Secure Xen on ARM: Source Code Release and Update

Sang-bum Suh
sbuk.suh@samsung.com
Software Lab.
SAIT, Samsung Electronics
June 24, 2008
Xen Summit North America 2008

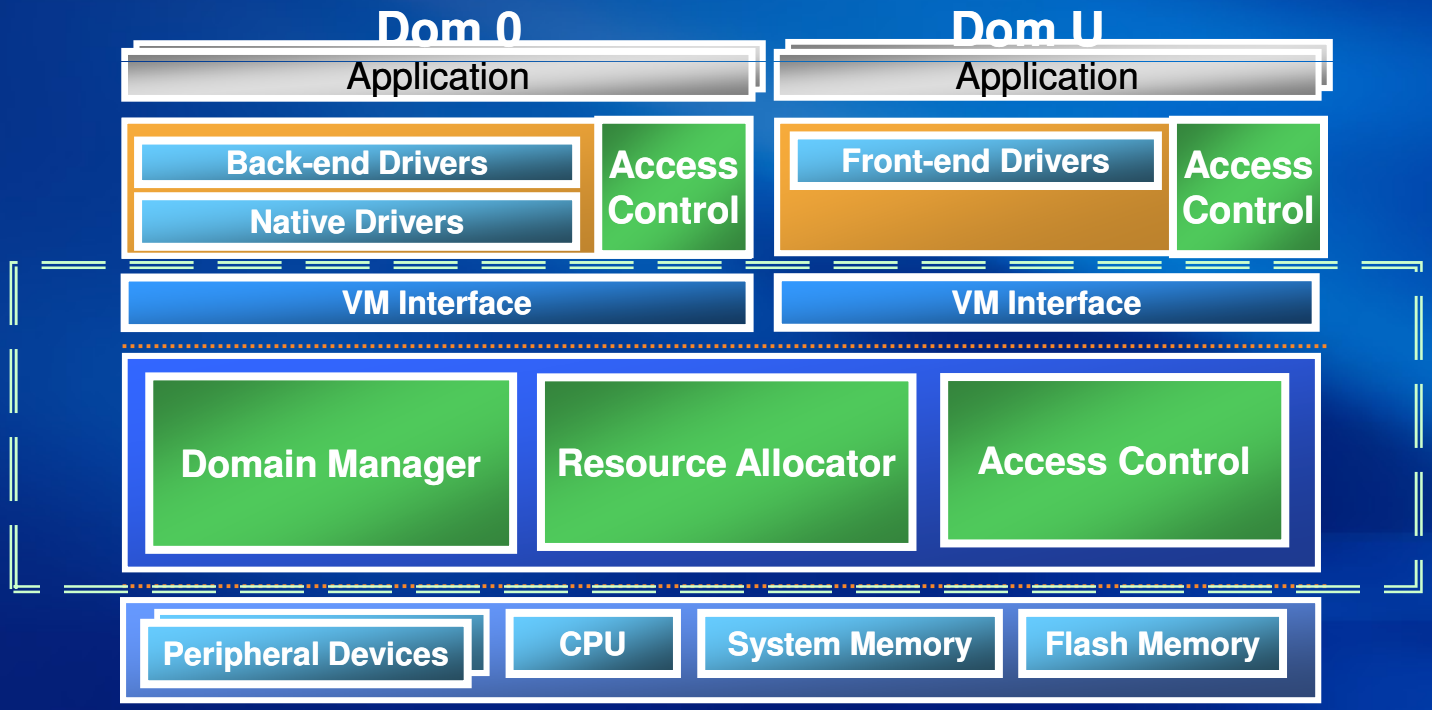
Agenda

SAMSUNG

- Secure Xen on ARM: source code release
  - Source Code
    - Overview
    - Source Code Tree
    - ARM Specific Files
    - Modified Common Files
  - New Hypercalls
  - Roadmap
- Migration for Interface Virtualization
  - Vision
  - Current Status: Demo
- Appendix

