www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 5 May 2015, Page No. 12095-12098

Efficient Technique for Providing Authentication of Short Encrypted Messages

T Vijaya[1], Sivagama Sundari G[2]

[1]MTECH (CSE), MVJCE, Bangalore, Karnataka, India.
vijaya.nitk@gmail.com

[2]Associate Professor (CSE), MVJCE, Bangalore, Karnataka, India
itsmevasigas@gmail.com

Abstract- ***with the advancement in the technology, many of the applications depend on the existence of the small devices to communicate by exchanging messages. In such applications, the messages exchanged are short. The confidentiality and integrity of communicated short messages is of at most important in such applications. Here in this paper, we propose two new techniques for authenticating short encrypted messages that meets the requirement of such applications. The basic notion behind the proposed techniques is exploiting the security that the encryption algorithm provides to design an authentication mechanism that is more efficient than the existing authentication technique in the literature of cryptography.***

Keywords-Authentication, universal hash-function families, block cipher.

1. INTRODUCTION

When a secret message that has to be transmitted through a communication channel must not be transmitted as a plaintext; else unintended receivers who are listening to the channel can infer the communicated secret.

In applications where third party or intruder can modify the transmitted message, encrypted messages are to be protected with mechanism to make sure of the integrity check.

In communications all the transmission through the communication channel is a data. The entity that will give the sender and the receiver the assurance of unaltered data is a fixed length data called MAC (Message authentication code). Fig 1 shows the MAC architecture.

There are two important observations about existing MAC algorithm. First, they are designed individually of any other operations that can be performed on the message to be authenticated. For Example, Existing Macs are not suitable if the authenticated message must also be encrypted whose functionality can be provided by the encryption algorithm. Second, existing Macs are designed for computer communication system, independent of the properties that the message possesses. For example, existing Macs are inefficient if the messages to be authenticated are short.

In this work, two techniques for authenticating short encrypted messages that are more efficient than existing approaches are proposed. In first technique, we exploit the fact that the message to be authenticated is also encrypted with any secure encryption, to append a short random string to be used in the authentication process. In second technique, an extra assumption is made that the encryption algorithm used is block cipher based to further improve the computational efficiency of the first technique. The motive behind the investigation is that using a generalpurpose MAC algorithm to authenticate messages might not be the efficient solution and can lead to waste of resources already available, specifically the security provided by encryption algorithm

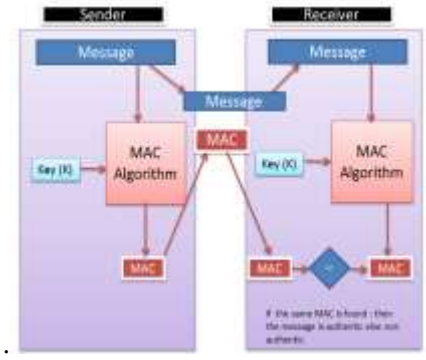

Fig 1: MAC architecture

The rest of our paper is organized as follows. In section 2 we list the notations and prefaces used. In section 3 we discuss the first authentication technique. In section 4 we discuss the second technique with assumption of block cipher based as encryption. In section 5 we conclude our paper.

2. NOTATIONS AND PREFACES

2.1 Notations

- Used Zp as the usual notation for the finite integer ring with the multiplication and addition modulo p.
- Used Zp* as the usual notation for multiplicative group modulo p.
- For two strings *a* and*b* of same length, ($a \oplus b$) is the bitwise exclusive-or (XOR) operation.
- For any two strings *a*and*b*, (*a* || *b*) denotes the concatenation operation.

2.2 Negligible functions

A function negl: N->R is said to be negligible if it converges to zero faster than the reciprocal of any polynomial function [2].

2.3 Indistinguishability under Chosen Plain Text Attacks

Indistinguishability under chosen plain text attack (IND-CPA) is the important security notion for encryption. Let A be an adversary who has access to oracle to an encryption algorithm, *E*, and ask the oracle to encrypt a polynomial number of messages to get their equivalent cipher texts. The encryption algorithm is said to be IND-CPA secure, if the adversary after calling the encryption a polynomial number of times is given a cipher text corresponding to one of the two plain text messages cannot determine the plaintext message corresponding to the given cipher text with an advantage higher ½.*E* is said to be IND-CPA secure, if adversary's advantage of determining plaintext corresponding to given cipher text <= ½+Negl (N), where N is security parameter, usually the length of the secret key [3].

