IJARES/August 2015/Volume-3/Issue-8/2042-2046 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

A NOVEL APPROACH TOWARDS VERIFICATION OF ENCRYPTED MESSAGE IN SUPPORT OF MOBILE NETWORKS

Chandrashekar Palerla[1], D.Sudheer Reddy[2]

[1]M.Tech Student, Dept of CSE, Arjun College of Technology & Sciences, Hyderabad, T.S, India

[2]Associate Professor, Dept of CSE, Arjun College of Technology & Sciences, Hyderabad, T.S, India

ABSTRACT:

There were important efforts devoted to designing of hardware resourceful implementations those suite small devices. There are quite a lot of message authentication code algorithms in literature that are intended for exclusive purpose of preservation of message reliability. In our work we suggest two new techniques for authentication of short encrypted messages that meet needs of mobile as well as pervasive applications. Proposed techniques make use of security that encryption algorithm can offer to intend more competent authentication mechanisms, as opposed to usage of standalone verification primitives. The innovation of proposed system is to make use of encryption algorithm to distribute a random string and utilize it to attain efficiency of one-time pad authentication without managing impractically long keys.

Keywords: Message authentication code, Short encrypted messages, Encryption algorithm, Verification primitives, Mobile applications.

1. INTRODUCTION:

Reserving of reliability of messages that are exchanged on public channels is one of important goals in cryptography. On basis of security, message authentication code is moreover unconditionally or else computationally secure. In computationally secure message authentication code, keys are used to validate an arbitrary number of

messages. Computationally secure message authentication codes are classified as three main categories such as block cipher basis, universal hash function or else cryptographic hash function basis. Universal hashing-based message authentication code provides improved performance when compared to block cipher or else cryptographic hashing-based message authentication code. Unconditionally secure message authentication code make available message reliability against forgers by limitless computational power [1]. The fundamental concept permitting for unconditional security is that authentication key confirms a restricted number of exchanged messages. While supervision of one-time keys is considered not practical in numerous applications, computationally secure message authentication code has turn out to be choice for the majority of real-life applications. Since universal hash functions are not at all cryptographic, numerous message-image pairs make known value of hashing key. The study of unconditionally secure message authentication on basis of universal hash functions were gained research attention, from design as well as analysis viewpoint. Computationally secure message authentication code on basis of universal hash functions are build by means of two rounds of computations [2][3]. In initial round, message is authenticated is compressed by means of a universal hash function and in second round, compressed image is processed by means of a cryptographic function. Unconditionally secure message authentication code based on universal hashing are more competent than computationally secured. In our work we recommend two new techniques for authentication of short encrypted messages that meet needs of mobile as well as pervasive applications. Proposed system makes use of encryption algorithm to distribute a random string and utilize it to reach effectiveness of one-time pad authentication devoid of managing impractically long keys. By consideration of fact that message to be authenticated should be encrypted, we recommend provably protected authentication codes that are resourceful than any message authentication code.

2. METHODOLOGY:

In the recent times, there is a rising demand for consumption of networks that consist of a collection of small devices. In numerous realistic applications, most important

intention is to converse short messages. There has been small effort in design of special algorithms that are used for designing of message authentication codes that make use of other operations and special properties of such networks. Universal hashing-based message authentication code provides improved performance when compared to block cipher or else cryptographic hashing-based message authentication code. Fastest message authentication codes in cryptographic literature are on basis of universal hashing. The most important reason behind performance benefit of universal hashing-based message authentication code is fact that processing messages by means of universal hash functions is orders of magnitude quicker than processing cryptographic hash functions. One of most important differences among unconditionally secure message authentication code based on universal hashing as well as computationally secure message authentication code based on universal hashing is necessity to process compressed image by means of cryptographic primitive. Since universal hash functions are not at all cryptographic, numerous message-image pairs make known value of hashing key [4]. Processing of compressed image by means of a cryptographic primitive is essential for security. Unconditionally secure message authentication code based on universal hashing are more competent than computationally secured. Unconditionally secure universal hashing-based message authentication codes are considered not practical in most recent applications, because of difficulty of managing one-time keys. We recommend two new techniques for authentication of short encrypted messages that meet needs of mobile as well as pervasive applications. Input output relation of employed encryption operation is recognized as a pseudorandom permutation. The important notion of proposed techniques are to make use of security that the encryption algorithm can offer to intend more competent authentication mechanisms, as opposed to usage of standalone verification primitives.

