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

Authentication for Mobile and Advanced Computing

K.Mareswara Rao
M.Tech Student,
Department of CSE,
Sree Rama institute of Technology and Science,
Kuppenakuntla, Penuballi, Khammam,TS India.

P.Karunakar Reddy
Assistant Professor,
Department of CSE,
Sree Rama institute of Technology and Science,
Kuppenakuntla, Penuballi, Khammam,TS India.

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.

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 We gman .

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 secureMACs 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 has h function family based

Existing System:

We use ZZp as the usual notation for the finite integer ring with the addition and multiplication operationsperformed modulo p. We use ZZ_p as the usual notation for the multiplicative group modulo p; i.e., ZZ_ p contains the integers that are relatively prime to p. For two strings a and b of the same length, denotes the bitwise exclusive-or (XOR) operation. For any two strings a and b denotes the concatenation operation. For a nonempty set S, the notation s S denotes the operation of selecting an element from the set S uniformly at random and assigning it to s. An important security notion for encryption algorithms that will be used in this paper is indistinguish ability under chosen plaintext attacks (IND-CPA). Let A be an adversary who is given access oracle to an encryption algorithm, E, and can ask the oracle to encrypt a polynomial number of messages to get their corresponding ciphertexts. The encryption algorithm is said to be IND-CPA secure if the adversary, after calling the encryption oracle a polynomial number of times, is given a ciphertext corresponding to one of two plaintext messages of her choice

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

cannot determine the plaintext corresponding to the given ciphertext with an advantage significantly higher than 1=2. Formally stated, let be the adversary's advantage of determining the plaintext corresponding to the given ciphertext. Then, E is said to be IND-CPA secure if

$$\mathrm{Adv}_{\mathcal{E}}^{\mathrm{ind-cpa}}(\mathcal{A}) \leq \frac{1}{2} + \mathrm{negl}(N),$$

where N is a security parameter, typically the length of the secret key

Proposed System:

Let N _ 1 be an upper bound on the length, in bits, of exchanged messages. That is, messages to be authenticated can be no longer than (N _ 1)-bit long. Choose p to be an N-bit long prime integer. (If N is too small to provide the desired security level, p can be chosen large enough tosatisfy the required security level.) Choose an integer ks uniformly at random from the multiplicative group ZZ_ p; ks is the secret key of the scheme. The prime integer, p, and the secret key, ks, are distributed to legitimate users and will be used for message authentication. Note that thevalue of p need not be secret, only ks is secret. Let E be any IND-CPA secure encryption algorithm. Let m be a short messages (N _ 1 bit or shorter) that is to be transmitted to the intended receiver in a confidential manner (by encrypting it with E). Instead of authenticating the message using a traditional MAC algorithm, consider the following procedure. On input a message m, a random nonce r 2 ZZp is chosen. (We overload m to denote both the binary string representing the message, and the integer representation of the message as an element of ZZp. The same applies to ks and r. The distinction between the two representations will be omitted when it is clear from the context.) We assume that integers representing distinct messages are also distinct, which can be achieved by appropriately encoding messages .

FROM WEAK TO STRONG UNFORGEABILITY:

As per [59], there are two notions of unforgeability in authentication codes. Namely, a MAC algorithm can be weakly unforgeable under chosen message attacks (WUFCMA), or strongly unforgeable under chosen message attacks (SUF-CMA). A MAC algorithm is said to be SUFCMA if, after launching chosen message attacks, it is infeasible to forge a message-tag pair that will be accepted as valid regardless of whether the message is "new" or not, as long as the tag has not been previously attached to the message by an authorized user. If it is only hard to forge valid tags for "new" messages, the MAC algorithm is said to be WUF-CMA.

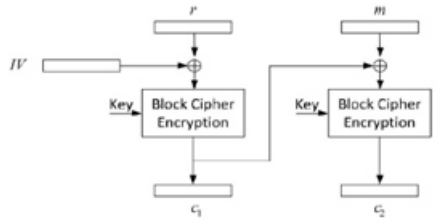

Fig. 2. The cipher block chaining mode of encryption used for message encryption. The random number, r, is treated as the first block of the plaintext.

