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

Novel Methods for Authenticating Short Encrypted Messages in Mobile and Pervasive Computing Applications

G.Sushmitha
M.Tech Student,
Department of CSE,
Vijaya Krishna Institute of Technology and Sciences,
Hyderabad.

H.M.Nagaraju
Associate professor,
Department of CSE,
Vijaya Krishna Institute of Technology and Sciences,
Hyderabad.

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.

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.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:

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

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.

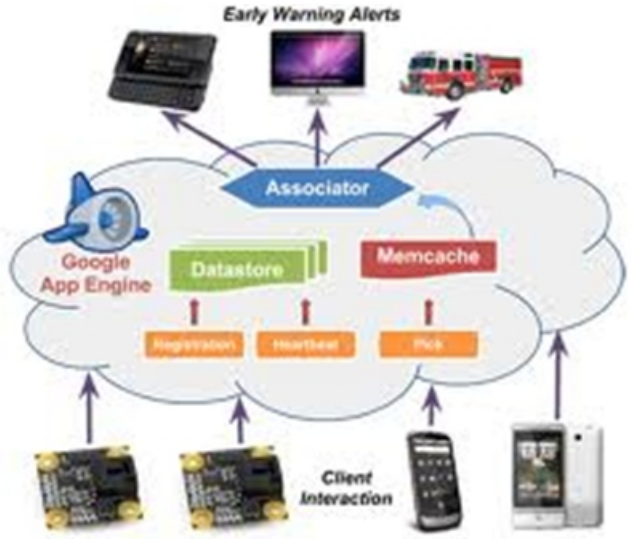
First, the random string is utilized to encrypt the authentication tag so that the privacy of the original text is not negotiable by its tag. Further, the arbitrary string can be utilized to randomize the private key of the utilized E-MAC so that it will be safe and sound beside key-recovery attacks.

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

Architecture Diagram:



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.

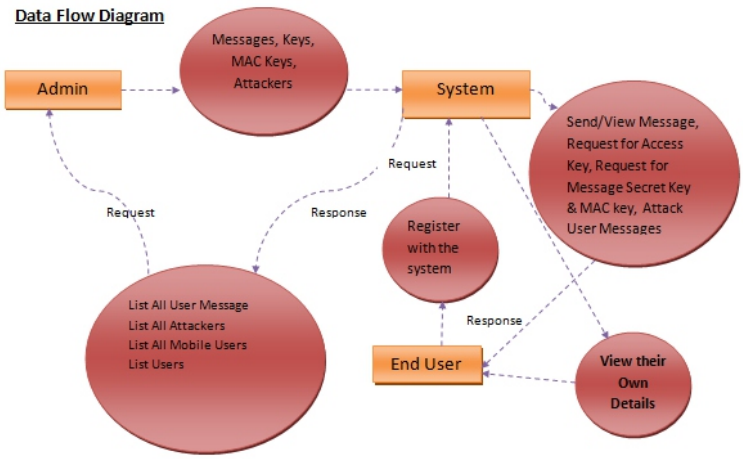
Proposed System:

We 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? We answer the question by proposing two new techniques for authenticating short encrypted messages that are more efficient than existing approaches. In the first technique, we 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.

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.



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

IMPLEMENTATION

• Admin

In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations like list all user messages, list users, list all attackers, view mobile users and logout.
List all user messagesIn this module, the admin can view list of all the user messages. If the admin click on the list all user messages button then the server will display all list of all messages with their tags message ID, message to, message from, Mobile no, E-mail, title Name, Key used, MAC key, Date & time.

List users:

In this module, the Admin can view list of all users. Here all registered users are stored with the details such as user Image, User name, DOB, E-Mail, Mobile, Location and Secret Key.

List all attackers:

In this module, the admin can view all attackers list. The attacker details are stores with the details such as Message ID, title name, key used, MAC key, Date & time, message. The admin can also view the mobile users with their tags user name, password, Email.

User:

In this module, there are n numbers of users present. User should register to a particular group before doing any operations. After registration successful he has to login by using authorized user name and password. After logged in he will do some operations such as view my details, send message, view messages, request for user access key, request for message SK and MAC key, attack user messages and logout. If user clicks on my details button, then the server will give response to the user with their tags such as user Image, User name, DOB, E-mail, Mobile and Location.

Send message:

In this module, the user can send messages to another user. To do this, user has to enter the access key provided by the admin and submit, then user has to enter the receiver name, title name and message, the message will be encrypted and a MAC value is generated based on the message content. This data will be stored in the data base.

View messages :

The user can view the all messages sent then the server will give response to the user with their tags such as message ID, message to, message from, Mobile no, E-mail, title Name, Key used, MAC key, Date & time, message and validity. To view the message content first user has to get the message secret key and message MAC key then user can download message.

Check message validity:

In this module, the user can check the message validity. To check the message validity the user has to click on the button check message validity and has to enter the Message ID, title name and message MAC key. Then message will display weather it is valid on not.

• Android test book:

In this module, the user can install this application in his android mobile, after installation to use this application user should register with the valid information. After successful registration user should login by the valid user name and password. After logged in user can perform operations like view users, view message pseudo random and MAC key, request key.The admin can also use this application in the android phone; the admin should login by the valid user name and password. After logged in the admin will perform the some operations like view all users, view all attackers, logout.

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.

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

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.

[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.