ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
DIIF 0.876

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 9, SEPTEMBER 2015, PP 617-621

Efficient Authentication Using Fine-grained Approach over Mobile and Pervasive Computing

[1] **Vemula Rohini, [2]Dr S.Prem Kumar**
[1](M.Tech), CSE,
[2]Professor & HOD, Department of computer science and engineering,
G.Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India.

Abstract:- Now a days in technology, many applications fall back on the existence of small devices that can swap information and form communication networks. In important portion of such applications, the confidentiality and integrity of the communicated messages are of fastidious attention. 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: Mobile computing, Pervasive Computing, message authentication code (MAC) algorithm.

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. 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 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

II. RELATED WORK

In 2013, Xu, Gaochao et al [1] presented A load balancing model based on cloud partitioning for the public cloud. The load balancing model is aimed at the public cloud which has numerous nodes with distributed computing resources in many different geographic locations. Thus, this model divides the public cloud into several cloud partitions. When the environment is very large and complex, these divisions simplify the load balancing.

There are many straightforward load balance algorithm methods such as the Weight Round Robin, the Random algorithm, and the Dynamic Round Robin [7]. When the cloud partition is normal, jobs are arriving much faster than in the idle state and the situation is far more complex, so a different strategy is used for the load balancing. Each user wants his jobs completed in the shortest time, so the public cloud needs a method that can complete the jobs of all users with reasonable response time [1]. Shivaratri et al [3] focuses on the problem of judiciously and transparently redistributing the load of the system among its nodes so that overall performance is maximized. They also discussed several key issues in load distributing for general-purpose systems, including the motivations and design trade-offs for loaddistributing algorithms. They also presented loaddistributing policies used in existing systems and draw conclusions about which algorithm might help in realizing the most benefits of load distributing. They compare various load distribution algorithms with their benefits and losses.

The ability of load distributing to improve performance is intuitively obvious when work arrives at some nodes at a greater rate than at others, or when some nodes have faster processors than others. Performance advantages are not so obvious when all nodes are equally powerful and have equal workloads over the long term [3]. Zhu, Yan et al [4] suggested "Efficient provable data possession for hybrid clouds. They focused on the construction of PDP scheme for hybrid clouds, supporting privacy protection and dynamic scalability. They first provide an effective construction of Cooperative Provable Data Possession (CPDP) using Homomorphic Verifiable Responses (HVR) and Hash Index Hierarchy (HIH). This construction uses homomorphic property, such that the responses of the client's challenge computed from multiple CSPs can be combined into a single response as the final result of hybrid clouds. By using this mechanism, the clients can be convinced of data possession without knowing what machines or in which geographical locations their files reside. More importantly, a new hash index hierarchy is proposed for the clients to seamlessly store and manage the resources in hybrid clouds. Their experimental results also validate the effectiveness of our construction [6]. Lori MacVitte presented a Cloud Balancing: The Evolution of Global Server Load Balancing. Cloud balancing is still new, but the technology to add value is available today.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 and the International Organization for Standardization . CMAC, a modified version of CBC-MAC, is presented in the NIST special publication, which was based on the OMAC of. Other block cipher based MACs include, but are not limited to, XOR-MAC and PMAC. The security of different MACs has been exhaustively studied.

III.LITERATURE SURVEY

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 under-lying 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 inefficientwhen the messages to be authenticated are short. (For instance, UMAC, the fastest reported message authentication code in the Cryptographic literature, has undergone large algorithmic changes to increase its speed on short messages)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 are 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. 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 Simplys 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.

IV.SYSTEM STUDEY

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

confidentiality and integrity of the communicated messages are of particular interest. 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. Following Figure 1 shows generalize system.

There will be five modules.

Here we use two new techniques for authenticating short encrypted messages that are more efficient than existing approaches.

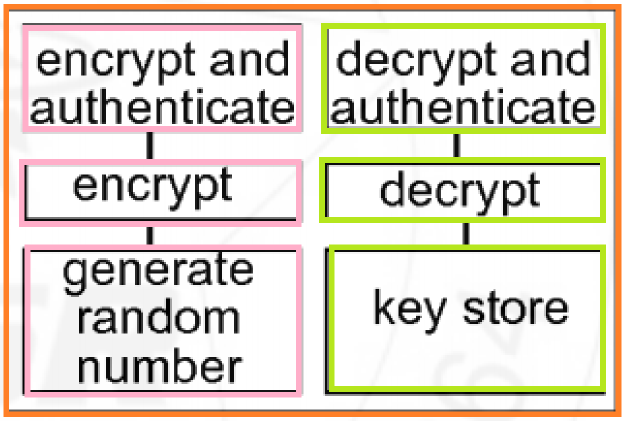
1.a) Authenticate short messages and encrypt those messages: In this module, first validation plot that might be utilized with any IND-CPA secure encryption calculation. A critical presumption is that messages to be verified are no more than a predefined length. This incorporates applications in which messages are of settled length that is known from the earlier, for example, RFID frameworks in which labels need to validate their identifiers, sensor hubs reporting occasions that have a place with certain area or estimations inside a certain extent.

In this first technique, we utilize the fact that the message to be authenticated is also encrypted, with any secure encryption algorithm, to append 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.

1.B) Encrypting With Pseudorandom Permutations (Block Ciphers): In this 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. More efficient than existing approaches. 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. The most efficient solution and can lead to waste of resources already available, namely, the security that is provided by the encryption algorithm. **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 (l) and N describing the length of the shared key and the resulting authentication tags.

3) Security of the Authenticated Encryption Composition: The first is integrity of plaintext (INT-PTXT) and 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 will be analyze.

4) Data Privacy and authenticity: - In this section, a message authentication approach that is faster than the existing. The main idea of this approach is that the input output relation of the used encryption operation can be realized as a pseudo random permutation. In what follows, will show how to utilize the pseudo randomness of block ciphers in a novel way to further improve the efficiency of an existing authentication algorithm. In today's reality, numerous applications depend on the presence of little gadgets that can trade data and structure correspondence systems. In a critical segment of such applications, the privacy and respectability of the imparted messages are specifically compelling. To maintain the security and integrity of the communication within the system required following methods. 1. Encryption methods. 2. Authentication methods. 3. Data and security analysis.



Finegrained based secure message authentication

While sharing message from sender to reciver via any mobile devices , inorder to providing message authentication sender need to add some attributes with that message , if reciver attributes matches with the sender attributes , them that message will be authenticated

VI. RESULTS

In existing system 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. Use of encryption algorithm is block cipher based to further improve the computational efficiency of the technique. The driving motive behind 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. In the proposed system have to deliberate the subsequent cryptographic methods that will be realistic in the input that input should be the short message that was called as the Multi-Security technique. Those encryption methods are the data encryption standard and the advanced encryption standard. Then it delivers the password based authentication method in the double encryption technique's cipher text. For significant the order of the operation they have to apply the avalanche effect but to make the method to secure the keys will be transmitted to the user through the mail of the personal contact of the user. In proposed system we have less time complexity, less computational cost, effective integrity, more secure while the transmission, more confidential

VII.CONCLUSION AND FUTURE WORK

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 onetime 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, And 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] 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 from Exponential Sums over Finite Fields and Galois Rings," Proc. 16th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '96), pp. 31-44, 1996.

[3] V. Shoup, "On Fast and Provably Secure Message Authentication Based 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-Function Family," J. Math. Cryptology, vol. 4, No. 2, 2010.

[5] B. Alomair and R. Poovendran, "E-MACs: Towards More Secure and More Efficient Constructions of Secure Channels," IEEE Trans. Computers, 2012.

[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 crypto-

graphic 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.