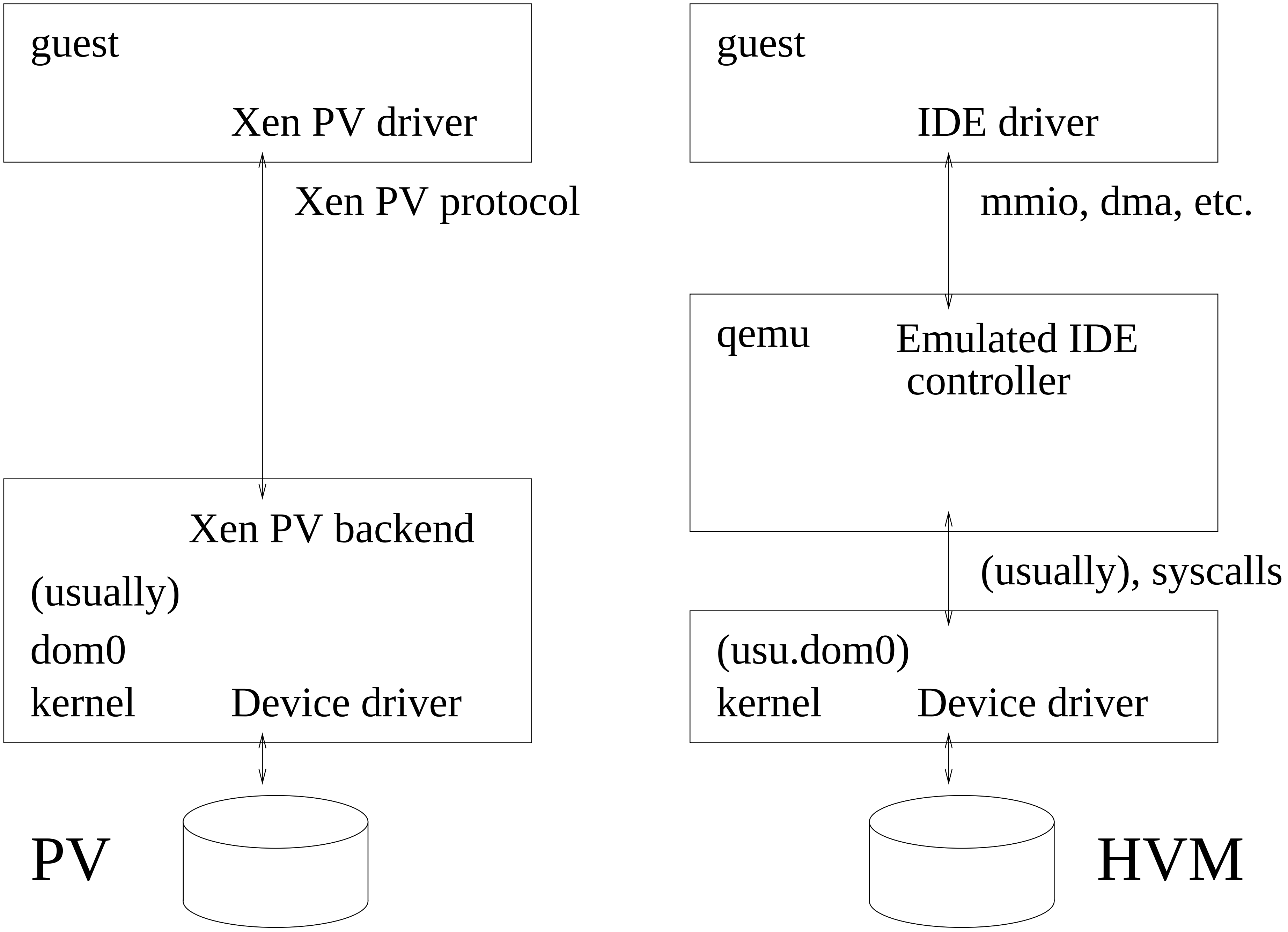
QEMU for Xen secure by default

Deprivileging the PC system emulator

Ian Jackson <ian.jackson@eu.citrix.com>

FOSDEM 2016

with assistance from Stefano Stabellini



guest

Xen PV driver

Xen PV protocol

Xen PV backend

(usually)

dom0

kernel

Device driver

PV

guest

IDE driver

mmio, dma, etc.

