ISSN 2348 – 8034
Impact Factor- 3.155

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

A SECURED SYMMETRIC ENCRYPTION ALGORITHM TO PROTECT STORED INFORMATION

Dipali K. Dakhole[*1], Deepenti H. Deshmukh[2] and Pallavi M. Sune[3]
[*1,2,3]Assistant Professor, CSE Department, Prof. Ram Meghe Institute of Technology & Research, Badnera, India

ABSTRACT

In every communication channel or methodology now-a-days, there is a necessity of secure transmission from sender to the authentic receiver. Therefore a number of data encryption techniques have come up in recent years for different information transfer systems. However, the major security challenges today focus on protecting the endpoints of channels. There are many cases where a persistent attacker can obtain the secret keys in use on a system, no matter how much the system tries to prevent this. Hence there is necessity of protecting a data even if the attacker is able to get secrete key and decrypted content.Here in this project, A solution that allows a device to symmetrically encrypt data without itself being able to decrypt it, and nor can any attacker that compromises the device, will be implemented. Both symmetric and asymmetric encryption as components of our solution (e.g. RSA and AES) will be used. The technique will be made more complicated in order to frustrate the attacker. This technique will also prevents the information from brute force attack, cold boot attack

Keywords- *Security, Cryptography, Image storage, Computer security, Data security.*

I. INTRODUCTION

Cryptography is the art of protecting the channel between two communicating parties. However, the major security challenges today focus on protecting the endpoints of channels. Modern cryptographic techniques are robust enough to defend against attacks (most of the time), and so the endpoints have become the weakest link in the security chain. There is no need for hackers to attempt to decipher messages in transit, when they can implant a trojan on your machine to harvest all the secrets that it processes. Some other attacks exploit the difficultly in verifying the remote party (trojans, phishing, DDOS), but increasingly important is securing the machine right in front of you. Whether the attacker is using a root kit to surreptitiously monitor the device, or has stolen the physical device it to exploit any stored data, information is at risk. There are plenty of examples of devices stolen with sensitive information [1] [2], and of drives disposed of incorrectly [3]. A good defense against many attacks is to have available on any device only the information that is strictly necessary.

The solution we describe in this project is specific to situations where information only has to be stored locally (and not processed) but still must be protected against theft. For any situation where a significant amount of data needs to be stored, symmetric encryption is the obvious solution. By the very nature of symmetric encryption, if a device can encrypt, then it can also decrypt. And whatever the device can do, it is possible an attacker can be manipulating it into doing for their advantage. There is an assumption in all this discussion, that in a device where a key exists and is used, it can be stolen. The key may be used by an obscure, proprietary, complex, or otherwise difficult to comprehend program.

This solution applies to any device that needs to store data, does not need to process the data itself, and the data is of sufficient value to increase the incentive of theft. The layout of this paper, we describe some related work in this field in section 2. In section 3, the algorithm is described in detail. In section 4, Algorithm is implemented. Finally we describe its application and give our conclusion.

II. REVIEW OF LITERATURE

The existing work related to the above mentioned work, is explained as follows -

1. An improved Data Encryption Standard has been developed by incorporating an ODD/EVEN bit conversion to the existing DES algorithm. The proposed algorithm is expected to provide greater security to further protect the data in Smart Cards. The data is secured from any illegal retrieval and intended modification. The program simulation also provides a good start to explore for a more robust encryption technique that will not require so

much mathematical computations. But when attacker gets the cipher text & security key, the data can be easily decrypted [8].

2. To achieve the maximum security required a Parallel Processing, User Reconfigurable Cryptographic RISC Microprocessor is sproposed in our paper. Rather than protecting the data using tools and external codes, a microprocessor is specially designed in our project to offer maximum digital security. Cryptographic processor can be classified either as asymmetric cryptography or a symmetric cryptography processor. Asymmetric cryptography has the advantage of Reception security but has the limitation of High resource Utilization. And a symmetric cryptography processor has the limitation of single key security but comparatively has the advantages of low area, resource and power consumption. Thus in this project we are proposing Hybrid architecture in which both the advantage of asymmetric and symmetric cryptographies are combined. For implementation, Asymmetric RSA cryptography and a symmetric lightweight SEA encryption is combined to mutate a reconfigurable Cryptographic processor. Upcoming devices will be secured using this technique, but what about the existing devices [9]?

