International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.2, 2015

REVIEW ARTICLE

ISSN: 2321-7758

AUTHENTICATION FOR MOBILE AND SELF EVIDENT COMPUTING

SIDHARTH ACHARYA[1], K.RAJAKUMARI[2*]

[1]B.Tech Final Year, Department of Computer science Engineering, Bharath University, Chennai

[2]Assistant Professor, Department of Computer science Engineering, Bharath University, Chennai

Article Received: 31/03/2015 | Article Revised on:09/04/2015 | Article Accepted on:13/04/2015

SIDHARTH ACHARYA

ABSTRACT

As in the upcoming technologies now many applications have come under existence which can be developed by the help of small devices with this our aim is to deliver short encrypted messages and that must be safe the ideology behind this technology is to exhibit and perform short messages in an efficient way so that the user which has sent the message can get information about the message sent so for that there is a security code generated and then this security key plays an vital role in order to get an encrypted message hence our aim is to deliver the topmost security which emphasizes upon the detailed description of the data or the messages which has to be encrypted and then by a security code it is to be decrypted to see the message this meet the requirements of the users and sender and as well as the receiver through a security code and then initialize by the code given to encrypt the message thus this code is being optimized to obtain the messages .Now by this security key generation we can encrypt and decrypt the messages sent. The messages received by the receiver determines that what message the sender has send and through the security code which is given it then encrypts the messages in the readable format hence the messages sent is successfully sent and the code is also generated in an effective manner.

Keywords – encryption, authentication, MAC keys, hash functions

I.INTRODUCTION

The emerging technology and the competition between the new devices yield the most significant role and hence the messages which are sent and received are here described in such efficient way that the user send the message to receiver and the receiver receives and then for the authentication of code a security key is being given these key are generated through a process of MAC algorithms (message algorithm code) this is introduced to the messages and in upcoming era their sole purpose is to deliver message security and message integrity .Now the security of the messages against the forgers is the most vital and important so as the data or the messages is kept to be in safe .One big advantages is that MACs provide unlimited

computational power whereas the MACs are secure when the forgers have limited computational power. These exchange of messages is based on secured authentication suppose if we send the messages and it confirms his messages through a security code the key has been generated for a secure and efficient authentication as now MACs have been applicable for real time applications and hence through this message is being encrypted and decrypted so then the secure key is generated hence the key is very highly secure and hence authenticated since the management of one time keys is not considered in a practical way so the MACs have become the choice .In computationally secure MACs keys can be used to generate key and authenticate an arbitrary no of messages. This is done only after agreeing on a key. Now as the MACs are specified in the ISO international organization for standardization ISO/IEC 9797-2[25] It was described by bosselaers et al that how the cryptographic hash functions can be carefully coded to take advantage of the structure of the older processor and speed up the authentication process .Now for the universal hash function families is not restricted to the design of the unconditional and secure authentication of computational resources which secure the MACs as they are based upon universal hash functions then the compressed image is efficiently processed with a cryptographic function .The universal hashing based on the MACs include give better performance when its compared to block cipher or the cryptographic hashing based MACs .As the MACs are independent and indifferent as they are the mobile authentication code and which are used for the encryption and the security of the messages hence these messages are the highly and solely dependable in accordance to the effort of the messages and hence which are used and send and the they are received and for the safe authentication the security key is also generated and the then it is efficient key authenticated .the optimum and significant effort has been put to implement the needs of the hardware efficient implementations that will suite all the smaller devices .In this project work we will come to see the application in which the messages are authenticated efficiently where there is no question of failure of the send messages now for optimization of the messages the security key given after the message is encrypted and before the message is securely sent when the option is being used for encrypt message then there is a code then the code is generated and the sender sends the message by applying his/her password now .This is the process of the secure authentication and which denotes the possible outcomes of the messages text and the confirmation of the messages which is sent and received . now there are very vital observations about the existing algorithms MACs algorithms so they are implemented and designed independently of any other operations which are required to be performed as the message which is to be authenticated for the short messages the UMAC the fastest reported message authentication code in the cryptographic literature it has undergone a large and efficient algorithms changes to increase its speed on short messages .As now there is deployment of the network in collection to the smaller devices .In the practical field of application the main purpose of the small devices is to communicate short messages. Now as in the application and developing technologies is the deployment of the body sensor networks it is used in the medical application as a body sensor network. In such application the sensors can be embedded in patient's body to report the vital signs. It is developed and designed of the hardware efficient implementation .The main motive behind our investigation is that to used a general purpose MAC algorithms so in the exchanged messages can be authenticated efficiently In other application considering the deployment of the radio frequency identification RIFD systems which are certain tags which are called RIFD tags they have to introduce and address themselves to authorized RIFD systems in such a efficient way so the their privacy is preserved thus for the short encrypted messages the MAC algorithms are independently and efficient produce error free results for exchange of the messages .the optimum security is the first most process for the message exchanges which yield to produce optimized and security generated code which is the efficient way to deliver the messages which are short and can send in high speed and error free .The optimization of the code is highly secured and then it is enhanced for designing the message authentication code the lifeline of the messages which are exchanged and are used for the

