ISSN 2395-1621

Security against SCA Attacks by Refreshing Key using AES Modes

[#1]Mr.Kunal Choudhari, [#2]Mr.Sujit Mane, [#3]Mr.Mahesh Pansare,
[#4]Mr.Ronit Haldar, [#5]Prof. Mr.Santosh T. Waghmode

[1]kunalchoudhari13@gmail.com
[4]ronit.haldar@gmail.com

[#1234]Department of Information Technology
[#5]Department of Information Technology
Jspm's
Imperial College Of Engineering & Research,
Wagholi, Pune-412207.

ABSTRACT

Side-channel analysis (SCA) exploits the information leaked through unintentional outputs (e.g., power consumption) to reveal the secret key of cryptographic modules. The real threat of SCA lies in the ability to mount attacks over small parts of the key and to aggregate information over different encryptions. The threat of SCA can be thwarted by changing the secret key at every run. Indeed, many contributions in the domain of leakage resilient cryptography tried to achieve this goal. However, the solutions were computationally intensive and were not designed to solve the problem of the current cryptographic schemes. So a generic framework of lightweight key updating that can protect the current cryptographic standards and evaluate the minimum requirements for SCA-security and also complete solution to protect the implementation of any standard mode of Advanced Encryption Standard has been proposed.

ARTICLE INFO

Article History

Received: 18th May 2016

Received in revised form :

19th May 2016

Accepted: 22nd May 2016

Published online :

24th May 2016

Keywords: **SCA, AES, CBC, cryptography.**

I. INTRODUCTION

Security of data is becoming an important challenge for a wide spectrum of applications, including communication systems (with high privacy requirements), secure storage supports, digital video recorders, smart cards, cellular phones. Resistance against known attacks is one of the main properties that an encryption algorithm needs to provide. When a new attack is demonstrated as effective (also in term of computation time), the update of the encryption system is a real necessity to guarantee the security of data.

AES (Advanced Encryption Standards)

A new block encryption algorithm called Rijndael has been developed and published by Daemen and Rijmen. This algorithm is an iterated block cipher with variable block length and a variable key length. The block and the key length can be independently specified to 128, 192, or 256 bits. The number of algorithm rounds depends on the block and key length. The different transformations of the algorithm architecture operate on the intermediate result, called State. The State can be pictured as a rectangular array of bytes. This array has four rows. The number of columns is called Nb and it is equal to block length divided by 32. The Key is also considered as a rectangular array with the same number of rows as State. The number of columns is equal to the key length divided by 32. This number is denoted as Nk. The number of rounds, Nr, depends on the values Nb and Nk. For block and key length equal to 128 bits, both values of Nb and Nk are equal to four and the number of rounds Nr is defined as 10. These specifications are served by the proposed implementations, which will be analyzed in detail in the next paragraphs. A basic round transformation relies on combining operations from four fundamental algebraic functions that operate on arrays of bytes.

Side-Channel Analysis (SCA)

SIDE-CHANNEL analysis (SCA) is an implementation attack that targets recovering the key of cryptographic modules by monitoring side-channel outputs which include, but are not limited to, electromagnetic radiation, execution time, acoustic waves, photonic emissions and many more. The real threat of SCA is that the adversary (Eve) can mount attacks over small parts of the key, and to aggregate the

information leakage over different runs to recover the full secret. SCA attacks are commonly based on three pillars,

1) Sensitive variables affect leakage traces.

2) Eve can calculate hypothetical sensitive variables.

3) She can combine information from different traces.

The design of countermeasures against SCA attacks is a vast research field. Contributions in this regard fall into three categories: Hiding, Masking and Leakage Resiliency.

II. LITERATURE SURVEY

[1]. Leak-resistant cryptographic indexed key update, P. C. Kocher, U.S. Patent 6 539 092, Mar. 25, 2003.
Analysis: In this paper described The transaction between client and server can be done by having a connection between a client and server using a protocol.in this process server undergoes series of operation to determine the correct session key from clients initial key value .then transaction is performed.

[2]. Towards super-exponential side-channel security with efficient leakage-resilient PRFs, M. Medwed, F.-X. Standaert, and A. Joux, Berlin, Germany: Springer-Verlag, 2012.
Analysis: Here in this paper proposed, has improved both the practical security and the leakage resilient of the system. has improved both the practical security and the leakage resilient of the system. These PRFs are compatible to AES and gives physical security and initializes the system properly can be used to secure the system.

