Comparison Between Encrypt-and-MAC Composite (CMAC CTR) and Encrypt-then-MAC Composite (AES EAX) Modes of Operation in Cryptography Systems for Use in SMS-based Secure Transmission

Bao Guo and William Emmanuel Yu

***Abstract*—In current mobile telecommunications systems, the security offered by these networks are limited. In order to be used in use cases that require a high degree of security, such as M2M (financial, voting system), more security guarantees are necessary. Therefore, additional security must be added on top of existing networks. A common way to add security is by the use of composite encryption schemes. Two (2) of these schemes are then compared in terms of performance: an Encrypt-and-MAC composite scheme represented by AES in CTR mode and in CMAC mode and an Encrypt-then-MAC scheme using the EAX mode. These schemes are used in the context of an over the top protocol in SMS networks used in M2M applications. Results show that performance in terms of transaction time is close between the two (2) composite schemes but the Encrypt-then-MAC scheme provides more guarantees. It is also show that online performance is better for the Encrypt-then-MAC composite scheme.**

***Index Terms*—Cryptography, AES, AEAD, SMS, GSM**

I. INTRODUCTION

Mobile communication technology is one of the fastest growing areas, which continues to make significant impacts in the human lives and social development. In the last 20 years, mobile communications has made significant leaps in both capabilities and acceptance. There are over four (4) billion mobile phone users in the world, more than 65% population of the world [1]. Along with this is the rise of mobile commerce, the area of machine-to-machine (M2M) technology applications is also growing quickly. Analysts' projections show the compounded annual growth rate of M2M technology adoption is at 30% [2]. Along with the general increase in M2M use will be M2M applications that require a high degree of security such as financial, logistics, voting systems, SCADA and potentially other applications. There is a need to provide these transactions with the appropriate security guarantees.

Manuscript received December 8, 2010; revised December 29, 2010. This work was supported by the Department of Information Systems and Computer Science of the Ateneo de Manila University.

B. Guo and W. Yu are with the Ateneo de Manila University. (B. Guo e-mail: guobao7@hotmail.com; W. Yu e-mail: wyu@ateneo.edu).

II. OBJECTIVES OF THE STUDY

For particular M2M applications, the security of data transmission security is crucial. Security requirements may vary depending on the type of service and business requirements. For example, remote banking would require privacy, authenticity and integrity while navigation systems would only need authenticity and integrity. It is shown that for these types of M2M applications Encrypt-then-MAC composite schemes provide the most comprehensive amount of security guarantee [3]. The goal of this study is to compare the performance of Encrypt-then-MAC versus Encrypt-and-MAC composite schemes in cryptography when providing the required security guarantees. Another study is done comparing this composite scheme with a PKI-based scheme [13]. We introduce two (2) representative implementations of each scheme (AES-EAX and AES-CMAC-CTR) as representatives of their respective composite scheme then compare them in terms of transaction time.

III. SCOPE AND LIMITATIONS

In this study we aim to determine the comparative performance of the two mechanisms (Encrypt-and-MAC versus Encrypt-then-MAC composite scheme) for the purposes of securing data traffic using an over-the-top protocol on an SMS network targeted for M2M applications [4].

The hardware, software platform, payload (data to be transmitted) and keys for both mechanisms are kept constant. That is not actually transmitted to enforce the assumption that the network transport layer component is constant.

IV. SECURITY AND MOBILE NETWORKS

AES algorithm is iterated block cipher. Its block size is 128-bits, and the key sizes are the 128-bits, 192-bits and 256-bits. AES encrypted data block size is the biggest 256bit, but the key size in theory no upper limit [4].

Block ciphers such as AES are used in various modes of operation. These modes of operation provide particular guarantees.

There are three general modes of operations: confidentiality mode (i.e. CTR), authentication mode (i.e.

ISBN: 978-988-18210-3-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

CMAC) and authenticated encryption mode (i.e. EAX). Confidentiality mode only provides confidentiality. Authentication mode only provides integrity and authentication. AE modes provide all three security guarantees [5].

A. Confidentiality mode of operation

Confidentiality is the network information is not disclosed to unauthorized users, entities or processes. The information is only use for authorized users. Confidentiality is an important tool to ensure network and information security which base on reliability and availability.

Commonly used encryption modes include electronic codebook (ECB) which is the simplest and earliest form of confidentiality mode of operation, cipher-block chaining (CBC) mode, and Counter (CTR) mode. The full name of CTR mode is Advanced Encryption Standard (AES) in Counter Mode [15].

