Journal of Computer Engineering
ISSN 10003428

Original Research Article
Vol 13, Issue 10, 2024 | ISSN: 1000-3428

Security Vulnerabilities in Smart Flow Meters: A Hardware Analysis of Fuel Dispensing Units

Dr. Nong Zhang
University of Technology Sydney (UTS), Australia.

Abstract
A fuel dispenser is an embedded system, which is used to transfer fuel from reservoir tank to vehicles fuel tank. Modern Fuel Dispensing Unit (FDU) contains both mechanical and electronic systems. Electronic parts control the working of the dispensing unit. Mechanical system consists of an electric motor, pump and valves, nozzle to control the fuel. In the case of FDU, both hardware and software attacks are possible, but software attacks will happen only through hardware such as communication interface or tapping wires from PCB. In this situation hardware security analysis of fuel dispenser unit is highly important. Smart flow meter (Pulsar) is one of the electro-mechanical components in the Fuel Dispensing Unit, which is used to convert the mechanical signal to an electrical signal. This project intends to do the hardware security analysis and identifying the various vulnerabilities present in the smart flow meter, thereby suggesting suitable mitigation techniques so as to provide maximum hardware security to the smart flow meter.

Indexed keywords: Fuel dispenser, pulser, optical smart flow meter, pulser ocd card, fuel dispensing unit, pulser card

Article History: Received: 07 August 2024 | Accepted: 03 October 2024 | Published: 19 October 2024

I. INTRODUCTION
In this modern world, vehicle usage is increasing day by day. The energy required for their working is supplied by fuels such as petrol, diesel, LPG, CNG. The fuel dispensers in fuel dispensing stations distribute these fuels. Fuel Dispensing Unit (FDU) is used to transfer fuel from the reservoir tank to vehicles fuel tank. Some of the components of FDU are responsible for pressurizing the fuel and moving it through the system. Some are involved in metering the liquid fuel, registering accurately the quantity delivered, and computing the price of the delivery. Finally, some components serve to control the operation of the system, switching it on and off, resetting the volume and price indicators, regulating the delivery, and so on. FDU is actually an embedded system, which contains both electronics and mechanical components.

II. PROPOSED SYSTEM
This project intends to do the hardware security analysis and identifying the various vulnerabilities present in the smart flow meter of FDU, thereby suggesting suitable mitigation techniques so as to provide maximum hardware security strength to the smart flow meter. Hardware security analysis is a developing stream of security analysis. The procedure for hardware security analysis is completely different from other fields like software, PCB design. The main aim of the analyzer is to find out the vulnerability on the electronic board and preventive measures against these attacks by using mitigation techniques. One of the most commonly used techniques is Reverse Engineering. This helps to reconstruct the circuit diagram of an unknown electronic board. To analyse the circuit

How to cite: University of Technology Sydney (UTS), Australia. (2024). Security Vulnerabilities in Smart Flow Meters: A Hardware Analysis of Fuel Dispensing Units. Journal of Computer Engineering, 13(10), 27–31. DOI: https://doi.org/10.5281/zenodo.19355227

diagram the designer should get a detailed view of original systems functionality and should be aware of the possible attacks.

A security analysis engineer is able to make a highly secure system. This can be achieved by providing some procedures which starts by obtaining a proper knowledge of the whole hardware component, studying its functionality and various attacks. Based on the study, the designer understands how a hacker plans to damage the actual system. So the designer must tries to avoid the vulnerability and finally the electronic board attacks can be reduced.

III. PROCEDURE FOR HARDWARE SECURITY ANALYSIS

Procedure involved in hardware security are:

1. Component Analysis.
2. Schematic Rebuilding.
3. PCB Analysis.
4. Hardware Security Analysis Report Preparation.

A. COMPONENT ANALYSIS

The main aim of this analysis is to identify the active and passive components that are present in the Electronic Board. Then study the functionality of each component in the Electronic board with the help of datasheet of each component from the internet. In this stage, the hardware security analyser gets the functionality of the electronic board. If the system functionality is changed then the analyser can identify the change.

B. SCHEMATIC REBUILDING

In this case, the pictures of both the top and bottom layer of the Electronic board is taken. Then identify its vias, next its tracks of the PCB layers and trace the path of the layer. Then the components mount on the top layer, then combine all the transparent layers of each side like vias, connection, track traces.

C. PCB ANALYSIS

Based on the datasheet of each component, the connection pins of the electronic board can be found .Through analysis it can be determined which pins of microcontroller are connected or not with the peripherals. Finally a continuity check is performed on the board which provides an overall view and increased accuracy.

