Int. J. Advanced Networking and Applications
Volume: 02, Issue: 05, Pages: 811-816 (2011)

Attacking Embedded Systems through Power Analysis

Dr. Sastry JKR,
Department of Information Technology, K L University, Vaddeswaram, Guntur District 522502
Email: drsatry@klce.ac.in,
Prof K. SubbaRao,
Department of Electrical and Electronics Engineering, K L University, Vaddeswaram,
Emal: Iksb_a_eee@klce.ac.in
Prof N Venkata Ram,
Department of Electronics and Communication Engineering, K L University, Vaddeswaram,
Email: venkatram@kluniversity.in
Ms.J. Sasi Bhanu
Department of Computer Science and Engineering, K L University, Vaddeswaram,
Email: sweetsasi2002@yahoo.co.in
,

---------- **ABSTRACT**----------

Embedded Systems are being used for the development and implementation of Safety and Mission Critical Systems. Malfunctions of such type of embedded systems will lead to disasters at times. The embedded systems must be fully secured from outside intervention in order to have effective functioning as well as to provide protective environment to these mission critical systems. There are several attacking systems discussed in the literature each requiring a kind of counter attacking system. Power Analysis and variations of power analysis are the significant attacking mechanisms discussed in the literature. Crypto servers are the main areas of attacking as they deal with securing the data that flow in-between several components of the embedded systems. Most of the attacking systems suggested in the literature suffer from lack of experimental models to emulate the attacking system. An attacking system could be amply proved when several samples of data are used for attacking and the samples of data provide for knowledge base. In this paper an experimental setup is proposed which is an embedded system by itself for creation of a Knowledgebase which shall form the basis for attacking. The experimental setup required for undertaking the actual attacking with the usage of the knowledgebase is also presented. Further, the proposed attacking system is applied for mission critical system and the experimental results obtained through the simulation are also presented.

Key words: Power Analysis, Attacking, Embedded Systems, Knowledge Base, Crypto Server

---

Paper submitted: 14th December 2010 **Revised Date: Nil** **Accepted Date: 16th February 2011**

---

1. Introduction:

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 should be integrated into the product during the conceptual design phase and should be taken into account for every part of the design. For this reason, manufacturers must secure their products against specific threats while 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, the 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.

Power Analysis attacks are one kind of side channel attacks that affect embedded systems by manipulating the power characteristics of the system especially manipulating the signal. The kind of side channel attacks that can be induced into embedded systems are dependent on the hardware used and the Applications Software implemented on such hardware. There are, however, several kinds of power analysis attacks that can be subjected to embedded systems. Differential Power Analysis (DPA) is the most threatening attack compared to other attacks.

Volume: 02, Issue: 05, Pages: 811-816 (2011)

Power analysis attack is a Passive attack that attempts to reveal the internal processing and data handled, inside a device such as microcontroller, on the basis of measurement of power consumption of the device.

Power analysis attacks are classified as simple power analysis (SPA), differential power analysis (DPA) and higher order differential power analysis (HO-DPA).Simple power analysis (SPA) is a technique whereby information about the operation performed in the device, or the operands manipulated in the operation, can be directly interpreted from a single power trace. DPA is carried out by taking the difference between measured and reference power. To carry out a DPA attack, an attacker must have a number of power consumption patterns collected from a device that has repeatedly executed an operation with different inputs and producing different outputs.

Higher-order DPA attacks consider several power analysis parameters and their Power Consumption Patterns are analyzed using statistics applied to a collection of points in time. The higher-order attacks are more powerful, but also more complicated as the choice of statistics and the points in time may depend on the specifics of algorithmic Implementation.

Power analysis attacks were discovered by Kocher, Jaffe and Jun in 1999[1]. To counteract timing attacks, dummy computations have to be introduced. Kocher noticed that this might be insufficient defense, as the power consumption of dummy computations is different from that of meaningful ones. The SPA attack was first performed by Kocher, Jaffe and Jun [1]. Power traces through power consumption measurements taken across a cryptographic operation of DES clearly revealed that, 16 rounds of DES were used for encryption. The detailed analysis of power traces have been tabulated and presented. Kocher specified that DPA is more threatening attack than SPA. Messerges et al [2] have shown that operations on data and address-buses is the dominant cause that effect changes in the power consumption and thereby into power traces at the attached gates to internal buses in typical smart-card microprocessor. They noticed that the Hamming weight information is best used for correlation of data to power consumption.

