INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 4, Issue 2 JULY 2015

A FRAMEWORK FOR AUTHENTICATING SHORT ENCRYPTED MESSAGES IN MOBILE AND PERVASIVE COMPUTING

[1]K. NAVEEN KUMAR, [2]G. Dr. S. MAGESH SRIRAMALU

[1]PG Scholar, Dept of IT

naveen9181@gmail.com

[2]Sr. Asst Professor, Dept of IT

magesh.s@ktr.srmuniv.ac.in

Abstract—

Now a day, several applications accept the existence of little devices that may exchange info and kind communication networks. And it's terribly difficult to supply security for such application. During a significant slice of such applications, the confidentiality and integrity of the communicated messages area unit of specific interest. During this work, we tend to propose 2 novel techniques for authenticating short encrypted messages supported Advance encryption crypto logic System that area unit directed to meet the wants of mobile and pervasive applications. The secret writing technique have the prospect of the information misusing thus we tend to add the password primarily based authentication technique. By victimization Advance encryption algorithmic program we tend to area unit authenticating the message that is encrypted and that we area unit up the decipherment speed and authentication accuracy to secure the communication the projected message authentication technique is additional economical than the previous MAC algorithms and therefore the aim of this projected techniques is to utilize the security that the encryption algorithmic program will give to implement additional effective authentication mechanisms, as against victimization standalone authentication primitives. It provides the protection to the information, but its high risk to the sender input file whereas the transmission to the receiver. The methods are going to be evaluated within the real time situation in terms of the networking surroundings. The performances are going to be evaluated in terms of the time quality of the complete method.

Keywords— message authentication code (MAC), mobile computing, radio frequency identification (RFID), Encrypt-and-Authenticate, indistinguishability under chosen plaintext attacks (IND-CPA).

I INTRODUCTION

Conserving the truthfulness of messages traded over open channels is one of the excellent objectives in cryptography also the literature is rich with message authentication Code (MAC) algorithm that are intended for the sole motivation behind Conserving message truthfulness. In light of their security, Macs can be either genuinely or computationally secure. Genuinely secure MACs give message

authentication against counterfeiter with boundless computational force.

On the other hand, computationally secure MACs are just secure at the point when counterfeiters have restricted computational force. We can use the universal hash-function families to the design of unconditionally secure authentication as these are not restricted. Automatically protected MACs relay on universal hash functions can be developed with couple of rounds of computations. In the initial round, the message which we are authenticating is squashed using a universal hash function. Then, in the later round, the squashed image is developed with a cryptographic function (typically a pseudorandom function 1) Popular automatically protected universal hashing-based MACs include, but are not inadequate to.

These days, there is a growing want for the creation of networks which consist of a gathering of little devices. In many useful applications, the key motivation of such devices is to exchange small messages. A sensor network, for instance, can be utilized to scrutinize specific events and show some collected data. In various sensor network applications, shown data consist of small secret measurements. Consider, for example, a sensor network deployed in a battlefield with the motivation of displaying the survival of other sequential activities or moving targets. In such area, the privacy and integrity of displayed events are of significant meaning.

One more application that is becoming gradually more significant is the exploitation of body sensor networks. In such related applications, little sensors can be set in the patient's body to account some crucial signs. Yet again, in some applications the privacy and reliability of such kind of reported messages can be essential.

In general the transmission takes place after encrypting the data by applying the cryptographic process. That was used to improving the data security and the integrity. In the prior work they consider only the single encryption technique and the message authentication code process. Those are not effective when the encrypted data is misused. Hence those not too secure and also there is chance of reducing the integrity level of the data. Our proposed system aims to improve the integrity level of the data while the transmission takes place in terms of cryptographic process. The another important process is that it combines the four important process they are key generation process, double encryption process and the password based authentication process.

