DESIGN AND DEVELOPMENT OF HARDWARE AND SOFTWARE FOR COUNTERING FAULT INJECTION ATTACKS

K. SUBBA RAO, JKR SASTRY
K L University, Vaddeswaram, Green Fields, Guntur District, PIN-522502
director.anqc@kluniversity.in

ABSTRACT
One of the side channel attacks which is considered as a threat for embedded system is Fault injection attack. Fault injection attack is defined as an attack which requires the injection of some sort of fault during the operation of the target system. Fault injection attacks rely on varying the external parameters and environmental conditions of a system such as the supply voltage, clock, temperature, radiation, etc., to induce faults in its components. Faults can be induced into the embedded system by Variations in supply voltage, Variations in the external clock, White Light, Laser, Glitches and Fault injection by radioactive particles. The attacking mechanism considered here is Latch up effect which occurs because of sudden variations in supply voltage. The methods for countering these attacks are presented and discussed along with the design and development of both hardware and software.

1. INTRODUCTION TO FAULT INJECTION ATTACKS
These attacks require the injection of some sort of fault during the operation of the target system. These attacks mainly aim at extracting useful information from a target system by injecting faults. Fault injection attacks rely on varying the external parameters and environmental conditions of a system such as the supply voltage, clock, temperature, radiation, etc., to induce faults in its components. The injected faults can be transient or permanent, and can compromise the security of a system in several ways.

Attacking Mechanism through a fault injection attack through triggering of a parasitic thyristors
Latch up is a mechanism existing potentially in any CMOS structure which results from the triggering of a parasitic thyristor. This process includes developing a low resistance path and a high current between power and ground. If current is not limited, it is able to induce irreversible damage of the component. Latch up phenomenon description: Latch up results from the triggering of a parasitic thyristor (p-n-p-n) structure inherent in CMOS inverters as shown in figure 1.

![Figure 1: Latch up phenomenon in CMOS IC](image)

It consists of two bipolar transistors in a feedback loop configuration. If a sufficient quantity of charges is deposited in the substrate, after these charges reach the reversed biased well/substrate junction, the (p-n-p-n) structure can turn on and allow the passage of a strong current between the supply contact and the ground.

![Figure 2: Variation of the current as a function of the applied Voltage](image)

Vhold corresponds to a threshold value below which it is not possible to establish a latch up in the structure. Above its value, for a given voltage, there are two different current states:
1. Low current, it corresponds to the normal operation mode (blocked state of the thyristor)
2. High current, it corresponds to latch up (low impedance state of the thyristor). When the operating voltage exceeds Vtrig, an electrical latch up is triggered as shown in Fig.2.

1.1 Overview

There are different counter attacking mechanisms in order to counter fault injection attacks and the counter attacking mechanism varies with the attacking mechanism. The attacking mechanism considered is latch up effect. Latch up is quantified for dc, ac and transient phenomena. The effects caused by latch up effect are severe in nature and they may even lead to breakage of the chip.

Following methods can be used to counter latch up effect:
1. Decoupling of parasitics – spatial separation: To avoid the interaction between the pnp and the npn transistor, spatial separation of the parasitic transistors inherently increases the latch up robustness.
2. Decoupling of parasitics – physical isolation (triple well): To avoid interaction between the pnp and the npn parasitic transistors, full decoupling can be achieved by physical separation using other structures between the transistors.
3. Semiconductor doping – high doping concentration: The semiconductor region can be doped in order to reduce the bipolar current gain through reduction in the minority carrier diffusion length. This can be achieved by reduction in both recombination time and minority carrier mobility.
4. Isolation design: The semiconductor isolation design can be optimized to improve the latch up robustness of the semiconductor technology.
5. Active guard rings – inversion of injection: Active guard rings can sense the potential of the substrate and using an inverting amplifier invert the potential response for latch up advantages.

All the above methods are to be implemented during manufacturing the chip which makes the design complex and more over these are not cost effective. So we externally introduce a current limiting circuit in order to limit the high currents. These current limiting circuits are simple in nature and are economical.

