IPHV8I1043X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

SECURITY OF THE CIPHER HASH FUNCTIONS FOR MESSAGE AUTHENTICATION

[#1]PEDDI SINDHUJA, M.Tech Student,
[#2]T.UPENDER, Associate Professor,
Dept of CSE,
MOTHER THERESSA COLLEGE OF ENGINEERING & TECHNOLOGY, KARIMNAGAR, T.S.,INDIA.

ABSTRACT: With today's technology, many applications rely on the existence of 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 of particular interest. In this work, we propose two novel techniques for authenticating short encrypted messages that are directed to meet the requirements of mobile and pervasive applications. More than applications rely on the existence of 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 of particular interest. In this work, to propose two novel techniques for authenticating short encrypted messages that are directed to meet the requirements of mobile and pervasive applications. By taking advantage of the fact that the message to be authenticated must also be encrypted, to propose provably secure authentication codes that are more efficient than any message authentication code in the literature. The key idea behind the proposed techniques is to utilize the security that the encryption algorithm can provide to design more efficient authentication mechanisms, as opposed to using standalone authentication primitives.

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

I.INTRODUCTION

PRESERVING the integrity of messages exchanged over public channels is one of the classic goals in cryptography and the literature is rich with message authentication code (MAC) algorithms that are designed for the sole purpose of preserving message integrity. Based on their security, MACs can be either unconditionally or computationally secure. Unconditionally secure MACs provide message integrity against forgers with unlimited computational power. On the other hand, computationally secure MACs are only secure when forgers have limited computational power. A popular class of unconditionally secure authentication is based on universal hash-function families, pioneered by Carter and Wegman. The study of unconditionally secure message authentication based on universal hash functions has been attracting research attention, both from the design and analysis standpoints. 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 considered impractical in many applications, computationally secure MACs have become the method of choice for most real-life applications. In computationally secure MACs, keys can be used to authenticate an arbitrary number of messages. That is, after agreeing on a key, legitimate userscan exchange an arbitrary number of authenticated messages with the same key. Depending on the main building block used to construct them, computationally secure MACs can be classified into three main categories: block cipher based, cryptographic hash function based, or universal hash-function family based. The security of different MACs has been exhaustively studied. The use of one-way cryptographic hash functions for message authenticatio. The popular example of the use of iterated cryptographic hash functions in the design of message authentication codes is HMAC, which was proposed. The use of universal hash-function families in the style is not restricted to the design of unconditionally secure authentication. Computationally secure MACs based on universal hash functions can be constructed with two rounds of computations. In the first round, the message to be authenticated is compressed using a universal hash function. Then, in the second round, the compressed image is processed with a cryptographic function. Popular examples of computationally secure universal hashing based MACs include, but are not limited to. Indeed, universal hashing based MACs give better performance when compared to block cipher or cryptographic hashing based MACs. In fact, the fastest MACs. Earlier designs used one-time pad encryption to process the compressed image. However, due to the difficulty to manage such on-time keys, recent designs resorted to computationally secure primitives. The main reason behind the performance advantage of universal hashing based MACs is the fact that processing messages block by block using universal hash functions is orders of magnitude faster than processing them block by block using block ciphers or cryptographic hash functions.

The use of one-way cryptographic hash functions for message authentication was introduced by Tsudik. A popular example of the use of iterated cryptographic hash functions in the design of message authentication codes is HMAC, which was proposed by Bellare. HMAC was later adopted as a standard. Another cryptographic hash function based MAC is the MDx-MAC proposed by Preneel and Oorschot. HMAC and two variants of MDx- MAC are specified in the International Organization for Standardization. Bosselaers et al. described how cryptographic hash functions can be carefully coded to take advantage of the structure of the Pentium processor to speed up the authentication process. The use of universal hash-function families in the Carter-Wegman style is not restricted to the design of unconditionally secure authentication. Computationally secure MACs based on universal hash functions can be constructed with two rounds of computations. In the first round, the message to be authenticated is compressed using a universal hash function. Then, in the second round, the compressed image is processed with a cryptographic function. Popular examples of computationally secure universal hashing based MACs include, but are not limited to.Indeed, universal hashing based MACs give better performance when compared to block cipher or cryptographic hashing based MACs. In fact, the fastest MACs in the cryptographic literature are based on universal hashing. The main reason behind the performance advantage of universal hashing based MACs is the fact that processing messages block by block using universal hash functions is orders of magnitude faster than processing them block by block using block ciphers or cryptographic hash functions.

