Building a Commercial Virtualized Mobile Device with seL4

Part 3

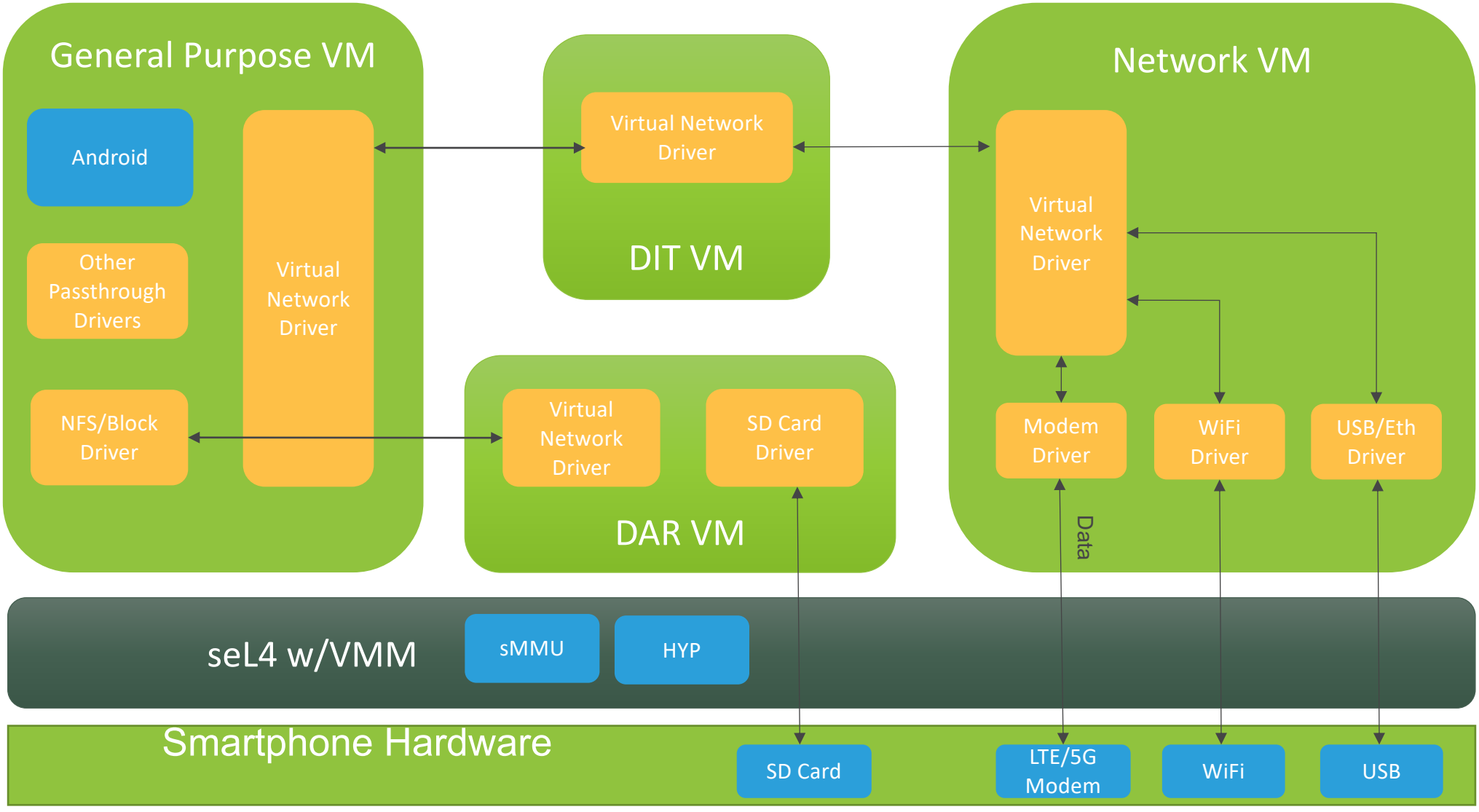
Jason Sebranek
CTO, Cog Systems

Why Part 3 ?

- Part 1 was a recorded presentation for the seL4 Summit in Nov 2020
  - Case study in applying seL4 to a product commercialization effort
- Part 2 was an update given at the 2023 Summit
  - Progress, but more blockers
- Wrapping this up
  - Moving forward without virtualization
- Quick update on progress, setbacks, challenges, lessons learned, and status

What Are We Trying To Accomplish ?

