Chapter 5
Applied Cryptography in E-Mail Services and Web Services

Lei Chen
Sam Houston State University, USA

Wen-Chen Hu
University of North Dakota, USA

Ming Yang
Jacksonville State University, USA

Lei Zhang
Frostburg State University, USA

ABSTRACT

E-mail services are the method of sending and receiving electronic messages over communication networks. Web services on the other hand provide a channel of accessing interlinked hypermeida via the World Wide Web. As these two methods of network communications turn into the most popular services over the Internet, applied cryptography and secure authentication protocols become indispensable in securing confidential data over public networks. In this chapter, we first review a number of cryptographic ciphers widely used in secure communication protocols. We then discuss and compare the popular trust system Web of Trust, the certificate standard X.509, and the standard for public key systems Public Key Infrastructure (PKI). Two secure e-mail standards, OpenPGP and S/MIME, are examined and compared. The de facto standard cryptographic protocol for e-commerce, Secure Socket Layer (SSL) / Transport Layer Security (TLS), and XML Security Standards for secure web services are also discussed.

INTRODUCTION

In e-mail services, Wiki-E-mail (2009), and Web services, Wiki-Web (2009), various cryptographic algorithms are used to achieve the security goals, Stallings, W. (2006) and Stallings, W. (2007), of confidentiality, integrity, authentication and non-repudiation. Data confidentiality is commonly provided via encryption. Since symmetric key ciphers, such as DES, Triple-DES and AES, perform faster than public key ciphers, such as RSA, they are preferable in choosing ciphers to protect the secrecy of data.

DOI: 10.4018/978-1-61520-783-1.ch005

Hash functions, such as MD5 and SHA-1, are used to preserve data integrity. The sender hashes the data content using one or multiple hash functions and sends the message digests to the receiver who is capable to verify the message integrity by running the same hash functions on the received message and then comparing the output digests to the received ones.

There are two types of authentication: entity authentication and data-origin authentication both of which make use of cryptographic mechanisms. Entity authentication is based on cryptographic keys, including both symmetric key-based authentication and public key-based authentication. SSL/TLS in web security services uses this type of authentication. Data-origin based authentication is accomplished through Message Authentication Code (MAC), Stallings, W. (2007) and Wiki-MAC (2009), and digital signatures. Secure email services provide data-origin authentication through digital signatures.

Non-repudiation, a security feature which makes a communication party not able to repudiate what has been done, utilizes public key cryptographic ciphers, such as RSA. These public key ciphers allow a party to sign a message using the private key and this signing can later be verified by applying the paired public key to the signed message. Before move on to the discussion of secure e-mail services and Web services, it is preferred to survey the common cryptographic ciphers and security protocols and standards in these services.

COMMONLY USED CRYPTOGRAPHIC CIPHERS AND SECURITY PROTOCOLS

Data Encryption Standard (DES) and Triple-DES

In 1973, National Institute of Standards and Technology (NIST, previously NBS) solicited proposals for a government-wide standard for encryption and decryption. Based on the IBM Lucifer cipher (developed by 1973Feistel and his colleagues in 1973! and 1974), DES was accepted as an official Federal Information Processing Standard (FIPS) for the U.S. in 1976, later widespread internationally. Many later ciphers, including RC5, Blowfish and CAST5, were designed based on DES. DES is basically an iterative symmetric key algorithm that uses a relatively short key with only 56 binary bits in length. In each of its 16 rounds, DES takes a 64-bit data block and a 48-bit sub-key as the inputs and goes through a series of steps including expansion, Substitution Boxes (S-Boxes) and Permutation Boxes (P-Boxes) resulting 64-bit output. Everything except the S-Boxes in DES is linear. Due to short key length of DES, Triple-DES or 3DES was introduced to increase the key length to 112-bit in EDE mode and 168-bit in EEE mode. DES and 3DES had been the most popular symmetric key block ciphers before the emergence of AES.

DES has eight different S-boxes, each of which maps a 6-bit input to a 4-bit output. The first bit and the last bit of the 6-bit input of an S-box form the binary row indexes and the rest 4-bit of the input forms the column indexes of a single S-box conversion table. The table then has the dimension of 4 (00 to 11) rows by 16 (0000 to 1111) columns and the 64 intersections show the possible values of the 4-bit output. Each possible 4-bit output value has 4 occurrences among the intersections. Therefore, a specific 6-bit input value points to a specific intersection and output value. On the other hand, a unique output value does not help find the input value due to the 4 occurrences.

Advanced Encryption Standard (AES)

AES, also known as Rijndael algorithm, was announced by NIST in 2001 as the new standard symmetric block cipher to replace DES and 3DES. AES was selected from fifteen proposed candidate algorithms and has become the most popular cipher of its kind. AES offers options of 128-bit, 192-bit

Integrating Psychological Ownership and Protection Motivation Theory in Chinese IT Organizations
Xiaofen Maand Hichang Cho (2026). *International Journal of Information Security and Privacy (pp. 1-24).*
www.irma-international.org/article/integrating-psychological-ownership-and-protection-motivation-theory-in-chinese-it-organizations/407403