generated code which in turn shows the output by the help of the generated security key . Now in this era of the new technology the high demand of the usage of the small devices and where the short and efficient secure messages are send and then received by a security code or we can address it as a secure key generation for the safety and proper authentication of the exchange of messages and which satisfies the clients and they have to receive and send messages depending upon the main building block used to construct the code and also to generate the code CBC-MAC is one of the most efficient block cipher which is based on cryptographic hash function. Other block cipher based MACs ,include but are not limited to XOR-MAC and PMAC. The use of iterated hash functions so as to implement the message authentication codes is HMAC ,which was later adopted as a standard message authentication code . UMAC The fastest reported message authentication code in the cryptographic literature and which is based on universal hashing .The main reason behind the performance and the advantage of universal hashing based MACs is that it processes the messages block by block using the universal hash functions.

II.RELATED WORKS

In this paper describes the concept of sensor networks which has been made viable by the convergence of micro electro-mechanical systems technology, wireless communications and digital electronics. First, the sensing tasks and the potential sensor networks applications are explored, and a review of factors influencing the design of sensor networks is provided. Then, the communication architecture for sensor networks is outlined, and the algorithms and protocols developed for each layer in the literature are explored .Constraints are highly stringent and specific for sensor networks new wireless ad hoc networking techniques are used [1]. In this paper, we addressed the problem of individual tag identification in large-scale RFID systems. We proposed a protocol that enables the private identification of tags in the system with constant-time consume .By utilizing the existence of a large storage device in the system, the constant-time identification is achieved by performing the necessary time consuming computations (independent of the reader-tag interactions). As opposed to tree-based protocols, the proposed protocol does not further complicate the already challenging problems in RFID systems, namely, collision avoidance and medium access control. Further, tag compromise threats can be mitigated by periodically updating the database which, due to independence of secret parameters amongst tags, can be performed independent of any tag-reader interaction [2]. The use of cryptographic hash functions like MD5 or SHA for message authentication has become a standard approach in many Internet applications and protocols. Though very easy to implement, these mechanisms are usually based on ad hoc techniques that lack a sound security analysis [3].We present new constructions of message authentication schemes based on a cryptographic hash function. Our schemes, NMAC and HMAC, are proven to be secure as long as the underlying hash function has some reasonable cryptographic strengths. Moreover we show, in a quantitative way, that the schemes retain almost all the security of the underlying hash function. In addition our schemes are efficient and practical. Their performance is essentially that of the underlying hash function. Moreover they use the hash function (or its compression function) as a black box, so that widely available library code or hardware can be used to implement them in a simple way, and replace ability of the underlying hash function is easily supported [4].More precisely, since the message to be authenticated is encrypted, universal hash functions based E-MACs can designed without the need to apply cryptographic operations on the compressed image, In this paper secure channels enable the confidential and authenticated message exchange between authorized users. A generic approach of constructing such channels is by combining an encryption primitive with an authentication primitive (MAC).In this work, we studied the generic composition of authenticated encryption systems. We introduced E-MACs, a new symmetric-key cryptographic primitive that can be used in the construction of E&A and AtE compositions. By taking advantage of the E&A and AtE structures, the use of E-MACs is shown to improve the efficiency and security of the authentication operation. since this can be replaced by operations performed by the encryption algorithm, further ,by appending a random string at the end plaintext message, E-MAC can be secured

against key-recovery attacks [4].The emphasis upon the entries of the hash efficiency message authentication code and hence this delivers the optimal usage of the denoted area of the technique and how the message is sent and then received thus the hash functions are used for the denoting the area which in accordance to the message sent and then it is then given code and by the security key it has to be generated. This paper gives an input independent average linear time algorithm for storage and retrieval on keys. The algorithm makes a random choice of hash function from a suitable class of hash functions. Given any sequence of inputs the expected time (averaging over all functions in the class) to store and retrieve elements is linear in the length of the sequence. The number of references to the data base required by the algorithm for any input is extremely close to the theoretical minimum for any possible hash function with randomly distributed inputs.Three suitable classes of hash functions which also can be evaluated rapidly. The ability to analyze the cost of storage and retrieval without worrying about the distribution of the input allows as corollaries improvements on the bounds of several algorithms [5]. In this project we describe a new application of algebraic coding theory to universal hashing and authentication without secrecy. This permits to make use of the hitherto sharpest weapon of coding theory, the construction of codes from algebraic curves. This show in particular how codes derived from Artin-Schreier curves, Hermitian curves and Suzuki curves yield classes of universal hash functions which are substantially better than those know before. Most importantly we sawthat Deligne-Lusztig curves and certain Artin-Schreier curves allow the construction of ASU2− classes of hash functions which use much less key space than the methods which had been used [6].