D. HARDWARE SECURITY ANALYSIS REPORT PREPARATION

By combining both Schematic Rebuilding and PCB Analysis, find out the possible vulnerabilities of the electronic board. By doing so, the analyser can take the preventive steps against the attacks due to the vulnerability in the systems. Analyser can then provide some suggestions to improve and secure the system more accurately and hackers will find it difficult to break the security systems. Using hardware security analysis, the Analyser can find the possible attacks and how to overcome that attacks. Since the analyser analysis both the fault path and the protective path, security of the electronic board can be ensured.

IV. HARDWARE SECURITY ANALYSIS REPORT

By combining both Circuit Rebuilding and PCB Analysis, find out the possible vulnerabilities of the Electronic board. By doing so, the analyser can take the preventive steps against the attacks due to the vulnerability of the systems. Analyser can then provide some suggestions to improve and secure the system more accurately and hackers will find it difficult to break the security systems. Using the hardware security analysis, the Analyser can find the possible attacks and how to overcome that attacks. Since the analyser analysis both the fault path and protective path and he can finally ensure the security of the Electronic board.

Some of the possible attacks are given in Table I.

TABLE I LIST OF ATTACKS

Serial No	Attacks Name	Description
1	Glitch Attack	• Manipulate the voltage outside its tolerant values. • If the clock is external to the circuit, manipulate that.
2	Temperature Attack	· Raise or lower the temperature to cause faulty behaviour
3	Light Induction	· Shine a light in the circuit to cause unexpected current.
4	Magnetic Faults	· Use a magnet to induce a current on the circuit. · Generally uses a laser.
5	Forced Attacks	· Forcing to change the logic state of the system.
6	Side Channel Attacks	· Observe the signal and then analyse the operation of the system
7	Timing Attacks	· Observe the clock cycles to access the memory. · System's password location in memory can be identified.
8	Power glitch attacks	· Focuses the input pad of the IC pins. The RF coil is brought near to that pin. The power applied to the RF coils due to the interaction of power and RF coils produces glitches and changes the logic state of the system.
9	Micro Probing	· Used to access the chip surface directly, so that one can observe, manipulate and interface with the IC.
10	Data Remanence	· The data in SRAM is freezed so that it is not lost during power off.
11	Man-in-the-Middle Attack	· By connecting an external wire to the data bus for accessing the received data.

V. TYPES OF ATTACKS

There are different types of attacks that occur in Electronic board. Based on the approach of hackers, they are classified into three types.

1. Non-Invasive Attack
2. Invasive Attack
3. Semi-Invasive Attack

1. NON-INVASIVE ATTACK

Here attacks are made on the surface of the chip. Non-invasive component are classified into active and passive .In active non-invasive attack focuses on the brute attack or forced attack. Passive non-invasive attack occurs as side channel attacks. Forced attacks means forcing to change the logic state of the system. But side channel attacks only observe the signal, and then analyse the operation of the system.

Encoding the information content with respect to high length of the code is inevitable, because it make the code difficult to analyse and thereby protect the system from attackers. But if the code is optimized, the hacker can easily understand the original message.

Timing attacks are done with respect to a clock cycle. Consider one clock cycle is complete, and then the password is passed from memory to the processor, so the attacker can find out the processor password with respect to the clock cycle. These attacks are known as Timing attacks.

Power glitch attack focuses the input pad of the IC pins. The RF coil is bought near to that pin. The power applied to the RF coils due to the interaction of power and RF coils to produce glitch .In this way we can change the logic state of the system.

In Data remanence, the hacker understands the information of the SRAM, by freezing the information of the SRAM. Finally, the data is not lost during power off.

2. INVASIVE ATTACK

Hackers doing the reverse engineering mechanism, find the vulnerability of the Electronic board, then add an additional module with the help of which it control the operation of the system. Invasive attacks are classified into two, Micro Probing and Reverse engineering.

One can observe, manipulate and interface with the IC by accessing the chip surface directly by using Micro probing techniques.

Reverse engineering is used to understand the inner structure of the semiconductor chip and learn to emulate its functionalities. Same technology which is used by semiconductor manufacturer is used here and it also gives the attacker similar capabilities Here transistor level attacks are possible, so it consumes more time compared to other attacks.

3. SEMI-INVASIVE ATTACK

A datasheet is used to identify the functionality with respect to model number. With the help of a laser beam one can change the logic state of the system. Here hacker breaks the seal of the board. Thus this type of attack requires depackaging the chip to get access to its surface. But the invasion layer remains intact, as these methods do not require electrical contact to the internal lines.

