Better Authentication Methods for Mobile Computing

Prof. Avinash Ingole
Assistant Professor
Department of Computer Engineering
BVCOE, Lavale

Salaskar Onkar
Department of Computer Engineering
Bharati Vidyapeeth, lavale

Saurabh S. Patil
Department of Computer Engineering
Bharati Vidyapeeth, lavale

Abstract

Today's many applications rely on small devices that can interact with each other through communication network. In this project we are proposing two new methods for authenticating encrypted message that are directed to assemble the requirements of mobile application. In this applications, the integrity and confidentiality of communicated messages are required. To getting benefit of that fact that the messages to be authenticated must also be encrypted, we propose provably methods for safe authentication codes that are more efficient than any message authentication code. The key idea behind the proposed techniques is to exert the security that the encryption algorithm can provide to design more efficient authentication mechanisms, as opposed to using single authentication primitives.

Keywords- Authentication, unconditional security, computational security, universal hash-function families, pervasive computing

I. INTRODUCTION

Cryptography is the art as well as science of secret writing of information and makes them non-readable. Techniques used to achieve cryptography are substitution techniques, transposition techniques, RSA, DES, and AES. One of the main goals is in cryptography using this cryptography integrity of message that can be exchanged over public channel and the literature is rich with message authentication code (MAC) algorithms. That is designed for the sole purpose of preserving message integrity. Based on their security, message authentication codes can be either unconditionally or computationally secure. Computationally secure MACs are only secure when forgers have limited computational power, On the other hand, UN-conditionally secure MACs provide message integrity against forgers with unlimited computational power. computationally secure MACs are only secure when forgers have limited computational power, in this work, we are proposing two new techniques for authenticating short encrypted messages. In the first technique, we utilize the fact that the message to be authenticated is also encrypted by the technique of MAC 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, without the difficulty to manage one-time keys. The driving motive behind our 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 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. Block Cipher break plain text messages into fixed blocks and encrypt each block with some key size (Fixed). Block cipher is basic building block for providing data security. In block cipher rather than encrypting one bit at a time, block of bits is encrypted at one go.

II. SURVEY OF PROPOSED SYSTEM

We represent the following research question: if there is an application in which messages that need to be interchanged 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 message authentication code algorithm? We answer the question we are proposing two new techniques for authenticating short encrypted messages that are more useful 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 blend a short random string to be used in the authentication process.

III. MODULES

A. Authenticating Short Encrypted Messages

In this module, we find our first authentication scheme that can be used with any in-distinguish ability under chosen plaintext attacks (IND-CPA) secure encryption algorithm this application include message are of fixed length that is known a priori, such as RFID systems that is radio frequency identification system in which tags need to authenticate their identifiers, here sensor nodes are used for reporting events that belong to certain domain or measurements within a certain range, etc. The novelty scheme is to utilize the encryption algorithm to deliver a random string and use it to reach the simplicity and efficiency of one-time pad authentication without the need to manage impractically long keys. A crucial assumption that messages to be authenticated are no longer than a predefined length.

B. Security Model

A message authentication scheme consists of a signing algorithm P and a verifying algorithm Q. The signing algorithm might be probabilistic, while the verifying one is usually not. Associated with the scheme are parameters and N describing the length of the shared key and the resulting authentication tag, respectively. On input an `-bit key k and a message m, algorithm P outputs an N-bit string called the authentication tag, or the MAC of m. On input an `-bit key k, a message m, and an N-bit tag, algorithm Q outputs a bit, with 1 standing for accept and 0 for reject. We ask for a basic validity condition, namely that authentic tags are accepted with probability one.) for a random but hidden choice of k. A can query P to generate a tag for a plaintext of its choice and ask the verifier Q to verify that is a valid tag for the plaintext.

C. Data Privacy

Remember that two sections of information are transmitted to the intended receiver (the cipher text and the authentication tag), both of which are functions of the private plaintext message. Now, when it comes to the authentication tag, observe that then once r serves as a one-time key (similar to the role r plays in the construction of Section). The formal analysis that the authentication tag does not compromise message privacy is the same as the one provided. The cipher text of equation, on the other hand, is a standard CBC encryption and its security is well-studied; thus, we give the theorem statement below without a formal proof (interested readers may refer to textbooks in cryptography.)

D. Security of the Authenticated Encryption Composition

In this module, we defined two notions of integrity and efficiency for authenticated encryption systems: the first is integrity of plaintext (INT-PTXT) and the second is integrity of cipher text (INT-CTXT). Combined with encryption algorithms that provide in-distinguish ability under chosen plaintext attacks (IND-CPA), for constructing generic compositions is analyzed by different methods of security. Note that our construction is an instance of the Encrypt-and-Authenticate (E&A) generic composition since the plaintext message goes to the encryption algorithm as an input, and the same plaintext message goes to the authentication algorithm as an input.

IV. CONCLUSION AND FUTURE WORK

In this work, we are used two algorithms first is Message authentication code algorithm (MAC). Second is in-distinguish ability under chosen plaintext attacks (IND-CPA). And new technique for authenticating short encrypted messages is proposed. The fact that the message to be authenticated must also be encrypted is used to deliver a random nonce to the intended receiver via the cipher text This allowed the design of an authentication code that benefits from the simplicity of unconditionally secure authentication without the need to manage one-time keys.

V. LITERATURE SURVEY

A. Drawback of Message authentication code

A better encrypted, authentic, and digitally signed information can be difficult to access even for an unauthorized user at a grand time of decision-making. The network or the computer system can be attacked and rendered non-functional by an attacker.

B. Advantage of Message Authentication Code

- Confidentiality − Encryption technique can care of the information and communication from unauthorized users and access of information.
- Authentication − The MAC and digital signatures can protect information against forgeries and spoofing
- Data Integrity − The hash functions of cryptography are playing crucial role in assuring the users about the data integrity.
- Non-repudiation − The digital signature provides the non-repudiation service to care of against the argue that may emerge due to denial of passing message by the sender.

ACKNOWLEDGEMENT

I would like to take this opportunity to thank my internal guide Avinash Ingole, Assistant professor of Computer Engineering Department, BVCOEL for giving me all the help and guidance I needed. I am really grateful to them for their kind support. Their valuable suggestions were very helpful.

REFERENCES

[1] 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.
[2] IEEE TRANSACTIONS ON MOBILE COMPUTING VOL:13 NO:3 YEAR 2014 Efficient Authentication for Mobile and Pervasive Computing Basel Alomair, Member, IEEE and Radha Poovendran, Senior Member, IEEE.
[3] E. B. Kavun and T. Yalcin, "A Lightweight Implementation of Keccak Hash Function for Radio-Frequency Identification Applications, " in Workshop on RFID Security"RFIDSec"10, 2010.