3. RSA algorithm and ECC algorithm are two of the most important asymmetric algorithm. The SM2 algorithm is independently developed by the State Cryptography Administration; it improves and expands the international standard ECC algorithm. This paper introduces the advantages of authenticating correctness and safety; it also put forward the further applications and some improvements for the SM2 algorithm. But when attacker gets the cipher text & security key, the data can be easily decrypted [10].

4. CAST and RC5 commonly used for network data encryption. We analyzed the encryption security, evaluated encryption speed and power consumption for both algorithms. Experimental results show that CAST algorithm runs faster than RC5 algorithm while consumes less power, which is demonstrated that CAST is more suitable for wireless network application [11].

III. SYSTEM ARCHITECTURE

There are two devices, Master and Recording (it is a simple matter to generalize the solution to many recorders, but for simplicity sake we will only discuss one). Some initial communications can be done securely between Master and Recording. Recording can also do some initialization which is assumed to be performed in a secure area (i.e. somewhere where we can assume there is no risk of compromise). The basic idea is to fill up all the storage with output from a seeded random number generator (a symmetric cipher in Counter mode). The key and IV are encrypted using the Master's public key and stored, and then scrubbed from memory. Encryption of any data is calculated as appropriate, but XOR'd with the random data rather than stored directly. Provided the keys from the initial pass have been cleared from the system, an attacker cannot decrypt the message. Even if they can get at all key material in memory during encryption, they will at most be able to obtain the current block (which would be in memory anyway). Without the keys from the initial pass or the Master's private key, they cannot decrypt anything.

There are TWO modules in this project. The modules are explained as follows-

- Recording Device
- Master Device

Figure 1: System Architecture

3.1 RECORDING DEVICE

The recording device is again used for two processes. One is for Set Up purpose, In this the all keys which are going to use in this project are encrypted, stored and then after the use of this keys all are purged. The other process is of Encryption, in which using above mentioned keys and public key generated by the device, the plaintext is encrypted. Both the processes are explained further in details.

3.2.1 Recording Device Set Up

There is a Recording Device that has a large storage capacity and is used for recording. Another device, Master, is the intended recipient of the data. This latter device creates a public/private key-pair (Kpub, Kpri). Recording Device stores the public key Kpub (any one-off reliable transportation method can be used to deliver the public key to Recording Device).

Figure 2: Recording Device Set Up Block Diagram

In preparation for recording, Recording Device does the following [14]:

1. Divide the available storage into blocks, two separate blocks addressed b00; b01 (each of the same length as the asymmetric algorithm block length, l1), the rest addressed b0; b1; : : : ; bn (each of the same length as the symmetric algorithm block length, l2).
2. Generate random key Kr1 and random IV1 [15].
3. In block b00 store eAS(Kpub;Kr1 jjIV1)
4. for each i from 0 to n do
5. in block bi store eS(Kr1 ; (IV1 _ i)) (where i is written as a l2 bit string)
6. end do.

This step needs to be done while the device is secure (not at high risk from theft), but not necessarily while in the same location as the Master device. More importantly, once this step is completed, all key remnants must be purged from the system. In a PC, this would require deleting all caches, and powering down the machine for a few minutes.

3.1.2 Recording Device Encryption

Let the data to be encrypted be in blocks Mi; i = 0; : : : ; n, each of length l2. After completing the setup process, The Recording Device encrypts the data as follows [14]:

Figure 3: Recording Device Encryption

1. Generate random Kr2 [16]
2. In b01 store eAS(Kpub;Kr2)
3. for each i from 0 to n
4. Encrypt input: Ci = eS(Kr2 ;Mi)
5. Assign mask := bi
6. Overwrite bi with the value mask _ Ci
7. end do

3.2 MASTER DEVICE

The complete decryption process occurs on Master Device. The public key shared by Recording Device and Storage Blocks are used for the decryption process [14].

3.2.1 Decryption

Decryption of the message is done as follows. All blocks are transferred to Master. Using its private key, it decrypts blocks b00 and b01 to get Kr1, IV1, Kr2 . The next step is to remove the mask:

Figure 4: Master Device Decryption Block Diagram

```
1.  for each i from 0 to n do
2.  Assign mask := eS(Kr1 ; (IV1 _ i))
3.  Update bi with the value bi _ mask
4.  end do
```

The blocks can then be decrypted:

```
5.  for each i from 0 to n do
6.  Mi = dS(Kr2 ; bi)
7.  end do
```

IV. APPLICATIONS

4.1 In Modern Military Vehicles

Modern military vehicles typically have a number of sensors, possibly including video recorders. While some are used purely for presenting live information, many will store all recordings. This can later be used for evaluation, resolution of disputed events, or forensics examinations. This is a situation where it would be desirable for the device in the vehicle to have the ability to encrypt all recordings in such a way that it does not itself possess the ability to decrypt.