III. PRELIMINARIES

In this work we see that if there is an application in which the messages that need to be exchanged and shortened and their privacy is also preserved. New techniques for authenticating short encrypting messages that are highly efficient than the existing approach .One can run one time keys to allow for secure authentication and for allow faster sending messages The main motive of the authentication of the faster secured encrypted messages are widely used in the small devices so that secret key generated for the message authentication is associated as for the need for the sender who is sending the message and the encrypting message is to be sent in an efficient and secured way so the data or the messages are safely enhanced

A. Organization

In this paper we will describe the first authentication technique assuming that the messages should not exceed more than required length we discuss how to data can be preserved and the security of the messages encrypted and efficiency about the short messages sent and received through the security key and how the privacy is preserved. The most effective way to enhance the security of the messages is the performance discussion and security model and the security analysis.

B. Authenticating Short Encrypted Messages

The messages which are to be authenticated should be no longer than the predefined length this includes application which are of the fixed length. It is to reach the simplicity and efficiency of one time pad authentication without the need of the long keys such as in the RIFD systems in which the tags are used to authenticate their identifiers they denote the sensor node reporting that belong to the domain name such as Java within a certain range

C. Problem Identification

The main objective in this is the problem identification computationally has a major revolutionary step in the line of research dating back to mid 1970 s. This figure represents new problems which are encountered as one move from left to right. In addition the solution of many previous encountered problems become more complex as the modulation symbol suggests this increase in complexity is multiplicative rather than additive. There are four key issues which pervasive computing shares many research themes in common with mobile computing they are as follows:-

1) Smart services: Embedding computational infrastructure in building infrastructure brings together two worlds that has been disjoin till now the fusion of these words enables mutual sensing and control of these words

2) Invisibility: the ideal expressed by Weiser is complete disappearance of pervasive computing technology from a user's consciousness. In practice,

a reasonable approximation to this ideal is minimal user distraction. If a pervasive computing environment continuously meets user expectations and rarely presents him with surprises, it allows him to interact almost at a sub conscious level.

3) Localized Scalability: as smart spaces grow in sophistication, the intensity of interactions between a user's personal computing space and its surroundings increases. This has severe bandwidth, energy and distraction implications for a wireless mobile user. Scalability, in the broadest sense, is thus a critical problem in pervasive computing. Like the inverse square laws of nature, good system design has to achieve scalability by severely reducing interactions between distant entities. This directly contradicts the current ethos of the Internet, which many believe heralds the "death of distance.

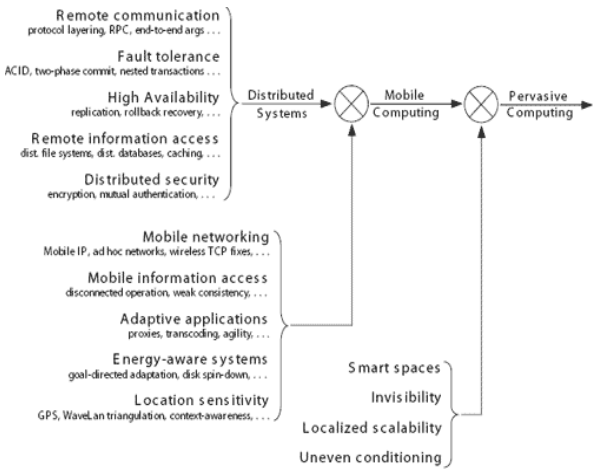

Figure. 1 Problem Identification Mechanism

D. Masking Uneven Conditioning

Uniform penetration of small devices computing technology into the infrastructure is many decades away. In the interim, there will persist huge differences in the "smartness" of different environments. This large dynamic range of "smartness" can be jarring to a user, detracting from the goal of making pervasive computing technology invisible. One way to reduce the amount of variation seen by a user is to have his personal computing space compensate for "dumb" environments. As a trivial example, a system that is capable of disconnected operation is able to mask the absence of wireless coverage in its environment

