IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 4, April 2015.

www.ijiset.com

ISSN 2348 – 7968

EMAC: Efficient Message Authentication Computing

Sunitha, S.Rajiya sulthana

CSE,BCETW,KADAPA , AP, INDIA

CSE,BCETW,KADAPA , AP, INDIA

ABSTRACT

Many applications rely on the existence of small devices that can exchange information and form communication networks. Preserving the integrity of messages exchanged over public channels is one of the classic goals in cryptography and the literature is rich with message authentication code (MAC) algorithms that are designed for the sole purpose preserving message integrity. With today's technology,. A new technique for authenticating short encrypted messages is proposed in MAC. MACs based on universal hashing are known to be more computationally efficient than MACs based on block ciphers and cryptographic hash function. In computationally secure MACs, keys can be used to authenticate an arbitrary number of messages . That is after ageering on a key legitimate users can exchange number of authenticated messages with the same key

KeyWords :*encrypted data, cryptography, universal hashing, Preserving computing, computational security*

1.Introduction

The basic concept allowing for unconditional security is that the authentication key can only be used to authenticate a limited number of exchanged messages. Since the management of one-time keys is considered impractical in many applications, computationally secure MACs have become the method of choice for most real-life applications. In computationally secure MACs, keys can be used to authenticate an arbitrary number of messages. hat is, after agreeing on a key, legitimate users can exchange an arbitrary number of authenticated messages with the same key.

There are two important observations to make about existing MAC algorithms. First, they are designed independently of any other operations required to be performed on the message tobe authenticated.

2. Existing system

A popular class of unconditionally secure authentication is based on universal hash-function families, pioneered by Carter and Wegman. Since then, the study of unconditionally secure message authentication based on universal hash functions has been attracting research attention, both from the design and analysis stand points

2.1 Proposed System

we propose two new techniques for authenticating short encrypted messages that are more efficient than existing approaches.

In the first technique, we utilize the fact that the message to be authenticate also encrypted, with any secure encryption algorithm, to append a short random string to be used in the authentication process

In the second technique, we make the extra assumption that the use dencryption algorithm is block cipher based to further improve the computational efficiency of the first technique.

3. Identations And Equations

$$T=mks+r(\bmod p) \qquad (1)$$

If the integrity check of is satisfied, the message is considered authentic

$$T= mk_s + r \ (\bmod p) \qquad (2)$$

the authentication tag computed according to (2), are transmitted to the intended receiver.

4. Figures

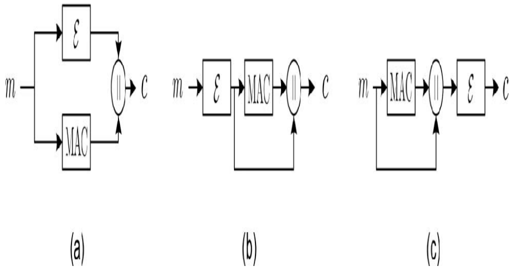

Fig.1. A schematic of the three generic compositions: (a) encrypt-andauthenticate, (b) encrypt-then-authenticate (EtA), and (c) authenticatethen-encrypt.

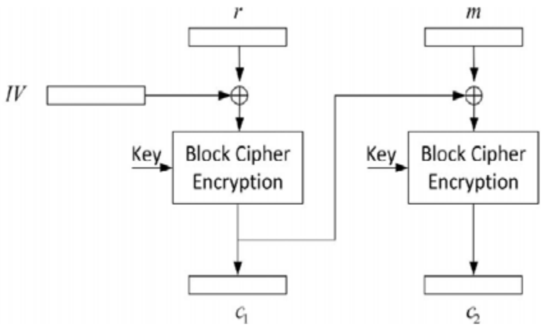

Fig. 2. The cipher block chaining mode of encryption used for message encryption. The random number, r, is treated as the firstblock of the plaintext.

5. Conclusion

A new technique for authenticating shortencrypted messages is proposed. The fact that the message to be authenticated must also be encrypted is used to deliver a random nonce to the intended receiver via the ciphertext.

The proposed schemes are shown to be orders of magnitude faster, and consume orders of magnitude less energy than traditional MAC algorithms. Therefore, they are more suitable to be used in computationally constrained mobile and pervasive devices.

6.Acknowledgments

A preliminary version of this paper appeared in the 12th International Conference on Information and Communications Security-ICICS 2010 [65].

References

Example follow

[1] M. Bellare, R. Guerin, and P. Rogaway, "XOR MACs: NewMethods for Message Authentication Using Finite PseudorandomFunctions," Proc. 15th Ann. Int'l Cryptology Conf. Advances inCryptology (CRYPTO '95), pp. 15-28, 1995.

Books

[2] L. Carter and M. Wegman, "Universal Hash Functions," J. Computer and System Sciences, vol. 18, no. 2, pp. 143-154, 1979.

Chapters in Books

[3] M. Bellare, J. Kilian, and P. Rogaway, "The Security of the CipherBlock Chaining Message Authentication Code," J. Computer andSystem Sciences, vol. 61, no. 3, pp. 362-399, 2000.

Theses:

G. *Tsudik, "Message Authentication with One-Way Hash Functions,"ACM SIGCOMM Computer Comm. Rev., vol. 22, no. 5,pp. 29-38, 1992.*