1.2 Requirements engineering for countering fault injection attack - Flow Requirements

1. Connect the hardware circuit diagram according to the developed hardware architecture.
2. The reset pin of the crypto server is set in order to start the process.
3. Using the LCD display a prompt is given to the user to enter the password and to swipe the smart card.
4. Enter the pin number through the key board interface.
5. The encryption is made for the data entered and is sent to the host interface.
6. The encrypted data is written on to the LCD.
7. The host decrypts the entered data and verifies whether the entered pin number is a valid one or not.
8. If the pin number is not a valid one it then displays a message for the user that the entered pin is not a valid one.
9. If the pin is a valid one then access is provided to start the TMCNRS.
10. Power flows from the power supply to the supply pin of the crypto server. This rated power supplied is utilized for the functioning of the crypto server under normal conditions.
11. For injecting a fault into the system we externally introduce an additional power supply in parallel with the existing power supply.
12. By sudden variations in the external power supply, voltage variations occur and parasitic thyristors are formed which leads to short circuit path.
13. To limit these high currents into the circuit we introduce a current limiting circuit. This current limiting circuit is arranged in such a way that it acts as feed back to the supply pin of the crypto server.
14. Whenever there is a flow of high currents into the crypto server, the current limiting circuit senses these currents and limits these currents so that normal operation is attained.
15. If the current is not in the limiting range of current limiting circuit buzzer should get activated to indicate that the latch up condition is persisting in the system.

2. FUNCTIONAL REQUIREMENTS

1. The current limiting circuit should regulate the supply before the initiation of latch up effect
2. A comparator shall be used in the current limiting circuit in order to compare the current flowing in the circuit with the reference current. It should be able to respond to the attack within 100milli seconds.

Use case Modeling

The Requirements projected in the above sections are modeled through Use Case modeling Language. Fig 3 depicts fault injection countering through current limiting circuit connected to the crypto server.

The user resets the crypto server through the reset pin. The prompt is displayed on the LCD. Then the smart card must be swiped on to the smart card reader which is one of the authentication mechanisms provided to the
TMCNRS. A valid password must be entered through the keyboard interface. The entered data is encrypted in the crypto server and is sent to the host for the validation. The encrypted data is written on the LCD.

![Flow Diagram](image)

Fig 4.1 Flow Diagram

![Use case modeling fault injection counter attacking mechanism](image)

Fig 3 Use case modeling fault injection counter attacking mechanism

Host decrypts the data and compares with the valid data. If the entered data matches with the reference password access is given to the TMCNRS. If not invalid status is displayed on the LCD. Input supply to the crypto server is provided externally. It is varied by using regulated power supply which is connected to the power supply.
This variation in supply results in the latch up phenomenon which results to the flow of high currents in the circuit. To avoid this effect, we are placing a current limiting circuit. This circuit limits the currents up to a pre-specified range. Whenever currents exceed this range, buzzer is set to activate.

3. HARDWARE ANALYSIS AND DESIGN FOR COUNTERING FAULT INJECTION ATTACK

The counter attacking system is presented through a hardware design to develop a Knowledge base and through a separate system using which the actual attacking is performed through usage of the Knowledge based systems. The hardware design of the experimental setup is presented through design of architecture, Component description and interaction among the various hardware components.

Crypto server power characteristics are known by connecting a one milli ohm resistor in series to the power supply pin (Vcc) of the oscillator. The voltage across the resistor is amplified using a differential amplifier (LM741CN). The amplification factor for the difference amplifier is approximately 2 lakhs under ideal conditions. The output voltage of the difference amplifier is compared to a reference value which is predetermined by calculation.

Whenever the current consumption exceeds from the normal value the output of the difference amplifier is set high or low (which depends on the configuration of the difference amplifier i.e. inverting or non-inverting respectively). The output of the difference amplifier is set to activate the buzzer or a signal is sent to the interrupt pin of the microcontroller.

