Efficient Authentication for Mobile and Pervasive Computing

[1]Mr. Swapnil Wani, [2]Mr.Farooqui Nabil, [3]Mr.Khan Inamullah, [4]Mr.Khan Mehboob

[1]Asst.Professor,[2,3,4] UG Student,[1,2,3,4]Computer Engg. Dept. Shivajirao S. Jondhle College of Engineering & Technology, Asangaon, Maharshatra, India.

[1]swapnilwani24@hotmail.com,[2]nabil.farooqui23@gmail.com,[3]inamkhan9172@gmail.com,

[4]mehboob7738@gmail.com.

Abstract- PRESERVING the integrity of messages changed over public channels is one in each of classic goals in cryptography and then the literature is made with message authentication code (MAC) algorithms that designed for the sole real purpose of conserving message integrity. Supported their security, MACS is either categorically or computationally secure. Categorically secure MACS offer message integrity against forgers with unlimited process power. On the opposite hand, computationally secure MACS solely secure once forgers have restricted computation.

Keywords- MAC (Message Authentication Codes), Cryptography

I. INTRODUCTION

The basic concept granting unconditional security is that the authentication key can only be accustomed authenticates a limited number of exchanged messages. Since the management of one-time keys is taken into account impractical in many applications, computationally secure MACS became the strategy of choice for many real-life applications. In computationally secure MACS, keys will be accustomed authenticate an arbitrary number of messages. That is, after agreeing on a key, legitimate users can exchange an arbitrary number of authenticated messages with constant key. Depending on the foremost building block accustomed construct them, computationally secure MACS are often classified into three main categories: block cipher based, cryptographic hash function based, or universal hash-function family based. 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 taken into account impractical in many applications, computationally secure MACs became the tactic of choice for many real-life applications. In computationally secure MACs, keys are often wont 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 an equivalent key. Depending on the foremost building block used to construct them, computationally secure MACs are often classified into three main categories: block cipher based, cryptographic hash function based, or universal hash-function family based. CBC-MAC is one of the most known blocks cipher-based MACs, specified in the Federal Information Processing Standards publication 113 and the International Organization Standardization ISO/IEC 9797-1. CMAC, a modified version of CBC-MAC, is presented in the NIST special publication 800-38B, which was based on the OMAC.

II. AIMS AND OBJECTIVE

a) Aim

It is supported employing a cryptographic hash or symmetric encryption algorithm. The authentication keys only shared by a minimum of two parties or two communicating devices but it'll fail within the existence of a 3rd party since the algorithm will no longer be effective in detecting forgeries. In addition, the key must even be randomly generated to avoid its recovery through brute force searches and related key attacks designed to spot it from the messages transiting the medium. Securing the user message by providing authentication and security if the authenticated message must also be encrypted.

b) Objective Authenticity and MACS

Verifying the integrity and authenticity of information is a prime necessity in computer systems and networks. In particular, two parties communicating over an insecure channel require a way by which information sent by one party are often validated as authentic (or unmodified) by the opposite. Most commonly such a mechanism is based on a secret key shared between the parties and takes the form of a Message Authentication Code (MAC).

MACing with cryptographic hash functions

It is easy to ascertain why people want to MAC with

 DOI : 10.35291/2454-9150.2020.0226

cryptographic hash functions: the favored hash functions are faster than block ciphers in software implementation; these software implementations are readily and freely available; and therefore, the functions aren't subject to the export restriction rules of the USA and other countries.

III. LITERATURE SURVEY

[1] J. Carter, M. Wegman, M. Bellare, R. Guerin and P. Rogaway, "Universal classes of hash functions, in Proceedings of the ninth annual ACM symposium on Theory of computing–STOC'77". IEEE, 2014.

PRESERVING the integrity of messages exchanged over public channels is one among the classic goals in cryptography and thus the literature is rich with message authentication code (MAC) algorithms that are designed for the only purpose of preserving message integrity. supported their security, MACs are often either unconditionally or computationally secure.

2) L. Carter and M. Wegman, "Universal hash functions," Journal of Computer and System Sciences, vol. 18, no. 2. 2012.

Computationally secure MACs are only secure when forgers have limited computational. a well-liked class of unconditionally secure authentication is predicated on universal hash-function families, pioneered by Carter and guan. Since then, the study of unconditionally secure message authentication supported universal hash functions has been attracting research attention, both from the planning and analysis standpoints.

