Assuring a Hardware TrustZone

Tony Boswell (CLEF Technical Manager, SiVenture)
&
Simon Moore (Engineering Manager, ARM)
Overview

A place for medium assurance hardware

The TrustZone concept

Making use of new-generation PPs
A Place for Medium Assurance (1)

- Security-related ICs have generally been smart card ICs, using the normal smart card assurance levels of EAL4+(AVA_VAN.5, etc.) or EAL5+ (AVA_VAN.5, etc.)

- Effort and feasibility does not scale so well to much larger, high functionality SoCs…
Generic Smart Card IC

From BSI-PP-0035:
Generic TrustZone SoC

- **Other cores & subsystems**
- **Processor (TrustZone core)**
- **Interrupt controller**

**SoC Interconnect**

- **ROM**
- **SRAM blocks**
- **DRAM control**
- **Off-SoC controllers (e.g. flash, display, input device)**
- **On-SoC peripherals (e.g. timers, counters, RNG)**

**SoC**

**Devices**

**DRAM**

September 2011 5
Can’t we pretend this isn’t our job?

- Tempting to stay with what we know; to deal only with devices targeting the highest possible security…

- But we repeatedly see demand for both stronger security and more mobile devices and applications

- Low and medium assurance are not just failures to achieve high assurance!
  - Cf. the assurance case approach for standard PC processors
  - We can combine medium and high assurance blocks
TrustZone ‘Worlds’

- Normal World
  - Peripherals
  - Memory
  - Software threads
    - User mode
    - Privileged mode
  - Shared memory
  - World transition request

- Secure World
  - Peripherals
  - Memory
  - Software threads
    - User mode
    - Privileged mode
  - Shared memory
  - Secure exceptions
  - Monitor
  - Dynamically configured peripheral, controlled by SecW software

- Transition
  - Monitor
The TrustZone TOE Concept

- This means that TrustZone is only a part of the SoC
- The simple security concept of world separation makes it tractable to separate out the important aspects even on a complex chip
- Significant parts of the assurance problem come from the mapping and integration of the worlds concept with the other devices and functionality on the chip
- The presence of certain basic components to enforce the world separation offers the potential for reuse of some evaluation results just as the components themselves are reused
Building on Segregated Worlds

Application security features

Device security features

SoC security features

TrustZone security features
Making use of new-generation PPs (1)

This fits well with the new-generation PPs because:

● The users of TrustZone form a natural community
  – E.g. as a basis for Global Platform’s Trusted Execution Environment it brings together hardware and software developers, risk owners, evaluators, CBs, etc.
  – This is not just about co-authoring a PP, it is about sharing understanding of what the PP requirements mean (e.g. for risk owners, or developers of dependent TOEs), how to evaluate them, how developers can best prepare for evaluation, and how to adapt to changing attack techniques and deployment requirements
Making use of new-generation PPs (2)

- Evaluating this sort of TOE requires quite detailed attention to the security of integration to the rest of the SoC
  - Therefore the way to get assurance is to look at this level of detail *in the right areas*
  - This is about much more detail than placing general CC requirements such as
    - “The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.”  
      (ADV_TDS.1.5C, as required at EAL2)

- We need the general level but also more specifics
  - E.g. looking for memory aliasing and equivalent paths
Making use of new-generation PPs (3)

- Evaluation with a low base EAL can focus on design, in a way that matches high-level architectural security properties such as world separation
  - But the assurance activities may require and use lower level detail in critical areas, e.g. to confirm world-separation of memories, or check results of failed access attempts

- Assurance Activities can also take advantage of developer techniques
  - e.g. a lot of effort goes into developing validation suites; these may help as developer test evidence and also in confirming that reuse of previous evaluation results is appropriate
Making use of new-generation PPs (4)

- Assurance Activities can capture more specifics about aspects such as secure boot...
  - e.g. expand to cover all reset cases, not just power-on
  - Consider specifically how resources may be accessed by other components while the TrustZone components are undergoing reset

- ...and secure debug
  - e.g. require the functional specification to describe debug interfaces and the relationship between SoC-level debug and component-level debug
Achieving Reuse

- If a set of TrustZone Components is evaluated on one SoC then it should be possible to reuse evaluation results about those components when they are used in another SoC.
- The Assurance Activities dealing with integration with the rest of the SoC give a clear set of activities to be carried out on the new SoC.
- ALC activities on the original SoC (such as ALC_CMx), plus use of verification tools on the new SoC (to confirm that the TOE is the same) enable confidence that the original results still apply.
Conclusions

- TrustZone is aimed at medium assurance products, and we should find a place for these in CC.
- The new generation PP approach is well-adapted to dealing with this – we can specify functional properties and Assurance Activities mainly at design level, but include lower-level evidence and activities in critical areas.
- Assurance Activities can also help us to deal with the fact that TrustZone enforcement is only done by some of the components on the SoC.
- They can also help to achieve reuse.
Questions?

Tony Boswell
tony.boswell@siventure.com
tel: +44 1628 651 361

September 2011