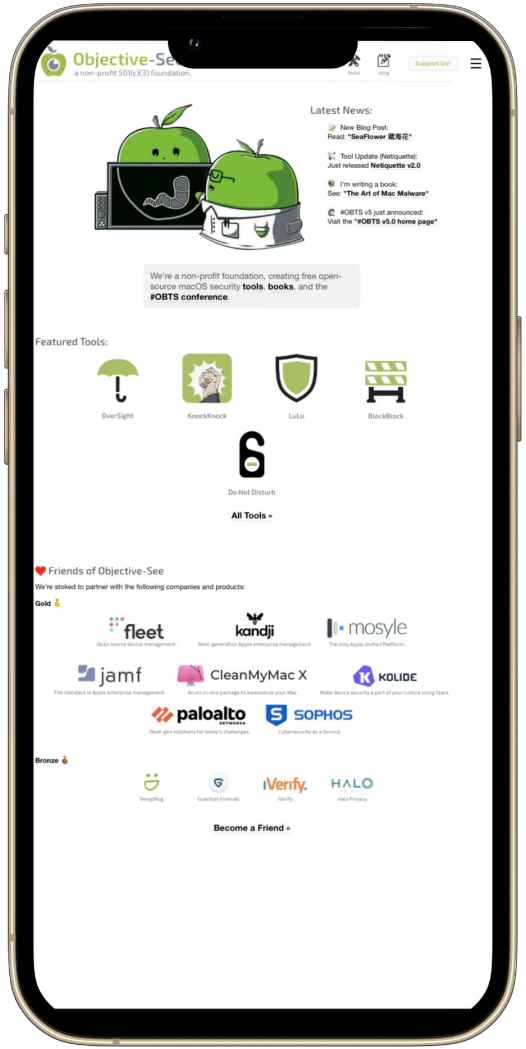
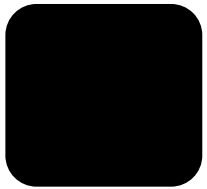
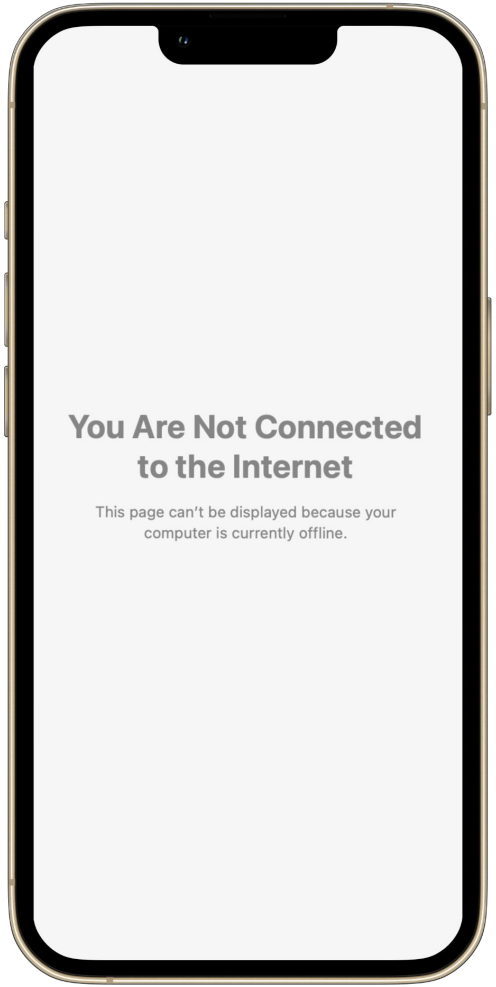
Abusing iPhone Co-Processors for Privilege Escalation

@i41nbeer

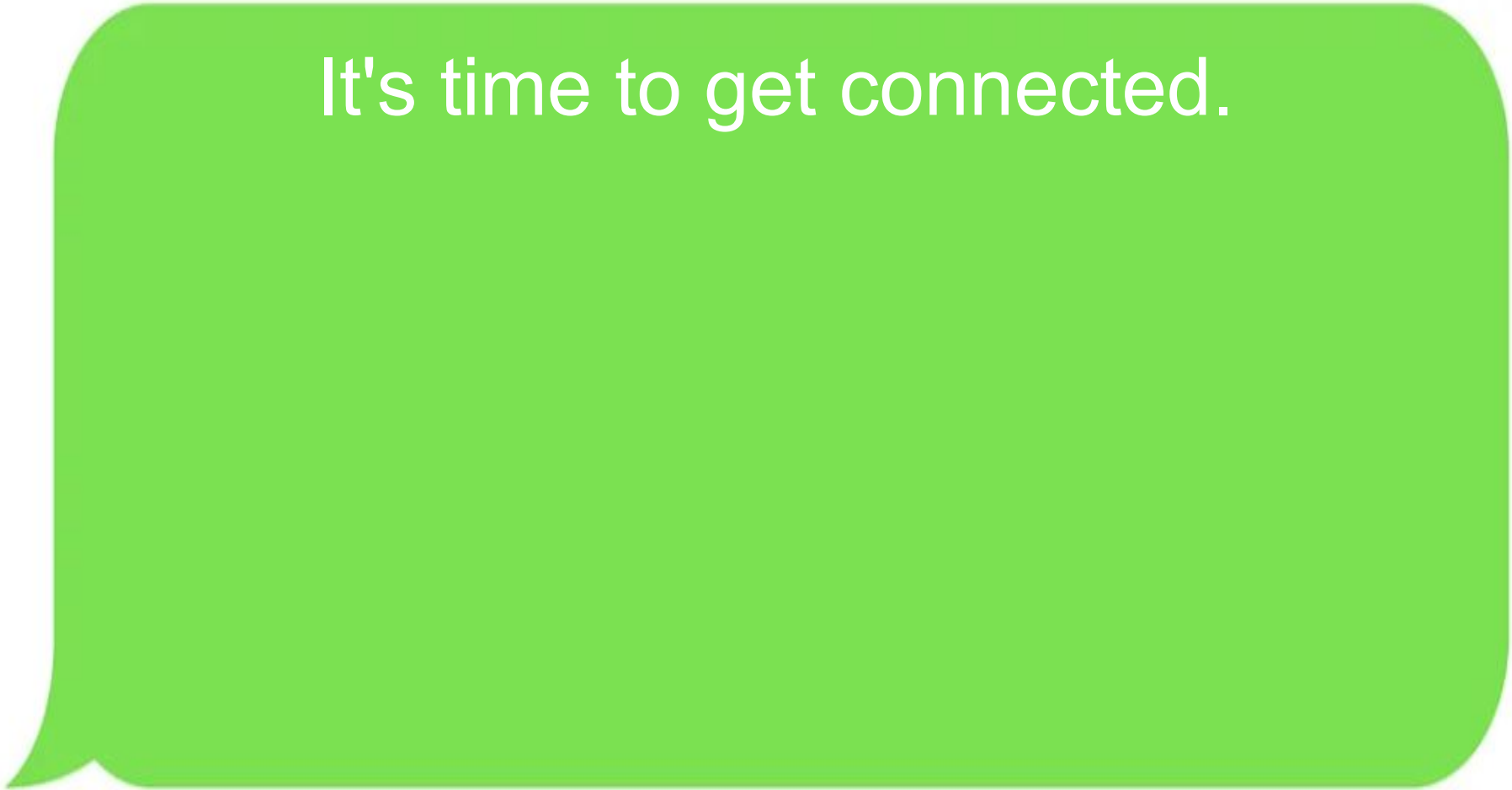




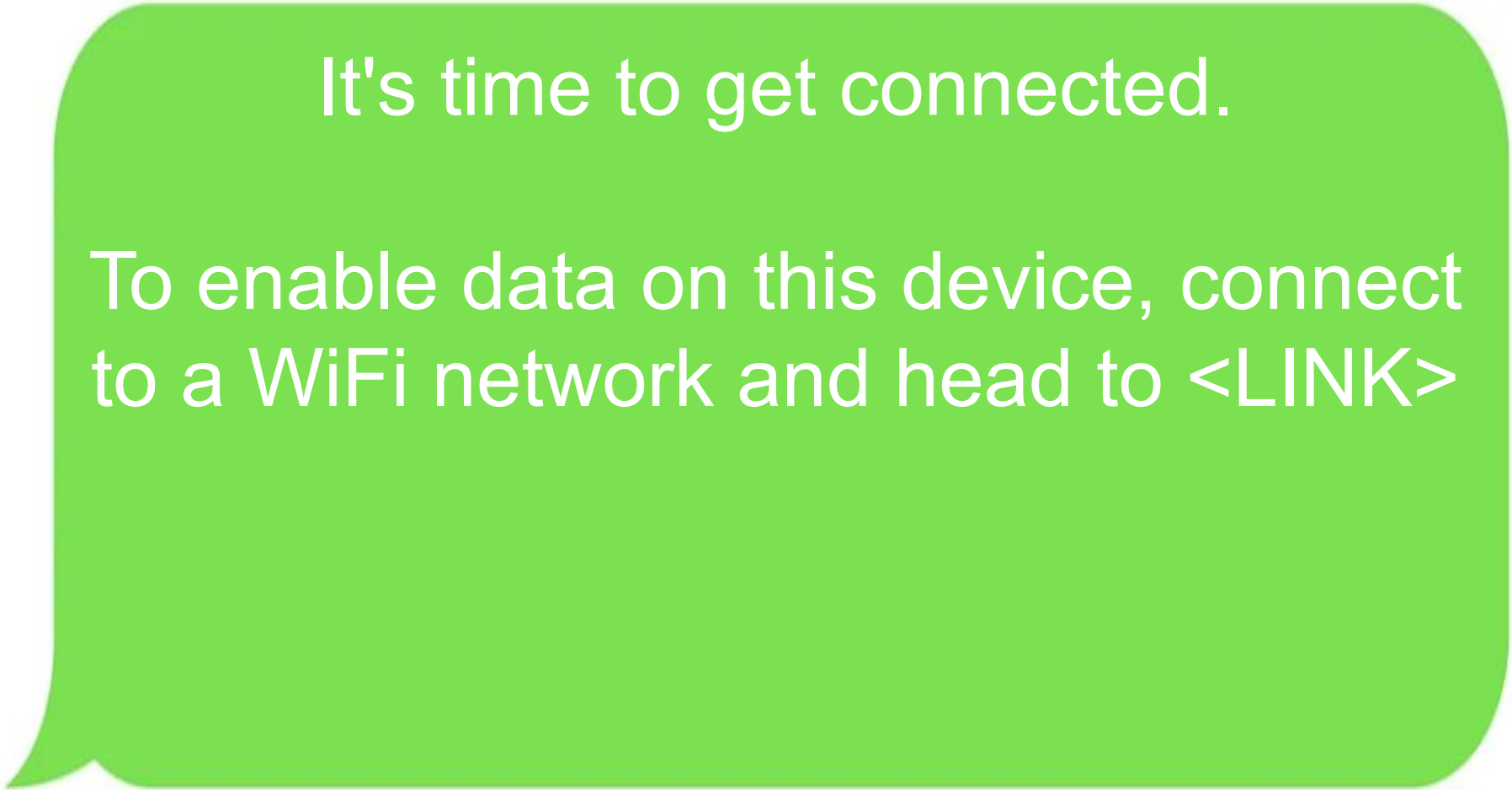



1

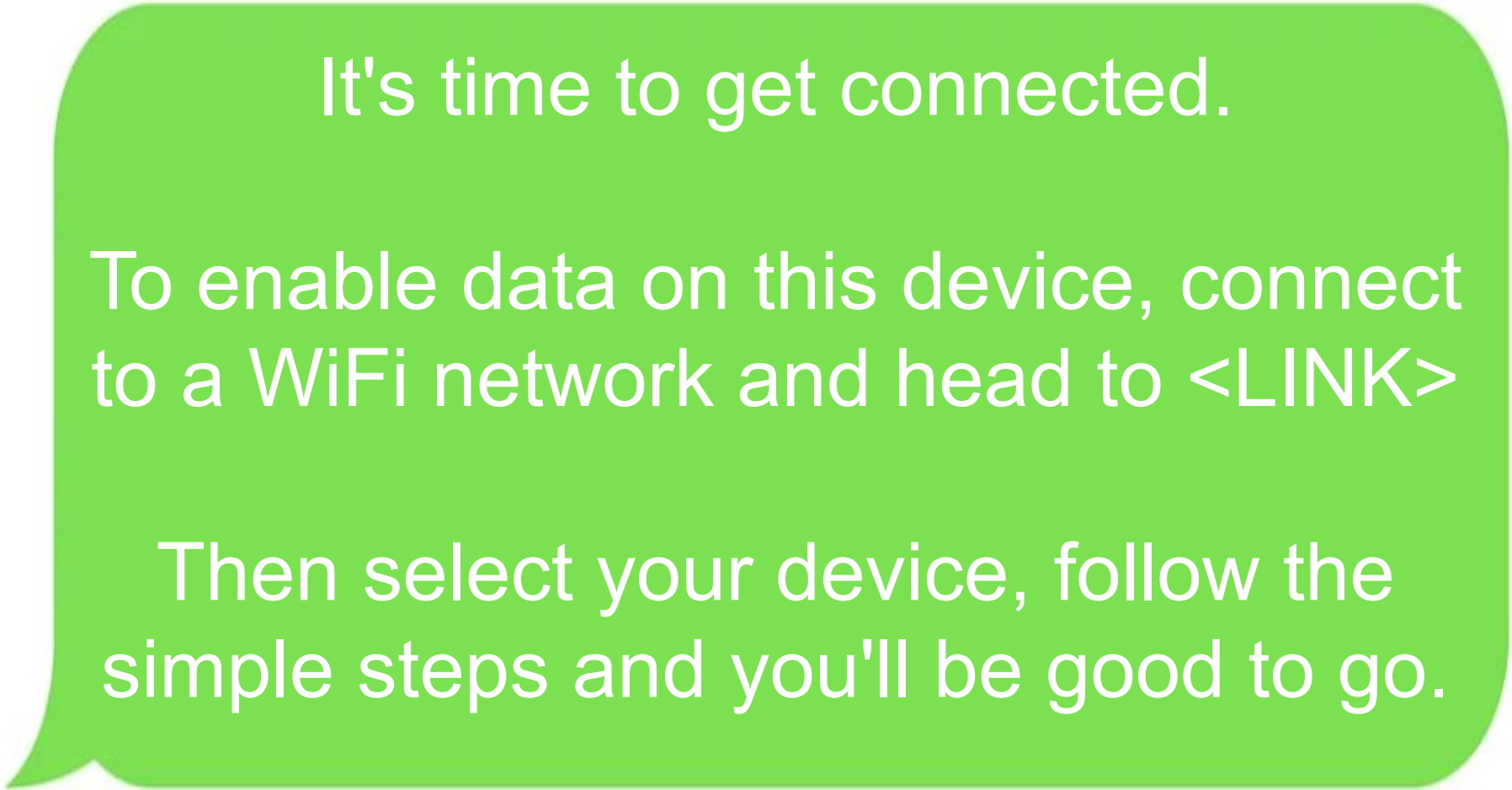
(an example SMS - not the real phishing message)



(an example SMS - not the real phishing message)



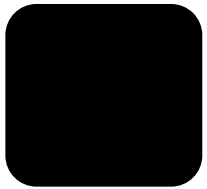
(an example SMS - not the real phishing message)

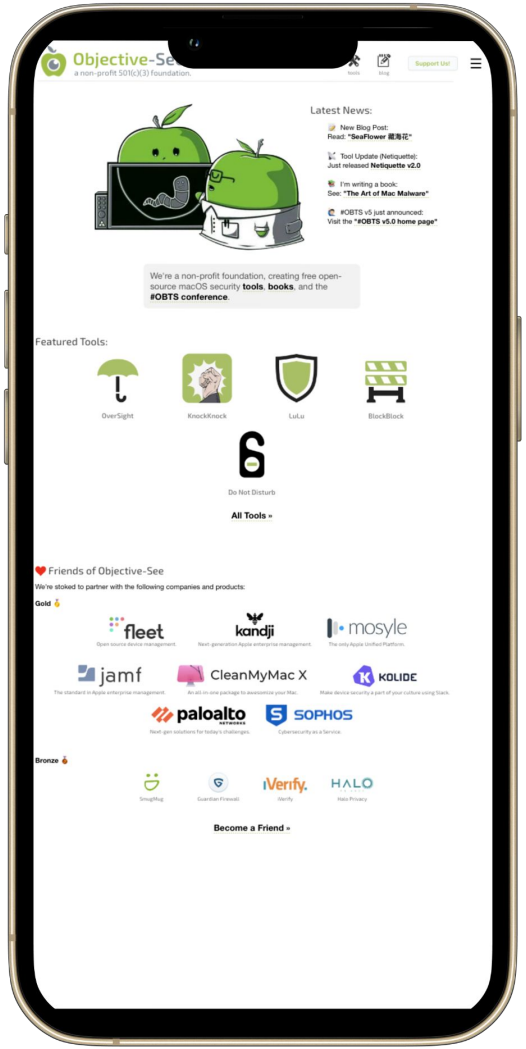


(an example SMS - not the real phishing message)

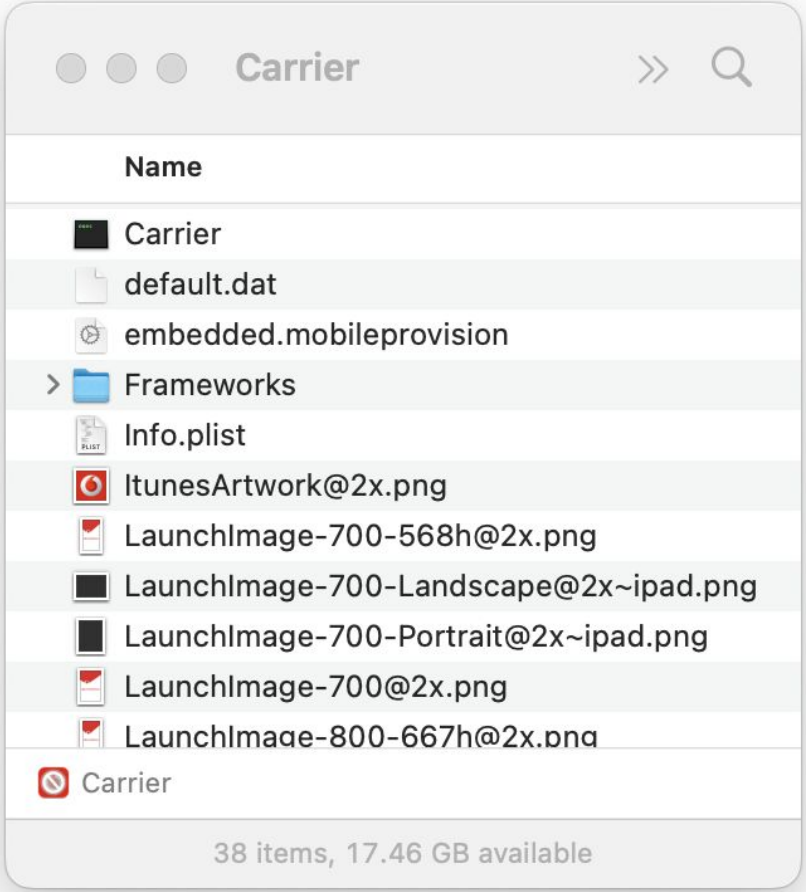
itms-services://?action=download-manifest?url=https://xxx

