Design and verification of Secure IoT Hub based on Virtual SoC Platform

Nelson Vithayathil Varghese[1], Won Jong Kim[2], Shin Seok Kang[3], Hyo Seung Lee[4]
Electronics and Telecommunications Research Institute[1,2] – Korea, Neowine[1,2] – Korea
nelson@etri.re.kr, wjkim@etri.re.kr, newstone86@neowine.com, godinus@neowine.com

Abstract

This paper describes about the design and verification of Secure IoT hub platform using the SoC Virtual Platform (SVP) oriented design methodology. Secure IoT virtual SoC platform is designed as a software oriented system which can fully mirror the functionality of real System-on-Chip. This virtual platform combines both processor model(s) and high-level fully functional models of the various peripheral blocks. Key objective of this design is to provide an abstract, executable representation of the IoT hub hardware to both software developers and system architects in advance. Virtual platform's ability to provide full visibility and controllability of software running on it, enables to unveil bugs which could be difficult with a same real hardware platform. The secure IoT hub virtual platform deployed on a host PC can communicate with physical IoT devices by using the semi-hosting library mechanism. Furthermore, it also functions to enhance the security level of communication between IoT enabled devices' with the help of advanced cryptographic methods such as AES, ARIA, SHA and ECC.

Keywords: Internet of Things; Hardware Security Module; Open Virtual Platform; Peripheral Simulation Engine.

1. Introduction

As Internet of Things (IoT) transforms the world of connected devices day by day, it is equally becoming more challenging in terms of addressing new complex security requirements as well as highly competitive market that always demands less time to market. In light of above facts, hardware designers often adopt more complex design methodologies such as multi-cores and simultaneous multiprocessing. As a result of this, complexity of the resulting platform software increases exponentially that eventually give rise to many challenges to embedded software developers while working on hardware platforms. Additionally, there are extra challenges related to the verification of such platforms where often the hardware prototypes have limitations on debugability, observability, and reproducibility while debugging complex multi-processor issues and the bugs. More importantly, on most occasions software developers will have access to hardware only very near to the end of the targeted product development schedule due to various tape-out issues.

This paper proposes, design methodology based on virtual platform environment for both design and verification of Secure IoT virtual SoC platform. Additionally, it also provides an opportunity for faster architecture exploration and platform re-modeling by means of software. Simultaneous design, simulation, and debug of both HW and SW is a big advantage of having the platform virtually on the host machine [1].

This paper is organized as follows: in section 2, we present the architecture details of secure IoT hub platform that will be modelled on SoC virtual platform. Section 3 sheds some light into the implementation of virtual SoC platform. Following to this, section 4 mentions about verification and associated results. Finally, section 5 gives a conclusion and mentions future works.

2. Architecture of Secure IoT Hub

IoT Hub

Key role of IoT hub is to act as a central controller device that connects a variety of smart devices either in a home network or office network with the external IoT server that can be directly reached by a user. Additionally IoT hub itself works as a fully managed service which enables both reliable and secure bidirectional communications between large number of IoT devices and a back end server. Hubs are often made to provide end-to-end security solutions that cover multiple cloud and connectivity layers and support resource-constrained IoT devices [2].

Platform Architecture

Secure IoT hub platform is designed as a combination of AP (Application Processor) based on ARM Cortex-A7 core and a HSM (hardware security module) sub system. Key focus behind the design of

HSM is to increase the level of security by moving entire cryptographic modules from SW to HW level. The main platform will house the HSM as a secure SoC subsystem. In other words, HSM will abstract the behavior of secure SoC module to both support and isolate the cryptographic aspects of the IoT security. Secure SoC module will be interfaced to the AP through the main system bus.

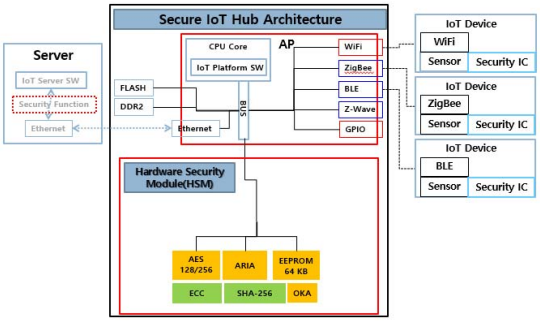

Fig. 1. Architecture of Secure IoT Hub System

3. Virtual SoC Platform Implementation

Design of Virtual SoC Platform

Design of virtual SoC platform requires firstly modeling each component of the designated system separately, then followed by models of system devices/components need to be interconnected by bus system [1].Typically processor and peripherals are represented using the SystemC/TLM models. In short a virtual SoC platform abstraction contains Instruction Set Simulator (ISS) of the processor and register accurate transaction level models (TLM) of peripherals.