qemu

Emulated IDE controller

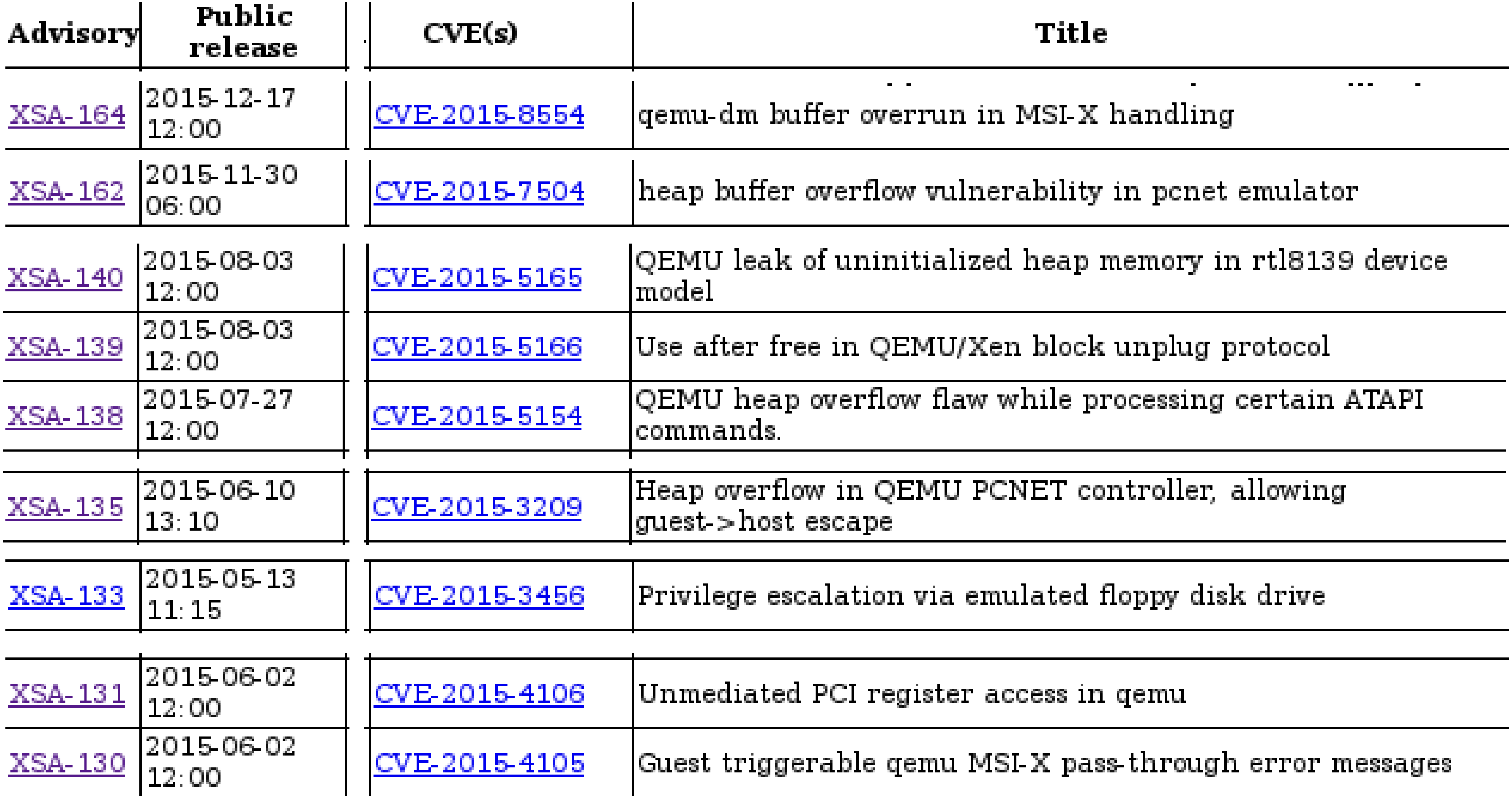
(usually), syscalls

(usu.dom0)

kernel

Device driver

HVM



Advisory	Public release	CVE(s)	Title
XSA-164	2015-12-17 12:00	CVE-2015-8554	qemu-dm buffer overrun in MSI-X handling
XSA-162	2015-11-30 06:00	CVE-2015-7504	heap buffer overflow vulnerability in pcnet emulator
XSA-140	2015-08-03 12:00	CVE-2015-5165	QEMU leak of uninitialized heap memory in rtl8139 device model
XSA-139	2015-08-03 12:00	CVE-2015-5166	Use after free in QEMU/Xen block unplug protocol
XSA-138	2015-07-27 12:00	CVE-2015-5154	QEMU heap overflow flaw while processing certain ATAPI commands.
XSA-135	2015-06-10 13:10	CVE-2015-3209	Heap overflow in QEMU PCNET controller, allowing guest->host escape
XSA-133	2015-05-13 11:15	CVE-2015-3456	Privilege escalation via emulated floppy disk drive
XSA-131	2015-06-02 12:00	CVE-2015-4106	Unmediated PCI register access in qemu
XSA-130	2015-06-02 12:00	CVE-2015-4105	Guest triggerable qemu MSI-X pass-through error messages
…	…	…	… …