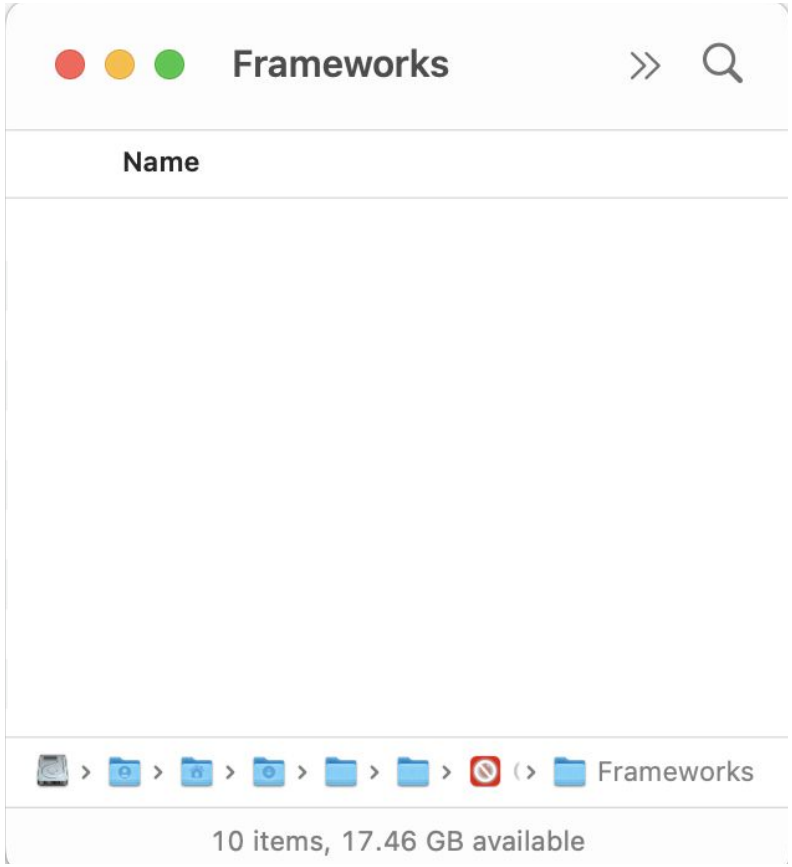
You click the link

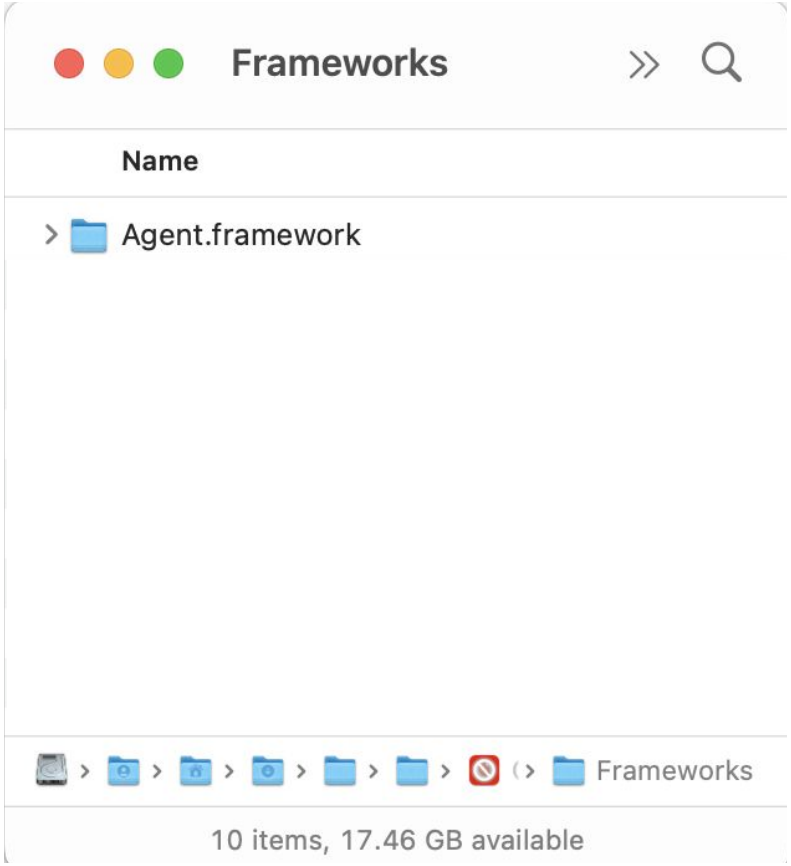


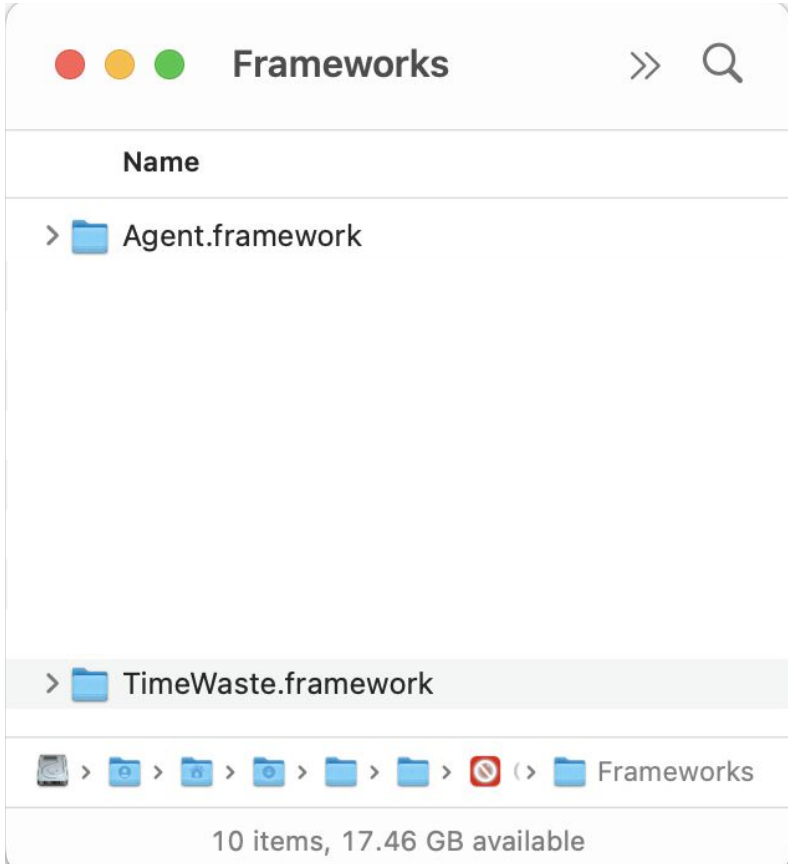


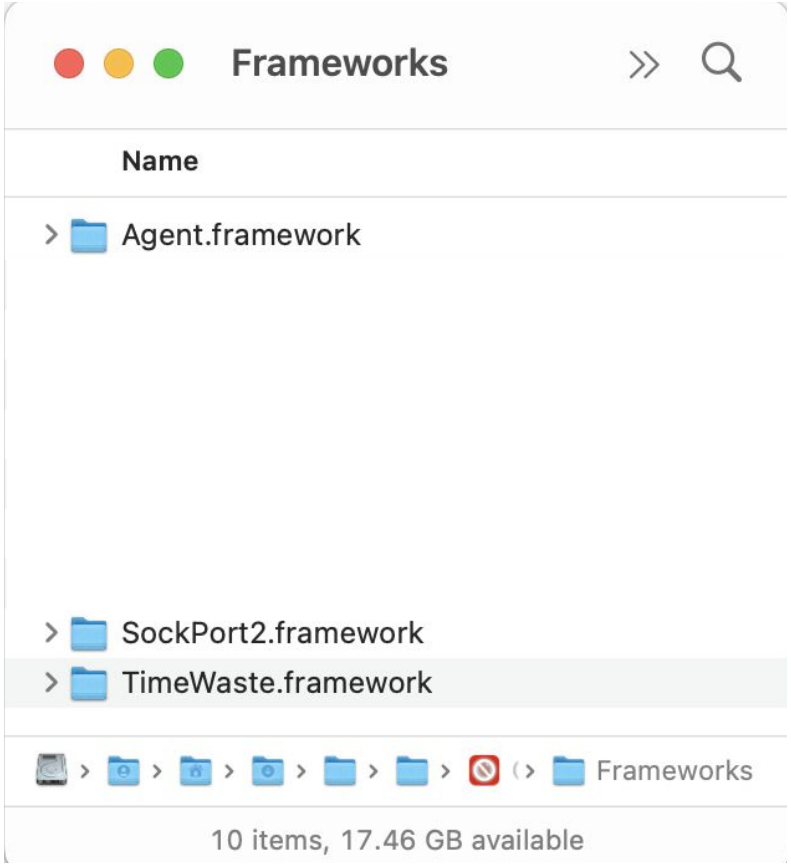
phishing?

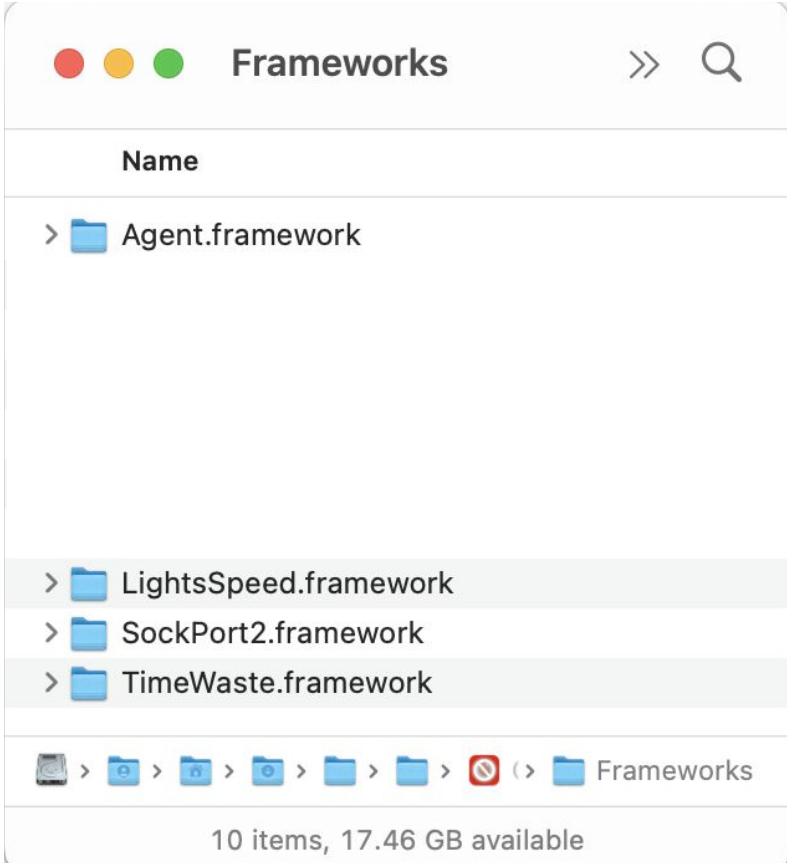

Carrier
Name
Carrier
default.dat
embedded.mobileprovision
Frameworks
Info.plist
ItunesArtwork@2x.png
LaunchImage-700-568h@2x.png
LaunchImage-700-Landscape@2x~ipad.png
LaunchImage-700-Portrait@2x~ipad.png
LaunchImage-700@2x.png
LaunchImage-800-667h@2x.png
Carrier
38 items, 17.46 GB available

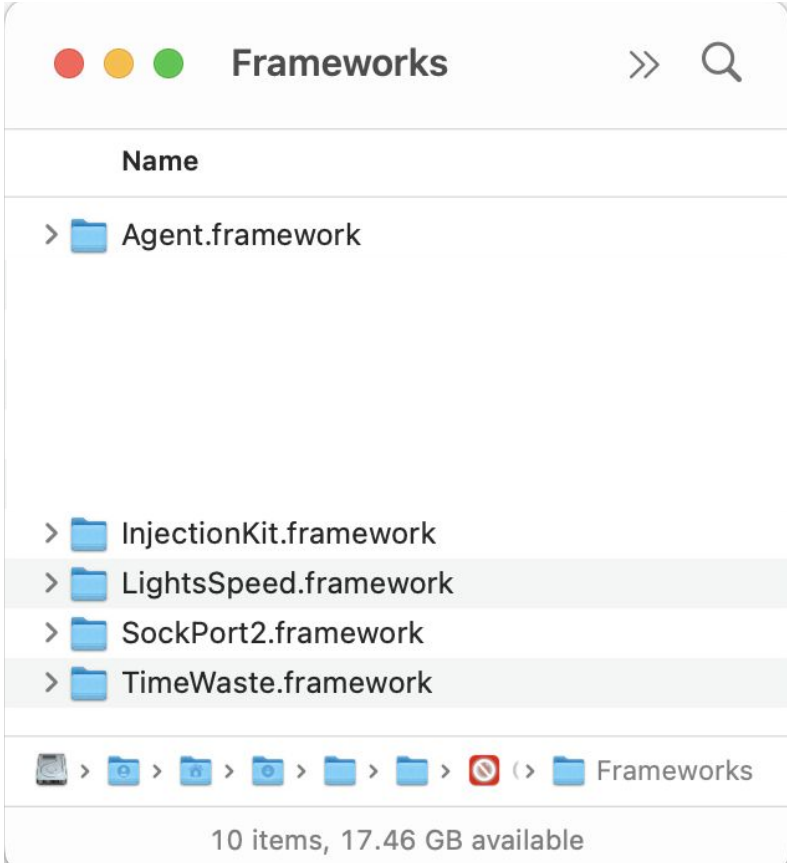

Frameworks
Name
Frameworks
10 items, 17.46 GB available

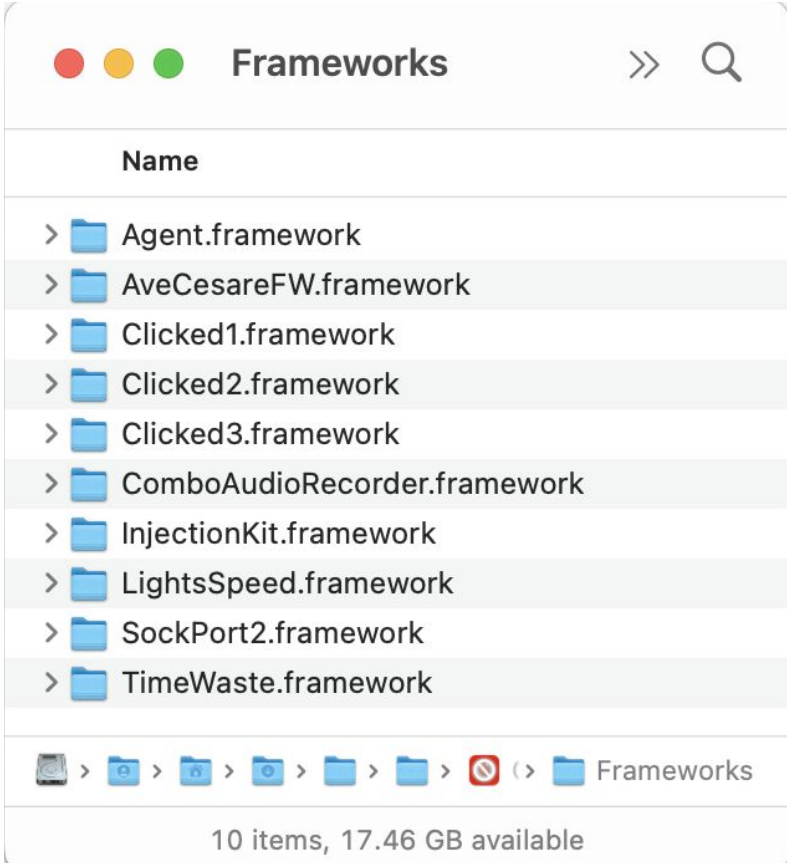

Frameworks
Name
Agent.framework
Frameworks
10 items, 17.46 GB available

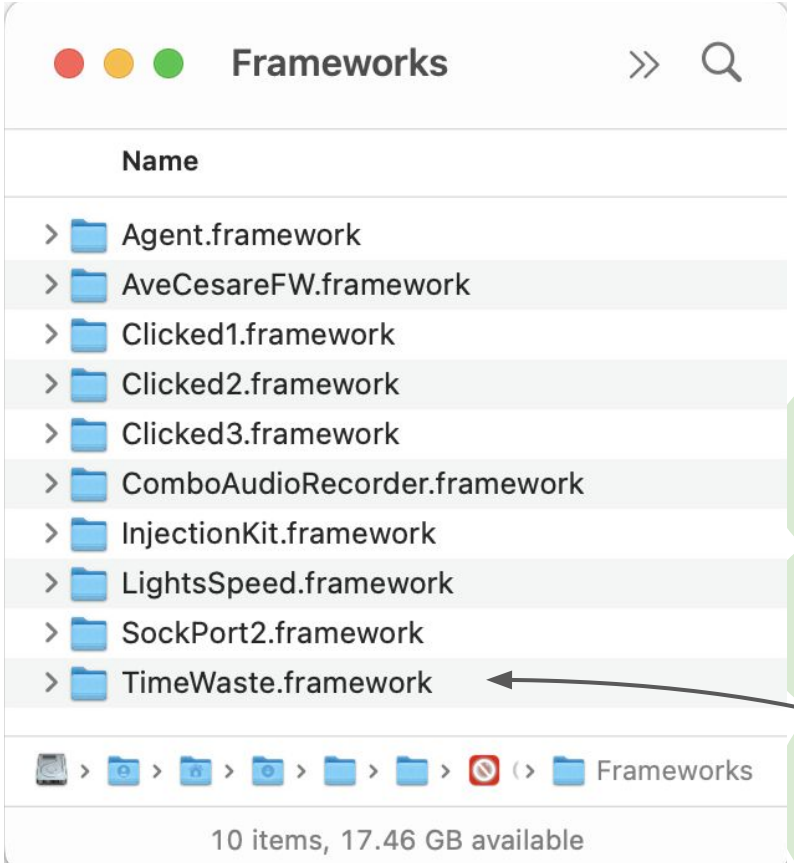

Frameworks
Name
Agent.framework
TimeWaste.framework
Frameworks
10 items, 17.46 GB available


Frameworks
Name
Agent.framework
SockPort2.framework
TimeWaste.framework
Frameworks
10 items, 17.46 GB available


Frameworks
Name
Agent.framework
LightsSpeed.framework
SockPort2.framework
TimeWaste.framework
Frameworks
10 items, 17.46 GB available


Frameworks
Name
Agent.framework
InjectionKit.framework
LightsSpeed.framework
SockPort2.framework
TimeWaste.framework
Frameworks
10 items, 17.46 GB available

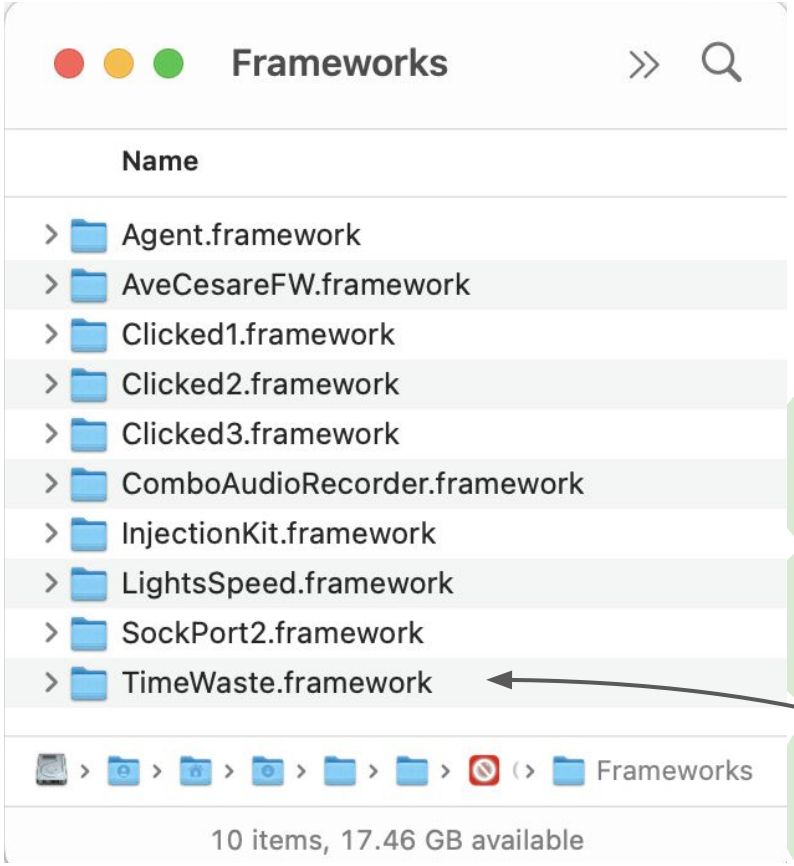

Frameworks
Name
Agent.framework
AveCesareFW.framework
Clicked1.framework
Clicked2.framework
Clicked3.framework
ComboAudioRecorder.framework
InjectionKit.framework
LightsSpeed.framework
SockPort2.framework
TimeWaste.framework
Frameworks
10 items, 17.46 GB available



from github:

time_waste

CVE-2020-3837

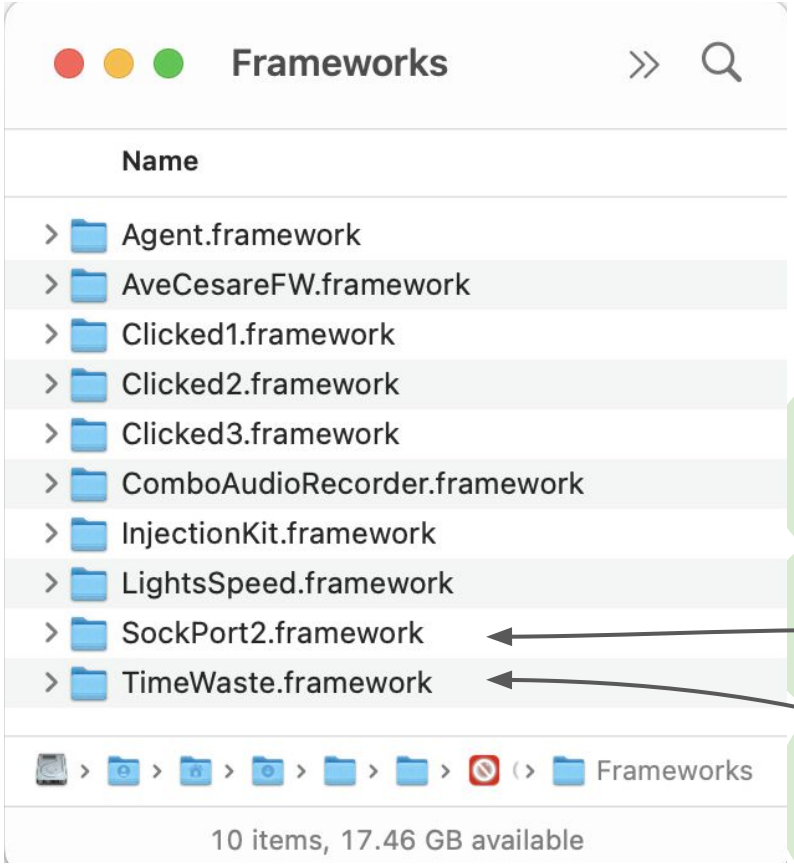


from github:

time_waste

CVE-2020-3837

GPL-licensed ;-)



from github:

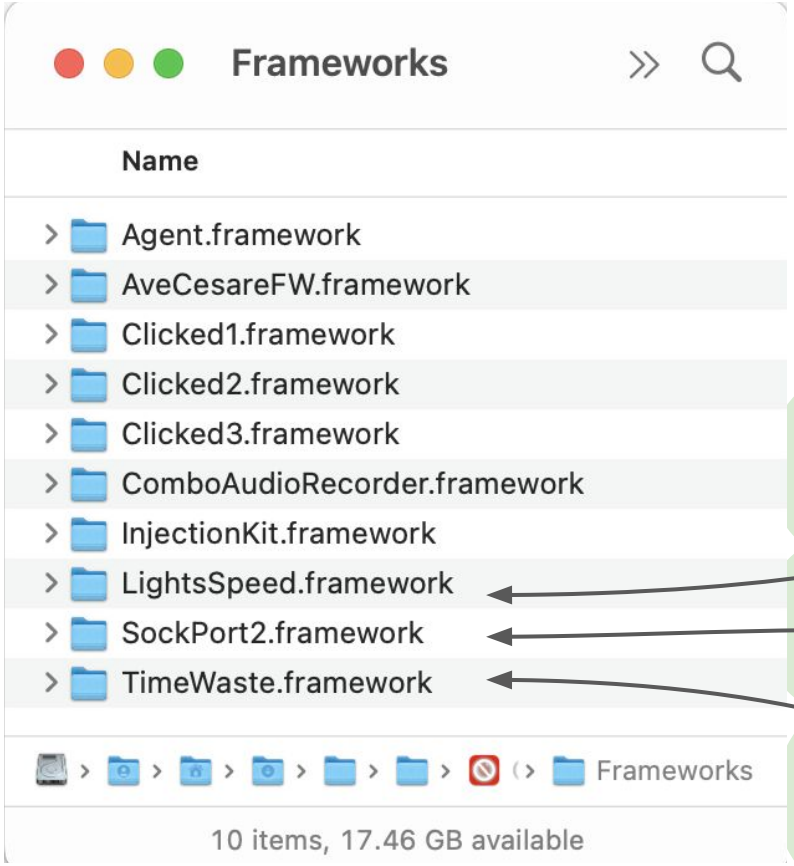
sockpuppet

CVE-2019-8605

time_waste

CVE-2020-3837

GPL-licensed ;-)



from github:

lio_listio

CVE-2018-4344

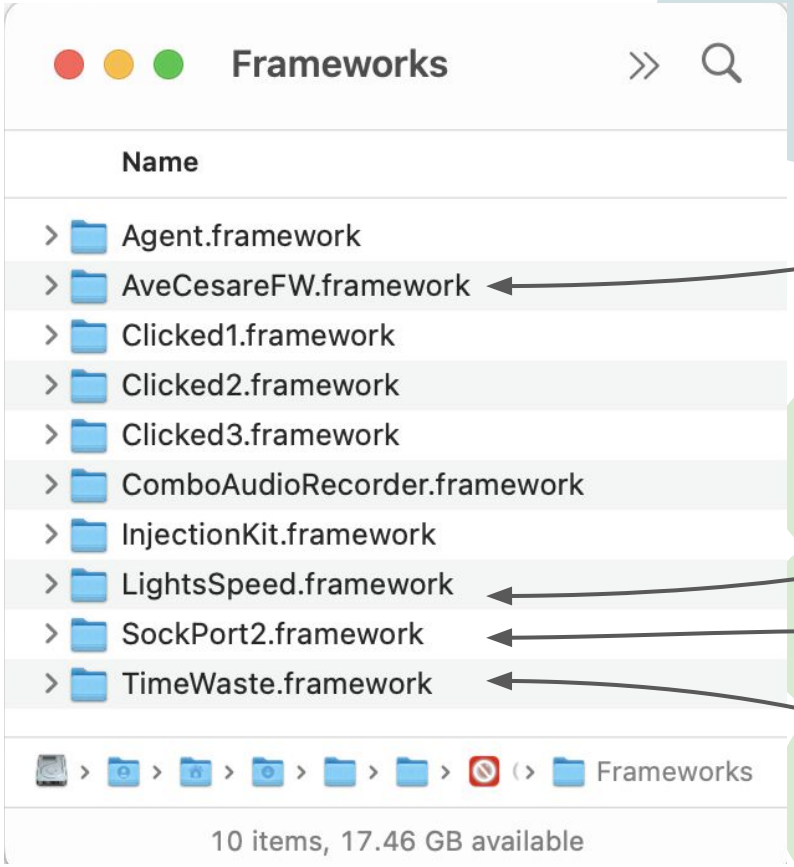
sockpuppet

CVE-2019-8605

time_waste

CVE-2020-3837

GPL-licensed ;-)



discussed by 08tc3wbb at BH EU 2020

CVE-2020-9907

from github:

lio_listio

CVE-2018-4344

sockpuppet

CVE-2019-8605

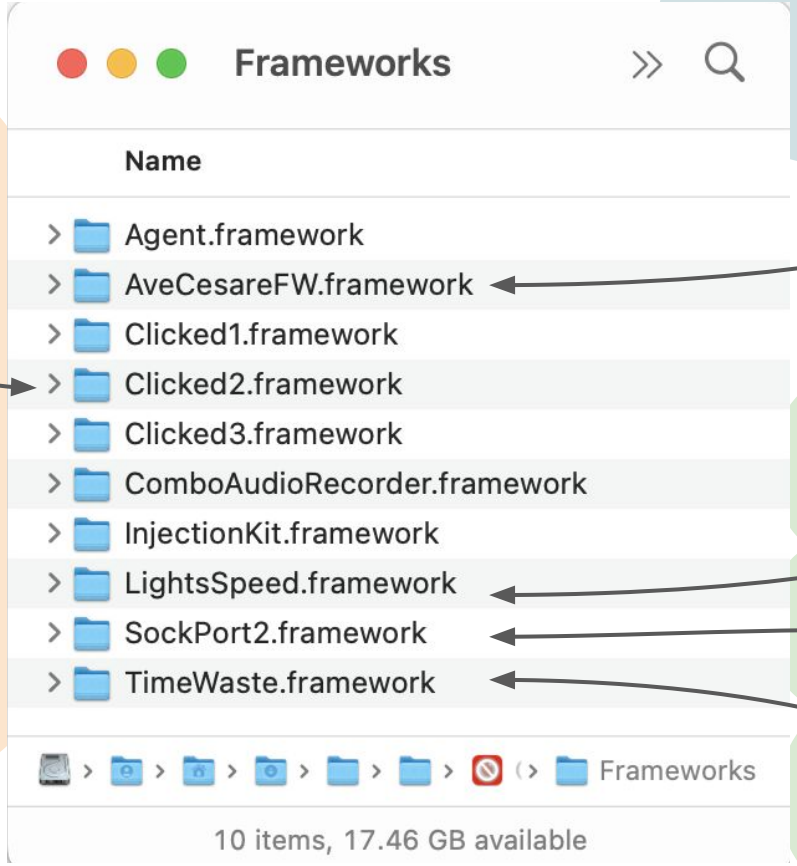
time_waste

CVE-2020-3837

GPL-licensed ;-)

