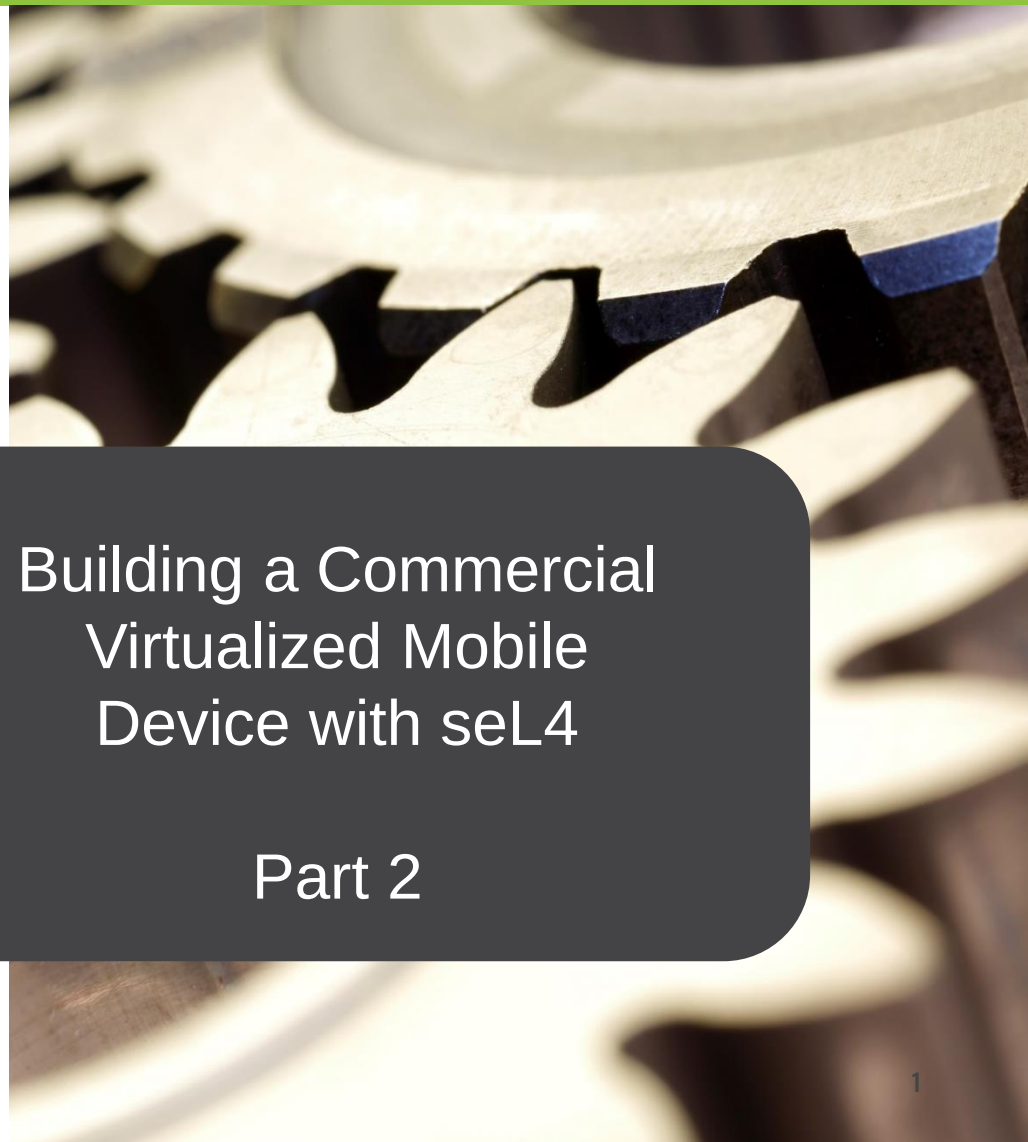


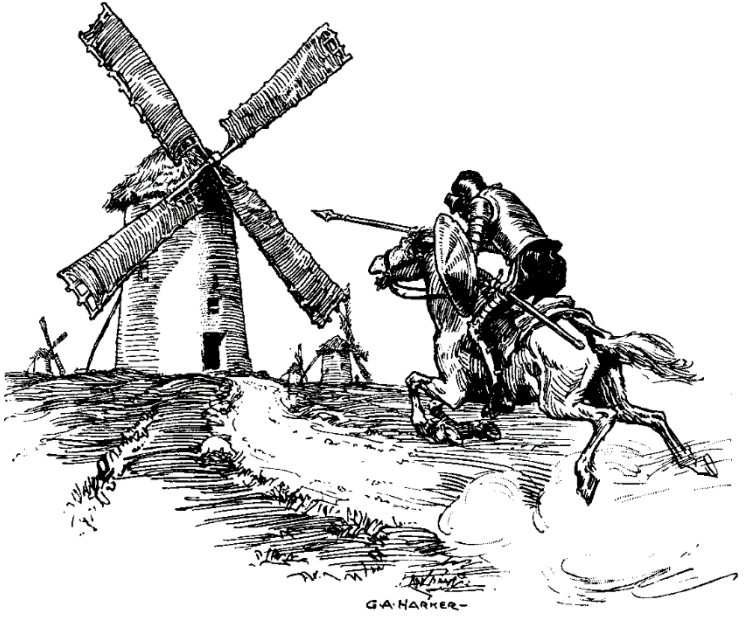
We Virtualize IoT

# Building a Commercial Virtualized Mobile Device with seL4

## Part 2

# Why Part 2 ?

- Part 1 was a recorded presentation for the seL4 Summit in Nov 2020
  - Case study in applying seL4 to a product commercialization effort
- It's been three years
  - A lot has changed, but a lot hasn't
- Quick update on progress, setbacks, challenges, lessons learned, and status



# What Are We Trying To Accomplish ?

- Bring to market an Ultra-Secure* mobile 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
- Provide the solution to customers with a need to protect sensitive/classified information

* **Allied Market Research Definition** - Ultra-secure smartphones are more secure than regular smartphones as they encrypt all communication and block unauthorized tracking systems. With these features, the privacy issue associated with android smartphones is resolved. Rise in customers' inclination toward ultra-secure smartphones fuels the adoption of ultra-secure smartphones. Further, increase in security threats and ongoing technological advancements provide the marketers immense scope to target their customers and enhance the user experience."

# Basic Principles

- Single Persona/Domain (Android) device on commercial smartphone hardware
- Leverage the approach of Modularization and Isolation by Virtualization.
- Vulnerable system components isolated from Android (WiFi, cell radio, storage).
- Intended for use in in Commercial Solutions for Classified (CSfC) solutions
  - Use pre-approved components from list of commercial HW/SW
- Approval via National Information Assurance Partnership (NIAP) evaluations
  - US window into the international Common Criteria community
  - Protection profiles around Full Device Encryption (FDE), VPN, and device itself

# Who Would Use This ?

- US Government
  - Initial focus on meeting demand and requirements for a market segment we know
  - DoD, Intel, Civilian

- Using the NSA CSfC process, agencies can use the device for classified SECRET use cases
  - VoIP, chat, mission apps

- First major hurdle – Funding
  - They want it off the shelf - will not commit to a large order of devices
