온칩버스를 이용한 악성 회로 공격 탐지 SoC 설계

Kanda Guard · 류광기

한밭대학교 정보통신전문대학원

SoC Design for Malicious Circuit Attack Detection Using on-Chip Bus

Kanda Guard · Kwang-ki Ryoo

Graduate School of Information and Communication, Hanbat National University

E-mail : guardkanda@gmail.com, kkryoo@hanbat.ac.kr

요 약

본 논문에서는 감염된 IP로부터 악성 공격을 감지하고 예방하기 위한 안전하고 효율적인 온칩버스를 기술한다. 대부분의 상호-연결 시스템(온칩버스)은 모든 데이터와 제어 신호가 밀접하게 연결되어있기 때문에 하드웨어 말웨어 공격에 취약하다. 본 논문에서 제안하는 보안 버스는 개선된 아비터, 어드레스 디코딩, 마스터와 슬레이브 인터페이스로 구성되며, AHB(Advanced High-performance Bus)와 APB(Advance Peripheral Bus)를 이용하여 설계되었다. 또한, 보안 버스는 매 전송마다 아비터가 마스터의 점유율을 확인하고 감염된 마스터와 슬레이브를 관리하는 알고리즘으로 구현하였다. 제안하는 하드웨어는 Xilinx ISE 14.7을 사용하여 설계하였으며, Virtex4 XC4VLX80 FPGA 디바이스가 장착된 HBE-SoC-IPD 테스트 보드를 사용하여 검증하였다. TSMC 0.13um CMOS 표준 셀 라이브러리로 합성한 결과 약 26.2K개의 게이트로 구현되었으며 최대 동작주파수는 250MHz이다.

ABSTRACT

A secure and effective on-chip bus for detecting and preventing malicious attacks by infected IPs is presented in this paper. Most system inter-connect (on-chip bus) are vulnerable to hardware Trojan (Malware) attack because all data and control signals are routed. A proposed secure bus with modifications in arbitration, address decoding, and wrapping for bus master and slaves is designed using the Advanced High-Performance and Advance Peripheral Bus (AHB and APB Bus). It is implemented with the concept that arbiter checks share of masters and manage infected masters and slaves in every transaction. The proposed hardware is designed with the Xilinx 14.7 ISE and verified using the HBE-SoC-IPD test board equipped with Virtex4 XC4VLX80 FPGA device. The design has a total gate count of 40K at an operating frequency of 250MHz using the 0.13μm TSMC process.

키워드

Hardware Trojan, SoC, on-chip bus, Malware, AHB Bus, IP

Ⅰ. INTRODUCTION

Silicon Chips are becoming more complex to design, manufacture, fabricate and test. Integrated Circuits (ICs) have gained much success as predicted by Moore's Law. New generations of silicon ICs are becoming smaller and complex in terms of transistor size. Due to this size and complexity , the production process of ICs have become independent. Designers are now able to include third party IPs, outsource and even perform offshore fabrication. With more of the design processes occurring in places where the security of the design cannot be ensured, the questions of the vulnerability of the ICs and its trustworthiness become inevitable.

IC fabrication Issues originated in the military sector with DARPA issuing a Broad Agency

Announcement (BAA) in 2006 and 2007 requesting proposal for the TRUST in Integrated Circuit (TIC) program which talks of IC supply chain problem in [1,2]. A malicious addition /modification to an IC for fraudulent purposes is termed a Trojan Circuit or a Hardware Trojan[3,4]. Figure 1 shows end-users trust chip designers who deliver the final product. Design houses outsource much of its work to lesser known companies. This act introduces semi-trusted and untrusted phases and create the opportunity where attackers can exploit for malicious interest

Trojan attacks then come easy when an outsourced IP is infected and there are no golden models to help identify the flaws in the outsourced IPs before deployment, the malicious circuits gets undetected and the after effect of this can be very costly depending on the kind attack.

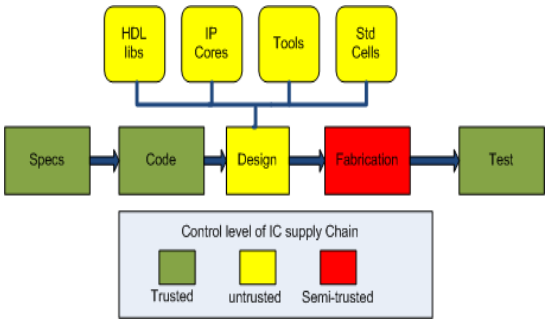

Fig 1. IC Supply Chain

While almost all aspects of an SoC design can be targeted by a Trojan attack, Most of these attackers would rather prefer the system bus where almost all the control and data signals of an SoC is routed. Successful attacks on the bus means the entire SoC is compromised.

This paper proposes architecture modifications that enable the system bus detect and isolate and defend itself against some system interconnect based Trojan attacks.

