSS) DFU Mode

Send iBEC

Recovery Mode

iBSS (ibss)

iBEC (ibec)

load /boot/devicetree
load /boot/ramdisk
load /boot/kernelcache

rootdev=/dev/md0

kernel

iOS
(Restore Mode)

Send DeviceTree
Send RestoreRamdisk
Send KernelCache

De Rebus Antiquis ramdiskH

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

Exploited!

auto-boot=false

jump back iBoot start point

Soft (LLB) DFU Mode

re-run

Recovery Mode

boot-command=fsboot
auto-boot=true
boot-partition=0
boot-path=/System/Library/Caches/com.apple.kernelcaches/kernelcache

boot-partition=2
boot-ramdisk="/a/b/c/d/e/f/g/h/i/j/k/m/disk.dmg"

LLB (illb)

iBoot (ibot)

kernel

rootdev=/dev/disk0s1s1

DFU Mode

Bootrom

boot-command=upgrade
auto-boot=true

upgrade partition = "3"
Mount "/dev/disk0s1s3" on "/boot"
↓
load /boot/iBEC

iOS
(Normal Mode)

kernel

Send iBSS

Send DeviceTree
Send KernelCache

Soft (iBSS) DFU Mode

Send iBEC

Recovery Mode

iBSS (ibss)

iBoot (ibec)