Overview

- Goal
  - Light-weight secure virtualization technology for 3G/4G mobile phone
- History
  - Secure Xen architecture and Xen on ARM demo presented at Xen Summit April 2007
  - Secure Xen on ARM demo presented at Xen Summit November 2007
- Release of source code: Xen Summit North America 2008
  - Xen on ARM, the associated Access Control, mini-OS



Secure Xen on ARM Architecture 1.0

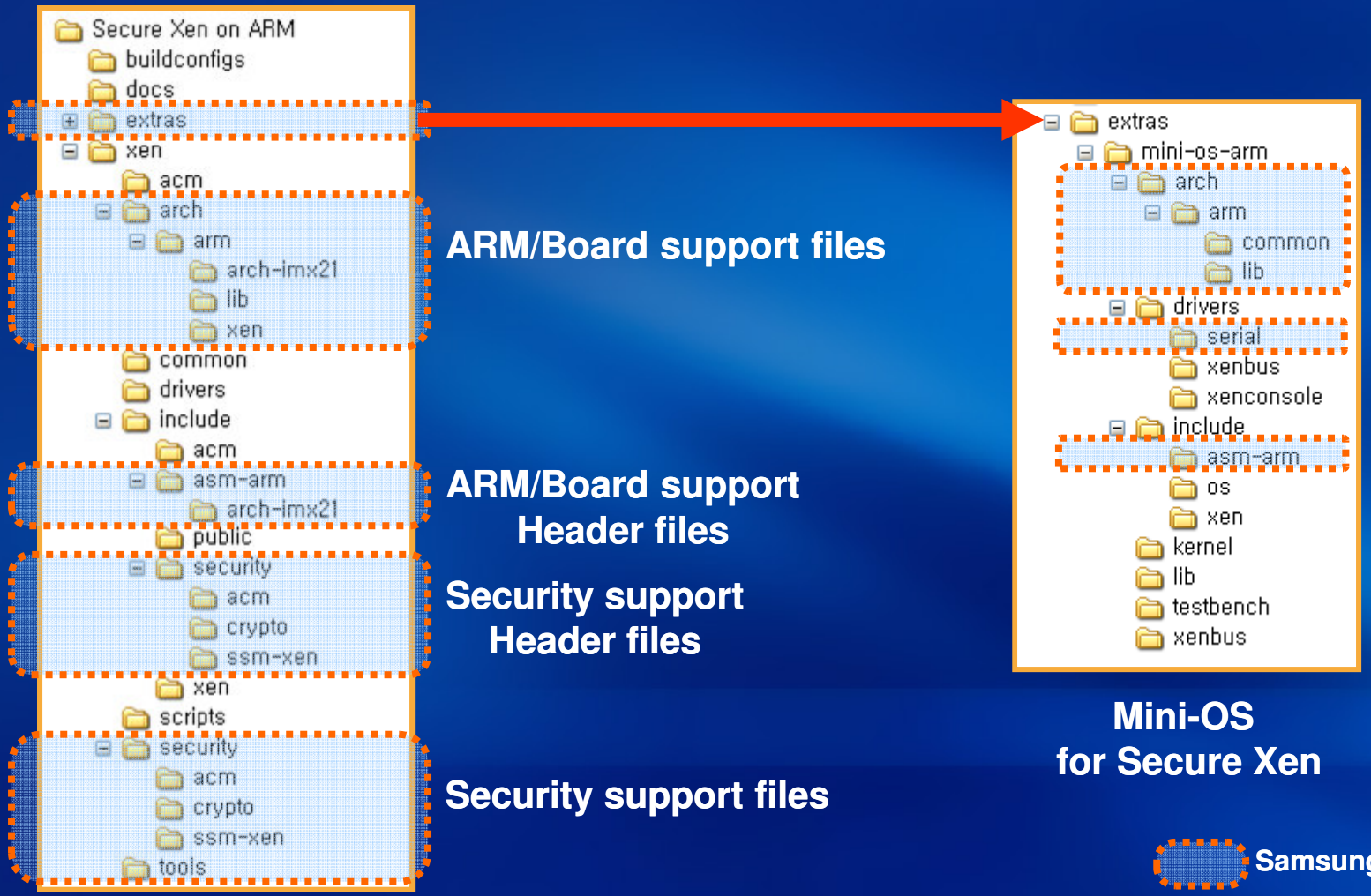
Environments

SAMSUNG

- HW and SW Environments
  - A Reference System for Implementation
    - SW
      - Xen : Xen-3.0.2
    - HW
      - Processor : ARM-9 266Mhz (Freescale i.MX21)
      - Memory : 64MB
      - Flash : NOR 32MB / NAND 64MB
      - LCD : 3.5 inch
      - Network : CS8900A 10Base-T Ethernet Controller
  - For details:
    - http://wiki.xensource.com/xenwiki/XenARM

Source Code Tree

- Samsung newly added about 20,000 loc on Xen 3.0.2
  - Added codes are for ARM support and security features
  - Some common files are modified for ARM support



ARM Specific Files

Path name	File name
xen/arch/arm	asm-offsets.s
xen/arch/arm/arch-imx21	debug.S
	platform.c
	start.S
	system.c
	time.c
	uart.c
xen/arch/arm/lib	clearbit.S
	delay.S
	div64.S
	findbit.S
	getuser.S
	lib1funcs.S
	memchr.S
	memcpy.S
	memset.S
	memzero.S
	muldi3.c
	putuser.S
	setbit.S
	strchr.S
	testchangebit.S
	testclearbit.S
	testsetbit.S
	uaccess.S

Path name	File name
xen/arch/arm/xen	arch_domain.c
	asm-offsets.c
	cache.c
	copypage-v4wb.S
	core-arm926.S
	dma-op.c
	dom0_ops.c
	domain_build.c
	domain_page.c
	entry.S
