Android Virtualization from Sierraware
Integration Challenges

- DRM Mandates TrustZone TEE
- Hypervisor provides the flexibility and security needed for BYOD
- Power management, responsibility spread across Multiple entities. TrustZone Monitor and Android Guests need co-operate.
- Efficient integration between TEE and Hypervisor is must to ensure seamless 1080p@60 video performance
- High performance GPU stack allowing for the ability to run un-modified apps on games.
Dual Android

SierraTEE – Secure OS
Malware Protection
DRM & Crypto
Secure Boot

SierraVisor – ARM Hypervisor

Android Work and Play. Bring Your Own Device to work
Dual Persona Android

- Primary Android
  - Full access to all the devices like Camera, LTE, SD Card
  - Hypervisor overhead is below 0.5%
  - Near native performance on GPU benchmarks and CPU benchmarks like Lmbench

- Secondary Android
  - Virtual Network, Virtual Block
  - Minimal changes to native Android stack
  - Full GPU access; all games and apps can use GPU
  - Gfxbenchmark with low overhead. Triangle, fill rate are near native performance.
Difficulties of Integrating TEE and Hypervisor

- TEE needs to be aware of 2 level memory translation
- Virtual Interrupts and VGIC are not directly visible for TEE
- Asynchronous task scheduling. Hypervisor scheduler needs to work with TEE scheduler to ensure one guest doesn’t starve the other guest by residing in secure world for too long
- Global Platform APIs and SMC calling conventions were not designed with multiple guests and TEE domains
How to secure the devices from Malware?

TrustZone Malware Protection
- File System Scanner
- Live Process Scanner
- Interrupt Table Scanner
- Kernel Scanner
  - KernelSystemCall, KernelSyscallTable, KernelProcRoot, KernelProcRootIops, KernelProcRootLookup

Insecure Android
- Filesystem, VFS
- Page Table, TLB
- Interrupt Table
- Kernel Memory map

Offline FS Integrity

Hypervisor Translated Memory

Normal World

TrustZone TEE
Difficulties of Integrating Android on a Hypervisor

- Linux Kernel is very conducive and been the most used guest operating system
- Android on the other hand is heavily tied to the hardware
  - Media Player
  - DRM
  - Power Management
  - Disk and I/O
and so many other things. Paravirtualizing all them and making sure they play well with TEE requires good pre-plan and well thought out design.
Integrating Remote GPU Rendering and Android

- Android is tightly integrated with OpenGLES & egl.
- Even simple things like cursor movement rely on Android GPU.
- A 1080p frame is 7+MB of data. So moving 60 frames per second via para-virtualized drivers incurs huge cost penalty.
GPU Rendering

App 1
- OpenGL
- EGL
- AGL
- HGL
- Surface

Gralloc
- Surface

App 2
- OpenGL
- EGL
- AGL
- HGL
- Surface
- SGL - Images
- Surface

SurfaceFlinger
- Render Loop

Layer Stack

Rendering Stack
- Color Buffer Manager
- OpenGL/EGL Remote
- Remote Rendering Thread
Paravirtualizing Android Audio

Android Guest (Slave)
- Media Player
- Recorder
- Audio Flinger
- Audio Flinger HW Interface

Para virtualized
- /dev/eac – Proxy driver
- Shared Memory & IPC

Master Guest0
- Audio Proxy
- Pulse Audio
- ALSA Driver
- IPC Driver
- Kernel

sierraware
DRM – Secure Video Data path

- DRM Mandates that both compressed and unencrypted content must be kept out of guest memory space
- A Single Video Rendering path executed on TEE must serve multiple Guest OSes
- Physical memory translation between guest and TEE has to handled by a Integrated Solution
- Arbitration of resources is also important
- Ability to share hardware codecs and devices like speakers between multiple guests in a secure way is critical
DRM: TEE and Hypervisor

SierraVisor – ARM Hypervisor

SierraTEE

HDCP, DRM Stub Agents

Video, Audio Data Sync

Translated Memory

Secure Video Buffer
Wireless Video/Miracast HDCP

Android
- libstagefright
- WIFI Display
- HDCP API
- Libstagefright_hdcp.so
- Controller & Session
- TEE Shared Queue

SierraTEE (Secure OS)
- HDCP 2.0
- SKE/AKE Key Management
- Time and Locality Check
- Cipher
- Session
- Crypto – RNG, RSA, AES, SHA256
- TEE Shared Queue

SierraVisor – ARM Hypervisor
Other I/O Devices that needs to be para-virtualized

- Mouse/Keyboard/Touch screen
- USB, SDIO. External Storage
- Android Debugging and Shell
- Power Management like idle screen time out
- LTE, Telephony stack
Para virtualized I/O: virtio provides an efficient abstraction for hypervisors and a common set of I/O APIs

Components of Virt I/O:
- Full support for SDIO, NAND, USB based storage devices
- Virtual Network with Jumbo frame support. Ability to bridge Ethernet, WIFI, LTE and other network interfaces
Support and Services

Simply Secure
Software Suite

- **SierraVisor:**
  - Hypervisor for ARM
  - Para-Virtualization, TrustZone Virtualization, HW Virtualization
  - 64 bit Support for Cortex A5x cores
  - Linux, uCOS and various RTOS

- **SierraTEE/Micro Kernel**
  - TrustZone/GlobalPlatform TEE
  - Android, uCos and various other Oses
  - Runs on various CPUs from ARM11, Cortex A9, A15 and Cortex A53/57

- **SierraSHIELD: Integrity Management**
  - Linux Kernel Integrity Management
  - Application Rootkit Scanner
  - Incremental Log Scanner

- **DRM and Content Protection:**
  - Hardware accelerated media streaming and DTCP toolkit
  - Integration with Microsoft Playready
Professional Services

Custom Services

- Porting software to processors
- Integrating TEE and SierraVisor with applications
- Developing drivers, encoders or apps

ARM Design Expertise

- Extensive experience with ARM processors and kernel code
- Android, Linux, BSD, and VxWorks development
- Hardware & FPGA

Project Management

- Phased approach from planning and development to testing & certification
- Carefully defined schedules and communication with customers to avoid surprises & delays
Technical Support

- Telephone and Email Support
- Online technical documentation
- Software updates for commercial products
- Previews of upcoming releases
- Ability to influence feature enhancements
- Commitment to Quality
  - Service Level Agreement (SLA) details support response times and escalation levels
Thank You!

sales@sierraware.com,

+1 408 337 6400