0-day when used:

CVE-2021-30883



discussed by 08tc3wbb at BH EU 2020

CVE-2020-9907

from github:

lio_listio

CVE-2018-4344

sockpuppet

CVE-2019-8605

time_waste

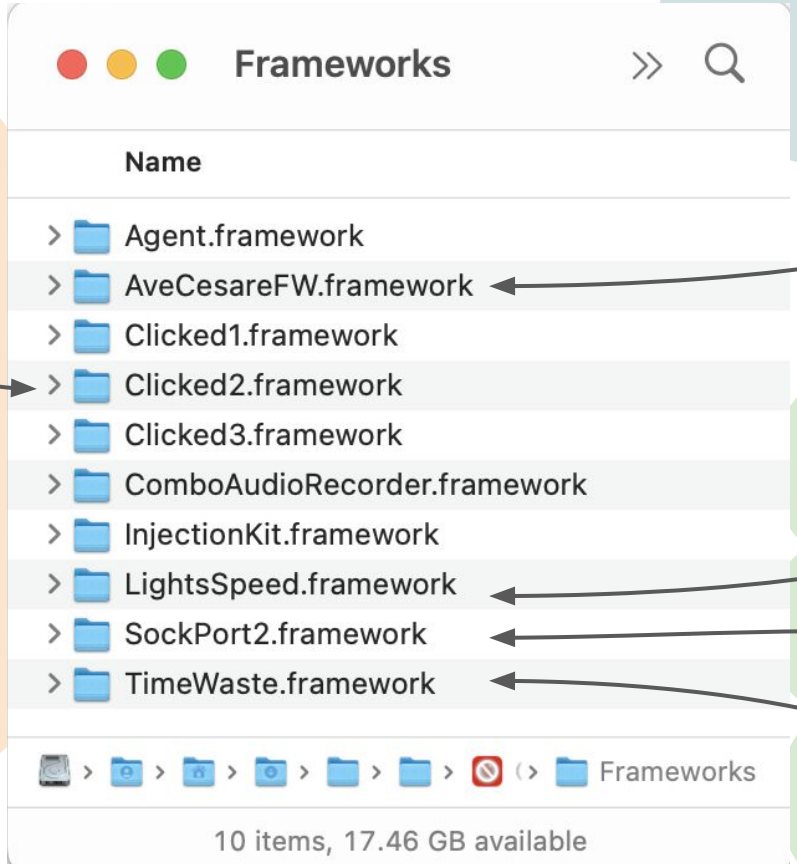
CVE-2020-3837

GPL-licensed ;-)

0-day when used:

Analysed by Saar Amar:
IOMFB_integer_overflow_poc

CVE-2021-30883



discussed by 08tc3wbb at BH EU 2020

CVE-2020-9907

from github:

lio_listio

CVE-2018-4344

sockpuppet

CVE-2019-8605

time_waste

CVE-2020-3837

GPL-licensed ;-)

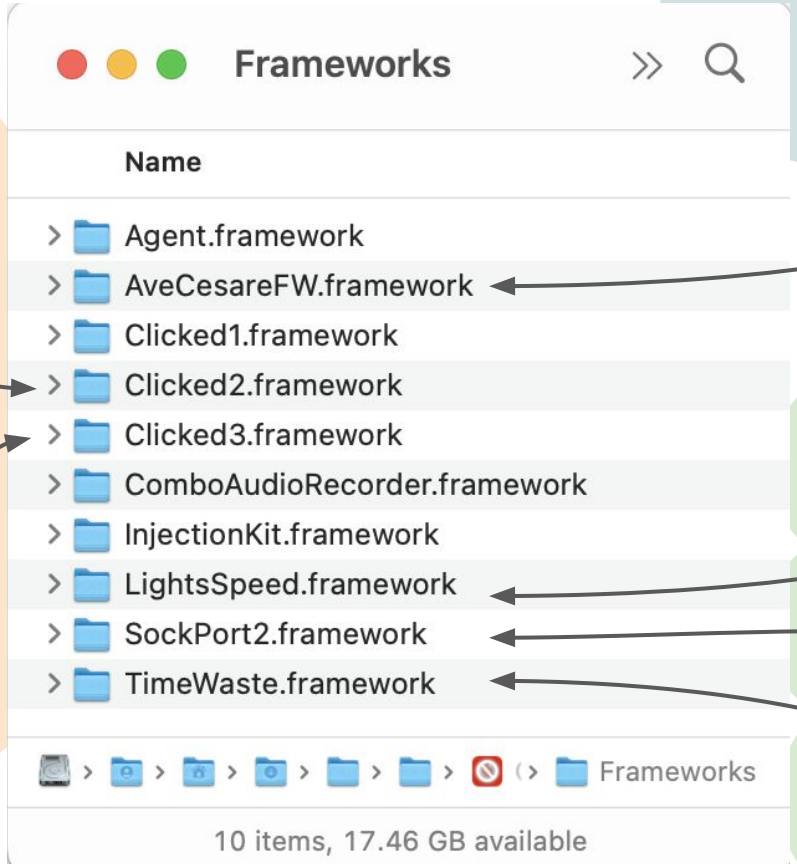
0-day when used:

Analysed by Saar Amar:
IOMFB_integer_overflow_poc

CVE-2021-30883

CVE-2021-30883

This talk



discussed by 08tc3wbb at BH EU 2020

CVE-2020-9907

from github:

lio_listio

CVE-2018-4344

sockpuppet

CVE-2019-8605

time_waste

CVE-2020-3837

GPL-licensed ;-)

one exploit is not like the others...

```
printf("Failed to prepare fake vtable: 0x%08x", ret);
```

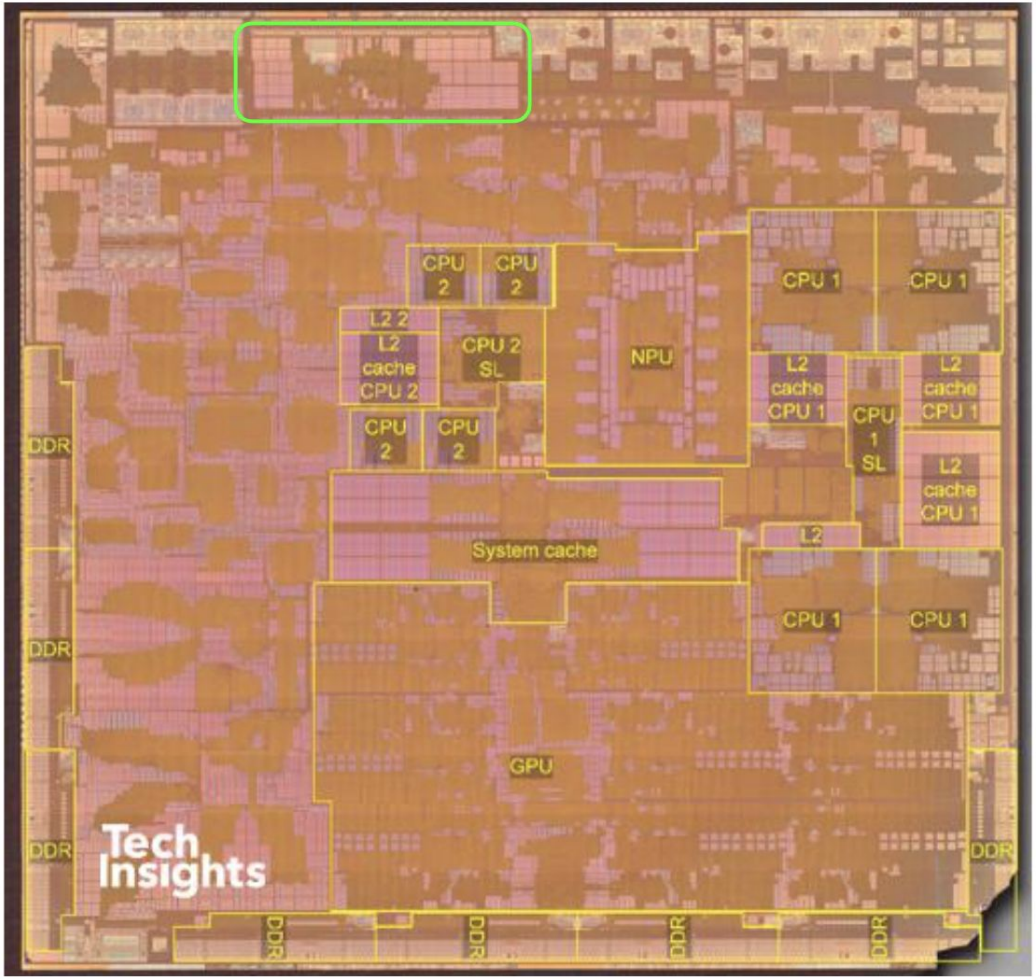
```
printf("Waiting for R/W primitives...");
```

```
printf("Unexpected data read from DCP: 0x%08x", v49);
```

```
printf("Unexpected data read from DCP: 0x%08x", v49);
```

DCP

Display co-processor



https://www.techinsights.com/blog/two-new-apple-socs-two-market-events-apple-a14-and-m1

```
$ ls -lh rawfw/iphone13dcp
```

```
$ ls -lh rawfw/iphone13dcp
-rw-r--r--  1 user primary 3.7M rawfw/iphone13dcp
```

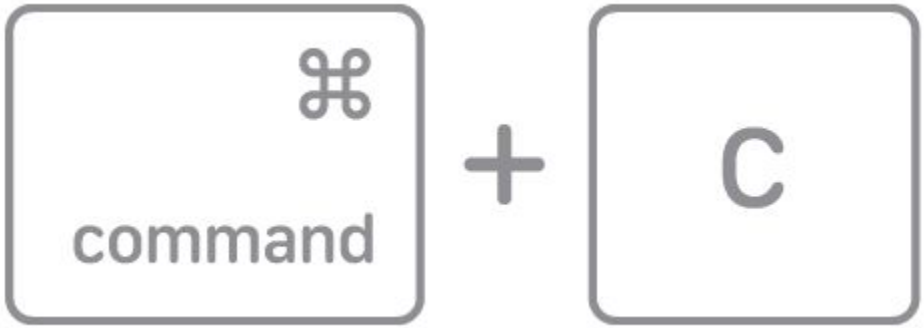
```
$ otool -h raw_fw/iphone13dcp
```

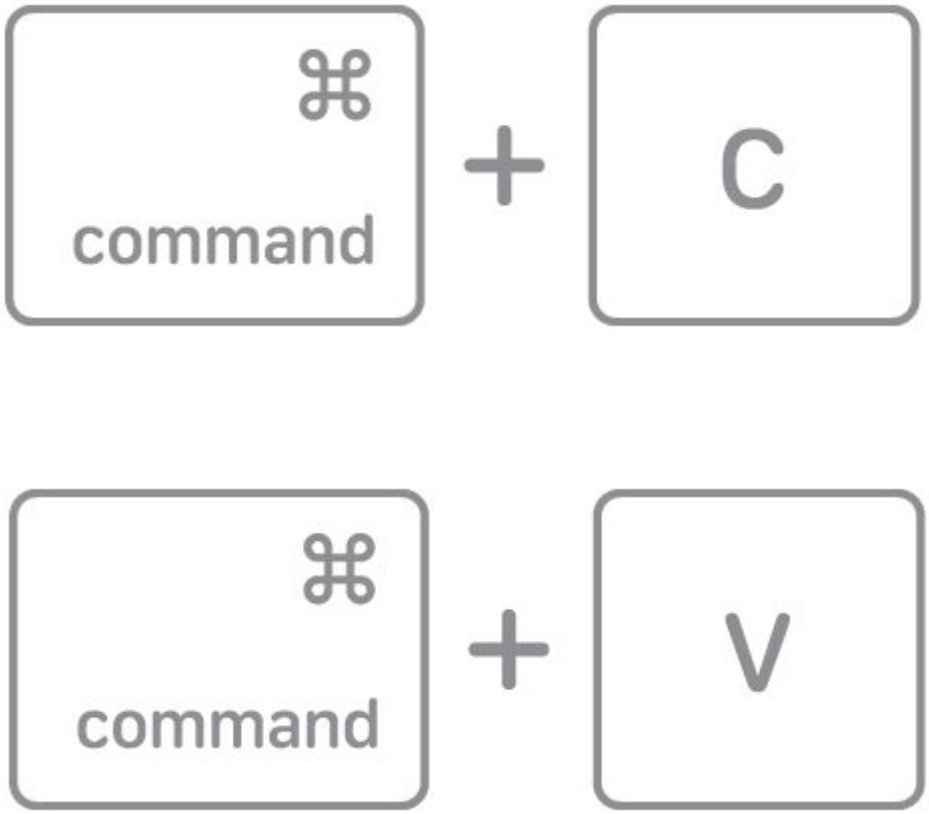
```
$ otool -h raw_fw/iphone13dcp
raw_fw/iphone13dcp:
Mach header
magic
0xfeedfacf
```

```
$ otool -h raw_fw/iphone13dcp
raw_fw/iphone13dcp:
Mach header
magic      cputype   cpusubtype
0xfeedfacf 0x100000C 0
```

```
$ otool -h raw_fw/iphone13dcp
raw_fw/iphone13dcp:
Mach header
magic      cputype   cpusubtype caps filetype ncmds sizeofcmds flags
0xfeedfacf 0x100000C 0          0x00 5        5     2240       0x00000001
```

IOMobileFramebuffer


⌘
command
+
C

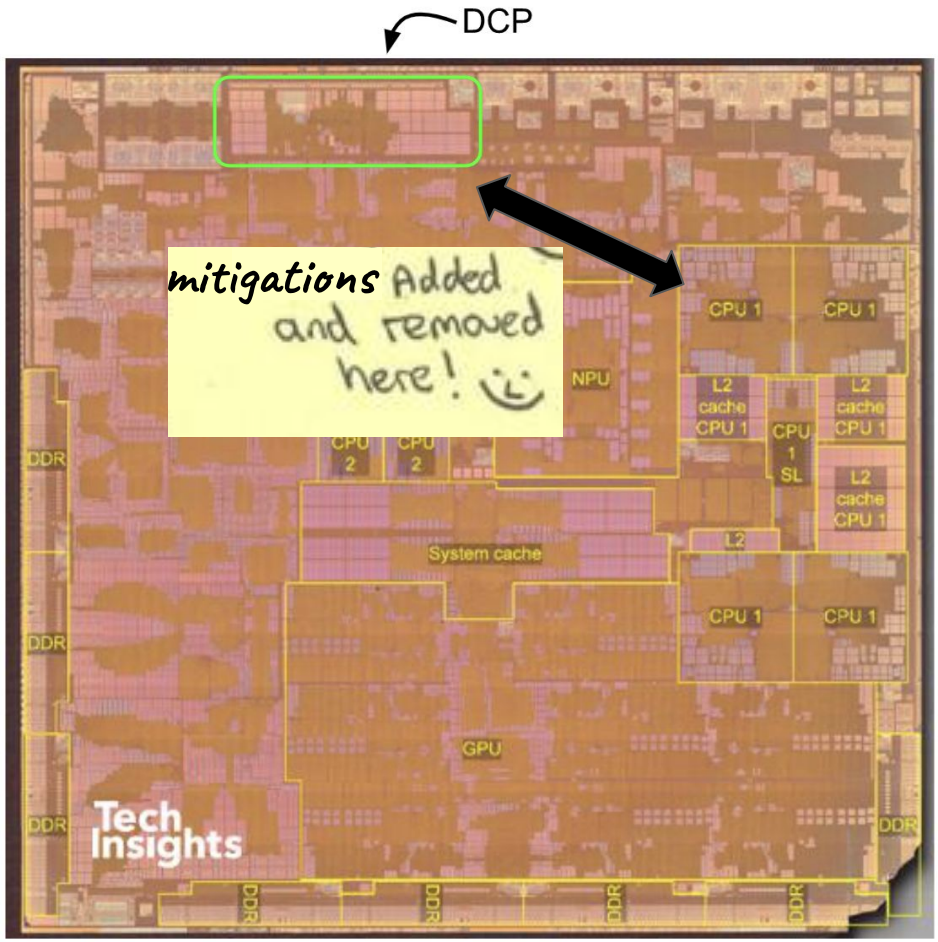

⌘
command
+
C
⌘
command
+
V

RTKit

No PAC

No PAC
No ASLR

No PAC
No ASLR
Predictable Heap Addresses



https://www.techinsights.com/blog/two-new-apple-socs-two-market-events-apple-a14-and-m1

