International Journal of Research

International Journal of Research (IJR)

e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015

Available at http://internationaljournalofresearch.org

Efficient message authentication system for Mobile and Pervasive Computing

[1]Hari Kumar & [2]MrAnnapareddy V N REDDY*

[1]Svcollege of engg

[2]M.Tech, (Ph.D); KL University, SV College of Engineering

Abstract

A method and system for authenticating messages is provided. A message authentication system generates an encrypted message by encrypting with a key a combination of a message and a nonce. The message authentication system generates a message authentication code based on a combination of the message and the nonce modulo a divisor. To decrypt and authenticate the message, the message authentication system generates a decrypted message by decrypting with the key the encrypted message and extracts the message and the nonce. The message authentication system then regenerates a message authentication code based on a combination of the extracted message and the extracted nonce modulo the divisor. The message authentication system then determines whether the regenerated message authentication code matches the original message authentication code. If the codes match, then the integrity and authenticity of the message are verified.

Keywords: Authentication; unconditional security; computational security; universal hash-function families; pervasive computing

1. 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 onetime 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. The security of different MACs has been exhaustively studied. The use of one-way cryptographic hash functions for message authentication. 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 those block by block using block ciphers or cryptographic hash functions. A popular class of unconditionally secure authentication is based on universal hash-function families, pioneered by Carter and Wegman [1]–[4]. 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 (see, e.g., [5]–[11]). 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 113 [12] and the International Organization for Standardization ISO/IEC 9797-1 [13]. CMAC, a modified version of CBC-MAC, is presented in the NIST special publication 800-38B [14], which was based on the OMAC of [15]. Other block cipher based MACs include, but are not limited to, XOR-MAC [16] and PMAC [17]. The security of different MACs has been exhaustively studied (see, e.g., [18]– [20]). The use of one-way cryptographic hash functions for message authentication was introduced by Tsudik in [21]. 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 et al. in [22]. HMAC was later adopted as a standard [23]. Another cryptographic hash function based MAC is the MDx-MAC proposed by Preneel and Oorschot [24]. HMAC and two variants of MDxMAC are specified in the International Organization for Standardization ISO/IEC 9797-2 [25]. 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 [26]. The use of universal hash-function families in the CarterWegman 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 (typically a pseudorandom function1). Popular examples of computationally secure universal hashing based MACs include, but are not limited to, [27]–[33].

2. UTHENTICATING 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.

2.1 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.

2.2 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.

3 AUTHENTICATING SHORT ENCRYPTED MESSAGES

In this section, 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 and so on. 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.

3.1 The Proposed System:

We 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? 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.

Delegation methodology to produce an assignment pass code for portable station confirmation, and it can successfully protect all known assaults to portable systems including the refusal of administration assault. Additionally, the versatile station just needs to get one message and send one message to validate itself to a guest's area register; furthermore the plan just obliges solitary elliptic-curve scalar point duplication on a cell phone. In this manner, this plan appreciates both computational effectiveness and correspondence productivity as contrasted with known versatile validation plans. 3. Problem Definition Presently, many applications rely on the existence of small devices that can exchange information and form communication networks. And it is very challenging to provide security for such application. In a significant portion of such applications, the confidentiality and integrity of the communicated messages are of particular interest. Therefore we proposed an application which increases the security of the application. We proposed an algorithm which increases the security and performance of the MAC algorithm. 4. Methodology In a mobile environment, a number of users act as a network nodes and communicate with one another to acquire location based information and services. In a significant portion of such applications, the "Body Sensor Network Security: An Identity-Based Cryptography Approach," Proc. First ACM Conf. Wireless Network Security, pp. 148-153, 2008 [12]

S. Sarma, S. Weis, and D. Engels, "RFID Systems and Security and Privacy Implications," Proc. Fourth Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '02), pp. 1-19, 2003. [13]W Thamba Meshach, "Secured and Efficient Authentication Scheme for Mobile Cloud", International Journal of Innovations in Engineering and Technology (IJIET). [14]Caimu Tang, Dapeng Oliver Wu, "An Efficient Mobile Authentication Scheme for Wireless Network", Journal IEEE Transactions on wireless communication.

CONCLUSION

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, 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] 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.

Hari Kumar
Svcollege of engg

MrAnnapareddy V N REDDY M.Tech, (Ph.D); KL University, SV College of Engineering