Tutorial

Uso de la Herramienta GNU Privacy Guard (GPG) para Criptografía, Firmas Digitales y Correo Electrónico Cifrado

Miguel A. Astor[a]

[a]*Universidad Central de Venezuela, Fac. de Ciencias, Esc. de Computación*
miguel.astor@ciens.ucv.ve

Resumen: En este taller los participantes podrán conocer los fundamentos de la criptografía desde un punto de vista práctico más que teórico, usando la herramienta GNU Privacy Guard (también conocida como GnuPG o GPG) para verificar la autenticidad de documentos y para verificar la identidad de otras personas a través de la red. Así mismo se examinará el uso del estándar OpenPGP como herramienta para proveer seguridad a las comunicaciones por correo electrónico, mediante la integración del cliente de correos Mozilla Thunderbird con GPG.

Palabras Clave: criptografía asimétrica, confidencialidad, OpenPGP, GPG.

1 Introducción

La criptografía asimétrica es una de las herramientas más importantes que provee la seguridad informática, siendo la piedra angular de las tecnologías de seguridad que proveen servicios de identificación y confidencialidad, siendo el protocolo HTTPS y la infraestructura de clave pública que proveen la seguridad del comercio electrónico sus principales usos a nivel general [1].

En 1991 Phill Zimmerman, desarrollador y miembro del grupo Cipherpunk, publica el código fuente de una herramienta llamada PGP, siglas de Pretty Good Privacy (Privacidad Bastante Buena) la cual implementa una considerable cantidad de algoritmos de cifrado simétrico y asimétrico [2]. La publicación de la herramienta cumplía dos propósitos [2]: (1) proveer una herramienta para comunicación privada que proveyera altos estándares de confidencialidad e identificación para el los grupos de activismo en los que estaba involucrado Zimmerman en dicho momento (no solo el grupo Cipherpunk, sino también grupos de activismo anti armas nucleares en Internet); (2) servir como mecanismo de protesta contra las restricciones del gobierno de los Estados Unidos para la exportación de software criptográfico.

Como parte de la protesta contra las restricciones de exportación, la IETF (*Internet Engineering Task Force* – Fuerza de Trabajo de Ingeniería de Internet) estandariza el funcionamiento de la aplicación PGP con la intención de que surgieran implementaciones adicionales de esta [2]. La versión más reciente de este estándar, conocido como OpenPGP, se documenta en el RFC 4880 [3], siendo GNU Privacy Guard una implementación libre de alta calidad de este estándar [4].

Como herramienta, el estándar OpenPGP provee una serie de funcionalidades que permiten el cifrado/descifrado de datos, la generación y verificación de firmas digitales para archivos y la verificación de identidad del remitente y receptor de mensajes. Las implementaciones de este estándar proveen un mecanismo descentralizado para la solución de todos estos problemas de comunicación privada y ha sido por mucho tiempo uno de los pilares de la criptografía práctica [2].

2 Objetivos

General

Presentar los fundamentos del uso de la herramienta GPG para el cifrado y firmado de datos y para el cifrado y verificación de la autenticidad de los correos electrónicos.

Específicos

1. Definir el concepto de criptografía y los distintos tipos y algoritmos criptográficos soportados por GPG.
2. Prácticar el uso básico de GPG para el cifrado de datos y para la creación y verificación de firmas digitales.
3. Presentar el concepto de red de confianza como solución descentralizada al problema de la identificación del propietario de una clave pública específica.
4. Configurar un cliente de correo electrónico Thunderbird para realizar cifrado y verificación de autenticidad de mensajes.

3 Contenidos del Tutorial

3.1 Introducción a la Criptografía

Tipos de criptografía, criptografía simétrica y asimétrica, algoritmos criptográficos, el estándar OpenPGP.

3.2 Tópicos de Criptografía Asimétrica

Historia de la criptografía asimétrica, usos de la criptografía asimétrica, cifrado, creación y verificación de firmas digitales, identificación.

3.3 Algoritmos de Criptografía Asimétrica

Diffie-Hellman, RSA.

3.4 Uso de GPG

Creación de llaveros, creación de pares de claves pública/privada, cifrado simétrico, cifrado asimétrico, firmado y verificación de archivos, manipulación de claves, servidores de claves, red de confianza.

3.5 Correo Electrónico Seguro

Integración de Thunderbird con GPG, firmado de correos salientes, verificación de correos entrantes, cifrado y descifrado de correos.

4 Metodología

4.1 Duración

4 horas.

4.2 Público Objetivo

Profesionales o estudiantes de Computación, Informática o Sistemas que tengan interés en la criptografía y en conocer el uso de la herramienta GnuPG.

4.3 Requerimientos técnicos y operativos

Para el presentador y los asistentes se requiere de computadoras con sistema operativo Windows o Linux que tengan instalados los siguientes programas:

- GNU Privacy Guard (suele estar instalado por defecto en los sistemas operativos Debian y Ubuntu).
- Mozilla Thunderbird en su versión más reciente.

Adicionalmente se requiere de un proyector en la sala para el presentador.

4.4 Idioma

Español

4.5 Resumen curricular del presentador

Licenciado en Computación, Universidad Central de Venezuela (UCV), Caracas, Venezuela (2014). Miembro del personal académico de la UCV (desde 2014). Actualmente es Profesor Ordinario, categoría Instructor a dedicación exclusiva en plan de formación (desde 2016). Adscrito al Centro de Investigación en Comunicaciones y Redes CICORE, Escuela de Computación, UCV.

Actualmente cursa estudios de Maestría en Ciencias de la Computación en el Postgrado de Computación de la Universidad Central de Venezuela, bajo la tutoría del Dr. Wilmer Pereira Gonzales.

Referencias

[1] Schneier, B., "*Applied Criptography: Protocols, Algorithms and Source Code in C*", Edición de 20º aniversario, Editorial Wiley, 2015.

[2] Lucas, M., "*PGP & GPG: Email for the Practical Paranoid*", 1a edición, Editorial No Starch Press, 2006.

[3] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, y R. Thayer, "*OpenPGP message format*" Estándar RFC 4880, Internet Engineering Task Force IETF, 2007.

[4] The GnuPG Project, "*The gnu privacy guard*", https://gnupg.org/, 1998.