Authentication Techniques That Work Well With Mobile and Distributed Systems

BESHINI AJAY KUMAR
M.Tech Student, Dept of CSE, Malla Reddy College of Engineering and Technology, Hyderabad, T.S, India

M.SANDEEP
Associate Professor, Dept of CSE, Malla Reddy College of Engineering and Technology, Hyderabad, T.S, India

Dr. M.SAMBASIVUDU
Associate Professor, Dept of CSE, Malla Reddy College of Engineering and Technology, Hyderabad, T.S, India

Abstract: **In the modern technological world, the existence of minuscule devices that are able to exchange data and build networks is necessary for the completion of numerous activities. In many of these applications, the confidentiality and dependability of the information that is being transferred are of the utmost importance. The purpose of this article is to offer two novel ways for authenticating short conversations that are encrypted, with the end objective of fulfilling the requirements of mobile and ubiquitous software. We take advantage of the fact that the message that has to be verified must also be encrypted in order to propose a set of authentication codes that are not only provably secure but also surpass every other message authentication code that has been published in the past. The recommended procedures make use of encryption techniques to provide an additional layer of protection, with the goal of enhancing the performance of the conventional authentication primitives.**

Keywords: **Verification; Unconditional Guarantee; Computational Guarantee;**

I. INTRODUCTION:

Universal hash-function families, which were first developed by Carter and Wegman, are the foundation of a well-known category of unconditionally safe authentication. At that time, the investigation of unconditionally safe message authentication based on universal hash functions had been gaining the interest of researchers in the field, both from the perspective of the design and the analysis [1]. The fundamental idea that makes it possible to achieve absolute security is that the authentication key may only be used to authenticate a certain number of messages that have been traded. The administration of one-time keys is seen as impracticable in many applications; hence, computationally secure MACs have emerged as the technique of choice for the majority of applications that are used in real life. In MACs that provide computational security, an unlimited number of messages can be authenticated using a key. That is to say, when valid users have agreed upon a key, they are able to communicate an unlimited number of times while using the same key to verify their communications. Block cyphers, cryptographic hash functions, and universal hash-function families are the three primary building blocks that can be used to construct computationally secure MACs. These MACs can be placed into one of three primary categories, depending on which one they use as their primary building block. Regarding the MAC algorithms that are now in use, there are two essential points to note. To begin, they were created so that they could be used independently of any other actions that needed to be carried out on the message that needed to be verified. Existing message authentication codes, for instance, are not intended to make use of the capability that may be given by the underlying encryption method in the event that the authenticated message also has to be encrypted. Second, the majority of the MACs that are now in use were developed for generic computer communication systems. This was done regardless of the qualities that messages may have. For instance, one might discover that the majority of the currently available MACs are inefficient when the messages that need to be authenticated are quite short. (For example, UMAC, which is currently the fastest recorded message authentication code in the cryptographic literature, has been subject to significant algorithmic adjustments in order to boost its performance while processing short messages.) In the modern day, on the other hand, there is a growing need for the deployment of networks that are comprised of a collection of tiny devices. In a wide variety of real-world contexts, the primary function of such devices is to convey succinct signals to one another [2][3]. For instance, you may set up a sensor network to keep track of particular happenings and relay the information that you've gathered. In many different applications for sensor networks, the data that is provided consists of brief, secret measurements. Take, for example, a sensor network that is installed on a battlefield with the intention of reporting the presence of moving targets or other actions that occur over time. In these kinds of applications, maintaining the secrecy and honesty of the events that are recorded is of the utmost significance.

II. PROBLEM STATEMENT:

Regarding the MAC algorithms that are now in use, there are two essential points to note. To begin, they were created so that they could be used independently of any other actions that needed to be carried out on the message that needed to be verified. Existing message authentication codes, for instance, are not intended to make use of the capability that may be given by the underlying encryption method in the event that the authenticated message also has to be encrypted. Second, the majority of the MACs that are now in use were developed for broad computer communication systems, and this was done regardless of the qualities that messages may have. For instance, one might discover that the majority of the currently available MACs are inefficient when the messages that need to be authenticated are quite short. (For example, UMAC, which is currently the fastest recorded message authentication code in the cryptographic literature, has been subject to significant algorithmic adjustments in order to boost its performance while processing short messages.) Current MACs are not intended to make use of the functionality that may be provided by the underlying encryption method [4]. This is because encryption algorithms are not designed to offer such capabilities. The vast majority of the MACs that are now in use were developed for generic computer communication systems. This was done regardless of the qualities that messages may have.

III. PROPOSED METHODOLOGIES:

We propose 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, is it possible to do better than simply encrypting the messages using an encryption algorithm and authenticating them using a standard MAC algorithm? This is the question we will be addressing in our investigation. We respond to the topic by presenting two novel methods for authenticating brief encrypted communications that are more time and resource effective than the ways that are currently in use [5]. In the first method, we take advantage of the fact that the message that has to be verified is likewise encrypted using any reliable encryption algorithm in order to attach a brief random string that will be used in the process of authenticating the message. Enhanced safety via the use of two distinct computer paradigms, namely mobile computing and ubiquitous computing. Since the random strings used for the various operations are kept separate from one another, the authentication algorithm can take advantage of the ease of use provided by unconditionally secure authentication. This makes it possible to conduct authentication in a manner that is both quicker and more effective, without the need for laborious management of one-time keys. With the second method, we make the additional assumption that the used encryption algorithm is based on a block cypher in order to further increase the computational efficiency of the first method. This was done so that the second method could compete with the first method [6].

