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

Authentication for Mobile and Permeative Computing Efectively

Bathula Kotiratnam
PG Scholar,
Department of CSE,
EVM College of Engineering & Technology,
Narasaraopet, AP, India.

Bhavanam Bhujanga Reddy
Assistant Professor,
Department of CSE,
EVM College of Engineering & Technology,
Narasaraopet, AP, 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.

1 INTRODUCTION AND RELATED WORK:

PRESERVING the integrity of messages exchanged overpublic channels is one of the classic goals in cryptographyand the literature is rich with message authentication code (MAC) algorithms that are designed for the sole purpose ofpreserving message integrity. Based on their security, MACscan be either unconditionally or computationally secure.Unconditionally secure MACs provide message integrityagainst forgers with unlimited computational power.Ontheother hand, computationally secure MACs are only securewhen forgers have limited computational power.A popular class of unconditionally secure authenticationis based on universal hash-function families, pioneered byCarter and Wegman [1]. Since then, the study of unconditionallysecure message authentication based on universalhash functions has been attracting research attention, both from the design and analysis standpoints (see, e.g., [2], [3],[4], [5]).

The basic concept allowing for unconditionalsecurity is that the authentication key can only be used toauthenticate 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-lifeapplications. In computationally secure MACs, keys can beused to authenticate an arbitrary number of messages. Thatis, after agreeing on a key, legitimate users can exchange anarbitrary number of authenticated messages with the samekey.Depending on the main building block used toconstruct them, computationally secure MACs can be classified into three main categories: block cipher based,cryptographic hash function based, or universal hashfunctionfamilybased.CBC-MAC is one of the most known block cipher-basedMACs, specified in the Federal Information ProcessingStandards publication 113 [6] and the International Organizationfor Standardization ISO/IEC 9797-1 [7]. CMAC, amodified version of CBC-MAC, is presented in the NISTspecial publication 800-38B [8], which was based on theOMAC of [9]. Other block cipher-based MACs include, butare not limited to, XOR-MAC [10] and PMAC [11]. Thesecurity of different MACs has been exhaustively studied(see, e.g., [12], [13]).The use of one-way cryptographic hash functions formessage authentication was introduced by Tsudik [14].Apopular example of the use of iterated cryptographic hashfunctions in the design of message authentication codes isHMAC, which was proposed by Bellare et al. [15]. HMACwas later adopted as a standard [16]. Another cryptographichash function-based MAC is the MDx-MAC proposed byPreneel and Van Oorschot [17]. HMAC and two variants ofMDx-MAC are specified in the International Organizationfor Standardization ISO/IEC 9797-2 [18]. Bosselaers et al.[19] described how cryptographic hash functions can becarefully coded to take advantage of the structure of thePentium processor to speed up the authentication process. One of the key component towards the successful roll-out of mobile or location based applications is toprovide security and privacy guarantees.

Without proper security and privacy guarantees, the rich functionalityand services provided by mobile ad-hoc networks can be abused, jeopardizing the safety of users, aswell as the performance of the entire network. For example, a malicious user can claim a fake traffic jam togain the right of the road and cause other vehicles to make an unnecessary detour. The user can also send unfounded negative comments regarding a local business to other users within the same mobile network.As a result, users should be authenticated before they are allowed to access services offered through thesedynamically formed mobile networks.Since a user's location can reveal the actual identity of the user, it is in the best interest of the usernot to be tracked by service providers or peer users. In many non critical scenarios, a service provider mayonly need to know whether the user is authenticated or not, but does not need to know the user's actualidentity. Thus, users' privacy should be preserved during authentication in that their identities should bekept private in order to avoid unlawful tracing and user profiling.