3.1 Hardware Architectural Diagram

Fig 4 shows the block diagram which represents both attacking and counter attacking mechanisms for crypto server. Under normal operating conditions switch across the regulated power supply is opened and the crypto server gives correct encrypted data. In order to introduce faults in the output of the crypto server we are introducing regulated power supply in order to change the input supply to the crypto server. To introduce faults we close the switch across the regulated power supply and supply is varied. When the system is attacked encrypted output of the crypto server changes. This erroneous encrypted data which can be observed in LCD. So, a counter attacking mechanism is introduced such that the effect of regulated power supply is nullified.

To limit the high currents produced due to latch up, we introduce a current limiting circuit as the counter attacking mechanism. Current limiting circuit consists of operational amplifiers and comparator circuits. A...
reference voltage value is given to the circuit initially. When the voltage value is less than the reference value the circuit works under normal conditions. Under abnormal conditions when there is a sudden change in voltage latch up occurs which leads to the formation of parasitic thyristors and hence short circuit condition arises. Due to this short circuit, a huge amount of current flows in the circuit. Then the voltage value is greater than the reference value. This fault makes the switch across the current limiting circuit to close and it comes into operation by activating the buzzer and sends a signal to the interrupting pin of the crypto server to reset the power supply.

3.2 Hardware Component Description
The Hardware components have been analyzed by referring to the components that are marketed by different Manufacturers through WEB.
A detailed investigation is made by referring to the principal of operation, functional specification, features, timing etc. The following is the tabulation of the Hardware components selected at the Analysis Stage.

<table>
<thead>
<tr>
<th>Component Number</th>
<th>Description</th>
<th>Purpose</th>
<th>Latency Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>comparator</td>
<td>To compare current flows in the circuit</td>
<td></td>
<td>100 milliseconds</td>
</tr>
<tr>
<td>P89C51RD2</td>
<td>8 Bit Flash crypto server</td>
<td>8 Bit CISC 8051 Core for encrypting the smart card data and keyed in user name and password</td>
<td>100 milliseconds</td>
</tr>
<tr>
<td>VN410</td>
<td>Buzzer</td>
<td>To activate user under attacked conditions</td>
<td>30 milliseconds</td>
</tr>
<tr>
<td>LM741CN,LM358AD</td>
<td>Operation amplifier</td>
<td>To amplify difference between voltages</td>
<td>100 nanoseconds</td>
</tr>
<tr>
<td>LM741CN</td>
<td>comparator</td>
<td>To compare the voltages</td>
<td>100 nanoseconds</td>
</tr>
</tbody>
</table>

Table 1 Description of Hardware elements in counter attacking mechanism

3.3 Hardware component Interaction for Fault Injection
Fig 5 shows the hardware interaction design for countering the fault injection attack. Crypto server is interfaced with key board and smart card reader in order to allow user to enter the validate password and to swipe a smart card. Keyboard gives analog outputs which are converted to digital using an A/D converter. The entered data is encrypted by the crypto server and is given to the host for verification purpose. The encrypted output is written on to the LCD.
Input supply to the crypto server is provided externally. It is varied by using regulated power supply which is connected to the power supply. This variation in supply results in the latch up phenomenon which results to the flow of high currents in the circuit. To avoid this effect, we are placing a current limiting circuit. This circuit limits the currents up to a pre specified range. Whenever currents exceed this range, buzzer is set to activate.

Fig 5 Hardware Class Diagram for countering Fault Injection attack
4. SOFTWARE DESIGN FOR COUNTERING FAULT INJECTION ATTACK

4.1 Software Architecture Design for countering Fault injection attack

Fig 6 shows the software architecture design for the fault injection attack. Here a smart card reader and a key board interface are provided to the crypto server. LCD is also interfaced in order to make user aware of the process going on in the crypto server. Host interface is provided to the crypto server in order to compare the entered password with the reference password. When the password is entered through the key board crypto server encrypts it and writes it on to the LCD. After the authentication process is completed user will be given access to the TMCNRS.

4.2 Software Component Description for countering Fault injection attack

The software part of the attacking system constitutes three processing locations which include TMNCRS System, HOST System, and Crypto server System. Each of the locations built with the components that provide a platform for implementing the attacking system.

**TMNCRS System**

This system has one interfacing component apart from the applications that helps establishing communication with the crypto server using RS232C communication protocol.