Counting mode (CTR mode) encryption is a series of input data block (called the count) is encrypted to produce a series of output block, the output of XOR plaintext block with the ciphertext [6]. Ciphertext with the same pseudo-random code after XOR re-produce the plaintext. CTR mode is widely used for ATM network security and IPSec applications.

B. Authentication mode of operation

An authentication mode of operation is used to provide message integrity and party authentication. Integrity refers to ensuring that the message sent is the same as the message receive. Authentication refers to being able to identify the sending party [5].

AES CMAC+CTR mode, we use CMAC to provide message integrity and party authentication and use CTR to provide the confidentiality security guarantee in our study.

AES-CMAC, the Advanced Encryption Standard-Cipher-based Message Authentication Code is based on CMAC's 128-bit Advanced Encryption Standard (AES) as a recognition algorithm. AES-CMAC use to achieve a purpose like the security of HMAC. For AES-CMAC in the information system is more suitable than a hash function [5].

C. Authenticated encryption mode of operation

This mode designed to simultaneously provide both authentication and confidentiality of the message (Authenticated encryption) [7]. It is typically implemented as a two-pass scheme: one pass for authenticity for each block and one for achieving confidentiality [4].

When one requires both confidentiality, integrity and authentication, then authenticated encryption scheme is used. Authenticated encryption schemes are implemented by compositing various modes of operation. Bellare points out that an Encrypt-and-MAC scheme does not provide the same amount of security guarantees when compared to Encrypt-before-MAC schemes [8].

EAX is a two-pass Authenticated Encryption with Associated Data (AEAD) scheme which supports no limit to the length of the messages, and has no limit on block cipher primitive to be used, nor on block size [7]. As an AEAD scheme, EAX can process Associated Data (AD) [14].

There are three composition methods for AE schemes described by Bellare namely Encrypt-and-MAC, MAC-then-encrypt, and Encrypt-then-MAC. Encrypt-and-MAC refers to a mode where encrypting the plaintext to achieve the ciphertext is generation and then appending a MAC of the plaintext. MAC-then-encrypt refers to the mode where appending a MAC to the plaintext and then encrypting all to achieve the encryption. Encrypt-then-MAC refers to a mode where encrypting the plaintext to achieve the ciphertext generation and then appending a MAC of the encrypted plaintext [8].

EAX is an Encrypt-then-MAC composite scheme; And CMAC+CTR is an Encrypt-and-MAC composite scheme.

Mobile networks require both security and performance. For particular M2M applications, to keep the data transmission secure and low costs are significantly for the entire M2M solution. The different service and business require different security requirements like privacy, authenticity and integrity. Thus, choose different technology will significantly affect the cost and secure of M2M applications. Our later studies will discuss these in detail.

V. Composition Modes

In our study, we focus on the EAX, CMAC (Cipher-based MAC) and CTR (Counter) modes of operation and use the AES block cipher. We now describe the two (2) mechanisms to be used in this study.

AES CMAC CTR mechanism and AES EAX mechanism are the two (2) representative composite modes which we want to compare.

AES EAX is the EAX mode of operation used with the AES block cipher using a pre-shared key (PSK) and is an Encrypt-before-MAC composite mode.

AES CMAC CTR mechanism is an Encrypt-and-MAC composite scheme using CTR as the encryption mode cipher and CMAC as the authentication mode cipher. This mechanism also assumes the use of a PSK. Both CTR and CMAC modes are executed on the data block separately.

VI. Experimental Setup

For the controlled environment we use the same hardware, payload and keys.

Base on this study, we try to compare AES CMAC+CTR and AES EAX cryptography mode of operation for use in SMS-based secure transmissions, these will be described later.

The procedure of the study:

First, a test bed was developed to process for data in terms of encryption, decryption, splitting and combination. The system was developed using Python 2.6 [9] and the cryptography primitives were implemented using the Botan 1.9.3 cryptography library with Python bindings [10]. The following table shows the environment of the experiment.

ISBN: 978-988-18210-3-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

TABLE I
EXPERIMENT ENVIRONMENT

Operating System	Linux Fedora 13 (32 bit)
Program Language	Python 2.6
Cryptography Library	Botan 1.9.3
Encryption modes	AES CMAC+CTR and AES EAX
Computer CPU	Intel Core2 Duo P7450 2.13GHz(only used 1 cpu)
Computer Memory	1024MB

Then, we will use two kinds of transmitter flow in order of encryption and break the data, which is encryption before split (ES) and split before encryption (SE). So there are compare four (4) different schemes: AES EAX SE, AES CMAC CTR SE, AES EAX ES, and AES CMAC CTR ES.

