Efficient message authentication for pervasive computing

Publication History
Received: 23 January 2015
Accepted: 3 March 2015
Published: 20 April 2015

Citation
Sivakumar C, Prabaharan G. Efficient message authentication for pervasive computing. Discovery, 2015, 30(135), 370-376
Efficient Message Authentication for Pervasive Computing

C. Sivakumar  
Department of Computer Science and Engineering  
Adhiparasakthi engineering college  
Melmaruvathur, India  
Email: c.sivakumar89@gmail.com

G. Prabaharan  
Assistant professor  
Department of Computer Science and Engineering  
Adhiparasakthi engineering college  
Melmaruvathur, India  
Email: c.sivakumar89@gmail.com

can be either unconditionally or computationally secure. Unconditionally secure MACs provide message integrity against forgers with unlimited computational power. On the other hand, computationally secure MACs are only secure when forgers have limited computational power.

Nowadays, 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.

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 suit such small devices. For instance, hardware efficient
implementations of block ciphers have been proposed. Implementations of hardware efficient cryptographic hash functions have also 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.

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

ORGANIZATION: The rest of the paper is organized as follows. In Section 2 list the notations and discuss some preliminaries. In Section 3 describe the first authentication technique assuming messages do not exceed a maximum length, discuss its performance advantages over existing techniques, and prove its security. In Section 4 propose a modification to the scheme of Section 3 that provides a stronger notion of integrity. In Section 5 describe the second technique assuming the encryption is block cipher based, discuss its performance, and prove its security. In Section 6 describe conclude the paper.

II. PRELIMINARIES AND NOTATIONS
A. INDISTINGUISHABILITY UNDER CHOSEN PLAIN TEXT ATTACKS (IND-CPA)

An important security notion for encryption algorithms that will be used in this paper is indistinguishability under chosen plaintext attacks (IND-CPA). Let \( A \) be an adversary who is given access oracle to an encryption algorithm, \( E \), and can ask the oracle to encrypt a polynomial number of messages to get their corresponding cipher texts. The encryption algorithm is said to be IND-CPA secure if the adversary, after calling the encryption oracle a polynomial number of times, is given a cipher text corresponding to one of two plaintext messages of her choice cannot determine the plaintext corresponding to the given cipher text with an advantage significantly higher than \( 1/2 \). Formally stated, let \( \text{Adv}_{\text{ind-CPA}} \) be the adversary’s advantage of determining the plaintext corresponding to the given ciphertext. Then, \( E \) is said to be IND-CPA secure if

\[
\text{Adv}_{\text{ind-CPA}}(A) = 1/2 + \text{negl}(N). \tag{1}
\]

Where \( N \) is a security parameter, typically the length of the secret key. Note that IND IND-CPA security implies that the encryption algorithm must be probabilistic. That is, encrypting the same message twice yields different cipher texts. To see that, let the adversary call the encryption oracle on a message \( m_1 \) and receiving its cipher text \( c_1 \). The adversary now chooses two messages, \( m_1 \) and \( m_2 \), ask the encryption oracle to encrypt them and receives the cipher text corresponding to one of them. If the encryption is deterministic, the adversary can determine, with high confidence, to which plaintext the cipher text corresponds by comparing it to \( c_1 \).

B. BLOCK CIPHERS

Block cipher is a basic encryption standard for cryptography techniques. It shares a key both private and public. Block cipher used for encrypting with pseudo-random permutations in this pervasive authentication systems.

C. ADVANCED ENCRYPTION STANDARD (AES)

AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. AES operates on a 4x4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field \([4]\). The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called
Message will be authenticated and also be encrypted. The key idea behind these systems is to utilize the security that the encryption algorithm with pseudo random permutations can provide to design more efficient authentication mechanisms than any existing authentication schemes. IND-CPA combined with encryption algorithm to provide more secure encryption scheme. Encryption with pseudo random permutations generates the random string for that message. Random string for that particular message consider as a key for decrypting a message. IND-CPA and pseudo random permutations combined with encryption algorithm to provide more secure communication between sender and receiver. Concatenation combines the result of encryption message and authentication to produce the cipher text. Cipher text send to the recipient from sender by use of communication networks. In receiver side decrypting the cipher text by use of random string of that message. Random string also send to the recipient in an encrypted format. Decrypting the random string of that message and use it for view a original message. Otherwise use a wrong key for decrypting a message it always fails. Random string avoids the long key difficulties. And also one time key is not suitable for some applications. These propose system gives more authentications for pervasive system.

