01 Apr 2008

Secured Hardware Design - an Overview

S. Burugapalli

Waleed K. Al-Assadi

Missouri University of Science and Technology, waleed@mst.edu

Secured Hardware Design – An Overview

Sasikiran Burugapalli and Waleed K. Al-Assadi, Senior Member, IEEE
Department of Electrical and Computer Engineering,
Missouri University of Science and Technology
Rolla, MO 65409-0040

***Abstract*-Security is a prime concern in the design of a wide variety of embedded systems and security processors. So the customer security devices such as smart cards and security processors are prone to attack and there are on going research to protect these devices from attackers who intend to extract key information from these devices. Also an active attacker can induce errors during computation and exploit the faulty result to extract the key information embedded in the processor. Due to the design time issues weakness in the design is often revealed in the manufactured chips. Also because the post-manufacture security evaluation is time consuming and expensive, these security issues have to be considered at the design phase. This paper outlines some of the hardware attacks and provides a general idea of the process of these attacks.**

Keywords: Hardware Attack, Optical Probing, Thermal Attack, Electromagnetic Attack, Timing Attack, Soft Errors

I. INTRODUCTION

Similar to the virus attacks on the software, hardware can also be attacked by either insertion of the malicious logic into the circuit or by the malicious attack on the integrated circuit. Malicious logic can be inserted at different levels of abstraction in the supply chain architecture of the semiconductor IC. Also these days most of the complex digital circuits use third party Intellectual property (IP) blocks, instead of designing the circuit from the scratch which saves lots of work and time [1]. These IP blocks are themselves are untrustable as they may contain malicious code incorporated into them thus affecting the trustability of the entire system. Also another source of malicious logic injection is through the CAD tools which were used to design the hardware. These CAD tools themselves may contain software virus or a bug which will insert the malicious logic into the design.

Further more many opportunities exist for the introduction of the unwanted features into the IC during the design cycle [3]. Although some of the phases in the supply chain structure of an ASIC design are trusted due to the fact that they are under the designer's control, most of the phases are untrusted. So it is up to the end user to rely on the trustability of the hardware.

The malicious logic can lead to various unwanted scenarios like causing the system to output data to the wrong port or address (information leakage), monitoring and modifying the system's output data (tampering), or disabling the system by changing the system's internal timing or control, e.g., holding the clock or bus (denial of service). All these can be done by changing or adding internal logic in such a way that it is very unlikely to be detected by traditional testing and verification tools and techniques [2].

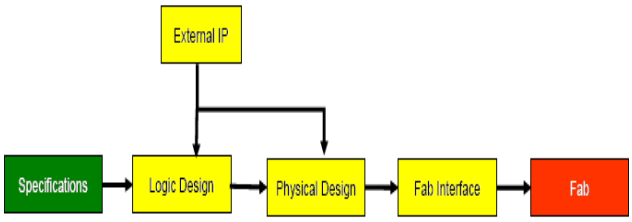

Fig. 1: ASIC design flow [3]

Different types of malicious logics are Trojan horse, trap door, logic bomb etc. A Trojan horse when invoked covertly performs some other action while performing its intended action, while a trap door is a secret entry into the program that allows some one who is aware of it to gain access to the program with out actually passing through the usual security procedures and logic bomb is a piece of code embedded in a legitimate program which becomes active at a predefined time or if a certain event is occurred.

As the technology is ever growing the usage of small hand held security devices is ubiquitous and they rely on a greater extent on the tamper resistance property of these devices. However these tamper resistance is not outright. An attacker having access to the semiconductor test equipment can easily retrieve the key information in the chip by any of the methods wide known. It was believed that given sufficient investment any chip can be tampered. So the level of tamper resistance offered by any chip is can be measured by the time and cost penalty. A number of less expensive attack techniques are also known [14].

In this paper we discussed various types of hardware attack techniques and possible remedies proposed by authors.

II. TYPES OF ATTACKS

A. Soft Errors

In earlier days chip manufacturing components contains

978-1-4244-2077-3/08/$25.00 ©2008 IEEE.

small amounts of radioactive contaminants. The decay of these contaminants cause the soft errors due to the emission of high energy particles like alpha particles. The other sources of soft errors are neutrons, cosmic rays etc. when these high energy particles interact with the semiconductor electron-hole pairs will be generated. For an alpha particle is interacted with silicon, an energy of 3.6 eV is lost for every electron hole pair created [4] thus causing charge deposition. The number of electron hole pairs created depends on the energy of the sub atomic particle. Transistor source and diffusion nodes can collect these charges. If the charge collected is sufficiently high then that may invert the state of a logic device such as an SRAM cell, a latch, or a gate thereby introducing a logical fault into the circuit's operation. [5].