IV.SYSTEM DESIGN

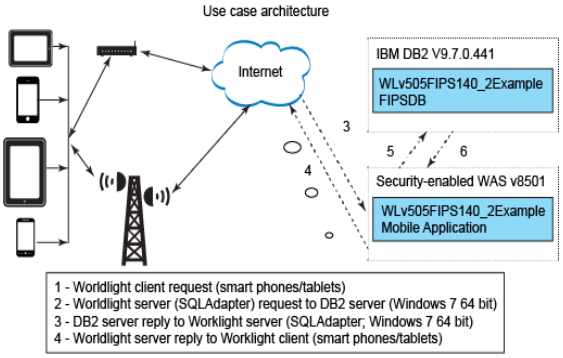

Figure. 2 Design of Message Transfer

In this paper we propose the authentication of the messages and signing algorithms where it is the verifying algorithm

1) A random string of the length is selected as l as the shared secret
2) If the A makes a signing query on message m then the oracles then computes and authentication tags
3) If A makes a verified query (m) the oracle then will compute the decision and it returns to A

   Hence this then continues as the security key is being generated for every messages the sent there is an authentication of the security key the key is generated and then the message is verified and the data is preserved in the secured way

A. Performance Discussion

Here in this section of performance discussion we introduce the classes of the message authentication codes that can be used for preserving the data and message integrity .when the message which are to be authenticated they are to be short and precise way and it is not time consuming .The significant advantages of this method is specially for low-powered devices and gadgets in such devices the hardware frequency is the foremost important aspect .The hardware which is required to perform the modular activity which is the modular multiplication is more time less than that of performing the sophisticated crypto operations The system has following modules :

B. Authenticating Short Encrypted Messages

In this section 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 application in which messages are of fixed length that is known a priori, such a RIFD systems in which tags need to authenticate their identifier, sensor nodes reporting events that to certain domain or measurements within a certain range etc . The novelty of the proposed scheme is to utilize the encryption algorithm algorithm to deliver a random string and use it to reach the simplify and efficiency of one-time pad authentication without the manage impractically long keys

C. SECURITY LEVEL

A message authentication scheme consist of 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 tag respectively Module Learning Outcomes:

1) Analyse and solve engineering problems and communicate the outcome effectively.
2) Synthesis information in a manner that may be innovative, utilising knowledge or processes from the forefront of the pervasive and mobile communication networks
3) Critically evaluate research and methodologies and argue alternative approaches for pervasive and mobile communication networks.
4) Solve problems with self-direction and originality and act autonomously in planning and implementing tasks for pervasive and mobile communication networks at a professional or equivalent level

V. CONCLUSION

Mobile computing and pervasive computing represent major evolutionary steps in a line of research dating back to the mid-1970s. New problems are encountered as one moves from left to right in this figure. In addition, the solutions of many previously-encountered problems become more complex — as the modulation symbols suggest, this increase in complexity is multiplicative rather than additive. It is much more difficult to design and implement a mobile computing system than a distributed system of comparable robustness and maturity; a pervasive computing system is even more challenging. As indicates, the conceptual framework and algorithmic base of distributed systems provides a solid At their core, all models of ubiquitous computing share a vision of small, inexpensive, robust networked processing devices, distributed at all scales throughout everyday life and generally turned to distinctly common-place ends. For example, a domestic ubiquitous computing environment might interconnect lighting and environmental controls with personal biometric monitors woven into clothing so that illumination and heating conditions in a room might be modulated, continuously and imperceptibly. Another common scenario posits refrigerators "aware" of their suitably tagged contents, able to both plan a variety of menus from the food actually on hand, and warn users of stale or spoiled food. Ubiquitous computing presents challenges across computer science: in systems design and engineering, in systems modeling, and in user interface design. Contemporary human-computer interaction models, whether command-line menu-driven, or GUI based, are inappropriate and inadequate to the ubiquitous case.

REFERENCES

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

[17] 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.

[18] 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.

[19] P. Rogaway, "Comments on NISTs RMAC Proposal," 2002.

[20] G. Tsudik, "Message authentication with one-way hash functions," ACM SIGCOMM Computer Communication Review, vol. 22, no. 5, p. 38,1992.

[21] M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," in Advances in Cryptology–CRYPTO'96, vol. 96, Lecture Notes in Computer Science. Springer, 1996, pp. 1–15.

[22] FIPS 198, "The Keyed-Hash Message Authentication Code (HMAC),"Federal Information Processing Standards Publication, vol. 198, 2002.

[23] B. Preneel and P. Van Oorschot, "MDx-MAC and building fast MACs from hash functions," in Advances in Cryptology-CRYPTO'95, vol. 963, Lecture Notes in Computer Science. Springer, 1995, pp. 1–14.

[24] ISO/IEC 9797-2, "Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function," 2002.

[25] A. Bosselaers, R. Govaerts, and J. Vandewalle, "Fast hashing on the Pentium," in Advances in Cryptology-CRYPTO'96, vol. 1109, Lecture Notes in Computer Science. Springer, 1996, pp. 298–312.