VI. SECURITY ANALYSIS OF OPTICAL SMART FLOW METER 1. PULSER AS SMART FLOW METER

Smart flow meter is an electro-mechanical component in the Fuel Dispensing Unit, which is used to convert the mechanical signal to an electric signal. It generates discrete pulses with respect to shaft rotation in the meter unit. The principle of operation of the smart flow meter is based on the optical photo detector mechanism. The rotating shaft has numerous slits associated with it. These slits cut the path between LED and photo detector, generating discrete pulses. The pulser is connected to the main motherboard of the FDU. The communication packet between mother board and pulser is encrypted. The discrete pulses are analysed in the motherboard and amount of fuel is calculated and dispensed from the reservoir tank to vehicle tank. In the old discrete piston syringe system of fuel flow meter, different sets of gears were used to dispense the fuel. Such a system requires frequent calibration. The new advanced smart flow meter available in markets has a feature that the pulser itself can calculate the price of the fuel dispensed. These calculated values are encrypted and are passed to the motherboard.

2. ANALYSIS OF ATTACK ON OPTICAL SMART FLOW METER

The smart flow meter (pulser) is the most critical unit in a FDU. This is because; the volume dispensed depends on the operation of the pulser unit. So the aim of the attacker is to change the actual discrete pulse with respect to the initial calibration which is based on the fuel dispensed (eg; 50 pulses correspond to 500ml).

Below mentioned are the most commonly used methods to manipulate the pulser.

- The slits in the rotating shaft is covered with tape or similar object to alter the pulses generated.
- An additional counter circuit is inserted between the pulser unit and the motherboard to change the number of pulses. Counter is used to reduce the actual discrete pulse cycle which is less than the original pulse cycle, which increments /decrements a binary value based on the clock input. Here by understanding the vulnerability of the board, attacker violates the system functionality with the help of an external circuit. Such an attack is called non-invasive attack.
- The pulser –motherboard communication can be tapped by connecting an external wire in the pulser side or motherboard side or in between the two units. Such an attack is called man-in-middle attack which is a sub type of non-invasive attack. These occur due to unencrypted data transfer. It can be avoided by using encryption algorithm.
- Disable the pulser unit and use a PWM generator in place of the pulser to get the required pulses. However scientific testing is to be completed.

VII. MITIGATION TECHNIQUES

- In a black box, components are arranged such that they are not close to the pins. In this way, glitch attacks can be avoided.
- Hackers try to attack between the processor and peripherals. So any abnormal activity feels the system with the help of the sensors. Then the system is suddenly reset. By doing so valuable information can be protected from the hackers.
- Hide the part number of the components used to build schematic of the circuit.
- Physical sealing of the pulser: The pulser is physically protected by sealing the whole unit by authorized government agency .Sealing has to be removed only with the proper permission from the authorized government agency. Whenever the sealing is broken without proper permission there may be a chance of fraudulent activity on the pulser unit.

- Data encryption: In the modern FDU, the communication between the pulser and the motherboard is encrypted with advanced encryption algorithm and is protected with encryption key. This helps to prevent Man-in-the-middle attacks to pulser unit.
- One Time Password (OTP): Another way of preventing unauthorized pulser opening is by OTP authorizer. In this case, whenever the pulser is opened for any purpose and after completing the work and OTP is required to dispense the fuel again.
- Potted pulser: In this case the pulser is provided with a self destructive tamper proof mechanism (either physical or electronically) against manipulation. This type of pulser is fully sealed and if anyone tries to open it, then the pulser unit will get damaged by some means and it cannot be reused.

VIII. ADVANTAGES

- Helps in identifying short delivery during fuel dispensing.
- Helps to strengthen the Hardware security of the Smart Flow Meter.Finding the hardware issues and software attacks and suggest some mechanism to prevent such issues in future.

IX. CONCLUSION

This paper presents the hardware security analysis and identifying the various vulnerabilities present in the smart flow meter of FDU, thereby suggesting suitable mitigation techniques so as to provide maximum hardware security strength to the smart flow meter. Hardware security analysis is a developing stream of security analysis. This report also lays out the procedure for hardware security analysis which is completely different from other fields like software, PCB design and also described one of the most commonly used techniques is Reverse Engineering. This helps to reconstruct the circuit diagram of an unknown electronic board.

REFERENCES

[1] Navid Asadizanjaniark, Mark Tehranipoor, Domenic Forte, "PCB reverse engineering using nondestructive x-ray tomography and advanced image processing", IEEE Transactions On Components, Packaging And Manufacturing Technology, Vol. 7, No. 2, February 2017.

[2] Ruzinoor Che Mata, Shahrul Azmi, Ruslizam Daud, Abdul Nasir Zulkiflid , Farzana Kabir Ahmad, “Reverse Engineering for Obsolete Single Layer Printed Circuit Board (PCB)", IEEE International Conference on Computing & Informatics ICOCI '06 , October 2009.