ENCRYPTING WITH PSEUDORANDOM PERMUTATIONS (BLOCK CIPHERS):

In this section, we describe a message authentication approach that is faster than the one described in previous sections. The main idea of this approach is that the input output relation of the used encryption operation can be realized as a pseudorandom permutation. In what follows, we will show how to utilize the pseudo randomness of block ciphers in a novel way to further improve the efficiency of the authentication algorithm of Section 3.

Performance Discussion:

First, we compare the scheme of this section to the scheme of Section 3, and then compare it to single-pass schemes. Assuming devices are already equipped with a secure block cipher to encrypt messages, the authentication technique of this section requires only one modular addition. While addition is performed in OðnÞ time, the fastest integer multiplication algorithms typically require Oðn log n log log nÞ time .4 Therefore, as efficient as the scheme proposed in Section 3, the authentication technique of this section is at least Oðlog n log log nÞ faster.Complexity analysis, however, can be in accurate by absorbing large constants. This is indeed the case in comparing the basic scheme of Section 3 to the scheme of this section. For n ¼ 32, the simple addition of this scheme runs in about 0.02 cycles/byte5 as opposed to the 1.5 cycles/ byte of the previous scheme. The reason that the improvement is better than Oðlog n log log nÞ is mainly due to the modular reduction. That is, while reduction modulo a prime integer is a nontrivial operation, reduction modulo 2n can be performed by simply stopping at the nth bit.

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

Security Model:

Recall that, to model the security of a message authentication scheme in the standard setup, a probabilistic polynomial time adversary, A, is given oracle access to the signing and verifying algorithms, and challenged to generate a new massage-tag pair that will be accepted as valid, for a tag that has not been attached to the message by the signing oracle. Observe, however, that the message to be authenticated in our setup must also be encrypted. That is, what the intended user receives is a cipher rtext-tag pair, as opposed to plaintext-tag pair in the standard model. This implies that the adversary must come up with a valid cipher text-tag pair for a successful forgery. In what follows, we modify the standard model of Section 2 to address the difference between standard MACs and our MAC in which the message must be encrypted.

Security Analysis:

In this section, we prove the privacy of the system, give a formal security analysis of the proposed message authentication mechanism, and then discuss the security of the composed authenticated encryption system.

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 that benefits from the simplicity of unconditionally secure authentication without the need to manage one-timekeys. 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 secondtechnique 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.

ACKNOWLEDGMENTS:

A preliminary version of this paper appeared in the 12th International Conference on Information and Communications Security-ICICS 2010 .

REFERENCES:

[1] L. Carter and M. Wegman, “Universal Hash Functions,”J. Computer and System Sciences, vol. 18, no. 2, pp. 143-154, 1979.
[2] T. Helleseth and T. Johansson, “Universal Hash Functions fromExponential Sums over Finite Fields and Galois Rings,” Proc. 16thAnn. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO ’96),pp. 31-44, 1996.
[3] V. Shoup, “On Fast and Provably Secure Message AuthenticationBased on Universal Hashing,” Proc. 16th Ann. Int’l Cryptology Conf.Advances in Cryptology (CRYPTO ’96), pp. 313-328, 1996.
[4] B. Alomair, A. Clark, and R. Poovendran, “The Power of Primes:Security of Authentication Based on a Universal Hash-FunctionFamily,” J. Math. Cryptology, vol. 4, no. 2, 2010.
[5] B. Alomair and R. Poovendran, “E-MACs: Towards More Secureand More Efficient Constructions of Secure Channels,” IEEETrans. Computers, 2012.
[6] Federal Information Processing Standards (FIPS) Publication 113,Computer Data Authentication, FIPS, 1985.
[7] ISO/IEC 9797-1:1999 Standard, Information Technology - SecurityTechniques - Message Authentication Codes (MACs) - Part 1:Mechanisms Using a Block Cipher, ISO/IEC, 1999.
[8] M. Dworkin, “Recommendation for Block Cipher Modes ofOperation: The CMAC Mode for Authentication,” 2005.
[9] T. Iwata and K. Kurosawa, “OMAC: One-Key CBC MAC,” Proc.Int’l Conf. Fast Software Encryption (FSE ’03), pp. 129-153, 2003.
[10] M. Bellare, R. Guerin, and P. Rogaway, “XOR MACs: NewMethods for Message Authentication UsingFinite PseudorandomFunctions,” Proc. 15th Ann. Int’l Cryptology Conf. Advances inCryptology (CRYPTO ’95), pp. 15-28, 1995.
[11] P. Rogaway and J. Black, “PMAC,” Proposal to NIST for aParallelizable Message Authentication Code, 2001.
[12] M. Bellare, J. Kilian, and P. Rogaway, “The Security of the CipherBlock Chaining Message Authentication Code,” J. Computer andSystem Sciences, vol. 61, no. 3, pp. 362-399, 2000.