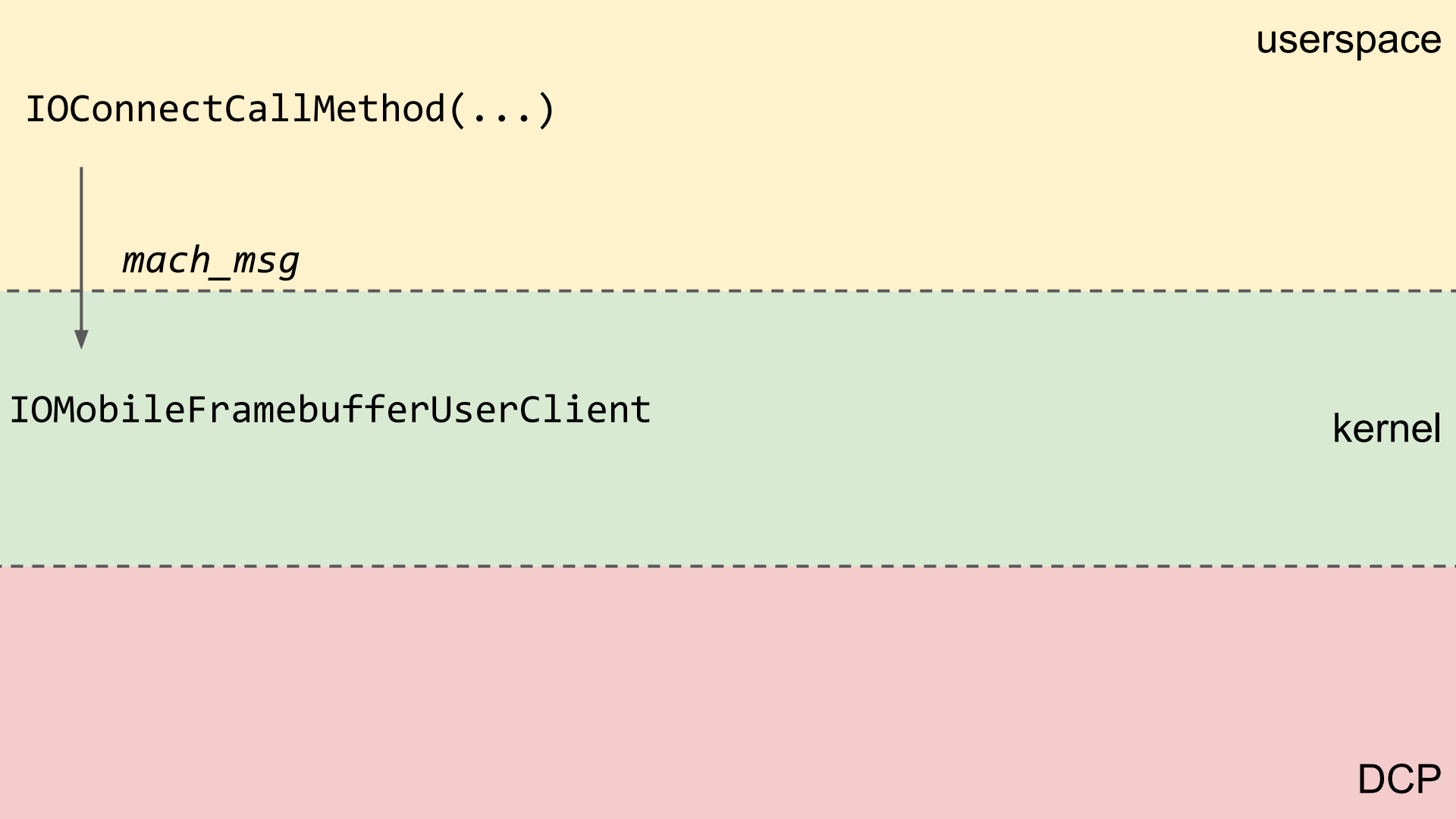
Talking to the DCP

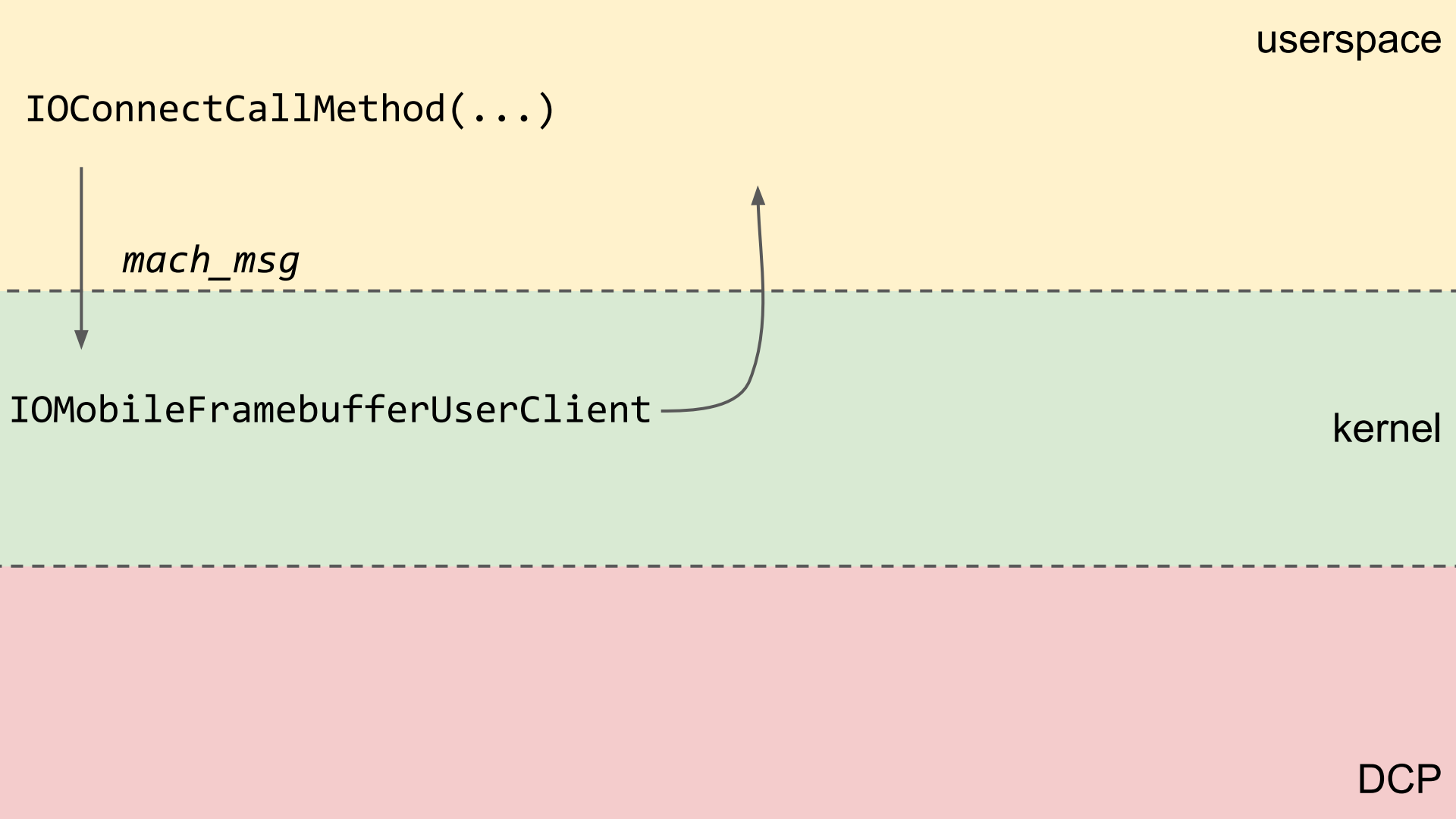
userspace

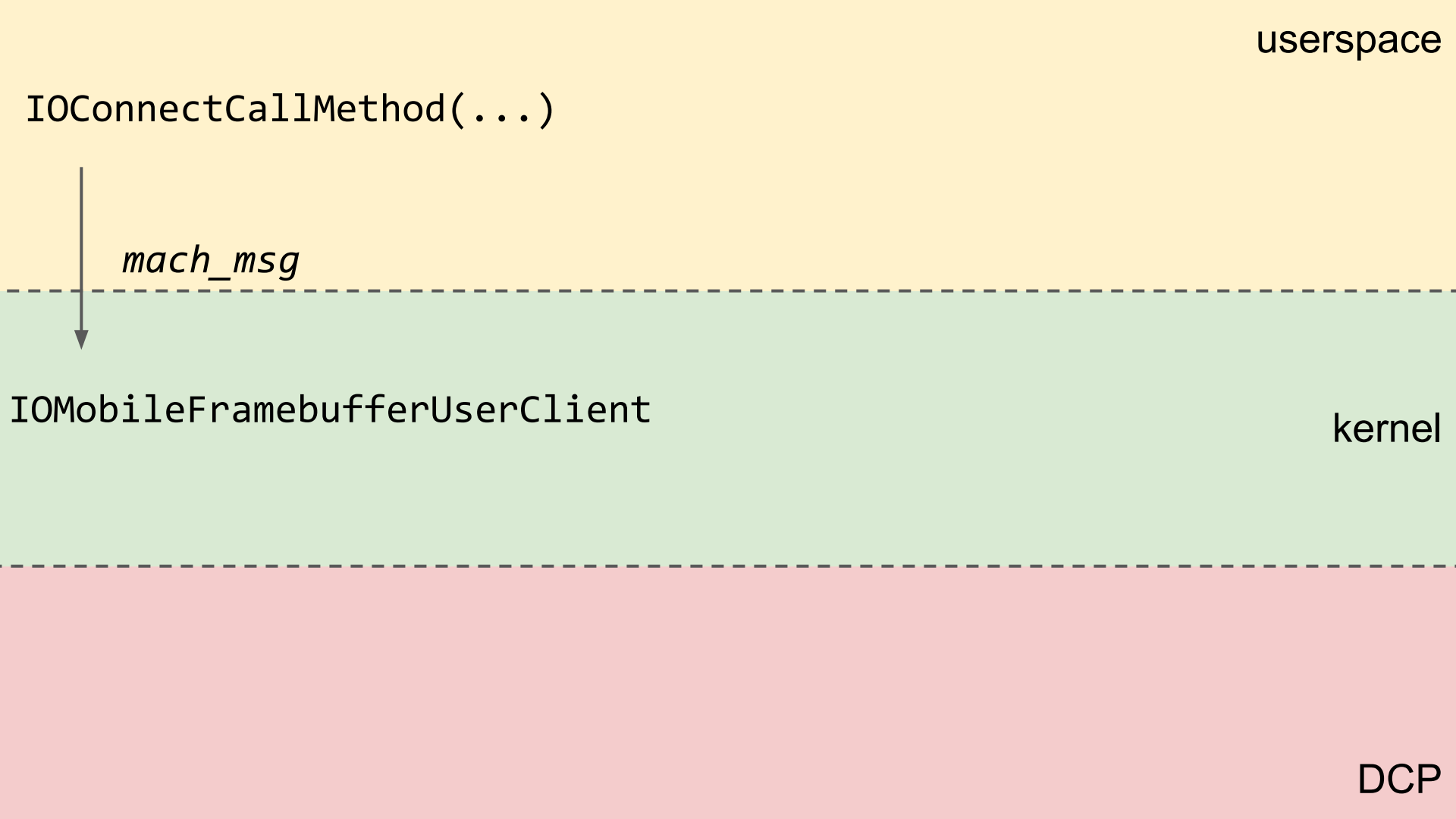
```
IOConnectCallMethod(...)
```

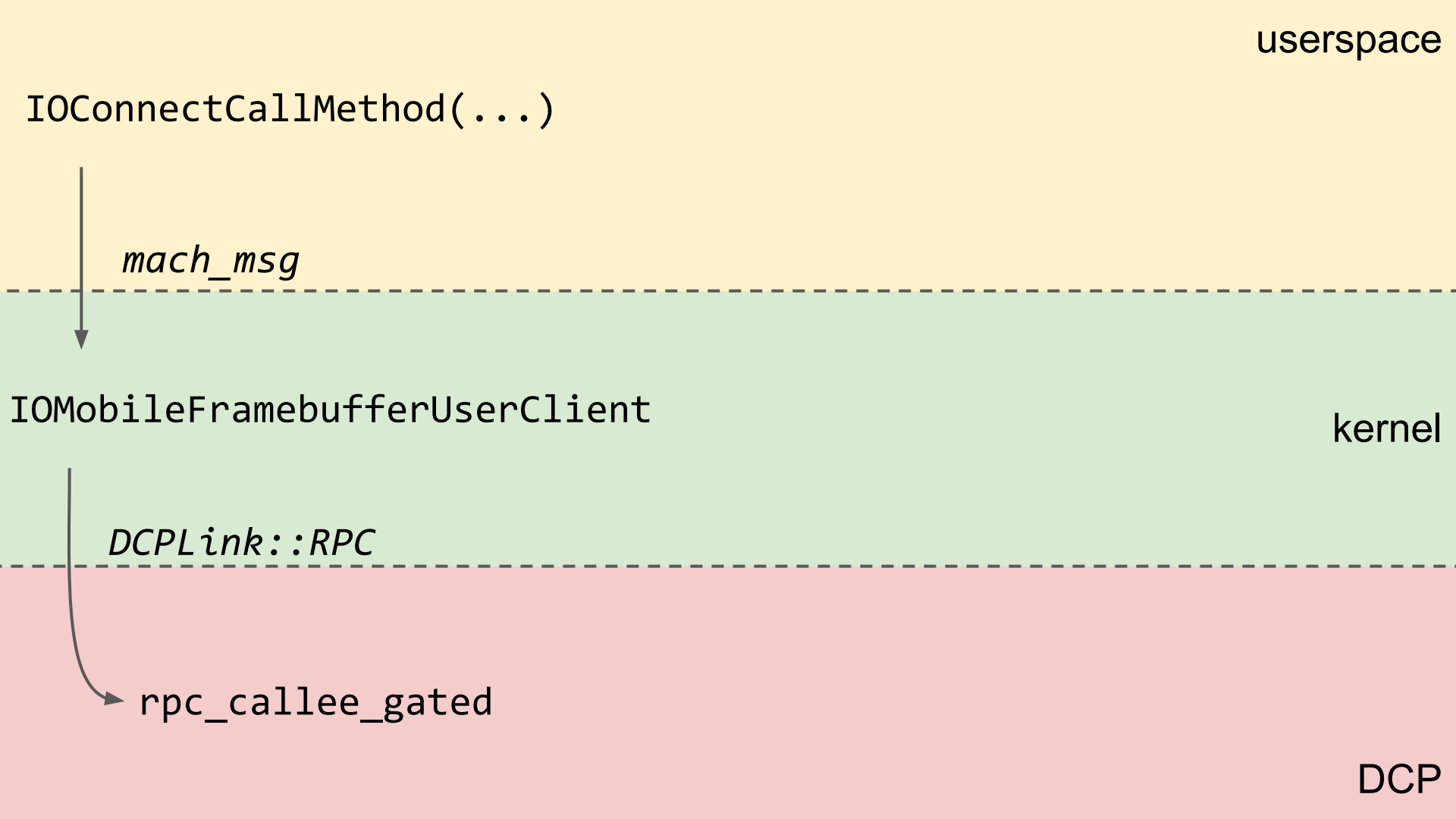
kernel

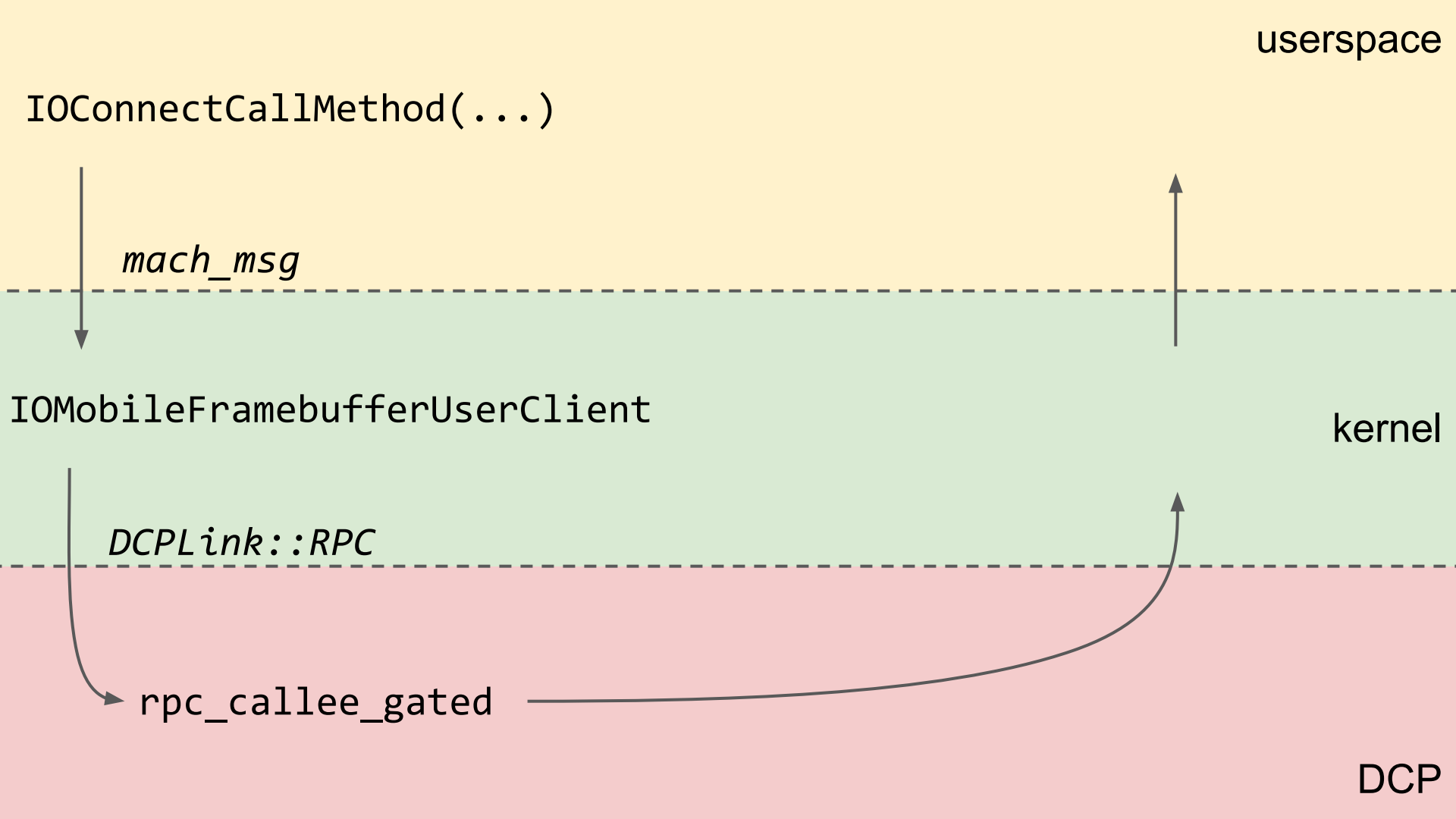
DCP


userspace
IOConnectCallMethod(...)
mach_msg
IOMobileFramebufferUserClient
kernel
DCP


userspace
IOConnectCallMethod(...)
mach_msg
IOMobileFramebufferUserClient
kernel
DCP


userspace
IOConnectCallMethod(...)
mach_msg
IOMobileFramebufferUserClient
kernel
DCP


userspace
IOConnectCallMethod(...)
mach_msg
IOMobileFramebufferUserClient
kernel
DCPLink::RPC
rpc_callee_gated
DCP

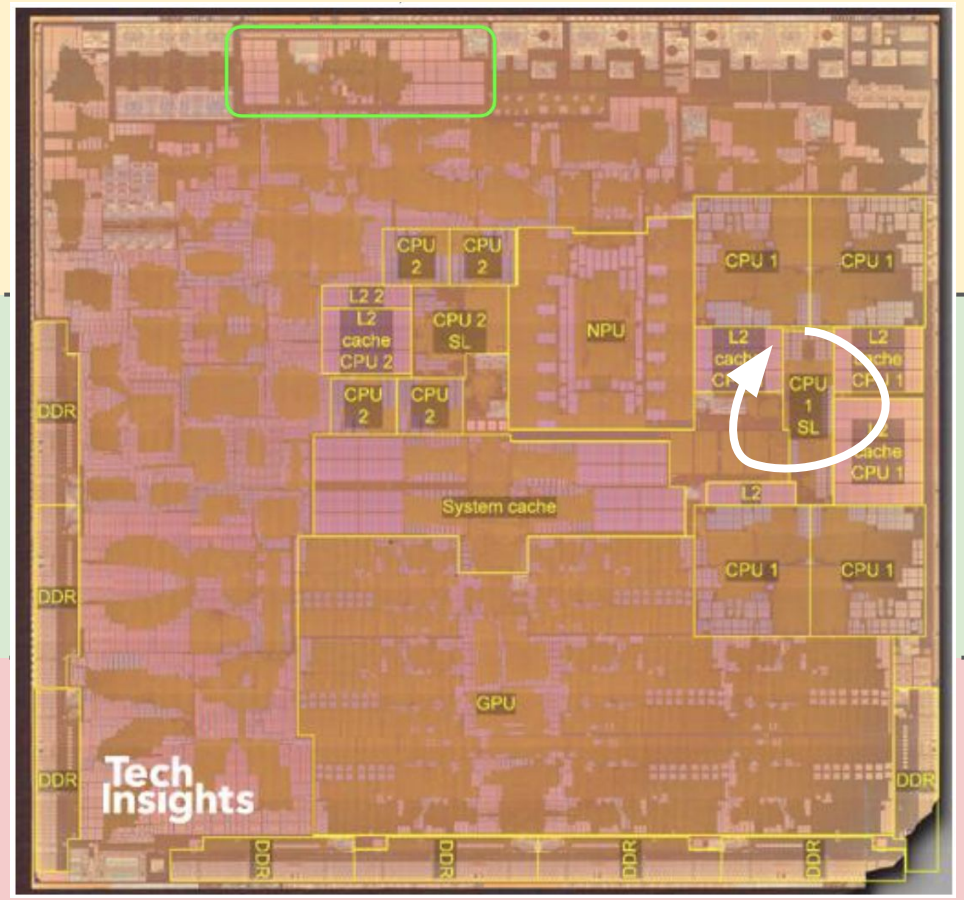

userspace
IOConnectCallMethod(...)
mach_msg
IOMobileFramebufferUserClient
kernel
DCPLink::RPC
rpc_callee_gated
DCP

userspace

IOConnectCallMethod(...)

mach_msg

IOMobileFramebuffer
UserClient



kernel

DCP

userspace

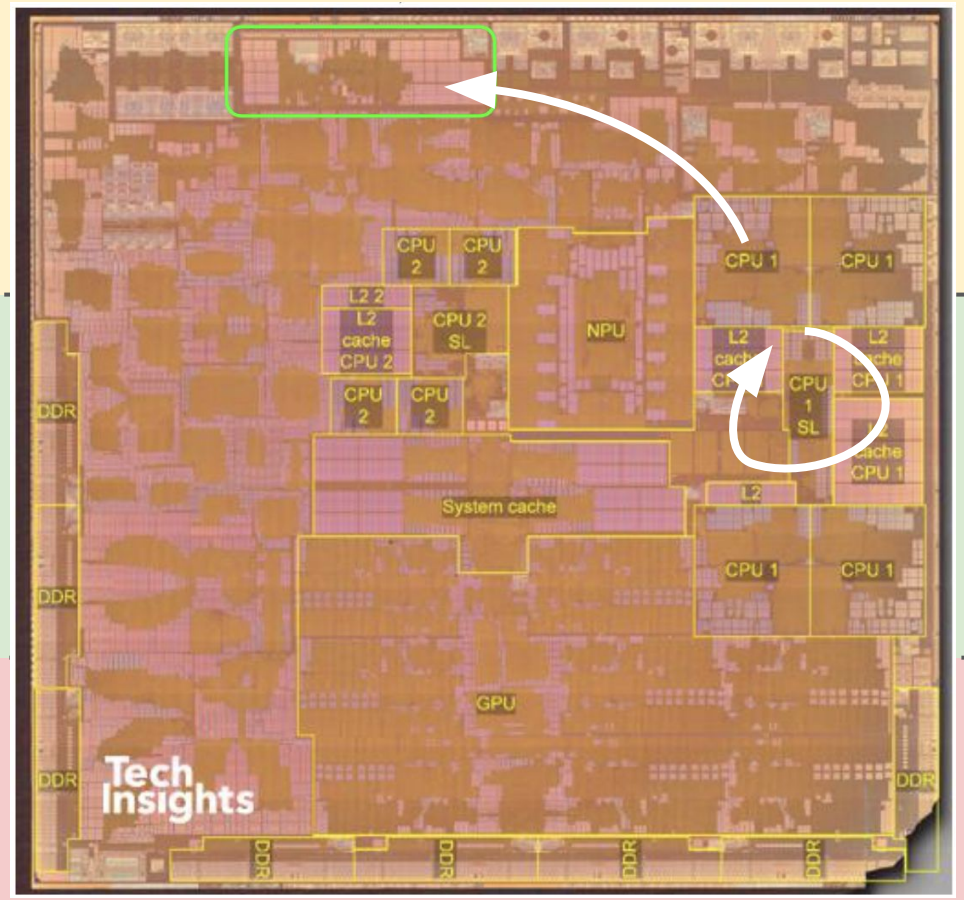
IOConnectCallMethod(...)

mach_msg

IOMobileFramebuffer
UserClient

DCPLink::RPC

rpc_callee_gated



kernel

DCP

userspace

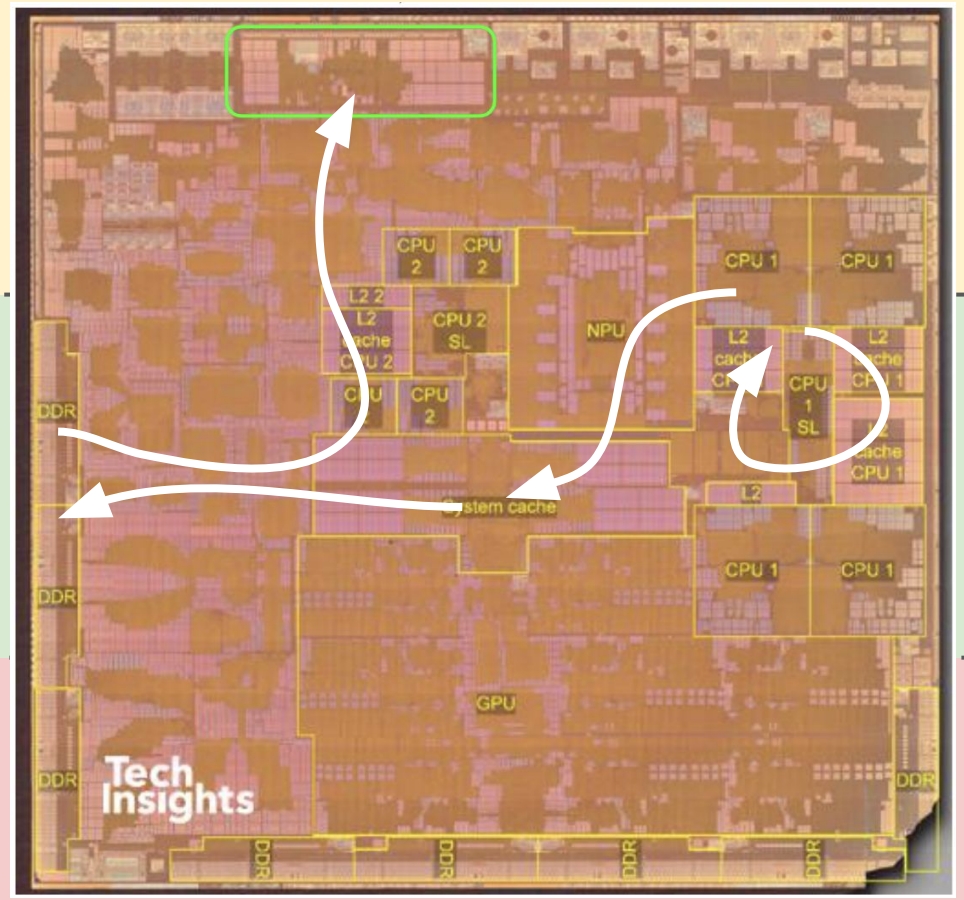
IOConnectCallMethod(...)