load /boot/devicetree
load /boot/ramdisk
load /boot/kernelcache

rootdev=/dev/md0

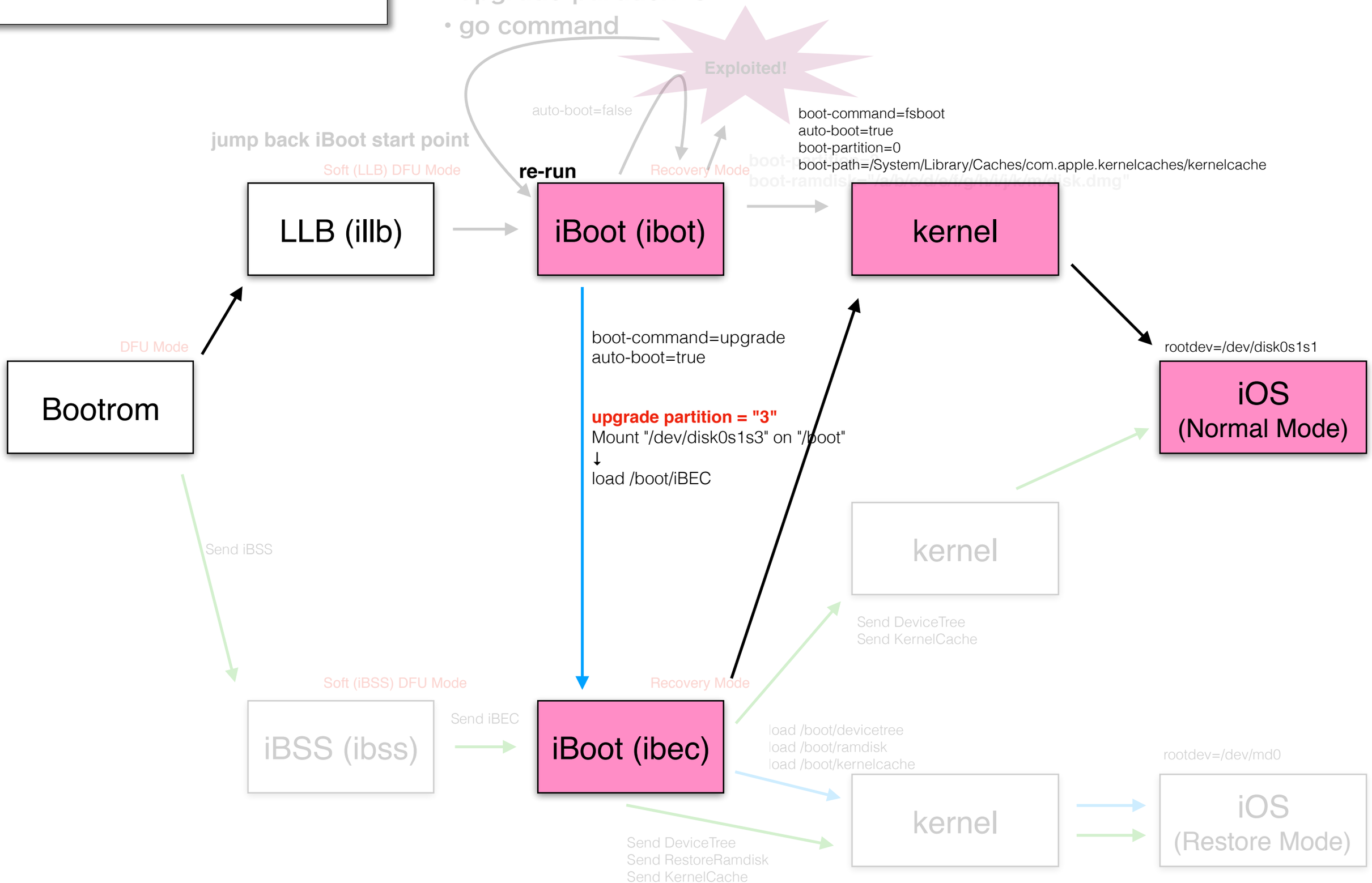
kernel

iOS
(Restore Mode)

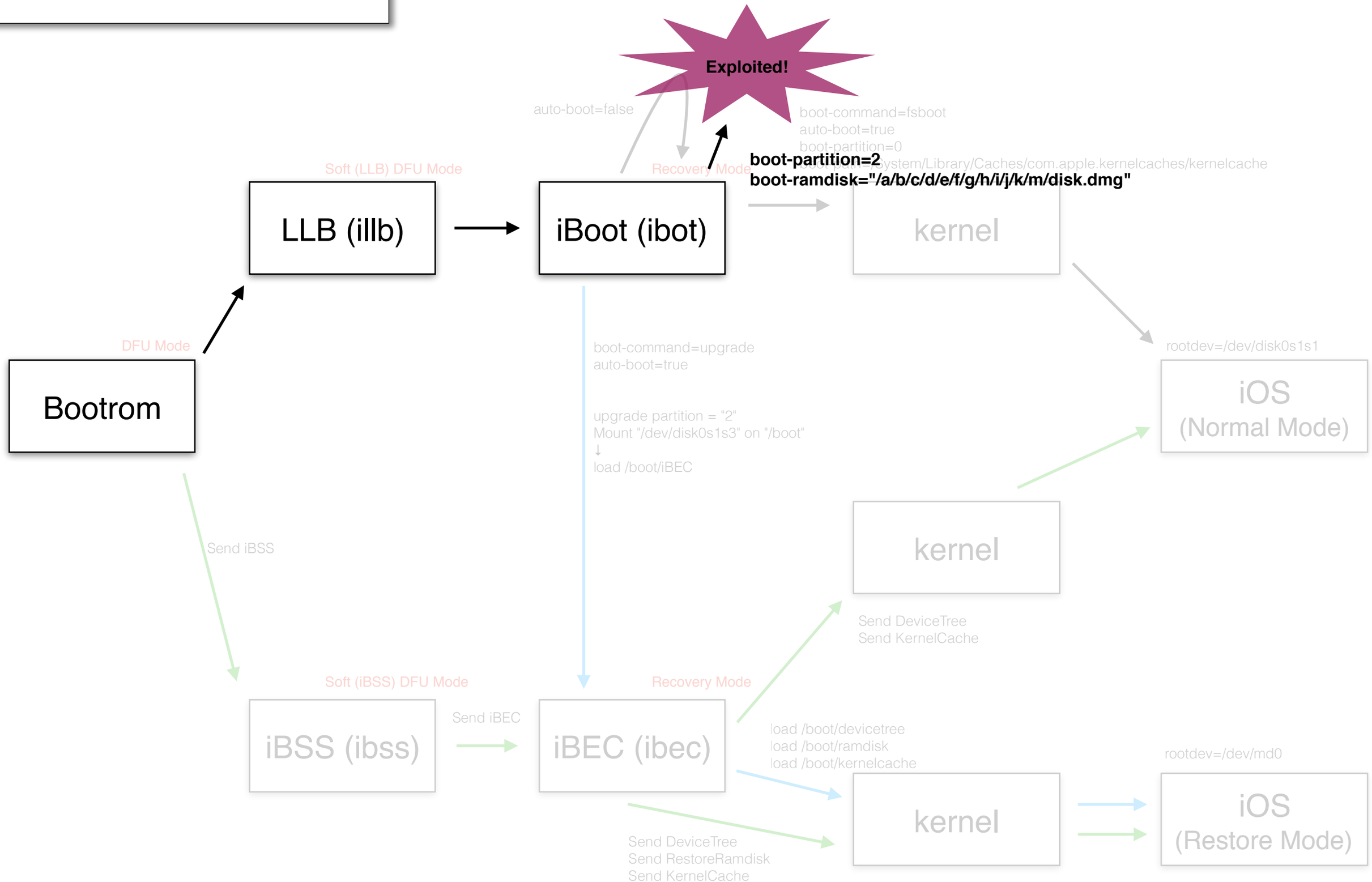
Send DeviceTree
Send RestoreRamdisk
Send KernelCache