Details of Implementation

For the secure IoT hub, SoC virtual platform is implemented using the Imperas OVP virtual platform environment, including cryptographic modules that handles the IoT cryptographic aspects. Cryptographic modules such as AES128/256, SHA256, ECC and ARIA are modelled in C with register –transfer level accuracy. SoC virtual platform runs on instruction-accurate model and could replicate the exact software debug environment as supported by a typical hardware platform.

Secure SoC subsystem provides a cryptographic platform and security schemes that are based on widely adopted encryption algorithms, and privacy standards [4]. Algorithms like Advanced Encryption Standard (AES) plays a vital role to assure the confidentiality with the adoption of cryptographic techniques like ARIA. The asymmetric algorithm RSA serves for asymmetric encryption, digital signatures, as well as for key management. SHA standards are used as secure hash functions [4].

4. Verification of Secure IoT Hub

Virtual platform based verification enable complete observability of failure caused responses by intercepting the instructions at simulation engine prior to execution - Instructions can be changed before execution and thereby complete control over generation of faults. Additionally, extensive controllability support under virtual platform environment enables to inject failures that are difficult or impossible to recreate deliberately in the actual hardware. Fault injection which can be either black box – hardware based or white box in nature where in virtual platform enables full control over triggering the fault and also provide support at simulation engine to perturb only what you want to control

Verification of Cryptographic Modules

Distinct test vectors are used to verify the operation of each of the cryptographic modules. From the test application, test vector data will be programmed into the predefined memory locations that are mapped with the registers for each of the cryptographic peripherals. This in turn triggers the appropriate function callbacks associated with respective cryptographic operation events.

Verification of Secure IoT Hub Architecture

The secure IoT hub virtual platform deployed on the host PC can communicate with real physical IoT devices by using the OneM2M standard. There are security mechanisms such as TLS and DTLS deployed on OneM2M, which internally use software modules like HTTPS and CoAP. It is also possible to have virtual models created for these.

Test Results

As of now, secure IoT hub virtual platform is tested with the peripheral models for AES, ARIA and SHA. Peripheral models for AES supports both ECB and CBC mode of operation for the key size 16 bytes and also ECB mode for the key size 32 bytes. Whereas the ARIA peripheral supports the ECB mode for key sizes values for 16, 24 and 32 bytes.SHA peripheral is tested for the support for SHA-2, especially for the hash function with hash value 256.

Peripheral Name	Simulated Instructions	Simulated Time	Simulated MIPS
AES-ECB(Mode)	327,791,726	3.28 s	546.3
AES-CBC(Mode)	328,996,521	3.29s	514.1
ARIA	334,724,902	3.35s	557.9
SHA	334,353,779	3.34s	586.6

5. Conclusions

In this paper, we explained the design and verification of Secure IoT hub based on SoC Virtual Platform (SVP) methodology. The amount of flexibility and controllability offered by SoC virtual platform methodology enable us to achieve fast architecture implementation. Feasibility test can be conducted quite easily by changing or configuring the desired simulation parameters and unveil bugs which could be difficult with a real hardware. More importantly, performance estimation can easily achieved as the instruction accurate SVP (SoC Virtual Platform) model offers the fastest possible simulation performance [3], which can reach 500 MIPS.Future works include the design and development for the peripherals for RSA and ECC.Additionally, using above virtual SoC platform an end to end communication will be created by using the concept of semi-hosting and secure SoC FPGA modules from Neowine.

Acknowledgement

This work was supported by the ICT R&D program for MSIP/IITP[2016-0-00147, Development of Smart SoC for Secure IoT Hub Supporting IoT Terminals with Local Area Communications].

References

[1] El-Moursy, Magady A., Ayman Sheirah, Mona Safar, and Ashraf Salem, "Efficient Embedded SoC hardware/Software Codesign using virtual Platform", International Design and Test Symposium , pp. 36-38, 2014.

[2] Symantec Corporation, "An Internet of Things Reference Architecture", pp. 1-22. 2016.

[3]LarryLapides,"Renesas_DevCon_2012_Imperas_Paper _Virtual_Platform_Based_Software_Testing.pdf", *Imperas Documents,* Imperas Software, pp. 1-38. October 2012.

[4]Nicolas Sklavos, I. D. Zaharakis, "Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and Implementations", 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp.1-2, 2016.