Developing a Multi Platform Countermeasure to Ensure a Secure Home

Ibraheem Frieslaar*†, Barry Irwin †
*Modelling and Digital Science, Council for Scientific and Industrial Research, Pretoria, South Africa.
*ifrieslaar@csir.co.za
†Department of Computer Science, Rhodes University, Grahamstown, South Africa.
†b.irwin@ru.ac.za

***Abstract*—This research proposes an investigation into the side channel analysis attacks against the AES algorithm on high powered devices. Currently the research field into this aspect is fairly new and there is room for more information to be discovered. This research proposes using a Raspberry Pi in conjunction with a Software Defined Radio to capture electromagnetic emanations in the low and high frequency domains. Two well known side channel attacks will be used to recover the secret information based on the electromagnetic emanations. Furthermore, this research proposes investigating into a possible software countermeasure by using the high powered devices features such as multi-threading.**

***Index Terms*—AES, Electromagnetic Analysis, Raspberry Pi, Software Countermeasure, SDR.**

I. Introduction

The security assurance of sensitive information for individuals or organisations have become a wide spread demand. Many applications have been introduced to provide a mechanism to protect sensitive information. These applications offer a form of cryptographic security to ensure the information is confidential. Theoretically cryptographic algorithms are mathematically secure. However, the implementation of these algorithms on an embedded device are susceptible to side channel analysis (SCA) attacks. SCA attacks are able to exploit the power consumption of the device to recover the sensitive information by discovering a correlation between the power consumption and intermediate values [11].

Electromagnetic Analysis (EMA) attacks is a well known alternative as oppose to using the power consumption [5]. Electromagnetic (EM) emanations are captured from the device and subsequently are used to retrieve the secret information. The advantage of using EM measurements do not require the attacker to have direct contact with the device. Therefore EMA is less intrusive than the conventional power analysis.

SCA attacks on small embedded devices have become prominent and the research in this field has shown to be beneficial. However, there are a limited number of studies performed on SCA attacks on more powerful general purpose devices such as computers and smartphones. This research field is a vital opportunity to discover critical information on the behaviour of these powerful devices. Furthermore, as mobile payments are becoming a norm it is important to provide protection from attackers on a multi platform level.

This research aims to investigate the susceptibility of a block-cipher implementation on a high powered device against two prominent attacks. The attacks used, are the correlation power analysis (CPA) [3] and template attacks [4]. The investigation will focus on the Advanced Encryption Standard (AES) cryptographic algorithm executing on a Raspberry Pi. Additionally, this research will implement a new countermeasure of using multi-threads to purposely leak out obfuscated information at critical points in the AES algorithm. Furthermore, low cost equipment will be used to capture the EM emanations in both the low and high frequency domains.

The remainder of this paper is organized as follows: a brief description of the research performed in the field of SCA attacks on high powered device is discussed in Section II; Section III will elaborate on the proposed experimental setup; and the paper is concluded with a discussion in Section IV.

II. Related Work

Traditionally, most of the research attention has been focused on the susceptibility of embedded devices as oppose to high powered devices to SCA attacks. There are two possible approaches to acquire the EM emanations from a high powered device. The first approach is to monitor the device in the low frequency domain and secondly to monitor the device at a high frequency domain.

Kenworthy and Rohatgi [10] made use of Simple Power Analysis (SPA) and leakage detection techniques to demonstrate the susceptibility of several implementations to EMA. Gebotys *et al.* [6] exhibited the ability to attack a Java implementation of AES executing on a PDA at 40 MHz. They demonstrated that their research was able to perform a differential EMA (DEMA) attack. Aboulkassimi *et al.* [1] improved on the previous work and demonstrated it was possible to extract secret keys on a Java mobile phone executing the AES algorithm. Furthermore, Nakudo *et al.* [12] carried out a SPA attack on the RSA implementation on an Android smartphone at 832 MHz. Finally, Balasch *et al.* [2] displayed in their research they were able to use DPA attacks on an ARM Cortex-A8 processor running at 1 GHz.

Genkin *et al.* performed attacks on the RSA cryptographic algorithm executing on a laptop running at 2 GHz [7]. They demonstrated the ability to extract decryption keys in the low frequency domain of less than 100 KHz. They were able to measure the EM emanations using a nonintrusive approach. The approach consisted of using a low cost Software Defined Radio (SDR) usb dongle attached to an EM probe to

capture the EM emanations. Additionally, they demonstrated the capabilities of capturing EM emanations from different rooms using a tuned loop antenna [8]. Furthermore, it was demonstrated they were able to recover the full secret key from an iPhone [9].

III. Experimental Setup

This section discusses the hardware and software to be used for the research. The device under attack will be the Raspberry Pi. The Raspberry Pi has been selected since it has an ARM Cortex-A7 processor, similarly to the processors used in smartphones. These ARM processors are also used in smarthphones. The hardware setup will consist of using two Raspberry Pi's. The one device will execute the AES algorithm – henceforth known as the device under test – while the secondary device will be used to capture the EM emanations, henceforth known as the attack device.