[3]. Practical leakage-resilient pseudorandom objects with minimum public randomness, Yu and F.-X. Standaert Berlin, Germany: Springer-Verlag, 2013,
Analysis: In this paper, practical relevance of two important leakage-resilient pseudorandom objects. The main drawback of the proposal is that the key bit sizes of 2n can only guarantee a security of most 2n.

III. PROBLEM IDENTIFIED

- There is no provably secure construction that supports stateless key-updating.
- Intuitively speaking, the secret key cannot be updated to a new key unless a public variable is used (assuming no synchronization). Once a public variable interacts with a secret key, SCA will be possible. Some contributions tried to secure the stateless key-updating mechanism through hiding and masking.
- Although this approach limits the implementation overhead exclusively to the key-updating mechanism, allowing the use of unprotected cryptographic cores, the overall overhead is still significant.

IV. PROPOSED SYSTEM

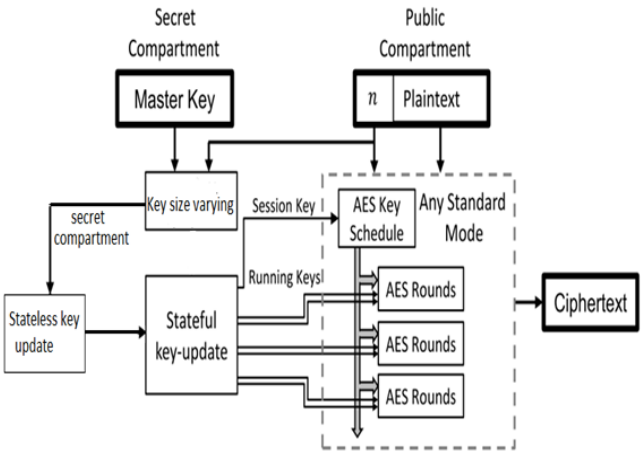


Fig 1. System architecture

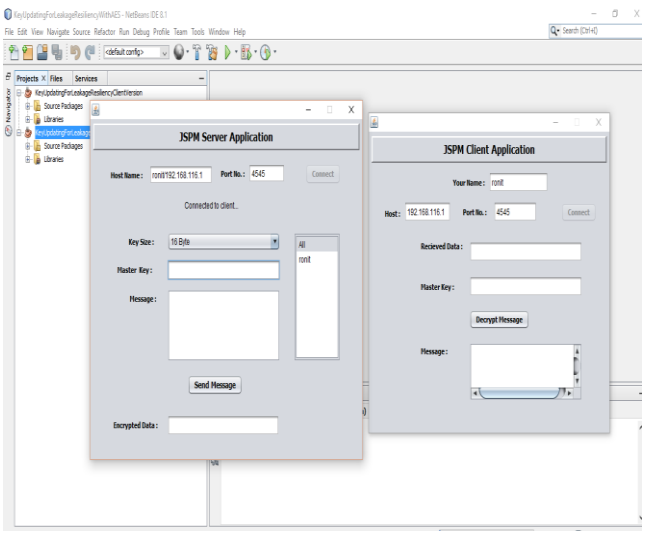
i) User Registration: This is a versatile peer who needs to get into the information that put away at the storage peer (e.g., an officer). In the event that a peer has an arrangement of characteristics fulfilling the access policy of the encoded information characterized by the sender, and is not disavowed in any of the qualities, then he will have the capacity to decode the ciphertext and acquire the information.

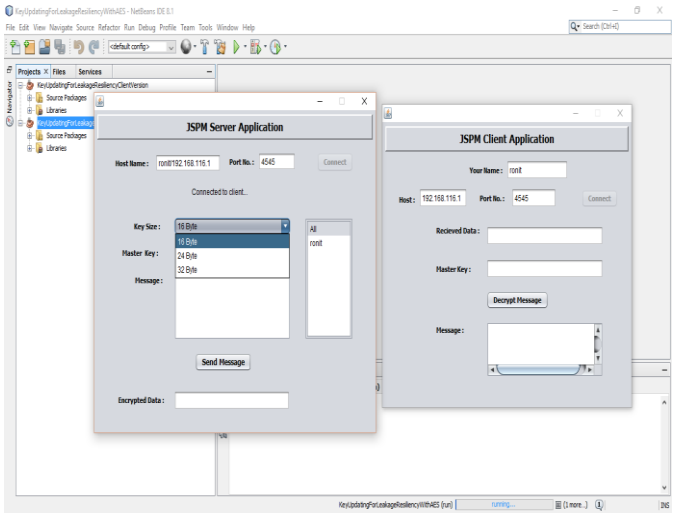
ii) Key Authorities: Key Generation is the process of creating keys using protection parameters to generate the secret key for the peers. The key is the combination of Message Sent Time (Ts) and the number of hops in the route (Hr).