More specifically, these parties may causeprivacy concerns: (i) the authentication server or service provider; (ii) peer users. The server may obtain thebehavior pattern or track the user locations according to the record of the users requesting for authentication.Similarly, other peer users may also be able to track one another through the authentication records. Werefer to the privacy concern caused by the server as the server-wise privacy and the privacy concern causedby peer users as the peer-wise privacy. Ideally, we should preserve both server-wise and peer-wise privacy foreach mobile user. On the other hand, we should also ensure traceability whereby law enforcement authoritiescan reveal a user's real identity required when disputes occur.an anonymous credential system that use zero-knowledge proof was proposed to achieve anonymousauthentication. Being the best among the exiting work, this scheme achieves several of our proposedgoals under privacy-preserving user authentication, but comparing to the proposed solution, the scheme isnot very efficient and it is only statistically secure. We will adopt this scheme as a baseline to demonstratethe advantages of our proposed protocol.

1.1Contributions:

To overcome the shortcomings in existing work, we propose a novel randomized / privacy-preserving authenticationprotocol (namely RAU) that truly preserves users' privacy while still ensure traceability.

Theproposed protocol is designed based on Homomorphic encryption [25] and it allows each user to self generateany number of authenticated identities to prove his or her legal status when communicating with peerusers, service providers, or other infrastructure (like road-side units in VANET). In fact, users will be ableto easily use a new identity for each newly established communication. These randomized identities canbe verified through the collaboration of a pair of authentication servers while each authentication serverwould not know the real identity of the authentication requester. In this way, we achieve both peer-wiseand server-wise privacy preservation. For traceability, the pair of authentication servers need to execute acollaborative protocol so that the real identity of the malicious user can be identified. We summarize theadvantages of our proposed authentication protocol as follows.

- Under our authentication protocol, users' real identities are hidden from each individual party includingauthentication servers, peer users, service providers, and other infrastructure.
- Our protocol achieves a set of desired security and privacy properties such as unforgeability, unlink ability and traceability. It is robust against various types of attacks (as discussed later in Section5).
- Our approach no longer has the key revocation problem neither the costly group management. Specifically,users using the proposed protocol no longer need to preload a huge number of keys (i.e.,pseudonyms) or rely on others (i.e., peers or infrastructure) to generate the pseudonyms. Our experimentalstudy demonstrates the proposed protocol is very efficiency.
- Our protocol does not require users to be equipped with high performance computing equipment sincealmost all computations are outsourced to the servers and the users only need to generate severalencryptions and random numbers.
- User authentication is very efficient in our protocol well under the 100ms requirement [20]. Sinceanonymity revocation needs not to be done as a real-time application (due to court orders), ourprotocol provides reasonable computation time (as presented in Section 6).

The rest of the paper is organized as follows. Section 2 reviews related works. Section 3 introducessome preliminary notions of encryption adopted in this work. Section 4 presents the proposed randomizedauthentication protocol. Section 5 discusses the possible attacks and the security and privacy properties ofthe protocol.

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

Then, Section 6 reports the experimental results. Finally, Section 7 concludes the paper andoutlines future research directions.

1.2 Organization:

The remainder of the paper is organized as follows: In-Section 2, we list our notations and discuss some preliminaries.In Section 3, we describe the first authentication technique assuming messages do not exceed a maximum-length, discuss its performance advantages over existing Techniques, and prove its security. In Section 4, we proposea modification to the scheme of Section 3 that provides astronger notion of integrity. In Section 5, we describe thesecond technique assuming the encryption is block cipherbased, discuss its performance, and prove its security. InSection 6, we conclude the paper.

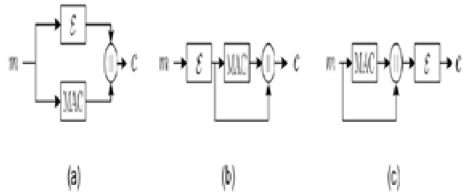
2 AUTHENTICATING SHORT ENCRYPTED MESSAGES:

In this section, we describe our first authentication schemethat can be used with any IND-CPA secure encryptionalgorithm. An important assumption we make is thatALOMAIR AND POOVENDRAN: EFFICIENT AUTHENTICATION FOR MOBILE AND PERVASIVE COMPUTING 471messages to be authenticated are no longer than apredefined length. This includes applications in whichmessages are of fixed length that is known a priori, such asRFID systems in which tags need to authenticate theiridentifiers, sensor nodes reporting events that belong tocertain domain or measurements within a certain range andso on. The novelty of the proposed scheme is to utilize theencryption algorithm to deliver a random string and use it toreach the simplicity and efficiency of one-time pad authenticationwithout the need to manage impractically long keys.