Impact on circuits [6]

An error due to a hit of a single particle was termed a single event upset (SEU). Its effects are temporary that lasts about 100ps and may corrupt the data stored and computed. For example consider an SRAM memory cell as shown in fig. 2. When the word line is low, the data will be stored in the cell using the inverters which are connected back-back. Now if an energetic particle strikes the cell and causes to flip one of the nodes, which in turn will be propagated to the other node causing both nodes to flip through a regenerative action. This way the data in the memory cell will be changes and the only way to get back to original state is to rewrite the content through the bit lines and this is not an ideal solution.

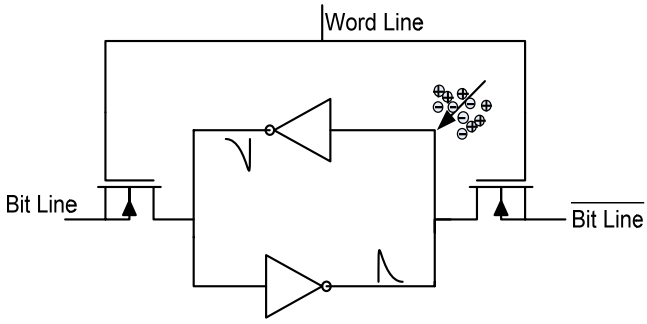

Fig. 2 : SRAM Cell

Soft errors can also be caused due to a particle interaction on the bit lines. In DRAM, in addition to the cell and bit line failure modes, another mode called combined cell bitline (CCB) failure mode is observed [7]. It was seen when both the cell and bitline collects the charge induced by the radiation but is insufficient to cause a SEU. Medium and Low end servers are largely affected by this soft error problem.

B. Optical probing

Optical probing is a semi-invasive method, which means it requires depackaging of the chick like invasive attacks but the passivation layer remains intact and because this method does not require electrical contact to the silicon and hence there is no mechanical damage to the silicon [8]. Laser radiations can ionize the IC's semiconductor region if the photonic energy is greater than the band gap of the semiconductor. So by precisely focusing the Laser on to an

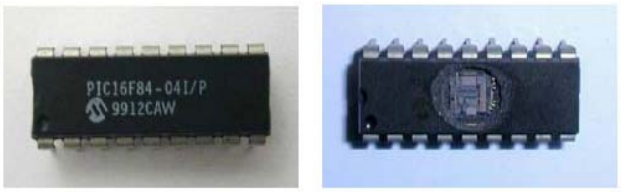

Fig. 3: Microcontroller before and after depackaging.

appropriately selected transistor on the chip, its state can be changed and there by corrupting the data stored. For example consider an attack on the typical SRAM memory. A standard depackaging procedure is applied on the chip to expose the SRAM memory and the results of depackaging are as shown in Fig. 3 [8].

Now using a probing station the laser light can be focused very precisely on a precisely selected SRAM cell (magnified to about x1500) and the final state of the cell depends on the exposed layer. So by this way any individual bit of the SRAM cell can be changed. In other words, laser is used to induce a transient fault in one or more gates in such a way as to cause information leakage.

These days this is the most powerful attack because unlike a glitch attack, the attacker can choose the location of the attack very precisely [13].

C. Electromagnetic attack [9]

Electromagnetic induction can be used to scan the data in the semiconductor. For this a miniature inductor can be built by wrapping several hundred turns of fine wire around the tip of the microprobe needle. When a current in injected into this coil, a magnetic field which is concentrated around the needle of the microprobe is generated. Now eddy current can be generated on the memory element when this test probe is placed a few microns over the surface of the element. These local currents in turn can be used to create faults. A map of the chip can be created by sensing this eddy current using an eddy current sensor [10]. A small perturbation on the memory cell using the same sensor is created to move the polarization point of the transistor a little [9]. Depending on the intensity of current required by the memory element to return to the initial value of the polarization point, the zero and one states can be identified.

D. Thermal attack [11]

Security processors handle very sensitive information which was not supposed to be read out or changed by any one. So these processors employ a volatile memory to store

this fragile information. On detection of a tampering attack these memory chips are powered down so that it can not be read by an attacker. But the problem here is if the data retention time of the chip is longer than the time taken by the attacker to read out the data, then obviously the sole purpose of security processor is doomed.

