Resumen

El correo electrónico es el medio de comunicación más utilizado por las empresas para compartir información entre sus empleados, proveedores y clientes sea ésta de carácter público o privado, no obstante, el protocolo utilizado para dicho intercambio de información es SMTP, el cual transmite la información en texto plano a través de la red, lo cual lo vuelve vulnerable a ser interceptado durante su transporte. Dentro de los procesos de seguridad es imprescindible garantizar la privacidad, confidencialidad y disponibilidad de la información, más aún durante las comunicaciones entre colaboradores (ejemplo transmisión de contraseñas), es por ello por lo que se plantea la utilización de cifrado en ambos extremos mediante correo electrónico con GPG, es necesario realizar un análisis y comparativa entre los dos protocolos utilizados en los sistemas de correos electrónicos para verificar el sistema que brinda más seguridad dentro de una organización. Este sistema permitirá que todos los emails enviados desde cualquier cliente de correo configurado sean cifrados con las claves públicas de los destinatarios y solo podrán ser leídos por el personal que disponga de la clave privada de cada cuenta, de igual manera al recibir los correos electrónicos los destinatarios podrán confirmar mediante la firma digital la autenticidad del remitente. Para garantizar la seguridad de la información transmitida el objetivo de GPG es proteger los datos enviados del acceso no autorizado por parte de terceros o personas externas, por lo tanto, los correos electrónicos cifrados no serán legibles ni podrán ser visualizados si estos son interceptados en su transporte.

Palabras clave: Protección de privacidad, Correo Electrónico, Texto cifrado, Firma electrónica, Protocolo Simple de Transferencia de Correo

Abstract

E-mail is the means of communication most used by companies to share information between their employees, suppliers and customers, whether public or private, however, the protocol used for this information exchange is SMTP, which transmits information in plain text through the network, which makes it vulnerable to interception during transport. Within the security processes it is essential to ensure the privacy, confidentiality and availability of information, even more so during communications between collaborators (e.g. transmission of passwords), which is why the use of encryption at both ends through email with GPG is proposed, it is necessary to perform an analysis and comparison between the two protocols used in email systems to verify the system that provides more security within an organization. This system will allow all emails sent from any configured email client to be encrypted with the public keys of the recipients and can only be read by personnel who have the private key of each account, likewise when receiving emails the recipients can confirm by digital signature the authenticity of the sender. In order to guarantee the security of the transmitted information, GPG's objective is to protect the sent data from unauthorized access by third parties or external persons, therefore, encrypted e-mails will not be readable nor can they be viewed if they are intercepted in transit.

Keywords: Privacy Guard, Email, Cipher Text, Electronic Signature, Simple Mail Transfer Protocol