3) Bierbrauer, "A2-codes from universal hash classes," in Advancesin Cryptology– EUROCRYPT'95, vol. 921, Lecture Notes in ComputerScience. Springer, 2013.

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.

IV. EXISTING SYSTEM

There are two important observations to form about existing MAC algorithms. First, they're designed independently of the other operations required to be performed on the message to be authenticated.

For instance, if the authenticated message must even be encrypted, existing MACs aren't designed to utilize the functionality which will be provided by the underlying 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 the majority existing MACs are inefficient when the messages to be authenticated are short. (For instance, UMAC, the fastest reported message authentication code within the cryptographic literature, has undergone large algorithmic changes to extend its speed on short messages).

Insufficient Bandwidth: Mobile Internet access is generally slower than direct cable connections, using technologies such as GPRS and EDGE, and more recently 3G networks. These networks are usually available within range of commercial cell phone to rs. Higher speed wireless LANs are inexpensive but have very limited range.

Security Standards: When working mobile, one is dependent on public networks, requiring careful use of Virtual Private Network (VPN). Security is a major concern while concerning the mobile computing standards on the fleet. One can easily attack the VPN through a huge number of networks interconnected through the line. Human interface with device: Screens and keyboards tends to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training

Potential hazards: People who use mobile devices while driving is often distracted from driving are thus assumed more likely to be involved in traffic accidents. Cell phones may interfere with sensitive medical devices. There are allegations that cell phone signals may cause health problems

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.

Disadvantages:

1. Existing MACs are not designed to utilize the functionality that can be provided by the underlying encryption algorithm.

2. Most existing MACs are designed for the general computer communication systems, independently of the properties that messages can possess.

3. Unconditionally secure universal hashing- based MACs are considered impractical in most modern applications, due to the difficulty of managing one-time keys.

4. Messages are relatively short; addition and modular multiplication can be performed faster than existing computationally secure MACs.

 DOI : 10.35291/2454-9150.2020.0226

V. COMPARITIVE STUDY

Table no.1

Sr No.	Paper Name	Author/Publication	Technology	Advantages	Disadvantages
1.	New hash functions and their use in authentication and set equality	Carter Journal of Computer and System Sciences	Digital signatures	It provides integrity verification while message authentication code does not.	
2.	Digital Signature simply does not provide confidentiality.	MK Thompson BBB publication vol. 1109, Lecture Notes in Computer Science	Message Authentication Code (MAC).	MACs can be either unconditionally or computationally secure.	MACs are inefficient when the messages to be authenticated are short
3.	Computer Data Authentication	IK Jackson ISO/IEC 9797-1 Cipher modes of operation: The CMAC Mode for authentication	Hash Function	hashes are used to guarantee the integrity of data	Does not use a private key
4.	The Security of the Cipher Block Chaining Message Authent-ication Code	Bellaire Journal of Computer and System Sciences, vol. 61, no. 3	MAC with Pseudo random number	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	Messages are relatively short, addition and modular multiplication can be performed faster than existing computationallysecure MACs.

VI. PROBLEM STATEMENT

In the pervasive computing environment, need a security policy which may simultaneously be an unobtrusive mechanism to the user have the power to urge the services available for the user in a transparent manner. The system needs a dynamic security policy which is flexible enough to update and modify on the fly. Due to the distributed and unplanned nature of the pervasive computing environment, this technique is hospitable several unique vulnerabilities and suffers from quite number of known problems whose reputed solutions are not applicable here.

VII. PROPOSED SYSTEM

The two new techniques for authenticating short encrypted messages that are more efficient than existing approaches. In the first technique, the very fact that the message to be authenticated is additionally encrypted, with any secure encryption algorithm, to append a brief random string to be used in the authentication process.

Advantages:

1. More security, using two concepts one is mobile computing and another one is pervasive computing.
2. The random strings used for various operations are independent; the authentication algorithm can enjoy 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, make the additional assumption that the used encryption algorithm is block cipher based to further improve the

 DOI : 10.35291/2454-9150.2020.0226

computational efficiency of the primary technique.

VIII. ALGORITHM

STEP 1: START

STEP 2: Entries from user

STEP 3: Admin check for user login and generates Secret key for user.

STEP 4: The key is shared between the sender and the receiver of the message. STEP 4: To send a message user enter its secret key as it's provided by Admin.

STEP 5: The message authentication system generates the message authentication code based on a combination of the message.

