International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Survey Paper on Pervasive Computing for Mobile Security

Kulashree Joshi[1], Sulochana Sonkamble[2]

[1]Rajarshi Shahu College of Engineering and Research, JSPM Narhe, Technical Campus, Pune-India

[2]Rajarshi Shahu College of Engineering and Research, JSPM Narhe, Technical Campus, Pune-India

Abstract: ***Now a day, many applications rely on the existence of small devices that can exchange information and form communication networks. And it is very challenging to provide security for such application. 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 based on Advance Encryption cryptographic System that are directed to meet the requirements of mobile and pervasive applications. The encryption technique have the chance of the data misusing hence we add the password based authentication technique. By using Advance Encryption algorithm we are authenticating the message which is encrypted and we are improving the decryption speed and authentication accuracy to secure the communication the proposed message authentication technique is more efficient than the previous MAC algorithms and the aim of this 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. It provides the security to the data. However it has high risk to the sender input data while the transmission to the receiver. The process will be evaluated in the real time scenario in terms of the networking environment. The performance will be evaluated in terms of the time complexity of the whole process.***

Keywords: gadgets, authentication code, communication systems, encrypt-and-authenticate, pervasive computing.

1. 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 function1). Popular automatically protected universal hashing-based MACs include, but are not inadequate to, [6], [7], [8].

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 [9], [10].

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 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 [11].

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.

In this paper our contribution is literature survey, our proposed system, comparison of existing and proposed system in brief, also conclusion and future scope of system.

2. Literature Survey

W Thamba Meshach [13] proposed validated key swap over scheme, namely Mobile Cloud Key Exchange (MCKE), which focuses at well-organized security-aware arrangement of scientific applications? Their system has been planned

relay on the mostly-used Internet Key Exchange (IKE) technique and randomness-reuse methodology. Both simulation results as well as theoretical analyses have confirmed that, differentiate with the IKE system, our MCKE technique has considerably enhanced the effectiveness by spectacularly minimizing time required and computation load with the similar kind of security.

In this report [5], Basel Alomair and Radha Poovendran examine the encrypt-and-authenticate generic work of protected channels. They launched E-MACs, a new symmetric-key cryptographic primeval that can be utilized in the creation of E&A compositions. By considering benefits of the E&A structure, the utilization of E-MACs is exposed to progress the effectiveness and precautions of the authentication process.

Moreover, because the message to be validated is encrypted, hash functions based E-MACs can considered without the need to be relevant cryptographic process on the squashed image, since this can be substitute by procedure performed by the encryption algorithm. Additionally, by attaching an arbitrary string at the end of the original message, couple of security methodologies have been pull off. First, the random string is utilized to encrypt the authentication tag so that the privacy of the original text is not negotiable by its tag. Further, the arbitrary string can be utilized to randomize the private key of the utilized E-MAC so that it will be safe and sound beside key-recovery attacks.

In this report [10], B. Alomair, A. Clark, J. Cuellar implemented a framework which is relay on binary hypothesis testing for model, examining and estimating statistical source secrecy in wireless sensor networks. They have initiated the concept of interval in discriminate capability to model source location confidentiality. They illustrate that the current methodologies for designing statistically unspecified systems bring in association in real intervals while duplicate intervals are uncorrelated. By denoting the difficulty of identifying source information to the statistical problem of binary hypothesis testing with nuisance parameters, they show why previous learning were not able to perceive the source of data outflow that was explained in this paper. Finally, they projected a alteration to presented solutions to develop their ambiguity to words correspondence tests.

In this paper [14], a productive confirmation plan is proposed which is suitable for low-power cell phones. It utilizes an elliptic-curve cryptosystem based trust delegation methodology to produce an assignment pass code for portable station confirmation, and it can successfully protect all known assaults to portable systems including the refusal of administration assault. Additionally, the versatile station just needs to get one message and send one message to validate itself to a guest's area register; furthermore the plan just obliges solitary elliptic-curve scalar point duplication on a cell phone. In this manner, this plan appreciates both computational effectiveness and correspondence productivity as contrasted with known versatile validation plans.

3. Problem Definition

Presently, many applications rely on the existence of small devices that can exchange information and form communication networks. And it is very challenging to provide security for such application. In a significant portion of such applications, the confidentiality and integrity of the communicated messages are of particular interest. Therefore we proposed an application which increases the security of the application. We proposed an algorithm which increases the security and performance of the MAC algorithm.

