ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Two Novel Techniques for Authenticating Short Encrypted Messages in Mobile and Pervasive Applications

C.Sudhakar
M.Tech,
Department of CSE,
Global Institute of Engineering and Technology,
Chilkur (V), RR District, Telganana.

Mrs. M.Jhansi Lakshmi
Associate professor,
HOD of CSE,
Global Institute of Engineering and Technology,
Chilkur (V), RR District, Telganana.

Abstract::

\

More than 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, to 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, to 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.

Index Terms:

Authentication, unconditional security, computational security, universal hash-function families, pervasive computing

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. 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 userscan 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. The security of different MACs has been exhaustively studied.

The use of one-way cryptographic hash functions for message authenticatio. The popular example of the use of iterated cryptographic hash functions in the design of message authentication codes is HMAC, which was proposed. The use of universal hash-function families in the 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In fact, the fastest MACs. Earlier designs used one-time pad encryption to process the compressed image. However, due to the difficulty to manage such ontime keys, recent designs resorted to computationally secure primitives. 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.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. 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. 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 in. Implementations of hardware efficient cryptographic hash functions have also been proposed. In the first technique, to 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, 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

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

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 standpoints.

DISADVANTAGES:

» Unconditionally secure universal hashing-based MACs are considered impractical in most modern applications, due to the difficulty of managing one-time keys

PROPOSED SYSTEM:

» In this paper 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 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.

ADVANTAGES:

» 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.

IMPLEMENTATION: AUTHENTICATING SHORT ENCRYPTED MESSAGES:

In this module, we describe our first authentication scheme that can be used with any IND-CPA secure encryption algorithm .An important assumption we make is that messages to be authenticated are no longer than a predefined length. This includes applications in which messages are of fixed length that is known a priori, such as RFID systems in which tags need to authenticate their identifiers, sensor nodes reporting events that belong to certain domain or measurements within a certain range, etc. The novelty of the proposed scheme is to utilize the encryption algorithm to deliver a random string and use it to reach the simplicity and efficiency of one-time pad authentication without the need to manage impractically long keys.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Security Model:

A message authentication scheme consists of a signing algorithm S and a verifying algorithm V. The signing algorithm might be probabilistic, while the verifying one is usually not. Associated with the scheme are parameters and N describing the length of the shared key and the resulting authentication tag, respectively.

Security of the Authenticated Encryption Composition:

In this module, it defined two notions of integrity for authenticated encryption systems: the first is integrity of plaintext (INT-PTXT) and the second is integrity of cipher text (INT-CTXT). Combined with encryption algorithms that provide in-distinguish ability under chosen plaintext attacks(IND-CPA), the security of different methods for constructing generic compositions is analyzed. Note that our construction is an instance of the Encrypt-and-Authenticate (E&A) generic composition since the plaintext message goes to the encryption algorithm as an input, and the same plaintext message goes to the authentication algorithm as an input.

Data Privacy:

Recall that two pieces of information are transmitted to the intended receiver (the cipher text and the authentication tag),both of which are functions of the private plaintext message. Now, when it comes to the authentication tag, observe that then once r serves as a one-time key (similar to the role r plays in the construction of Section. The formal analysis that the authentication tag does not compromise message privacy is the same as the one provided . The cipher text of equation ,on the other hand, is a standard CBC encryption and its security is well-studied; thus, we give the theorem statement below without a formal proof (interested readers may refer to textbooks in cryptography.

RESULTS:

In existing system 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. Use of encryption algorithm is block cipher based to further improve the computational efficiency of the technique. The driving motive behind 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.

In the proposed system have to deliberate the subsequent cryptographic methods that will be realistic in the input that input should be the short message that was called as the Multi-Security technique. Those encryption methods are the data encryption standard and the advanced encryption standard. Then it delivers the password based authentication method in the double encryption technique's cipher text. For significant the order of the operation they have to apply the avalanche effect but to make the method to secure the keys will be transmitted to the user through the mail of the personal contact of the user. In proposed system we have less time complexity, less computational cost, effective integrity, more secure while the transmission, more confidential.

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

FUTURE SCOPE:

In the future have to investigate about the further implementation of encryption techniques to enhance the process with the less time complexity and the high integrity in the process. And have to improve the whole performance by implementing the other process oriented to the security of the data in the mobile computing process. And also need to investigate about the other possible ways to improving the data security other than the cryptogrpahic techniques as the additional process to the data security of the data.

REFFERENCES:

[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.

[3] L. Carter and M. Wegman, "Universal hash functions," Journal of Computer and System Sciences, vol. 18, no. 2, pp. 143–154, 1979.

[4] M. Wegman and L. Carter, "New hash functions and their use in authentication and set equality," Journal of Computer and System Sciences, vol. 22, no. 3, pp. 265–279, 1981.

[5] 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.

[6] M. Atici and D. Stinson, "Universal Hashing and Multiple Authentication," in Advances in Cryptology–CRYPTO'96, vol. 96, Lecture Notes in Computer Science. Springer, 1996, pp. 16–30.

[7] T. Helleseth and T. Johansson, "Universal hash functions from exponential sums over finite fields and Galois rings," in Advances in cryptology– CRYPTO'96, vol. 1109, Lecture Notes in Computer Science. Springer, 1996, pp. 31–44.

[8] 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.

[9] J. Bierbrauer, "Universal hashing and geometric codes," Designs, Codes and Cryptography, vol. 11, no. 3, pp. 207–221, 1997.

[10] B. Alomair, A. Clark, and R. Poovendran, "The Power of Primes: Security of Authentication Based on a Universal Hash-Function Family," Journal of Mathematical Cryptology, vol. 4, no. 2, 2010.

[11] 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.

[12] FIPS 113, "Computer Data Authentication," Federal Information Processing Standards Publication, 113, 1985.

[13] ISO/IEC 9797-1, "Information technology – Security techniques –Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher," 1999.

[14] M. Dworkin, "Recommendation for block cipher modes of operation: The CMAC mode for authentication," 2005.

[15] 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.

[16] 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.