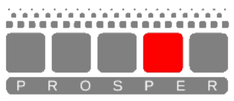
HASPOC

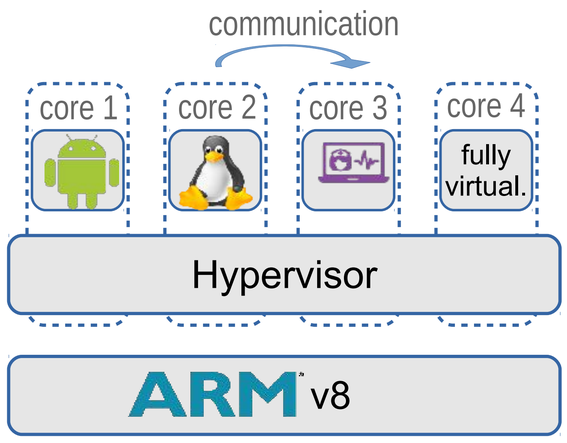
Turning an academic prototype for isolation into a real world security product

Virtualization

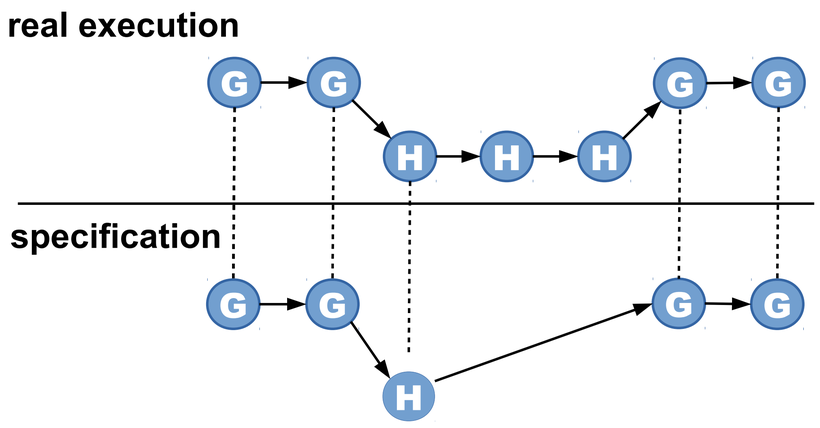
SWEDISH ICT SICS

- main property: isolation
- open source
- successor of the SICS Thin Hypervisor from the SSF-funded PROSPER-project





Verification



KTH VETENSKAP OCH KONST

platform security	hypervisor correctness
• integrity + confidentiality • HOL4 theorem prover • Cambridge models for ARM • automated analysis • multicore, memory, peripherals, interrupts, ... u | p1 → u' | p1 u | p2 → u' | p2	• functional correctness • on binary level • static analysis (BAP + SMT solvers) • new tool to lift ARM • binary to BAP code
	boot

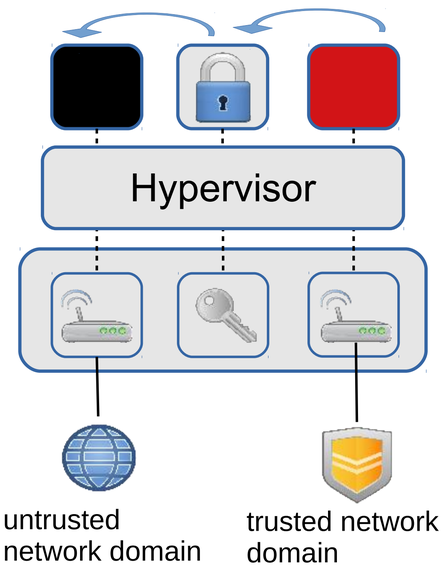
Applications

ERICSSON

TUTUS DIGITAL GATEKEEPERS

SECTRA

- network security appliance (red/black separation)
- secure smart phone (business/private modes)
- SCADA systems, mobile communication networks, vehicular systems, IoT devices, ….



Secure Boot

- basic initialization and hardware configuration
- assure integrity of hypervisor and guests
- assign resources
- chain of trust:
  ROM → boot loader → … → hypervisor
- public RSA-keys tamper resistant

T2 DATA

CC Certification

@SEC the information security provider

- preparation for Common Criteria Evaluation
- EAL 6

Contact

Reference Group:
MSB, PTS, MUST, ABB

Web:
haspoc.sics.se

Funding:
Vinnova

Contacts at SICS:
Rolf Blom (rolfb@sics.se)
Christian Gehrmann (chrisg@sics.se)
Oliver Schwarz (oliver@sics.se)

VINNOVA

SWEDISH ICT SICS