ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Improving Efficiency and Security by Authentication of Short Encrypted Messages in Mobiles and Pervasive Computing Applications

Seepana Sridhara Rao
M.Tech,
Department of CSE,
Sarada Institute of Science Technology & Management, Srikakulam.

Mula.Sudhakar
Assistant Professor,
Department of CSE,
Sarada Institute of Science Technology & Management, Srikakulam.

Abstract:

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. In this paper, an efficient key generation and key transfer protocol has been proposed where KGC can broadcast groupkey information to all group members in a secure way. Hence, only authorized group members will beable to retrieve the secret key and unauthorized members cannot retrieve the secret key. Another concept is encryption and decryption of transferring message by using reverse binary xor encryption algorithm. The generation of authentication code for message we are using hash function. By implementing those concepts we can improve efficiency and more security of transferring message.

Keywords:

Small Gadgets, authentication code, communication systems, encrypt-and-authenticate, pervasive computing.

Introduction:

Pervasive computing is a concept in software engineering and computer science where computing is made to appear everywhere and anywhere. In contrast to desktop computing, ubiquitous computing can occur using any device, in any location, and in any format. A user interacts with the computer, which can exist in many different forms, including laptop computers, tablets and terminals in everyday objects such as a fridge or a pair of glasses. The underlying technologies to support ubiquitous computing include Internet, advanced middleware, operating system, mobile code, sensors, microprocessors, new I/O and user interfaces, networks, mobile protocols, location and positioning and new materials.

This paradigm is also described as ambient intelligence, ambient media or 'everyware'. Each term emphasizes slightly different aspects. When primarily concerning the objects involved, it is also known as physical computing, the Internet of Things, haptic computing, and 'things that think'. Rather than propose a single definition for ubiquitous computing and for these related terms, a taxonomy of properties for ubiquitous computing has been proposed, from which different kinds or flavors of ubiquitous systems and applications can be described.

Pervasive computing touches on a wide range of research topics, including distributed computing, mobile computing, location computing, mobile networking, context-aware computing, sensor networks, human-computer interaction, and artificial intelligence.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

At their core, all models of Pervasive computing share a vision of small, inexpensive, robust networked processing devices, distributed at all scales throughout everyday life and generally turned to distinctly common-place ends. For example, a domestic ubiquitous computing environment might interconnect lighting and environmental controls with personal biometric monitors woven into clothing so that illumination and heating conditions in a room might be modulated, continuously and imperceptibly. Another common scenario posits refrigerators "aware" of their suitably tagged contents, able to both plan a variety of menus from the food actually on hand, and warn users of stale or spoiled food.Pervasive computing presents challenges across computer science: in systems design and engineering, in systems modelling, and in user interface design. Contemporary human-computer interaction models, whether command-line, menu-driven, or GUI-based, are inappropriate and inadequate to the ubiquitous case. This suggests that the "natural" interaction paradigm appropriate to a fully robust ubiquitous computing has yet to emerge - although there is also recognition in the field that in many ways we are already living in a ubicomp world (see also the main article on Natural User Interface). Contemporary devices that lend some support to this latter idea include mobile phones, digital audio players, radio-frequency identification tags, GPS, and interactive whiteboards.

Pervasive or Ubiquitous computing may be seen to consist of many layers, each with their own roles, which together form a single system:

Layer 1: task management layer

•Monitors user task, context and index.
•Map user's task to need for the services in the environment.
•To manage complex dependencies.

Layer 2: environment management layer

•To monitor a resource and its capabilities.
•To map service need, user level states of specific capabilities.

Layer 3: environment layer

•To monitor a relevant resource.
•To manage reliability of the resources.

Such pervasive computing and mobile computing devices rely on short messages for which MAC can be computed more efficiently. Based on their security MACs can either be unconditionally secure or computationally secure. MACs provide message integrity against the forgers with unlimited computational power. On the other hand, computationally secure MACs are only secure when forgers have limited computational power.

Related Work:

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Existing System:

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. (For instance, UMAC, the fastest reported message authentication code in the cryptographic literature, has undergone large algorithmic changes to increase its speed on short messages).

Disadvantages:

1.Existing MACs are not designed to utilize the functionality that can be provided by the underlying encryption algorithm.

2.Most existing MACs are designed for the general computer communication systems, independently of the properties that messages can possess.

