INTERNATIONAL JOURNAL OF MERGING TECHNOLOGY AND ADVANCED RESEARCH IN COMPUTING

IJMTARC – VOLUME – V – ISSUE – 20 , DEC , 2017

ISSN: 2320-1363

EFFICIENT MESSAGE AUTHENTICATION APPROACH IN MOBILE NETWORKS

[1] P.Sravani
M.Tech(CSE)
Sree Dattha Institute Of Engineering & Sciences, Hyd

[2] B.Kumara Swamy
Assistant professor
Computer Science Department
Sree Dattha Institute Of Engineering & Sciences, Hyd

Abstract:

With today's technology, many applications rely on the existence of small devices that can form communication networks and exchange information in the form of messages. The confidentiality and integrity of the communicated messages are of particular interest in a significant portion of such applications. Encryption is a key factor in the authentication of messages. Hence we propose provably secure authentication codes that are more efficient than any message authentication code in the literature. Generally standalone authentication primitives are used for message authentication. The key idea behind the proposed techniques is to design more efficient authentication codes by utilizing the security that the encryption algorithm can provide.

1. INTRODUCTION

• Obeservant of the integrity of messages exchanged over public channels is the classic goals in cryptography and the literature is rich with message authentication code (MAC) algorithms that are designed for the sole purpose of preserving message integrity. Based on their security, MACs can be either unconditionally or computationally secure. Computationally secure MACs are only secure when forgeters have limited computational power.

• A popular class of unconditionally secure authentication is based on universal hash-function families, pioneered by Carter and Wegman. That is, after agreeing on a key, legitimate users can exchange an arbitrary number of authenticated messages with the same key. Depending on building block used to construct them, computationally secure MACs can be classified into three main tpes: block cipher based, cryptographic hash function based, or universal hash-function family based.

• CBC-MAC is one of the most known block cipher based MACs, specified in the Federal Information Processing Standards publication 113 and the International Organization for Standardization ISO/IEC 9797-1. CMAC, a modified version of CBC-MAC, is presented in the NIST special publication 800-38B, which was based on the OMAC of. Other block cipher based MACs include, but are not limited to, XOR-MAC and PMAC. The security of different MACs has been exhaustively studied.

• A popular example of the use of iterated cryptographic hash functions in the design of message authentication codes is HMAC, which was proposed by Bellare. HMAC was later adopted as a standard. Another cryptographic hash function based MAC is the MDx-MAC proposed by Preneel and Oorschot. HMAC and two variants of MDx- MAC are specified in the International Organization for Standardization ISO/IEC 9797-2. Bosselaers et al. described how cryptographic hash functions can be carefully coded to take advantage of the structure of the Pentium processor to speed up the authentication process.

• Is compressed using a universal hash function. Then, in the second round, the compressed image is processed with a cryptographic function (typically a pseudorandom function1). Computationally secure universal hashing based MACs but are not limited to.

• One of the main differences between unconditionally secure MACs is depence on universal hashing and computationally secure MACs based on universal hashing is the requirement to process the compressed image with a cryptographic primitive in the latter class of MACs. This round of computation is necessary to protect the secret key of the universal hash function.

• Reveal the value of the hashing key. Thus, processing the compressed image with a cryptographic primitive is necessary for the security of this class of MACs. There are two important observations to make about existing MAC algorithms. One can find that existing MACs are invalid when the messages to be authenticated are short.

• Now-a-days, however, there is an increasing demand for the deployment of networks consisting of a collection of small devices. In many practical applications, the main purpose of such devices is to communicate short messages. A sensor network, for example, can be deployed to monitor certain events and report some collected data. In many sensor network applications, reported data consist of short confidential measurements. Consider, for instance, a sensor network deployed in a battlefield with the purpose of reporting the existence of moving targets or other temporal activities. In such applications, the confidentiality and integrity of reported events are of critical importance.

• In another application, consider the increasingly spreading deployment of radio frequency identification (RFID) systems. In such systems, RFID tags need to identify themselves to authorized RFID readers in an authenticated way that also preserves their privacy. In such scenarios, RFID tags usually encrypt their identity, which is typically a short string (for example, tags unique identifiers are 64-bit long in the EPC Class-1 Generation-2 standard [39]), to protect their privacy. Since the RFID reader must also authenticate the identity of the RFID tag, RFID tags must be equipped with a message authentication mechanism.

• Another application that is becoming increasingly important is the deployment of body sensor networks. In such applications, small sensors can be embedded in the patient's body to report some vital signs. Again, in some applications the confidentiality and integrity of such reported messages can be important.