**HOST System**

This system has one interfacing component apart from the applications that helps establishing communication with the crypto server using RS232C communication protocol.

**Crypto server system**

The crypto server system has the components that help in interfacing with both the TMNCRS and HOST based systems using RS232C interface protocol. Further the system has components that help dealing with the Keyboard for inputting the PIN number, inputting the MAC access code through Smart Card, and for writing output onto LCD.

**LCD manager component**

The LCD Manager helps in writing the output on the multiline multi column display. This component has functions that help in initializing the LCD, Writing commands and data, and checking the busyness of the LCD. The LCD is interfaced to the Micro Controller

**Keyboard manager component**

Keyboard manager takes input from 4 x4 matrix key board. This component is used for entering the PIN number of the smart card which is used for providing access to the user. This component is responsible for entering the reference temperatures to the TMCNRS. This is interfaced through I2C communication.

**Smart card manager component**

Smart card manager reads the data stored on the magnetic strip of the smart card and sends the encrypted data to HOST system. This smart card code is sent to the crypto processor for decryption. This code is sent to the HOST system for verification purpose thus providing authorization for the user. The PIN number entered
through the KEY board is bid with the MAC code by the crypto server, encrypted and sent to HOST. At HOST the encrypted code is decrypted and a verification about the validity of the code is undertaken and a message is passed to the crypto server about the authenticity of the code.

4.3 Software Component Interaction design for countering Fault injection attack

Fig 7 shows the software interaction design for the fault injection attacking mechanism. Crypto server is interfaced with the smart card reader and the key board interface. The key board output is analog so it is converted to digital using A/D converter. The input data is encrypted by crypto server and is written on to the LCD. Encrypted data is given to the host interface and is compared with the reference password. On entering the correct password the reset pin of the main micro controller is set high by the crypto server.

4.4 Software and Hardware Integration design for countering fault injection attack

Fig 4.6 shows the hardware and software interaction design for countering the fault injection attack. Crypto server is interfaced with keyboard and smart card reader in order to allow user to enter the validate password and to swipe a smart card. Keyboard gives analog outputs which are converted to digital using an A/D converter.

The entered data is encrypted by the crypto server and is given to the host for verification purpose. The encrypted output is written on to the LCD. Input supply to the crypto server is provided externally. It is varied by using regulated power supply which is connected to the power supply. Crypto server is interfaced with the smart card reader and the key board interface. The key board output is analog so it is converted to digital using A/D converter. The input data is encrypted by crypto server and is written on to the LCD.

Encrypted data is given to the host interface and is compared with the reference password. On entering the correct password the reset pin of the main micro controller is set high by the crypto server. After the authentication process is completed user will be given access to the TMCNRS. When the value of supplied voltage to the crypto server varies which results in latch up effect. Latch up effect leads to the formation of parasitic thyristor in the CMOS structure which results in the establishment of large value of current between the power supply and the ground and result in the damage of the chip or even loss of the sensitive information. Due to latch up effect encrypted output of the crypto server changes which can be seen on the LCD. To avoid this effect, we are placing a current limiting circuit .This circuit limits the currents up to a pre specified range. Whenever currents exceed this range, buzzer is set to activate.

4.5 Testing

4.5.1 Simulating the Fault Injection Counter attacking System

We are replacing the crypto server with the oscillator circuit as both are same types of loads and have the same voltage and current characteristics. An oscillator based on operational amplifier (LM358AD) is being used as a load and it’s power characteristics are known by connecting a one milli ohm resistor in series to the power supply pin (Vcc) of the oscillator. The voltage across the resistor is amplified using a differential amplifier (LM741CN).

The amplification factor for the difference amplifier is approximately 2 lakhs. The output voltage of the difference amplifier is compared to a reference value which is predetermined by calculation. When ever the
current consumption exceeds from the normal value the output of the difference amplifier is set high or low (which depends on the configuration of the difference amplifier i.e. inverting or non-inverting respectively). The output of the difference amplifier is set to activate the buzzer or a signal is sent to the interrupt pin of the microcontroller.

