ISSN:0975-9646

Dynamic Message Authentication Code for Short Messages

D.Ganesh, A.Jahnavi, M.Trivikram
Department of Computer Science
Sree Vidyanikethan Engineering College, Andhra Pradesh, India

***Abstract*—Now-a-days with the increase of technology in every field, many applications rely on the existence of small devices that can exchange information and form communication networks. Short messages are widely in use these days. So many applications rely on the existence of small devices for communication. Here the confidentiality and the integrity play a major role. So we propose two techniques. In the first technique we authenticate the message and encrypt it with a short random string. In the second technique the extra assumptions are made whether the algorithm used is a block cipher and also improve them. MACs provide integrity for messages. Without taking it as an advantage the message must be checked whether it is encrypted or not. The main goal is to utilize the security that the algorithm can provide to design more efficient authentication mechanism.**

Keywords—Tag generation; Authentication; Performance

I. INTRODUCTION

The main goal of cryptography is to preserve the integrity of messages exchanged over public channels. A message authentication code algorithm (MAC) is designed for the sole purpose of preserving message integrity. Pervasive computing is the growing trend towards embedding microprocessors in everyday objects, it means "existing everywhere". Pervasive computing devices are completely connected and constantly available. They combine the current network technologies with wireless computing, voice recognition, internet capability and artificial intelligence is to create an environment where the connectivity of devices is embedded in such a way that the connectivity is unobtrusive and always available. Such pervasive computing and mobile computing devices rely on short messages for which MAC can be computed more efficiently.

Based on their security MACs can either be unconditionally secure or computationally secure. MACs provide message integrity against the forgers with unlimited computational power. On the other hand, computationally secure MACs are only secure when forgers have limited computational power.

The use of universal hash function families in the carter-wegman style is not restricted to the design on unconditionally secure authentication. Computationally secure MACs based on universal hash functions can be constructed with two rounds of computations. In the first round the message to be authenticated is compressed using a universal hashing function. Then in the second round, the compressed image is processed with a cryptographic function. Universal hashing based MACs give better performance when compared to block cipher or cryptographic hashing based MACs.

One of the main differences between unconditionally secure MACs based on universal hashing is the requirement to process the compressed image with a cryptographic primitive in the latter class of MACs.

Two observations to me made are:

1) They are designed independently of any other operations required to be performed on the message to be authenticated.
2) The most existing MACs are designed for the general computer communication systems, independently of the properties that messages can possess.

There have been significant efforts devoted to the design of hardware efficient implementation that suite such small devices. However, there has been little or no effort in the design of message authentication codes that can utilize other operations and the special properties of such networks.

II. LITERATURE SURVEY & RELATED WORK

The previous approaches for MAC include "A2 – codes from universal hash classes" the purpose of this traditional theory of unconditional authentication (A-Codes) is to protect the transmitter and receiver from deception by an outside opponent. It is assumed that transmitter and receiver trust each other, Simmons extended this model to include protection against certain frauds by transmitter and receiver. This model uses an arbiter, who distributes partial keys to transmitter and receiver and decides in cases of controversy between transmitter and receiver. It is assumed that the arbitrary is trust worthy. The corresponding systems have been termed A2-codes by Simmons.

Another approach "Fast hashing on Pentium" here a cryptographic hash function h maps bit strings of arbitrary finite length into strings of fixed length. Given h and an input x computing h(x) must be easy. A one way hash function must provide both pre-image resistance and second pre-image resistance i.e. it must be computationally infeasible to find respectively, any input which hashes to any pre-specified input. We try to make use of the existing approaches and improve them to utilize their underlying functionality more efficiently.

One of the most known block cipher is CBC-Mac based MACs. It is specified in the federal information processing standards publication and ISO. CMAC, a modified version of CBC-MAC is presented in the NIST special publication which was OMAC. Some other block cipher based MACs include XOR-MAC and PMAC.

Can MAC provide full integrity?

The answer for this is the two techniques are proposed

1) The message that is authenticated must also be encrypted with any secure encryption algorithm by appending the short random string. Since the random strings used for different operations are independent, the authentication algorithm can benefit from the simplicity of unconditional secure authentication to allow for faster and more efficient authentication.
2) We make extra assumptions that the used encrypted algorithm is a block cipher based to further improve the computational efficiency of the first technique.