3. FIRST TECHNIQUE

In this section, the first authentication scheme that can be used with any IND-CPA secure encryption algorithm is described. An important assumption is made that the message that needs to be authenticated is no longer than a predefined length.

Let N-1 be the upper bound on the length, in bits of exchanged messages. The messages to be authenticated can no longer be greater than N-1 bit long. Choose p as an n bit long prime integer. Choose an integer *K* (secret key) uniformly at random from the multiplicative group Zp*.

The prime integer *p* and secret key k are distributed to the intended user and will be used for message authentication. Let *E* be any IND-CPA encryption algorithm, m be short message. Instead of authenticating the message using a traditional MAC algorithm, consider the following concept.

On input message *m*, a random nonce *r* an element of Zp is chosen. Now, *r* is appended to the message and the resulting *m* || *r*, where "||" denotes the concatenation operation, goes to the encryption algorithm as an input. Then, the authentication tag of the message can be obtained as

$$T = mk + r \pmod{p} \qquad (1)$$

Since the generation of pseudorandom numbers can be measured expensive for computationally limited devices, there have been a several attempts in designing true random number generators that are suitable for RFID tags ([4]–[6]) and for low-cost sensor nodes ([7]–[9]). Thus we are assuming the availability of such random number generators.

3.1 Security and Performance discussion

Since Mac based on universal hashing is known to be more efficient than the Macs based on block ciphers and cryptographic hash function [10]. We compare the proposed MAC to the universal hash function based MACs.

Two phases of computations are required in MAC based on universal hashing: 1. a message compression phase using a universal hash function and, 2. a cryptographic phase wherein the compressed image is processed with a cryptographic primitive (a block cipher or a cryptographic hash function). The compression phase is similar to the computation of equation (1) of the proposed MAC. As opposed to standard universal hash functions based MACs; there is no need to process the result of equation (1) with a cryptographic function in the proposed technique.

When the messages that need to be authenticated are short, the modulus prime, *p*, can also be small. For a small modulus, the modular multiplication of equation (1) is not a time consuming task. That is, for short messages, the

cryptographic phase is the most time consuming part. Since we focus on applications in which messages are short, excluding the need to perform such a cryptographic operation will have a significant impact on the performance of the MAC operation. For instance, while the cryptographic hash functions SHA-256 and SHA-512 run in about 23.73 cycles/byte and 40.18 cycles/byte, respectively [11], the modular multiplication of equation (1) runs in about 1:5 cycles/byte [12], which clarifies the importance of removing the cryptographic phase from our MAC.

Another major advantage of the proposed method especially in case of low-power devices is hardware efficiency. The hardware required to perform modular multiplication is less than the hardware required to perform cryptographic operations. As a result, there is a reduction in energy consumption. For instance, the cryptographic hash functions consume 20-30 J/bit [13], whereas modular multiplication can consume as low as 0:02 J/bit [14].

The confidentiality and the security of the composed authenticated encryption system are discussed in [1].

4. 4.SECOND TECHNIQUE

In this section, we define an approach for message authentication mechanism that is faster than the one defined in previous section.

4.1 Proposed System

Let *m* be a short message which has to be transmitted to a receiver in a secure manner. For every message that is transmitted, a random nonce r an element of $Z_{2N}$is chosen.

The concatenation of *r* and *m* goes to the encryption algorithm, say *E*, as input. We may desire *E* to be strong pseudorandom permutation; but, since N can be sufficiently long, constructing a block cipher that maps 2N-bit strings to 2N-bit strings may be expensive. Therefore, we resort to the well-studied CBC (Cipher Block Chaining) mode of operation to construct *E*as illustrated in Fig 2. The cipher text

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

is then transmitted to the indented receiver.