	flushtlb.c
	hypercalls.S
	irq.c
	mm.c
	physdev.c
	time.c
	tlb-v4wbi.S
	traps.c
	xen.lds.S
	xensetup.c
Xen/security/acm	Aci_generator.c
	Acm_hooks.c
	Acm_integrator.c
	Blp.c
	Decision_cache.c

Path name	File name
Xen/security/acm	Aci_generator.c
	Acm_hooks.c
	Acm_integrator.c
	Blp.c
	Decision_cache.c

*** Header files are not shown**

Modified Common Files

Path	File name
xen-3.0.2/common (1346 lines are modified)	dom0_ops.c
	elf.c
	event_channel.c
	grant_table.c
	memory.c
	page_alloc.c
	sched_bvt.c
	schedule.c
	softirq.c
	timer.c
	xmalloc.c
xen-3.0.2/drivers/char (86)	console.c
	serial.c
xen-3.0.2/include/public (278)	acm_ops.h
	dom0_ops.h
	event_channel.h
	grant_table.h
	sched.h
	xen.h
xen-3.0.2/include/xen (138)	config.h
	hypercall.h
	iocap.h
	irq.h
	sched.h
	smp.h
	softirq.h
xen-3.0.2/tools/console/client (20)	main.c

Path	File name
xen-3.0.2/tools/console/daemon (57)	io.c
	main.c
	utils.c
xen-3.0.2/tools/libxc (198)	xc_domain.c
	xc_evtchn.c
	xc_linux_build.c
	xc_linux_restore.c
	xc_linux_save.c
	xc_load_aout9.c
	xc_load_elf.c
	xc_misc.c
	xc_private.c
	xenctrl.h
	xenguest.h
	xg_private.h
xen-3.0.2/tools/python/xen (220)	__init__.py
xen-3.0.2/tools/python/xen/lowlevel	__init__.py
xen-3.0.2/tools/python/xen/sv	__init__.py
xen-3.0.2/tools/python/xen/util	__init__.py
	auxbin.py
xen-3.0.2/tools/python/xen/web	__init__.py
xen-3.0.2/tools/python/xen/xend	XendDomainInfo.py
	XendRoot.py
xen-3.0.2/tools/python/xen/xend/server	DevController.py
	SrvDaemon.py
	__init__.py
xen-3.0.2/tools/python/xen/xend/xenstore (244)	__init__.py