Messerges suggested that a way to decrease the number of power consumption measurements is to use multiple-bit DPA attacks. Popp et al. [3] demonstrated a DPA attack to show how it reveals the first byte of the secret key of an Advanced Encryption Standard (AES) software implementation. Chari et al. [4] have shown that the complexity of performing a higher-order DPA attack increases with the exponent of the number of points used in the computation of the statistics. A new variant of power analysis attack, named template attack was proposed by this author. Clavier et al. [5] also proposed an improvement to the general DPA technique, called Hamming integration variant method.

Most of the methods suggested by various authors for attacking embedded systems are related to specific embedded systems. The authors have not provided for multiple samples of data that are to be collected from the embedded systems. Few samples do not provide accurate results and it is difficult to attack using such minimum number of samples.

In this paper an attacking system is proposed through a Knowledge based created by a separate experimental setup and also a process are presented that help attacking an embedded system using the knowledge as the basis. The algorithms required for doing such a kind of attacking have also been presented. A system is designed using which the actual attacking of the embedded system is carried using the knowledge base created through a different experimental setup.

2.0 A Pilot Project – Secured Embedded System

An embedded system has been developed for monitoring and controlling of temperatures within a Nuclear Reactor (TMCNRS). Fig 2.1 shows the hardware layout of the TMCNRS. This pilot model has been developed and attacking of the pilot model has been made using the methods proposed in this paper.

89C51 Micro controller is at the heart of the TMCNRS. It has interaction with several components like A/D converters, relays, buzzer, LCD etc. All the devices have certain latency time set for them. The mechanical setup is fitted with two temperature sensors which are terminated at the Target Embedded System (TMCNRS). The sensors generate signals equivalent to temperatures sensed and the same are amplified and converted to data by A/D Converter connected to the embedded systems. The communication between the Micro Controller and the A/D converter is achieved through I^2C communication. The Analog data is converted to digital data by A/D converter. The reference temperatures that must be maintained within the Nuclear Reactor are fed to Embedded System through a remote host computer system.

The mechanical setup of the Nuclear reactor is connected with a pumping system to pump coolant into the nuclear reactor for cooling down the temperatures if the temperature rises above the reference temperatures. The application running in the embedded system compares the temperature sensed through temperature sensors with the reference temperature. If reference Temperature is less than the actually sensed temperature

then a relay is activated to start the pump to pump the coolant into the reactor. If the Reference Temperature is less than the actual temperature the relay is set off so that the pumping gets stopped. This kind of logic is implemented in respect of both the Temperatures. If absolute difference between both the sensed temperatures is greater than 2 degrees, then the buzzer is triggered; else the buzzer is reset.

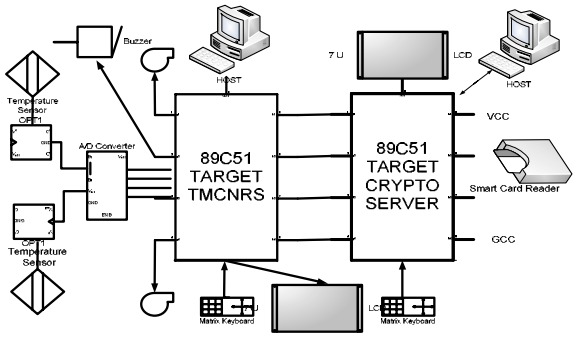


Figure 2.1 hardware design of TMCNR system

The security for this system is built around a Crypto server which encrypts the data read from a smart card reader and the access code entered through a Key Board. The crypto server communicates the encrypted code to a remote host where it is decrypted and a validation of the same is carried. The acknowledgement from the HOST in turn will enable the resetting of the TMCNRS.