3. AN OVERVIEW OF PROPOSED SYSTEM:

With the technology in modem days numerous applications rely on existence of small devices that exchanges information and structure communication networks. The

important motive behind our study is usage of general purpose message authentication code algorithm to validate exchanged messages in such systems may not be efficient solution and can cause wastage of available resources to be exact, the security that is offered by encryption algorithm. There has been minute attempt in designing of special algorithms that are used for designing of message authentication codes that make use of other operations and special properties of such networks. Here two new techniques for authentication of short encrypted messages were introduced that meet needs of mobile as well as pervasive applications that are more competent than existing approaches. Proposed techniques make use of security that the encryption algorithm can offer to intend more competent authentication mechanisms, as opposed to usage of standalone verification primitives. By consideration of fact that message to be authenticated should be encrypted, we recommend provably protected authentication codes that are resourceful than any message authentication code. In the initial technique, we make use of the fact that the message that has to be valid is moreover encrypted, by any protected encryption algorithm, to add on short random string in authentication procedure. The novelty of proposed system is to make use of encryption algorithm to distribute a random string and utilize it to reach effectiveness of one-time pad authentication devoid of managing impractically long keys. Another significant benefit of proposed method, particularly for low-power devices, is hardware effectiveness [5]. The hardware necessary to carry out modular multiplication is less than hardware required to carry out complicated cryptographic operations therefore, energy consumption is in turn decreased. In second method, we make extra assumption that make use of encryption algorithm is block cipher-basis to recover computational effectiveness of initial technique. The most important proposal of this approach is that input output relation of employed encryption operation is recognized as a pseudorandom permutation [6].

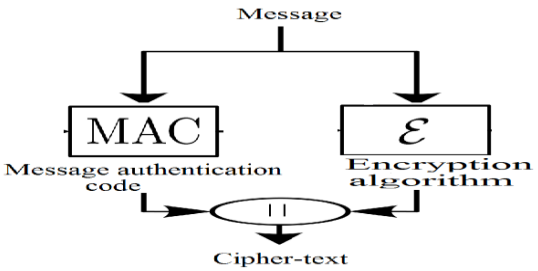

Fig1: overview of generic composing of authenticated encryption system.

4. CONCLUSION:

Unconditionally secure message verification on basis of universal hash functions were gained research attention, from design as well as analysis point of view. In our work we suggest two new techniques for verification of short encrypted messages that meet needs of mobile as well as pervasive applications. By consideration of fact that message to be authenticated have to be encrypted, we suggest provably protected authentication codes that are resourceful than any message authentication code. The important views of projected techniques are to utilize security that the encryption algorithm can offer to intend more competent authentication mechanisms, as opposed to usage of standalone verification primitives. In initial method, we take advantage of the fact that the message that has to be valid is moreover encrypted, by any protected encryption algorithm, to add on short random string utilized in authentication procedure. In second method, we make additional assumption that make use of encryption algorithm is block cipher-basis to recover computational effectiveness of initial method.

REFERENCES

[1] Federal Information Processing Standards (FIPS) Publication 113, Computer Data Authentication, FIPS, 1985.

[2] ISO/IEC 9797-1:1999 Standard, Information Technology – Security Techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms Using a Block Cipher, ISO/IEC, 1999.

[3] M. Dworkin, "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication," 2005.

[4] M. Bellare, J. Kilian, and P. Rogaway, "The Security of the Cipher Block Chaining Message Authentication Code," J. Computer and System Sciences, vol. 61, no. 3, pp. 362-399, 2000.

[5] B. Preneel and P. Van Oorschot, "On the Security of Iterated Message Authentication Codes," IEEE Trans. Information Theory, vol. 45, no. 1, pp. 188-199, Jan. 1999.

[6] G. Tsudik, "Message Authentication with One-Way Hash Functions," ACM SIGCOMM Computer Comm. Rev., vol. 22, no. 5, pp. 29-38, 1992.

Chandrashekar Palerla, Graduated in B.Tech IT from Samskruthi College of Engineering & Technology, Rangareddy (Dt) in 2012.

D.Sudheer Reddy B.Tech Computer Science and Information Technology Graduated in 2005 from Swami Ramanand Thirde Institute of Science &Technology(SRTIST),Nalgonda Dist. He received Masters Degree in M.Tech [CSE] ST.Marrys Group of nstitutions, Dheshmuki, Hayathnagar, R.R. Dist presently he is working as Assistant Professor in CSE Dept. in Arjun College of Technology & Sciences, Hayathnagar, and R.R. Dist Telangana State, India