• There have been significant efforts devoted to the design of hardware efficient implementations that suite such small devices. For instance, hardware efficient implementations of block ciphers have been proposed. However, there has been little or no effort in the design of special algorithms that can be used for the design of message authentication codes that can utilize other operations and the special properties of such networks. In this paper, we provide the first such work.

II. EXISTING SYSTEM

There are two surves 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, to utilize the functionality that can be provided by the underlying encryption algorithm. Second, MACs are designed for computer communication systems, properties that messages can hold. For example, one can find that most existing MACs are inefficient when the messages to be authenticated are short.

Disadvantages

• Existing MACs are not designed to avail the functionality can be secured by the underlying encryption algorithm.

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

III. PROPOSED SYSTEM

Propose if there is an application in which messages that need to be transformed 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? Proposing two new techniques for authenticating encrypted messages that are productive than existing approaches.

Advantages

- security using two concepts are 1)mobile computing and 2) pervasive computing.

- The strings used for operations are self-sufficiency, the authentication algorithm can gain from simplicity of unconditional secure authentication to allow efficient authentication, without the difficulty to manage one-time keys. In second technique, we assume the used encryption algorithm is block cipher based on betterment of the computational efficiency of the first technique.

III. IMPLEMENTATION

3.1 Admin

In this module, the Admin has to login by using valid user name and password. After login successful we can perform operations as given below:

3.2 List all user messages

The admin can view list of all the user messages. If the admin press on the list all user messages button then the server will display all list of all messages with their tags like message ID, message to, message od, Mobile number, E-mail, title Name, Key used, MAC key, Date & time.

3.3 List users

The Admin can see 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.

3.4 List all attackers

The admin can check all attackers list. The attacker details 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.

3.5 User

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. Similarly as admin got logged in user also has the operations for login like 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.

3.6 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.

3.8 View messages

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

3.9 Check message validity

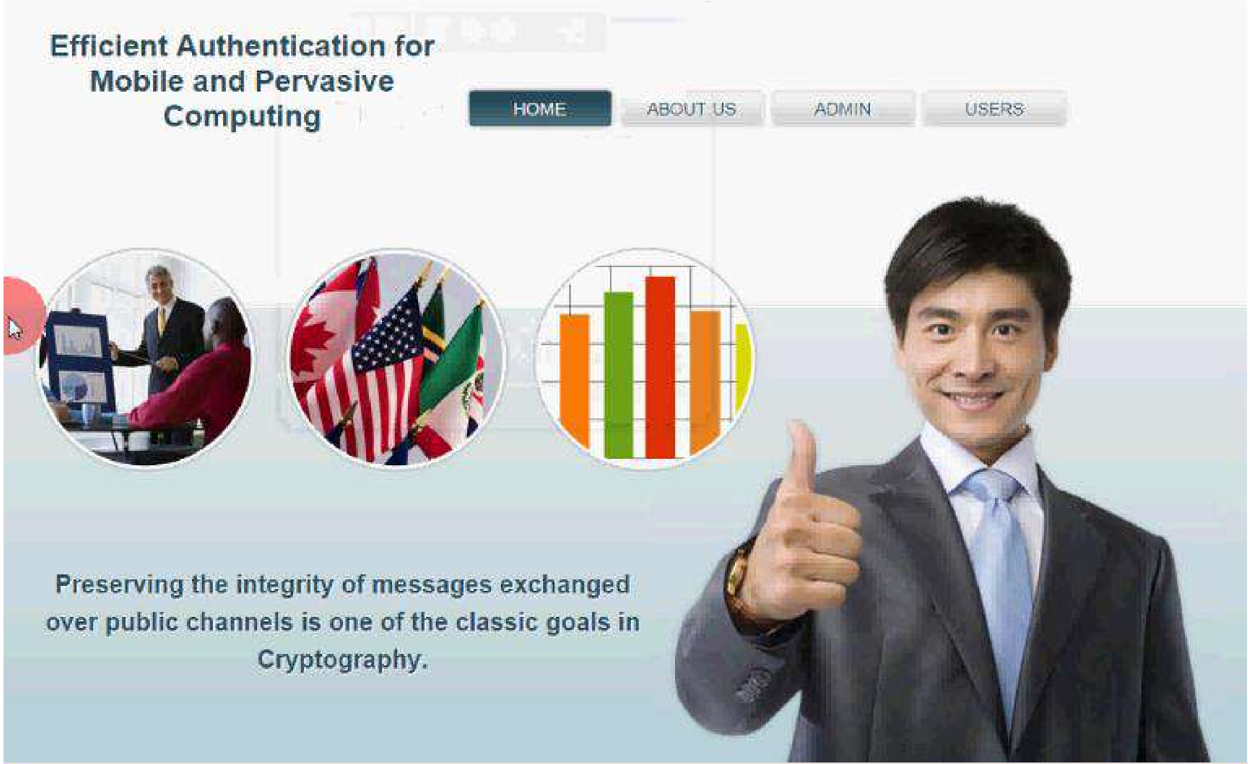
The user can find the message validity. To check the validity of a message user need to click on the button to check message validity and has to enter the Message ID, title name and message MAC key. Then message will display weather it is valid on not.