The main security issue is to preserve the information related to Input Data, Key used for encryption, output data and the encryption algorithm used by the Crypto server for undertaking the encryption. Essentially it is the crypto server which will be attacked to reveal the secret information.

3.0 Comparative Analysis

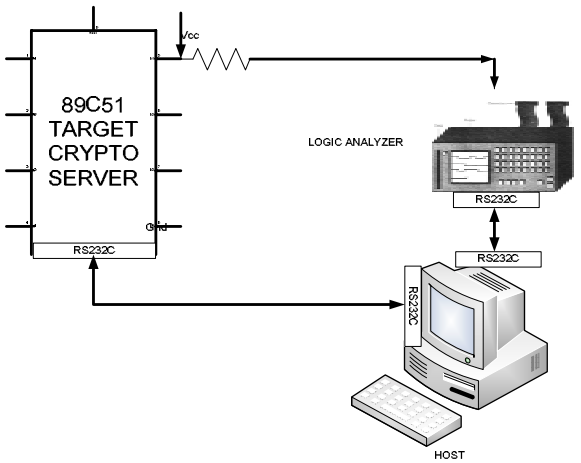
Comparative analysis of various attacking systems based on power analysis is shown at Table 3.1. The analysis reveals that most of the attacking systems lack experimental setup and knowledgebase and most of the methods used in the literature are based on trial and error. The systems available in the literature are not accurate; meaning the attacking methods are weak.

4.0 Experimental Setup:

The main basis of attacking a crypto server is based on development of a Knowledgebase. The knowledgebase is acquired through a separate experimental setup built around an embedded system.. Fig 4.1 shows the experimental setup used for the acquisition of knowledge base. The 89c51 crypto server is fed with known Input data, Encryption Algorithm and the key value from HOST using RS232 communication. The crypto server performs the encryption operation. During the encryption, HOST sends a command signal for current consumption data to Logic analyzer. Logic Analyzer senses the amount of current consumed across series resistor and transmits the same to the HOST. Crypto Server also makes available the Encrypted output to the HOST. A knowledgebase is created by the HOST combining the inputs and outputs received from crypto server and Logic Analyzer.

The knowledgebase is created for different samples of data sent from the HOST and the results generated by the crypto server and the Logic Analyzer is padded with the input data to form an entry into the Knowledgebase.

Table 4.1 shows the knowledgebase created out of execution of several samples of data submitted through the HOST and the output obtained from Crypto Sever and the Logic Analyzer.



Figuer.4.1 experimental setup of power analysis attacks

5.0 Attacking through experimental setup:

Fig 5.1 shows actual attacking mechanism through power analysis using the experimental setup and the knowledgebase created in section 4.0. HOST sends the input data, and encryption algorithm through crypto server interface and this information is received by the 89C51 crypto server using the HOST application interface. Crypto server encrypts the data. Simultaneously HOST sends a request to Logic Analyzer for current consumption data and then Logic Analyzer measures the amount of current consumed across series resistor and sends the same to the HOST.

A process at the HOST forms a data structure combining the inputs with current data received from Logic Analyzer and makes a rigorous query to find the matched records in the knowledge base. The matched records thus reveal the secret key used for undertaking the encryption.

Table 5.1 Knowledge base of attacking System

Input Data	Type of Algorithm	Encrypted Output from Crypto Server	Output from Logic Analyzer Current Consumed (µA)	Secret Key
POWER	RSA	REWOP	10	168
POWER	RSA	REWOP	15	212
POWER	RSA	REWOP	12	184
ANALYSIS	RSA	SISYLANA	27	248
ANALYSIS	RSA	SISYLANA	30	294
ANALYSIS	RSA	SISYLANA	25	208
TEMPERATURE	RSA	ERUTAREPMET	36	213
NUCLEAR	RSA	RAELCUN	28	156
SECURITY	RSA	YTIRUCES	26	210
ATTACK	RSA	KCATTA	14	422

Table 5. 1 shows the experimental results obtained from the knowledgebase for a given set of inputs sent through the HOST to the Crypto server and the output received from the crypto server and Logic Analyzer. Table 5.2 presents the queried results obtained from the Knowledgebase.

