IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Survey on Efficient Authentication for Mobile and Pervasive Computing

Mukesh M. Patil[1], Ass. Prof. Nalini A. Mhetre[2]

Dept. of Computer Engineering, SKNCOE, Pune, India[1,2]

Abstract: In this survey, we endorse new techniques for authenticate the short encrypted messages which can be fulfill the requirements of pervasive applications. With the help of these advantage that the message to be authenticated must also be encrypted, we suggest provably secure authentication codes which can be greater efficient than any message authentication code there are used an inside the literature. The key point of this concept at the back of the proposed techniques is to use the security that help the encryption algorithm would provide to implements the more efficient authentication mechanisms, as opposed to use standalone authentication primitives.

Keywords: Authentication, unconditional security, computational security, universal hash-function families, pervasive computing.

I. INTRODUCTION

Maintaining the integrity of messages exchanged over public channels is one of the conventional dreams in cryptography and the literature is wealthy with message authentication code (MAC) algorithms that are designed for the sole purpose of retaining message integrity. Based totally on their security, MACs may be both un conditionally or computationally secure. Unconditionally secure MACs allow for message integrity opposed to forgers with unlimited computational energy. On the other hand, computationally cozy MACs are handiest comfortable when forgers have constrained computational strength.

The study of unconditional security is that the authentication key can only be used to authenticate a several number of transmitted messages. So the one time key for secure communication considered as impractical in many application.

MACs have come to be the technique of preference for maximum real-life applications. With the help of keys, authenticate an arbitrary number of messages in computationally secure MACs. That is, after authenticate the keys, legitimate users can exchange an several number of authenticated messages with the same key. Depending on the main building block utilized to implement them, computationally secure MACs can be divided into three main types such as: block cipher based, cryptographic hash function based and universal hash function family based.

The principle motive behind the performance benefit of typical hashing-primarily based MACs is the fact that processing messages block through block the usage of time-honored hash features is orders of magnitude faster than processing them block through block the usage of block ciphers or cryptographic hash functions. There are vital observations to make approximately current MAC algorithms. First, they're designed independently of any other operations required to be completed at the message to be authenticated. As an instance, if the authenticated message has to also be encrypted, current MACs aren't designed to make use of the functionality that could be furnished with the aid of the underlying encryption algorithm. Second, maximum current MACs are designed for the overall general computer communication systems, independently of the properties that messages can possess.

An application where in messages that need to be exchanged are brief and each their privacy and integrity want to be preserved, can one do better than simply encrypting the messages using an encryption algorithm and authenticating them using standard MAC algorithm. The two new techniques for authenticating short encrypted messages those are greater than present procedures. First approach, message to be authenticated is also encrypted, with any cozy encryption algorithm, to append a brief random string to be used within the authentication procedure.

For the reason that random strings used for distinctive operations are unbiased, the authentication set of rules can benefit from the simplicity of unconditional cozy authentication to allow for quicker and greater efficient authentication, without the difficulty to manage one-time keys.

Inside the Second approach, we survey on make the extra assumption that the used encryption set of rules is block cipher primarily based to in addition enhance the computational efficiency of the first approach.

The using cause behind our investigation is that the use of a standard cause MAC set of rules to authenticate exchanged messages in such structures may now not be the most green answer and might lead to waste of sources already to be had, specifically, the security that is supplied via the encryption algorithm.

II. RELATED WORK

V. Shouppproposed on Fast and Provably Secure Message Authentication Based on Universal Hashing [1] like well-known techniques for message authentication the use the universal hash features. This novel technique come out with very promising, as it offer system which can be each efficient and provably secure under affordable assumptions. They gave novel method in this line of research. First, it examines the simple implementation and a few editions under extra sensible and realistic assumptions. Second, it advise how those methods can be effectively applied, and it reviews at the results of empirical overall performance assessments that show that those schemes are aggressive with other commonly employed schemes whose security is less properly-installed.

G. Tsudik implements in Message Authentication with One-Way Hash Functions [2]. A one-way hash function is a necessarily cryptographic primitive for digital signatures and authentication. There execution toward an implementation of different cryptographic algorithms (e.g. MACs) the usage of hash functionality. Particularly, such algorithms could be easy to enforce with existing codes of hash functions when they are used as a black box without modification. They derived such constructions for block ciphers and MACs in a few preferred forms (i.e. with variable key sizes, block lengths and MAC lengths).

T. Krovetz look into on UMAC: Fast and Provably Secure Message Authentication to depict a message authentication algorithm [3], UMAC, which can authenticate messages (in software, on contemporary machines) in an order of magnitude effectively faster than current scheme (e.g. HMAC-SHA1), and about double faster times previously reported for the universal hash-function family MMH. To gain such high speeds, UMAC uses a new universal hash-function family, NH, and an implementation which offers effective exploitation of SIMD parallelism. The "cryptographic" work of UMAC is done using standard primitives of the user's choice, such as a block cipher or cryptographic hash function; no new heuristic primitives are implements here. Instead, the security of UMAC is strictly proved, in the sense of providing exact same and quantitatively strong results which present an inability to forge UMAC-authenticated messages assuming an inability to break the underlying cryptographic primitive. Unlike conventional, inherently serial MACs, UMAC is parallelizable, and will have faster implementation speeds as machines offer up increasing amounts of parallelism. They envision UMAC as a practical algorithm for next-generation message authentication.