The data retention time of the SRAM depends on the temperature. It was believed that at about -20ºC the data in the memory element is frozen which can be retrieved by the attacker. So some devices are designed with temperature sensing equipment which interprets any temperatures lower then -20ºC as a tampering event and shuts down the memory cell, there by erasing the secret keys stored. So an attacker who can get access to this location can subject the process to a lower temperature and causing the entire system to power down there by incurring heavy loss to the organization. Another point that has to be taken into consideration is that the data retention time in these processors depends on the temperature, i.e. the lower the temperature the greater the data retention period. Experiments proved that when a DRAM is subjected to a temperature of liquid nitrogen, the data decay is only 0.17% when isolated from the power [18]

E. Glitch attack

Clock signal glitches are currently the simplest and most practical glitch attacks. An attacker intentionally increases the clock frequency temporarily so that some flip-flops at the slower portion of the circuit fail to respond thus causing an error. This is particularly used to attack some part of the circuit because of different number of gate delays in various paths of the circuit. The effect of the attack depends on the timing and the duration of the glitch. For example in a CPU generally the program logic is much simpler than the instruction unit [15]. So any increase in the frequency causes instruction cycle to skip and instruction execution. This skipped instruction can be precisely chosen to be a password verification step or rather a crucial step. So by this way an attacker with a malicious intention can get access to valuable data. In addition these glitch attacks can reduce the run time of the cryptographic algorithm, so that the cipher can be decrypted easily [15].

F. Timing attack

Timing attack exploits the fact that the execution time of the cryptographic computation depends on the data that was being computed. So by analyzing the time taken by this computation the crypto key can be inferred [12, 16]. Since the instructions take a different number of cycles depending on the data inputs, a wide range of timing data is collected and analyzed to infer the crypto key [12].

III. COUNTERMEASURES

Similar to electrical fencing protection for houses, a metal layer is deposited on top of the actual circuit so that this metal layer can act as a sensor mesh. All the paths in the sensor mesh are continuously monitored for any interruption and short circuits [11]. This prevents selective etching and laser cutting accessing the bus which contains data. When an interruption or a short circuit is detected, mesh alarm can be triggered and countermeasures are initialized. Such meshes also make the penetration to the lower levels very difficult and thus complicating automatic reconstruction of the chip. But there are some limitations for using these sensor meshes as explained by [11].

Another defense approach proposed is chip coating. In this approach, a top layer metal shield is used to reflect the incident light thus making optical attack more difficult. Light sensors can also be used to detect a de-capsulated chip and prevent it from functioning.

Mitigation techniques for single event upsets are classified as system-level methods (error detection and correction, lockstep execution, and redundant systems) and circuit level methods (radiation hardened circuits). The disadvantage of these techniques is they increase the transistor count and the area overhead [17] and this is because of the presence of additional circuitry on the chip. Another error correction design called Built-in soft error resilience (BISER) effectively overcomes this area overhead problem by utilizing the on chip resources such as on-chip scan design-for-testability for soft-error protection during normal operation [19].

The technique to protect from non-invasive attack is by using randomized clock signal. To protect the circuit from timing attacks the internal clock is driven by a random bit-sequencer which in turn is driven by an external clock. It is also necessary for the processor to show an even characteristic current activity during the delay phases of the random clock else it is possible to construct the internal clock from the consumed current [11].

The suggested counter measure for the thermal attack is to redesign the SRAM that looses their state quickly when the power is removed even at lower temperatures. Another approach is to scatter the vital information such as passwords and crypto keys while storing in the RAM.

IV. CONCLUSION

In this paper we analyzed various ways in which the malicious attacks can be performed on the embedded hardware. We also presented a basis which makes microcontrollers easy to penetrate and gather required information. We also presented some counter measures along with their limitations. Although some of the attacks like soft errors which may not be controlled completely at the design phase of the hardware, counter measures for most of the other attacks were widely available and can be implemented considering the tradeoffs associated with the development of particularly robust and secure hardware.

Because the post-manufacture security evaluation is time consuming and expensive a proper security protocol has to be considered at the design level of the hardware.