Fig 8 Software and Hardware Integration design for countering fault Injection Attack

### 4.5.2 Simulation results

Under normal conditions when the rated supply voltage is given, no latch up condition occurs and the obtained value is less than the reference value. So, the circuit works under normal operating conditions. When additional voltage is given to the system latch up condition arises in the circuit and high currents flow through the circuit. A voltage corresponding to the developed current is generated and then amplified. This amplified value is compared with the reference value in the difference amplifier. As the difference is negative it gives an output of $-V_{sat}$ which activates the buzzer. Buzzer is provided for the user identification.

Tabulated results for simulation:

<table>
<thead>
<tr>
<th>S.NO.</th>
<th>$V_{input}$ (volts)</th>
<th>$V_{output}$ (volts)</th>
<th>Circuit condition</th>
<th>State of the buzzer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>5v</td>
<td>+3.661</td>
<td>Normal operating condition</td>
<td>Not activated</td>
</tr>
<tr>
<td>2.</td>
<td>6.5v</td>
<td>-5.016</td>
<td>Fault condition</td>
<td>Activated</td>
</tr>
<tr>
<td>3.</td>
<td>7v</td>
<td>-5.479</td>
<td>Fault condition</td>
<td>Activated</td>
</tr>
</tbody>
</table>

Table 2 Simulation Results after Counter attacking the Fault Injection Attack

From the above results it could be seen that under normal operating conditions the current limiting circuit will not operate and under faulty conditions i.e., change in power supply can be nullified by activation of current limiting circuit and buzzer will be activated for the user identification.

### CONCLUSION AND SUMMARY

Today, secure embedded system design remains a field in its infancy in terms of research and pervasive deployment. Although historically, various security issues have been investigated in the context of cryptography, network security and computer security, the challenges imposed by the process of securing emerging environments or networks of embedded systems compel us to take a fresh look at the problem. Security is not usually taken into account during the design phase of the product and it is difficult to implement once the product is completed. Security should be integrated into the product during the conceptual design phase.
and should be taken into account for every part of the design. As 100% security does not exist, an attacker having enough time, resources and motivation could always break into any system. For this reason, manufacturers must secure their products against specific threats trying to achieve a balance between the cost of security implementation and the benefits obtained. We believe that a combination of advances in architectures and design methodologies would enable us to scale the next frontier of embedded system design, wherein, embedded systems will be “secure” to the extent required by the application and the environment. To realize this goal, we should look beyond the basic security functions of an embedded system and provide defenses against broad classes of attacks — all without compromising performance, area, energy consumption, cost and usability. In this paper, we examined the various ways in which embedded systems can be attacked by malicious agents from side channels especially using fault injection mechanism. For the fault injection scenarios, we studied how a wide array of countermeasures has been developed by researchers to provide tamper resistance in embedded systems and then proceeded to implement our research finding to provide full proof and elegant attacking and countering systems using fault injection as the basic mechanism.

REFERENCES
[1] [Artemios G. Voyiatzis and Dimitrios N. Serpanos (2004)] “A Fault-Injection Attack on Fiat-ShamirCryptosystems” proceedings of the 24th International conference on Distributed computing Systems workshops(ICDCSW ’04)
[3] [Hagai bar- El, Hamid Choukri, David Naecache, Michael Tunstall and Claire Whelan] “The sorcerer’s apprentice guide to fault attacks”
[7] [Jem bnERKES, 2006], Lecture notes University of Waterloo
[9] [TAO ZHANG, XIAOTONG ZHUANG, SANTOSH PANDE, WENKE LEE 2005]”Anomalous Path Detection with Hardware Support” CASES’05 San Francisco, CA ,USA
[10][Tilman Wolf, Dhruv Kumar, Basab Datta, Wayne Burleson and Guy Gogniat,2006]”Collaborative Monitors for Embedded Systems Security” First workshop on embedded system security in conjunction with EMSOFT, Seol South Korea
[11][Yong Hong, Z. Abid and Wei Wang, 2004]”proceedings of the 4th IEEE International workshop on system-on-chip for Real-time Applications (IWSoC’04)
[16][Latch up,Steven H.Voldman, John Wiley & sons,2008, 1st Edition