M. Feldhofer, S. Dominikus and J. Wolkerstorfer designs Strong Authentication for RFID Systems [4] with the help of AES Algorithm. Radio frequency identity (RFID) is a rising technology which takes large productiveness benefits in applications where entities have to be identified automatically. They provide problems regarding protection and privacy of RFID systems that are great extent discussion in public. In contrast to the RFID network, which claims that cryptographic components are too expensive for RFID tags, author suggest a solution to use the robust symmetric authentication which is suitable for nowadays necessities concerning low power consumption and low die-size. They introduced an authentication protocol which serves as a proof of concept for authenticating an RFID tag to a reader device using the Advanced Encryption Standard (AES) as cryptographic primitive. The main concept of this work is a new method of an AES hardware implementation which encrypts a 128-bit block of data within 1000 clock cycles and has power consumption below 9 µA on a 0.35 µm CMOS technique.

M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, designed Concrete Security Treatment of Symmetric Encryption. [5] Notions and schemes are utilized for symmetric (i.e. personal key) encryption in a concrete safety framework. They provide four kinds of notions for security in against to elect plaintext attack and analyze the concrete complexity of discounts between them, supply both upper and lower bounds, and getting tight relations. In this way they classified notions (despite the fact that polynomially reducible to each other) as stronger or weaker in phrases of concrete protection. Next they provide concrete protection analyses of schemes to encrypt the use of a block cipher, such as the most famous encryption technique, CBC. They set up tight bounds (which mean matching higher bounds and attacks) on the achievement of adversaries as a function in their assets.

M. Bellare and C. Namprempre, An authenticated encryption method is a symmetric encryption method [6] whose goal is to offer both privacy and integrity. They assumed two possible notions of authenticity for such schemes, namely integrity of plaintexts and integrity of cipher texts, and associate them (when coupled with IND-CPA) to the belief of privacy (IND-CCA, NM-CPA) by presenting significance and interval between all notions considered. Then they examined the security of authenticated encryption methods designed by "generic composition," meaning making black box use of a given symmetric encryption method and a given MAC. Three kinds of composition methods are considered such as first Encrypt-and-MAC, second MAC-then-encrypt, and third is Encrypt-then-MAC. For each of these, and for each notion of security, they indicated whether or not the resulting methods achieve the notion in question presuming the given symmetric encryption method is secure opposed to chosen-plaintext attack and the assume MAC is not able to be forged under chosen-message attack.

B. Alomair and R. Poovendran, an Efficient Authentication for Mobile and Pervasive Computing [7], they derived the many applications rely on the existing of small device that can interchange information and make the communication networks. The main motive of such application is to provide the confidentiality and integrity

of the communicated messages. In the proposed work, they implements the novel technique for authenticating short encrypted messages that are fulfill the all the requirements of mobile and pervasive applications. To provide the such security message to be authenticated must also be encrypted. They designed provably secure authentication codes that are more effective than any message authentication code in the literature. The basic idea behind the proposed method is to concatenate a short random string to the plaintext message before encryption to help a more efficient authentication.

.

III. CONCLUSION

The survey paper on a new idea for authenticating short encrypted messages is implemented.In which plain message should be authenticated must also be encrypted is used to deliver a random number to the meant receiver through the ciphertext. This gives the permission to design of an authentication code that benefit from the simplicity of unconditionally at ease authentication without the want to manipulate one-time keys. Specially, that authentication tags can be generated through the one addition and a one modular multiplication. Given that messages are generally small, addition and modular multiplication can be complete faster than present computationally secure MACs in the literature of cryptography. Main assumption that 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 design in orders of magnitude faster and consume orders of magnitude less energy than existing MAC algorithms. Therefore, this technique is more suitable to be used in computationally constrained mobile and pervasive devices.

REFERENCES

[1]. 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.
[2]. G. Tsudik, "Message Authentication with One-Way Hash Functions," ACM SIGCOMM Computer Comm. Rev., vol. 22, no. 5, pp. 29-38, 1992.
[3]. T. Krovetz, "UMAC: Fast and Provably Secure Message Authentication," http://fastcrypto.org/umac, 2006.
[4]. M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," Proc. Workshop Cryptographic Hardware and Embedded Systems (CHES '04), pp. 357-370, 2004.
[5]. M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A Concrete Security Treatment of Symmetric Encryption," Proc. 38th Ann. Symp. Foundation of Computer Science (FOCS '97), pp. 394-403, 1997.
[6]. M. Bellare and C. Namprempre, "Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm," J. Cryptology, vol. 21, no. 4, pp. 469-491, 2008.
[7]. B. Alomair and R. Poovendran, "Efficient Authentication for Mobile and Pervasive Computing," Proc. 12th Int'l Conf. Information and Comm. Security (ICICS '10), 2014.