from Xen Security Team advisories page, `http://xenbits.xen.org/xsa/`

Xen on x86 modes, and device model bug implications

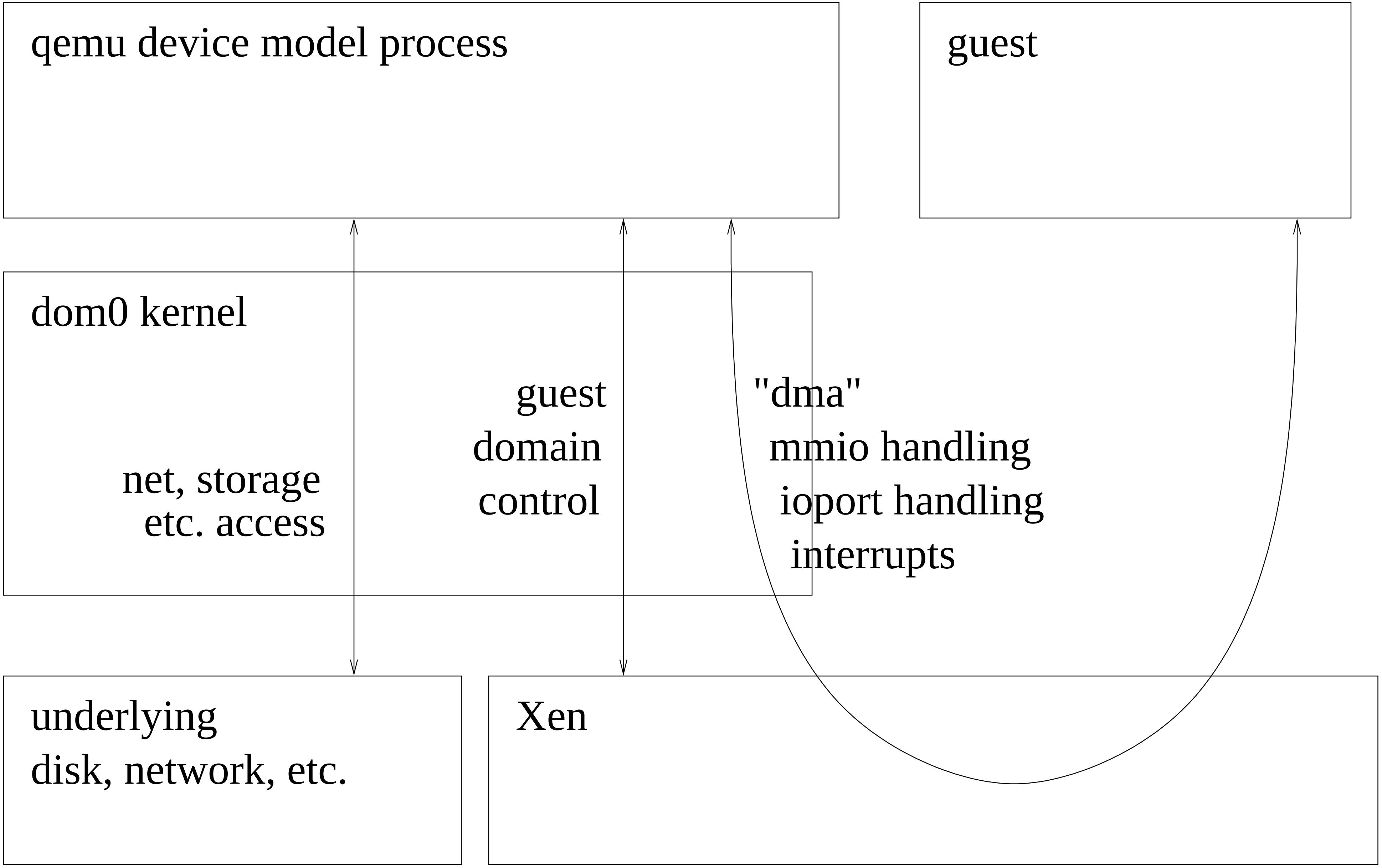
Current status for users of upstream Xen and distros

		Status	Device model bugs mean	Notes
PV		Fully supported	Safe (no DM)	Only modified guests
HVM	qemu in dom0	Fully supported	Vulnerable	Current default
HVM	qemu stub DM	Upstream but not in most distros.	Safe	Ancient qemu Build system problems

Xen on x86 modes, and device model bug implications

Current status for users of upstream Xen and distros and future plans

		Status	Device model bugs mean	Notes
PV		Fully supported	Safe (no DM)	Only modified guests
HVM	qemu in dom0 as root	Fully supported	Vulnerable	Current default
HVM	qemu stub DM qemu-xen-trad.	Upstream but not in most distros.	Safe	Ancient qemu Build system problems
HVM	qemu stub DM rump kernel	In progress Hard work!	Safe	Rump build system is mini distro
HVM	qemu dom0 not as root	**Targeting Xen 4.7**	No privilege esc. Maybe dom0 DoS	Defence in depth Hopefully, will be default



qemu device model process

guest

dom0 kernel

net, storage
etc. access

guest
domain
control

"dma"
mmio handling
ioport handling
interrupts

underlying
disk, network, etc.

Xen

Xen on x86 modes, and device model bug implications

Current status for users of upstream Xen and distros and future plans

		Status	Device model bugs mean	Notes
PV		Fully supported	Safe (no DM)	Only modified guests
HVM	qemu in dom0 as root	Fully supported	Vulnerable	Current default
HVM	qemu stub DM qemu-xen-trad.	Upstream but not in most distros.	Safe	Ancient qemu Build system problems
HVM	qemu stub DM rump kernel	In progress Hard work!	Safe	Rump build system is mini distro
HVM	qemu dom0 not as root	**Targeting Xen 4.7**	No privilege esc. Maybe dom0 DoS	Defence in depth Hopefully, will be default