Proposed System:

In this section we are mainly proposed message authentication approach that is faster than the existing approach. Before performing message authentication the key generation center will generate secret key and sent to public channel members for message encryption and decryption. After generating secret key the channel member or group member will send message to specified member of the group.

Before sending message the group member will encrypt message and generate signature for that message. After completion of encryption and signature generation the group member will send message and signature to specified member of the group.

The specified group member will retrieve the cipher message and signature. After retrieving the group member again generate signature and compare both signature are equal the message is authenticated or not equal it will block the message. The following concepts are specifying generation of secret key, encryption and decryption of message and generate signature for encrypted message.

Advantages:

1.More security, using two concepts one is mobile computing and another one is pervasive computing.

2.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, without the difficulty to manage one-time keys. In the second technique, we make the extra assumption that the used encryption algorithm is block cipher based to further improve the computational efficiency of the first technique.

Users Registration:

This module explains the process computation of key and users registration. After registering users the KGC will generate id for individual users Ui and sent to users. During registration process each user will choose a random secret value Siand send to KGC.Once user registration process is completed, KGC assigns a permanent secret id, denoted by Pi for each Member Ui in the group.

Key generation and distribution to group member:

In this module each user will request for group key, the KGC will randomly generate secret. After generating secret key the KGC will send that key to each user with in secure manner. By providing security for secret key the KGC will generate a message and send to all users. The KGC will now generation of message and its value is calculated by using following formula.

Message=(P1 ® S1) * (P2® S2) * ……..* (Pn ® Sn) + secret key.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

After generating message the KGC will sent the message to all group members. The group member will retrieve the message get secret key from the message. Upon receiving the message M, the each member in the groups will generate the keyin the following manner.

Secret key = M mod (Pi ® Si) for all i.

After completion of secret key each user will encrypt the message by using following algorithm.

Reverse Binary xor Encryption Algorithm:

We will be presenting the steps of the encryptionalgorithm of the reverse binary xor Algorithm. The followingsteps are as shown in Figure 1:

1. Input secret key and transferring message to encryption process.
2. Get each character from the message and convert into ASCii values.
3.After converting ascii values each value xor with key until the length of message is completed.
4.The completion of xor operation each ascii value can converted into binary format.
5.Reverse previous binary data until completion length of message.
6.After reversing binary data that data can be perform once complement.
7.The previous complement data convert into ascii format.
8.Divide each ascii value by secret key and get remainder and coefficient until completion of length of message.
9.Each character of remainder and coefficient become one point and those points send to specified group member.

Before sending the cipher data to specified group member the user will generate signature for encrypted message by using MD5 algorithm. After generating signature the user will send cipher message and signature to specified group member. The specified group member will retrieve the cipher message and signature and again will generate signature for cipher message. The group member will compare both signatures are equal the message is authenticated otherwise the message will corrupt and block the message. If the message is authenticated then specified group member will retrieve cipher message and get the original message by performing decryption process of reverse binary xor encryption algorithm. The Decryption process of Reverse binary xor encryption algorithm as follows.

1.Retrieve the point from the sender group member.
2.Get the single ascii value from the point by using following formula.
Asciival= quotient *secretkey + remainder.
3.The previous asciival will be convert into binary format.
4.The previous binary data can be perform the once complement.
5.After performing once complement that binary data will be reverse until the completion message length.
6.After reversing that binary data will convert into ascii format.
7.The previous ascii values will be xor with secret key until completion of message length.
After performing xor operation that ascii values can be converted characters get the original 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.

References:

[1] Basel Alomair & Radha Poovendran, Efficient Authentication for Mobile and Pervasive Computing, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 3, MARCH 2014.

[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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[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 MessageAuthentication 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.

Author's Details:

Seepana Sridhara Rao, is student in M.Tech(CSE) in Sarada Institute of Science Technology and Management, Srikakulam. He has received his B.Tech(C.S.E) from SRI SIVANI COLLEGE OF ENGINEERING CHILAKAPALEM, SRIKAKULAM his interesting areas are Network security & Software Engineering.

Mula.Sudhakar, is working as a Asst.professor in Sarada Institute of Science, Technology And Management, Srikakulam, Andhra Pradesh. He received his M.Tech (SE) from Sarada Institute of Science, Technology And Management, Srikakulam. JNTU Kakinada Andhra Pradesh. His research areas include Cloud Computing,Dataminig,Network Security.