One of the main differences between unconditionally secure MACs based on universal hashing and computationally secure MACs based on universal hashing is the requirement to process the compressed image with a cryptographic primitive in the latter class of MACs. This round of computation is necessary to protect the secret key of the universal hash function. That is, since universal hash functions are not cryptographic functions, the observation of multiple message-image pairs can reveal the value of the hashing key. Since the hashing key is used repeatedly in computationally secure MACs, the exposure of the hashing key will lead to breaking the security of the MAC. Thus, processing the compressed image with a cryptographic primitive is necessary for the security of this class of MACs. This implies that unconditionally secure MACs based on universal hashing are more efficient than computationally secure ones. On the negative side, unconditionally secure universal hashing based MACs are considered impractical in most modern applications, due to the difficulty of managing one-time keys. There are two important observations to make about existing MAC algorithms. First, they are designed independently of any other operations required to be performed on the message to be authenticated. For instance, if the authenticated message must also be encrypted, existing MACs are not designed to utilize the functionality that can 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 most existing MACs are inefficient when the messages to be authenticated are short.

II. RELATEDWORK

The beginning researches on pervasive systems have focused on the contextual data management and context modelling. That is why the contextual data processing layer was highlighted in the initial related work. Researchers have been deeply interested in the optimal arrangement for managing and modelling this layer Thus, the first systems were largely involved the interfacing between the contextual data management and the pervasive applications. The adaptation's concept in these systems has particularly concerned the adaptation to contextual situations. Nevertheless, in these solutions the adaptation strategies are not detailed or they are completely neglected. For example, the main goal of CIS1 architecture [9] is to collect, to model and to provide the contextual information. The SOCAM2 architecture was especially proposed to convert the physical spaces, thus contextual information can be converted into a semantic space and can be shared between the context-aware services. Moreover, the key component in the CoBrA3 architecture is responsible for managing and processing the contextual information while maintaining the contextual model. However, a number of recent architectures regard as a major priority the adaptation stage in such architecture, given with specific adaptation strategies.

III. OVERVIEW OF THE PROPOSED ARCHITECTURE

The RADEM system, which stands for Realtime Adaptation based on Dynamic and Evolutionary Models, comprises three functional phases that roughly constitute the adaptation process. This section provides an overview of these phases and describes the structures of its components. But first it's important to elucidate the motivations and goal settings of the intended architecture.

3.1 Motivations and goals of the proposed architecture

The goal of our work is to build a standards-based architecture that provides flexibility and scalability of

IPHV8I1043X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

pervasive systems in smart environments. There is a need to dynamically create models and enable them to be supported in such environments. For that reason, models used for the user-system interaction should be built with context-awareness capabilities, so that they can properly adapt to the changing context of a moving user. Pervasive systems must adapt the information it provides by implicitly deriving the user's requirements from his context of use, whereas, the context tends to vary at runtime in smart environments. The goal is to enhance the adaptation system's operation while improving models at runtime. Owing to the fact that fixed models cannot handle the high amount of information in such environments, the models should progress and change its structure to better match the user's requirements. Consequently, propose an efficient functioning constructed on the basis of dynamic models to cater to the runtime requirements of each mobile user is the primary challenge of RADEM architecture.

3.2 Functional Description of the RADEM Architecture

The functional description of the proposed architecture, given in figure 1, consists of three dependently functional modules: the knowledge repository module, the current context of use and the adaptation engine that is the main module. The retrieval mechanism is built on a realtime and dynamic user activity modelling. Oftentimes, the user is involved in a variety of activities over the course of his work. These can be routine activities, unexpected activities; they can be also activities that change according to working conditions, etc. In any case, the activity solicits specific information in order to be accomplished. Thus, the models should be built in proportion as runtime evolving of the pervasive system as well as according to available information. The following describes the conceptual model of the architecture contemplated to model the user system interaction at real-time and according to the current context of use.

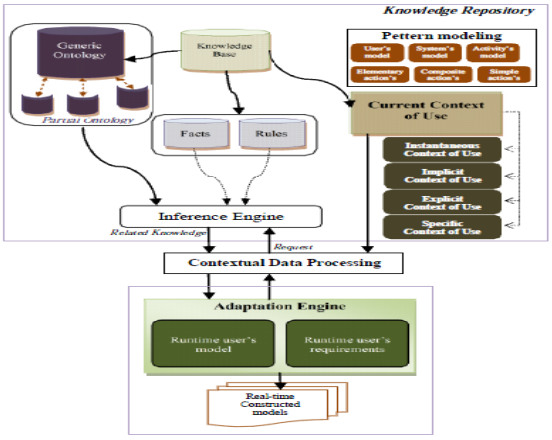

Figure 1. Overall Conceptual Model of RADEM System

IV. NOTATIONS

To use Zp as the usual notation for the finite integer ring with the addition and multiplication operations performed modulo p. to use Z_ p as the usual notation for the multiplicative group modulo p; i.e., Z_ p contains the integers that are relatively prime top. For two strings a and b of the same length, (a _ b) denotes the bitwise exclusive-or (XOR) operation. For any two strings a and b, (ajjb) denotes the concatenation peration.