3.10 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 login user can perform operations like view users, view message pseudo random and MAC key, request key.

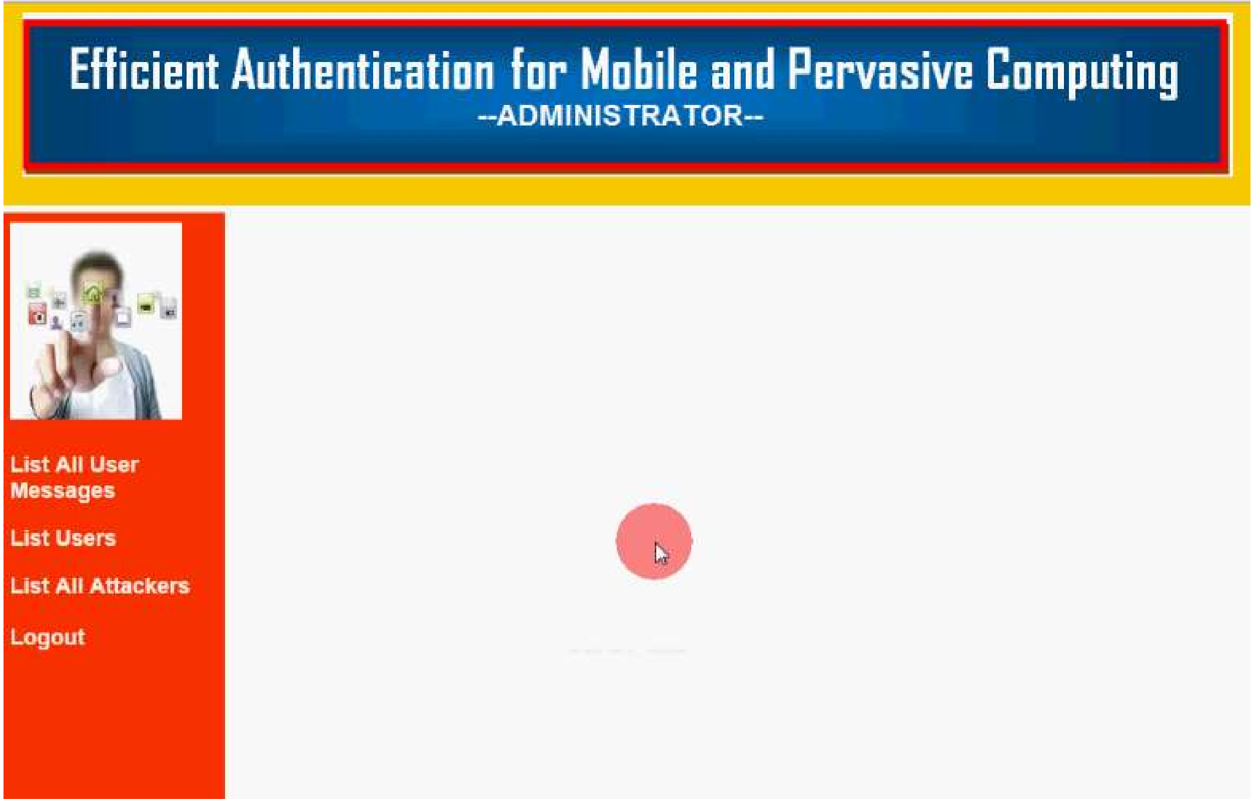
The admin can use this application in android phone, the admin should login by valid user name and pswd. After logged in the admin will perform the some operations like view all users, view all attackers, logout.

