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

A Robust Authentication Mechanism for Mobile Computing

D. Ramadevi
M.Tech (CSE)
Department of Computer Science and Engineering,
St Theressa Institute of Engineering and Technology,
Garividi, Andhra Pradesh 535101, India.

G. Ramadevi
Assistant Professor
Department of Computer Science and Engineering,
St Theressa Institute of Engineering and Technology,
Garividi, Andhra Pradesh 535101, India.

Abstract
Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link. 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.

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

I. Introduction

Mobile computing is human–computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications. 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[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

Cite this article as: D. Ramadevi & G. Ramadevi, "A Robust Authentication Mechanism for Mobile Computing", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 6 Issue 2, 2019, Page 8-13.

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

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 Standard 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 [4], 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]–[2]).

The use of one-way cryptographic hash functions for message authentication was introduced by Tsudik in [11]. 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 [2]. HMAC was later adopted as a standard [13]. Another cryptographic hash function based MAC is the MDx-MAC proposed by Preneel and Oorschot [20]. HMAC and two variants of MDx-MAC are specified in the International Organization for Standardization ISO/IEC 9797-2 [7]. 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 [16]. 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 (typically a pseudorandom function1). Popular examples of computationally secure universal hashing based MACs include, but are not limited to, [17]–[13]. 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 cryp- tographic literature are based on universal hashing [14]. 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.

II Problem Statement

Interconnected 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.

III Related Work

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

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

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. (For instance, UMAC, the fastest reported message authentication code in the cryptographic literature [14], has undergone large algorithmic changes to increase its speed on short messages [15].) 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 areof critical importance [16], [18]. 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 [19]), 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 [10]–[12]. 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 [3]–[15]. 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, e.g., [16]–[5]. Implementations of hardware efficient cryptographic hash functions have also been proposed in, e.g., [2]–[6]. 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. In this paper, we provide the first such work

CONTRIBUTIONS*:*

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. Security of the Authenticated Encryption Composition In [9], Bellare

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

and Namprempre defined two notions of integrity for authenticated encryption systems: the first is integrity of plaintext (INT-PTXT) and the second is integrity of ciphertext (INT-CTXT). Combined with encryption algorithms that provide indistinguishability 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. Figure 1 illustrates the differences between the three methods for generically composing an authenticated encryption system. It was shown in [19] that E&A compositions do not generally provide IND-CPA. This is mainly because there exist secure MAC algorithms that leak information about the authenticated message (a detailed example of such a MAC can be found in [19]).

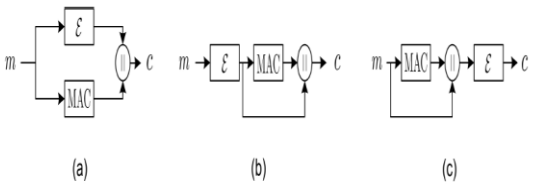

Fig. 1. A schematic of the three generic compositions; (a) Encrypt-and-Authenticate (E&A), (b) Encrypt-then-Authenticate (EtA), and (c) Authenticate-then-Encrypt (AtE).

Obviously, if such a MAC is used to compose an E&A system, then the authenticated encryption does not provide IND-CPA. By Theorem 1, however, the proposed authenticated encryption scheme is at least as private as the underlying encryption algorithm. Since the encryption algorithm is IND-CPA secure, the resulting composition provides IND-CPA. Another result of [19] is that E&A compositions do not provide INT-CTXT. However, the authors also point out that the notion of INT-PTXT is the more natural requirement, while the main purpose of introducing the stronger notion of INTCTXT is for the security relations derived in [19]. The reason why E&A compositions do not generally provide INT-CTXT is because there exist secure encryption algorithms with the property that the ciphertext can be modified without changing its decryption. Obviously, if such an encryption algorithm is combined with our MAC to compose an E&A composition, only INT-PTXT is achieved (since the tag in our scheme is a function of plaintext). A sufficient condition, however, for the proposed composition to provide INT-CTXT is to use a one-to-one encryption algorithm (most practical encryption algorithm are permutations, i.e., one-to-one [8]). To see this, observe that, by the one-to-one property, any modification of the ciphertext will correspond to changing its corresponding plaintext and, by Theorem 2, a modified plaintext will go undetected with a negligible probability.

Message Authentication

With the encryption described above, authentication becomes simpler than the ones in previous sections; the authentication tag of message m is calculated as follows:

$$\tau \equiv m + r \pmod{2^N}. \quad (16)$$

Upon receiving the ciphertext, the intended receiver decrypts it to extract r and m. Given τ, the receiver can check the validity of the message by performing the following integrity test:

$$\tau \stackrel{?}{\equiv} m + r \pmod{2^N}. \quad (17)$$

If the integrity check of equation (17) is satisfied, the message is considered authentic. Otherwise, the integrity of the message is denied.

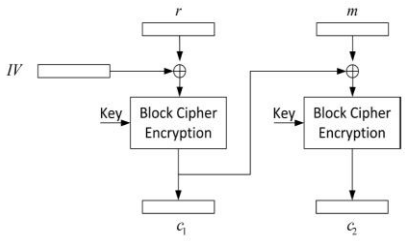

Fig. 2. The Cipher Block Chaining (CBC) mode of encryption used for message encryption. The random number, r,

Let E be the encryption algorithm of Figure 2
And let F be the block cipher used to construct E. Then given an adversary A against the privacy of E, one can construct an adversary B against the pseudorandomness of F such that Furthermore, the experiment for B takes the same time as the experiment for A and, if A makes at most q_e oracle queries, then B makes at most $2q_e$ oracle queries. Theorem 4 states that an adversary breaking the

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

privacy of the encryption algorithm of Figure 2 is also able to break the pseudorandomness of the underlying block cipher. Therefore, the adversary's advantage of breaking the privacy of the encryption algorithm is negligible, provided the use of a secure block cipher.

IV Enhancements

To provide additional security to the existing authentication system for mobile computing, we have made the following enhancements.

- Instead of showing the secret key to the user on the screen it is received by the user through mail.
- And the secret key contains 4 digits, 2 digits each from the sender and receiver from their respective secret keys.
- Further the secret key encrypted and wrapped with a number that is to be send as a One Time password (OTP) to the receiver.
- On receiving the OTP the Receiver the decrypts the secret key and downloads the file

V 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 ciphertext. This allowed the design of an authentication code those 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] 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.

[17] P. Rogaway and J. Black, "PMAC: Proposal to NIST for a parallelizable message authentication code," 2001.

[18] M. Bellare, J. Kilian, and P. Rogaway, "The Security of the Cipher Block Chaining Message Authentication Code," Journal of Computer and System Sciences, vol. 61, no. 3, pp. 362–399, 2000.

[19] B. Preneel and P. Van Oorschot, "On the security of iterated message authentication codes," IEEE Transactions on Information theory, vol. 45, no. 1, pp. 188–199, 1999.