ZIMPERIUM®

Treble or Trouble

Where Android's latest security enhancements help, and where they fail

Tamir Zahavi-Brunner
@tamir_zb

BSIDES LAS VEGAS

$ whoami

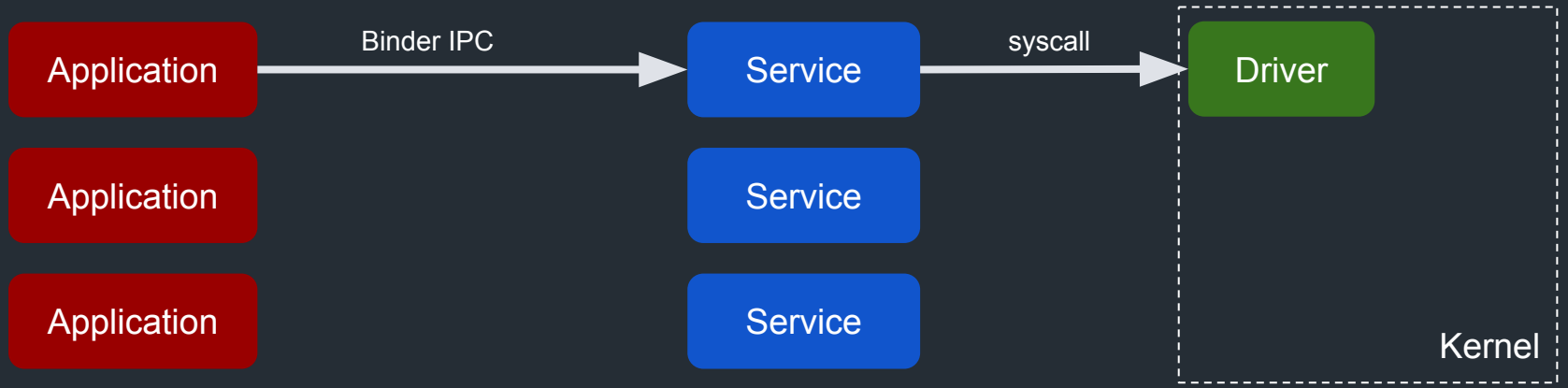
- Tamir Zahavi-Brunner (@tamir_zb)
- Security Researcher at Zimperium
- Focusing on Android research
- Previously: Reversing Linux & proprietary embedded systems

Security Enhancements

Security enhancements

- Human-written code is prone to bugs
- Security enhancements are introduced as an extra line of defense
  - ASLR
  - NX bit
  - Stack canary
  - Many more…
- This approach is well used in Android
  - Best example: SELinux

SELinux in Android



Stagefright

- Series of bugs reported in 2015 by Joshua Drake from Zimperium
- Attack vector is extremely dangerous
- Remote compromise via media file
- Compromised MediaServer process is **very** high privileged

https://www.blackhat.com/docs/us-15/materials/us-15-Drake-Stagefright-Scary-Code-In-The-Heart-Of-Android.pdf