- Bring to market a commercial smartphone device, built around a Type-1 hypervisor and very small Trusted Computing Base (TCB)
- Use Commercial Off the Shelf (COTS) hardware and open-source software
- Place the seL4 microkernel and Virtual Machine Manager (VMM) at the heart of the system architecture
- Create Isolated VMs dedicated to
  - User Interface (Android)
  - Data at Rest (DAR) and Data in Transit (DIT) encryption
  - Managing networking and radios


General Purpose VM
Android
Other Passthrough Drivers
NFS/Block Driver
Virtual Network Driver
Virtual Network Driver
DIT VM
Network VM
Virtual Network Driver
Modem Driver
WiFi Driver
USB/Eth Driver
Data
Virtual Network Driver
SD Card Driver
DAR VM
seL4 w/VMM
sMMU
HYP
Smartphone Hardware
SD Card
LTE/5G Modem
WiFi
USB

Defining “Commercial”

- Who would use such a device?
  - Consumer – overkill, prohibitively expensive
  - Enterprise – Executives/Management, still expensive
  - Government – Security standards mandate use, expense can be borne

- US Government
  - Cog focuses on meeting demand and requirements for a market we know
  - DoD, Intel, Civilian use cases and security standards

- NSA’s Commercial Solutions for Classified (**CSfC**) enables the opportunity
  - Use off-the-shelf HW/SW components in a layered, risk-mitigated fashion
  - Allows for classified use of otherwise vulnerable devices

Market Challenges

- Overarching problem – Industry and Government are very different worlds
  - Models of operation are largely incompatible
  - Cog's mission has been to bridge the gap

- Industry
  - Dealing with millions, require a large Minimum Order Quantity (MoQ) to do anything special
  - Want to push new product upgrade every year, force EOL for old devices
  - Very reluctant to do yet another certification for a tiny market

- Government
  - Mostly deployments in the hundreds, some in the thousands
  - Very decentralized - multiple competing solutions, all tied to different contracts
  - Yearly funding cycles, often delayed and interrupted (*throw in an election!*)
  - Need to sustain solutions for many years before a refresh
  - Want fully baked, certified solutions, but won't commit to MoQ (*sometimes* NRE)

Where Have We Been ?

- Performed four successive R&D-focused contracts with USG on this topic
  - Currently executing two prototype -> productization efforts
- Established long-term Agreement and relationship with smartphone OEM
  - Access to third-party Qualcomm license
- Met R&D contract requirements, but fell short of productization readiness goals
- Experienced major challenges with Qualcomm platform
  - No more ability to alter the bootchain and run seL4 in EL2
  - Not a problem specific to seL4, but available resources and community matters
- Long term, sustainable virtualization solution still seems out of reach for now

Where Do We Go Now ?

- Gov desires a smartphone baseband which is isolated by virtualization
  - Still very elusive on smartphones
  - Need a short-term solution

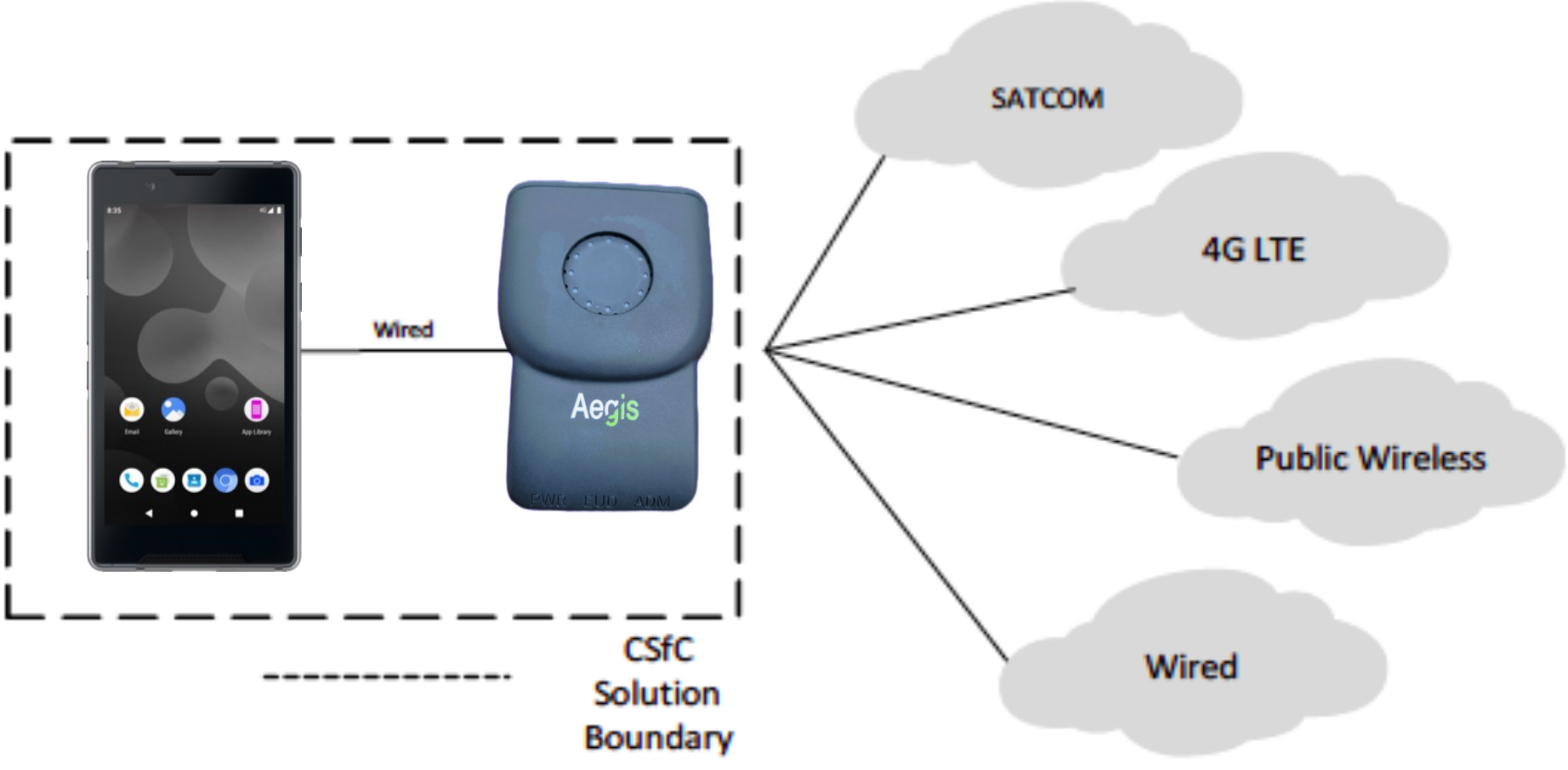
- Moved to a strategy of isolation by Hardware Separation/Isolation
  - Think of VMs as Physical Machines (PMs)
  - Create trustworthy PMs, dedicated to sensitive tasks