The general purpose of MAC algorithm that is used to exchange the messages in the system might not be the efficient solution and may lead to the waste of resources.

The example for iterated cryptographic hash function in the design of message authentication code is HMAC. It was later adopted as a standard. Another cryptographic hash function based MAC is the MDx-MAC. HMAC and two variants of MDx-MAC are specified in the ISO/IEC.

III. Abbreviations And Acronyms

A. Notations

- Z_p – Finite integer ring with the addition and multiplication operations performed modulo p.
- Z_p* - Multiplicative group modulo p
- If two strings are of same length then XOR operation is performed.
- If there are any two strings then concatenation operation is done on the two strings (a||b);
- S$s – Selecting an element from the set s uniformly at random and assigning it to the letter S.

B. Negligible functions

Function Negl: N->R is said to be negligible if for any two nonzero polynomial poly, there exists N_0 such that for all N>N_0;

|Negl(N)|<1/|poly(N)|

C. Indistinguishability under choosen plain text attacks

Security notion for encryption algorithm

- in distinguishability under chosen plaintext attacks (IND-CPA)
- A – Adversary
- E – Encryption Algorithm
- Encryption Algorithm is IND-CPA secure if the adversary, after calling the encryption a polynomial number of timer, is given a cipher text corresponding to one or two plaintext messages cannot determine the plaintext corresponding to the cipher text.
- Let Adv_{Σ}^{Priv}(A) be an adversary's advantage

Then E is said to be IND-CPA secure if

$$Adv_{\Sigma}^{Priv}(A) <= ½+negl(N)$$

IV. Proposed System

Let N-1 be the upper bound on the length of the messages to be authenticated and should not be longer than N-1 bits Integer k_s at random from multiple group Z_p*. Here p denotes prime number. k_s is the secret key and is used to legitimate users for the message authentication. P need not to be secret. Let e be any IND-CPA secure algorithm. M denotes the short messages that are to be transmitted confidentially. Instead of authenticating the message using MAC this following procedure. Input message m, at random nonce r∈ Z_p. Integers representing the distinct messages are also distinct. m||r is appended to a message. Message m is calculated as

$$T=mk_s+r \text{ (mod p)}$$

Remark 1: nonce r is generated internally and is not a part of the chosen attack. R needs no special key management. It is delivered to the receiver as a part of encrypted cipher text.

Now cipher text c=e(m||r), authentication tag T are computed and transmitted to the intended receiver. The receiver decrypts is to extract m and r.

V. Performance Discussion

There are three classes of standard message authentication codes

1) MAC based on clock ciphers
2) MAC based on cryptographic hash functions
3) MAC based on universal hash function families

Universal hashing function is more computationally efficient than block ciphers and cryptographic hash functions.

It has two phases

1) Message compression phase using a universal hashing function
2) Cryptographic phase in which the compressed image is processed with a cryptographic primitive.

When the messages are to be authenticated are short, the modules prime p can also be small. For short messages, the cryptographic phase is the most time consuming phase. Since we target application in which messages are short eliminating the need to perform such a cryptographic operation will have a significant impact on the performance of the MAC operation. The cryptographic hash functions SHA-256 and SHA-512 run

in about 23.73 cycles/byte and 40.18 cycles/byte, respectively
the modular multiplication of equation) runs about 1.5 cycles/byte.Another advantage of proposed method is low power devices and increases hardware efficiency.

VI. Security Model

Message authentication scheme consists of signing algorithm s, and verifying algorithm v. signing algorithm is probabilistic and verifying algorithm is not probabilistic. l is the length of the shared key and N is the resulting authentication tag. The input is given as a l bit key k and the message m, N-bit tag T, algorithm v. The output is accept when it is displayed as 1 and rejected if displayed as 0. A can query s to generate a tag for a plaintext of its choice and ask the verifier v to verify that T is a valid tag for the plaintext.
A's attack on the scheme is described as

1) A random string of length l is selected as the shared secret.
2) A is the signing query on m is T=s(k,m) and it returns to A.
3) A makes verify query(m,T) decision d=V(k,m,T) and it returns to A.