AES-EAX

As a sender, encrypt the entire data (plaintext) by AES-EAX, then split the ciphertext into block size; as a receiver, restore the ciphertext block files, and then decrypt. In the following experiments, "eax-es" can be used to refer to this set of data;

As a sender, split the data (plaintext), and then encrypt each block plaintext file by AES-EAX; as a receiver, decrypt each block ciphertext file, and then restore the plaintext. In the following experiments, "eax-se" can be used to refer to this set of data;

AES-CMAC+CTR

As a sender, encrypt the entire data (plaintext) by AES-CMAC+COUNTER first, the ciphertext into block size; as a receiver, restore the ciphertext block files, and then decrypt. In the following experiments, "cmac+ctr-es" can be used to refer to this set of data;

As a sender, split the data (plaintext), and then encrypt each block plaintext file by AES-CMAC+COUNTER; as a receiver, decrypt each block ciphertext file, and then restore the plaintext. In the following experiments, "cmac+ctr-se" can be used to refer to this set of data;

The figure shows the two different kinds of transmitter flow:

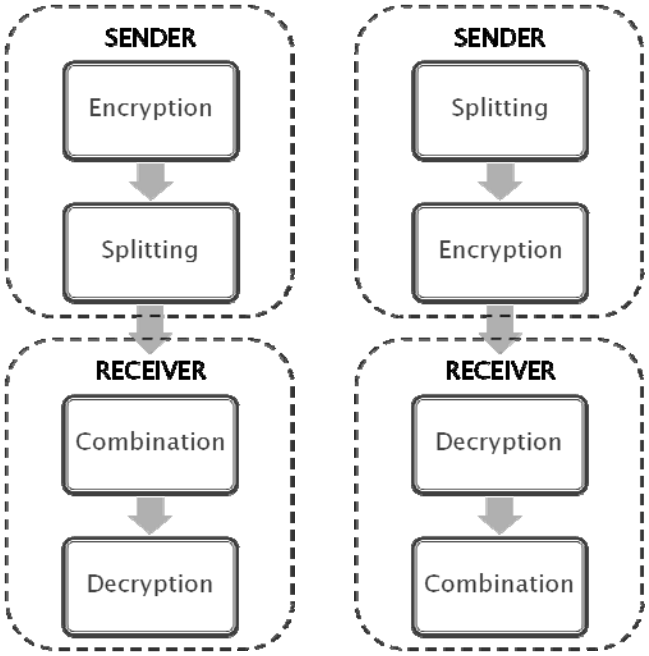

Fig. 1. Two Kinds of Transmitter Flow.

All the experiments will be under the same environment to ensure the fair of the comparison. The measures of the performance are the transaction time of encryption and decryption of each scheme. Measurements are the time efficiency.

The experiments will be carried out on four (4) different sizes of data files, which are 1KB, 10KB, 100KB and 1MB.

The block size for each experiment will be the same size——140 bytes, which is the standard size of SMS transmission [11]. Each experiment mode will be repeated 100 times, that's for the purpose of guarantee the accuracy of experiment result as possible.

VII. RESULTS

There are four sets of data for each experiment, which is "eax-es", "eax-se", "cmac+ctr-es", "cmac+ctr-se". The system was developed to output timings in logs files with the format of each output results are as follows:

TABLE II
RESULTS FORMAT

Action	File Name	Creation Time	File Size (bytes)	Block Sise (bytes)	Part	Repeat Number	Time (ms)

"Action" item can be "Splitting", "Combination", "Encryption" or "Decryption". "File Name" refers to the name of the file which is going to be encrypted. "Creation Time" item can be accurate to the second. Both "File Size" and "Block Size" are in bytes. The values of the "Part" represent the number of files which original document can be divided into. The "Repeat Number" refers to the current number of repetitions. "Time" is in milliseconds. For example,

ISBN: 978-988-18210-3-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

TABLE III
SAMPLES OF RESULTS

Action	*File Name*	*Creation Time*	*File Size (bytes)*	*Block Size (bytes)*	*Part*	*Repeat Number*	*Time (milliseconds)*
Encryption	test10kb	2010/10/4 5:14	10240	140	74	1	21.861791
Splitting	test10kb	2010/10/4 5:14	10240	140	74	1	183.78281

In table, this output means do the 8th time repetition, encrypt the "test10kb" file first, then split the encrypted file into 140 bytes, which becomes 74 parts, and the encryption time is 21.861791 milliseconds, the splitting time is 183.78281 milliseconds.