mach_msg

IOMobileFramebuffer
UserClient

DCPLink::RPC

rpc_callee_gated

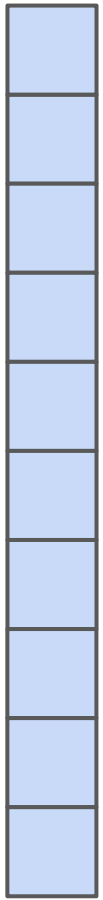


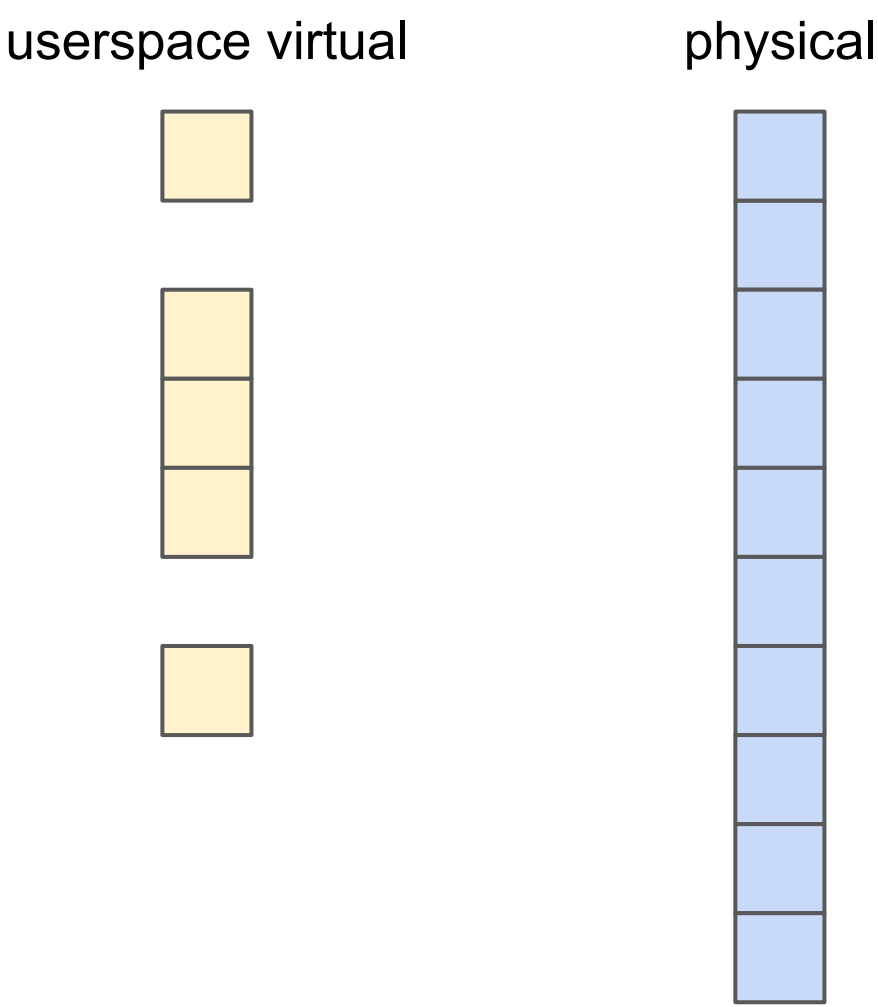
kernel

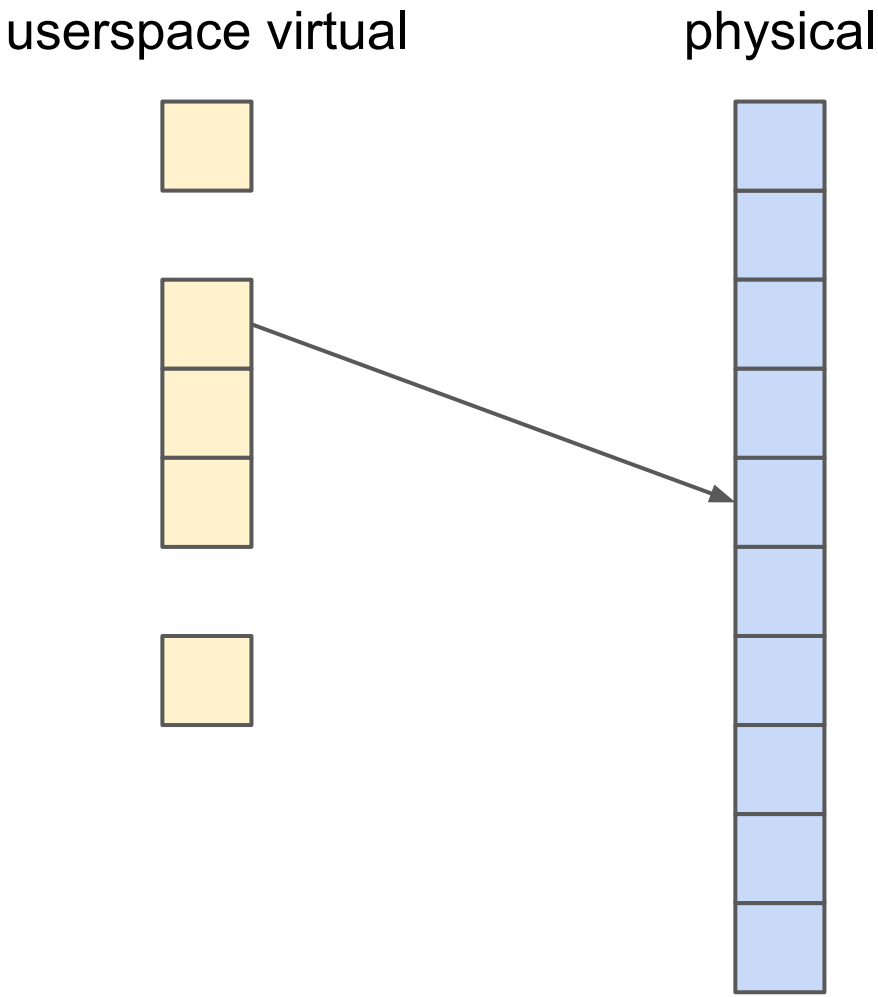
DCP

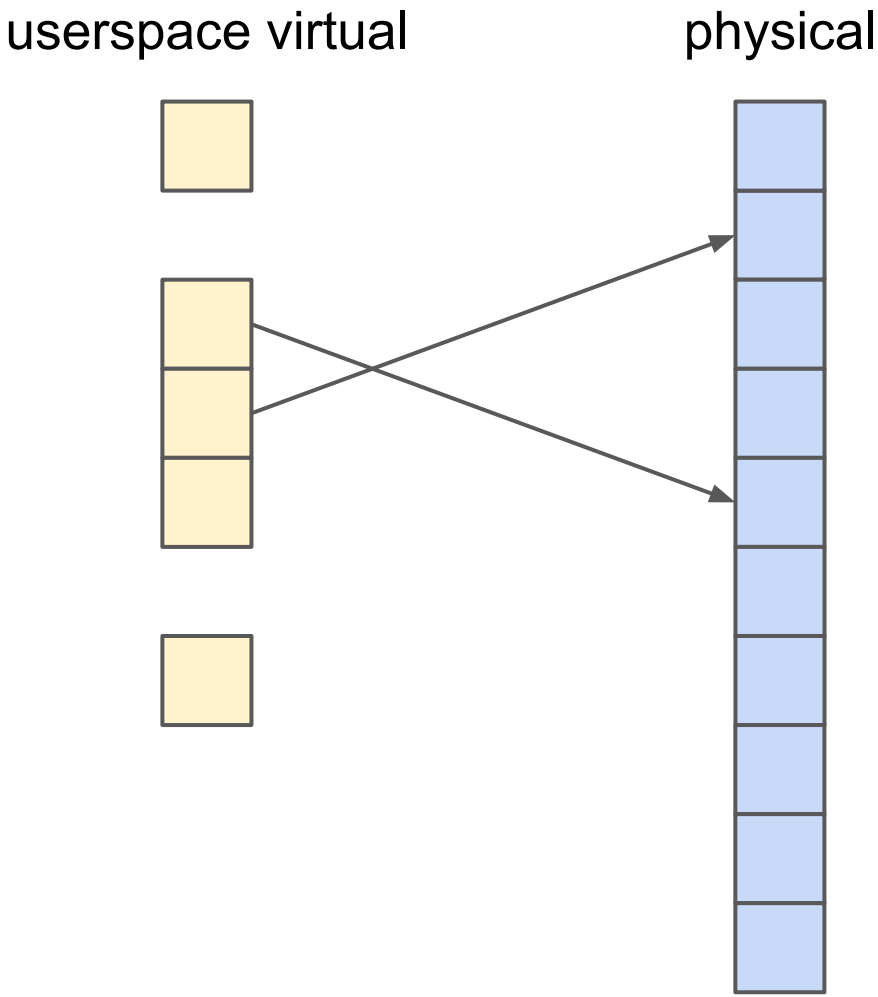
IOMMU/SMMU/DART

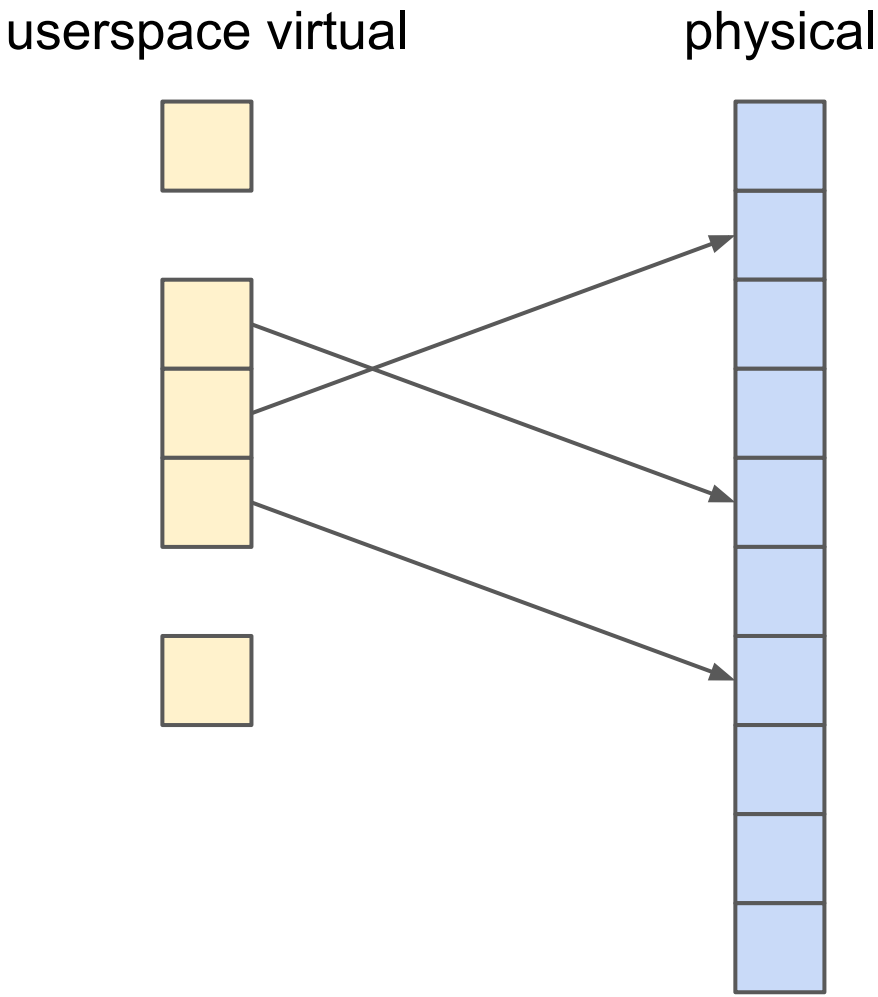
physical

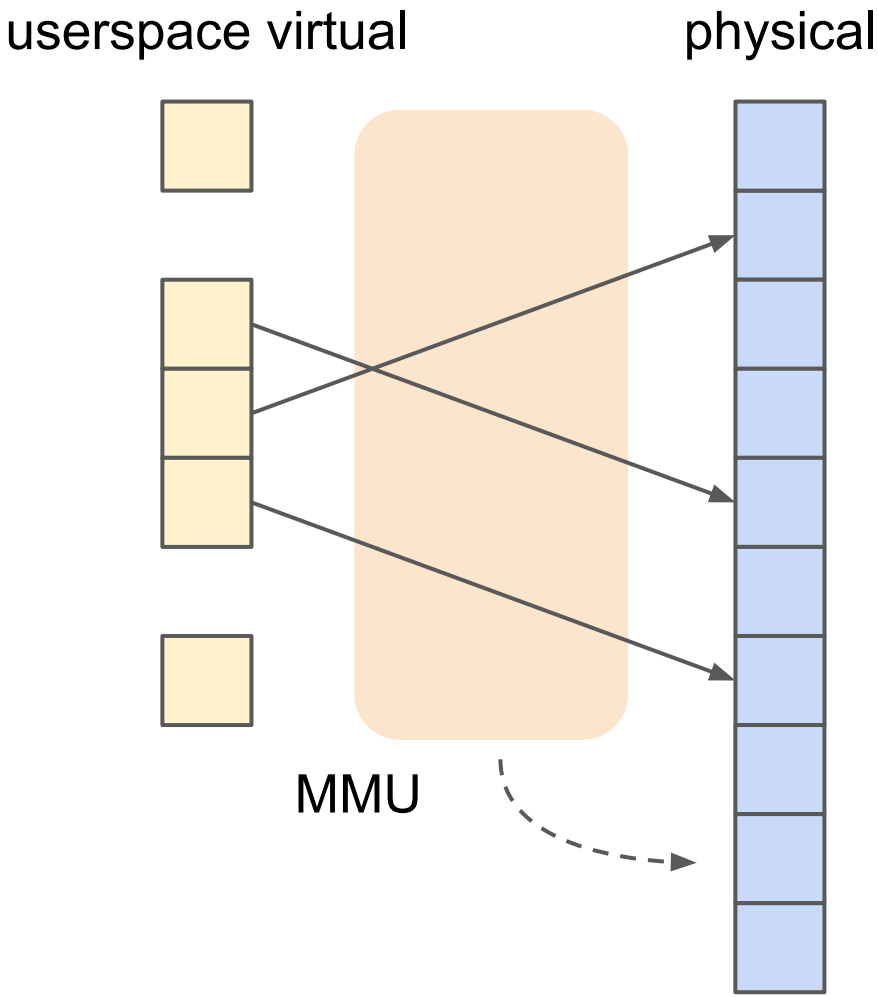


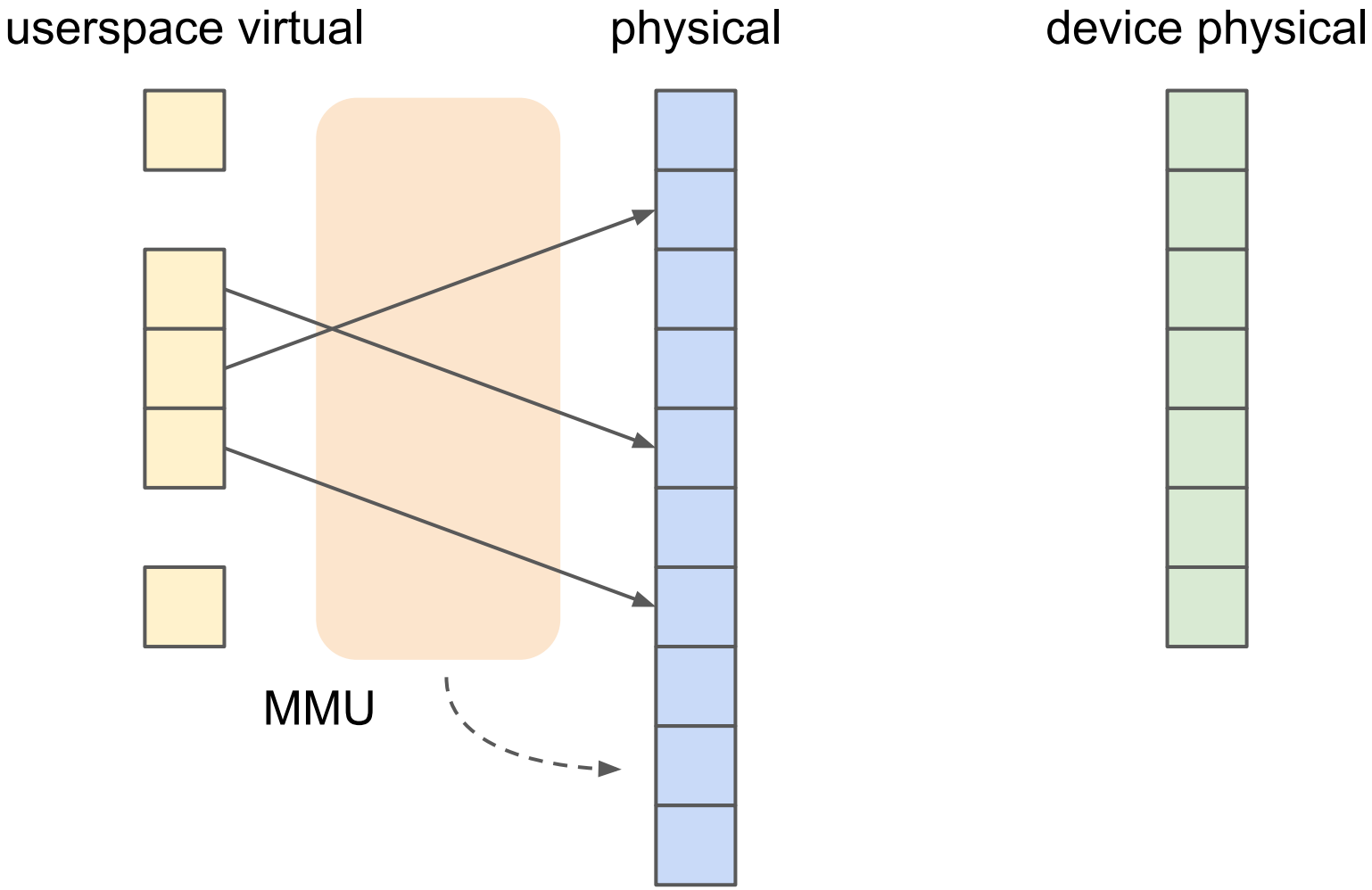

userspace virtual
physical

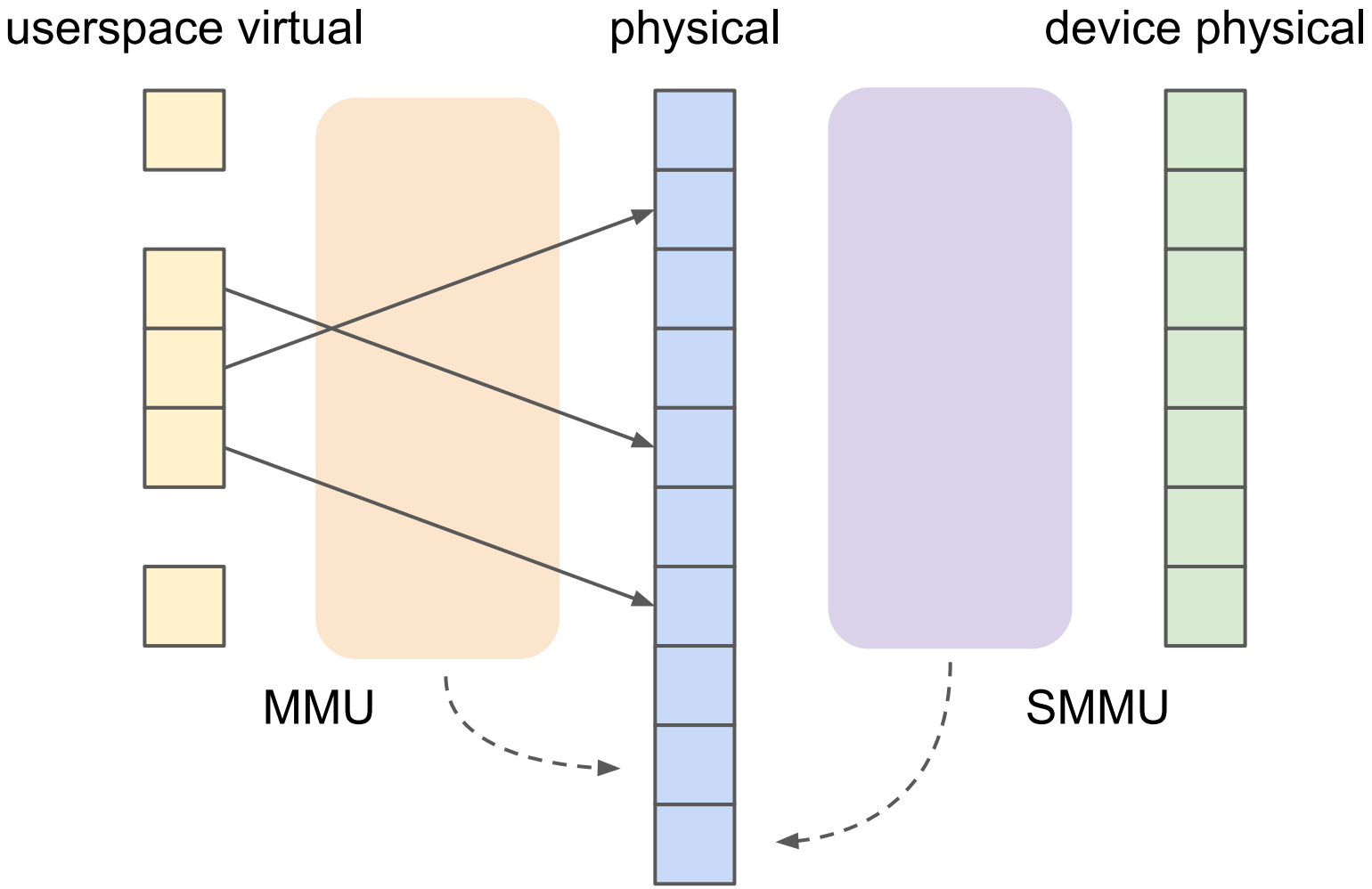

userspace virtual
physical

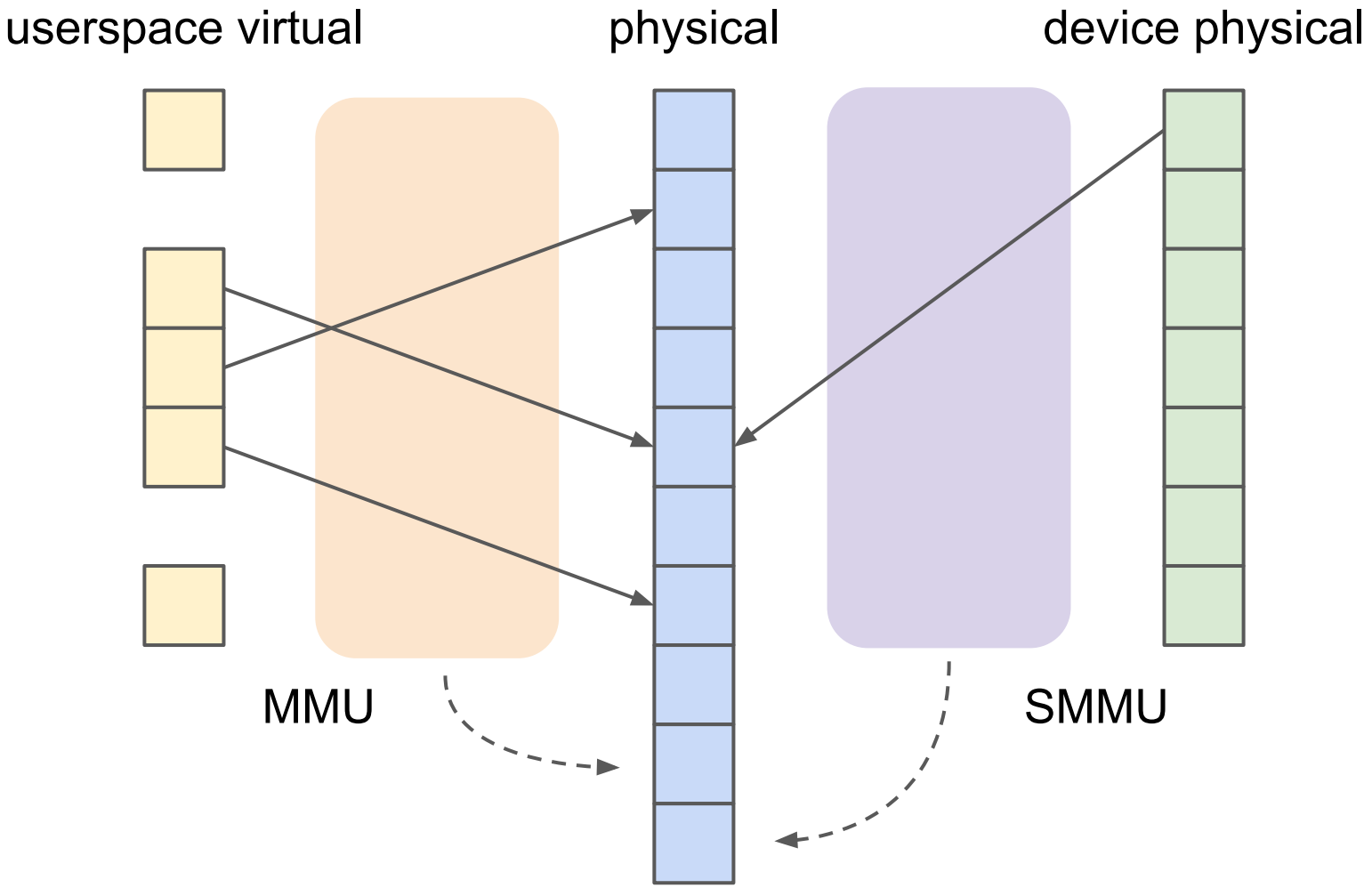

userspace virtual
physical