Parsing media files is hard

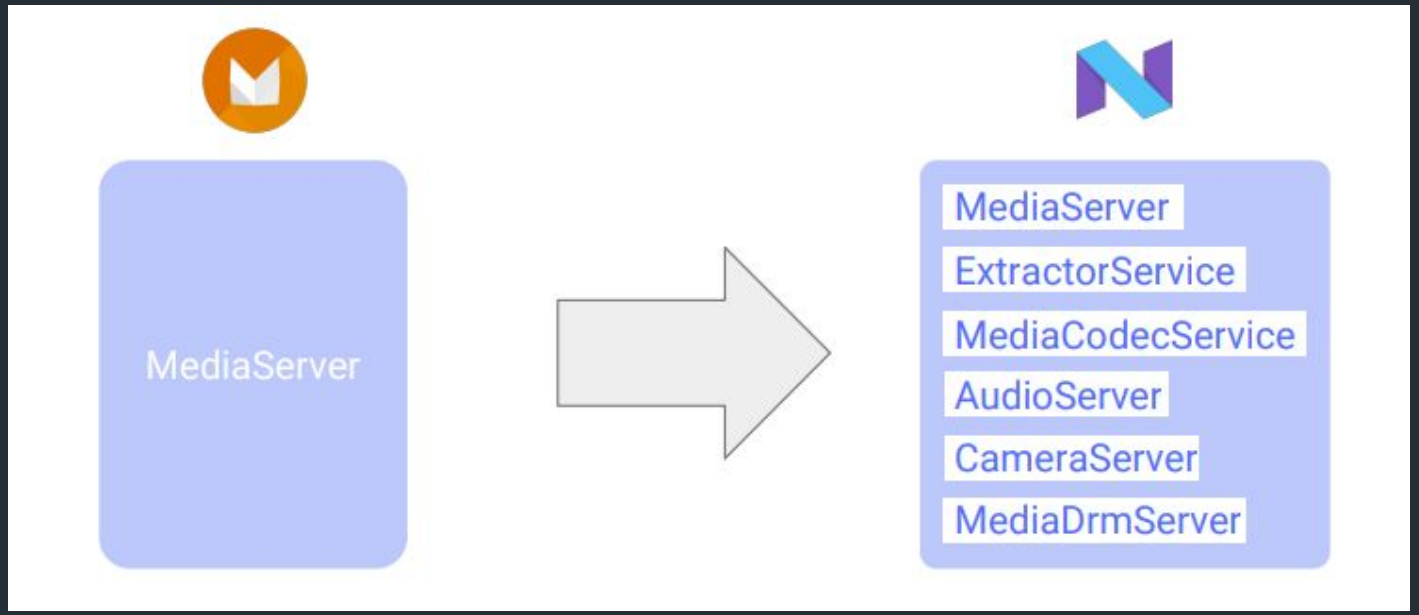
Media framework

The most severe vulnerability in this section could enable a remote attacker using a specially crafted file to execute arbitrary code within the context of a privileged process.

CVE	References	Type	Severity	Updated AOSP versions
CVE-2017-13248	A-70349612	RCE	Critical	6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0, 8.1
CVE-2017-13249	A-70399408	RCE	Critical	6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0, 8.1
CVE-2017-13250	A-71375536	RCE	Critical	6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0, 8.1
CVE-2017-13251	A-69269702	EoP	Critical	6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0, 8.1

https://source.android.com/security/bulletin/2018-03-01

MediaServer hardening in Android Nougat

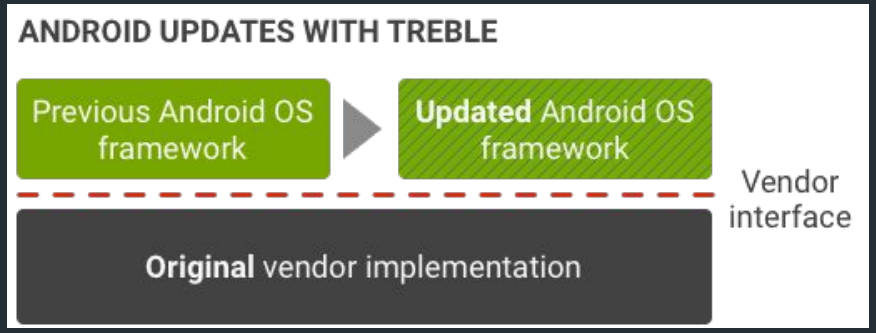


https://www.blackhat.com/docs/us-17/thursday/us-17-Kralevich-Honey-I-Shrunk-The-Attack-Surface-Adventures-In-Android-Security-Hardening.pdf

