International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 4 Issue 6|| June 2015 || PP.38-41

An Efficient privacy preserving for Mobile and Pervasive Computing

[1]S.Hemalatha , [2]V.Nirmala
[1] *Assistant Professor, Department of Computer Application, Shrimati Indira Gandhi College, Trichy-2.*
[2]*Research Scholar, Department of Computer Science Shrimati Indira Gandhi College, Trichy-2.*

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.*

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

I. 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. 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 on-time 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.

II. Notations

To use Zp as the usual notation for the finite integer ring with the addition and multiplication operations performed modulo p. to use Z_ p as the usual notation for the multiplicative group modulo p; i.e., Z_ p contains the integers that are relatively prime top. For two strings a and b of the same length, (a _ b) denotes the bitwise exclusive-or (XOR) operation. For any two strings a and b, (ajjb) denotes the concatenation peration. For a nonempty set S, the notation s $ denotes the operation of selecting an element from the set S uniformly at random and assign . 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.

To propose 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? to answer the question by proposing two new techniques for authenticating short encrypted messages that are more efficient than existing approaches. 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. The advantages for proposed to More security, using two concepts one is mobile computing and another one is pervasive computing.

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, to make the extra assumption that the used encryption algorithm is block cipher based to further improve the computational efficiency of the first technique.

2.1AUTHENTICATING SHORT ENCRYPTED MESSAGES:

In this module, to describe our first authentication scheme that can be used with any IND-CPA secure encryption algorithm .An important assumption to 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.

2.2 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. On input an `-bit key k and a message m, algorithm S outputs an N-bit string called the authentication tag, or the MAC of m. On input an `-bit key k, a message m, and an N-bit tag , algorithm V outputs a bit, with 1 standing for accept and 0 for reject. To ask for a basic validity condition, namely that authentic tags are accepted with probability one.) for a random but hidden choice of k. A can query S to generate a tag for a plaintext of its choice and ask the verifier V to verify that _ is a valid tag for the plaintext. Formally, A's attack on the scheme is described by the following experiment:

1) A random string of length ` is selected as the shared secret.

2) Suppose A makes a signing query on a message m. Then the oracle computes an authentication tag _ = S(k; m)and returns it to A. (Since S may be probabilistic, this step requires making the necessary underlying choice of a random string for S, anew for each signing query.)

3) Suppose A makes a verify query (m; _). The oracle computes the decision

d = V(k; m; _) and returns it to A.

2.3 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.

2.4 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, to give the theorem statement below without a formal proof (interested readers may refer to textbooks in cryptography.

III. Conclusion

The 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 benefits 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, 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.

REFERENCES

[1] Z. Liu and D. Peng, "True Random Number Generator in RFID Systems Against Traceability," in IEEE Consumer Communications and Networking Conference–CCNS,06, vol. 1. IEEE, 2006, pp. 620–624.

[2] D. Holcom,W. Burleson, and K. Fu, "Initial SRAM state as a Fingerprint and Source of True Random Numbers for RFID Tags," in Workshop on RFID Security–RFIDSec'07, 2007.

[3] D. Holcomb, W. Burleson, and K. Fu, "Power-up SRAM State as an Identifying Fingerprint and Source of True Random Numbers," IEEE Transactions on Computers, vol. 58, no. 9, 2009.

[4] 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.

[5] S. Paul and B. Preneel, "Solving systems of differential equations of addition," in Australasian Conference on Information Security and Privacy–ICISP'05, vol. 3574, Lecture Notes in Computer Science. Springer, 2005, pp. 75–88.

[6] "Near Optimal Algorithms for Solving Differential Equations of Addition with Batch Queries," in Progress in Cryptology–INDOCRYPT'05, vol. 3797, Lecture Notes in Computer Science. Springer, 2005, pp. 90–103.

[7] H. Wu and B. Preneel, "Differential-linear attacks against the stream cipher Phelix," in Fast Software Encryption–FSE'07, vol. 4593, Lecture Notes in Computer Science. Springer, 2007, pp. 87–100.

[8] D. Stinson, Cryptography: Theory and Practice. CRC Press, 2006.

[9] M. Bellare and C. Namprempre, "Authenticated Encryption: Relations Among Notions and Analysis of the Generic Composition Paradigm," Journal of Cryptology, vol. 21, no. 4, pp. 469–491, 2008.

[10] J. Katz and Y. Lindell, Introduction to modern cryptography. Chapman & Hall/CRC, 2008.

[11] M. F¨urer, "Faster integer multiplication," in ACM symposium on Theory of computing–STOC'07. ACM, 2007, p. 66.

[12] C. Jutla, "Encryption modes with almost free message integrity," Journal of Cryptology, vol. 21, no. 4, pp. 547–578, 2008.

[13] P. Rogaway, M. Bellare, and J. Black, "OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption," ACM Transactions on Information and System Security, vol. 6, no. 3, pp. 365–403, 2003.

[14] A. Menezes, P. Van Oorschot, and S. Vanstone, Handbook of applied cryptography. CRC, 1997.

[15] B. Alomair and R. Poovendran, "Efficient Authentication for Mobile and Pervasive Computing," in The 12th International Conference on Information and Communications Security–ICICS'10. Springer, 2010.

[16] S. Callegari, R. Rovatti, and G. Setti, "Embeddable ADC-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos," IEEE Transactions on Signal Processing, vol. 53, no. 2 Part 2, pp. 793–805, 2005.

[17] A. Francillon, C. Castelluccia, and P. Inria, "TinyRNG: A cryptographic random number generator for wireless sensors network nodes," in Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks– WiOpt'07. Citeseer, 2007, pp. 1–7.

[18] J. Nakajima and M. Matsui, "Performance analysis and parallel implementation of dedicated hash functions," in Advances in Cryptology– EUROCRYPT 2002. Springer, 2002, pp. 165–180.

[19] B. Preneel, "Using Cryptography Well," Printed handout available at http://secappdev.org/handouts/2010/Bart%20Preneel/using crypto well. pdf, 2010.

[20] J. Großsch¨adl, R. Avanzi, E. Savas¸, and S. Tillich, "Energy-efficient software implementation of long integer modular arithmetic," in Proceedings of the 7th international conference on Cryptographic hardware and embedded systems – CHES'05, vol. 3659. Springer-Verlag, 2005, pp. 75–90.