IV. SCREENSHOTS



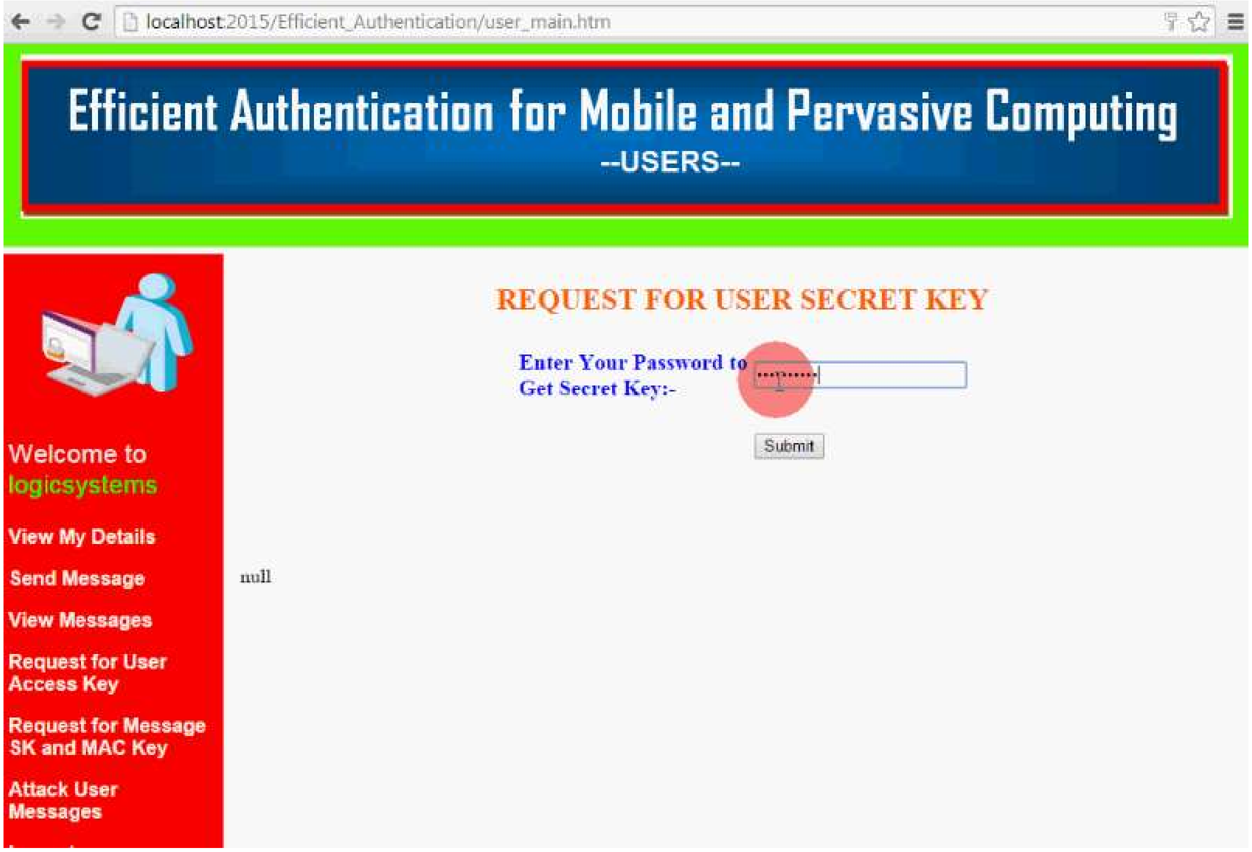
Efficient Authentication for Mobile and Pervasive Computing

Preserving the integrity of messages exchanged over public channels is one of the classic goals in Cryptography.



