Chapter 4
Cryptography in E-Mail and Web Services

Wasim A. Al-Hamdani
Kentucky State University, USA

ABSTRACT

Cryptography has been used since ancient times in many different shapes and forms to protect messages from being intercepted. However, since 1976, cryptography started to be part of protected public communication when e-mail became commonly used by the public. Webmail (or Web-based e-mail) is an e-mail service intended to be primarily accessed via a web browser, as opposed to through an e-mail client, such as Microsoft Outlook, Mozilla's Thunderbird Mail. Very popular webmail providers include Gmail, Yahoo! Mail, Hotmail and AOL. Web based email has its advantages, especially for people who travel. Email can be collected by simply visiting a website, negating the need for an email client, or to logon from home. Wherever a public terminal with Internet access exists one can check, sends and receive email quickly and easily. Another advantage of web based email is that it provides an alternate address allowing user to reserve his/her ISP address for personal use. If someone would like to subscribe to a newsletter, enter a drawing, register at a website, participate in chats, or send feedback to a site, a web based email address is the perfect answer. It will keep non-personal mail on a server for you to check when you wish, rather than filling up your private email box. Web service is defined as "a software system designed to support interoperable machine-to-machine interaction over a network". Web services are frequently just Internet application programming interfaces (API) that can be accessed over a network, such as the Internet, and executed on a remote system hosting the requested services. Other approaches with nearly the same functionality as web services are Object Management Group's (OMG) Common Object Request Broker Architecture (CORBA), Microsoft's Distributed Component Object Model (DCOM) or SUN's Java/Remote Method Invocation (RMI). Integrating Encryption with web service could be performing in many ways such as: XML Encryption and XML Signature. In this article we present client and Web-based E-mail, next generation E-mail and secure E-mail, followed by cryptography in web service and the last part is the future of web service security. The article start with the integration of cryptography with E-mail client and web base then the integration of cryptography

DOI: 10.4018/978-1-61520-783-1.ch004

and web service is presented. At the end of the major two sections: e-mail service and web service there is a general prospect vision of encryption future for e-mail service and web service. This section presents our view for the cryptography integration with the second generation of e-mail and web service.

INTRODUCTION

Encryption is the process of transforming information (plaintext) using an algorithm to make it unreadable through using a key. The result of the process is encrypted information (ciphertext). In many contexts, the word encryption also implicitly refers to the reverse process, decryption, to make the encrypted information readable again. The use of encryption/decryption is as old as the art of communication. In wartime, a cipher – often called a "code" – can be employed to keep the enemy from obtaining the contents of transmissions (examples are Morse code and ASCII). Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals.

In a Web services world, everyone communicates with everyone else. Many intermediaries could exist between, say, supplier and buyer. What if one of these intermediaries becomes compromised? End-to-end security becomes fundamentally important if someone wants to do something considered more significant operations (such as a money transaction or international e-commerce). For all these reasons and others, this chapter is written to present two subjects: (a) E-mail and web service integrating with encryption algorithms to protect personal, business, and financial information, and (b) authenticating and authorizing a user or business entity.

Web service is defined by the W3C as, "a software system designed to support interoperable machine-to-machine interaction over a network" (Web Services Glossary from W3 organization, 2004) It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.

WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages, regardless of what message formats or network protocols are used to communicate. However, the only bindings described in this document explain how to use WSDL in conjunction with SOAP 1.1, HTTP GET/POST, and MIME.

XML Encryption, also known as XML-Enc, is a specification governed by a W3C recommendation that defines how to encrypt the contents of an XML element. Although XML Encryption can be used to encrypt any kind of data, it is nonetheless known as "XML Encryption" because an XML element (either an EncryptedData or EncryptedKey element) contains or refers to the ciphertext, keying information, and algorithms.

In the section which covers Web service and the use of encryption algorithms, we will look at XML security, signature, encryption algorithms, and security requirements for Web service infrastructure. This section is the expected future for encryption with Web services protecting privacy and b2b infrastructure.

The next generation of Cryptography integration with e-mail service and web service is the subject of the last section with cryptography combination with e-mail and web service. And the