



Ramdump for Trusted VMs

Efficient Crash Debugging
Without Rebooting The Device

Cong Zhang

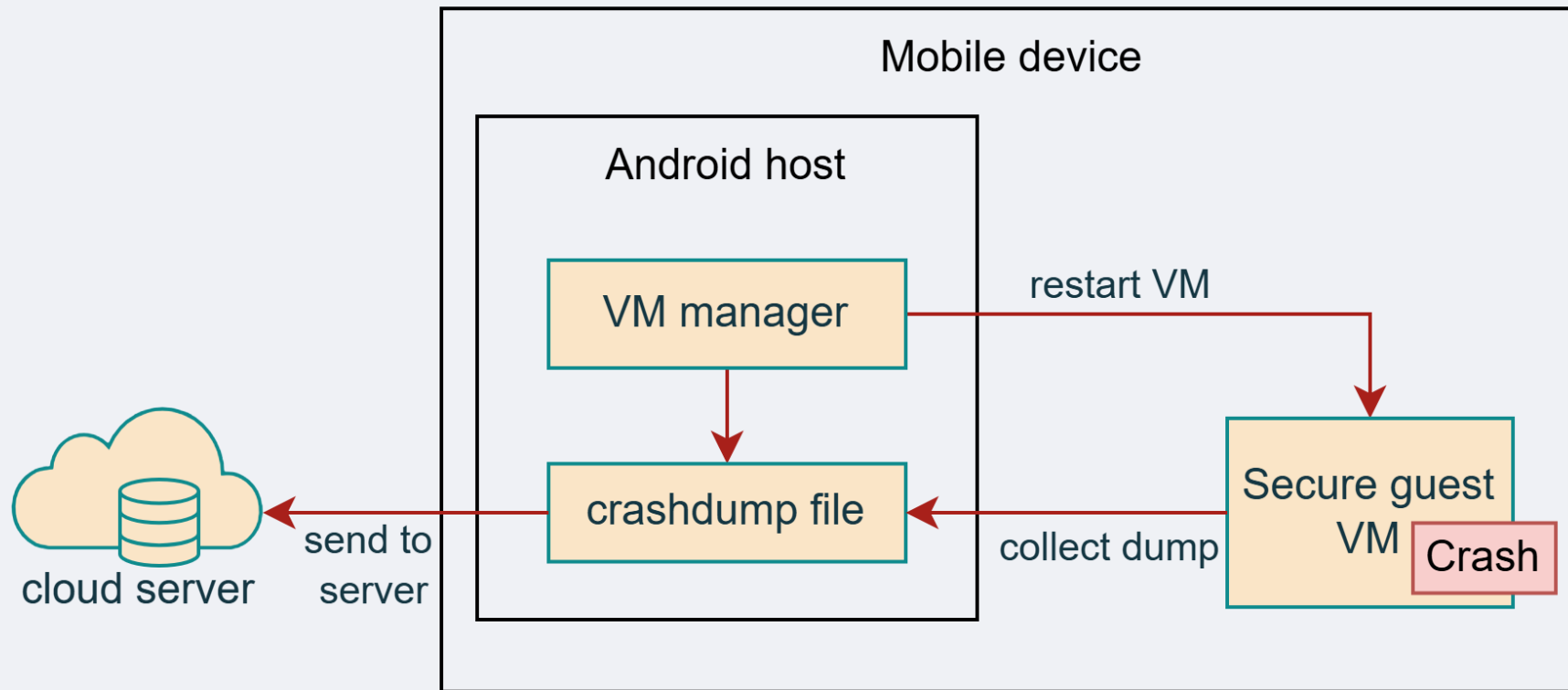
cong.zhang@oss.qualcomm.com
Qualcomm CSE Linux kernel team

Snapdragon and Qualcomm branded products are products of Qualcomm Technologies, Inc. and/or its subsidiaries.
Qualcomm patented technologies are licensed by Qualcomm Incorporated.