Efficient Authentication for Mobile and Pervasive Computing

--ADMINISTRATOR--



localhost:2015/Efficient_Authentication/user_main.htm

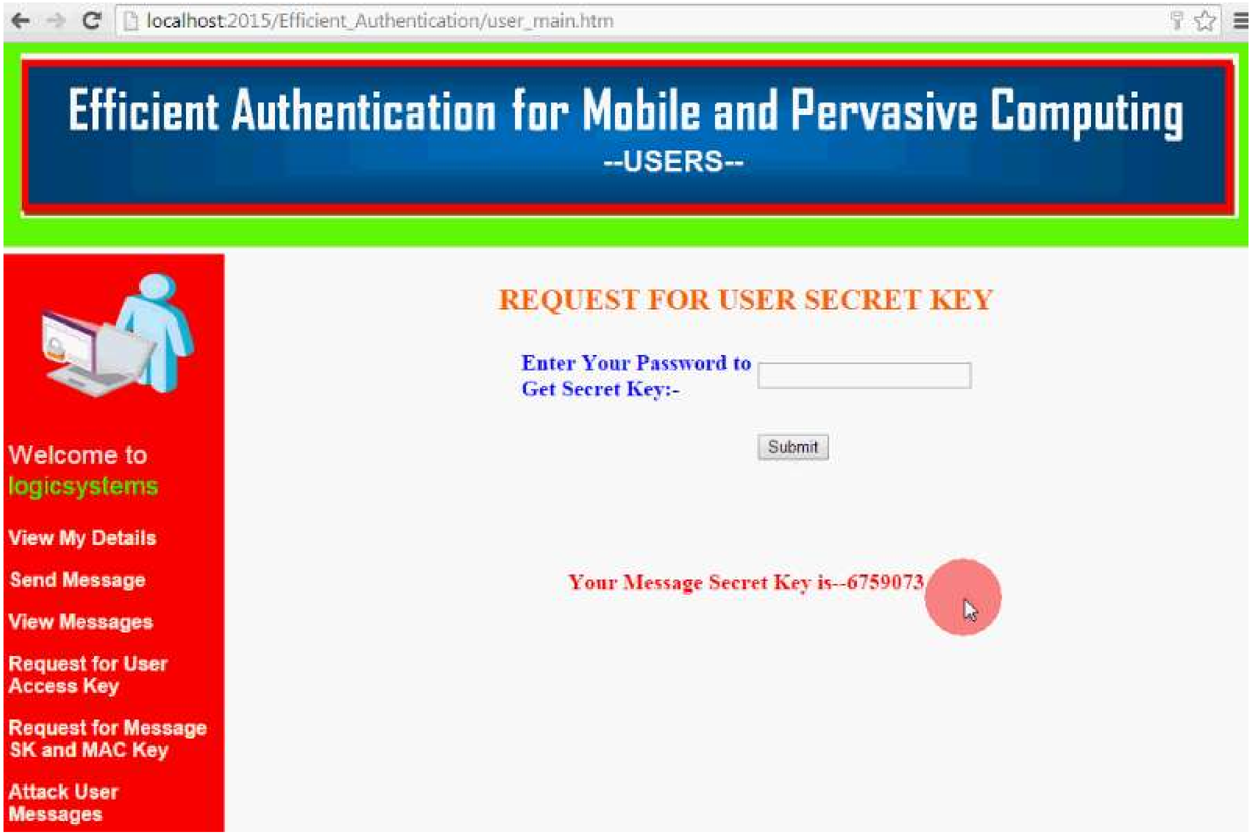
Efficient Authentication for Mobile and Pervasive Computing

--USERS--

REQUEST FOR USER SECRET KEY

Enter Your Password to Get Secret Key:- ••••••••

null



localhost:2015/Efficient_Authentication/user_main.htm
Welcome to
logicsystems
View My Details
Send Message
View Messages
Request for User Access Key
Request for Message SK and MAC Key
Attack User Messages
Submit