VIII. OBSERVATIONS

A box plot, sometimes called a box and whisker plot, is a quick graphic approach for examining one or more sets of data. In descriptive statistics, a box plot is a convenient way of graphically depicting groups of numerical data through their five-number summaries: the smallest observation (sample minimum), lower quartile (Q1), median (Q2), upper quartile (Q3), and largest observation (sample maximum).

In the experiment of this paper, every time of the experiment, there are four sets of data come out, which is "eax-es", "eax-se", "cmac+ctr-es", "cmac+ctr-se". Box plot can be well reflected the distribution of the data in this experiment.

The following are the resulting box plots against the experimental data.

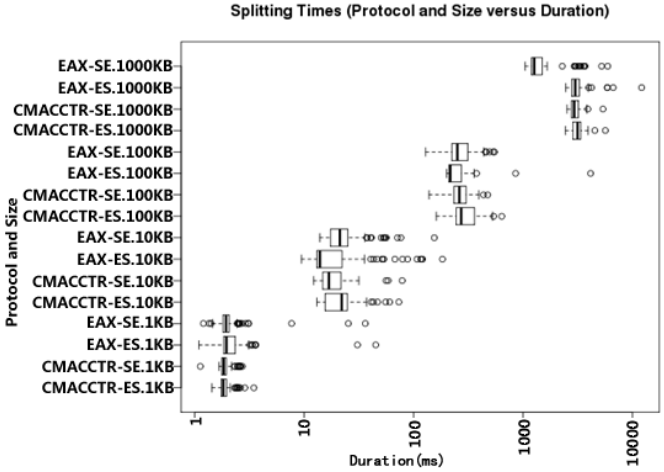

Fig. 2. Comparison of Splitting Times.

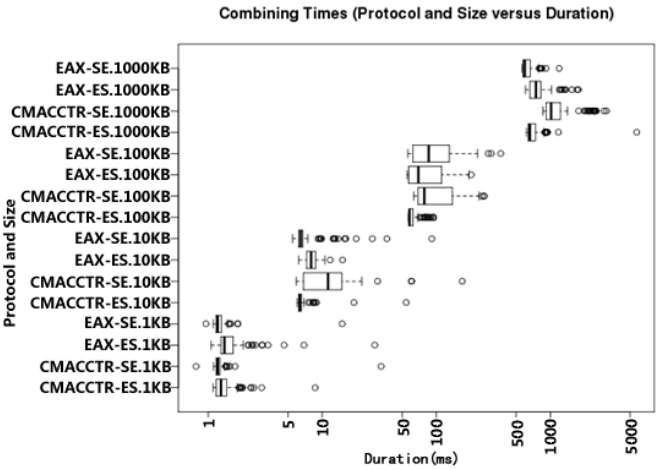

Fig. 3. Comparison of Combining Times.

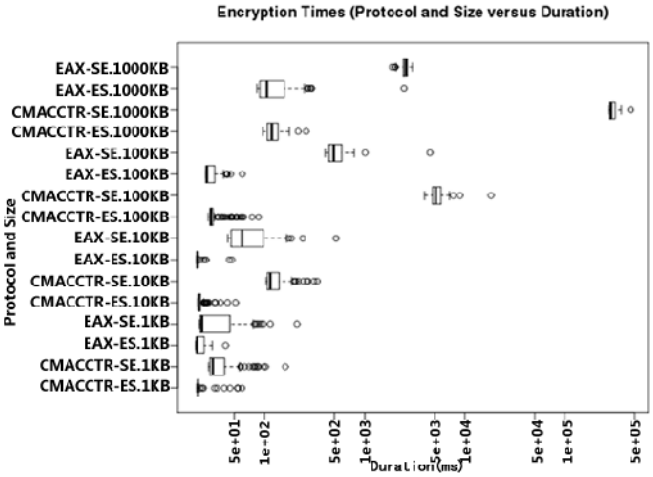

Fig. 4. Comparison of Encryption Times.

