

RESEARCH ARTICLE



ISSN: 2321-7758

EFFICIENT AUTHENTICATION FOR MOBILE AND PERVASIVE COMPUTING

B.SUJATHA

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
RAJOLI VEERA REDDY PADMAJA ENGINEERING COLLEGE FOR WOMEN, KADAPA

Article Received:01/06/2015

Article Revised on:17/06/2015

Article Accepted on:20/06/2015



ABSTRACT

With today's technology, many applications rely on the existence of small devices that can exchange information and form communication networks. In a significant portion of such applications, the confidentiality and integrity of the communicated messages are of particular interest. In this work, we propose two novel techniques for authenticating short encrypted messages that are directed to meet the requirements of mobile and pervasive applications. By taking advantage of the fact that the message to be authenticated must also be encrypted, we propose provably secure authentication codes that are more efficient than any message authentication code in the literature. The key idea behind the proposed techniques is to utilize the security that the encryption algorithm can provide to design more efficient authentication mechanisms, as opposed to using standalone authentication primitives.

©KY Publications

INTRODUCTION

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

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 standpoints. 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. That is, after agreeing on a key, legitimate users can exchange an arbitrary number of authenticated messages with the same key. Depending on the main building block used to construct them, computationally secure MACs can be classified into

three main categories: block cipher based, cryptographic hash function based, or universal hash-function family based.

CBC-MAC is one of the most known block cipher based MACs, specified in the Federal Information Processing Standards publication and the International Organization for Standardization. CMAC, a modified version of CBC-MAC, is presented in the NIST special publication, which was based on the OMAC of. Other block cipher based MACs include, but are not limited to, XOR-MAC and PMAC. The security of different MACs has been exhaustively studied.

The use of one-way cryptographic hash functions for message authentication was introduced by Tsudik. A popular example of the use of iterated cryptographic hash functions in the design of message authentication codes is HMAC, which was proposed by Bellare. HMAC was later adopted as a standard. Another cryptographic hash function based MAC is the MDx-MAC proposed by Preneel and Oorschot. HMAC and two variants of MDx-MAC are specified in the International Organization for Standardization. Bosselaers et al. described how cryptographic hash functions can be carefully coded to take advantage of the structure of the Pentium processor to speed up the authentication process.

The use of universal hash-function families in the Carter-Wegman style is not restricted to the design of 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 hash function. Then, in the second round, the compressed image is processed with a cryptographic function. Popular examples of computationally secure universal hashing based MACs include, but are not limited to.

Indeed, universal hashing based MACs give better performance when compared to block cipher or cryptographic hashing based MACs. In fact, the fastest MACs in the cryptographic literature are based on universal hashing. The main reason behind the performance advantage of universal hashing based MACs is the fact that processing messages block by block using universal hash functions is orders of magnitude faster than processing them

block by block using block ciphers or cryptographic hash functions.

One of the main differences between unconditionally secure MACs based on universal hashing and computationally secure MACs based on universal hashing is the requirement to process the compressed image with a cryptographic primitive in the latter class of MACs. This round of computation is necessary to protect the secret key of the universal hash function. That is, since universal hash functions are not cryptographic functions, the observation of multiple message-image pairs can reveal the value of the hashing key. Since the hashing key is used repeatedly in computationally secure MACs, the exposure of the hashing key will lead to breaking the security of the MAC. Thus, processing the compressed image with a cryptographic primitive is necessary for the security of this class of MACs. This implies that unconditionally secure MACs based on universal hashing are more efficient than computationally secure ones. On the negative side, unconditionally secure universal hashing based MACs are considered impractical in most modern applications, due to the difficulty of managing one-time keys.

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 to be authenticated. For instance, if the authenticated message must also be encrypted, existing MACs are not designed to utilize the functionality that can be provided by the underlying encryption algorithm. Second, most existing MACs are designed for the general computer communication systems, independently of the properties that messages can possess. For example, one can find that most existing MACs are inefficient when the messages to be authenticated are short.