Background

Crash handling workflow for Secure Guest VM in Android Host VM

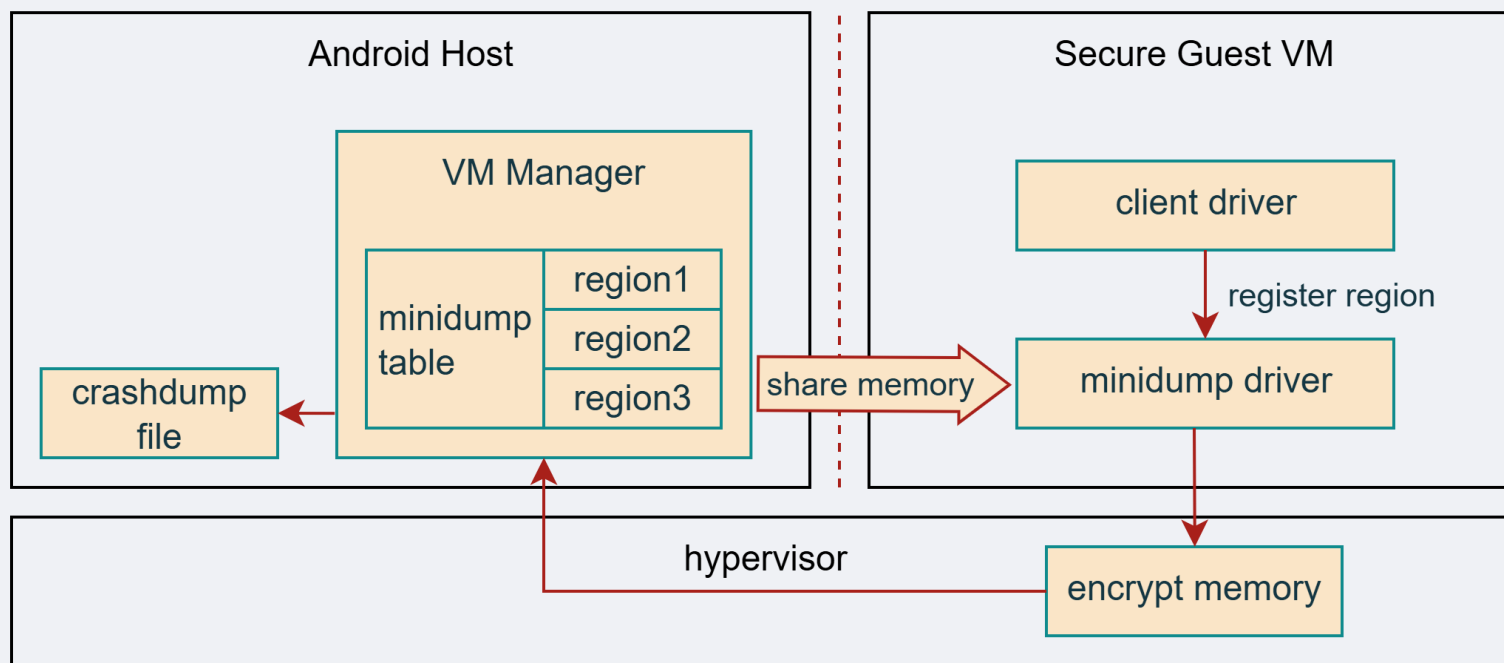


Problem

- Guest VM memory is isolated from the host and contains sensitive data, so leakage must be prevented.
- A full crash dump can be very large, especially when there are many devices and crash instances. This requires significant storage and makes cloud upload difficult.
- Secure guest VM reboot should be fast, and crash dump collection cannot cause long delays.