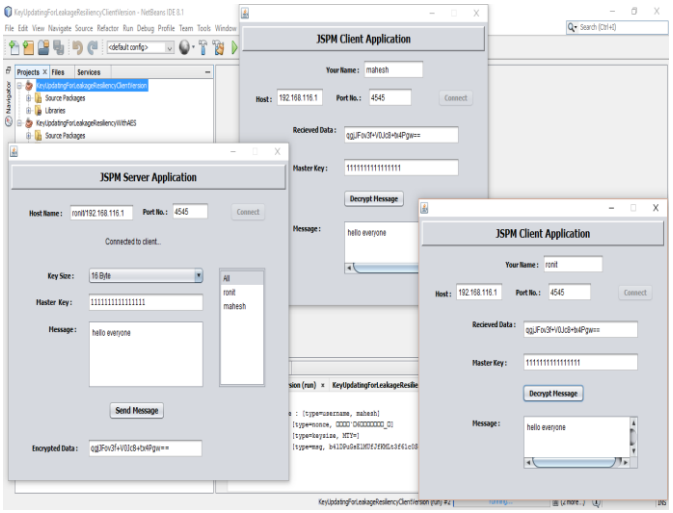
iii) Sender: The translation of data into a ciphertext is known as encryption. Encryption is the most effective way to prevent data from leakage resiliency. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

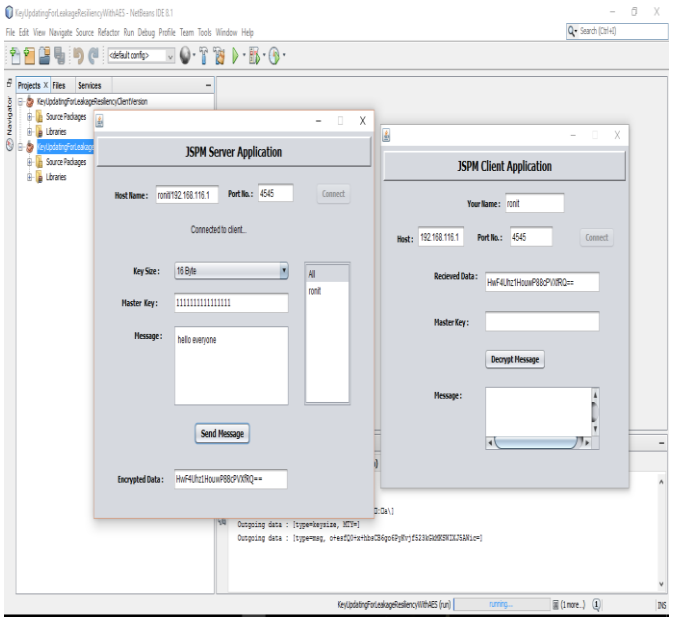
iv) User: Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of unencrypting the data manually or with un-encrypting the data using the proper codes or keys.