De Rebus Antiquis ramdiskH

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

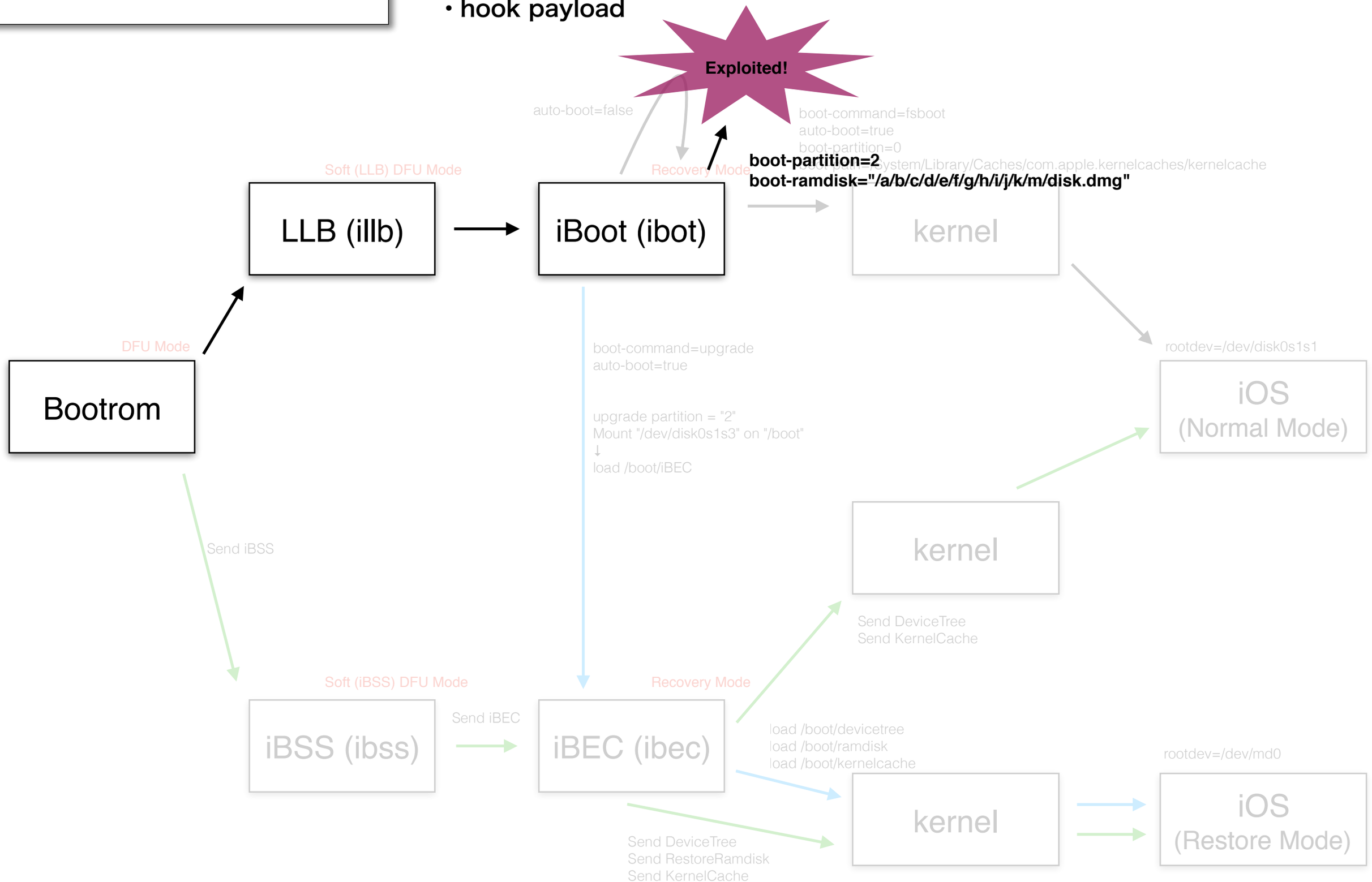


De Rebus Antiquis ramdiskl



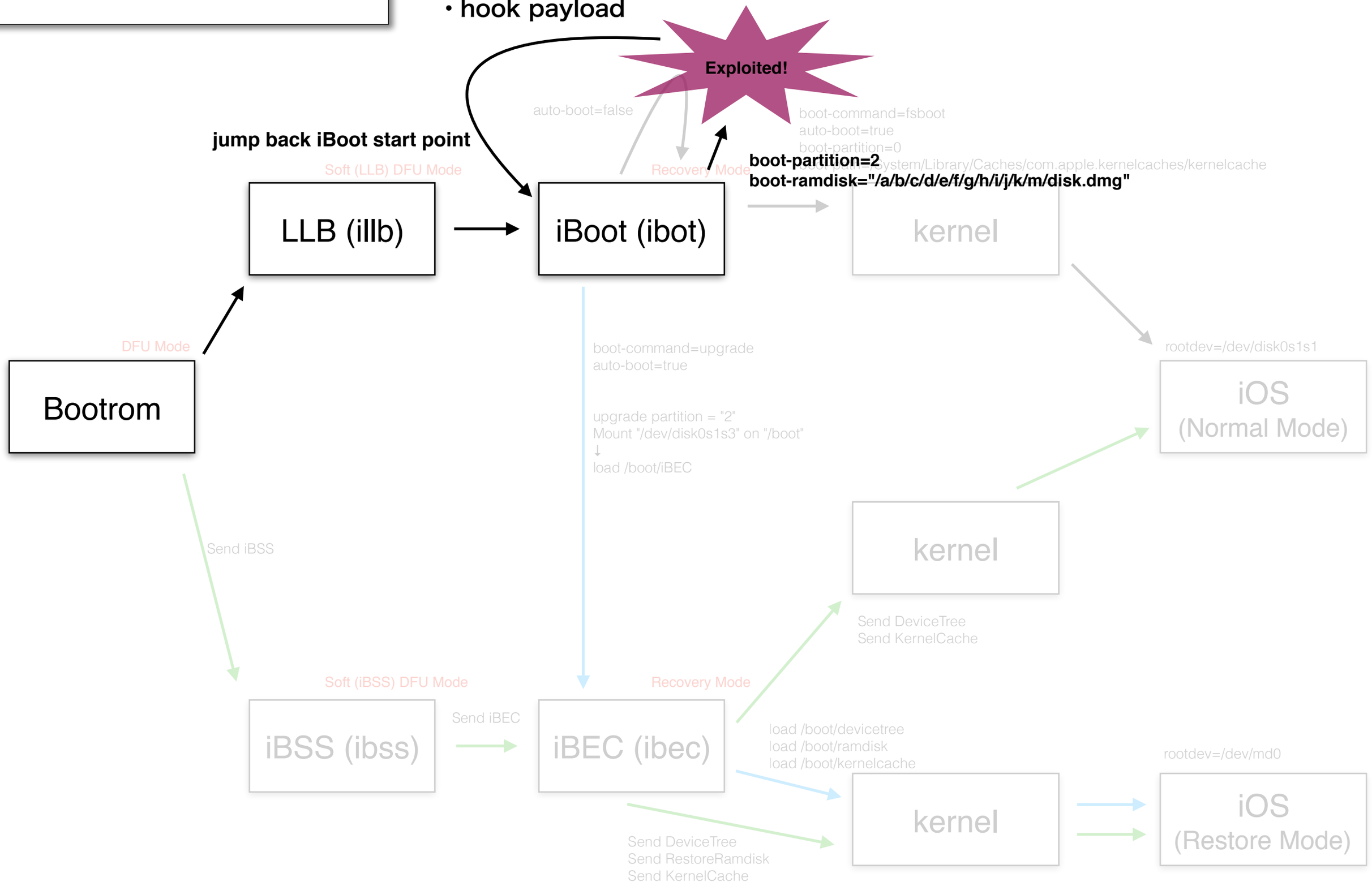
De Rebus Antiquis ramdiskl