II. RELATED WORK

Previous works related to this paper are in two broad areas: (a) Works addressing hardware Trojan and (b) those generally addressing the issues of after detection such as reliability and reconfiguration. Category (a) includes publications that handles the methods of hardware malware identification before deployment. A method of voting on an even number of Same IP from different vendors and calculate a Cyclic Redundancy Check (CRC) value for each IP and are voted for the best IP based on least votes[5]. N. Yoshimizu detected hardware Trojan by breaking of symmetries and measuring of the path delay as presented in [6]. Activating a Trojan may sensitize a functional path whose propagation delay is adversely affected by the malicious circuit inclusion. However, the impact of a Trojan on a path delay can be very small. Current integration methodology was used to observe Trojan activity in the circuit and a localized current analysis approach to isolate the Trojan[7]. The presence of a Trojan circuit reflects in the current drawn from the power supply even if no switching occurs in the Trojan circuit hence an extra gate will cause a change in power consumption. B. Khaleghi presents a low-level Hardware Trojan Horse protection scheme for FPGAs by filling the unused resources with proper dummy logic .Category (b) is presented in [8-9].

III. BUS ARCHITECTURE

On-chip buses are not physical buses yet perform the function of inter-connecting modules to enhance smooth communication and information interchange. Several SoC buses such as the AMBA (Advanced Micro-controller Bus Architecture) from ARM, the CoreConnect from IBM, Wishbone from Opencores and STBus from STMicroelectronics come with their various architectures, advantages, and protocols but they all perform the same identical function of basically translating addresses from bus masters to select signals of a bus slave.

Fig. 2 shows a conventional AMBA bus architecture and signal interconnection. Any IP that is capable of sending data is a bus master and any IP capable of providing data is a bus slave. Basically a Master write and a slave performs a read transaction. An IP ready to use the bus will send the HBUSREQ request signal to the arbiter. the arbiter based on some arbitration scheme,(high priority and Fair-Chance round robin) for the purpose of this paper, grants the master the bus with HGRANT. The arbiter also provides HMASTER (master ID) to the M2S mux to ensure the address, data and control information are routed to the slave. Fig. 2 shows the connection of the conventional bus.

The granted master places the address and data to be written on to the bus. the address is decoded into HSEL(slave select) signals to determine the appropriate slave and deliver the data to that slave as in fig 2.

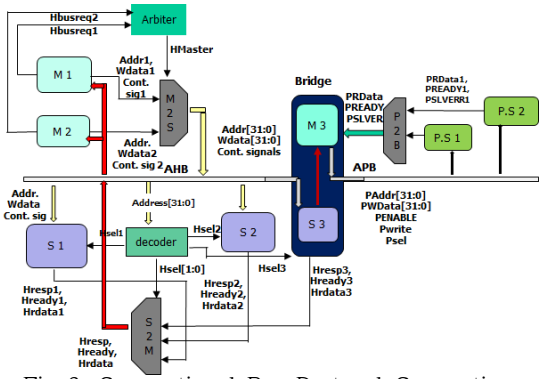

Fig 2. Conventional Bus Protocol Connection

When a master wants to use the bus exclusively, it asserts the HLOCK during bus request. In a Trojan attack, a malicious master can cause this HLOCK signal asserted indefinitely hence depriving other masters the chance to use the bus.

Malicious Lock Detector (MLD) circuit as shown in fig 3, is based on a simple counter is used to detect and isolate a malicious Master in a system. When a particular Master asserts its lock for a predefined amount of clock cycles, the particular Master is flagged as Malicious using the master ID HMASTER. MLD circuit in fig 3 also prevents grants to known Trojan Masters hence the Master ID is registered upon detection.

Other control signals such as the HBURST and the HSIZE are also checked in the same manner to detect if a malicious attack is being carried out on them.

From figure 2, the slave basically has three response signals which it uses to communicate to a master. the HREADY signal is used to add additional cycles to a transaction. A bus operating at 100MHz and a slave operating at 25MHz will need to assert the HREADY signal for four cycles to provide the valid data. Malicious attacks plotted on these signal can result in a system hold up and depriving other bus users access to the bus.

Since the AMBA AHB protocol is pipelined, the HSEL is registerd using the HREADY signal so the final data phase is not lost. Not all, since data is available to all slaves on the bus interface, a malicious master can also have access to data when not part of the current transaction. To avoid this, first of all, the HSEL signal is used as an enable signal to the operation of the FSM on the interface. in this case a slave not selected will not have data being present at its interface. HGRANT, HSEL, HSEL_REG are the main mux select and/or enable signals for routing data and other signals at the Master and Slave Interface.