STEP 6: Then message is transmitted to the intended receiver in a confidential manner.

STEP 7: After receiving the encrypted message and the message authentication code, the message authentication system of the receiver's device decrypts and authenticates the message.

STEP 8: The message authentication system generates a so decrypted message by decrypting with the key the encrypted message and extracts the message

STEP 9: The message authentication system then determines whether the regenerated message authentication code matches.

STEP 10: If the codes match,

then the integrity and authenticity of the message are verified.

STEP 11: The message is attacked or changed by an attacker.

STEP 12: Admin then recover the message of the user and verifying the content of the message.

STEP 13: END.

IX. MATHEMATICAL MODEL

Associated with the scheme are parameters and N describing the length of the shared key and the resulting authentication tag, respectively. On input an `-bit key k and a message m, algorithm S outputs an N-bit string τ called the authentication tag, or the MAC of m. On input an `-bitkey k, a message m, and an N-bit tag τ , algorithm V output sa bit, with 1 standing for accept and 0 for reject. It's basically validity condition, namely that authentic tags are accepted with probability one. That is, if τ = S(k, m), it must be the case that V(k, m, τ) = 1 for any key k, message m,and tag τ

In general, an adversary against a message authentication scheme is a probabilistic algorithm A, which is given oracle access to the signing and verifying algorithms S(k, ·) and V(k, ·, ·) for a random but hidden choice of k. A can query S to generate a tag for a plaintext of its choice and ask the verifier V to verify that τ is a valid tag for the plaintext. Formally, A's attack on the scheme is described by the following experiment:1. A random string of length ` is selected as the shared secret.2. Suppose A makes a signing query on a message m. Thent he oracle computes an authentication tag τ = S(k, m)and returns it to A. (Since S may be probabilistic, this step requires making the necessary underlying choice of a random string for S, anew for each signing query.)3. Suppose A makes a verify query (m, τ). The oracle computes the decision d

= V(k, m, τ) and returns it to A.

$$\Sigma \quad \Sigma$$

$$Adv^{ind\text{-}cpa}(B)=Pr\ b^{J}=b\,.$$

LetΣbetheauthenticatedencryptioncompo

-sition described using E as the underlying encryptionalgorithm.Thengivenanadversary,A,againsttheprivacyofΣ,onecanconstr uctanadversary,B,against E suchthat