Project Treble

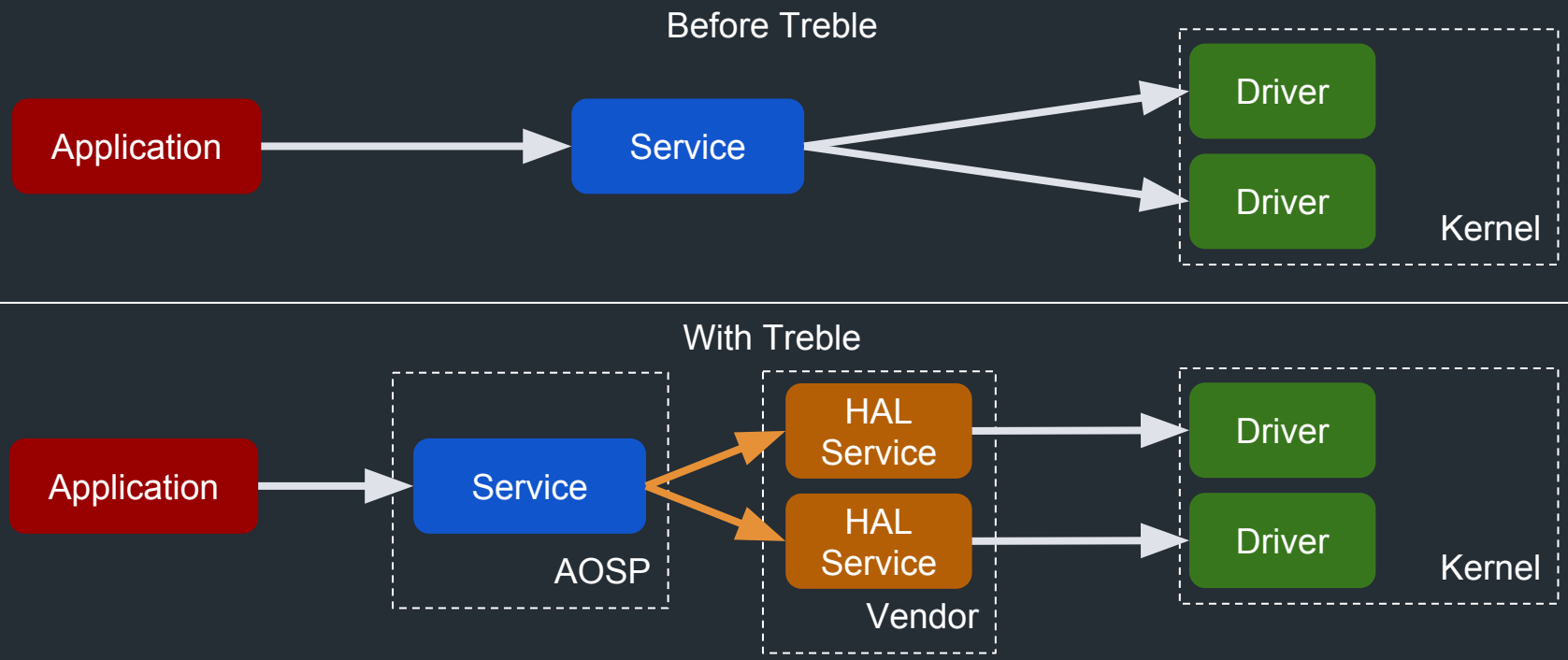
Project Treble

- Large re-architect of Android introduced in Android Oreo
- Main objective is to separate vendor code from AOSP code



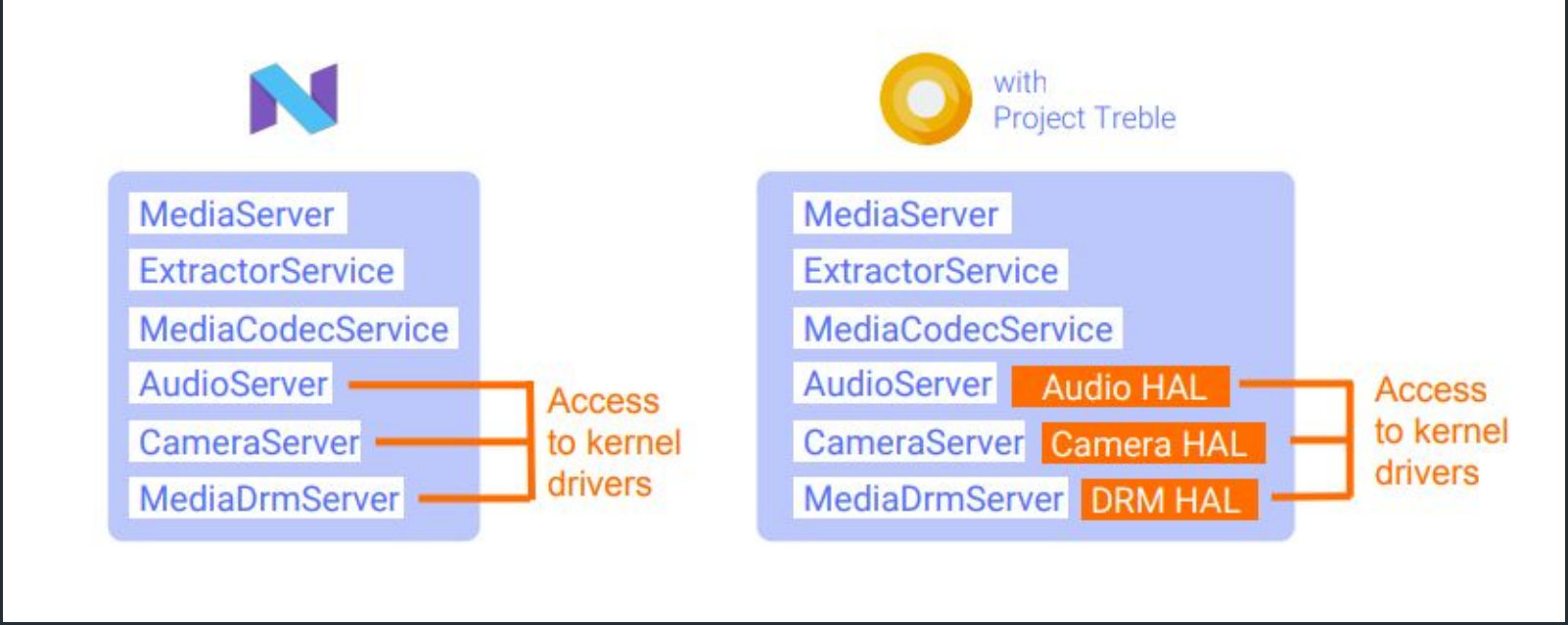
- Also described by Google as a security enhancement