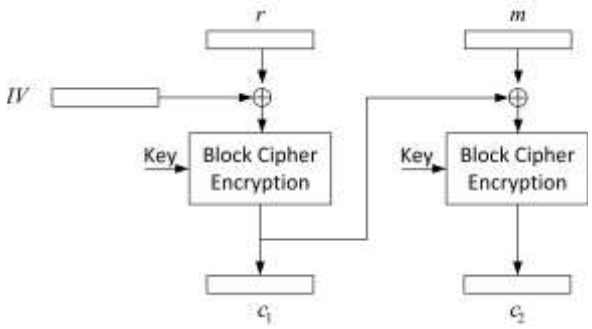

Fig 2: CBC mode of encryption

With the encryption described above, authentication becomes simpler than the one described in previous section. The authentication tag is calculated as

$$T = m + r \ (mod\ 2^N) \qquad (2)$$

The intended receiver upon receiving the cipher text decrypts it to extract *r* and *m*. The receiver then calculates the tag from extracted *m* and *r* as in equation 2. If the received tag and the calculated tag are matching, the integrity is satisfied, the message is considered authentic. Otherwise, the message integrity is denied. The authentication technique of this section is faster than that described in section 3[1].

5. CONCLUSION

A new technique for authenticating short encrypted message is proposed. We utilize the fact that the message to be authenticated must also be encrypted, to deliver a random nonce via the cipher text to the intended receiver. In this paper it is demonstrated that authentication tag can be computed with one addition and one modular multiplication. For messages that are short, addition and modular multiplication can be performed than existing MAC in the literature of cryptography. If the devices are equipped with block ciphers to encrypt message, by using the fact that block ciphers can be modeled as strong pseudorandom Permutations, the second technique can be used to authenticate message using a single modular addition. The proposed mechanism is shown to be computationally faster and consume less energy than the traditional MAC algorithms.

References:

1. Basel AlomairHur and RadhaPoovendran"Efficient Authentication for Mobile and Pervasive Computing" inMobile Computing, IEEE Transactions on (Volume: 13, Issue: 3) February 2014
2. O. Goldreich, Foundations of Cryptography. Cambridge UniversityPress, 2001.
3. S. Goldwasser and S. Micali, "Probabilistic encryption," Journal ofComputer and System Sciences, vol. 28, no. 2, pp. 270–299, 1984.
4. Z. Liu and D. Peng, "True Random Number Generator in RFIDSystems Against Traceability," in IEEE Consumer Communications and Networking Conference–CCNS,06, vol. 1. IEEE, 2006, pp. 620–624.
5. D. Holcom,W. Burleson, and K. Fu, "Initial SRAM state as a Fingerprintand Source of True Random Numbers for RFID Tags," in Workshop onRFID Security–RFIDSec'07, 2007.
6. D. Holcomb, W. Burleson, and K. Fu, "Power-up SRAM State as anIdentifying Fingerprint and Source of True Random Numbers," IEEETransactions on Computers, vol. 58, no. 9, 2009.
7. C. Petrie and J. Connelly, "A noise-based IC random number generatorfor applications in cryptography," IEEE Transactions on Circuits andSystems I: Fundamental Theory and Applications, vol. 47, no. 5, pp.615–621, 2000.
8. S. Callegari, R. Rovatti, and G. Setti, "Embeddable ADC-based truerandom number generator for cryptographic applications exploitingnonlinear signal processing and chaos," IEEE Transactions on Signal Processing, vol. 53, no. 2 Part 2, pp. 793–805, 2005.
9. A. Francillon, C. Castelluccia, and P. Inria, "TinyRNG: A cryptographicrandom number generator for wireless sensors network nodes," inModeling and Optimization in Mobile, Ad Hoc and Wireless Networks–WiOpt'07. Citeseer, 2007, pp. 1–7.
10. H. van Tilborg, Encyclopedia of cryptography and security. Springer,2005.
11. J. Nakajima and M. Matsui, "Performance analysis and parallel implementationof dedicated hash functions," in Advances in Cryptology–EUROCRYPT 2002. Springer, 2002, pp. 165–180.
12. J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, "UMAC:Fast and Secure Message Authentication," in Advances in Cryptology–CRYPTO'99, vol. 1666, Lecture Notes in Computer Science. Springer,1999, pp. 216–233.
13. B. Preneel, "Using Cryptography Well," Printed handout availableathttp://secappdev.org/handouts/2010/Bart%20Preneel/usingcrypto well.pdf, 2010.
14. J. Großsch¨adl, R. Avanzi, E. Savas¸, and S. Tillich, "Energy-efficientsoftware implementation of long integer modular arithmetic," in Proceedingsof the 7th international conference on Cryptographic hardwareand embedded systems – CHES'05, vol. 3659. Springer-Verlag, 2005,pp. 75–90.