II RELATED WORK

Related Fields Pervasive computing represents a major evolutionary step in a line of work dating back to the mid-1970. Two distinct earlier steps in this evolution are distributed systems and mobile computing. Some of the technical problems in pervasive computing correspond to problems already identified and studied earlier in the evolution. In some of those cases, existing solutions apply directly; in other cases, the demands of pervasive computing are sufficiently different that new solutions have to be sought. There are also new problems introduced by pervasive computing that have no obvious mapping to problems studied earlier.

Mobile Computing

The appearance of full-function laptop computers and wireless LANs in the early 1990s led researchers to confront the problems that arise in building a distributed system with mobile clients. The field of mobile computing was thus born. Although many basic principles of distributed system design continued to apply, four key constraints of mobility forced the development of specialized techniques. These constraints are: unpredictable variation in network quality, lowered trust

and robustness of mobile elements, limitations on local resources imposed by weight and size constraints, and concern for battery power consumption. Mobile computing is still a very active and evolving field of research, whose body of knowledge awaits codification in textbooks. The results achieved so far can be grouped into the following broad areas:

• Mobile networking, including Mobile IP, ad hoc protocols, and techniques for improving TCP performance in wireless networks.

• Mobile information access, including disconnected operation, bandwidth-adaptive file access, and selective control of data consistency.

• Support for adaptative applications, including trans coding by proxies and adaptive resource management.

• System-level energy saving techniques, such as energy aware adaptation, variable-speed processor scheduling, and energy-sensitive memory management.

• Location sensitivity, including location sensing and location-aware system behavior.

Pervasive Computing

Earlier in this paper, we characterized a pervasive computing environment as one saturated with computing and communication capability, yet so gracefully integrated with users that it becomes a ‘‘technology that disappears.’’ Since motion is an integral part of everyday life, such a technology must support mobility; otherwise, a user will be acutely aware of the technology by its absence when he moves. Hence, the research agenda of pervasive computing subsumes that of mobile computing, but goes much further.

III PROPOSED WORK

Let N_1be a bound on the length, in bits, of changed messages. That is, messages to be documented are now not than (N_ 1)-bit long. Select p to be AN N-bit long prime integer. (If N is just too tiny to supply the required security level, p is chosen massive enough to satisfy the specified security level.) Select A number ks uniformly randomly from the multiplicative cluster ZZ_ p; ks is that the secret key of the theme. The prime number, p, and the secret key, ks, area unit distributed to legitimate users and can be used for message authentication. Note that the worth of p needn't be secret, solely American state is secret.

Let E be any IND-CPA secure cryptography formula. Let m be a brief messages (N_1 bit or shorter) that's to be transmitted to the supposed receiver in an exceedingly confidential manner (by encrypting it with E). Rather than authenticating the message employing an ancient MAC algorithm, take into account the subsequent procedure. On input a message m, a random nowadays r 2 ZZp is chosen. (We overload m to denote each the binary string representing the message, and the integer illustration of the message as a component of ZZp. a similar applies to ks and r. The distinctions between the two representations are omitted once it's clear from the context.) We assume that integers representing distinct messages are distinct, which might be achieved by fitly encryption messages.

IV METHODOLOGY

In a mobile environment, a number of users act as a network nodes and communicate with one another to acquire location based information and services. In a significant portion of such applications, the confidentiality and integrity of the communicated messages are of particular interest. By taking advantage of the fact that the message to be authenticated must also be encrypted, we propose provably secure authentication codes that are more

efficient than any message authentication code in the literature. Following Figure 1 shows generalize system.

