
Google Android Kernel Debugging

Using GDB

Zhaohui Wang, Angelos Stavrou
zwange@gmu.edu, astavrou@gmu.edu
George Mason University

GDB setup

- ❑ `cd ~/mydroid`
- ❑ `Build /envsetup.sh`
- ❑ `Lunch 1`
- ❑ `emulator -verbose -show-kernel -netfast`

emulator: control console listening on port 5556, ADB on port 5557

GDB setup

- telnet localhost 5556
 - In telnet, type: `redir add tcp:10000:10000`
 - Press `CTRL-]` and, at the `telnet>` prompt, type: `quit`
- `adb shell gdbserver 10.0.2.15:10000 --attach <PID of program>`
- `arm-eabi-gdb out/target/product/generic/symbols/system/bin/app_process`

Reading symbols from `/root/mydroid/out/target/product/generic/symbols/system/bin/app_process...done.`

GDB setup

□ In *gdb* :

- set solib-search-path out/target/product/generic/symbols/system/lib:out/target/product/generic/symbols/system/bin
- target remote localhost:10000

□ Debugging is an art.... (which can be learned)

□ GDB Cheat sheet:

http://cs.gmu.edu/~astavrou/courses/ISA_673/GDBCheatSheet.pdf

GDB setup (kernel)

- emulator -verbose -show-kernel -netfast -kernel /
root/mydroid/kernels/android/arch/arm/
boot/zImage
- qemu -monitor telnet::6666,server &

QEMU waiting for connection on: telnet::
6666,serve

- telnet localhost 6666
 - QEMU 0.10.50 monitor - type 'help' for more information
 - (qemu)

GDB setup (kernel)

- ▣ `arm-eabi-gdb ~/mydroid/kernels/NexusOne/vmlinux`
- ▣ `target remote localhost:1234`

[New Thread 1]

0xafe09ec4 in ?? ()