$$Adv^{priv}(A) \le Adv^{ind\text{-}cpa}\ B.$$

X. SYSTEM ARCHITECTURE

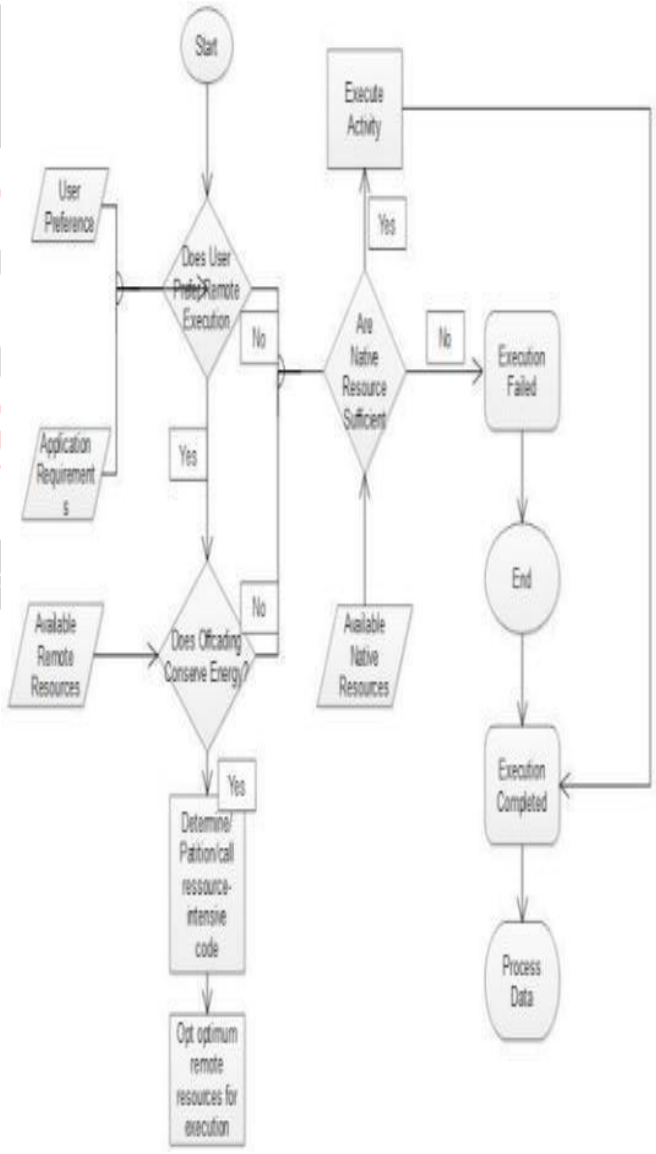

Fig.1: System Architecture

 DOI : 10.35291/2454-9150.2020.0226

XI. DESIGN DETAILS

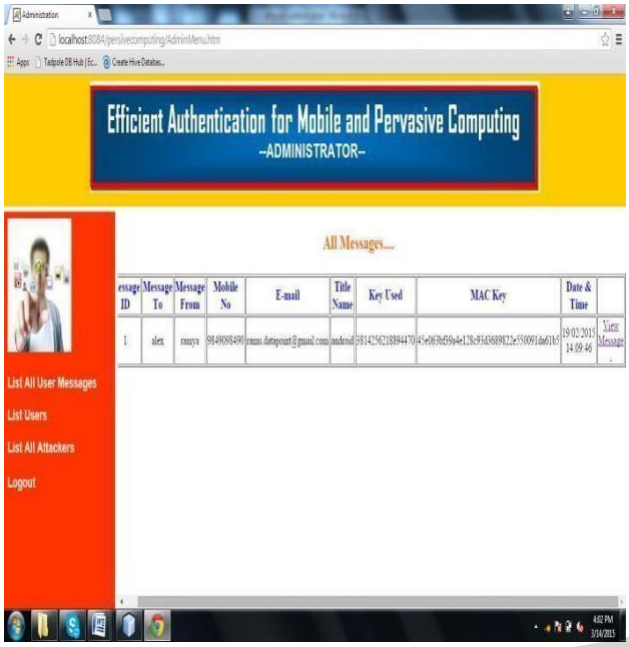

Fig 2: Result

XII. CONCLUSION

Thus, we have tried to implement the paper "J. Carter, M. Wegman, M. Bellare, R. Guerin senior member IEEE and P. Rogaway","Efficient Authentication For mobile and pervasive computing",IEEE 2014, And according to implementation the conclusion is a new technique for authenticting 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-time keys.

REFERENCE

[1] J. Carter, M. Wegman, M. Bellare, R. Guerin and P. Rogaway, "Universal classes of hash functions, in Proceedings of the ninth annual ACM symposium on Theory of computing–STOC'77". IEEE, 2014.

[2] M. Wegman and J. Carter, "New classes and applications of hashfunctions," in 20th Annual Symposium on Foundations of ComputerScience–FOCS'79. IEEE, 2010.

[3] L. Carter and M. Wegman, "Universal hash functions," Journal ofComputer and System Sciences, vol. 18, no. 2. 2012.

[4] M. Wegman and L. Carter, "New hash functions and their use in authenticationand set equality," Journal of Computer and System Sciences,vol. 22. 2011.

[5] J. Bierbrauer, "A2-codes from universal hash classes," in Advancesin Cryptology–EUROCRYPT'95, vol. 921, Lecture Notes in ComputerScience. Springer, 2013.

[6] M. Atici and D. Stinson, "Universal Hashing and Multiple Authentication,"in Advances in Cryptology–CRYPTO'96, vol. 96, Lecture Notesin Computer Science. Springer, 2014.

[7] T. Helleseth and T. Johansson, "Universal hash functions from exponentialsums over finite fields and Galois rings," in Advances in cryptology–CRYPTO'96, vol. 1109, Lecture Notes in Computer Science. Springer,2011.

[8] V. Shoup, "On fast and provably secure message authentication based onuniversal hashing," in Advances in Cryptology– CRYPTO'96, vol. 1109,Lecture Notes in Computer Science. Springer, 2012.

[9] J. Bierbrauer, "Universal hashing and geometric codes," Designs, Codesand Cryptography, vol. 11, no. 3.2012.

[10] B. Alomair, A. Clark, and R. Poovendran, "The Power of Primes:Security of Authentication Based on a Universal Hash-FunctionFamily," Mathematical Cryptology, vol. 4, no. 2, 2010.

 DOI : 10.35291/2454-9150.2020.0226