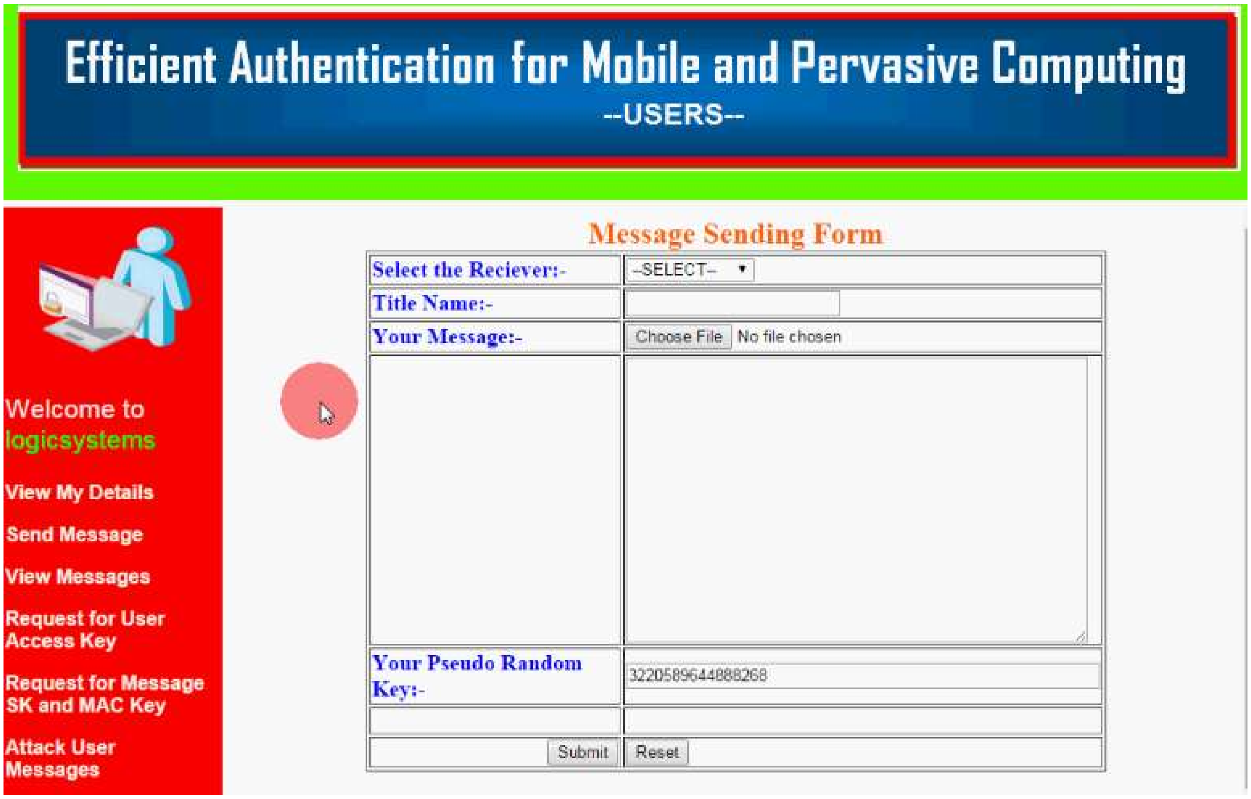
Efficient Authentication for Mobile and Pervasive Computing

