Software security and hypervisors isolation

Arash Vahidi
SICS security lab
isolation

computer
isolation
Basic memory isolation
Linux containers

Disposable VMs”, Joanna Rutkowska
Type 2 hypervisors
Type 1 hypervisors

guest OS

hypervisor

CPU

applications
Dual mode: normal/secure

- Normal applications
- Secure applications
- Normal OS
- Secure OS
- Monitor
- CPU
Some related projects at SICS
• Collaboration between SICS and KTH
• Very small type 1 hypervisor for ARMv7 (32-bit)
• Formal verification of the hypervisor
next irpt s =
  (clear-alist =>_nav
     (λu. if irpt = NoInterrupt then
        waiting_for_interrupt =>_nav
        (λwfi. condT (~wfi)
           (fetch_instruction =>_t
            (λ(opc, ins). is_viol =>_t (λav. clear-alist =>_nav
              (λu. if av then prefetch_abort
                else
                (execute ins =>_t (λu. is_viol =>_t
                    (λav. condT av
                      (clear-alist =>_nav
                        (λu. data_abort)))))))))
               else take_exception irpt =>_nav (λu. clear_wait_for_irpt)))) s
Collaboration between SICS, KTH, Ericsson, Tutus, Sectra, T2Data and @atsec

Type 1 hypervisor for ARMv8 (64-bit)

Utilize virtualization support on COTS hardware

Common Criteria EAL6 evaluation for high assurance
Hypervisor

ARMv8 CPU

core 1

core 2

core 3

fully virtual.

core 4

communication

Hypervisor

ARMv8 CPU
https://haspoc.sics.se

https://bitbucket.org/sicssec/haspoc-hypervisor
“Embedded Multi-Core systems for Mixed Criticality applications in dynamic and changeable real-time environments”

European collaboration with 100 partners

Isolation software for use in multi-core real-time systems
https://www.artemis-emc2.eu/
moped: https://moped.sics.se/
Thank You!