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



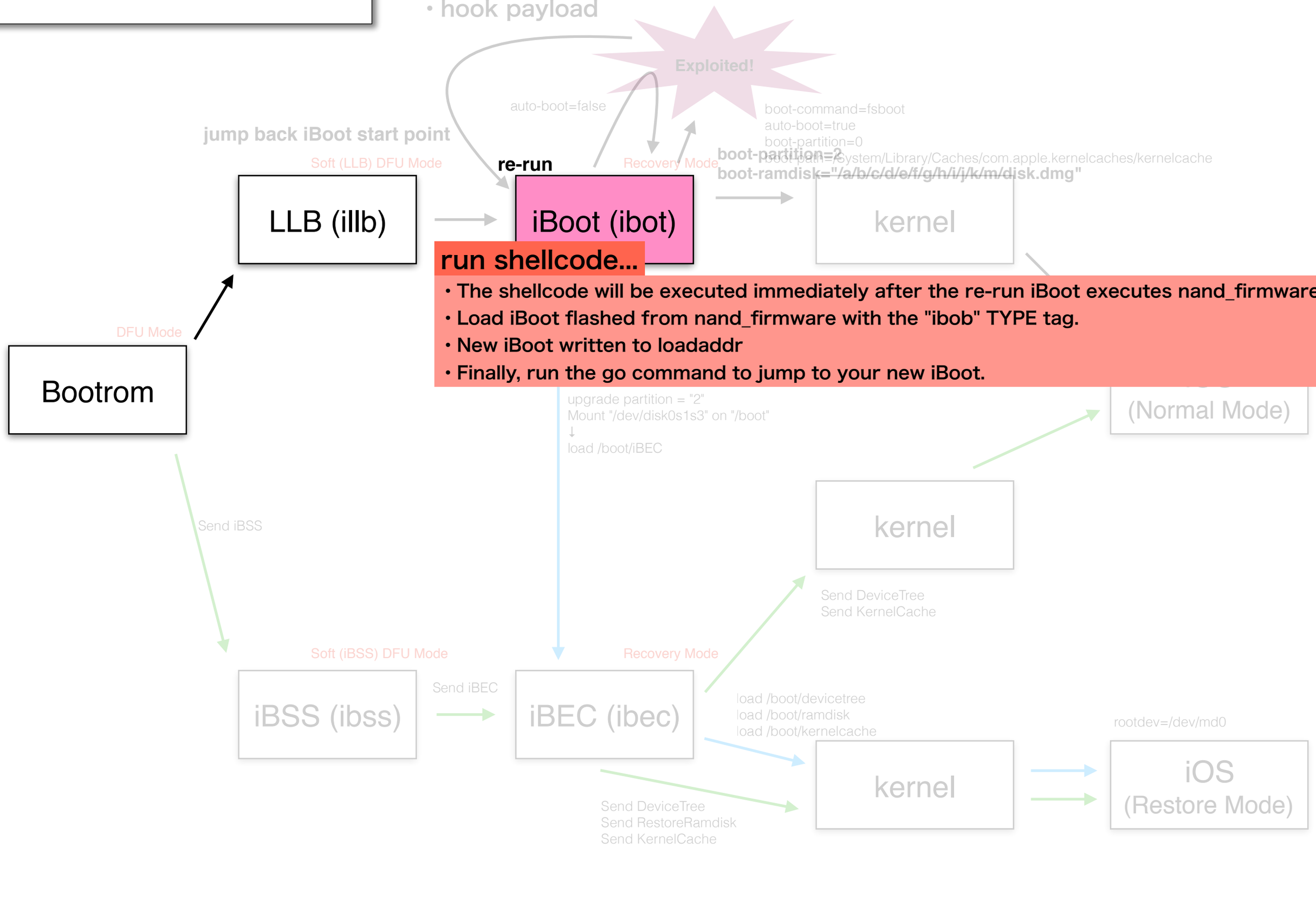
De Rebus Antiquis ramdiskl

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



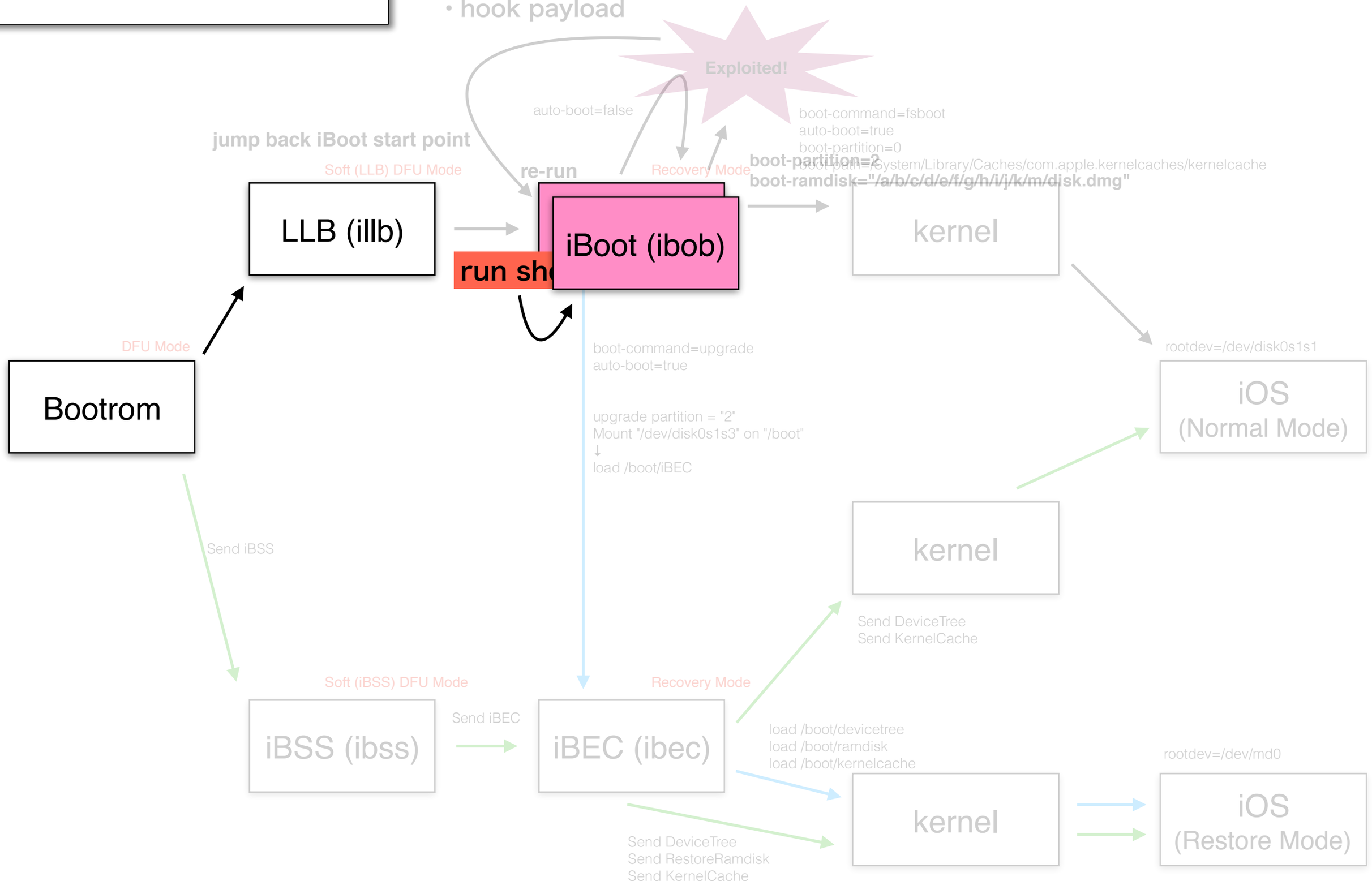