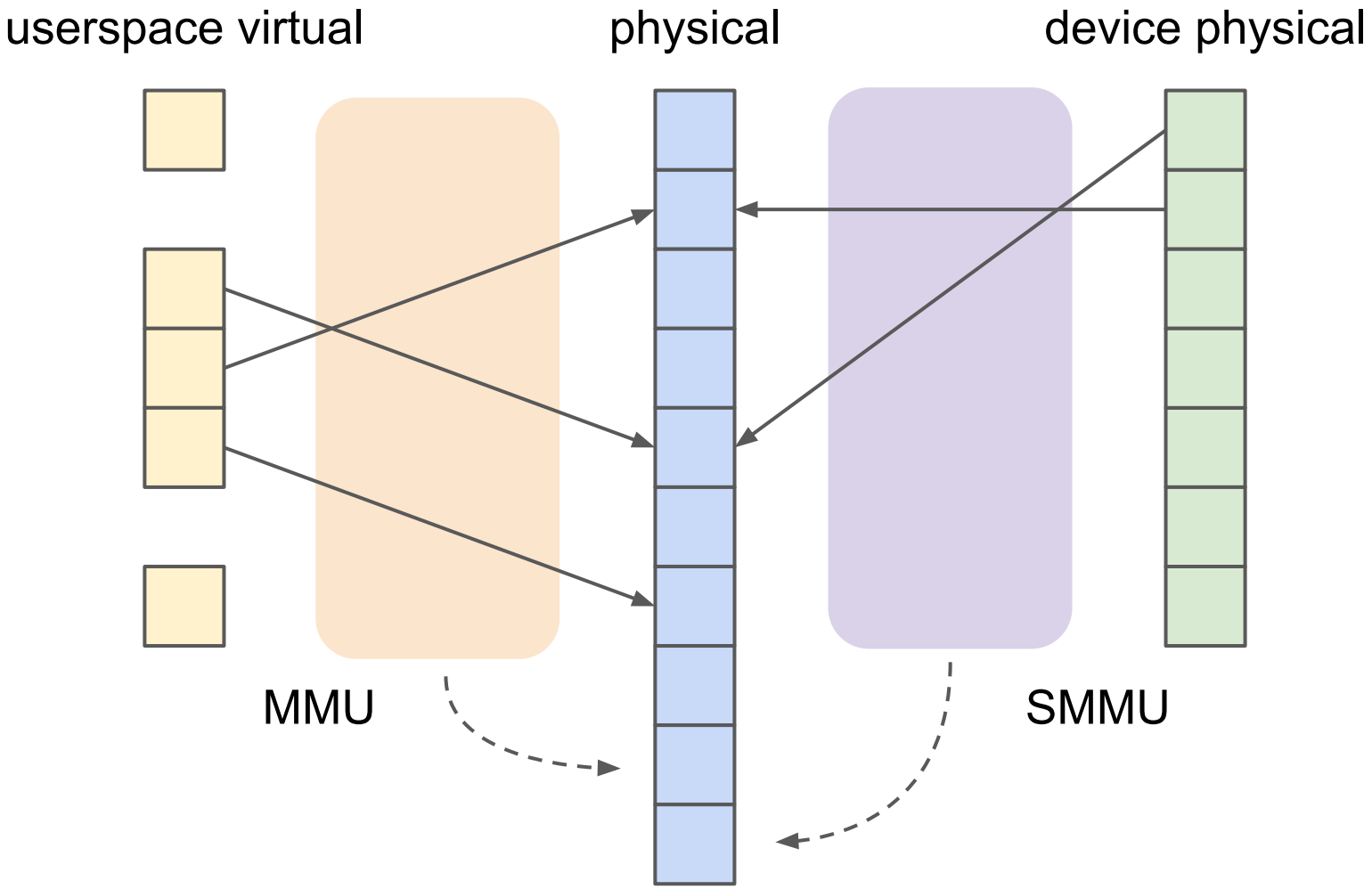

userspace virtual
physical

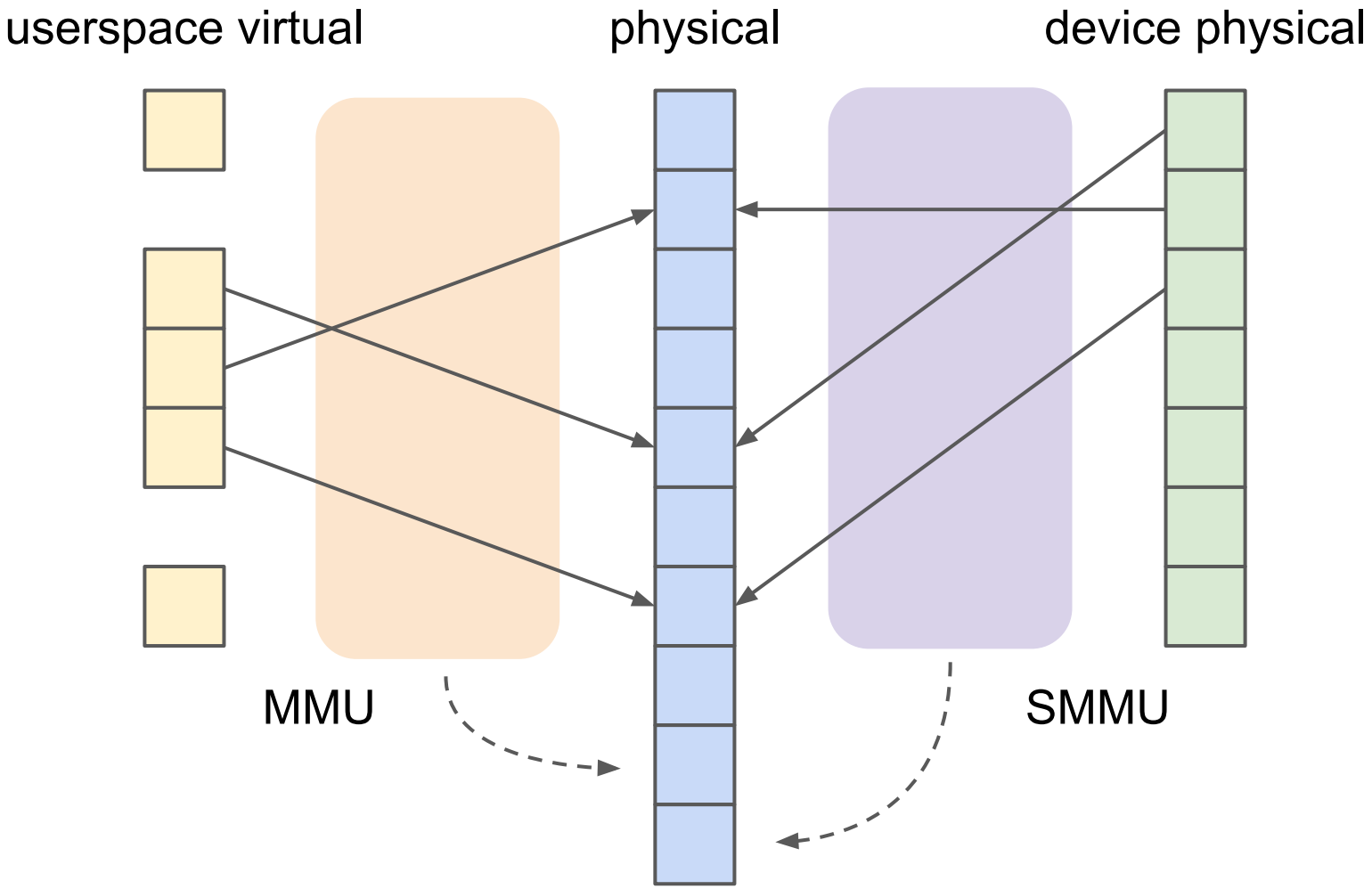

userspace virtual
physical
MMU


userspace virtual
physical
device physical
MMU


userspace virtual
physical
device physical
MMU
SMMU

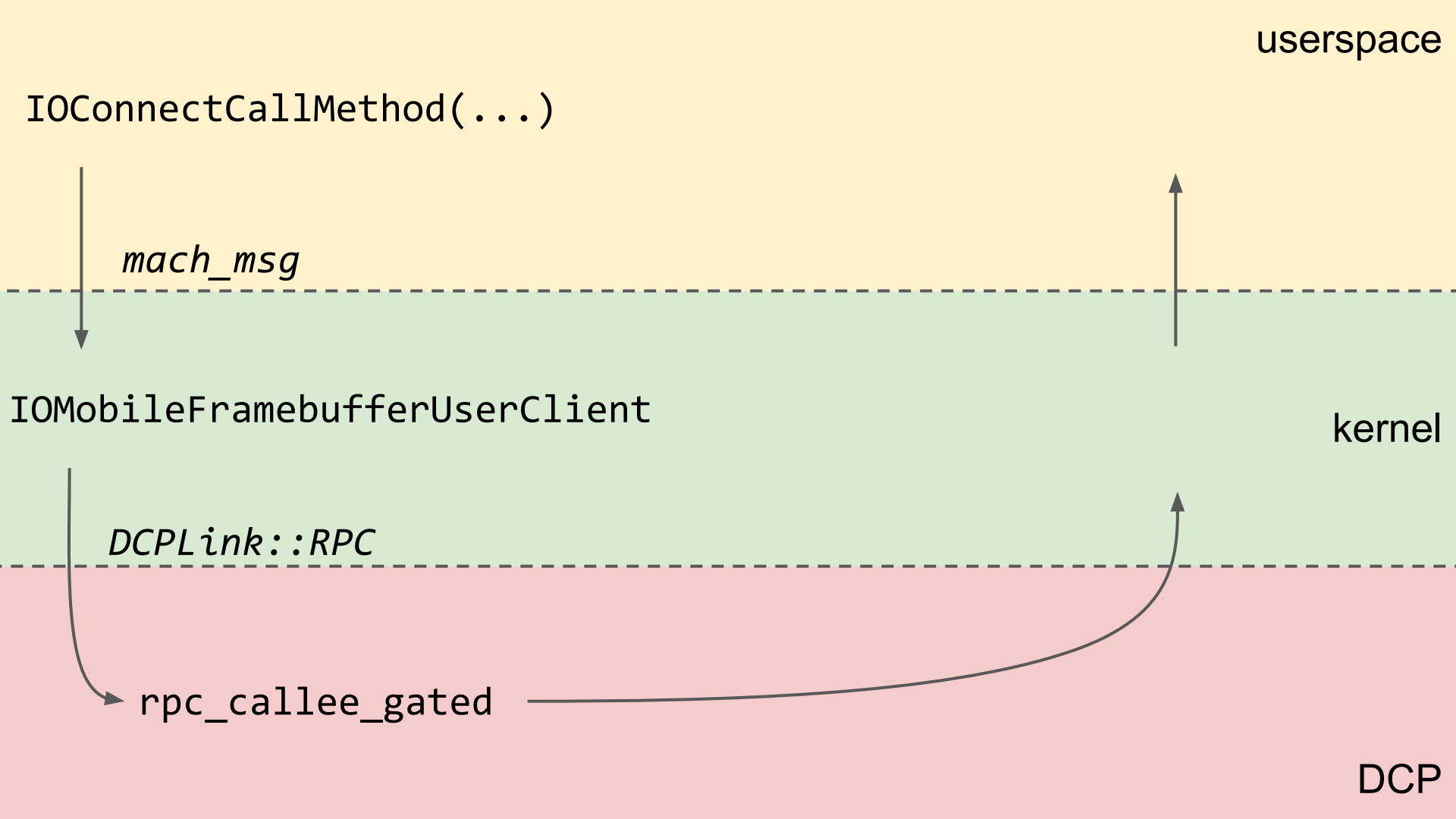

userspace virtual
physical
device physical
MMU
SMMU

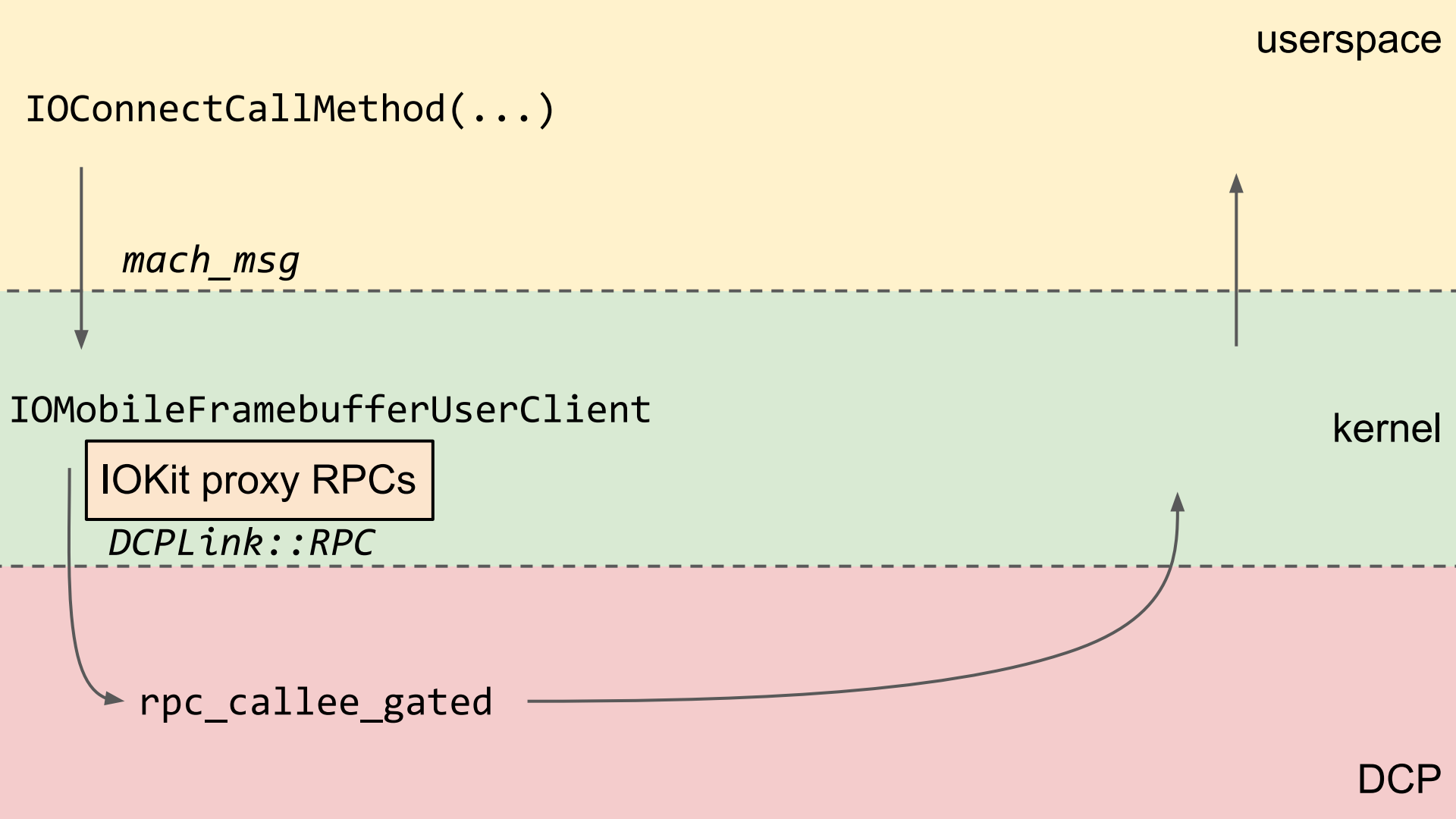

userspace virtual
physical
device physical
MMU
SMMU

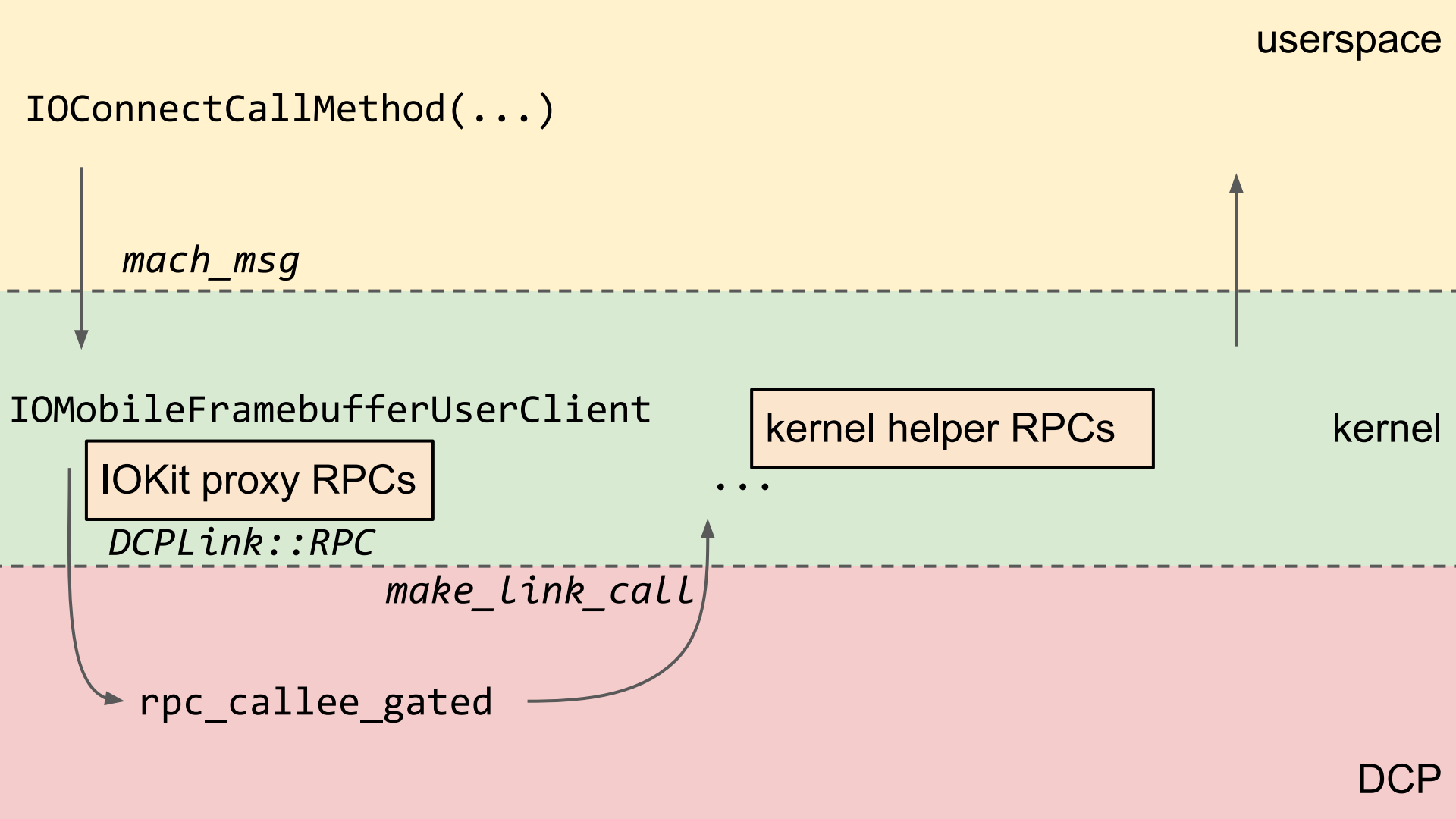

userspace virtual
physical
device physical
MMU
SMMU

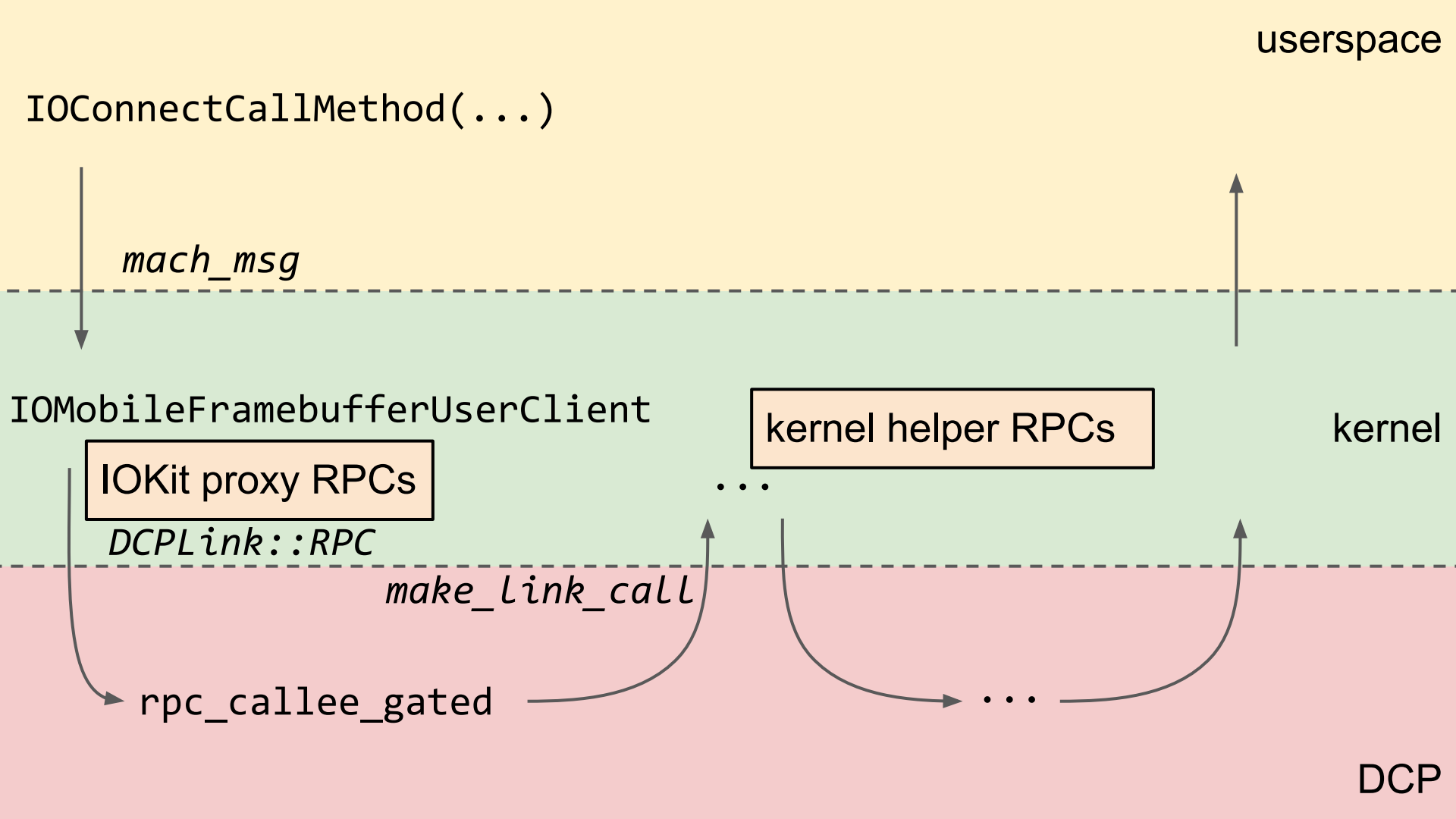
EL1 -> DCP?