4.2 In Commercial Black Boxes

Another possible use is in commercial "black boxes". Insurance companies wish to charge their customer premiums based on the distances that they travel, and they are looking to install black box recorders in cars to monitor the driver's road use. End-users may be uncomfortable knowing that a complete history of their travel is stored in a device that could be hacked or abused. This history would contain the locations of their home, work, family, friends and any confidential services they receive (i.e. medical) and so should be protected.

4.3 In Electronic Voting Machine

Electronic voting machines in particular would benefit from not being able to decrypt the confidential vote just recorded, but allowing a central device to do so (to frustrate vote tampering). This solution applies to any device that needs to store data, does not need to process the data itself, and the data is of sufficient value to increase the incentive of theft.

V. CONCLUSION

Encryption is not a panacea that can solve any confidentiality problems. The fact remains that if the user is able to obtain data on a device, then it is possible that an attacker can too. Consequently, where the user does not need access to the data they are recording, they should not, in order to frustrate any attacker. A project has been demonstrated how to achieve this with standard encryption techniques. The application of these methods is far from universal in most cases they would not be applicable. However, there are several situations where they are suitable. Good security comes from applying the principle of least privilege. With the decreasing costs of storage, and as more and more information of value gets stored, it is important to apply the most appropriate measures.

REFERENCES

1. *J. Salter, "Camera sold on eBay contained MI6 files (2008)" http://www.telegraph.co.uk/news/uknews/3107003/Camera-sold-on-eBay-contained-MI6-files.html Cited 04 Nov 2008.*
2. *S. Coates, "Hazel Blears accused of breaching Official Secrets Act after laptop stolen (2008)" http://www.timesonline.co.uk/tol/news/politics/article4159555.ece Cited 13 Nov 2008.*
3. *A. Jones, G. Dardick, G. Davies, I. Sutherland, C. Valli, "The 2008 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market" Journal of International Commercial Law and Technology, North America, Jul. 2009.*
4. *D. Gadher, "Black box to cut car insurance (2006)" http://www.timesonline.co.uk/tol/news/article656361.ece Cited 05 2008.*
5. *J. A. Halderman, S. D. Schoen, N. Heninger, W.Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman,J. Appelbaum, and E. W. Felten, "Lest We Remember:Cold Boot Attacks on Encryption Keys" Proc.17th USENIX Security Symposium (Sec '08), SanJose, CA, July 2008.*
6. *R. Cramer, V. Shoup, "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack" SIAM Journal on Computing Vol 33 2001.*
7. *Ariel M. Sison, Bobby D. Gerardo, Yung-Cheol Byun, "An improved Data Encryption Standard to Secure Data using Smart Cards", Ninth International Conference on Software Engineering Research, Management and Applications, 2011.*
8. *A Chitra, T Blessin Sheeba, "A Hybrid Reconfigurable Cryptographic Processor with RSA and SEA", IEEE, 2012.*
9. *Liantao Bai, Yuegong Zhang, Guoqiang Yang, "SM2 Cryptographic Algorithm Based On Discrete Logarithm Problem And Prospect", IEEE, 2012.*
10. *Tingyuan Nie, Yansheng Li, Chuanwang Song, "Performance Evaluation for CAST and RC5 Encryption Algorithms", International Conference on Computing, Control and Industrial Engineering, 2010.*
11. *M. Dworkin, "Recommendation for Block Cipher Modes of Operation" NIST Special Publication 800- 38A, 2001.*
12. *Zenon Hotra, Natalia Dorosh, Halina Kuchmiy, Vladyslav Cherpak, "Modeling of Walsh Functions Synthesis Algorithms With a Different Type of Functions Arrangement", TCSET'2004, Feb 2004.*
13. *Thomas Martin, " UNDECRYPTABLE SYMMETRIC ENCRYPTION", IEEE GCC Conference & Exhibition, 2011.*
14. *Guang Gong, Amr M. Youssef, "Cryptographic Properties of the Welch–Gong Transformation Sequence Generators", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 48, NO. 11, NOVEMBER 2002*