2.1 The Proposed System:

Let N _ 1 be an upper bound on the length, in bits, ofexchanged messages. That is, messages to be authenticatedcan be no longer than (N _ 1)-bit long. Choose p to be anN-bit long prime integer. (If N is too small to provide thedesired security level, p can be chosen large enough to satisfy the required security level.) Choose an integer ksuniformly at random from the multiplicative group ZZ_p; ksis the secret key of the scheme.

The prime integer, p, andthe secret key, ks, are distributed to legitimate users andwill be used for message authentication. Note that thevalue of p need not be secret, only ks is secret.



Note, however, that the authentication tag is a functionof the confidential message. Therefore, the authenticationtag must not reveal information about the plaintext since,otherwise, the confidentiality of the encryption algorithm iscompromised. Before we give formal security analysis ofthe proposed technique, we first discuss its performancecompared to existing techniques.

2.2 Data Privacy:

We show in this section that the privacy of the proposedcompositions is provably secure assuming the underlyingencryption algorithm provides indistinguishability underchosen plaintext attacks (IND-CPA). Consider an adversary,B, who is given oracle access to the encryption algorithm, E.The adversary calls the encryption oracle on a polynomialnumber of messages of her choice and records thecorresponding ciphertexts. The adversary then choosestwo equal-length messages, m0 and m1, and gives them tothe encryption oracle. The oracle draws a bit b 2 f0; 1guniformly at random, encrypts mb, and gives the adversarythe resulting ciphertext. The adversary is allowed toperform additional call to the encryption oracle andeventually outputs a bit, b0. We define the adversary'sadvantage of breaking the IND-CPA security of theencryption algorithm, E, as her probability of successfullyguessing the correct bit (equivalently knowing to whichplaintext the ciphertext corresponds) As stated in (1), E provides IND-CPA if the adversary has anegligible advantage of guessing the right bit over anadversary choosing a bit uniformly at random.Now, let _ denote the proposed authenticated encryptioncomposition described in Section 3.1. Let A be anadversary against the privacy of _ and let Advpriv_ ðAÞ denoteadversary's A advantage in breaking the privacy of thesystem, where the privacy of the system is modeled as itsindistinguishability under chosen plaintext attacks. Onegets the following theorem. Theorem 1.

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

Let _ be the authenticated encryption compositiondescribed in Section 3.1 using E as the underlying encryptionalgorithm. Then given an adversary, A, against the privacy of_, one can construct an adversary, B, against E Theorem 1 states that an adversary breaking the privacyof the proposed system will also be able to break the IN-DCPAof the underlying encryption algorithm. Therefore, if Eprovides IND-CPA, the adversary's advantage of exposingprivate information about the system is negligible. Note thatprivate information here refers not only to the encryptedmessages, but also the secret key, ks, as well as the secretkey of the encryption algorithm.

3.CONCLUSION:

In this work, a new technique for authenticating shortencrypted messages is proposed. The fact that the messageto be authenticated must also be encrypted is used todeliver a random nonce to the intended receiver via theciphertext. This allowed the design of an authenticationcode that benefits from the simplicity of unconditionallysecure authentication without the need to manage one-timekeys. In particular, it has been demonstrated in this paperthat authentication tags can be computed with one additionand a one modular multiplication. Given that messages arerelatively short, addition and modular multiplication canbe performed faster than existing computationally secureMACs in the literature of cryptography. When devices areequipped with block ciphers to encrypt messages, a secondtechnique that utilizes the fact that block ciphers can bemodeled as strong pseudorandom permutations is proposedto authenticate messages using a single modularaddition. The proposed schemes are shown to be orders ofmagnitude faster, and consume orders of magnitude lessenergy than traditional MAC algorithms. Therefore, theyare more suitable to be used in computationally constrainedmobile and pervasive devices.

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.ALOMAIR AND POOVENDRAN: EFFICIENT AUTHENTICATION FOR MOBILE AND PERVASIVE COMPUTING 479.

[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.