- In CSfC, this has manifested as a requirement for an Enhanced Retransmission Device (ERD)

- Pair a smartphone with an ERD when using an untrusted network
  - ERD is a physical standoff for the phone and uses its cellular/WiFi to make the connection
  - Phone user/policy must turn off its radios and physically tether to the ERD for traffic
  - Allows user's device to safely connect to untrusted Wide Area Networks (WiFi or LTE)


Aegis
PWR EUD ADM
Aegis
R51
Enhanced Retransmission Device (ERD)
Aegis

Cog Systems ERD – Aegis R51

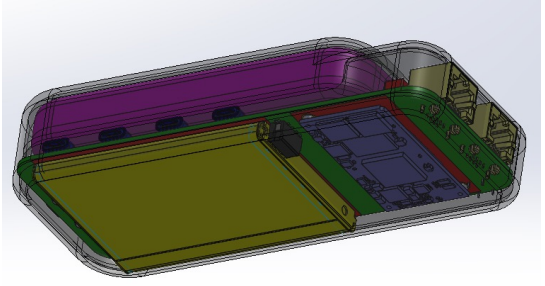


Decomposing the Problem

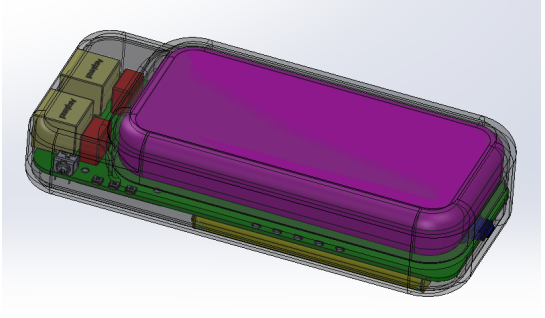
- Bumped the problem down one level of attack surface - could keep going
  - Turtles all the way down
- Early versions of Cog's ERD indeed were virtualized
  - Performance was poor on our chosen 4G hardware – 1 GB RAM
- Upgraded 4G to 5G hardware, way more RAM
  - Technique for getting seL4 into EL2 no longer valid

Next Version

- Next-gen ERD will also incorporate internal Hardware Separation
  - LAN and WAN facing chipsets, connected by a controlled USB bus
  - Remove Qualcomm dependency
- New and improved hardware gives us the option to re-visit virtualization on the new chipsets
- Perhaps makes more sense to just run seL4 with single OS on each chipset
  - Alternate use cases using spin-offs of this hardware configuration will really benefit



Aegis R52 ERD Prototype



Thank You

Questions ???

Feel free to drop me a note:

Jason Sebranek
jason@cog.systems