International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 14 Issue 2 –APRIL 2015.

SURVEY PAPER ON EFFICIENT AUTHENTICATION FOR MOBILE AND PERVASIVE COMPUTING

Devendra Byahatti[#1] and Pundalik R[*2]

[#]MTECH, Dept. of Computer Science and Engineering
KLE DR. M. S. Sheshgiri College of Engineering and Technology, Belagavi
Karnataka, India

[*] M.E, Dept. of Computer Science and Engineering
KLE DR. M. S. Sheshgiri College of Engineering and Technology, Belagavi
Karnataka, India

***Abstract*— In now a days, so many applications depend on the existence of the 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 very important. In this work we propose a method and system for authenticating messages is provided. A message authentication system generates random string and that will be sent to the recipient's mobile and message sent to the recipient via mail at the other side the receiver got the message through the mail and that will be in encrypted form and the recipient will decrypt the message with key that is sent to his mobile. The message authentication system then determines whether the regenerated message matches the original message. If the codes match, then the integrity and authenticity of the message are verified.**

***Index Terms*— Authentication codes, short messages, confidentiality, integrity, pervasive computing.**

I. INTRODUCTION

Conserving the truthfulness of messages traded over open channels is one of the excellent objectives in cryptography also the literature is rich with message authentication Code (MAC) algorithm that are intended for the sole motivation behind Conserving message truthfulness. In light of their security, MACs can be either genuinely or computationally secure. Genuinely secure MACs give message authentication against counterfeiter with boundless computational force. On the other hand, computationally secure MACs are just secure at the point when counterfeiters have restricted computational force.

We can use the universal hash-function families [1] to the design of unconditionally secure authentication as these are not restricted. Automatically protected MACs relay on universal hash functions can be developed with couple of rounds of computations. In the initial round, the message which we are authenticating is squashed using a universal hash function. Then, in the later round, the squashed image is developed with a cryptographic function (typically a pseudorandom function1). Popular automatically protected universal hashing-based MACs include, but are not inadequate to, [2], [3], [4].

These days, there is a growing want for the creation of networks which consist of a gathering of little devices. In many useful applications, the key motivation of such devices is to exchange small messages. A sensor network, for instance, can be utilized to scrutinize specific events and show some collected data. In various sensor network applications, shown data consist of small secret measurements. Consider, for example, a sensor network deployed in a battlefield with the motivation of displaying the survival of other sequential activities or moving targets. In such area, the privacy and integrity of displayed events are of significant meaning [5], [6].

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 [39]), 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 [7]–[9].

In this paper our contribution is Literature survey, our proposed method, architecture diagram and advantages also conclusion and future scope.

II. LITERATURE SURVEY

Basel Alomair, Andrew Clark and Radha Poovendran [10] proposed universal hash functions that has been appeared repeatedly in the literature and provide a detailed algebraic analysis for the security of authentication codes based on this universal hash family.

In particular, the universal hash family under analysis, as appeared in the literature, uses operation in the finite field Zp. No previous work has studied the extension of such universal hash family when computations are performed modulo a non-prime integer n. In this work, they provide the first such analysis. They investigate the security of authentication when computations are performed over arbitrary finite integer rings Zn and derive an explicit relation between the prime factorization of n and the bound on the probability of successful forgery. More specifically, they show that the probability of successful forgery against authentication codes based on such a universal hash-function family is bounded by the reciprocal of the smallest prime factor of the modulus n.

Basel Alomair and Radha Poovendran [11] proposed a generic approach of constructing such channels is by combining an encryption primitive with an authentication primitive (MAC). In this work, they introduce the design of a new cryptographic primitive to be used in the construction of secure channels. Instead of using general purpose MACs, they propose the employment of special purpose MACs, named \E-MACs". The main motive behind this work is the observation that, since the message must be both encrypted and authenticated, there can be a redundancy in the computations performed by the two primitives. If this turned out to be the case, removing such redundancy will improve the efficiency of the overall construction. In addition, computations performed by the encryption algorithm can be further utilized to improve the security of the authentication algorithm. In this work, they show how E-MACs can be designed to reduce the amount of computations required by standard MACs based on universal hash functions, and show how E-MACs can be secured against key-recovery attacks.

Antoori Bosselaers. R e d Govaerts and Joos Vandewalle [12] proposes the advent of the Pentium processor parallelization finally becarne available to Intel based computer systems. One of the design principles of the MD4-family of hash functions (MD4, MD5, SHA-1, FLIPEMD-160) is to be fast on the 32-bit Intel processors. This paper shows that carefully coded implementations of these hash functions are able to exploit the Pentium's superscalar architecture to its maximum effect: the performance with respect to execution on a non-parallel **ar**chitecture increases by about 60%. This is an important result in view of the recent claims on the limited data bandwidth of these hash functions. Moreover, it is conjectured that these implementations are very close to optimal. It will also be shown that performance penalty incurred by non-cached data and endianness conversion is limited, and in the order of 10% of running time.

III. PROBLEM STATEMENT

Presently, many applications depend 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. At the same time, 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.

IV. PROPOSED SYSTEM

In now a day's preserving the confidentiality and integrity of the communicated messages are very important so in our proposed methodology the message will be encrypted first then it sent over the Internet and at the receiver side intended receiver will decrypt the message with key.

Here sender will generate key send it to the receiver's mobile and with help of the key the receiver will decrypt the message.

