الخلاصة

البريد الإلكتروني أو ما يسمى بالـ(Email) هو من اكثر الخدمات المعتمدة على الشبكات استخداماً, أيضاً هو التطبيق الأكثر استخداماً على كل المعماريات ومنصات المجهزين.

مع التنامي الكبير للأعتمادية على البريد الإلكتروني في كل الأغراض المتاحة، اصبح هناك طلب متنامي على دعمه بخدمات التوثيق والسلامة.

البريد الإلكتروني يعتمد على بروتوكولين خاصين بعملية نقل الرسائل من مستخدم إلى مستخدم (أو مستخدمين), هذين البروتوكولين هما بروتوكول نقل البريد البسيط (SMTP) وبروتوكول دائرة البريد الإصدار الثالث(POP3). البروتوكول الأول ليس فيه أيَ خصائص حماية أما البروتوكول الثاني ففيهِ خصائص حماية ضعيفة.

هذه الأطروحة تقدم تطور نظام بريد إلكتروني آمن يدعى (Emailsec) والذي يجهز بروتوكولات البريد الإلكتروني بإمكانيات أمنية مبنية والتي هي خدمات الموثوقية والسلامة.

هذه الإمكانات تتم بتطبيق مقترح بروتوكول توثيق جديد ويُضَمَنْ مع بروتوكولات البريد الإلكتروني . البروتوكول المقترح يعتمد على خدمتي توثيق هما الاختبار والاستجابة بكل الاتجاهين وكلمة السر المستخدمة لمرة واحدة.

هذه الخدمتين مبنية على اكثر الـ(Hash functions) أمناً وهما خوارزمية (MD5) و خوارزمية (SHA-1).

النظام المقترح سيكون اكثر أمناً من الأنظمة التي تعتمد على خوارزميات التشفير فقط, بسبب أن المهاجم يجب أن يحلل ويكسر خدمتين أمنيتين مختلفتين.

PDF created with pdfFactory trial version www.pdffactory.com

Abstract

Electronic mail or Email is the most heavily used network based service. It is also the only distributed application that is widely used across all architectures and vendor platform.

With the explosive growing reliance on electronic mail for every conceivable purpose, there is a growing demand for authentication and integrity services.

The Email is based on two essential message transfer protocols that transfer messages from user to user(s) through the Email system components. These protocols are Simple Mail Transfer Protocol (SMTP), and Post Office Protocol (POP3). The former protocol has no built-in security features, while the latter has weak built-in security features, which make them under many security threats.

This work presents the development of a secure email system (called Emailsec) that supports Email protocols with built-in security capabilities, which are authentication and integrity capabilities.

These capabilities can be achieved by applying a new proposed authentication protocol within these Email protocols. The proposed authentication protocol is based on two different authentication services, which are Two-Way Challenge-Response authentication service, and One-Time Password authentication service. These two services are based on two of the most secure hashing functions, which are Message Digest version 5 (MD5), and Secure Hashing Algorithm (SHA-1).

The proposed Email system will be more secure than systems that depend only on cryptography algorithms, since the attacker should analyze and break

PDF created with pdfFactory trial version www.pdffactory.com