A cannot compute verify predicate, so verify queries are allowed. A must not see the secret key k, coin tosses s. The outcome of running the experience in the presence of an adversary is used to define security.

A. *Security analysis*

Providing confidentiality of the system is security analysis

1) **Data privacy**:

Theorem: Adversary chooses the messages be m1 and m2 of equal length B϶{0,1}. When encryption is done it gives the cipher text. As of the previous equations the value will be less than ½. The proposed authentication is

$$Adv_{\Sigma}^{Priv}(A)<=Adv_{\epsilon}^{ind-cpa}(\beta)$$

Proof: T=mk_s+r
r is not a part of the message. So the equation is perfectly secret.

$$Adv_{\Sigma}^{priv}(A)<=Adv_{\epsilon}^{ind-cpa}(\beta)$$

2) **Data authenticity:**

Theorem: $Adv_{\Sigma}^{auth}(A)<=Adv_{\epsilon}^{ind-cpa}(\beta)+1/(p-1)$

This states that if the adversary's advantage in breakage the IND-CPA security of underlying encryption is negligible then so is breaking the integrity.

Proof: let m=m_i+e (mod p) for any I ∈ {1,2,3,…9}

R=r_i+s

T=mk_s+r (mod p)

=(m_i+ ϵ) k_s+(r_i+δ) (mod p)

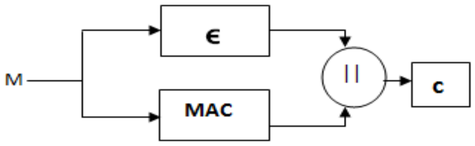
T=T_i+∈k_s+s (mod p)

(m,T) requires $T_i + \epsilon k_s + s$ modulo p. ks is the secret as long as it does not break encryption successful forgery 1/p-1. k_s and r are used only once.

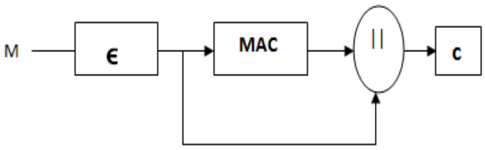
3) **Security encryption:**

Security is provided in one of 3 ways as such

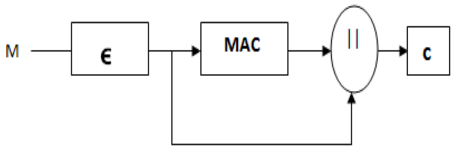
a) Encrypt and authenticate
b) Encrypt then authenticate
c) Authenticate then encrypt



a) Encrypt and authenticate



b) Encrypt then authenticate



b) Encrypt then authenticate

VII. From Weak To Strong Forgeability

There are two notions of forge ability

1) A MAC algorithm can be weakly un-forgeable under chosen message attacks (WUF-CMA)
2) Strongly un-forgeable under chosen message attacks (SUF-CMA)

To determine ∈ input a message m and it generates the output as random string s. then computes the PRF_x (S). Here the PRF is the pseudorandom function by x which is secret. It then transmits c=(S, PRF_x (S)+m)

The next cipher text is calculated as c=(S, PRF_x (S)+m||r)

Then the tag is calculated as T=mk_s+r (mod p)

In the next case let s1 be the string then the cipher text is denoted as c1 which is

C1=(S, PRF_x (S) + (m||k) + s1) = (a, PRF_x (S) + (m||k+s1))

After the cipher text is generated the two tags are generated.

T1=mk_s+r+1 (mod p)

T2=mk_s+r-1 (mod p)

A message can be authenticated using the different tags with the high probability. If the tag has the fixed identity then the message is to be authenticated. WUF-CMA allows the authentication of the same identity by malicious users. If the adversary modifies the value of r then forgery is successful. To rectify the message must be authenticated. This can be done with another secret key $k_s^{|}$

T=mk_s+r$k_s^{|}$ (mod p)

σ =mk_s (mod p) This is the efficient way of achieving the same. Then the r is removed from the equation then the result must also be encrypted.