6.0 Simulation and Experimental Results

The hardware setup designed for forming the actual attacking system has been simulated to test the working of the system properly considering both hardware and software separately.

The inputs to be provided to crypto server by the HOST for undertaking encryption and making available the encrypted output are simulated through 4 different types GUI gadgets which are TEXT Boxes.

The code necessary to read the data through manual interaction is supported by the simulator. Proteus simulator is used to simulate the system. Proteus has a simulated component that simulates the current being generated.

The host application has a software component introduced to read the simulated components. All the data that is either emanated from the HOST or read from the simulated GUI components is encapsulated into a data structure and the same is used by the HOST to query the knowledgebase and report the tuples that have the Input Data, Type of algorithm, encrypted output data and the Current. The matching tuples shall have the secret key used for undertaking the encryption.

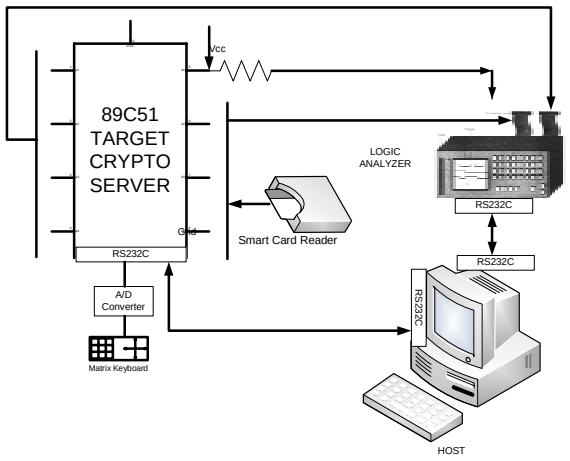


Figure 5.1 Experimental setup for attacking through power analysis

***Table* 5.2 Inputs and outputs from/to Attacking System**

Input		Output	
Input Data	Type of Algorithm	Encrypted Output from Crypto Server	Output from Logic Analyzer Current Consumed (µA)
POWER	RSA	REWOP	12
ANALYSIS	RSA	SISYLANA	27
TEMPERATURE	RSA	ERUTAREPMET	36
NUCLEAR	RSA	RAELCUN	28
ATTACK	RSA	KCATTA	14
SECURITY	RSA	YTIRUCES	26

The Table 6.1 shows the query results. Looking at query results one can make out the secret key used for undertaking the encryption.

The database consists of the attributes named serial number, key value, Input data, algorithm, Encrypted data and current consumed during the operation. For example, the 89c51 crypto server is fed with known Input data POWER, with Encryption Algorithm RSA and the key value is 123 from HOST. During encryption current consumed data is measured by the logic analyzer and its mean value is 10 micro amperes for this present operation. The encrypted data resulted from the operation is REWOP, which is sent to HOST by the crypto server

***Table* 6.1 Queried results from knowledgebase**

Input Data	Type of Algorithm	Output from Crypto Server Encrypted Output	Output from Logic Analyzer Current Consumed	**Secret Key**
POWER	RSA	REWOP	12	**184**
ANALYSIS	RSA	SISYLANA	27	**248**
SECURITY	RSA	YTIRUCES	26	**210**
NUCLEAR	RSA	RAELCUN	28	**156**
ATTACK	RSA	KCATTA	14	**422**
TEMPERATURE	RSA	ERUTAREPMET	36	**213**

The data highlighted forms the secret key that is revealed through querying the knowledgebase.

Table 6.2 Simulation results

Serial Number	Key value	Input Data	Algorithm	Encrypted data	Current in Micro Amps
1	123	POWER	RSA	REWOP	10
2	123	POWER	RSA	REWOP	11
3	**123**	**POWER**	**RSA**	**REWOP**	**10**
4	124	POWER	RSA	REWOP	11
5	125	POWER	RSA	REWOP	12

7. Conclusions:

The effectiveness of an attacking system can only be proved through a separate experimental setup and attacking through several samples of the data and creation of knowledgebase system. The actual attacking of an embedded system can be undertaken through a separate experimental setup. The data acquired through attacking system can be used to query the knowledge base and arrive at the secret key which is used for encrypting the Input Data.