The below fig.1 shows the architecture of our proposed system

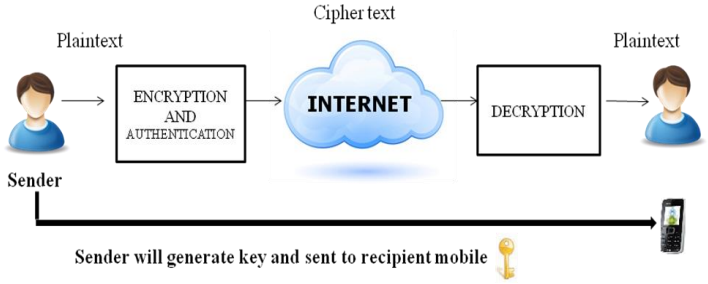

Figure.1 Architecture of proposed system

IMPLEMENTATION MODULES

1. Authenticating Short Encrypted Messages
2. Security Model
3. Security of the authenticated encryption composition
4. Data privacy

1. Authenticating short encrypted messages

In this module [15], we describe our 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 applications in which messages are of fixed length that is known a priori, such as RFID systems in which tags need to authenticate their identifiers, sensor nodes reporting events that belong to certain domain or measurements within a certain range, etc. The novelty of the proposed scheme is to utilize the encryption algorithm to deliver a random string and use it to reach the simplicity and efficiency of one-time pad authentication without the need to manage impractically long keys.

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 and N describing the length of the shared key and the resulting authentication tag.

3. Security of the Authenticated Encryption Composition:

In this module [15], it defined two notions of integrity for authenticated encryption systems: the first is integrity of plaintext (INT-PTXT) and the 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 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.

4. Data Privacy:

Recall that two pieces of information are transmitted to the intended receiver (the cipher text and the authentication tag),both of which are functions of the private plaintext message. Now, when it comes to the authentication tag, observe that then once r serves as a one-time key (similar to the role r plays in the construction of Section.

The formal analysis that the authentication tag does not compromise message privacy is the same as the one provided. The cipher text of equation, on the other hand, is a standard CBC encryption and its security is well-studied; thus, we give the theorem statement below without a formal proof (interested readers may refer to textbooks in cryptography.

Advantages:

1. More security.

2. 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.

V. 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 unique, 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 we generate the random string and that random string is used as a key that will sent to the recipient directly to his personal mobile phone so that there should be integrity in the communicated messages, and encryption methods are the data encryption standard and the advanced encryption standard which includes the modular operations which are fast. For instance, while the cryptographic hash functions SHA-256 and SHA-512 run in about 23.73 cycles/byte and 40.18 cycles/byte, respectively [13], the modular multiplication runs in about 1.5 cycles/byte [14]

In proposed system we have less time complexity, less computational cost, effective integrity, more secure while the transmission, more confidential.

VI. CONCLUSION

In this work, a new technique which will provide confidentiality and integrity of the communicated short messages, the key idea behind this technology is to 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 one-time keys.

Particularly, it has been confirmed in this report that validation tags can be calculated with one calculation and a one modular multiplication. Stated that messages are comparatively short, addition and modular multiplication can be execute quicker than presented computationally secure MACs in the journalism 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.

VII. FUTURE SCOPE

In the future have to investigate about the further implementation of encryption techniques to enhance the process with the less time complexity and the high integrity in the process. And have to improve the whole performance by implementing the other process oriented to the security of the data in the mobile computing process. And also need to investigate about the other possible ways to improving the data security other than the cryptographic techniques as the additional process to the data security of the data.

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] D.Bernstein "The Poly1305AES Message-Authentication Code," Proc. 12th Int'l Conf. Fast Software Encryption (FSE '05), pp. 32-49, 2005.

[3] S. Halevi and H. Krawczyk, "MMH: Software Message Authentication in the Gbit/Second Rates," Proc. Int'l Conf. Fast Software Encryption (FSE '97), pp. 172-189, 1997.

[4] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, "UMAC: Fast and Secure Message Authentication," Proc. 19th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '99), pp. 216-233, 1999.

[5] I. Akyildiz, W. Su, Y. ankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.

[6] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Toward a Statistical Framework for Source Anonymity in Sensor Networks," IEEE Trans. Mobile Computing, vol. 12, no. 2, pp. 248-260, doi : 10.1109 / TMC.2011.267, Feb. 2013.

[7] S. Sarma, S. Weis, and D. Engels, "RFID systems and security and privacy implications," Cryptographic Hardware and Embedded Systems- CHES 2002, pp. 1–19, 2003.

[8] A. Juels, "RFID security and privacy: A research survey," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 381–394, 2006.

[9] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, "RFID systems: A survey on security threats and proposed solutions," in Personal Wireless Communications. Springer, 2006, pp. 159–170.

[10] B. Alomair, A. Clark, and R. Poovendran, "The Power of Primes: Security of Authentication Based on a Universal ash-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] 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.

[13] J. Nakajima and M. Matsui, "Performance Analysis and Parallel Implementation of Dedicated Hash Functions," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT), pp. 165-180, 2002.

[14] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway,"UMAC: Fast and Secure Message Authentication," Proc. 19th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '99), pp. 216-233, 1999.

[15] B.Alomair and R. Poovendran, "Efficient Authentication for Mobile and Pervasive Computing," Proc. 12th Int'l Conf. Information and Comm. Security (ICICS '10), 2010.