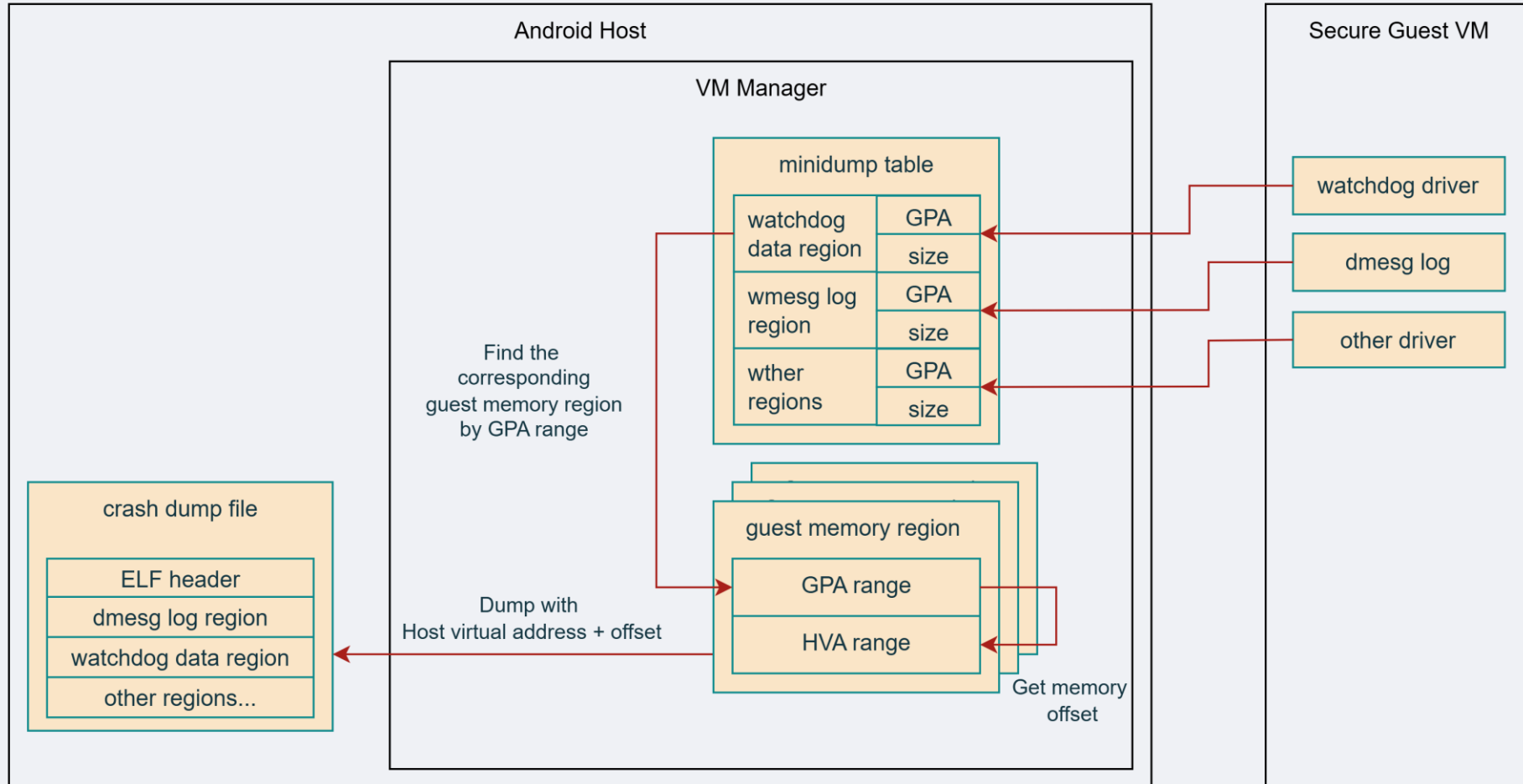
Design

- Collect only critical areas.
- Gather data from the host side.
- Encrypt memory in the hypervisor.
- We call it “minidump.”
- Meminspect upstream is in progress and may follow this design after acceptance.



