NICTA

# Hands-on Session

## 14 August 2015

Ihor Kuz & Adrian Danis

Australian Government

# Overview

- seL4 API and Libraries
  - hello-1: simple hello world
  - debugging
  - hello-2: create a thread
  - hello-3: IPC to the thread
  - hello-4: create a new process
- CAmkES
  - hello-camkes-1: simple RPC
  - hello-camkes-2: events and dataports

# Getting the code

- Get it from github
  - mkdir sel4-tutorials-sel4
  - cd sel4-tutorials-sel4
  - repo init -u https://github.com/sel4-projects/sel4-tutorials-manifest.git
  - repo sync -m sel4-tutorials.xml
  - cd ..
  - mkdir sel4-tutorials-camkes
  - cd sel4-tutorials-camkes
  - repo init -u https://github.com/sel4-projects/sel4-tutorials-manifest.git
  - repo sync -m camkes-tutorials.xml
- Get it from zip file
  - unzip sel4-tutorials.zip
- Getting solutions
  - projects/sel4-tutorials/solutions

# Building and running the code

- For seL4 API and Libraries
  - make ia32_hello-1_defconfig
  - make silentoldconfig
  - make
  - qemu-system-i386 -nographic -m 512 -kernel images/kernel-ia32-pc99 -initrd images/hello-1-image-ia32-pc99
- For CAmkES
  - make arm_hello-camkes-1_defconfig
  - make silentoldconfig
  - make
  - qemu-system-arm -M kzm -nographic -kernel images/capdl-loader-experimental-image-arm-imx31
- Cleanup
  - make clean
  - make mrproper

# Debugging

- VM fault

  Caught cap fault in send phase at address 0x0

  while trying to handle:

  **vm fault** on **data at address 0x0** with status 0x6

  in thread 0xffaf9900 "rootserver" **at address 0x80480db**

- use objdump
  - objdump -dS build/x86/pc99/hello-1/hello-1.bin | less
  - look for instruction at address: 80480db

```
  printf("hello world\n");
80480d1:       68 40 c8 04 08          push   $0x804c840
80480d6:       e8 c8 02 00 00          call   80483a3 <puts>
   *(char*)0x0 = 'a';
80480db:       c6 05 00 00 00 00 00    movb   $0x0,0x0
80480e2:       0f 0b                   ud2
```