REFERENCES

[1] J. Di and S. C. Smith, "A Hardware Threat Modeling Concept for Trustable Integrated Circuits," *IEEE Region 5 Technical Conference*, April 2007

[2] S. C. Smith and J. Di, "Detecting Malicious Logic Through Structural Checking," *IEEE Region 5 Technical Conference*, April 2007.

[3] DARPA, "Failure mode of radiation-induced soft errors in dynamic memories," Electron Device Letters, IEEE , vol.9, no.12, pp.644-646, Dec 1988

[4] S. L. Miller, "Ionization rates for holes and electrons in silicon", *Physics Review,* Feb. 1957.

[5] Mukherjee, S.S.; Emer, J.; Reinhardt, S.K., "The soft error problem: an architectural perspective," High-Performance Computer Architecture, 2005. HPCA-11. 11th International Symposium on , vol., no., pp. 243-247, 12-16 Feb. 2005

[6] Karnik, T.; Hazucha, P., "Characterization of soft errors caused by single event upsets in CMOS processes," Transactions on Dependable and Secure Computing , vol.1, no.2, pp. 128-143, April-June 2004

[7] Rajeevakumar, T.V.; Lu, N.C.C.; Henkels, W.H.; Hwang Wei; Franch, R., "A new failure mode of radiation-induced soft errors in dynamic memories," *Electron Device Letters, IEEE* , vol.9, no.12, pp.644-646, Dec 1988

[8] Skorobogatov, S. P. and Anderson, R. J. 2003. Optical Fault Induction Attacks. In *Revised Papers From the 4th international Workshop on Cryptographic Hardware and Embedded Systems* (August 13 - 15, 2002). B. S. Kaliski, Ç. K. Koç, and C. Paar, Eds. Lecture Notes In Computer Science, vol. 2523. Springer-Verlag, London, 2-12.

[9] Samyde, D.; Skorobogatov, S.; Anderson, R.; Quisquater, J.-J., "On a new way to read data from memory," *Security in Storage Workshop, 2002. Proceedings. First International IEEE* , vol., no., pp. 65-69, 11 Dec. 2002

[10] Gomez, J.; Esteve, D.; Simonne, J., "A CMOS eddy current sensor for microsystems," *Devices, Circuits and Systems, 2000. Proceedings of the 2000 Third IEEE International Caracas Conference on* , vol., no., pp.I54/1-I54/4, 2000

[11] Kömmerling, O. and Kuhn, M. G. 1999. "Design principles for tamper-resistant smartcard processors," *Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology* (Chicago, Illinois, May 10 - 11, 1999). USENIX Association, Berkeley, CA, 2-2.

[12] Ravi, S.; Raghunathan, A.; Chakradhar, S., "Tamper resistance mechanisms for secure embedded systems," *VLSI Design, 2004. Proceedings. 17th International Conference on* , vol., no., pp. 605-611, 2004

[13] Chong Hee Kim; Quisquater, J.-J., "Faults, Injection Methods, and Fault Attacks," *IEEE Design & Test of Computers* , vol.24, no.6, pp.544-545, Nov.-Dec. 2007

[14] Anderson, R. J. and Kuhn, M. G. 1998. Low Cost Attacks on Tamper Resistant Devices. In *Proceedings of the 5th international Workshop on Security Protocols* (April 07 - 09, 1997). B. Christianson, B. Crispo, T. M. Lomas, and M. Roe, Eds. Lecture Notes In Computer Science, vol. 1361. Springer-Verlag, London, 125-136.

[15] David Naccache, "Finding Faults," *IEEE Security and Privacy* ,vol. 3, no. 5, pp. 61-65, September/October, 2005.

[16] Kocher, P. C. 1996. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In *Proceedings of the 16th Annual international Cryptology Conference on Advances in Cryptology* (August 18 - 22, 1996). N. Koblitz, Ed. Lecture Notes In Computer Science, vol. 1109. Springer-Verlag, London, 104-113.

[17] Dodd, P.E.; Massengill, L.W., "Basic mechanisms and modeling of single-event upset in digital microelectronics," *Nuclear Science, IEEE Transactions on* , vol.50, no.3, pp. 583-602, June 2003

[18] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten, "Lest We Remember: Cold Boot Attacks on Encryption Keys," http://citp.princeton.edu/pub/coldboot.pdf

[19] Mitra, S.; Seifert, N.; Zhang, M.; Shi, Q.; Kim, K.S., "Robust system design with built-in soft-error resilience," Computer , vol.38, no.2, pp. 43-52, Feb. 2005