Project Treble as a security enhancement



https://android-developers.googleblog.com/2017/07/shut-hal-up.html

Project Treble as a security enhancement

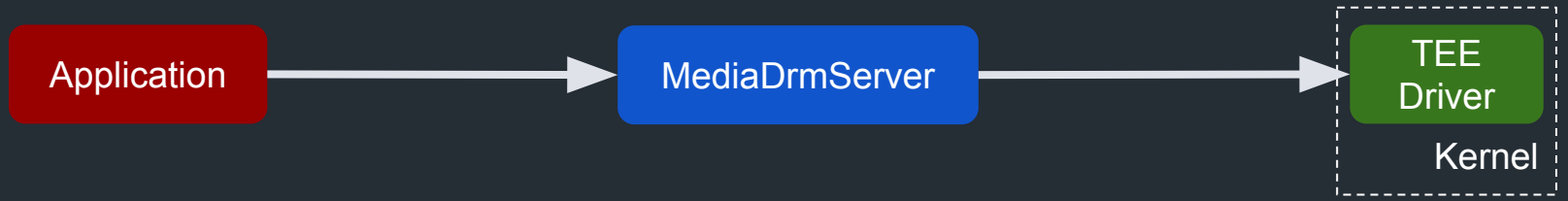


https://www.blackhat.com/docs/us-17/thursday/us-17-Kralevich-Honey-I-Shrunk-The-Attack-Surface-Adventures-In-Android-Security-Hardening.pdf