The security parameters n and the N-bit prime integer p is the input and the shared key is the k_s ϵ $\mathbb{Z}_p$*. The input message m belongs to $\mathbb{Z}_p$

σ= mk_s (mod p)

C=E(m, σ)

E(m)||E(σ)

They can be calculated separately

c=E(m)

t=E(σ)

If IND-CPA is secure then it generates the type authenticate then encrypt.

Theorem 3: The proposed scheme is strongly forgeable under chosen message attacks (SUF-CMA) provided the adversary's inability to break the IND-CPA security of the underlying encryption algorithm. (m,T) are the message and Tag

m-> σ with same message and different tag. σ is same and the difference between t and t1 is the probabilistic behavior

$Adv_{\Sigma}^{suf-cma}$(A)<=$Adv_{\varepsilon}^{ind-cpa}$(β)+negl(N)

Proof: For a successful forgery, the adversary must predict the correct cipher text. However, that by the definition of IND-CPA security, the adversary's chance of predicting the correct cipher text is negligible. Therefore, the adversary's advantage of breaking the SUF-CMA security of the scheme is negligible provided the IND-CPA security of the encryption algorithm. That is,

$Adv_{\Sigma}^{suf-cma}$(A)<=$Adv_{\varepsilon}^{ind-cpa}$(β)+negl(N)

VIII. Encryption Using Pseudorandom Permutation

1) *Encryption :*

Cipher block chaining (CBC) mode of operation can be used to encrypt the messages. We will show the idea of utilizing the pseudo randomness of block ciphers in simple way to further improve the efficiency of the authentication algorithm.

A pseudo random function is a collection of efficiently computable functions which emulate a random oracle in the following way. No efficient algorithm can distinguish between a function chosen randomly from the PRF family and a random oracle. Pseudo random functions are vital tools in the construction of cryptographic primitives, especially secure encryption schemes.

A PRF is an efficient deterministic function that maps two distinct sets. Essentially a true random function would just be composed of a look up table filled with random entries.

A PRF is considered to be good if its behavior is indistinguishable from a true random function. Therefore given a true random function and a PRF, there should be no efficient method of determining if the output was produced by a true random function or the PRF.

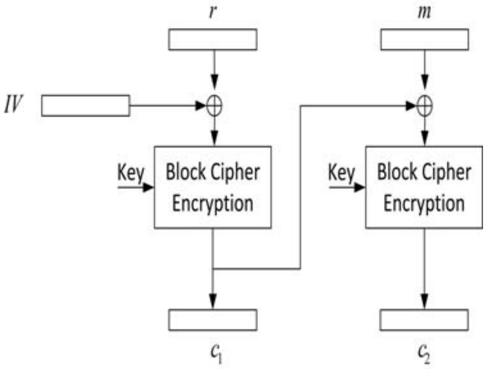


Fig: Cipher block chaining mode

The figure shows the cipher block chaining mode of operation. Consider how the concatenation of r and m goes to the encryption algorithm E, as an input.We may desire E to be a strong pseudorandom permutation; however, since N can be sufficiently long (e.g., 128 or larger), constructing a block cipher that maps 2N-bit strings to 2N-bit strings can be expensive

Therefore the nonce r is treated as the first plaintext block and is XORed with the initialization vector (IV) to insure IND-CPA security. The first cipher text block,

$$c1 = F_{kE} (IV \oplus r);$$

is then XORed with the second plaintext block, m in our construction, to produce the second cipher text block,

$$c2 = F_{kE} (c1 \oplus m);$$

Where kE is the key corresponding to the block cipher. The resulting

$$c = E(r , m) = IV ||c1||c2$$

is then transmitted to the intended receiver as the cipher text.

2) *Performance Discussion :*

The authentication technique here requires only one modular addition.

- Addition is performed in O(n) time
- The fastest integer multiplication algorithms typically require O(n log n log log n) time

Therefore, as efficient as the scheme proposed the authentication technique of of this section is at least
O(log n log log n) faster.