--USERS--

REQUEST FOR USER SECRET KEY

Enter Your Password to Get Secret Key:-

Your Message Secret Key is--6759073

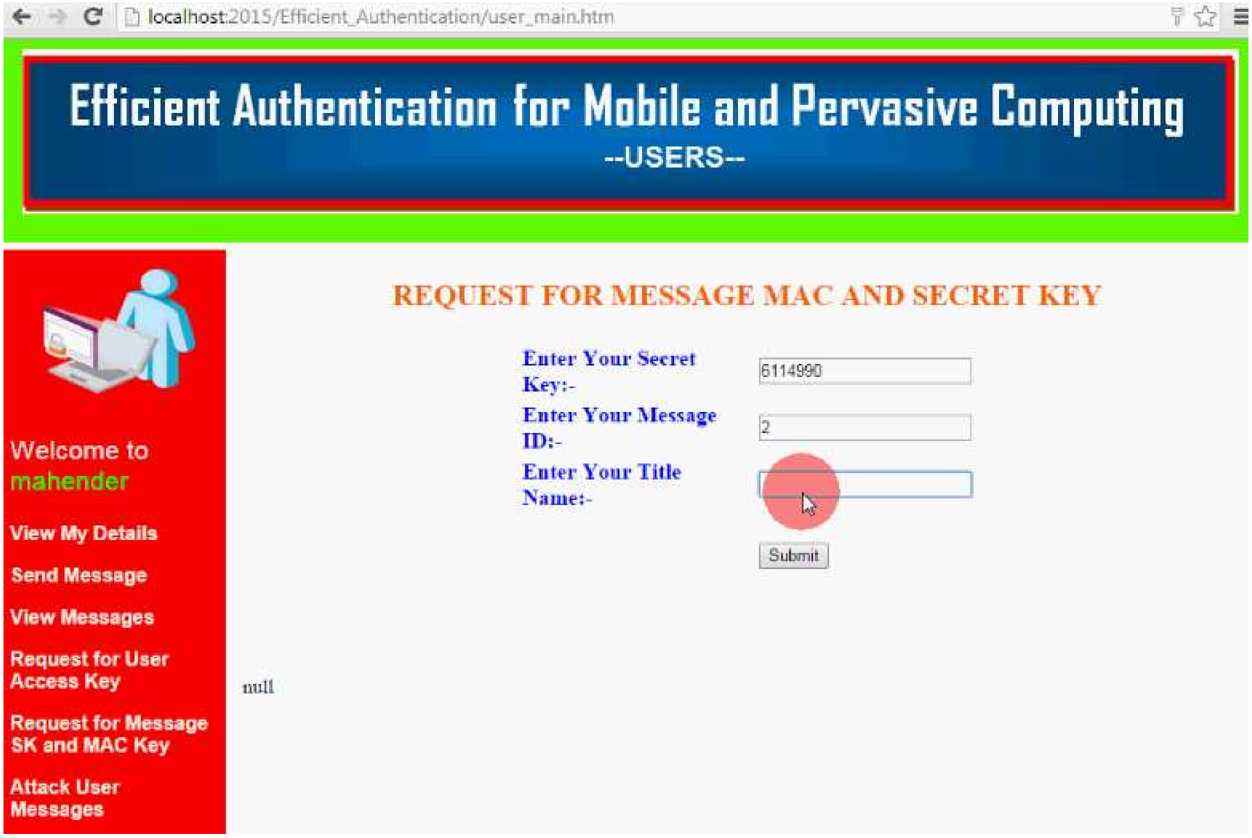


Efficient Authentication for Mobile and Pervasive Computing

--USERS--

Message Sending Form

Select the Reciever:-	--SELECT-- ▾
Title Name:-	
Your Message:-	Choose File No file chosen
Your Pseudo Random Key:-	3220589644888268
Submit	Reset



localhost:2015/Efficient_Authentication/user_main.htm

Efficient Authentication for Mobile and Pervasive Computing

--USERS--

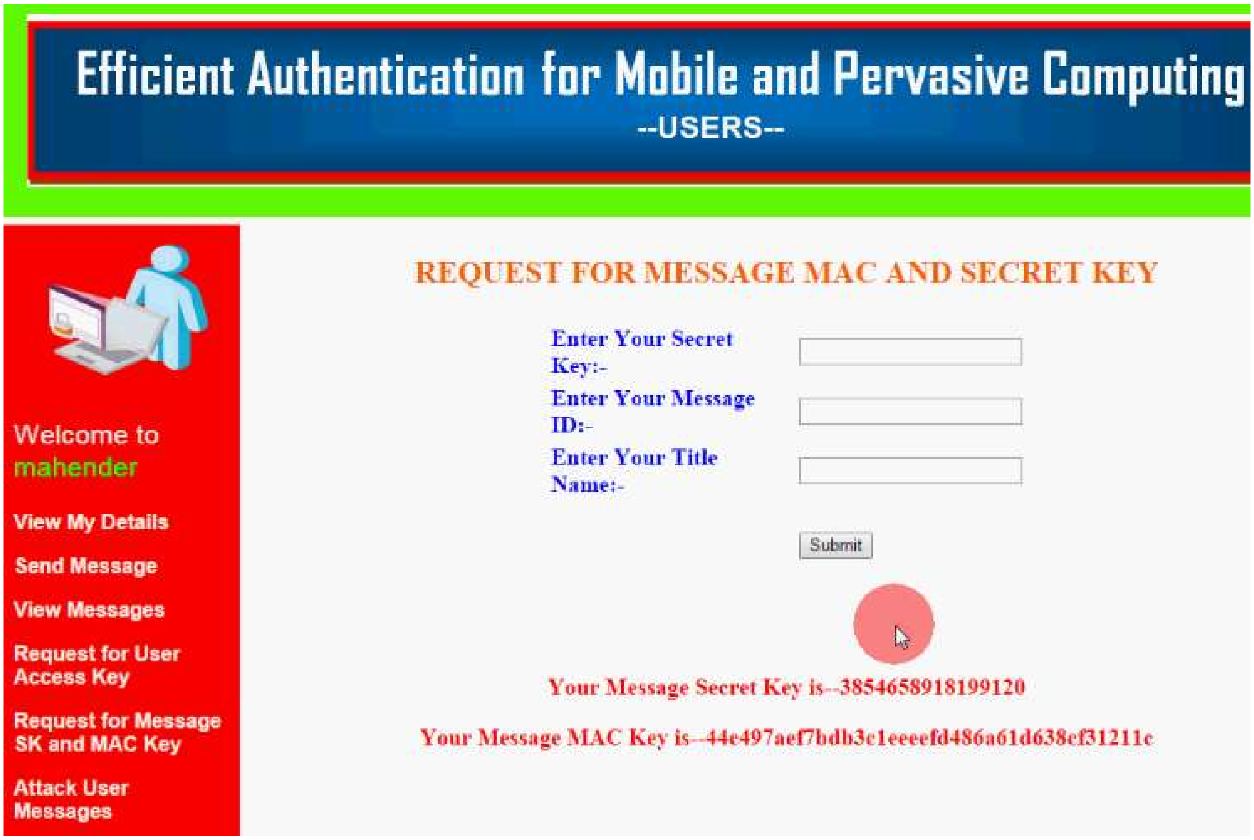
REQUEST FOR MESSAGE MAC AND SECRET KEY

Enter Your Secret Key:-	6114990
Enter Your Message ID:-	2
Enter Your Title Name:-	