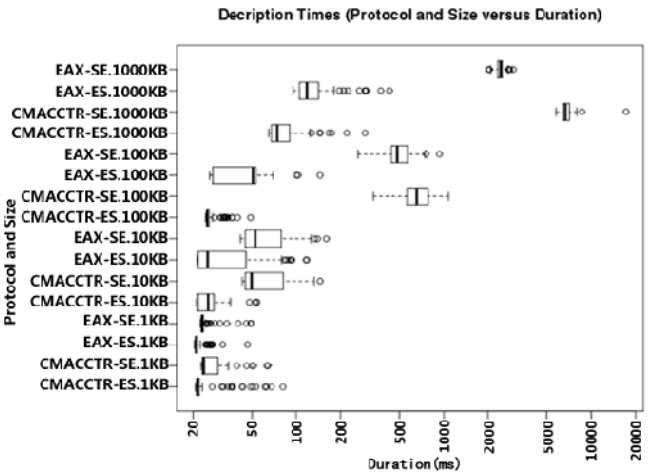

Fig. 4. Comparison of Decryption Times.

IX. CONCLUSION

These boxplots show the performance amongst the various actions between AES CMAC+CTR and AES EAX cryptography in both SE and ES operations. We can see that encryption/decryption first (ES) then splitting/combination always faster than splitting/combination first (SE) then encryption/decryption. This can be attributed to the fact that the current implementation writes the resulting files to the file system and as the number of files increase it causes an I/O

ISBN: 978-988-18210-3-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

bottleneck. AES EAX performs slightly poorer than AES CMAC+CTR in decryption while it performs insignificantly better in encryption than AES CMAC+CTR. It is interesting to note that, AES EAX performs significantly better in splitting before encryption cases than AES CMAC+CTR. This makes AES EAX better in streaming or online use cases. Considering AES-EAX performs similarly than AES CMAC+CTR in ES cases but better in SE use cases, and that AES-EAX provides more security guarantees [12] we suggest it be used for SMS-based data transport.

In future work, we will attempt to compare other modes of operation like CBC, CBC-MAC and CCM; and more constraints like system resources can be varied. Such as use with varying amounts of available memory. This can be used to study effects on resource constraints. Also a version of the experiment will be run without splitting files using the disk but instead in memory. This removes our I/O effect in the SE results.

REFERENCES

[1] W. Intelligence, Quarterly World Review Q3 2009, January 2010.
[2] GSMA, Embedded Mobile: M2M solutions and beyond, November 2008.
[3] Yu, W. S. and Tagle, P. U.: Cryptography Enabled Security Guarantees for Over the Top Networks Using GSM Short Messaging Service, Submitted to be presented the 2011 World Congress on Computer Science and Information Engineering (CSIE 2010), pp. 1-5, 2011.
[4] M. Bellare, P. Rogaway, and D. Wagner: The EAX mode of operation, in Fast Software Encryption. Springer, pp. 389 – 407, 2004.
[5] NIST, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B.
[6] J.Jonsson: On these curity of CTR+CBC-MAC. Contribution to NIST. [Online] Available: http://csrc.nist.gov/encryption/modes/proposedmodes/. Proceeding aversion to appearing in Proceedings from Selected Areas of Cryptography (SAC), 2002.
[7] M. Dworkin, “NIST Special Publication 800-38C,” NIST Special Publication, vol. 800, p. 38C, May 2004.
[8] M. Bellare and C. Namprempre: Authenticated encryption: Relations among notions and analysis is of the generic composition paradigm, Journal of Cryptology, vol. 21, no.4, pp. 469–491, 2008.
[9] Python Programming Language. Available: http://www.python.org/
[10] Botan cryptography library, 2010. [Online]. Available: http://botan.randombit.net/
[11] GSM Recommendation 03.03, “European Digital Telecommunications System (Phase2+); Security related network functions (GSM03.20 version 8.0.0 Release 1999),” European Telecommunications Standards Institute.
[12] Yu, W. S. and Tagle, P. U.: Development of an Over-the-Top Network Protocol for Pervasive, Secure and Reliable Data Transmission over GSM Short Messaging Service, To be presented at the 2010 International Conference on Computer and Software Modeling (ICCSM 2010), pp. 1-7, 2010.
[13] H. Wang and W. Yu, “Draft: Comparison between pki and symmetric key cryptography mode of operation for use in sms-based secure trans-missions,” Work in Progress, October 2010.
[14] P. Rogaway: "Authenticated-Encryption with Associated-Data," ACM Conference on Computer and Communications Security 2002 (CCS'02), ACM Press, pp. 98-107, September 2002.
[15] NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation - Methods and Techniques, December 2001.

ISBN: 978-988-18210-3-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)