Complexity analysis, however, can be inaccurate by absorbing large constants. For n = 32, the simple addition of this scheme runs in about 0.02 cycles/bytes as opposed to the 1.5 cycles/byte of the previous scheme. The reason that the improvement is better than O(log n log log n) is mainly due to the modular reduction. That is, while reduction modulo a prime integer is a non-trivial operation, reduction modulo 2n can be performed by simply stopping at the nth bit.

IX. Conclusion

With the rapid growth and innovations witnessed in the mobile industry, the communication field has greatly transformed. Continued innovation in the industry, such as mobile Internet and social networking applications has further had a measurable impact in the communication field. In such mobile and pervasive computing where the messages to be authenticated are short we can further improve the present existing Message authentication codes.It has been demonstrated in this paper that authentication tags can be computed with one addition and a one modular multiplication.

Given that messages are relatively short, addition and modular

Multiplication can be performed faster than existing computationally secure MACs in the literature of cryptography. When devices are equipped with block ciphers to encrypt messages, a second technique that utilizes the fact that block ciphers can be modelled as strong pseudorandom permutations is proposed to authenticate messages using a single modular addition. Thus the present scheme reduces the energy consumption and running time for computing MAC tags.

References

[1] J. Bierbrauer, “A2-codes from universal hash classes,” in Advances in Cryptology–EUROCRYPT’95, vol. 921, Lecture Notes in Computer Science. Springer, 1995, pp. 311–318.

[2] V. Shoup, “On fast and provably secure message authentication based on universal hashing,” in Advances in Cryptology–CRYPTO’96, vol. 1109, Lecture Notes in Computer Science. Springer, 1996, pp. 313–328.

[3] G. Tsudik, “Message authentication with one-way hash functions,” ACM SIGCOMM Computer Communication Review, vol. 22, no. 5, p. 38,1992.

[4] D. McGrew and J. Viega, “The security and performance of the Galois/Counter Mode (GCM) of operation,” in Progress in Cryptology- INDOCRYPT’04, vol. 3348, Lecture notes in computer science. Springer, 2004, pp. 343–355.

[5] K. Venkatasubramanian, A. Banerjee, and S. Gupta, “Ekg-based key agreement in body sensor networks,” in INFOCOM Workshops 2008, IEEE. IEEE, 2008, pp. 1–6.

[6] N. Ferguson, D. Whiting, B. Schneier, J. Kelsey, and T. Kohno, “Helix: Fast encryption and authentication in a single cryptographic primitive,” in Proceedings of Fast Software Encryption–FSE’03, vol. 2887, Lecture notes in computer science. Springer, 2003, pp. 330–346

[7] B. Alomair and R. Poovendran, “E-MACs: Towards More Secure and More Efficient Constructions of Secure Channels,” in the 13th International Conference on Information Security and Cryptology – ICISC’10. Springer, 2010.

[8] J. Carter and M. Wegman, “Universal classes of hash functions,” in Proceedings of the ninth annual ACM symposium on Theory of computing–STOC’77. ACM, 1977, pp. 106–112.

[9] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. Culler, “SPINS: Security protocols for sensor networks,” Wireless networks, vol. 8, no. 5, pp. 521–534, 2002.

[10] T. Iwata and K. Kurosawa, “omac: One-key cbc mac,” in Fast Software Encryption–FSE’03, vol. 2887, Lecture notes in computer science. Springer, 2003, pp. 129–153

[11] M. Bellare, R. Guerin, and P. Rogaway, “XOR MACs: New methods for message authentication using finite pseudorandom functions,” in Advances in Cryptology–CRYPTO’95, vol. 963, Lecture Notes in Computer Science. Springer, 1995, pp. 15–28

[12] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagord “RFID systems: A survey on security threats and proposed solutions,” in Personal Wireless Communications. Springer, 2006, pp. 159–170.

[13] F. Muller, “Differential attacks against the Helix stream cipher,” in Fast Software Encryption–FSE’04, vol. 3017, Lecture Notes in Computer Science. Springer, 2004, pp. 94–108.

[14] O. Goldreich, Foundations of Cryptography. Cambridge University Press, 2001

[15] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, “A concrete security treatment of symmetric encryption,” in 38th Annual Symposium on Foundation of Computer Science–FOCS’97. IEEE Computer Society, 1997, pp. 394–403.