Welcome to mahender

View My Details
Send Message
View Messages
Request for User Access Key
Request for Message SK and MAC Key
Attack User Messages

null


Efficient Authentication for Mobile and Pervasive Computing
--USERS--
Welcome to
mahender
View My Details
Send Message
View Messages
Request for User Access Key
Request for Message SK and MAC Key
Attack User Messages
Submit

REQUEST FOR MESSAGE MAC AND SECRET KEY

Enter Your Secret Key:-

Enter Your Message ID:-

Enter Your Title Name:-

Your Message Secret Key is--3854658918199120

Your Message MAC Key is--44e497aef7bdb3c1eeeefd486a61d638cf31211c

V. CONCLUSION

The fact is the message to be authenticated also to be encrypted is used to deliver a random convictor to the intended receiver via the cipher text. This allowed the design of an authentication code that benefit from the simplicity of unconditionally secure authentication without the need to manage one-time keys. It has been demonstrated in paper that authentication tags can be computed and a one modular multiplication. Messages are secured with secret key and MAC key. We can access the messages through mobiles also for the individuals. Therefore, they are more suitable to be used in computationally constrained mobile and pervasiv1e devices.

REFERENCES

[1] J. Carter and M. Wegman, “Universal classes of hash functions,” in Proceedings of the ninth annual ACM symposium on Theory of computing–STOC’77. ACM, 1977, pp. 106–112.

[2] M. Wegman and J. Carter, “New classes and applications of hash functions,” in 20th Annual Symposium on Foundations of Computer Science–FOCS’79. IEEE, 1979, pp. 175–182.

[3] L. Carter and M. Wegman, “Universal hash functions,” Journal of Computer and System Sciences, vol. 18, no. 2, pp. 143–154, 1979.

[4] M. Wegman and L. Carter, “New hash functions and their use in au-thentication and set equality,” Journal of Computer and System Sciences, vol. 22, no. 3, pp. 265–279, 1981.

[5] J. Bierbrauer, “A2-codes from universal hash classes,” in Advances in Cryptology–EUROCRYPT’95, vol. 921, Lecture Notes in Computer Science. Springer, 1995, pp. 311–318.

[6] M. Atici and D. Stinson, “Universal Hashing and Multiple Authentica-tion,” in Advances in Cryptology–CRYPTO’96, vol. 96, Lecture Notes in Computer Science. Springer, 1996, pp. 16–30.

[7] T. Helleseth and T. Johansson, “Universal hash functions from exponen-tial sums over finite fields and Galois rings,” in Advances in cryptology– CRYPTO’96, vol. 1109, Lecture Notes in Computer Science. Springer, 1996, pp. 31–44.

[8] V. Shoup, “On fast and provably secure message authentication based on universal hashing,” in Advances in Cryptology–CRYPTO’96, vol. 1109, Lecture Notes in Computer Science. Springer, 1996, pp. 313–328.

[9] J. Bierbrauer, “Universal hashing and geometric codes,” Designs, Codes and Cryptography, vol. 11, no. 3, pp. 207–221, 1997.

[10] B. Alomair, A. Clark, and R. Poovendran, “The Power of Primes: Security of Authentication Based on a Universal Hash-Function Family,” Journal of Mathematical Cryptology, vol. 4, no. 2, 2010.

[11] B. Alomair and R. Poovendran, “E-MACs: Towards More Secure and More Efficient Constructions of Secure Channels,” in the 13th International Conference on Information Security and Cryptology – ICISC’10. Springer, 2010.

[12] FIPS 113, “Computer Data Authentication,” Federal Information Pro-cessing Standards Publication, 113, 1985.

[13] ISO/IEC 9797-1, “Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher,” 1999.

[14] M. Dworkin, “Recommendation for block cipher modes of operation: The CMAC mode for authentication,” 2005.

[15] T. Iwata and K. Kurosawa, “omac: One-key cbc mac,” in Fast Software Encryption–FSE’03, vol. 2887, Lecture notes in computer science. Springer, 2003, pp. 129–153.