4. 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.

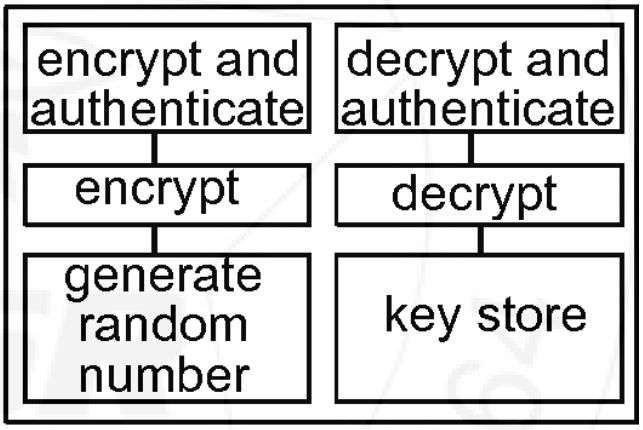

Figure 1: Generalize system.

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.

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

3) **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.

4) **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.

5. Results

In existing system 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. Since the random strings used for different operations are independent, the authentication algorithm can benefit from the simplicity of unconditional secure authentication to allow for faster and more efficient authentication. Use of encryption algorithm is block cipher based to further improve the computational efficiency of the technique. The driving motive behind investigation is that using a general purpose MAC algorithm to authenticate exchanged messages in such systems might not be the most efficient solution and can lead to waste of resources already available, namely, the security that is provided by the encryption algorithm.

In the proposed system have to deliberate the subsequent cryptographic methods that will be realistic in the input that input should be the short message that was called as the Multi-Security technique. Those encryption methods are the data encryption standard and the advanced encryption standard. Then it delivers the password based authentication method in the double encryption technique's cipher text. For significant the order of the operation they have to apply the avalanche effect but to make the method to secure the keys will be transmitted to the user through the mail of the personal contact of the user.

In proposed system we have less time complexity, less computational cost, effective integrity, more secure while the transmission, more confidential.

6. 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.

7. Future Scope

In the future have to investigate about the further implementation of encryption techniques to enhance the process with the less time complexity and the high integrity in the process. And have to improve the whole performance by implementing the other process oriented to the security of the data in the mobile computing process. And also need to investigate about the other possible ways to improving the data security other than the cryptogrpahic techniques as the additional process to the data security of the data.

References

[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.
[10] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Toward a Statistical Framework for Source Anonymity in Sensor Networks," IEEE Trans. Mobile Computing, vol. 12, no. 2, pp. 248-260, doi : 10.1109 / TMC.2011.267, Feb. 2013.
[11] C. Tan, H. Wang, S. Zhong, and Q. Li, "Body Sensor Network Security: An Identity-Based Cryptography Approach," Proc. First ACM Conf. Wireless Network Security, pp. 148-153, 2008
[12] S. Sarma, S. Weis, and D. Engels, "RFID Systems and Security and Privacy Implications," Proc. Fourth Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '02), pp. 1-19, 2003.
[13] W Thamba Meshach, "Secured and Efficient Authentication Scheme for Mobile Cloud", International Journal of Innovations in Engineering and Technology (IJIET).
[14] Caimu Tang, Dapeng Oliver Wu, "An Efficient Mobile Authentication Scheme for Wireless Network ", Journal IEEE Transactions on wireless communication, volume 7 issue 4April 2008.

Author Profile

Ms. Kulashree Joshi pursuing Masters of Engineering in Computer Science at Rajarshi Shahu College of Engineering and Research, JSPM NTC Pune-India. She obtained Bachelor of Engineering in Information Technology Science in 2009 at BVPCOEW, Pune-India. Her area of interest is Mobile Computing, Wireless Networks, and Network Security.

Mrs. Sulochana Sonkamble is HOD of Computer Science Department at Rajarshi Shahu College of Engineering and Research, JSPM NTC Pune-India. She obtained Bachelor of Engineering, Masters of Engg. And PhD in Computer Science Shri Guru Gobind Singhji Institute of Engineering and Technology, Swami Ramand Tirth Marathwada University, Vishnupuri, Nanded-India.