2018 9th ACM/IEEE International Conference on Cyber-Physical Systems

Towards a Green and Secure Architecture for Reconfigurable IoT End-Devices

D. Oliveira, T. Gomes, and S. Pinto
Centro Algoritmi - University of Minho
{daniel.oliveira, mr.gomes, sandro.pinto}@dei.uminho.pt

***Abstract*—With the advent of the Internet of Things (IoT), objects are becoming smaller, smarter and increasingly connected. IoT devices are being deployed in massive numbers, and the success of this new Internet era is heavily dependent upon the trust and security built over billions of heterogeneous devices. However, securing IoT devices can be a quandary, with hardware requirements, energy consumption and cost limitations pulling in opposite directions. This work-in-progress proposes a novel architecture for reconfigurable IoT end-devices, where several constrains, such as the security, performance and power budget must be seriously considered. The proposed architecture intends to go beyond state-of-the-art by focusing on a trade-off between device security and power consumption, in an attempt to find an optimal design point in the energy-security space.**

***Index Terms*—Internet-of-Things (IoT), reconfigurable devices, hardware security, low-power, embedded systems.**

I. Introduction

The Internet of Things (IoT) is connecting myriads of devices to the Internet. While early concerns were related to the connectivity and interoperability of devices, the nowadays focus comprises security and privacy issues. For such systems, a variety of security architectures have been proposed, mainly relying on software-based isolation and virtualization [1,2]. The addition of hardware virtualization extensions in ARM and Intel processors brought a set of hardware-assisted virtualization solutions [3,4] with reduced trusted computing base (TCB) complexity and significant performance advantages. Notwithstanding, hypervisors are not, per se, magic bullets, and they have been struggling with their own security problems [5]. In this sense, hypervisors must be complemented with other security-oriented technologies that guarantee security from the outset. Secure processor architectures, such as ARM TrustZone and Intel Software Guard Extensions (SGX), have found widespread applicability on the high- and middle-end sector. ARM TrustZone has been attracting a lot of attention due to the massive presence of ARM application processors in the mobile and embedded segments. At the heart of the TrustZone stands the concept of secure and non-secure worlds, completely hardware-isolated, with non-secure software prevented from directly accessing secure resources. A lot of research has been steamed by TrustZone, ranging from trusted execution environment (TEE) kernels and services [6,7], to efficient real-time (RT) virtualization solutions [8].

The aforementioned approaches are typically too complex for low-end devices, which are commonly designed for specific tasks, optimized in size, weight, power and cost (SWaP-C), and often constrained by strict RT requirements. ARM recently decided to span TrustZone technology to the new generation of Cortex-M (TrustZone-M) processors and released the Platform Security Architecture (PSA). Since the PSA project is still in a very embryonic stage, it is not particularly focused on exploring reconfigurable platforms to enable the efficient implementation of systems that perfectly fit the heterogeneous nature of IoT applications. Targeting heterogeneous devices, promising approaches such as HaloMote [9], and CUTE Mote [10] were recently introduced, proposing the use of heterogeneous architectures for deploying low-power motes. These heterogeneous solutions explore field-programmable gate array (FPGA) technology to perform computing intensive software tasks (e.g., data aggregation, data compression and high-level radio tasks) in hardware accelerators. Furthermore, they explore low-power operation modes (with very low static energy drain offered by modern FPGA technology) and implement dynamic power management systems, which allow specific node components to be completely shutdown when not in use. Although HaloMote and CUTE Mote implementing promising power optimized architectures, they lack in providing secure primitives for protecting critical data at rest (secure storage) and in processing (secure execution environment).

This work proposes a novel architecture aligned with ARM PSA, anchored by ARM TrustZone-M technology. The established roadmap has identified several important requirements, such as the need for real-time guarantees, secure hardware primitives, efficient power management mechanisms, and full integration of reconfigurable platforms in the ecosystem.

II. Proposed Architecture

ARM TrustZone is a hardware technology that adds significant value to the security picture, mainly due to ARM processors being currently the most widely used processors on mobile and embedded segments. ARM TrustZone for Cortex-M microcontrollers provides the same high-level features as used on application processors (Cortex-A); however the underlying operations were re-designed from the scratch, in order to provide faster transitions and greater power efficiency . While TrustZone is a mature technology with huge applicability on high-end devices, TrustZone-M is a complete unexplored area.

Figure 1 depicts the proposed architecture, which is based on a reconfigurable System-on-Chip that integrates, on the same device, a hardcore microcontroller unit (TrustZone-enabled ARM Cortex-M processor) besides a Reconfigurable

0-7695-6378-3/18/$31.00 ©2018 IEEE
DOI 10.1109/ICCPS.2018.00041

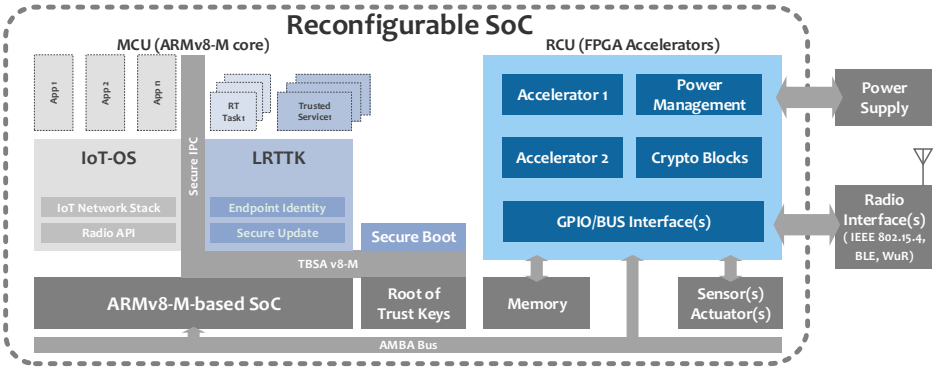

Figure 1. Architecture overview.

