UNIVERSITI TEKNOLOGI MARA

DEVELOPMENT OF TRUSTED BOOT PROCESS FOR WIRELESS SENSOR NODE USING ARM11 PLATFORM

LUKMAN HAKIM BIN ADNAN

Thesis submitted in fulfilment
of the requirements for the degree of
Master of Science

Faculty of Electrical Engineering

December 2013

AUTHOR'S DECLARATION

I declare that the work in the thesis was carried out in accordance with the regulations of Universiti Teknologi MARA. It is original and is the result of my own work, unless otherwise indicated or acknowledged as referenced work. This thesis has not been submitted to any other academic institution or non-academic institution for any degree of qualification.

I, hereby, acknowledge that I have been supplied with the Academic Rules and Regulations for Post Graduate, Universiti Teknologi MARA, regulating the conduct of my study and research.

Name of Student	:	Lukman Hakim Bin Adnan
Student I.D. No.	:	2009321941
Programme	:	Master in Electrical Engineering (EE780)
Faculty	:	Electrical Engineering
Thesis Title	:	Development of Trusted Boot Process for Wireless Sensor Node Using ARM11 Platform
Signature of Student	:	....
Date	:	December 2013

ABSTRACT

Trusted platforms have been proposed as a promising approach for providing security for wireless sensor nodes platform, particularly, from physical type of attacks. However, implementation of a separate Trusted Platform Module (TPM) chip on the platform is not acceptable in the design of wireless sensor nodes because it increases the size and total power consumption of the node. Alternative to that is to use embedded microprocessors with built-in security module, which implements functions similar to the TPM, on the embedded processor. However, since the sensor node is a resource constrained platform with limited processing capabilities, it is important to ensure that the computation and energy consumption for running security functions in the microprocessor are at an acceptable rate. In this study, a trusted boot process for sensor node is developed to provide a trusted platform for wireless sensor node. It comprises of first and second level boot process. The purpose of this research is to implement the "trusted boot process" on the embedded microprocessor to provide security on the hardware layer of sensor node. The proposed system involves integration of hardware and software subsystems. The hardware subsystem, utilize ARM1176JZF-S Development Board with ICE-JTAG. For the software subsystem, the proposed system will have two levels of boot process; which are first level bootloader, acting as the root of trust of the system and, second level bootloader with security module to check the integrity of the kernel or applications that will run on the platform. The results show that the proposed system is able to provide basic security implementations to support image verification of a sensor node through trusted boot process. A brief energy consumption study is also presented to support the work.

TABLE OF CONTENTS