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

[13] B. Preneel and P. Van Oorschot, "On the Security of IteratedMessage Authentication Codes," IEEE Trans. Information Theory,vol. 45, no. 1, pp. 188-199, Jan. 1999.
[14] G. Tsudik, "Message Authentication with One-Way Hash Functions,"ACM SIGCOMM Computer Comm. Rev., vol. 22, no. 5,pp. 29-38, 1992.
[15] M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functionsfor Message Authentication," Proc. 16th Ann. Int'l Cryptology Conf.Advances in Cryptology (CRYPTO '96), pp. 1-15, 1996.
[16] Federal Information Processing Standards (FIPS) Publication 198, TheKeyed-Hash Message Authentication Code (HMAC), FIPS, 2002.
[17] B. Preneel and P.V. Oorschot, "MDx-MAC and Building FastMACs from Hash Functions," Proc. 15th Ann. Int'l Cryptology Conf.Advances in Cryptology (CRYPTO '95), vol. 963, pp. 1-14, 1995.
[18] ISO/IEC 9797-2:2002 Standard, Information Technology - SecurityTechniques - Message Authentication Codes (MACs) - Part 2:Mechanisms Using a Dedicated Hash-Function, ISO/IEC 2002.
[19] A. Bosselaers, R. Govaerts, and J. Vandewalle, "Fast Hashing onthe Pentium," Proc. 16th Ann. Int'l Cryptology Conf. Advances inCryptology (CRYPTO '96), pp. 298-312, 1996.
[20] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway,"UMAC: Fast and Secure Message Authentication," Proc. 19thAnn. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '99),pp. 216-233, 1999.
[21] D. Bernstein, "The Poly1305-AES Message-Authentication Code,"Proc. 12th Int'l Conf. Fast Software Encryption (FSE '05), pp. 32-49,
[22] S. Halevi and H. Krawczyk, "MMH: Software Message Authenticationin the Gbit/Second Rates," Proc. Int'l Conf. Fast SoftwareEncryption (FSE '97), pp. 172-189, 1997.
[23] H. van Tilborg, Encyclopedia of Cryptography and Security. Springer,2005.
[24] T. Krovetz, "UMAC: Fast and Provably Secure Message Authentication,"http://fastcrypto.org/umac, 2006.
[25] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,"Wireless Sensor Networks: A Survey," Computer Networks,vol. 38, no. 4, pp. 393-422, 2002.
[26] A. Perrig, J. Stankovic, and D. Wagner, "Security in WirelessSensor Networks," Comm. ACM, vol. 47, no. 6, pp. 53-57, 2004.
[27] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Toward aStatistical Framework for Source Anonymityin Sensor Networks,"IEEE Trans. Mobile Computing, vol. 12, no. 2, pp. 248-260,doi:10.1109/TMC.2011.267, Feb. 2013.
[28] Class-1 Generation-2 UHF Radio Frequency Identification ProtocolStandard Version 1.2.0, EPCglobal, Inc., 2008.
[29] S. Sarma, S. Weis, and D. Engels, "RFID Systems and Securityand Privacy Implications," Proc. Fourth Int'l Workshop CryptographicHardware and Embedded Systems (CHES '02), pp. 1-19,2003.
[30] A. Juels, "RFID Security and Privacy: A Research Survey," IEEE J.Selected Areas in Comm., vol. 24, no. 2, pp. 381-394, Feb. 2006.

Author's:

K.Mareswara Rao M.Tech Student,Department of CSE,Sree Rama institute of Technology and Science, Kuppenakuntla, Penuballi, Khammam,TS India.

P. Karunakar Reddy is an efficient teacher, received M.Tech from JNTU Kakinada is working as an Assistant Professor in Department of C.S.E, Sree Rama Institute of Technology & Science, Kuppenakuntla, Penuballi, Khammam, TS,India. He has published many papers in both National & International Journals. His area of Interest includes Data Communications & Networks, Information Security, Database Management Systems, Computer Organization, C Programming and other advances in Computer Applications