Using QEMU for industrial embedded applications

Pierre Ficheux (pierre.ficheux@openwide.fr)

CTO Open Wide / OS4I

15/10/2009
Topics

- Who am I?
- What is QEMU?
- Installing QEMU
- Using QEMU in a standard way
- QEMU for embedded development
- Hacking QEMU
- The « COUVERTURE » project
Who am I?

- CTO of Open Wide (open-source software service company)
- Open Wide: created in 2001, 70 employees in Paris & Lyon
- OS4I : industrial software department of OW
- Author of « Linux embarqué » (Editions Eyrolles) the unique french book about « embedded Linux »
What is QEMU?

- Hardware emulator designed by Fabrice Bellard (author of FFmpeg)
- Licensed under the GPL
- Initially based on BOCHS (x86)
- Supported CPUs: x86, PPC, ARM, MIPS...
- Support for common peripherals => full board emulation
- User space application!
- Target OS agnostic => can run Linux, Win$, ...
- Some « hardware » acceleration with \textit{kqemu} kernel module (x86, obsolete?)
- Competitors: GXemul, BOCHS, VirtualBox
Installing QEMU

- Available for Linux, Mac OS X, Windows
- Current stable version: 0.11.0
- Binary installation (Linux):
  - $ sudo yum install qemu
  - $ sudo apt-get install qemu
- Compilation from sources:
  - $ ./configure --target-list=...
  - $ make
  - $ make install
Using QEMU in a standard way

- Typically, using OS inside another one
- Live CD:
  - $ qemu -cdrom F10-i686-Live.iso
- Home-made image
  - $ qemu linux-0.2.img
- OS installation
  - $ qemu-img create -f raw xp.img 1500M
  - $ qemu -hda xp.img -boot d -cdrom xp.iso
- Running installed OS from image
  - $ qemu -hda xp.img -boot c
QEMU Network support

- Some famous Ethernet controllers supported (x86): NE2000, RTL8139, PCNet
- Several ways to use network:
  - VLAN
  - TUN/TAP (bridge)
  - User mode (SLIRP) => no ICMP, no access from host to QEMU
- Lots of documentation available from the net...
- Option:
  - net nic,model=ne2k_pci -net user
QEMU for embedded development/training

• Embedded boards are « expensive », university and schools are poor...
• Most of training companies & schools have PC
• (Board + power supply + cable) x Nstudent x CPU => heavy load for teacher
• « Please could you send me your precious hardware prototype to start my dev ? »
• « I like to work in the TGV but policeman don't take my board, it's not a bomb :) »
• Binary compatibility in most cases
ARM9 emulation + embedded Linux

- Build a system with Buildroot, Open Embedded or home-made => 1 kernel image + 1 rootfs image
- Check-out emulated boards:
  - `$ qemu-system-arm -M ?`
  - Supported machines are:
    - integratorcp ARM Integrator/CP (ARM926EJ-S) (default)
    - versatilepb ARM Versatile/PB (ARM926EJ-S)
    - versatileab ARM Versatile/AB (ARM926EJ-S)
    - ...
ARM9 emulation + embedded Linux, testing...

• Test with:
  − $ qemu-system-arm -M versatilepb -m 16
    -kernel kernel.img -initrd rootfs.gz
  − -M: emulated board
  − -m: allocation RAM in Mb
  − -kernel: kernel image (zImage)
  − -initrd: initrd image (CPIO + gz)

• Of course we can use INITRAMFS (rootfs in kernel image)

• Very FAST boot (< 1s with Core 2 Duo PC)
Hacking QEMU

- When do you need to hack QEMU
  - New CPU?
  - New hardware controller?
  - New/updated board support?
  - New network protocol?

- Not so simple:
  - Lack of internal documentation
  - Some «unstable» API

- But: large community including famous companies (Red Hat, IBM)
Use case (in real world)

- "Hey you, I have an old fashioned software running on obsolete hardware. Of course no sources available, could you help?"
  - Text based software, binary only
  - Runs on very old PC (ISA, 4 Mb RAM) under C-DOS (Concurrent DOS, Digital Research)
  - ARCnet based (what's that ??)
    - Attached Resource Computer NETwork
    - Designed by Datapoint Corp. In 1976
    - Linux kernel support for ISA and PCI adapter
The QEMU answer

• Running C-DOS in QEMU inside Linux host
• Linux host includes **PCI** ARCnet adapter (SH-ARC PCI, still available)
• Adding ARCnet **ISA** adapter support to QEMU (90C65 chipset, no more available)
• Adding ARCnet raw socket support to QEMU
• ARCnet data from application sent by emulated ISA adapter to Linux host...which sends data to the ARCnet network...
• First test « Linux to Linux », then QEMU/C-DOS with real application
The QEMU answer, architecture
The « COUVERTURE » project

- Led by AdaCore, the GNAT Company
- New approach for software coverage in DO-178B environment
- Standard approach: embedded software IS instrumented, tested in « real » environment
- New approach: software is NOT instrumented, tested in instrumended virtual environment (QEMU)
- Open source solution
- Already used by industry as internal projects => fast testing (cf: QEMU ARM9 on standard PC)
Classical vs Virtualization

**Conventional Approach**
- Sources
  - Compilation Link
  - Instrumentation
  - Executable

**Coverage Information**
- Pure Functional Test
- Instrumented Functional Test

**TARGET**
- Coverage Data

**Approach by Virtualization**
- Sources
  - Compilation Link
  - Executable

**Virtual Machine**
- Instrumented Functional Test

**HOST**
- Binary Branch Information
Testing program with COUVERTURE

- Build executable with the powerpc-elf GNAT toolchain, with special glue to let the program run into QEMU
- Run through instrumented QEMU to generate an execution trace,
- Use « xcov » coverage analyzer to generate user level relevant info, eg annotated sources, from one or more traces.
- Reference board is Wind River SBC8349E (support added to QEMU by OS4I)
- http://www.os4i.com
- http://www.qemu.org
- http://savannah.nongnu.org/projects/qemu
- http://www.projet-couverture.com