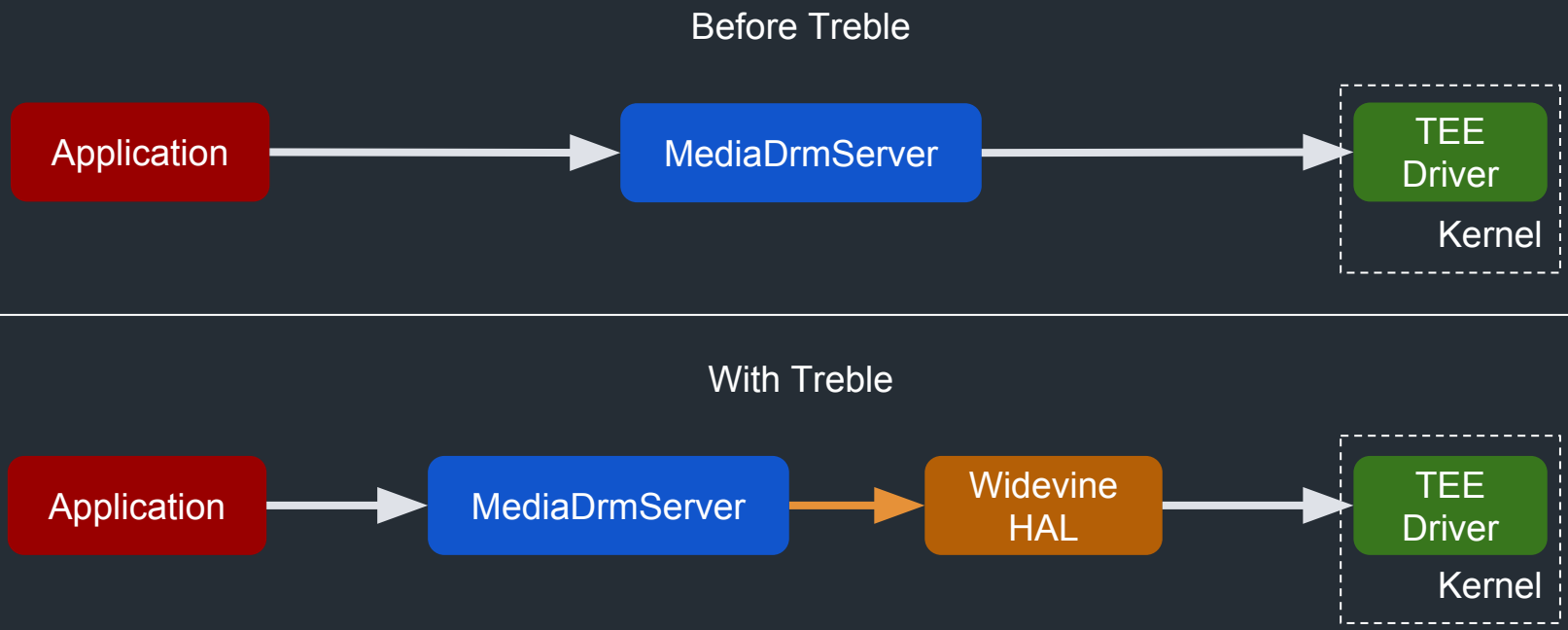
The vulnerability

MediaDrmServer

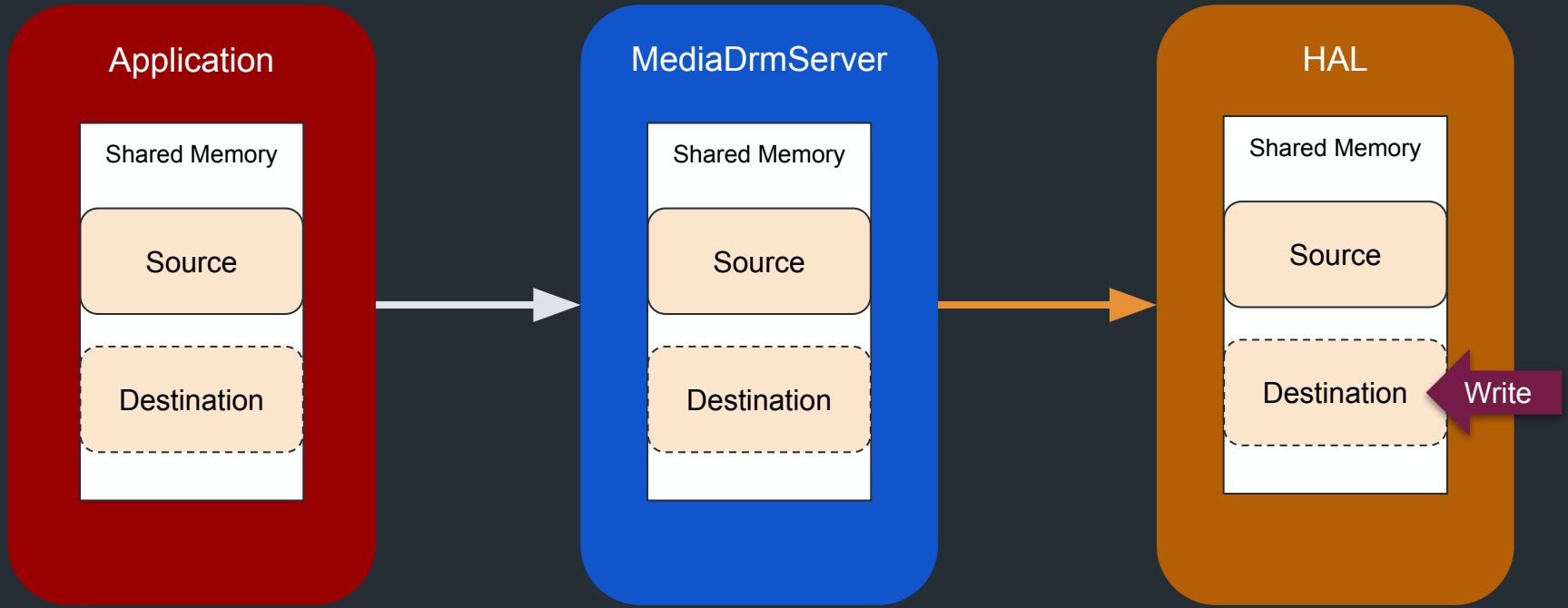
- In charge of decrypting DRM media
- Has access to the TEE driver