De Rebus Antiquis ramdiskl

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



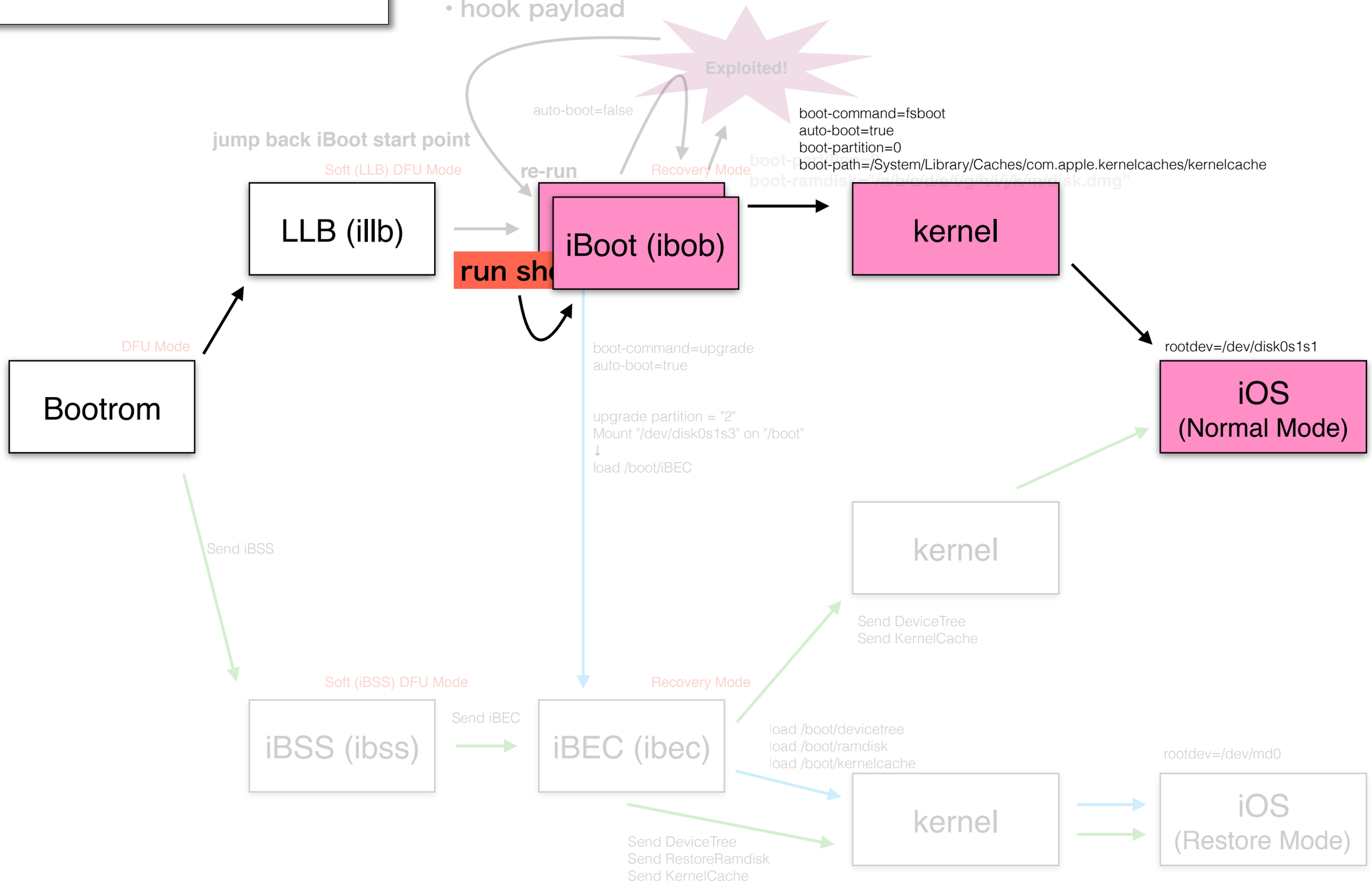
De Rebus Antiquis ramdiskl

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