For a nonempty set S, the notation s $ denotes the operation of selecting an element from the set S uniformly at random and assign . There are two important observations to make about existing MAC algorithms. First, they are designed independently of any other operations required to be performed on the message to be authenticated. For instance, if the authenticated message must also be encrypted, existing MACs are not designed to utilize the functionality that can 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 most existing MACs are inefficient when the messages to be authenticated are short.

To 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, can one do better than simply encrypting the messages using an encryption algorithm and authenticating them using standard MAC algorithm? to answer the question by proposing two new techniques for authenticating short encrypted messages that are more efficient than existing approaches. In the first technique, to 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. The advantages for proposed to More security, using two concepts one is mobile computing and another one is pervasive computing.

4.1authenticating Short Encrypted Messages:

In this module, to describe our first authentication scheme that can be used with any IND-CPA secure encryption algorithm .An important assumption to 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.

4.2 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, respectively. On input an `-bit key k and a message m, algorithm S outputs an N-bit string called the authentication tag, or the MAC of m. On input an `-bit key k, a message m, and an N-bit tag , algorithm V outputs a bit, with 1 standing for accept and 0 for reject. To ask for a basic validity condition, namely that authentic tags are accepted with probability one.) 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 _ 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. Then the oracle computes an authentication tag _ = 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; _). The oracle computes the decision

d = V(k; m; _) and returns it to A.

4.3 Security of the Authenticated Encryption Composition:

In this module, 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.

4.4 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, to give the theorem statement below without a formal proof (interested readers may refer to textbooks in cryptography.

V. CONCLUSION

The new technique for authenticating 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 cipher text. 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. In particular, it has been demonstrated in this paper that authentication tags can be computed with one addition and a one modular multiplication. Given that messages are relatively short, addition and modular multiplication can be performed faster than existing computationally secure MACs in the literature 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. it has been demonstrated in this paper that authentication tags can be computed with one addition and a one modular multiplication. Given that messages are relatively short, addition and modular multiplication can be performed faster than existing computationally secure MACs in the literature 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 a strong pseudorandom permutation 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.

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]. 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.

[3]. J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, "UMAC: Fast and Secure Message Authentication," in Advances in Cryptology– CRYPTO'99, vol. 1666, Lecture Notes in Computer Science. Springer, 1999, pp. 216–233

[4]. 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.

[5]. A Design Proposal of Security Architecture for Medical Body Sensor Networks Shu-Di Bao1, Yuan-Ting Zhang, Lian-Feng Shen

[6]. 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.

[7] Ramón Hervás, , José Bravo. Towards the ubiquitous visualization: Adaptive user-interfaces based
on the Semantic Web. In Interacting with Computers Volume 23, Issue 1, January 2011, Pages 40–56

[8] A. Dey, D. Salber, and G. Abowd: "A Conceptual Framework and a Toolkit for Supporting the Rapid Prototyping of Context-Aware Applications", Special issue on Context-Aware Computing in the Human-Computer Interaction (HCI) Journal, vol. 16 (2-4), pp. 97-166, 2001

[9] J. S. Pascoe, R. J. Loader and V. S. Sunderam. An Election Based Approach to Fault-Tolerant Group MemberShip in Collaborative Envrionment. In Proc. of the 25th IEEE Anniversary Annual International Computer Software and Applications Conference (COMPSAC), pages 196-201, Chicago, II, October 2001. IEEE Press. ISBN: 0-7695-1372-7.

[10] Gu, T., Pung, H.K., Zhang, D.Q.: A service-oriented middleware for building context-aware services. Journal of Network and Computer Applications (2005), Volume: 28, Issue: 1, Publisher: Elsevier, Pages: 1-18

[11] H Chen, T Finin, A Joshi."An Intelligent Broker Architecture for Context-Aware Systems". Adjunct Proceedings of Ubicomp, 2004

[12] Tarek Chaari, Frederique Laforest. Adaptation in Context-Aware Pervasive Information Systems: The SECAS Project. Journal of Pervasive Computing and Communications, Vol. 2, No. 2, June 2006

[13] F. Buttussi, "A user-adaptive and context-aware architecture for mobile and desktop training applications", in Proc. Mobile HCI, 2008

[14] Mahmoud Hussein, Jun Han, and Alan Colman. An Architecture-based Approach to Context-aware Adaptive Software Systems. Technical Report #C3-516_01, Swinburne University of Technology, Australia. January 2011

[15] Daqiang Zhanga, Minyi Guoa, Jingyu Zhoua, Dazhou Kangb, Jiannong Caoc. Context reasoning using extended evidence theory in pervasive computing environments. In Future Generation
Computer Systems. Volume 26, Issue 2, February 2010, Pages 207–216.