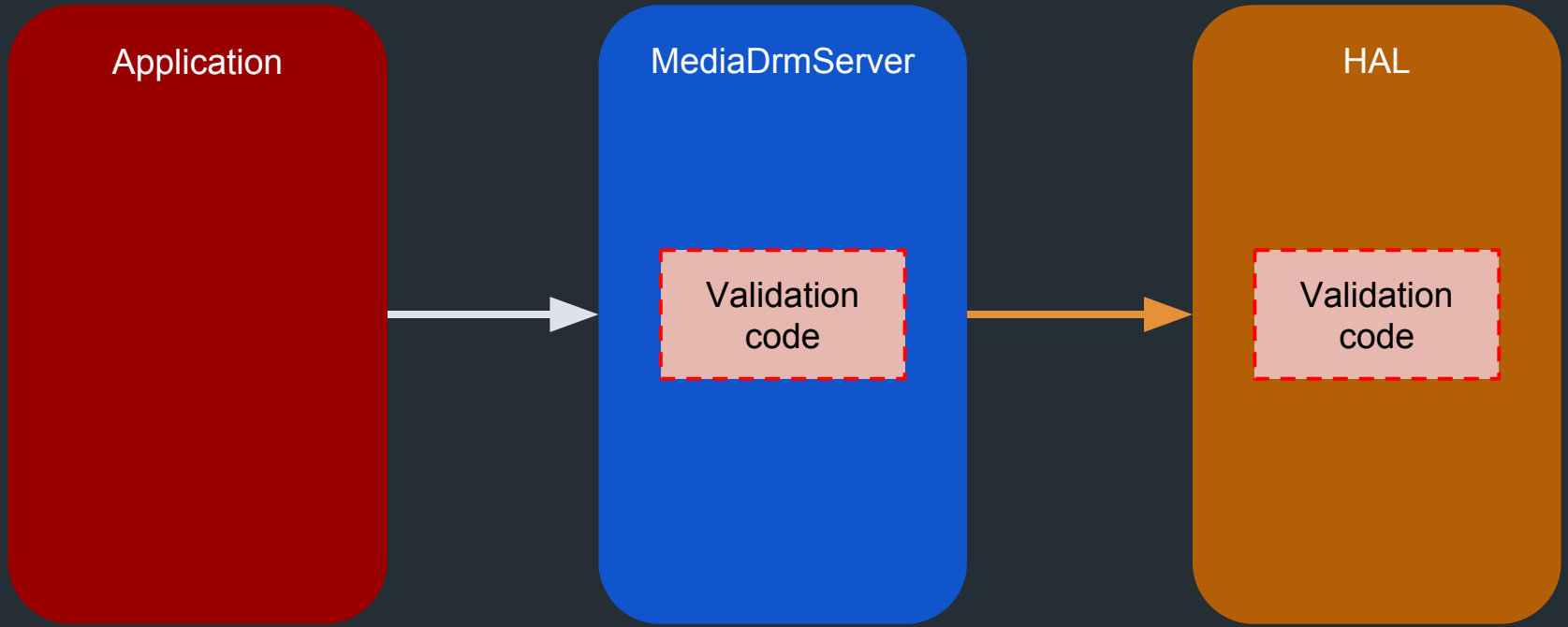
MediaDrmServer refactoring



MediaDrmServer's decrypt method



MediaDrmServer’s decrypt method



The bug - CVE-2017-13253

MediaDrmServer

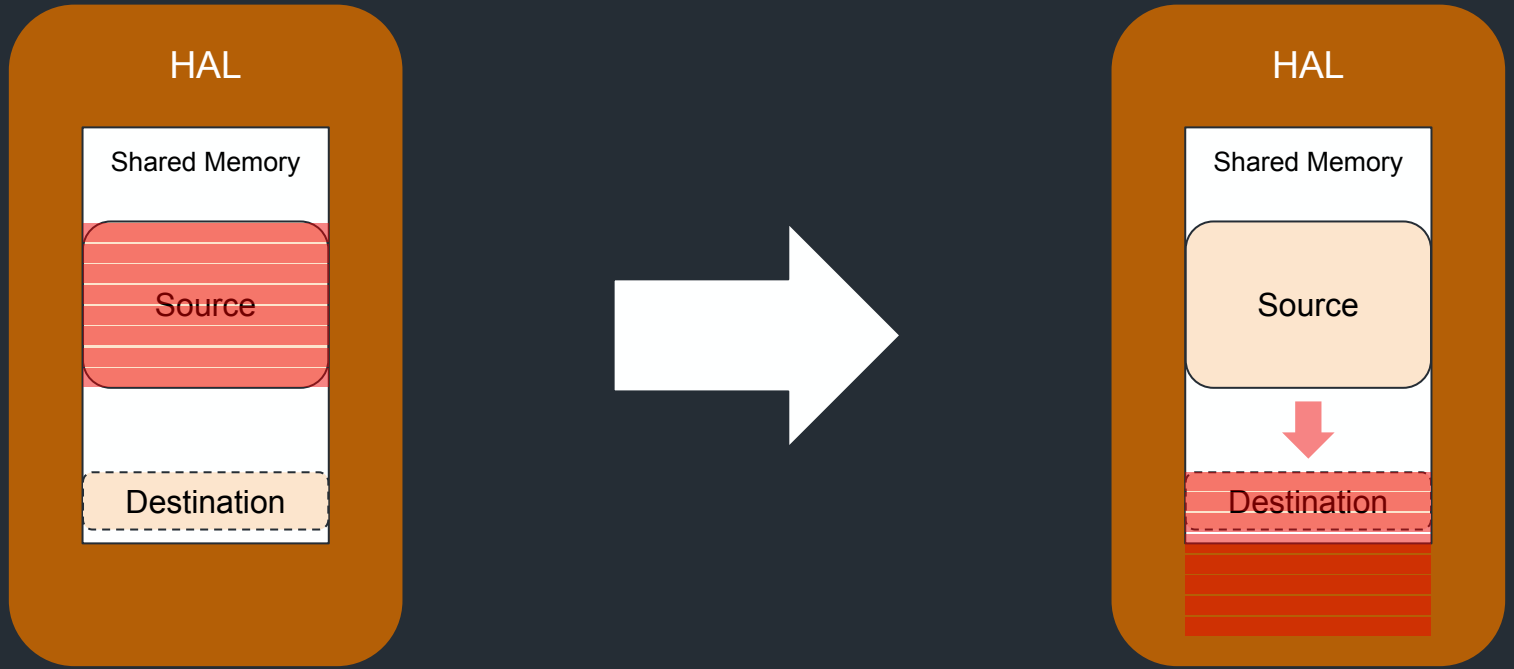
```
if (overflow || sumSubsampleSizes != totalSize) {
    result = -EINVAL;
} else if (totalSize > source.mSharedMemory->size()) {
    result = -EINVAL;
} else if ((size_t)offset > source.mSharedMemory->size() - totalSize) {
    result = -EINVAL;
```