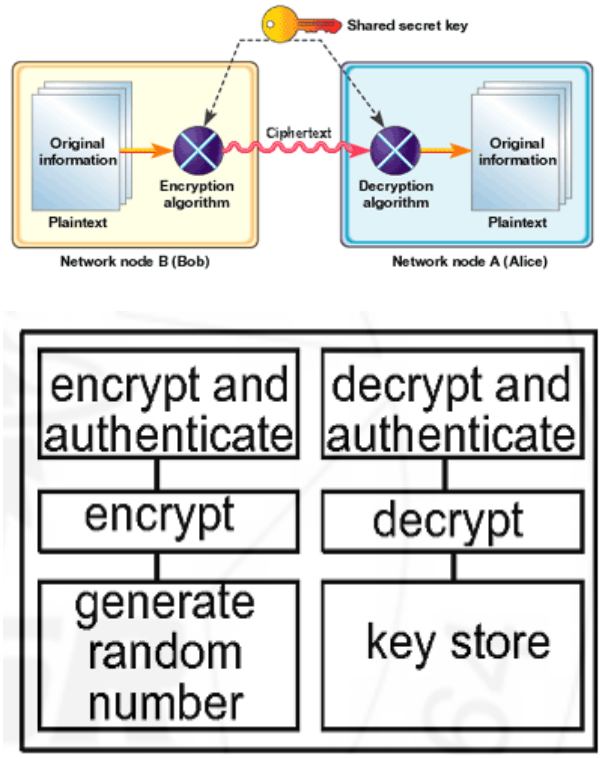


Figure 1: Generalize system.

There will be five modules. 1) Authenticate short messages and encrypt those messages: In this module, first validation plot that might be utilized with any IND-CPA secure encryption calculation. A critical presumption is that messages to be verified are no more than a predefined length. This incorporates applications in which messages are of settled length that is known from the earlier, for example, RFID frameworks in which labels need to validate their identifiers, sensor hubs reporting occasions that have a place with certain area or estimations inside a certain extent.

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 (l) and N describing the length of the shared key and the resulting authentication tags.

Security of the Authenticated Encryption Composition:

The first is integrity of plaintext (INT-PTXT) and 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 will be analyze.

Data Privacy and authenticity

In this section, a message authentication approach that is faster than the existing. The main idea of this approach is that the input output relation of the used encryption operation can be realized as a pseudo random permutation. In what follows, will show how to utilize the pseudo randomness of block ciphers in a novel way to further improve the efficiency of an existing authentication algorithm. In today's reality, numerous applications depend on the presence of little gadgets that can trade data and structure correspondence systems. In a critical segment of such applications, the privacy and respectability of the imparted messages are specifically compelling. To maintain the security and integrity of the communication within the system required following methods.

1. Encryption methods.

2. Authentication methods.

3. Data and security analysis.

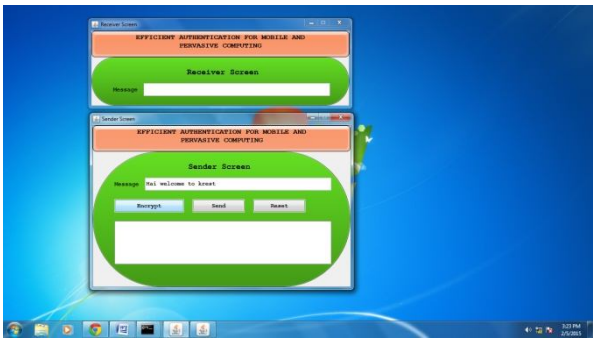
V EXPERIMENTAL RESULTS

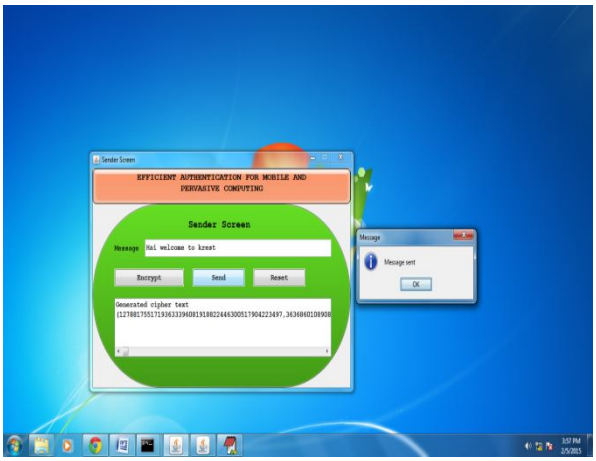
In this application we can send the message from the sender to receiver. Enter the message in the text box and click on **"Encrypt"** button.

