# Power Consumption Analysis for Security attack in TPM

Grace Kennedy, DongSub Cho
Dept.of Computer Science and Engineering
Ewha Womans University, Seoul, Rep.of Korea
e-mail : gkennedy@ewhain.net, dscho@ewha.ac.kr

## Abstract

Recently, most network communication chips are powered; which causes power consumption a heavily constraint. Since, there are a lot of expectations on TPM to have a high performance in terms of authentication of its device. During the design process there is a need to estimate the security of the design but it always when the chip has already been manufactured. This paper designed a power consumption control monitor in TPM device which evaluate the voltage drop during processing of use. Therefore we will analyze the power consumption profile. The result shows that the voltage drop leads to vulnerability of the system to attackers during communication process.

### 1. Introduction

Currently, many researchers have observed the important of power consumption in secure module platform. There are increases in the demand of secure module platforms in different aspect of discipline. In today's technology there is an urgent need of securing of network communications, especially as the number of the demand for a broad range of information and applications increase. We cannot over emphasis the need for securing a network. The biggest challenge facing computing device is insecurity and unstable power consumption.

An embedded system is a special-purpose system in which the computer is completely encapsulated by the device it controls [10]. Though not like a general-purpose computer, such as a personal computer, an embedded system performs pre-defined tasks, usually with very specific requirements. Since the system is dedicated to a specific task, design engineers can optimize it, reducing the size and cost of the product. Embedded systems are often mass-produced, so the cost savings may be multiplied by millions of items.

Trusted platform module (TPM) is an embedded system that is used as a secure module [10]. TPM is a dedicated security chip of a microcontroller that stores keys, passwords and digital certificates. A typical TPM is attached to the motherboard a notebook [8]. TPM stores some confidential and secret data which is prom to attackers. TPM extend network lifetimes by reducing the activities of the higher power consuming devices of the secure platform. The tradeoffs secure network throughout and latency (delay), power efficiency synchronize network communication to create opportunities for the TPM with active duty cycle under minimal traffic conditions [9]. There is need to consider both normal and abnormal source of power loss while constructing a power control manager in some network communication such as PCs, servers, storage devices, mobile phones, PDAs, and the network.

In this paper we designed power monitor control for observing normal and abnormal secure device based on time frame. This design evaluates the power consumption during sleep time, idle time and communication time. Our result proved that during communication TPM are exposed to the attackers more. Our future work is to implement this unique idea.

### 2. The architecture of an Embedded System

Fig.1. Below shows the architecture of a hypothetical embedded system. It shows more than one microprocessor (2 DSPs and 1 µC) are employed to carry out different tasks, the µC is generally meant for simpler and slower jobs such as carrying out a Proportional Integral (PI) control action or interpreting the user commands etc. The DSP is a more heavy duty processor capable of doing real time signal processing and control. Both the DSPs along with their operating systems and codes are independent of each other [5]. They share the same memory without interfering with each other.

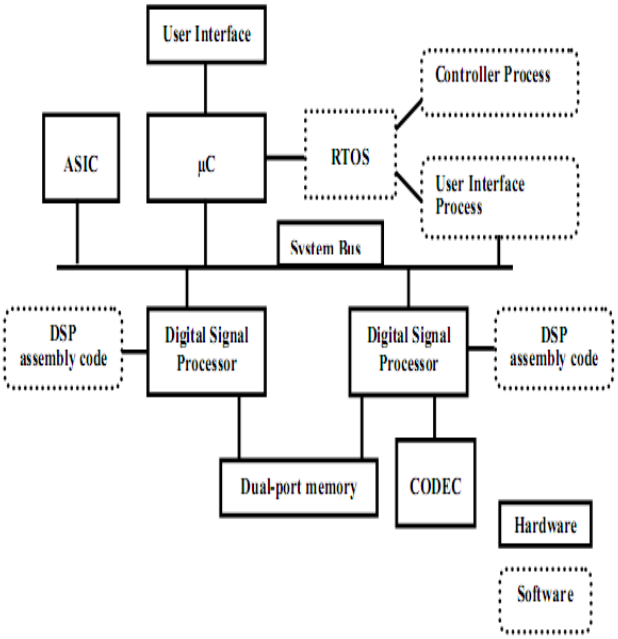


Fig 1 Architecture of an Embedded System

This kind of memory is known as dual ported memory or two-way post-box memory [4]. The Real Time Operating System (RTOS) is responsible for the controlling of the time requirement of all the devices. It executes the overall control algorithm of the process while diverting more complex tasks to the DSPs. It also specifically controls the µC for the necessary user interactivity [4]. The ASICs are specialized units capable of specialized functions such as motor control, voice encoding, modulation/demodulation (MODEM) action etc. They can be digital, analog or mixed signal VLSI circuits. CODECs are generally used for interfacing low power serial Analog-to-Digital Converters (ADCs) [5]. The analog signals from the controlled process can be monitored through an ADC interfaced through this CODEC.