References

[1]. P. Kocher, J. Jaffe, and B. Jun. "*Differential Power Analysis"* . In M. J.Wiener, editor, The Proceedings of the 19th Annual International Conference on Advances in Cryptology (CRYPTO'99), *volume* 1666-LNCS, pages 388–397. Springer-Verlag 1999.

[2]. T. S. Messerges, E. Dabbish, and R. Sloan, "*Investigations of Power Analysis Attacks on Smartcards*" In USENIX Workshop on Smartcard Technology, pages 151–161. USENIX Association, 1999

[3]. S. Mangard, T. Popp, and B. Gammel, "*Side-Channel Leakage of Masked CMOS Gates*", CT-RSA, Feb. 2005.

[4]. S. Chari, C. Jutla, J. Rao, and P. Rohatgi, "*Towards Sound Approaches to Counteract Power-Analysis Attacks*", In M. J. Wiener, editor, The Proceedings of the 19th Annual International Conference on Advances in Cryptology (CRYPTO'99), volume 1666-LNCS, pages 398–412. Springer-Verlag, 1999

[5]. C. Clavier, J.-S. Coron, and N. Dabbous, "*Differential Power Analysis in Presence of Hardware Countermeasures*", In C. K. Koc¸ and C. Paar, editors, The Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2000), volume 1965-LNCS,

[6]. S. Mangard, "*Hardware Countermeasures against DPA – A Statistical Analysis of Their Effectiveness"*, CT-RSA, LNCS 2964, pp. 222 - 235, February 2004.

Authors' Biographies

Dr JKR Sastry is presently working as Professor of Computer Science and Engineering at K L University, vaddeswaram and has 35 Years of experience in the field of information Technology. Has served the IT industry for 29 Years worldwide and has been serving the education industry for the last 6 Years. Has published 44 Papers in the fields of Embedded Systems, Data warehousing and Mining, Software Engineering and Wireless Communication. Has been the reviewer for several IEEE sponsored International and national Conference. Has Chaired 2 International Conferences. Has directed 4 PhD programs and has been directing 8 PhD programs concurrently.

Prof K Subba Rao is presently working as professor of Electrical and Electronics Engineering and Director (Q&A) at K L University, Vaddeswaram. His fields of Interests include Embedded Systems, Power Systems and Power Electronics. Has 22 Years of Teaching Experience. Has been the Principal Investigator for an R&D project sponsored by AICTE. He has published several of the papers in the field of securing the embedded systems.

Prof N Venkata Ram is presently working as professor of Electronics and Communication Engineering and Associate Dean (FED) at K L University Vaddeswaram. His fields of Interests include Embedded Systems, Image Processing and security Systems. Has 20 Years of Teaching Experience. Has published several of the papers in the filed of Imaging and water marking.

Ms. J Sasi Bhanu is presently working as Assistant Professor of Computer Science and Engineering at K L University, Vaddeswaram. She has 5 Years of teaching experience and has been pursuing her PhD program in the field of embedded systems.

Her research interest includes Embedded Systems, Remote Monitoring and Control, and distributed Embedded Systems. Has published 6 papers in internationally reputed Journals and Conferences.

Table 3.1 Comparative Analysis of Various Attacking Systems

Serial Num	TYPE	SPA	DPA	HO-DPA	KNOWLEDGE BASE
1	Complexity	less	high	Very high	moderate
2	Feasibility of attacking	more	Less compared to that of SPA	less	less
3	Accuracy of obtaining information	medium	good	good	good
4	Cost of attacking	low	More compared to that of SPA	high	Moderate
5	Speed at which attacking can be done	high(but more assumptions)	Moderate	low	Moderate
6	Supported by Experimental Setup	NO	NO	NO	YES
7	Supported by Knowledge Base	NO	NO	NO	YES