Internally IND-CPA Algorithm will take a random number, key and prime number with a message; it will generate a cipher text.

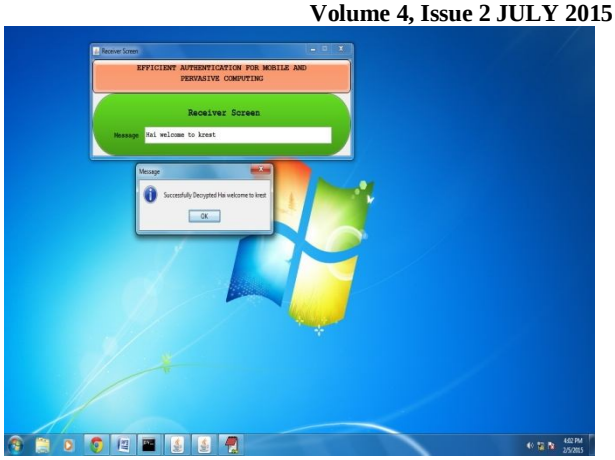
Click on **"Send"** Button. Then it will send the encrypted message to the Receiver

In this application we can send the message from the sender to receiver. Enter the message in the text box and click on **"Encrypt"** button.





At the Receiver end it will be in decrypted mode, the user directly will read that message



CONCLUSION

In this report a new methodology for validating tiny encrypted messages is projected. The truth that the message which is to be validated must need to be encrypted is utilized to provide a arbitrary nonce to the proposed receiver via the cipher text. This permits the design of a validation code those profits from the simplicity of absolutely secure validation with no need to handle one-time keys. Particularly, it has been confirmed in this report that validation tags can be calculated with one calculation and a one modular multiplication. Stated that messages are comparatively short, addition and modular multiplication can be execute quicker than presented computationally secure MACs in the journalism of cryptography. When devices are prepared with block ciphers to encrypt messages, an another method that uses the fact that block ciphers can be modeled as strong pseudorandom permutations is projected to validate messages using a single modular addition. The projected patterns are shown to be orders of magnitude quicker, and consume orders of magnitude less energy than traditional MAC algorithms. Since, they are more appropriate to be utilized in computationally constrained pervasive devices and mobile

REFERENCE

[1] L. Carter and M. Wegman, "Universal Hash Functions," J. Computer and System Sciences, vol. 18, no. 2, pp. 143-154, 1979.

[2] T. Helleseth and T. Johansson, "Universal Hash Functions from Exponential Sums over Finite Fields and Galois Rings," Proc. 16th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '96), pp. 31-44, 1996.

[3] 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.

[4] B. Alomair, A. Clark, and R. Poovendran, "The Power of Primes: Security of Authentication Based on a Universal Hash-Function Family," J. Math. Cryptology, vol. 4, No. 2, 2010.

[5] B. Alomair and R. Poovendran, "E-MACs: Towards More Secure and More Efficient Constructions of Secure Channels," IEEE Trans. Computers, 2012.

[6] D. Bernstein, "The Poly1305-AES Message Authentication Code," Proc. 12th Int'l Conf. Fast Software Encryption (FSE '05), pp. 32-49, 2005.

[7] S. Halevi and H. Krawczyk, "MMH: Software Message Authentication in the Gbit/Second Rates," Proc. Int'l Conf. Fast Software Encryption (FSE '97), pp. 172-189, 1997.

[8] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, "UMAC: Fast and Secure Message Authentication," Proc. 19th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '99), pp. 216-233, 1999.

[9] I. Akyildiz, W. Su, Y. ankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks, vol. 38, no. 4, pp. 393-422, 2002. .