Eng. & Tech. Journal, Vol.29, No.16, 2011

A Proposed Secure Protocol for E-Mail System Based on Authentication and Hash Function

Dr. Muna Mohammed Al-Nayar*

Received on: 27/ 3 / 2011
Accepted on: 3 /11 / 2011

Abstract

Internet has opened new channel of communication enabling an e-mail to be sent to a relative thousands of kilometers away. This medium of communication opens doors for virtually free mass e-mailing, reaching out to hundreds of thousands users around the globe within seconds, so e-mail becomes the most popular form of communication today. E-mail systems have suffered from increasing attacking problem that threatens the validity and integrity of communication. Many different approaches for fighting this attack have been proposed, ranging from various sender authentication protocols to encrypt the message itself. This paper demonstrates a promising protocol. The proposed protocol ensures the authentication and integrity of the data and avoids the problem of key distribution or breaking by using multiple random keys generated automatically during communication session.

Keywords: E-Mail System, Security Protocol, Authentication, Hash Function, Randomization, Message Integrity and Confidentiality.

مقترح بروتوكول آمن لنظام البريد الالكتروني مستند على تعريف الهوية ودالة الـ Hash

الخلاصة

فتحت الانترنت قناة جديدة للاتصال تمكن من ارسال بريد الكتروني عبر الاف الكيلومترات. هذه الوسيلة من الاتصال فتحت ابواب امام ارسال كميات من الرسائل الى الاف المستخدمين حول العالم خلال ثواني، لذلك اصبح البريد الالكتروني هو الاتصال الاكثر شيوعا اليوم. يعاني نظام البريد الالكتروني من مشكلة الهجوم المتزايد والذي يهدد صحة وتكامل الاتصال. وقد اقترحت طرق عديدة لمحاربة هذا الهجوم تتراوح ما بين بروتوكولات مختلفة لتعريف الهوية الى تشفيرالرسالة نفسها. يقدم هذا البحث بروتوكول معتمد على تعريف الهوية ودالة الـHash للمحافظة على امنية المعلومات. يأكد البروتوكول المقترح على هوية المستخدم وتكامل البيانات ويتجاوز مشاكل توزيع او كسر المفتاح باستخدامه مفاتيح متعددة وعشوائية وتولد اتوماتيكيا خلال فترة الاتصال.

* Computer Engineering Department, University of Technology / Baghdad

PDF created with pdfFactory Pro trial version www.pdffactory.com