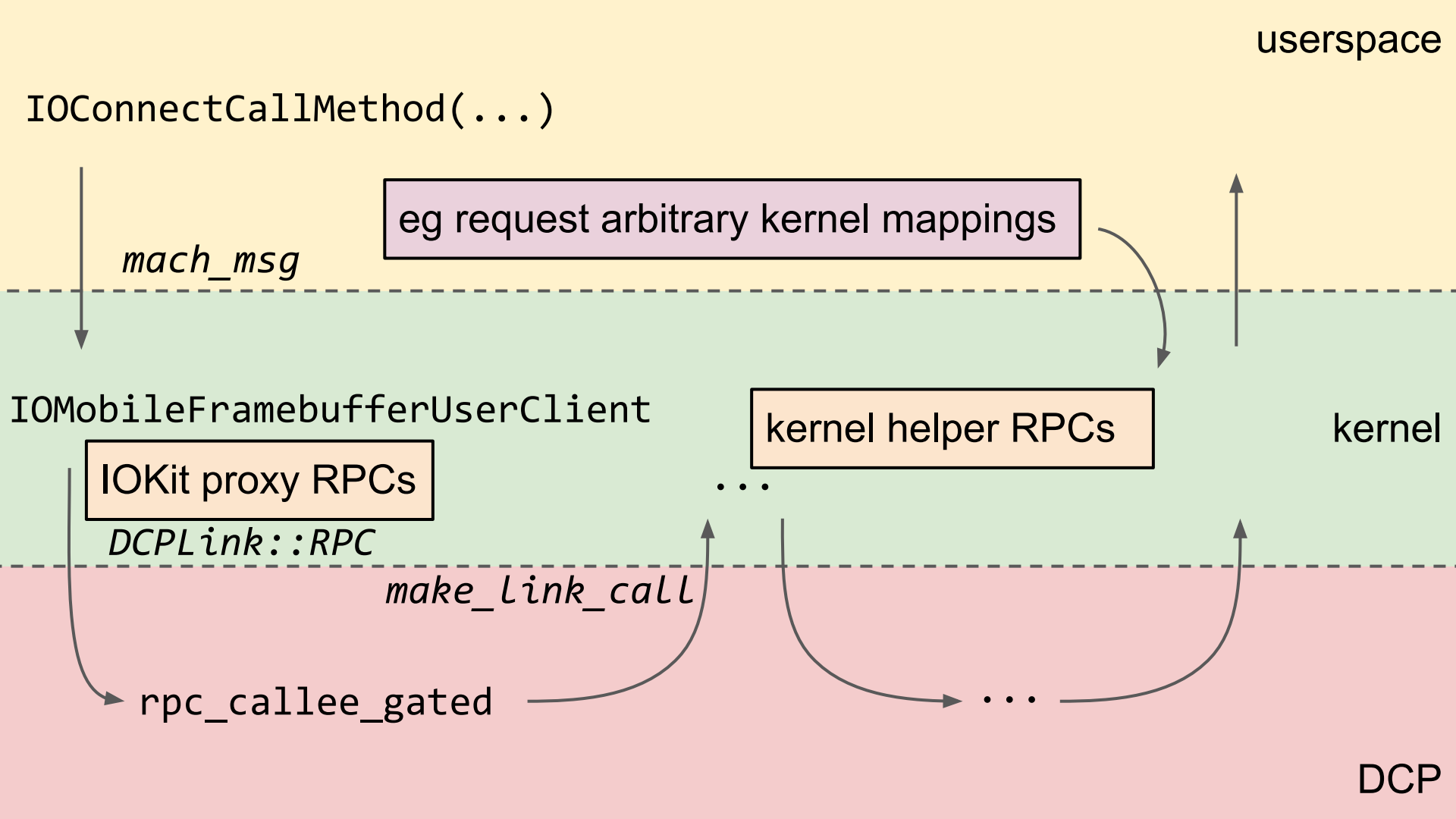
How to solve that?


userspace
IOConnectCallMethod(...)
mach_msg
IOMobileFramebufferUserClient
kernel
DCPLink::RPC
rpc_callee_gated
DCP


userspace
IOConnectCallMethod(...)
mach_msg
IOMobileFramebufferUserClient
kernel
IOKit proxy RPCs
DCPLink::RPC
rpc_callee_gated
DCP


userspace
IOConnectCallMethod(...)
mach_msg
IOMobileFramebufferUserClient
kernel helper RPCs
kernel
IOKit proxy RPCs
...
DCPLink::RPC
make_link_call
rpc_callee_gated
DCP


userspace
IOConnectCallMethod(...)
mach_msg
IOMobileFramebufferUserClient
IOKit proxy RPCs
DCPLink::RPC
kernel helper RPCs
kernel
...
make_link_call
rpc_callee_gated
...
DCP


userspace
IOConnectCallMethod(...)
mach_msg
eg request arbitrary kernel mappings
IOMobileFramebufferUserClient
kernel helper RPCs
kernel
IOKit proxy RPCs
...
DCPLink::RPC
make_link_call
rpc_callee_gated
...
DCP

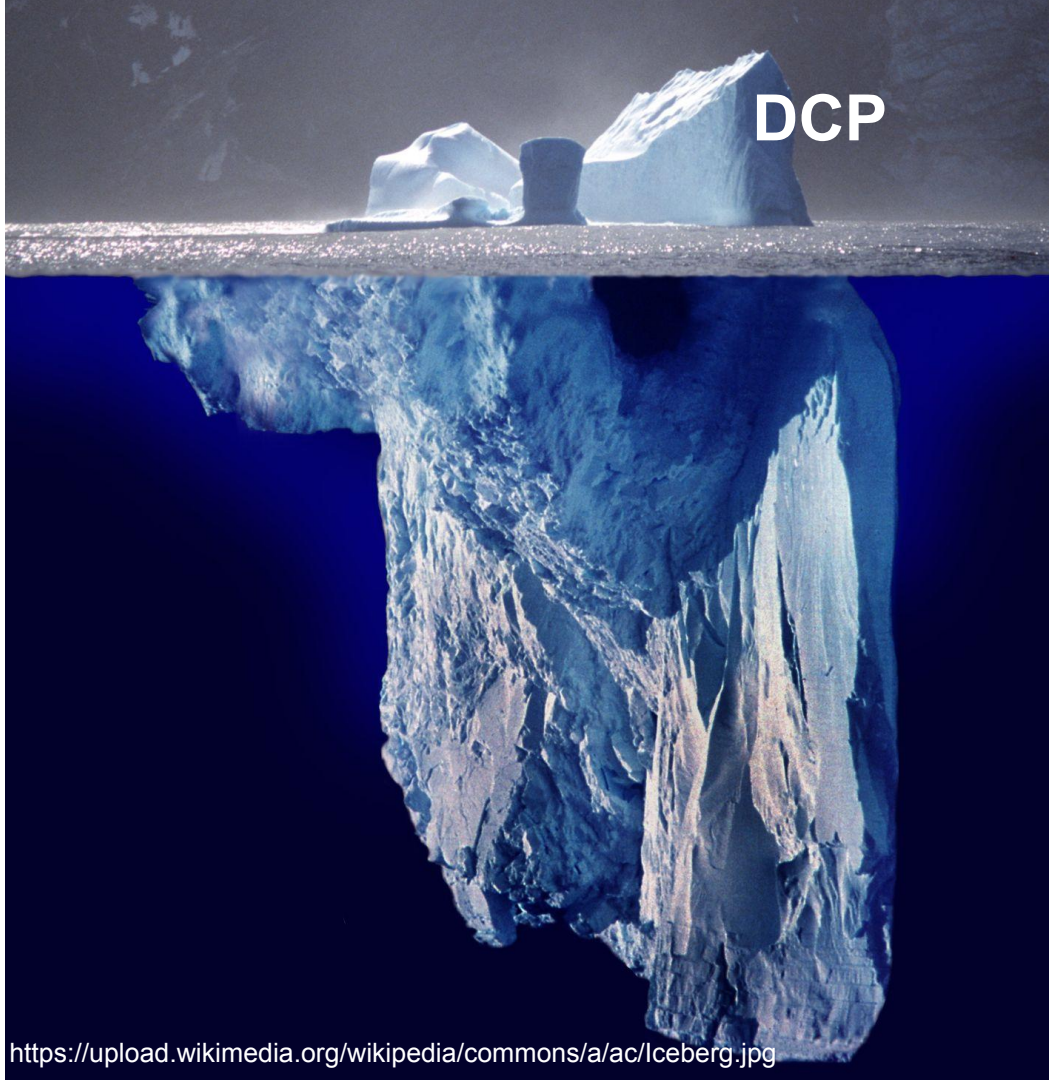
The ITW bug

Uniformity compensation

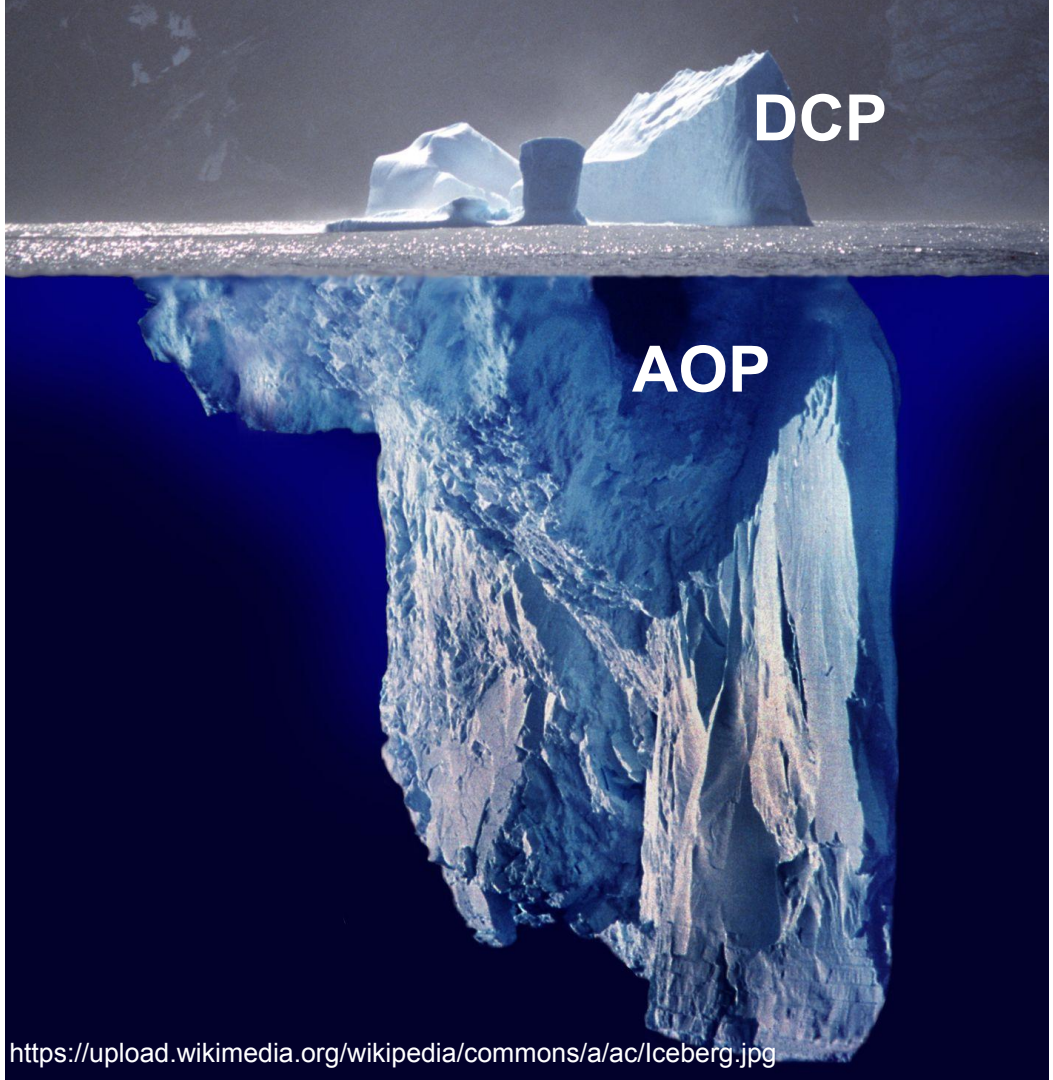
Sounds like it would need, a 2d array?

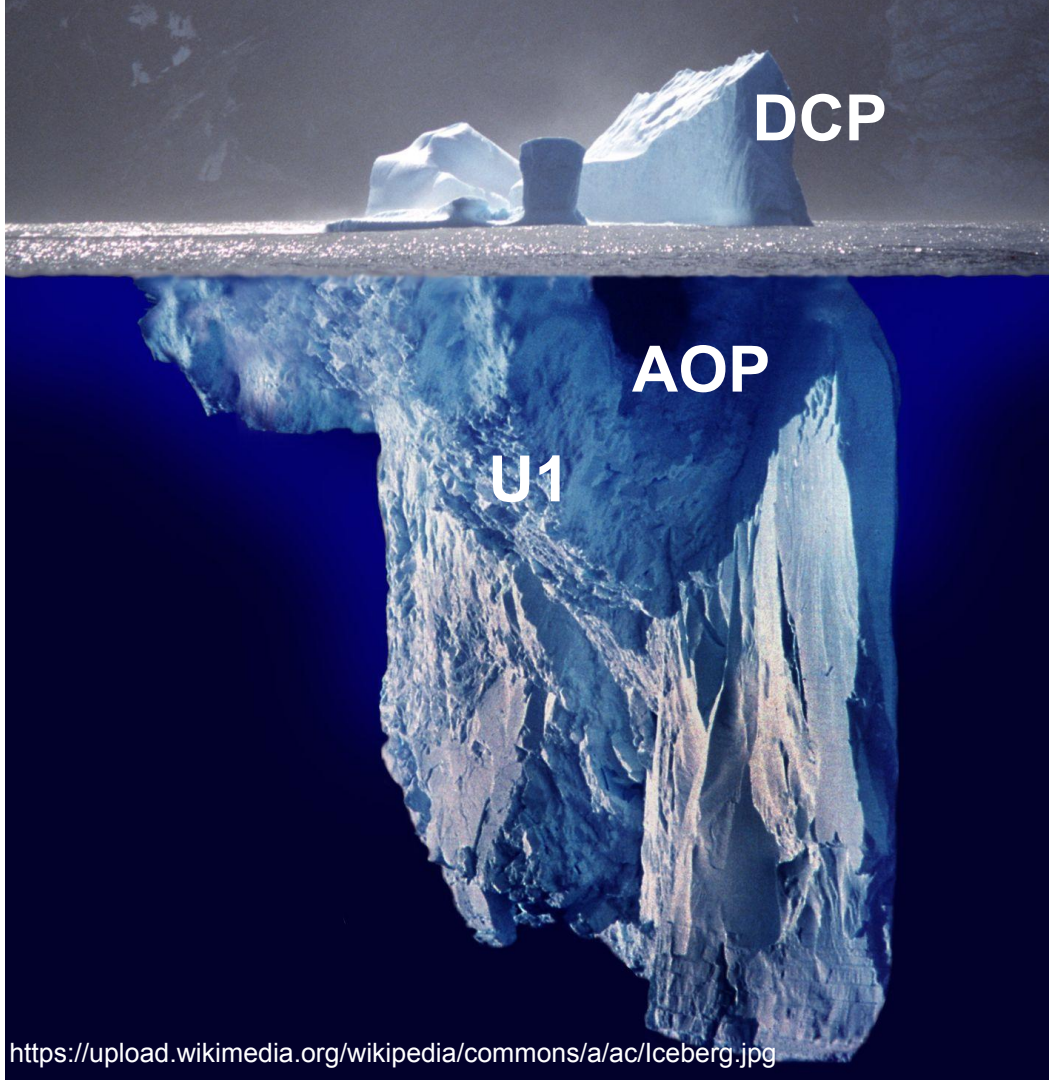
```
uint8_t* pages = compensator->inline_buffer; // +0x24
for (int pg_cnt = 0; pg_cnt < 3; pg_cnt++) {
  uint8_t* this_page = pages;
  for (int i = 0; i < controlled_size; i++) {
    memcpy(this_page,
           indirect_buffer_ptr,
           4 * controlled_size);
    indirect_buffer_ptr += 4 * controlled_size;
    this_page += 0x100;
  }
  pages += 0x4000;
}
```

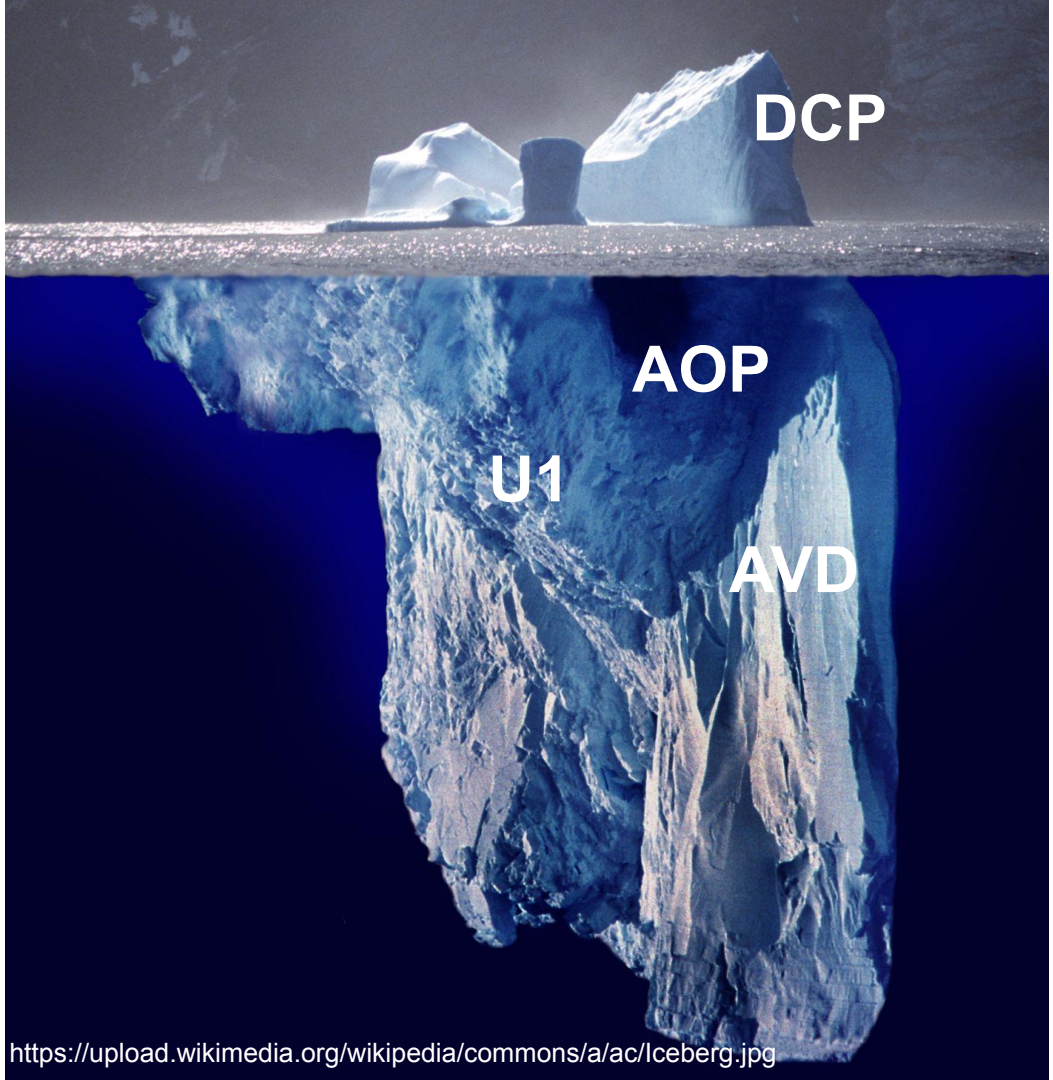
Not necessarily new bugs; just much easier exploits

