Chapter 3
E-Mail, Web Service and Cryptography

Wasim A. Al-Hamdani
Kentucky State University, USA

ABSTRACT

Cryptography is the study and practice of protecting information and has been used since ancient times in many different shapes and forms to protect messages from being intercepted. However, since 1976, when data encryption was selected as an official Federal Information Processing Standard (FIPS) for the United States, cryptography has gained large attention and a great amount of application and use. Furthermore, cryptography started to be part of protected public communication when e-mail became commonly used by the public. There are many electronic services. Some are based on web interaction and others are used as independent servers, called e-mail hosting services, which is an Internet hosting service that runs e-mail servers. Encrypting e-mail messages as they traverse the Internet is not the only reason to understand or use various cryptographic methods. Every time one checks his/her e-mail, the password is being sent over the wire. Many Internet service providers or corporate environments use no encryption on their mail servers and the passwords used to check mail are submitted to the network in clear text (with no encryption). When a password is put into clear text on a wire, it can easily be intercepted. Encrypting email will keep all but the most dedicated hackers from intercepting and reading a private communications. Using a personal email certificate one can digitally sign an email so that recipients can verify that it's really from the sender as well as encrypt the messages so that only the intended recipients can view it. Web service is defined as "a software system designed to support interoperable machine-to-machine interaction over a network" and e-mail is "communicate electronically on the computer". This chapter focus on introduce three topics: E-mail structure and organization, web service types, their organization and cryptography algorithms which integrated in the E-mail and web services to provide high level of security. The main issue in this article is to build the general foundation through Definitions, history, cryptography algorithms symmetric and asymmetric, hash algorithms, digital signature, suite B and general principle to introduce the use of cryptography in the E-mail and web service.

DOI: 10.4018/978-1-61520-783-1.ch003

INTRODUCTION

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.

The Internet is a big place with a lot of people on it. It is very easy for someone who has access to the computers or networks through which someone information is traveling to capture this information and read it; this could cause threat such as: identity theft, message modification, false messages, message replay, unprotected backups and repudiation.

Web service is defined as "a software system designed to support interoperable machine-to-machine interaction over a network" and e-mail is "communicate electronically on the computer".

There are many electronic services. Some are based on web interaction and others are used as independent servers, called e-mail hosting services, which is an Internet hosting service that runs e-mail servers. E-mail hosting services usually offer quality e-mail at a cost as opposed to advertising-supported free e-mail or free webmail. E-mail hosting services thus differ from typical end-user e-mail providers, such as webmail sites. They outfit mostly to demanding e-mail users and small and mid-size businesses, while larger enterprises usually run their own e-mail hosting service. E-mail hosting providers allow for quality e-mail services besides the custom configurations and large number of accounts. Hosting providers manage a user's own domain name, including any e-mail authentication scheme that the domain owner wishes to enforce in order to convey the meaning that using a specific domain name identifies and qualifies e-mail senders.

The chapter starts with a general definition and short history of the two major themes, e-mail and Web service, followed with a cryptography section that discusses an encryption algorithm and the practical application of encryption as a digital signature, general cryptography classifications, and the standard cryptography suites authorized by the National Security Agency (NSA). Next are the short studies on e-mail protocols as a general then a deep look at encryption e-mail protocols such as S/MIME and PGP.

Cryptography is the practice and study of hiding information; the Integration of cryptography in email and web service provides:

- Confidentiality (the information cannot be understood by anyone for whom it was unintended),
- Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected),
- Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information) and
- Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information.

The cryptography section covers: definition, symmetric, asymmetric, stream cipher, hash, digital signature, the suite B standard, authentication, cryptography message syntax an the last section is general introduction to Cryptography standards algorithms.

The article start with definition and history, followed with detail description for the three elements of this article.