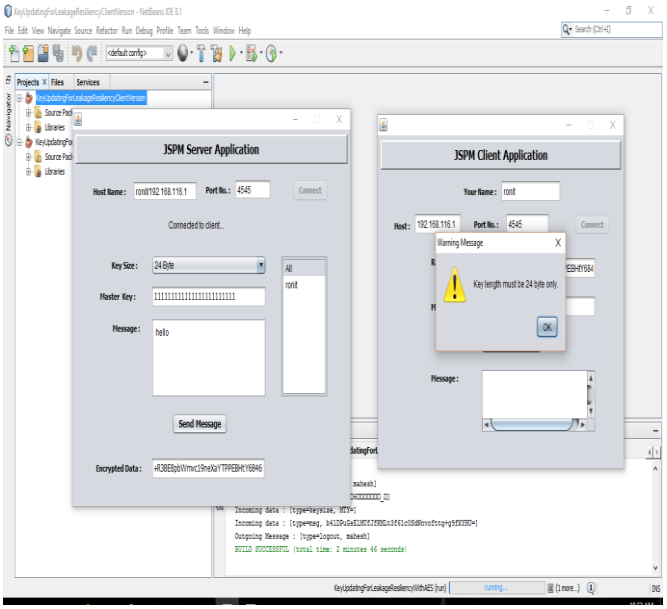
V. RESULT

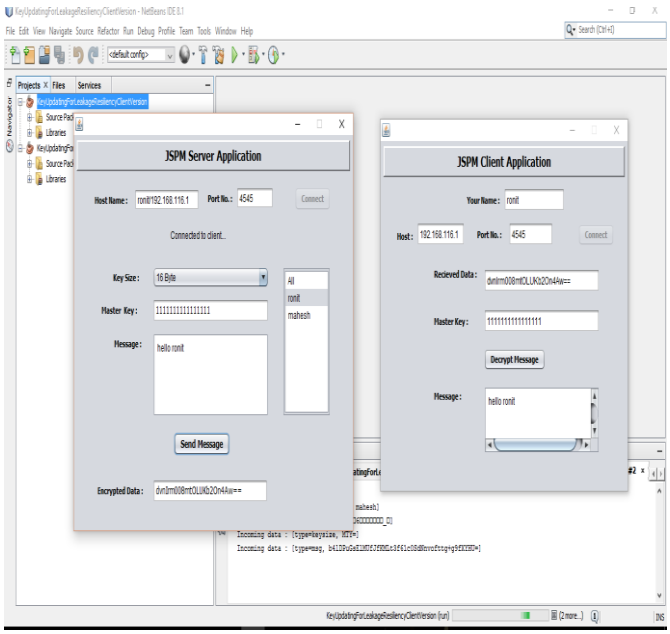












VI. CONCLUSION

In this project, we proposed a lightweight key-updating framework for efficient leakage resiliency. We proposed the minimum requirements for heuristically secure structures. We proposed a complete solution to protect the implementation of any AES mode of operation. Our solution utilized two rounds of the underlying AES itself achieving negligible area overhead and very small performance overhead.

This work can further be implemented in large scale network to reduce the internet threat as well as theft in E-Commerce and military field.

REFERENCES

[1]. F.-X. Standaert, O. Pereira, Y. Yu, J.-J. Quisquater, M. Yung, and E. Oswald, "Leakage resilient cryptography in practice," in Towards Hardware-Intrinsic Security. Berlin, Germany: Springer-Verlag, 2010, pp. 99–134.

[2]. Y. Dodis and K. Pietrzak, "Leakage-resilient pseudorandom functionsand side-channel attacks on Feistel networks," in Proc. 30th CRYPTO,2010, pp. 21–40.

[3]. S. Faust, K. Pietrzak, and J. Schipper, "Practical leakage-resilient symmetric cryptography," in Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer-Verlag, 2012, pp. 213–232.

[4]. K. Tiri et al., "Prototype IC with WDDL and differential routing—DPAresistance assessment," in Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer-Verlag, 2005, pp. 354–365.

[5]. D. Martin, E. Oswald, and M. Stam, "A leakage resilient MAC,"Dept. Comput. Sci., Univ. Bristol, Bristol, U.K., Tech. Rep. 2013/292, 2013. [Online]. Available: http://eprint.iacr.org/.

[6]. S. Dziembowski and K. Pietrzak, "Leakage-resilient cryptography," inProc. IEEE 49th Annu. IEEE Symp. Found. Comput. Sci. (FOCS), Oct. 2008, pp. 293–302.

[7]. A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang, "Pushingthe limits: A very compact and a threshold implementation of AES," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2011, pp. 69–88.

[8]. S. Belaïd et al., "Towards fresh re-keying with leakage-resilient PRFs:Cipher design principles and analysis," J. Cryptograph. Eng., vol. 4, no. 3, pp. 157–171, Sep. 2014.

[9]. Y. Yu and F.-X. Standaert, "Practical leakage-resilient pseudorandomobjects with minimum public randomness," in Topics in Cryptology. Berlin, Germany: Springer-Verlag, 2013, pp. 223–238.

[10]. P. C. Kocher, "Leak-resistant cryptographic indexed key update,"U.S. Patent 6 539 092, Mar. 25, 2003.

[11]. A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, "Factoring polynomialswith rational coefficients," Math. Ann., vol. 261, no. 4, pp. 515–534, Dec. 1982.