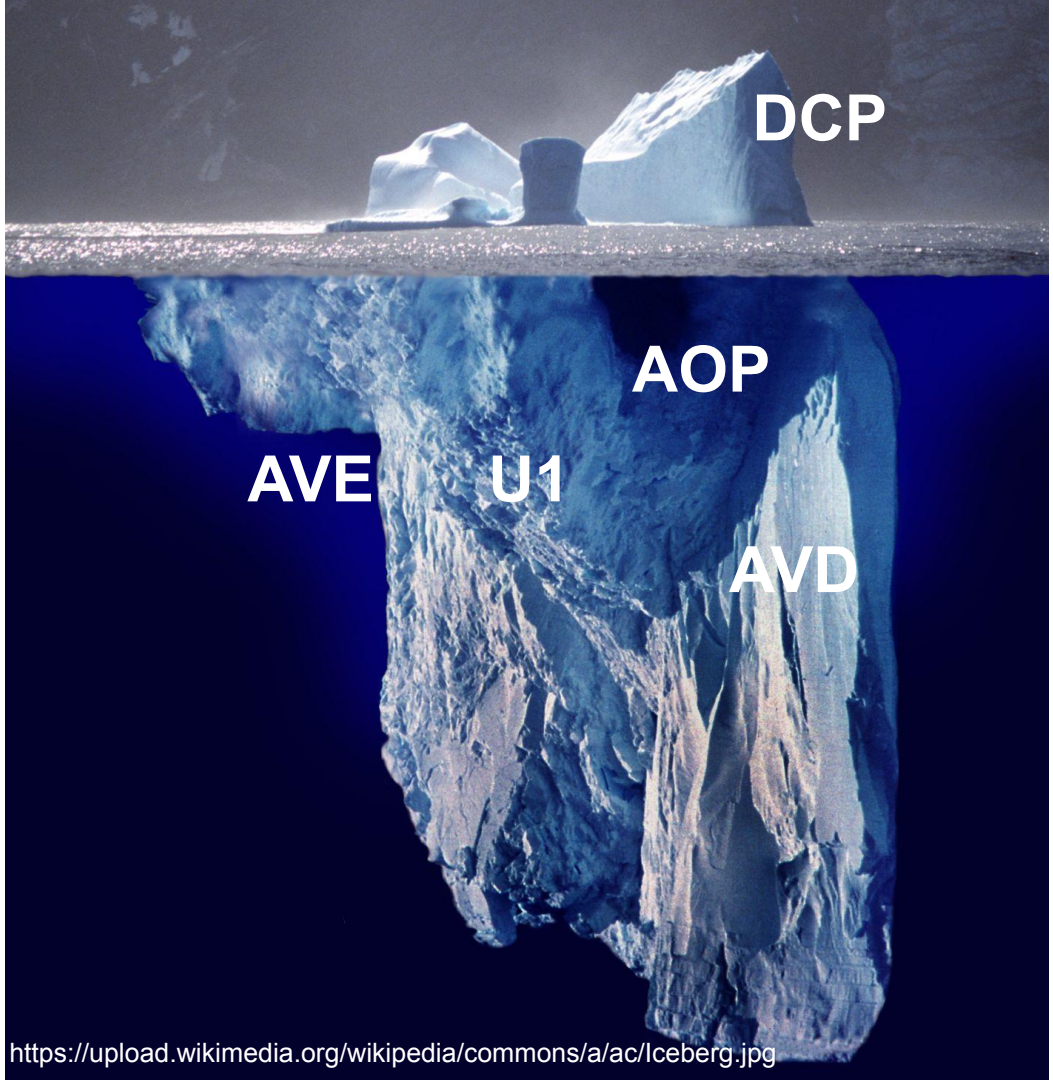


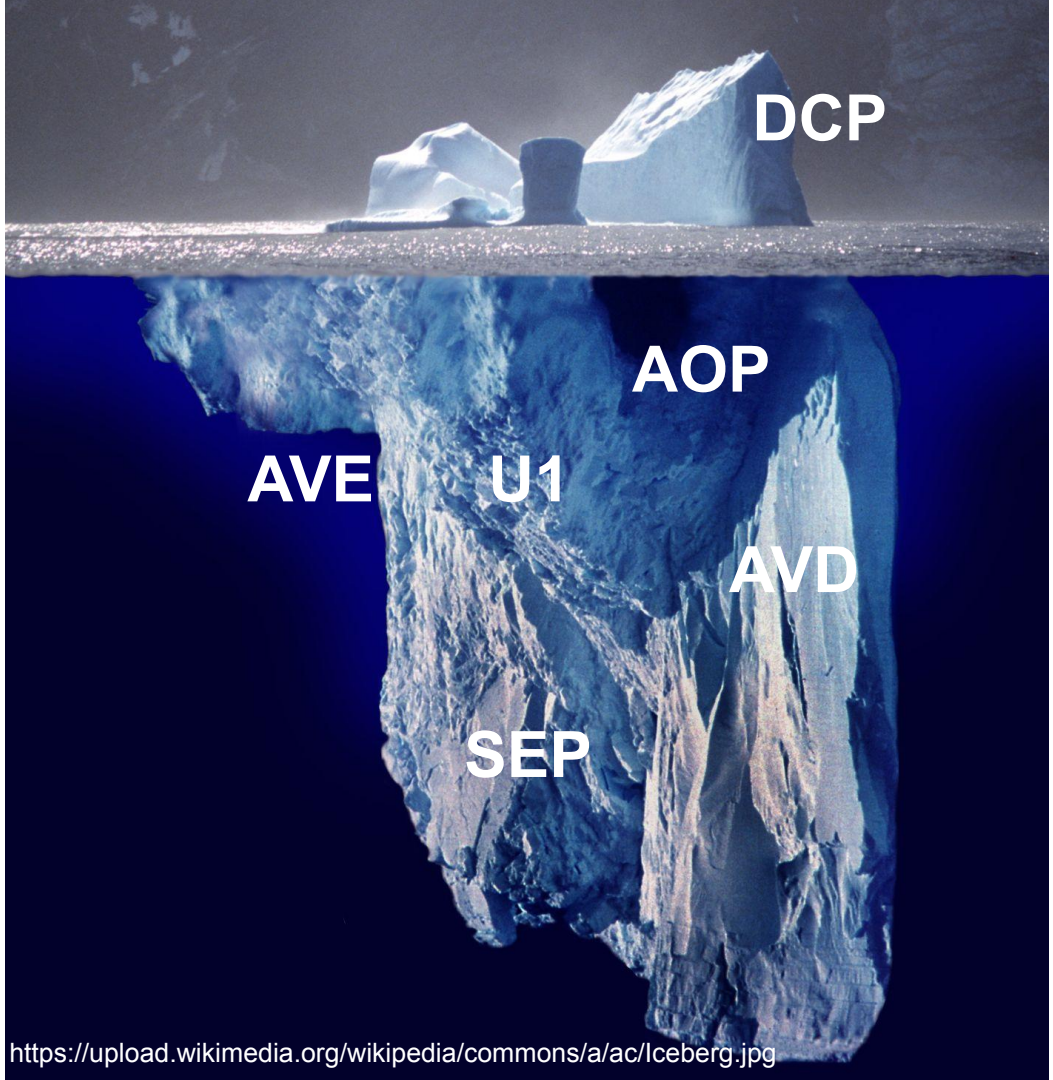
https://upload.wikimedia.org/wikipedia/commons/a/ac/Iceberg.jpg

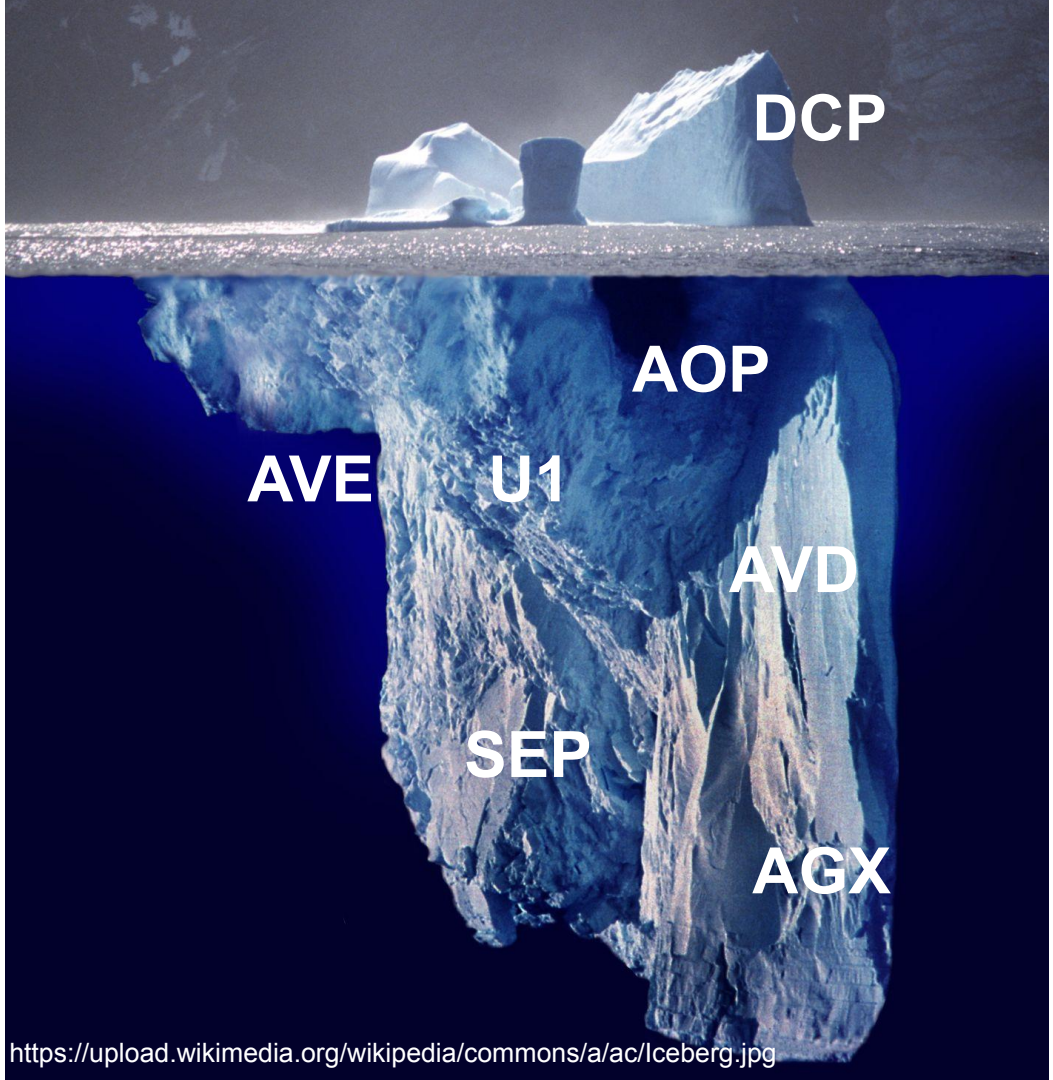

DCP
AOP
https://upload.wikimedia.org/wikipedia/commons/a/ac/Iceberg.jpg

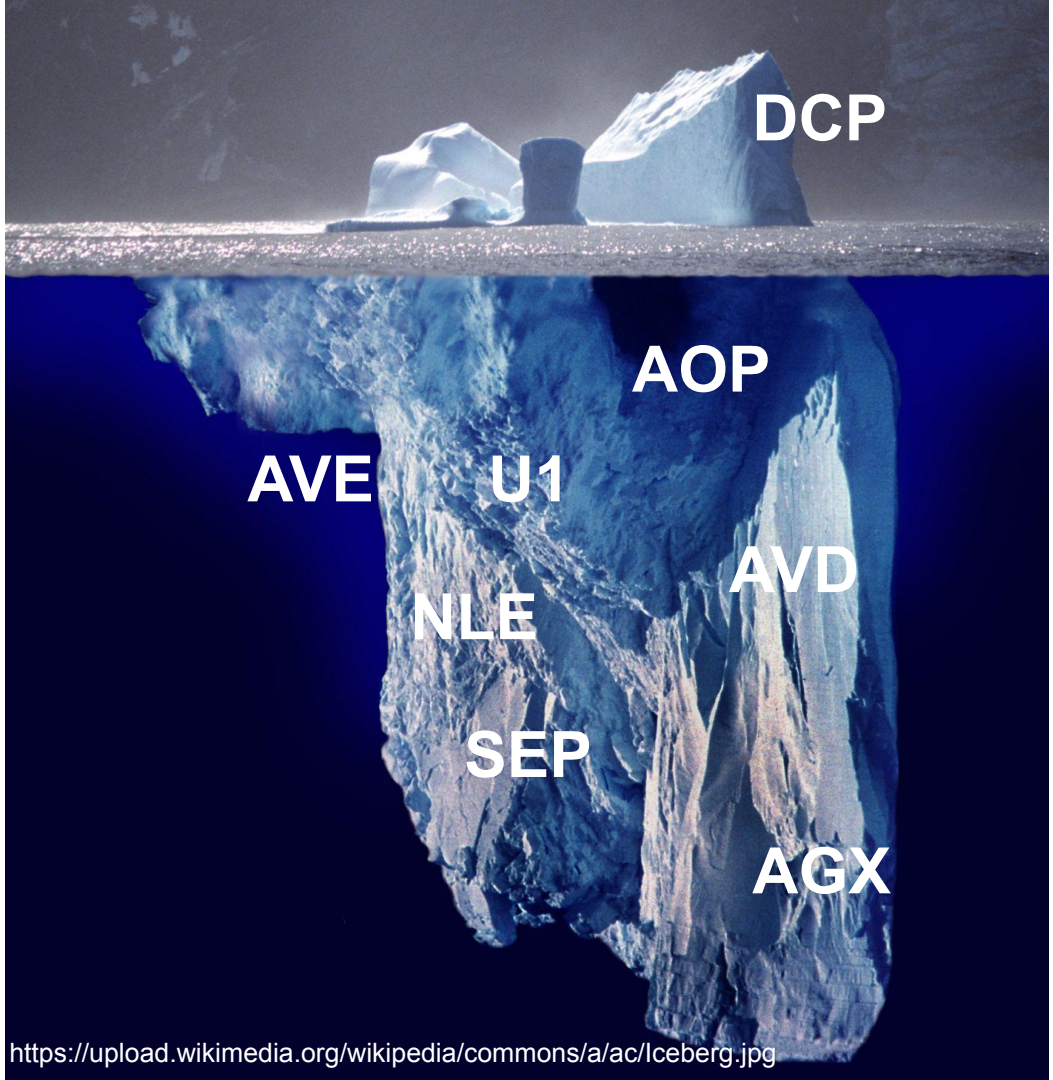

DCP
AOP
U1
https://upload.wikimedia.org/wikipedia/commons/a/ac/Iceberg.jpg


DCP
AOP
U1
AVD
https://upload.wikimedia.org/wikipedia/commons/a/ac/Iceberg.jpg

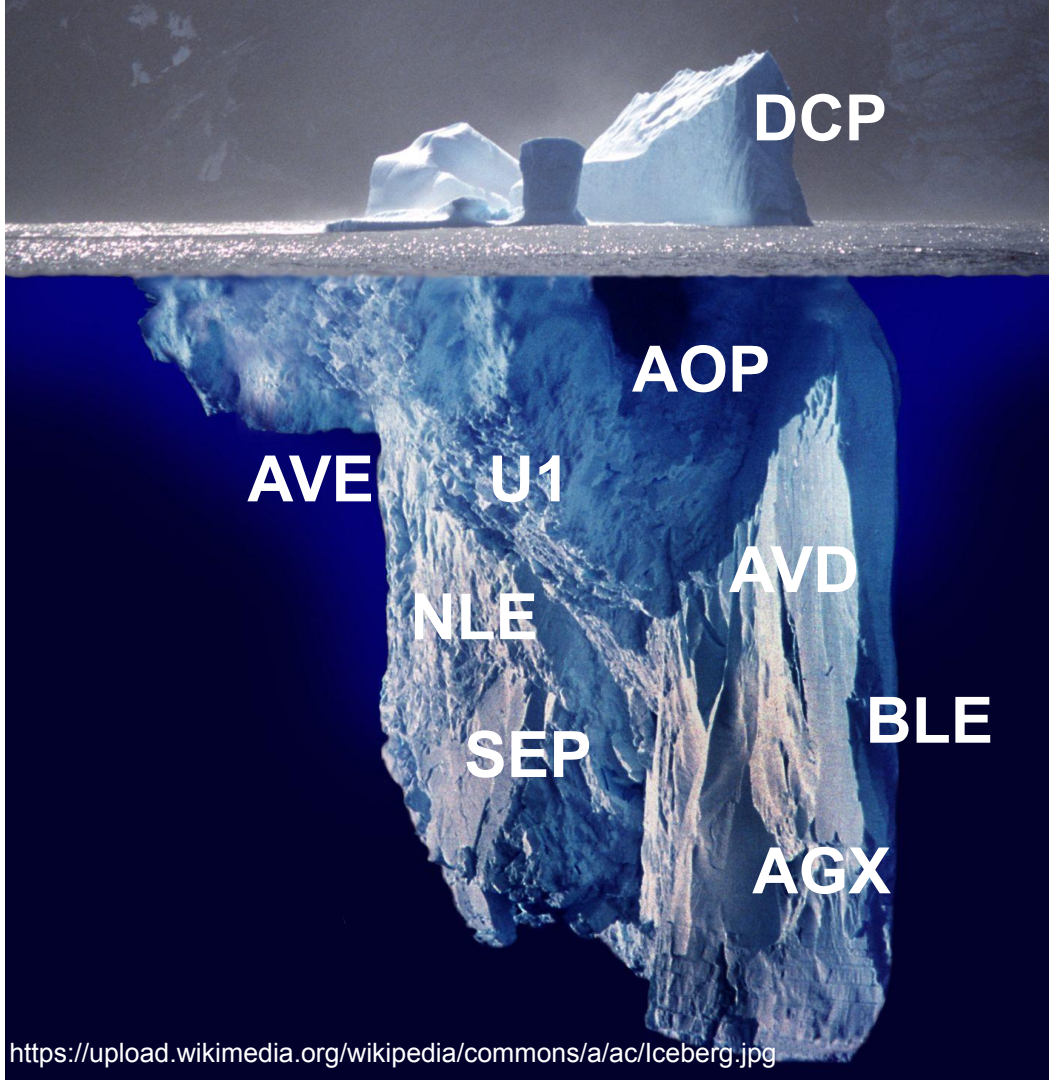

DCP
AOP
AVE
U1
AVD
https://upload.wikimedia.org/wikipedia/commons/a/ac/Iceberg.jpg

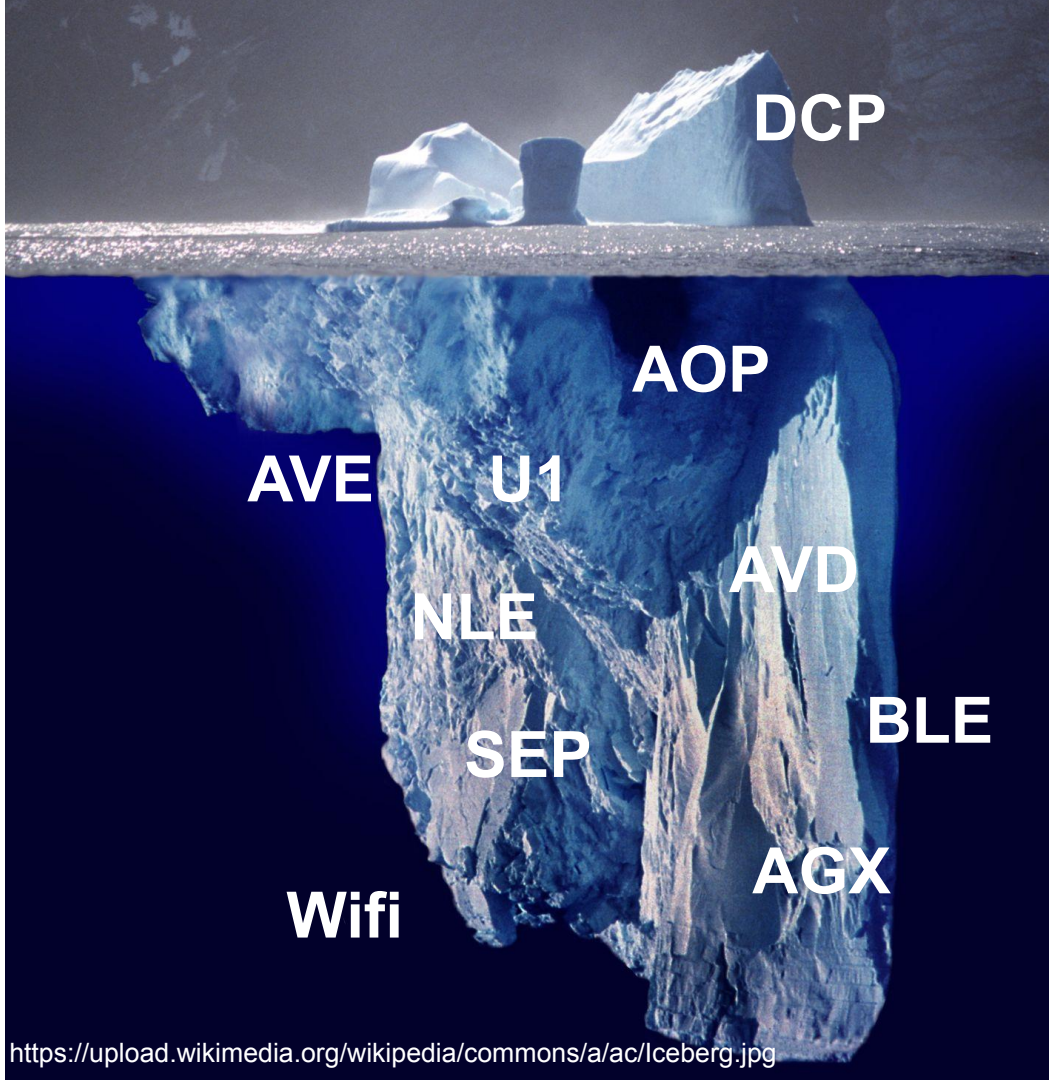

DCP
AOP
AVE
U1
AVD
SEP
https://upload.wikimedia.org/wikipedia/commons/a/ac/Iceberg.jpg


DCP
AOP
AVE
U1
AVD
SEP
AGX
https://upload.wikimedia.org/wikipedia/commons/a/ac/Iceberg.jpg

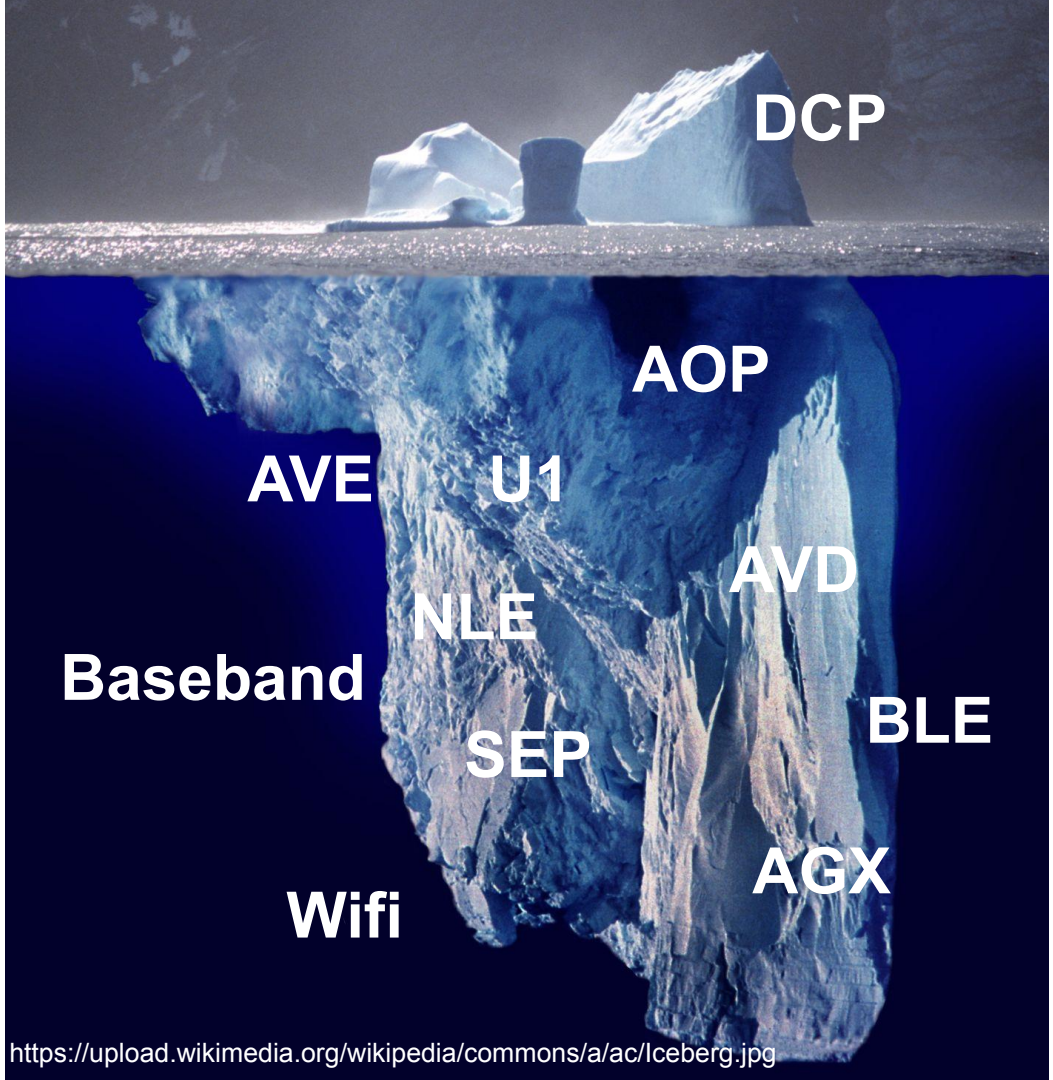


https://upload.wikimedia.org/wikipedia/commons/a/ac/Iceberg.jpg


DCP
AOP
AVE
U1
AVD
NLE
BLE
SEP
AGX
https://upload.wikimedia.org/wikipedia/commons/a/ac/Iceberg.jpg



https://upload.wikimedia.org/wikipedia/commons/a/ac/Iceberg.jpg


DCP
AOP
AVE
U1
AVD
NLE
Baseband
BLE
SEP
AGX
Wifi
https://upload.wikimedia.org/wikipedia/commons/a/ac/Iceberg.jpg

References:

Asahi Linux: https://asahilinux.org/2021/08/progress-report-august-2021/

TAG blog post: https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/

P0 blog post: https://googleprojectzero.blogspot.com/2022/06/curious-case-carrier-app.html

CVE-2020-9907: https://i.blackhat.com/eu-20/Thursday/eu-20-Hu-Story-Of-Jailbreaking-IOS-13-wp.pdf

CVE-2018-4344: https://github.com/Synacktiv-contrib/lightspeed/blob/master/lightspeed.c

CVE-2019-8605: https://googleprojectzero.blogspot.com/2019/12/sockpuppet-walkthrough-of-kernel.html

CVE-2020-3837: https://github.com/jakeajames/time_waste

CVE-2021-30883: https://saaramar.github.io/IOMFB_integer_overflow_poc/