III. AUTHENTICATING SHORT ENCRYPTED MESSAGES

In this section, describe first authentication scheme that can be used with any IND-CPA secure encryption algorithm. An important assumption we make is that messages to be authenticated are no longer than a predefined length. This includes applications in which messages are of fixed length that is known a priori, such as RFID systems in which tags need to authenticate their identifiers, sensor nodes reporting events that belong to certain domain or measurements within a certain range, etc. The novelty of the proposed 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. DATA PRIVACY

The privacy of the proposed compositions is provably secure assuming the underlying encryption algorithm provides indistinguishability under chosenplaintexttext attacks (IND-CPA). Consider an adversary, B, who is given oracle access to the encryption algorithm, E. The adversary calls the encryption oracle on a polynomial numberof messages of her choice and records the corresponding cipher texts. The

---

**Figure 1. System Architecture for Pervasive Authentication System**

Figure 1 shows the system architecture diagram for pervasive authentication system. It has two new novel techniques for authenticate exchange information over pervasive computing.
adversary then chooses two equal-length messages, \( m_0 \) and \( m_1 \), and gives them to the encryption oracle. The oracle draws a bit \( b \) uniformly at random, encrypts \( m_b \), and gives the adversary the resulting ciphertext. The adversary is allowed to perform additional calls to the encryption oracle and eventually outputs a bit, \( b_0 \). Define the adversary’s advantage of breaking the IND-CPA security of the encryption algorithm, \( E \), as her probability of successfully guessing the correct bit (equivalently knowing to which plaintext the ciphertext corresponds); that is,

\[
\text{Adv}_{E}^{\text{ind-cpa}}(B) = \Pr[b'=b_0]
\]  

As stated in equation (1), \( E \) provides IND-CPA if the adversary has a negligible advantage of guessing the right bit over an adversary choosing a bit uniformly at random.

### B. DATA AUTHENTICITY

Now proceed with the main theorem formalizing the adversary’s advantage of successful forgery against the proposed scheme. As before, let \( E \) denotes the proposed authenticated encryption composition of Section A and let \( \text{Adv}_{\text{auth}}^{u}(A) \) denotes adversary’s \( A \) advantage of successful forgery against \( E \).

### C. SECURITY OF THE AUTHENTICATED ENCRYPTION COMPOSITION

Bellare and Namprempre defined two notions of the integrity for the authenticated encryption systems: the first one is the integrity of plain text (INT-PTXT) and the second is integrity of ciphertext (INT-CTXT). Combined with encryption algorithms that provide indistinguishability under chosen plaintext attacks (IND-CPA), the security of different methods for constructing generic compositions is analyzed. 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 [6]. Figure 2 illustrates the differences between the three methods for generically composing an authenticated encryption system. It was shown in that E&A compositions do not generally provide IND-CPA. This is mainly because there exist secure MAC algorithms that leak information about the authenticated message. Obviously, if such a MAC is used to compose an E&A system, then the authenticated encryption does not provide IND-CPA. The proposed authenticated encryption scheme is at least as private as the underlying encryption algorithm. Since the encryption algorithm is IND-CPA secure, the resulting composition provides IND-CPA.

Another result of is that E&A compositions do not provide INT-CTXT. However, the authors also point out that the notion of INT-PTXT is the more natural requirement, while the main purpose of introducing the stronger notion of INT-CTXT is for the security relations is because there exist secure encryption algorithms with the derived in. The reason why E&A compositions do not generally provide INT-CTXT property that the ciphertext can be modified without changing its decryption. Obviously, if such an encryption algorithm is combined with our MAC to compose an E&A composition, only INT-PTXT is achieved (since the tag in our scheme is a function of plaintext). A sufficient condition, however, for the proposed composition to provide INT-CTXT is to use a one-to-one encryption algorithm (most practical encryption algorithms are permutations, i.e., one-to-one).

Figure 2. A schematic of the three generic compositions; (a) Encrypt-and-Authenticate (E&A), (b) Encrypt-then-Authenticate (EtA), and (c) Authenticate-then-Encrypt (AtE).

### IV. ENCRYPTING WITH PSEUDORANDOM PERMUTATIONS (BLOCK CIPHERS)

In this section describe a message authentication approach that is faster than the one described in previous sections. The main idea of this approach is that the input-output relation of the used encryption operation can be realized as a pseudorandom permutation [5]. Utilize the pseudo randomness of block ciphers in a novel way to further improve the efficiency of the authentication of section III.

