Security and Privacy Issues in Secure E-Mail Standards and 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

Secure e-mail standards, such as Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extension (S/MIME), apply cryptographic algorithms to provide secure and private e-mail services over the public Internet. In this article, we first review a number of cryptographic ciphers, trust and certificate systems, and key management systems and infrastructures widely used in secure e-mail standards and services. We then focus on the discussion of several essential security and privacy issues, such as cryptographic cipher selection and operation sequences, in both PGP and S/MIME. This work tries to provide readers a comprehensive impression of the security and privacy provided in the current secure e-mail services.

Keywords: Cryptographic Ciphers, DES, DSA, PGP, PKI, RSA, S/MIME, Web of Trust, X.509

One of the most popular Internet services is e-mail services which provide sending and receiving electronic messages of communication networks. E-mail standards and services apply various cryptographic algorithms to achieve the security goals (Stallings, 2006; Stallings, 2007) of confidentiality, integrity, authentication and non-repudiation.

Data confidentiality in e-mail services is commonly made available via cryptographic encryption. Since symmetric key ciphers, such as DES, Triple-DES and AES, process data at higher rates than public key ciphers, such as RSA, they are preferable in protecting the secrecy of data. 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’s integrity by running the same hash functions over the received message and then comparing the output digests to the received ones.

DOI: 10.4018/jisp.2009100701
There are two types of authentication: entity authentication and data-origin authentication, both of which make use of cryptographic algorithms. Entity authentication is based on cryptographic keys, including both symmetric key-based authentication and public key-based authentication. Secure Socket Layer / Transport Layer Security (SSL/TLS) in secure web services uses this type of authentication. Data-origin based authentication is accomplished through Message Authentication Code (MAC) (Stallings, 2007) and digital signatures. Secure email services provide data-origin authentication through digital signatures.

Non-repudiation, a security feature making a communication party not able to deny the past transactions, uses 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. In the follow section, we review the common cryptographic ciphers and security protocols and standards in secure e-mail services.

**CIPHERS AND STANDARDS**

**Cryptographic Ciphers and Security Protocols**

**Data Encryption Standard (DES) and Triple-DES**

Proposals for government encryption and decryption standard were solicited in 1973 by the National Institute of Standards and Technology (NIST). In 1976, DES, based on the IBM Lucifer cipher which was developed by Feistel and his colleagues in the early nineteen seventies, was accepted as an official Federal Information Processing Standard (FIPS) for the U.S. and later other countries. DES is the predecessor of multiple cryptographic ciphers including RC5, Blowfish and CAST5.

Being an iterative symmetric key cipher, DES has relatively short key at 56 binary bits in length. In each of its 16 iterative rounds, DES takes a 64-bit data block and a 48-bit sub-key as the input and goes through a sequence of operating including Expansion, Substitution (S-Boxes) and Permutation (P-Boxes) producing 64-bit output. Only the S-Boxes are not linear in DES. Each of DES’ eight different S-Boxes converts a 6-bit input to a 4-bit output. The conversion table has 4 rows and 16 columns with 64 intersections each of which holds a possible output value. With 4 binary bits, the output from each S-Box can only have 16 ($2^4$) possible values. Therefore, each of these 16 values appears at four different intersections, making each S-Box a one-way function. In other words, a 6-bit input, with its first and last bits as the row index and the rest bits as the column index, of an S-Box locates a single intersection in the conversion table and further determines the 4-bit output value. However, knowing an output value only helps find the four possible appearances in the conversion table leaving the input value in vague. With 8 different S-Boxes in each round and 16 rounds in total, DES is basically irreversible. Due to the limited length of key in DES, Triple-DES or 3DES was introduced extending the key length to 112-bit in EDE mode and 168-bit in EEE mode. Before the emergence of AES, DES and 3DES had been the most popular symmetric key block ciphers.

**Advanced Encryption Standard (AES)**

AES, also known as the Rijndael algorithm, was announced by NIST in 2001 as the new standard symmetric block cipher to replace DES and 3DES. AES was selected out of fifteen proposed candidate algorithms and has become the most popular cipher of its kind. AES offers options of 128-bit, 192-bit and 256-bit key sizes depending on the number of rounds that the algorithm goes through in the encryption process. No successful or effective attack on the algorithm has been reported so far. However, Side Channel Attacks can be used to assail the implementation of the AES cipher on system which leaks data.
Related Content

Global Supply Chain Management Conference
[www.irma-international.org/article/global-supply-chain-management-conference/65732/](www.irma-international.org/article/global-supply-chain-management-conference/65732/)

Laws and Regulations Dealing with Information Security and Privacy: An Investigative Study
[www.irma-international.org/article/laws-regulations-dealing-information-security/2482/](www.irma-international.org/article/laws-regulations-dealing-information-security/2482/)

Gender Differences in the Navigation of Electronic Worlds
[www.irma-international.org/chapter/gender-differences-navigation-electronic-worlds/23245/](www.irma-international.org/chapter/gender-differences-navigation-electronic-worlds/23245/)

Do We Need Security Management Systems for Data Privacy?
[www.irma-international.org/chapter/do-we-need-security-management-systems-for-data-privacy/123537/](www.irma-international.org/chapter/do-we-need-security-management-systems-for-data-privacy/123537/)

Risk Management Research Design Ideologies, Strategies, Methods and Techniques
[www.irma-international.org/article/risk-management-research-design-ideologies/77903/](www.irma-international.org/article/risk-management-research-design-ideologies/77903/)