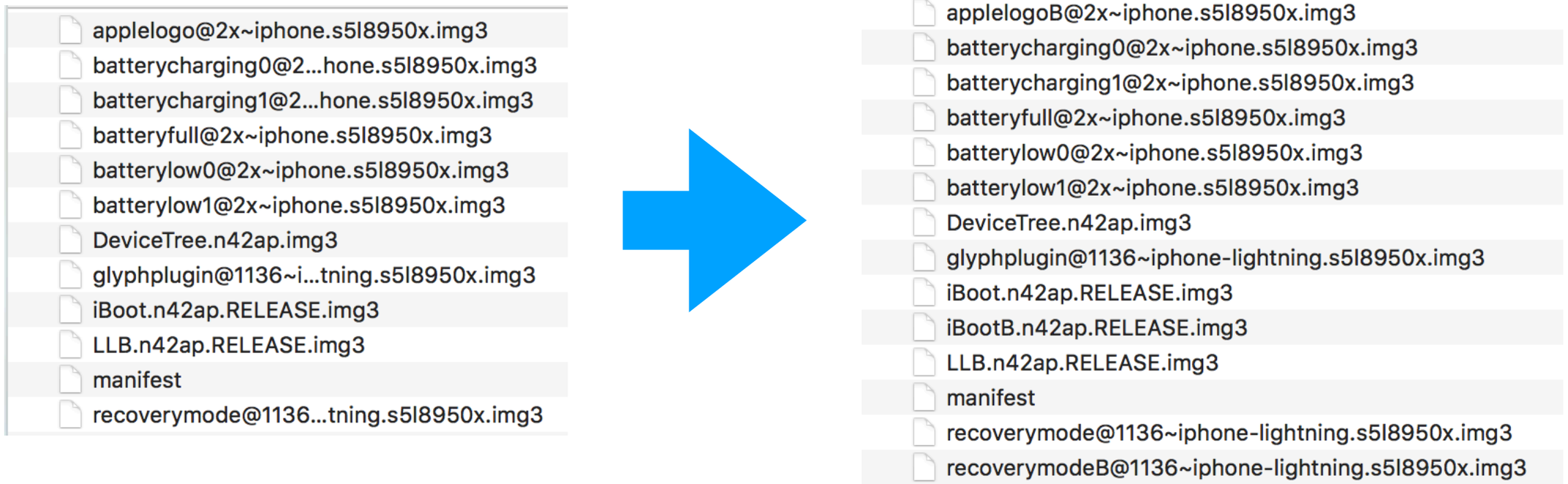
De Rebus Antiquis ramdiskl

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



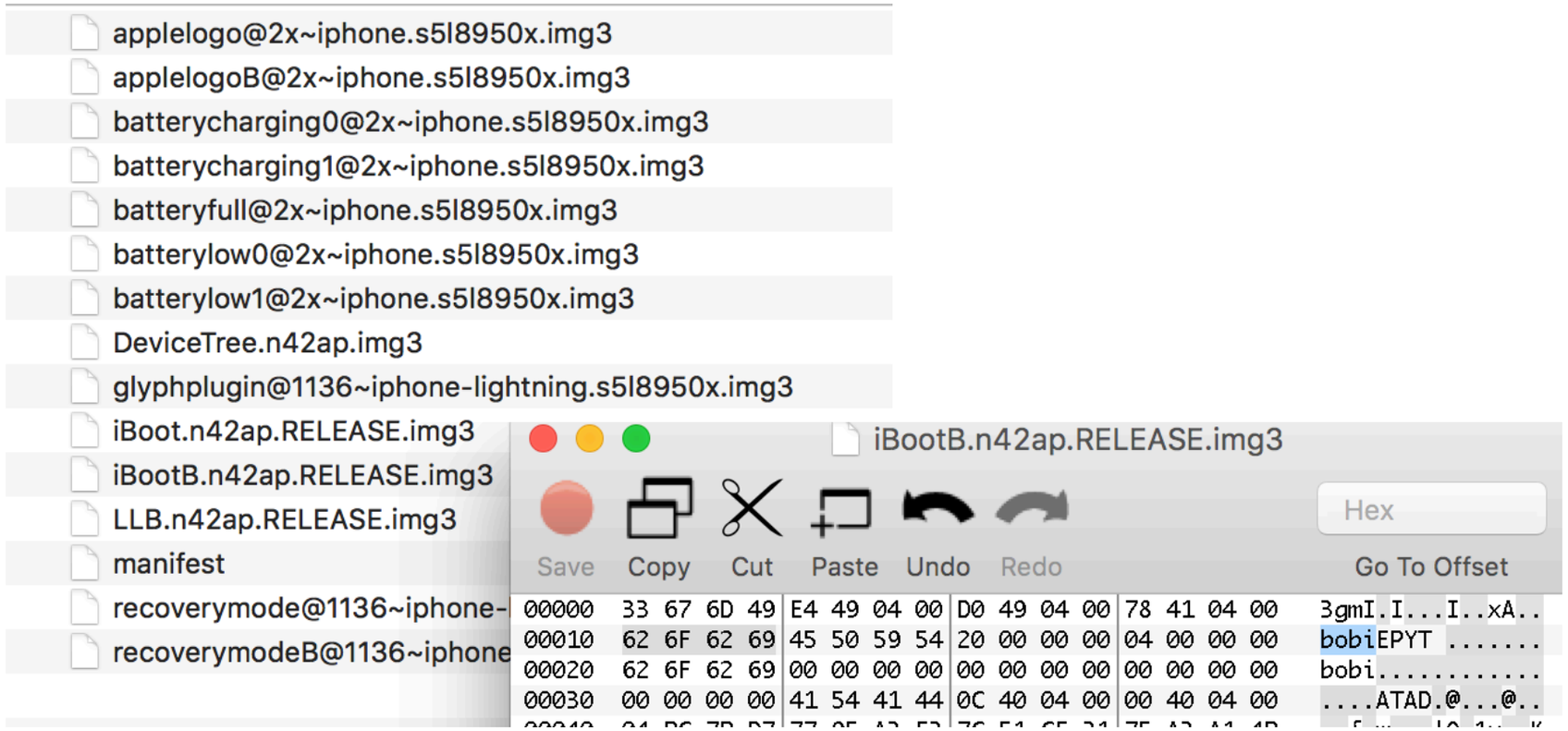
De Rebus Antiquis
How to use ramdiskl?

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



De Rebus Antiquis
How to use ramdiskI?

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 "AppleIogoB" 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 ramdiskI?

iBoot vs iBootB

iBoot

Do not do anything

iBootB

Apply patches

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

De Rebus Antiquis
How to use ramdiskI?

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...**