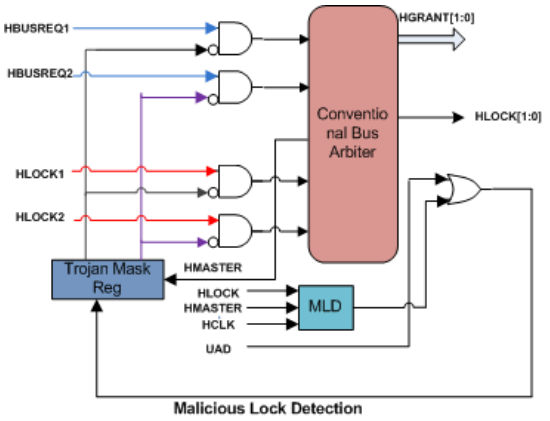

Fig 3. Modified Arbiter

Simple Counters and comparator as that used in fig 3 are used to modify the Slave to Master(S2M) Mux to detect a slave that is being attacked maliciously based on how long its response signals have been asserted. A malicious slave detect signal is sent to the Modified address decoder shown in fig 4. this signal is also used to mask out any slave with the Trojan infested characteristics.

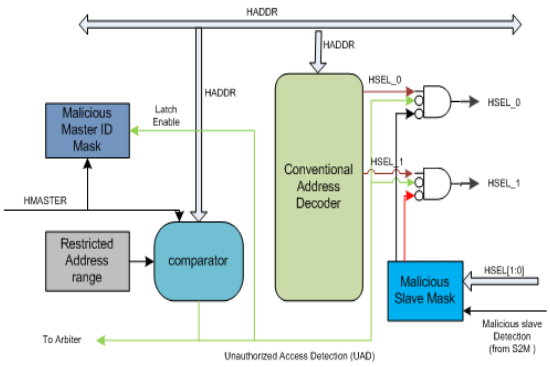

Fig 4. Modified Address Decoder

Furthermore, some restricted area of memory can be specified where only some masters can access, if a master provides a read or write address which is within the range specified, the transaction is quickly masked out and sent to the default slave as shown in fig 4.

Finally, for smaller designs, some security critical IPs can be duplicated if its being outsourced from different sources. the bus is designed to switch from one IP to the next upon detection of an ill operation of the main. This approach will help for smaller systems. even though it will help increase security, it will add an overhead cost and increase total area of the final chip.

IV. EXPERIMENT AND RESULTS

AMBA 3.0 was designed for this experiment. The added security features were tested with an SoC Architecture. The test was performed on HBE-SoC-IPD test board equipped with Virtex4 XC4VLX80 FPGA device. Specific threshold values were set for the security features testing and dummy Trojans were created to keep some signals asserted for as long as the threshold values. Also the bus which is able to reroute was tested with TEA and XTEA encryption algorithm. A simple circuit is used to compare the input data and the output (encrypted data). A Trojan is embedded in one of the encryption IPs (TEA) to cause the output data to be equal to the input data .and if they are same, a trigger is sent to a Switch_Mux module to handle the input output pin switch to the system bus. The modified secure bus architectures were designed with the Xilinx 14.7 ISE, using Verilog HDL and synthesized with Synopsys' Design Compiler using TSMC 0.13μm cell library. Table 1 shows the results of the conventional and modified architectures

TABLE 1: IMPLEMENTATION RESULT

Section	Conv. bus	Modified bus	% Incr
Process(TSMC)	0.13μm	0.13μm	-
Frequency	250MHZ	250MHz	-
Area(K gate)	31K	40K	29

V. Conclusion

This paper proposes solutions and architectures that provide some level of resistance and detection to on chip system bus. Though this modified architecture causes some overhead cost and increase in area as compared to the conventional architecture, it is worth the security it provides.

Acknowledgement

This research was supported by the Ministry of Science, ICT and Future Planning(MSIP), Korea, under the Global IT Talent support program (IITP-2015-R0134-15-1019) supervised by the Institute for Information and Communication Technology Promotion(IITP)

References

[1] DARPA BAA 07-24-solicitations-microsystem s technology office. http://www.darpa.mil/MTO/solicitations/baa07-24/index.html, 2007.
[2] S. Adee, The hunt for the kill switch, Spectr. IEEE 45 (5) May (2008) 34--39.
[3] G. Bloom, E. Leontie, B. Narahari, R. Simha. Hardware and Security: Vulnerabilities and Solutioins.
[4] S Bhunia, M.S.Hsiao, Mainak B, and Seetharam N "Hardware Trojan Attacks - Threat Analysis and Countermeasures"
[5] Amr Al-Anwar, Yousra Alkabani, M. Watheq El-Kharashi, Hassan Bedour "Hardware Trojan Detection Methodology for FPGA" IEEE PACRIM,sept 2013
[6] Yoshimizu N "Hardware Trojan Detection By Symmetry Breaking In Path Delays"IEEE international Symposium on Hardware-OrientedSecurity and Trust(HOST),April 2014
[7] Xiaoxiao Wang, H Salmani, M Tehranipoor and J Plusquellic "Hardware Trojan Detection and Isolation Using Current Integration and Localized Current Analysis" IEEE DFTVS'08
[8] Lok-Won K, J. D. Villasenor, "Dynamic Function Replacement for System-on-Chip Security in the Presence of Hardware -Based Attacks"IEEE Trans on Reliability
[9] Lok-Won K, J. D. Villasenor, "A System -On-Chip Bus Architecture for Thwarting Integrated Circuit Trojan Horses" IEEE transaction on VLSI, Oct, 2011