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

Efficient Authentication for Mobile and Pervasive Computing

Srikanth
B.Tech Student,
Department of CSE,
Sphoorthy Engineering College,
Nadergul (Vill.), Sagar Road,
Saroonagar (Mdl), R.R Dist.T.S.

M.Bhanu Prakash
Assistant Professor,
Department of CSE,
Sphoorthy Engineering College,
Nadergul (Vill.), Sagar Road,
Saroonagar (Mdl), R.R Dist.T.S.

J.Deepthi
Associate Professor & HOD,
Department of CSE,
Sphoorthy Engineering College,
Nadergul (Vill.), Sagar Road,
Saroonagar (Mdl), R.R Dist.T.S.

Abstract:
With today's technology, many 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, we 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, we 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.

Architecture Diagram:

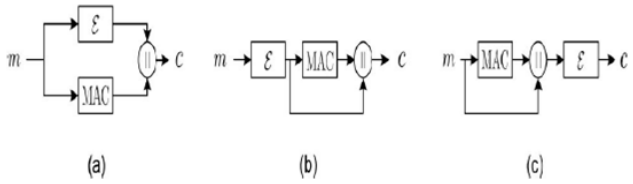

Fig. 1. A Schematic Of The Three Generic Compositions: (A) Encrypt-And authenticate, (B) Encrypt-Then-Authenticate (Eta), And (C) Authenticate then- Encrypt.

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.
3. Unconditionally secure universal hashing-based MACs are considered impractical in most modern applications, due to the difficulty of managing one-time keys

Proposed System:
- In this paper we propose two new techniques for authenticating short encrypted messages that are more efficient than existing approaches.

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

- 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. 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.

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.

Implementation Modules:

1. Authenticating Short Encrypted Messages
2. Security Model
3. Data Privacy
4. Security of the Authenticated Encryption Composition

AUTHENTICATING SHORT ENCRYPTED MESSAGES:

In this module, we describe our 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-timepad authentication without the need to manage impractically long keys.

Security Model:

A message authentication scheme consists of a signing algorithm S and a verifying algorithm V. 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 S 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 V 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 S to generate a tag for a plaintext of its choice and ask the verifier V to verify that _ is a valid tag for the plaintext. Formally, A's attack on the scheme is described by the following experiment:

1) A random string of length ` is selected as the shared secret.
2) Suppose A makes a signing query on a message m. Then the oracle computes an authentication tag _ = S(k;m)and returns it to A. (Since S may be

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

probabilistic, this step requires making the necessary underlying choice of a random string for S, anew for each signing query.)
3) Suppose A makes a verify query (m; _). The oracle computes the decision d = V(k; m; _) and returns it to A.

Security of the Authenticated Encryption Composition:

In this module, it defined two notions of integrity for authenticated encryption systems: the first is integrity of lain text (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), 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.

Data Privacy:

Recall that two pieces 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.

System Configuration:

H/W System Configuration:

Processor	-	Pentium –III
Speed	-	1.1 Ghz
RAM	-	256 MB(min)
Hard Disk	-	20 GB
Floppy Drive	-	1.44 MB
Key Board	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse
Monitor	-	SVGA

S/W System Configuration:

Operating System	:	Windows95/98/2000/XP
Front End	:	java, jdk1.6
Database	:	My sqlserver 2005
Database Connectivity	:	JDBC.

Author's Details:

Srikanth
B.Tech Student,
Department of CSE,
Sphoorthy Engineering College,
Nadergul (Vill.), Sagar Road,
Saroonagar (Mdl), R.R Dist.T.S.

M.Bhanu Prakash
Assistant Professor,
Department of CSE,
Sphoorthy Engineering College,
Nadergul (Vill.), Sagar Road,
Saroonagar (Mdl), R.R Dist.T.S.

J.Deepthi
Associate Professor & HOD,
Department of CSE,
Sphoorthy Engineering College,
Nadergul (Vill.), Sagar Road,
Saroonagar (Mdl), R.R Dist.T.S.