New Hypercalls

SAMSUNG

- We introduce new 8 hypercalls in order to
  - Support ARM architectures
  - Enable new security features

Hypercall name	Description
__HYPERVISOR_restore_guest_context	Restore CPU context stored in guest kernel stack
__HYPERVISOR_do_print_profile	Dispatch profiling data
__HYPERVISOR_do_set_foreground_domain	Change foreground domain
__HYPERVISOR_do_set_HID_irq	Register HID irq. The HID irq is only delivered to foreground domain select by __HYPERVISOR_do_set_foreground_domain hypercall
__HYPERVISOR_dma_op	Request DMA operations
__HYPERVISOR_set_pirq_type	Change IRQ type and attributes
__HYPERVISOR_do_acm_op	Override native Xen hypercall. User can choose native or Secure Xen hypercall via menuconfig
__HYPERVISOR_sra_op	Manage secure storage data

Roadmap: release of source code

SAMSUNG

2008		2009
June	~ 4Q	~ 2Q

VMM

- Secure Xen on ARM 9
  - Static domain memory partition
- Mini-OS

- Para-virtualized Linux and device drivers
- Xen tools for ARM: interface compatible with Xen-x86

- Align Xen mainline
  - Catch up Xen version
- ARM 11 support
- Power management

Security

- Access Control (TE, BLP)
  - Physical I/O, logical resources
- Secure boot/ secure storage