Both devices will have the Linux operating system, Lubuntu 15.10 installed. The attack device will have a SDR inserted into a usb socket. The Funcube Dongle Pro + is used as the SDR. This dongle will be used in tandem with an EM probe to capture the EM emanations from the device under test. Figure 1 illustrates the experimental setup, with the device under attack on the left and on the right the attack device with the SDR and EM probe.

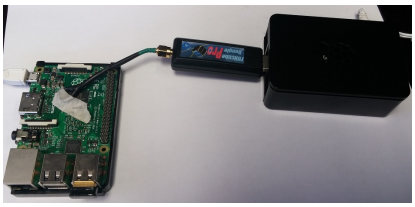

Fig. 1. Proposed experimental captruing setup.

The device under test will use the *libcryptopp* cryptographic library to encrypt secret messages. While these messages are being encrypted the attack device will use GNU Radio to monitor the frequency spectrum and capture the EM emanations. Upon acquiring the data, a CPA and template attack will be carried out to retrieve the secret key.

To mitigate the secret information from being captured. This ongoing research implements a new approach consisting of multi-threads and a task scheduler as a software countermeasure to mitigate SCA attacks. This approach is applied to four different multi-thread frameworks. The four frameworks are POSIX Threads (Pthreads); C++11 threads; Threading Building Blocks (TBB); and OpenMP. The preliminary results indicates to be fruitful.

IV. Discussion and Conclusion

The research field into side channel attacks against high powered devices is slowly progressing. In the last couple of years, attacks on RSA in the low frequency domain has started to progress. However, there has not been a study on the AES algorithm behaviour at this low frequency. Although, Balasch *et al.* [2] showed they were able to recover AES secret keys in the high frequency domain, the countermeasure they introduced was a hardware solution. Therefore, there are still many unanswered questions. This research would allow us to answer the following questions:

1) How vulnerable is the *libcryptopp* implementation of AES on a Raspberry Pi to side channel attacks.
2) Would the same software countermeasure on an embedded device work on a high powered device.
3) What effect would a multi-threaded software countermeasure have on the EM emanations.
4) Does the four multi-thread libraries behave differently in terms of EM emanations.

Acknowledgement

This work was undertaken in the Distributed Multimedia CoE at Rhodes University, with financial support from the department of Modelling and Digital Science at CSIR, Telkom SA, Tellabs/CORIANT, Easttel, Bright Ideas 39, THRIP and NRF SA (UID 90243). The authors acknowledge that opinions, findings and conclusions or recommendations expressed here are those of the author(s) and that none of the above mentioned sponsors accept liability whatsoever in this regard.

References

[1] D. Aboulkassimi, M. Agoyan, L. Freund, J. Fournier, B. Robisson, and A. Tria, "Electromagnetic analysis (EMA) of software AES on Java mobile phones," in *Information Forensics and Security (WIFS), 2011 IEEE International Workshop on*. IEEE, 2011, pp. 1–6.

[2] J. Balasch, B. Gierlichs, O. Reparaz, and I. Verbauwhede, "DPA, bitslicing and masking at 1 GHz," in *Cryptographic Hardware and Embedded Systems–CHES 2015*. Springer, 2015, pp. 599–619.

[3] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Cryptographic Hardware and Embedded Systems-CHES 2004*. Springer, 2004, pp. 16–29.

[4] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *Cryptographic Hardware and Embedded Systems-CHES 2002*. Springer, 2002, pp. 13–28.

[5] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Cryptographic Hardware and Embedded SystemsCHES 2001*. Springer, 2001, pp. 251–261.

[6] C. H. Gebotys, S. Ho, and C. C. Tiu, "EM analysis of rijndael and ECC on a wireless java-based PDA," in *Cryptographic Hardware and Embedded Systems–CHES 2005*. Springer, 2005, pp. 250–264.

[7] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "Stealing keys from PCs using a radio: Cheap electromagnetic attacks on windowed exponentiation," in *Cryptographic Hardware and Embedded Systems–CHES 2015*. Springer, 2015, pp. 207–228.

[8] ——, "ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs," in *Topics in Cryptology-CT-RSA 2016*. Springer, 2016, pp. 219–235.

[9] D. Genkin, L. Pachmanov, I. Pipman, E. Tromer, and Y. Yarom, "ECDSA key extraction from mobile devices via nonintrusive physical side channels," Cryptology ePrint Archive, Report 2016/230, Tech. Rep., 2016.

[10] G. Kenworthy and P. Rohatgi, "Mobile device security: The case for side channel resistance," 2012.

[11] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology–CRYPTO99*. Springer, 1999, pp. 388–397.

[12] Y. Nakano, Y. Souissi, R. Nguyen, L. Sauvage, J.-L. Danger, S. Guilley, S. Kiyomoto, and Y. Miyake, "A pre-processing composition for secret key recovery on android smartphone," in *Information Security Theory and Practice. Securing the Internet of Things*. Springer, 2014, pp. 76–91.

Ibraheem Frieslaar is currently perusing his PhD. in Computer Science at Rhodes University. The focus of his research is embedded security and cryptanalysis.

Barry Irwin is the founder and head of the Security and Networks Research Group at Rhodes University. His research focuses on passive traffic analysis, Internet background radiation, Web-based malware and national level cyber defence.