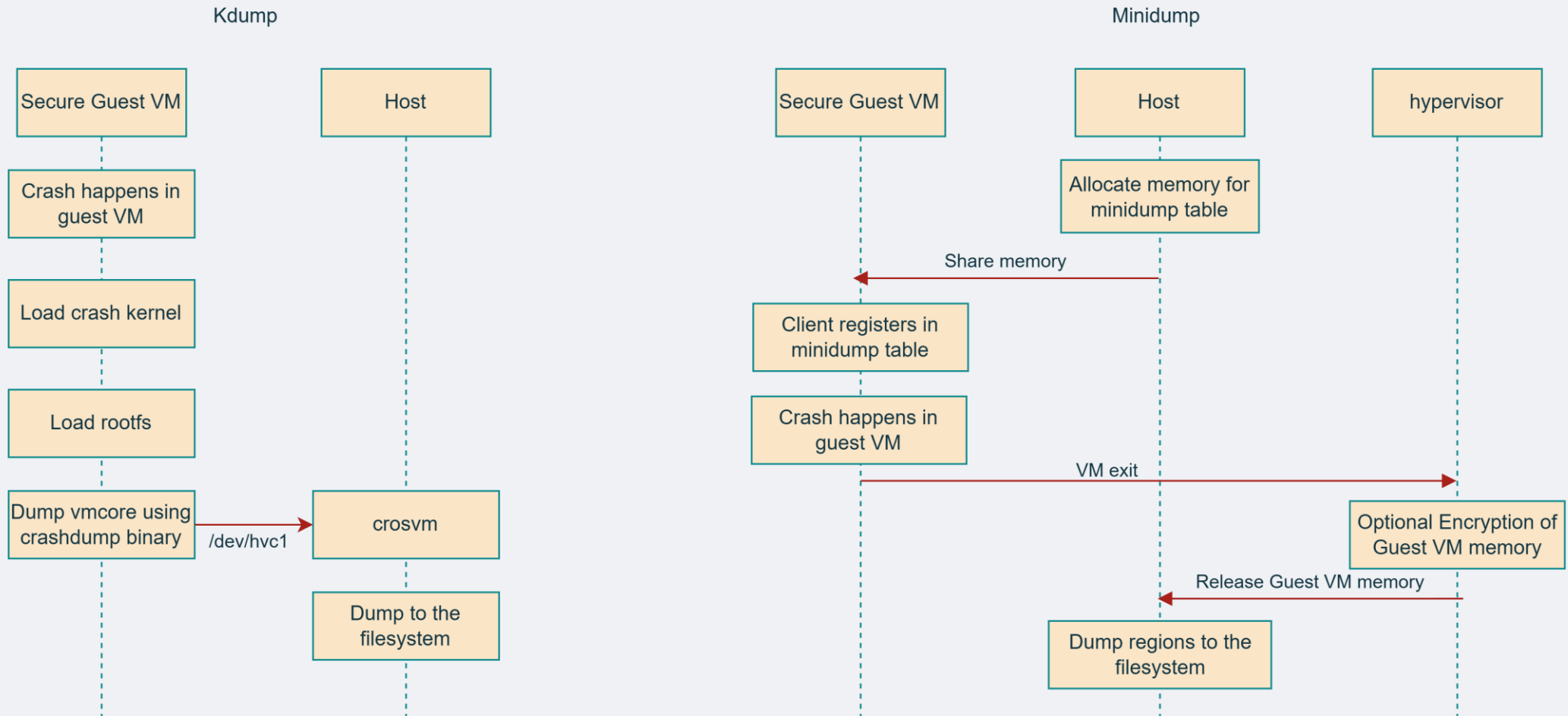
Design

How to get a specific region in the Android host?



Design

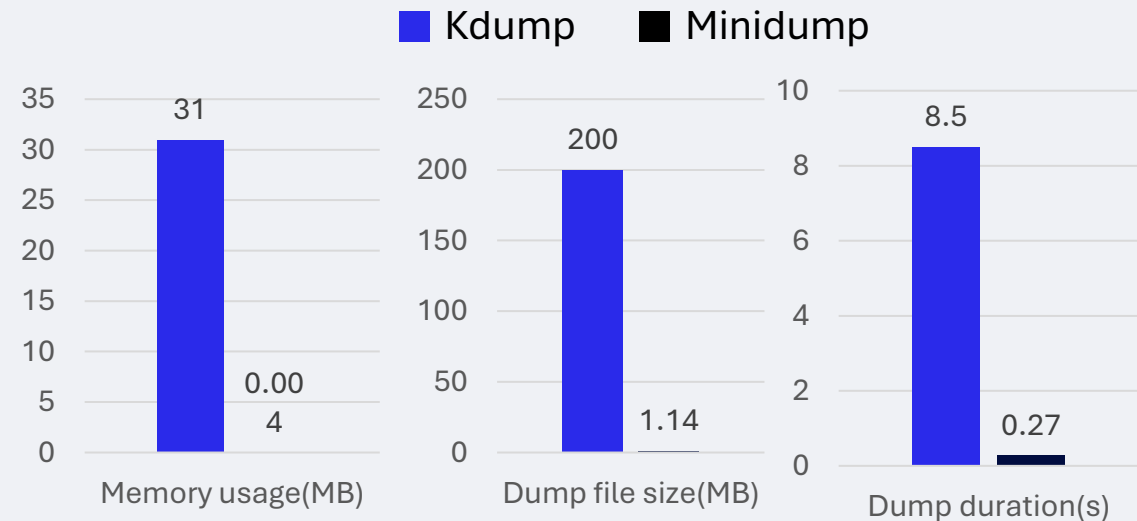
Comparison of minidump and kdump process