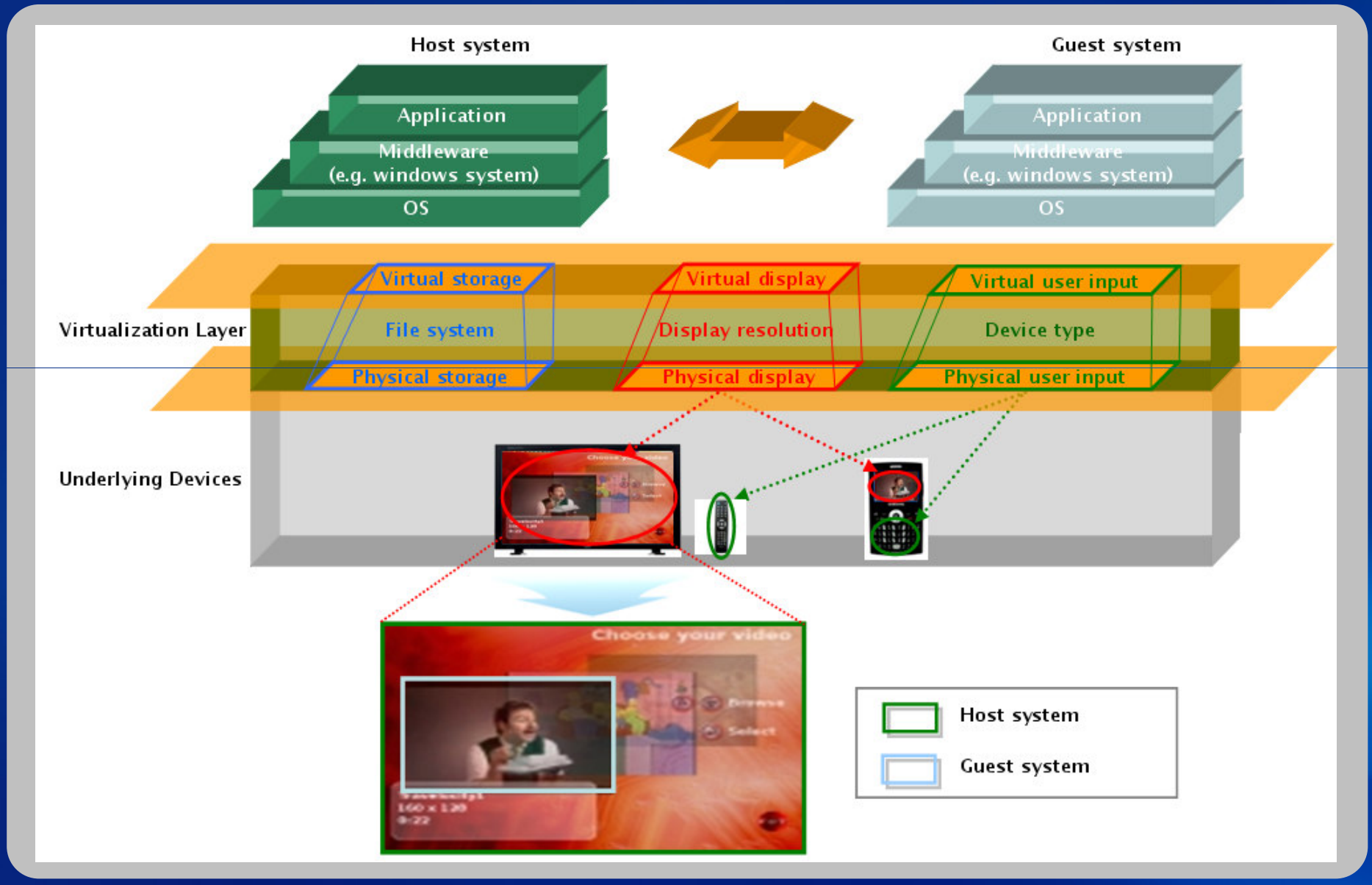
- GUI Policy Manager: access control

- TPM support

Agenda

- Secure Xen on ARM: source code release
  - Source Code
    - Overview
    - Source Code Tree
    - ARM Specific Files
    - Modified Common Files
  - New Hypercalls
  - Roadmap
- Migration for Interface Virtualization
  - Vision
  - Current Status: Demo
- Appendix

Vision: service/UI migration

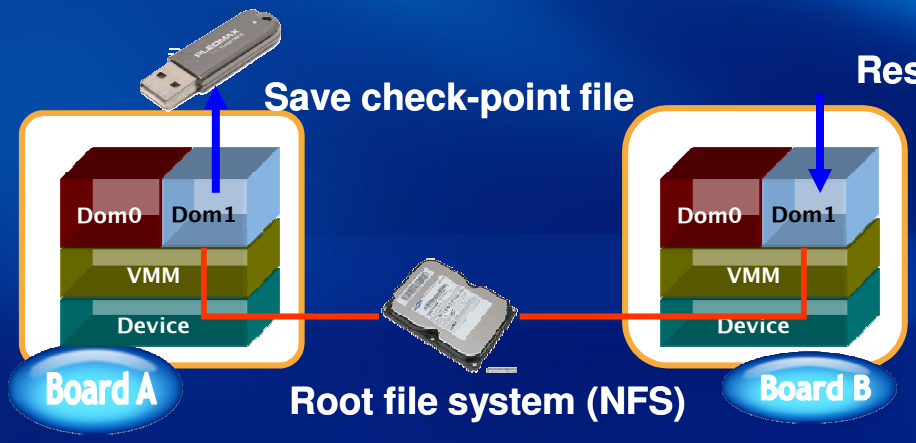


Current Status: early stage

- HW and SW Environments
  - A Reference System for Implementation
    - SW
      - Xen: Secure Xen on ARM, OS: ARM Linux 2.6.11
    - HW (Board A,B)
      - Processor: ARM-9 266Mhz (Freescale i.MX21)
      - Memory: 64MB
  - NFS is used for sharing root file system
- Demo Scenarios
  - Suspend guest domain of target board A
    - Check-point data file is saved on USB flash drive (UFD)
  - Resume the guest domain at target board B
    - UFD has a check-point file

Video clip (Game)

Video clip (Movie)



* Board A, B are identical.

SAMSUNG

- Thank you!
- Welcome Xen developers and eco-system companies who are interested in making contributions to Secure Xen on ARM!
  - Contact: Sang-bum Suh

email: sbuk.suh@samsung.com
Software Lab, SAIT
Samsung Electronics