frameworks/av/drm/libmediadrm/ICrypto.cpp

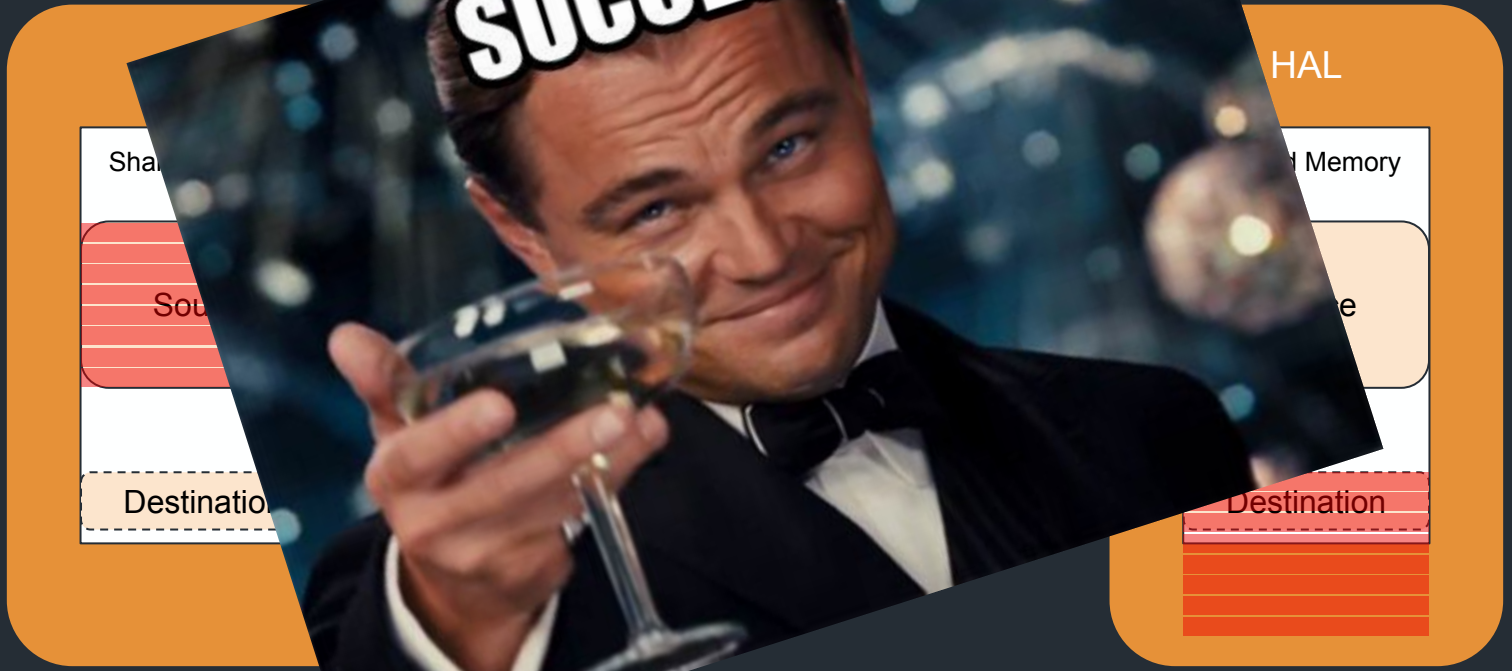
Checks that the data size (`totalSize`) fits into the source buffer on the shared memory (`source.mSharedMemory`).

There's no similar check for the destination buffer!

Buffer overflow



Buffer overflow



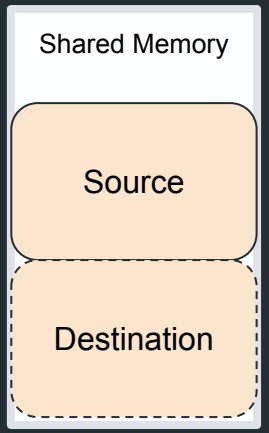
Project Treble & the vulnerability

The effect of Project Treble's refactoring

Before Treble

Output overwrites the input

With Treble



Input & output are separated

The vulnerability would not exist without Project Treble!

Other issues in MediaDrmServer’s refactoring

- Use of uninitialized value (CVE-2017-13252)
- Multiple memory leaks
- Multiple null dereferences
- Redundant code
- Seriously, LOTS of redundant code

Did this code receive enough attention?

MediaDrmServer is just an example

- CVE-2017-13209 - Gal Beniamini
- CVE-2017-13231 - Mingjian Zhou (周明建)
- CVE-2018-9344 - Mingjian Zhou (周明建)
- CVE-2018-9411 - me

All caused by Project Treble’s refactoring

Conclusion

- Project Treble can be a good security enhancement

BUT

Its implementation so far isn’t the best

- When adding new security enhancements, it is important not to neglect their implementation

Thanks

- Sneha Rajguru (@Sneharajguru)
- Rani Idan (@raniXCH)
- Ziggy (@z4ziggy)
- Adam Donenfeld (@doadam)
- Ori Karliner

References

- https://blog.zimperium.com/cve-2017-13253-buffer-overflow-multiple-android-drm-services/
- https://github.com/tamirzb/CVE-2017-13253

Thank you!

Questions?