Comparison of kdump and minidump

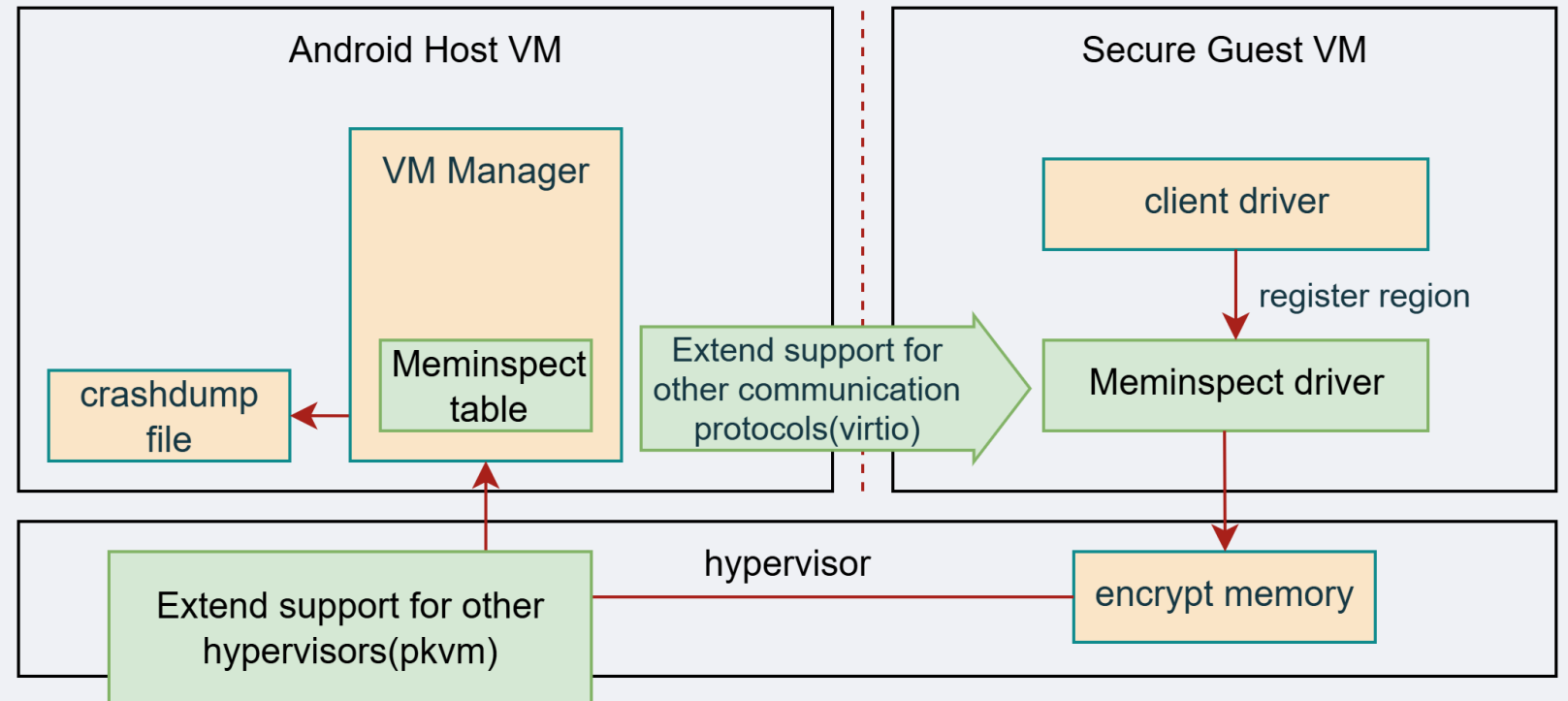
- Only critical memory regions
 - Smaller dump file size
- No crash kernel
 - Lower memory usage
 - Shorter dump duration
- Encrypt by hypervisor
 - More secure

	Kdump	Minidump
Dump file size	200 MB	1.14 MB
Memory usage	31 MB	4 KB
Dump duration	8.5 s	0.27 s



What's Next?

- Follow the meminspect design
- Extend support for
 - other communication protocols such as virtio
 - other hypervisors such as pkvm



Thank you

Nothing in these materials is an offer to sell any of the components or devices referenced herein.

© Qualcomm Technologies, Inc. and/or its affiliated companies. All Rights Reserved.

Qualcomm and Snapdragon are trademarks or registered trademarks of Qualcomm Incorporated. Other products and brand names may be trademarks or registered trademarks of their respective owners.

References in this presentation to “Qualcomm” may mean Qualcomm Incorporated, Qualcomm Technologies, Inc., and/or other subsidiaries or business units within the Qualcomm corporate structure, as applicable. Qualcomm Incorporated includes our licensing business, QTL, and the vast majority of our patent portfolio. Qualcomm Technologies, Inc., a subsidiary of Qualcomm Incorporated, operates, along with its subsidiaries, substantially all of our engineering, research and development functions, and substantially all of our products and services businesses, including our QCT semiconductor business.

Snapdragon and Qualcomm branded products are products of Qualcomm Technologies, Inc. and/or its subsidiaries. Qualcomm patented technologies are licensed by Qualcomm Incorporated.

Follow us on: [in](#) [X](#) [@](#) [v](#) [f](#)

For more information, visit us at qualcomm.com & qualcomm.com/blog

We are Hiring Linux Kernel Engineers

San Diego



tsoni@quicinc.com

Linux maintainers(remote)



ndechesn@quicinc.com

Hyderabad



China



QIPL