IV. ENHANCED SYSTEM:

We will discuss our first authentication technique that is compatible with any IND-CPA-safe encryption algorithm. This strategy may be used to protect sensitive data. One of the most significant presumptions that we make is that the length of communications that need to be verified does not exceed a certain threshold. This includes applications in which messages are of a 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 domains or measurements within a certain range, etc.; for example, RFID systems in which tags need to authenticate their identifiers. The suggested method is new in that it makes use of an encryption technique to generate a random string and then applies that string to provide the ease of use and effectiveness of one-time pad authentication without requiring the management of keys that are impractically lengthy. A signature method, denoted by S, and a verifying algorithm, denoted by V, makes up the components of an authentication system for messages. While the process for confirming the signature may not be probabilistic, the signing procedure could be. The parameters and the number N, which each describe the length of the shared key and the resultant authentication tag, respectively, are associated with the scheme. Integrity of plaintext (INT-PTXT) and integrity of cypher text (INT-CTXT) are the two ideas of integrity that were described for authenticated encryption systems in this module. The first of these was introduced in this module (INT-CTXT). The security of several ways for creating generic compositions is evaluated, and this process is combined with encryption algorithms that give indistinguishable abilities under selected plaintext assaults (IND-CPA). It is important to keep in mind that the construction that we have created is an example of the Encrypt-and-Authenticate (E&A) generic composition. This is due to the fact that the plaintext message is fed into the encryption algorithm as an input, and then the same plaintext message is fed into the authentication algorithm as an input. It is important to keep in mind that the cypher text and the authentication tag are both functions of the private plaintext message, and that both of these pieces of information are delivered to the intended recipient. When it comes to the authentication tag, it is important to note that once r acts as a one-time key (similar to the function that r performs in the building of Section), the rigorous analysis that was given may be used to confirm that the authentication tag does not in any way undermine the confidentiality of the communication. The cypher text of equation, on the other hand, is a standard CBC encryption with well-studied security; as a result, we present the theorem formulation below without a formal demonstration (interested readers may refer to cryptography textbooks for more information).

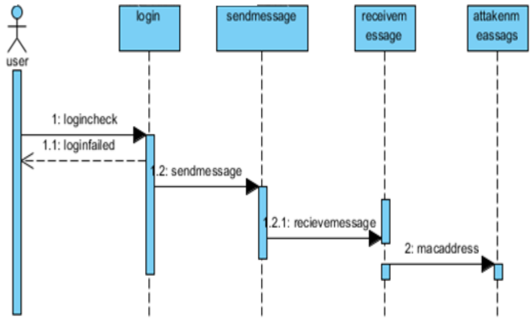

Fig 1: Sequence of System

V. CONCLUSIONS:

In this piece of work, a creative method for authenticating brief communications that have been encrypted has been suggested. Since the communication that has to be authenticated also needs to be encrypted, the cypher text is the medium via which a nonce that is generated at random is sent to the person who is supposed to receive it. Because of this, it was possible to build an authentication code that benefited from the ease of use provided by unconditionally safe authentication but did not require the management of one-time keys. In particular, it has been proven in this study that authentication tags may be calculated using one addition and one modular multiplication. As compared to other computationally secure MACs in the cryptography literature, the operations of addition and modular multiplication may be carried out much more quickly. This is due to the fact that messages are often not very long. Messages that are encrypted by devices that use block cyphers can be authenticated with the help of a single modular addition, thanks to a second method that makes use of the fact that block cyphers can be modeled as strong pseudorandom permutations. This method was developed in response to the fact that block cyphers are commonly used to encrypt messages. It has been shown that the suggested strategies are orders of magnitude quicker than conventional MAC algorithms while also using orders of magnitude less energy. As a result, they are more appropriate for use in devices with limited processing capabilities, such as mobile and ubiquitous devices.

REFERENCES:

[1] B. Alomar, 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.

[2] B. Alomar 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.

[3] FIPS 113, “Computer Data Authentication,” Federal Information Processing Standards Publication, 113, 1985.

[4] ISO/IEC 9797-1, “Information technology – Security techniques –Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher,” 1999.

[5] M. Working, “Recommendation for block cipher modes of operation: The CMAC mode for authentication,” 2005.

[6] 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.

[7] M. Bellare, R. Guerin, and P. Rogaway, “XOR MACs: New methods for message authentication using finite pseudorandom functions,” in Advances in Cryptology–CRYPTO’95, vol. 963, Lecture Notes in Computer Science. Springer, 1995, pp. 15–28.

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

[9] 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.

[10] 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.