Nowadays, however, there is an increasing demand for the deployment of networks consisting of a collection of small devices. In many practical applications, the main purpose of such devices is to communicate short messages. A sensor network, for example, can be deployed to monitor certain events and report some collected data. In many sensor network applications, reported data consist of short confidential measurements. Consider, for instance, a sensor network deployed in a battlefield with the

purpose of reporting the existence of moving targets or other temporal activities. In such applications, the confidentiality and integrity of reported events are of critical importance. In another application; consider the increasingly spreading deployment of radio frequency identification (RFID) systems. In such systems, RFID tags need to identify themselves to authorized RFID readers in an authenticated way that also preserves their privacy. In such scenarios, RFID tags usually encrypt their identity, which is typically a short string (for example, tags unique identifiers are 64-bit long in the EPC Class-1 Generation-2 standard, to protect their privacy. Since the RFID reader must also authenticate the identity of the RFID tag, RFID tags must be equipped with a message authentication mechanism. Another application that is becoming increasingly important is the deployment of body sensor networks. In such applications, small sensors can be embedded in the patient's body to report some vital signs. Again, in some applications the confidentiality and integrity of such reported messages can be important.

There have been significant efforts devoted to the design of hardware efficient implementations that suite such small devices. For instance, hardware efficient implementations of block ciphers have been proposed. Implementations of hardware efficient cryptographic hash functions have also been proposed. However, there has been little or no effort in the design of special algorithms that can be used for the design of message authentication codes that can utilize other operations and the special properties of such networks.

SECTION-1

LITERATURE SURVEY

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 to be authenticated. For instance, if the authenticated message must also be encrypted, existing MACs are not designed to utilize the functionality that can be provided by the under-lying encryption algorithm. Second, most existing MACs are designed for the general computer communication systems, independently of the properties that messages can possess. For example, one can find that most existing MACs are inefficient when the messages to be authenticated are short. (For instance, UMAC,

the fastest reported message authentication code in the Cryptographic literature, has undergone large algorithmic changes to increase its speed on short messages) Nowadays, however, there is an increasing demand for the deployment of networks consisting of a collection of small devices. In many practical applications, the main purpose of such devices are to communicate short messages. A sensor network, for example, can be deployed to monitor certain events and report some collected data. In many sensor network applications, reported data consist of short confidential measurements. In this work, we pose the following research question: if there is an application in which messages that need to be exchanged are short and both their privacy and integrity need to be preserved, can one do better than Simply encrypting the messages using an encryption algorithm and authenticating them using standard MAC algorithm? We answer the question by proposing 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 authenticated is also encrypted, with any secure encryption algorithm, to append a short random string to be used in the authentication process. 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, without the difficulty to manage one-time keys. In the second technique, we make the extra assumption that the used encryption algorithm is block cipher based to further improve the computational efficiency of the first technique. The driving motive behind our investigation is that using a general purpose MAC algorithm to authenticate exchanged messages in such systems might not be the most efficient solution and can lead to waste of resources already available, namely, the security that is provided by the encryption algorithm.

SECTION-2

APPROACH

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

AUTHENTICATING SHORT ENCRYPTED MESSAGES:

In this first technique, we utilize the fact that the message to be authenticated is also encrypted, with any secure encryption algorithm, to append short random string to be used in the authentication process. 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, without the difficulty to manage one-time keys.

ENCRYPTING WITH PSEUDORANDOM PERMUTATIONS (BLOCK CIPHERS):

In this second technique, we make the extra assumption that the used encryption algorithm is block cipher based to further improve the computational efficiency of the first technique. The driving motive behind our investigation is that using a general purpose MAC algorithm to authenticate exchanged messages in such systems might not be the most efficient solution and can lead to waste of resources already available, namely, the security that is provided by the encryption algorithm. More efficient than existing approaches. The authentication algorithm can benefit from the simplicity of unconditional secure authentication to allow for faster and more efficient authentication, without the difficulty to manage one-time keys. The most efficient solution and can lead to waste of resources already available, namely, the security that is provided by the encryption algorithm.

CONCLUSION and FUTURE WORK

In this work, a new technique for authenticating short encrypted 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 cipher text. This allowed the design of an authentication code that benefit from the simplicity of unconditionally secure authentication without the need to manage one-time keys. In particular, 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, And a second technique that utilizes the fact that block ciphers can be modeled as strong

pseudorandom permutations is proposed to authenticate messages using a single modular addition. 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.

ACKNOWLEDGEMENT

We are happy to express our thanks to G.Prathap and all other asst.professors for their guidance. We are also like to thanks to our college members and all those people who have helped directly or indirectly to complete this research paper.

REFERENCES

- [1]. 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.
- [2]. M. Wegman and J. Carter, "New classes and applications of hash functions," in 20th Annual Symposium on Foundations of Computer Science—FOCS'79. IEEE, 1979, pp. 175–182.