  - First thing they ask - “Is it certified?"

- Does the market really value ‘Formal Methods’ enough to pay for the associated premium?

- Logical adjacency is Regulated Industry – medical, financial, utilities, mining/gas/oil.

# It's been done before…kind of

- Virtualized solutions exist on Intel, laptop form factor (SecureView, ForcePoint, IGS)
  - Nothing currently on ARM/Smartphone
- CSfC approved smartphones exist as well – Samsung shows up a lot on that list
  - Knox is "good enough", but we can definitely do better
- CSfC driven by what commercial market is putting out there – Cog is pushing virtualization and having an impact in evolving the requirements

# Ecosystem Challenges

- Forced to deal with the hardware at an intimate level
  - Need access to internals and sometime driver source
  - Dealing with proprietary, black box binaries
  - Need to maintain secure boot chain and EL2 access
  - Should leverage unique hardware features

- Essential to have a good OEM partner to reduce risk
  - Window into Qualcomm licensed materials
  - Very little financial incentive for OEMs to do small batch or custom solutions - usually require a large Minimum Order Quantity (MoQ)
  - Ongoing support for device through software updates over a useful lifecycle.

- Do **NOT** get in the hardware business!
  - Want to integrate with OEM's supply chain, fulfillment, and support process

# Where Have We Been ?

- Established long-term Agreement and relationship with smartphone OEM - Bittium
- Executed funded R&D effort to get up and running
  - Met requirements, but fell short of productization readiness goals
- Experienced major challenges with Qualcomm platform
  - Not a problem specific to seL4, but available resources and community matter
- Switched horses to BedRock Systems … then reversed course back to seL4
  - Like I said, community matters and ARM is hard for hypervisors

# Where are We Now ?

- Looking back to the seL4 Community to help
- Infrastructure Improvements
  - Microkit
  - Device Driver Framework
- Kry10's work with verifiable SMP VMs
- TII's work on virtualization support with virtIO/QEMU
- Lots of other ongoing work which we may be able to leverage

# Thank You

## Questions ???

Feel free to drop me a note:

Jason Sebranek
jason@cog.systems