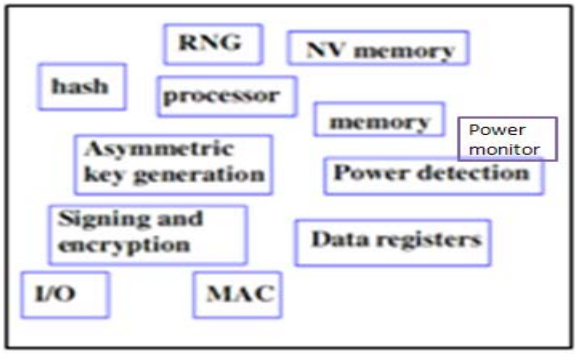


Fig. 2 Component of TPM

## 3. Related Works

James Northern et al developed the next generation tools that achieve high accuracy by estimating power consumption earlier in the design process [1]. In their paper they limited their knowledge only on the design process, but implementation process is more important and more sensitive. Yu Hu et al in their paper “Run-time Power Consumption Modeling for Embedded Multimedia Systems”, proposed fast and accurate power usage estimation, where the model depends on the specific application routine involved as well as the applied voltage and the operating frequency [4].

Shuhaizar Daud et al studied the effects of compiler optimizations on embedded systems energy usage and power consumption in real time situations and the importance of running efficient binary codes in realizing a more power efficient, and better performance [7]. David A.Ortiz et al applied source code optimizations on a set of representative benchmarks for embedded processors (MiBench) to analyze whether the techniques have or not an effect on power dissipation of microprocessor based platforms [6]. Smail Niar et al deals on the ways to accelerate performance and power consumption evaluation for embedded system [5].

## 4. Evaluation Result

Fig.3. The component of TPM is a Microcontroller which stores processor and memory, Power detection, NV memory, Hash (measuring of integrity), Random Number Generator (RNG), Asymmetric key generation, signing and encryption, Data registers, MAC, and input/output.

Hash is used to measure the integrity where there is no regular structure. Random Number Generation has the capability to build in protection against analysis and attacks. Asymmetric key generation executes RSA coprocessor for speed and low power consumption. Data registers are for storing data. Power detection is used to evaluate the power consumption. And processor is used to read the data. We used the power meter to evaluate the performance of the power detection by our designed power monitor in Fig 2, which shows that during the communication that is transferring and receiving of data the TPM are more exposed to attackers.

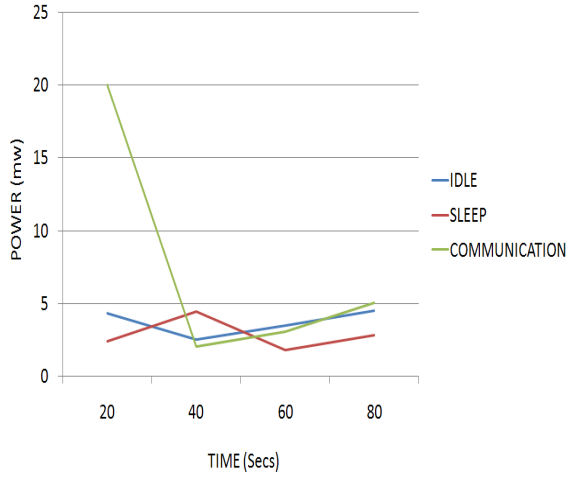


Fig. 3 Evaluation Result

## 5. Conclusions

This paper proposed a methodology for evaluating power consumption and its effects on the TPM device. We observed that the TPM device is exposed more to the attacker during the communication time. This means that data transmission is a very sensitive time for the TPM. Then, after getting our result we propose a design of a power monitor to block the attackers during the communication time.

Our future work will be the implementation of this idea.

## 6. References

1. James Northern, III and Michael Shanblatt; “An Evolutionary Approach to configuring an Embedded System Based on Power consumption”, Proceeding of The 3rd IEEE International Workshop on System-on-Chip for Real-Time Application ISBN 0-7695-1929 2003.
2. M. Tim. Jones, Emulex Corp. "Optimization in GCC", The Linux Journal, January 2005.
3. W. Ye, N. Vijaykrishnan, M. J Irwin and W. Ye, "The design and use of SimplePower: A cycle-accurate energy estimation tool", Proceedings to DAC'OO, June2000.
4. Yu Hu, Qing Li, C.-C. Jay Kuo, “Run-time Power Consumption Modeling for Embedded Multimedia

Systems”; Proceedings of the 11th IEEE International Conference on Embedded and Real-Time Computing Systems an Applications (RTCSA’05) 1533-2306 2005.
5. Smail Niar, Nicolas InglartRapid, “Performance and Power Consumption Estimation Methods for Embedded System Design”; Proceedings of the Seventeenth IEEE International Workshop on Rapid System Prototyping (RSP'06) 0-7695-2580 2006.
6. David A. Ortiz, Nayda G. “SantiagoImpact of Source Code Optimizations on Power Consumption of Embedded Systems”; 978-1-4244-2332 2008.
7. Shuhaizar Daud, R. Badlishah Ahmad, Nukala S. Murhty,”The Effects of Compiler Optimizations on Embedded System Power Consumption”; 978-1-4244-2315, 2008.
8. Trusted Computing Group, TCG Specification Architecture Overview v1.2. 2004. p. 11-12..
9. Trusted Computing Group. TPM Main Part 3 Commands Specification Version 1.2. 2007.
10. www.wikipedia.com