### A. MESSAGE ENCRYPTION

Let \( m \) be a short message that is to be transmitted to the intended receiver in a confidential manner. For every message to be transmitted, a random nonce is chosen. Now, the concatenation of \( r \) and \( m \) goes to the encryption algorithm, call it \( E \), as an input. Ideally, we may desire \( E \) to be a strong pseudorandom permutation; however, since \( N \) can be sufficiently long (e.g., 128 or larger), constructing a block cipher that maps
2N-bit strings to 2N-bit strings can be expensive. Therefore, we resort to the well-studied cipher block chaining (CBC) mode of operation to construct E from F, as illustrated in Figure 3. Consider the CBC mode of operation depicted in Figure 3. The nonce r is treated as the first plaintext block and is XORed with the initialization vector (IV) to ensure IND-CPA security. The first ciphertext block, is then XORed with the second plaintext block, m in our construction, to produce the second ciphertext block, where key corresponding to the block cipher. The resulting is then transmitted to the intended receiver as the ciphertext.

![Figure 3. The Cipher Block Chaining (CBC) mode of encryption used for message encryption. The random number r is treated as the first block of the plaintext.](image)

**B. MESSAGE AUTHENTICATION**

With the encryption described above, authentication becomes simpler than the ones in previous sections; the authentication tag of message m is calculated as follows:

\[ M + r \mod 2N \] (3)

Upon receiving the cipher text, the intended receiver decrypts it to extract r and m. Given the receiver can check the validity of the message by performing the following integrity test: If the integrity check of equation is satisfied, the message is considered authentic. Otherwise, the integrity of the message is denied.

**C. SECURITY MODEL**

Recall that, to model the security of a message authentication scheme in the standard setup, a probabilistic polynomial time adversary, A, is given oracle access to the signing and verifying algorithms, and challenged to generate a new message-tag pair that will be accepted as valid, for a tag that has not been attached to the message by the signing oracle. Observe, however, that the message to be authenticated in our setup must also be encrypted. That is, what the intended user receives is a cipher text-tag pair, as opposed to plaintext-tag pair in the standard model. This implies that the adversary must come up with a valid cipher text-tag pair for a successful forgery. Modify the standard model of Section B to address the difference between standard MACs and our MAC in which the message must be encrypted.

**D. SECURITY ANALYSIS**

In this section, we prove the privacy of the system, give a formal security analysis of the proposed message authentication mechanism, and then discuss the security of the composed authenticated encryption system.

i. **Data Privacy**

Recall that two pieces of information are transmitted to the intended receiver (the cipher text and the tag), both of which functions of the private plaintext are message. Now, when it comes to the authentication tag, observe that once r serves as a one-time key (similar to the role r plays in the construction of Section 3).

ii. **Data Authenticity**

Before providing a bound on the probability of successful forgery, give an informal discussion on how the structure of the authenticated encryption composition will be utilized. Recall that, in standard MACs, the security is modelled by the adversary's probability of predicting a valid authentication tag for a certain message. That is, given the adversary's knowledge of a polynomial number of valid message-tag pairs, the goal of the adversary is to forge a new message-tag pair that will be accepted as valid. MACs in and our authenticated encryption composition, on the other hand, are fundamentally different than standard MACs. The intended receiver in an authenticated encryption system receives a cipher text-tag pair as opposed to message tag pair. This implies that, for an attempted forgery to be successful, the adversary must come up with a cipher text tag pair that will be accepted as valid, not a message-tag pair.

**V. SECURITY OF THE AUTHENTICATED ENCRYPTION COMPOSITION**

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. Figure 1 illustrates the differences between the three methods for generically composing an authenticated encryption system.

The same discussion of Section III-C applies here.

VI. CONCLUSION

In this work, a 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 benefit from the simplicity of unconditionally secure authentication without the need to manage one-time keys. In particular, it has been demonstrated in this paper that authentication tags can be computed with one addition and a one modular multiplication. Given that messages are relatively short, addition and modular multiplication can be performed faster than existing computationally secure MACs in the literature of cryptography. When devices are equipped with block ciphers to encrypt messages, a second technique that utilizes the fact that block ciphers can be modeled as strong pseudorandom permutations is proposed to authenticate messages using a single modular addition. The proposed schemes are shown to be orders of magnitude faster, and consume orders of magnitude less energy than traditional MAC algorithms. Therefore, they are more suitable to be used in computationally constrained mobile and pervasive devices.

VII. FUTURE WORK

This system is only to provide efficient message authentication for short length of information. In future it can be developed for large length of information.

REFERENCES