Computing Unit (RCU). The RCU enables the deployment of customized hardware accelerators. Due to the lack of existing solutions with built-in connectivity support, a radio interface must be attached to the mote. Such configuration allows the IoT-enabled OS to properly explore the TrustZone isolation in favor of security, while the RCU can host application-specific or generic accelerators for performance purposes. The use of reconfigurable platforms for offloading to FPGA the computing intensive software is also a new trend in the IoT domain with proven advantages in terms of flexibility, performance and power consumption [11]. Moreover, recent advances on flash-based FPGAs are demonstrating that modern FPGA-based solutions are able to provide a better performance-energy ratio when compared with microcontroller-based solutions.

III. Research Roadmap

In order to accomplish the proposed architecture, the following research roadmap is being adopted:

1) Lightweight real-time trusted kernel (LRTTK): Due to the inexistence of a trusted execution environment for low-end devices, we are currently developing a lightweight RT trusted kernel for TrustZone-enabled microprocessors, following a secure by design approach, i.e., using MISRA C coding standard and static analysis tools (i.e., PRQA QA) for code validation. While there are no TrustZone-M platforms available on the market, we got early access to a prototype of a Nuvoton NuMicro M2351. This is, however, on its initial stage of development.

2) Secure architecture: The secure runtime environment (running on the secure world) will be extended with endpoint identity, secure boot process, and a secure update mechanism. These are essential architectural requirements to implement a trustworthy IoT endpoint device. An IoT-enabled OS (e.g., Contiki-OS, RIOT) will be ported to run on the non-secure world, guaranteeing full IP connectivity to the device, while keeping security-critical code completely isolated from non-critical one.

3) Smart power management module: In order to explore new power management techniques, while preventing hacks to power management operations on TrustZone-enabled devices [12], a smart power management module will be implemented. Further studies will be performed in order to investigate how the exploration of low-power modes can potentially compromise security and disregard other system requirements.

4) Reconfigurable hardware accelerators: Intensive computing software tasks will be offloaded to reconfigurable hardware accelerators. Dynamic partially reconfiguration will be also explored in a hardware/software co-design approach.

IV. Acknowledgments

This work has been supported by COMPETE: POCI-01-0145-FEDER-007043 and FCT - *Fundação para a Ciência e Tecnologia* within the Project Scope: UID/CEC/00319/2013.

References

[1] F. Armand and M. Gien, "A Practical Look at Micro-Kernels and Virtual Machine Monitors," in *6th IEEE Consumer Communications and Networking Conference*, Jan. 2009, pp. 1–7.

[2] G. Heiser and B. Leslie, "The OKL4 Microvisor: Convergence Point of Microkernels and Hypervisors," in *First ACM Asia-pacific Workshop on Workshop on Systems*, 2010, pp. 19–24.

[3] U. Steinberg and B. Kauer, "NOVA: A Microhypervisor-based Secure Virtualization Architecture," in *Proceedings of the 5th European Conference on Computer Systems*, 2010, pp. 209–222.

[4] C. Dall and J. Nieh, "KVM/ARM: The Design and Implementation of the Linux ARM Hypervisor," *SIGPLAN Not.*, vol. 49, no. 4, pp. 333–348, Feb. 2014.

[5] M. Pearce, S. Zeadally, and R. Hunt, "Virtualization: Issues, Security Threats, and Solutions," vol. 45, no. 2, Mar. 2013, pp. 17:1–17:39.

[6] N. Santos, H. Raj, S. Saroiu, and A. Wolman, "Using ARM Trustzone to Build a Trusted Language Runtime for Mobile Applications," *SIGPLAN Not.*, vol. 49, no. 4, pp. 67–80, Feb. 2014.

[7] S. Pinto, T. Gomes, J. Pereira, J. Cabral, and A. Tavares, "IIoTEED: An Enhanced, Trusted Execution Environment for Industrial IoT Edge Devices," *IEEE Internet Computing*, vol. 21, no. 1, pp. 40–47, Jan. 2017.

[8] S. Pinto, J. Pereira, T. Gomes, A. Tavares, and J. Cabral, "LTZVisor: TrustZone is the Key," in *29th Euromicro Conference on Real-Time Systems*, vol. 76, 2017, pp. 4:1–4:22.

[9] A. Engel and A. Koch, "Heterogeneous Wireless Sensor Nodes that Target the Internet of Things," *IEEE Micro*, vol. 36, no. 6, pp. 8–15, Nov. 2016.

[10] T. Gomes, F. Salgado, A. Tavares, and J. Cabral, "CUTE Mote, A Customizable and Trustable End-Device for the Internet of Things," *IEEE Sensors Journal*, vol. 17, no. 20, pp. 6816–6824, Oct. 2017.

[11] T. Gomes, F. Salgado, S. Pinto, J. Cabral, and A. Tavares, "A 6LoWPAN Accelerator for Internet of Things Endpoint Devices," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 371–377, Feb. 2018.

[12] A. Tang, S. Sethumadhavan, and S. Stolfo, "CLKSCREW: Exposing the perils of security-oblivious energy management," in *26th USENIX Security Symposium*, 2017, pp. 1057–1074.