CASTOR
Container Allowing for Secure and Trustworthy OS Refinement
{jnordholz, peter, japseifert}@sec.t-labs.tu-berlin.de

Motivation
continuing growth in hardware capabilities
- opens up new opportunities
- permanent network connectivity

more varied stakeholders
- mutually distrustful
- owner
- manufacturer
- network operator
- service/content provider

tendency towards commodity OS
- tools
- developers
- apps
- supported platforms
- yet: lacking in security

deep defense
- account for long life cycles
- remain operational after security incident
- remote management (over-the-air updates)
- only attainable through advanced system architecture

Existing Solutions
virtualization
- depends on hardware support for efficient implementations
type-2 hypervisors for embedded systems
- integrates well with shipping environments
- proprietary guest modifications
- huge attack vector through host OS interface
microkernel-based systems
- still evolving
- geared towards native ecosystem
- not developed with virtualization in mind
- unnecessary complexity in guest

Use Cases
government / business
- BYOD
- mobile secure network access
consumer
- media hub
- entertainment
- e-health
- content streaming
- smart metering
automotive
- remote maintenance
- navigation, infotainment
- management of e-mobility
- C2X

Architecture
objectives
- small trusted computing base
- secure encapsulation
- little guest modifications
- efficiently implementable without hardware virt. support
guest interface
- vCPU
- vTLB
- hypercall interface
flexible implementation
- execution monitor
- kernel

Preliminary Results
platform: Samsung Galaxy S2
secure infrastructure
- preboot authentication
- GUI
- 3D driver
multiple OS compartments
- open Android
- secure Android
- infrastructure
- VPN manager

Credits & References
CASTOR builds on contributions by Adam Lackorzynski and Alexander Warg, who are authors of Fiasco-OC and L4Linux, and on contributions by Steffen Lierenberg and Janis Danielsen, who developed the KARMA VMM, the ancestor of CASTOR.

[1] Pocket hypervisors: Opportunities and challenges; Landon P. Cox and Peter M. Chen; Workshop on Mobile Computing Systems and Applications; 2007
[3] The VMware mobile virtualization platform: is that a hypervisor in your pocket?; Barr et. al. ACM SIGOPS Operating Systems Review; 2010

Deutsche Telekom Innovation Laboratories - TU Berlin / FG SecT