

Taller de Seguridad

Criptografía para todos los días

Daniel Marcos Martín

GUL UC3M

04/03/2010

Parte I

Introducción

Criptografía clave privada

- Clave compartida
- Misma clave cifrar/descifrar
- DES, AES, etc.

Criptografía clave pública

- Dos claves: pública y privada
- Una clave se cifra y con la otra se descifra
- Más lenta
- Mayor utilidad
- GPG, RSA, Diffie-Helman

Cifrado de información

- Clave pública y privada (más utilizada)
 - Fichero
 - Sistema de ficheros
 - Comunicaciones
- Clave pública
 - Firma digital
 - Certificados
- Híbrido
 - SSL

Certificados

- Comunicaciones seguras
- Listas de revocación

Funciones resumen

- Firma digital
- No repudio

Gestión de contraseñas

- pwman3
- pwsafe
- password-gorilla

Cifrado comunicaciones

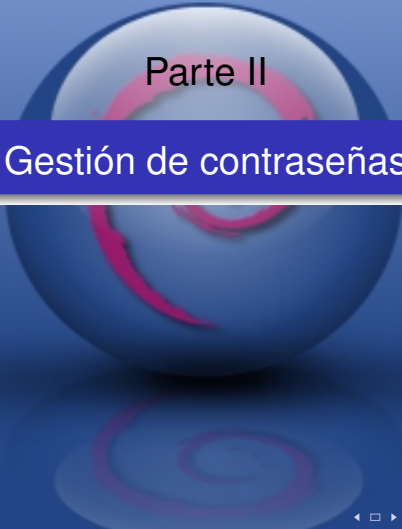
- SSL
 - openssl
 - Módulo Apache
- PGP
 - gnupg
 - FireGPG

Cifrado ficheros

- Mcrypt
- TrueCrypt
- vim plugin
- emacs plugin

Cifrado sistema de ficheros

- Cryptoloop
- Loop-AES
- Dmccrypt
- Truecrypt



Parte II

Gestión de contraseñas

Número de contraseñas

- ¿En cuantos servicios estamos dados de alta?
 - ordenador personal, empresa, gmail, hotmail, uc3m, foros, etc.
- ¿Cuántas contraseñas diferentes utilizamos?
 - Baja seguridad
 - Alta seguridad

Caducidad

- ¿Cada cuanto las cambiamos?
 - Cuando nos las olvidamos
 - Cada 30 días, etc.

Robustez

- ¿Aleatorias?
 - Top 10 palabras (por ejemplo 01-12)
 - Palabras de uso común

Justificación

Número de contraseñas

- ¿En cuantos servicios estamos dados de alta?
 - ordenador personal, empresa, gmail, hotmail, uc3m, foros, etc.
- ¿Cuántas contraseñas diferentes utilizamos?
 - Baja seguridad
 - Alta seguridad

Caducidad

- ¿Cada cuanto las cambiamos?
 - Cuando nos olvidamos
 - Cada mes, 3º

Robustez

- ¿Aleatorias?
 - Top 10 palabras (por ejemplo 01-12)
 - Pasaseguridad

Número de contraseñas

- ¿En cuantos servicios estamos dados de alta?
 - ordenador personal, empresa, gmail, hotmail, uc3m, foros, etc.
- ¿Cuántas contraseñas diferentes utilizamos?
 - Baja seguridad
 - Alta seguridad

Caducidad

- ¿Cada cuanto las cambiamos?
 - Cuando nos olvidamos
 - Cada mes, 3º

Robustez

- ¿Aleatorias?
 - Top 5 palabras (por ejemplo 01-12)
 - Alta seguridad

Número de contraseñas

- ¿En cuantos servicios estamos dados de alta?
 - ordenador personal, empresa, gmail, hotmail, uc3m, foros, etc.
- ¿Cuántas contraseñas diferentes utilizamos?
 - Baja seguridad
 - Alta seguridad

Caducidad

- ¿Cada cuanto las cambiamos?
 - Cuando nos olvidamos
 - Cada mes, etc.

Robustez

- ¿Aleatorias?
 - Tipo: Seguridad por fuerza bruta
 - Tipo: Seguridad por fuerza de cálculo

Número de contraseñas

- ¿En cuantos servicios estamos dados de alta?
 - ordenador personal, empresa, gmail, hotmail, uc3m, foros, etc.
- ¿Cuántas contraseñas diferentes utilizamos?
 - Baja seguridad
 - Alta seguridad

Caducidad

- ¿Cada cuanto las cambiamos?
 - Cuando nos olvidamos
 - Cuando expira

Robustez

- ¿Aleatorias?
 - De 8 caracteres con mayúsculas, minúsculas, números y caracteres especiales

Número de contraseñas

- ¿En cuantos servicios estamos dados de alta?
 - ordenador personal, empresa, gmail, hotmail, uc3m, foros, etc.
- ¿Cuántas contraseñas diferentes utilizamos?
 - Baja seguridad
 - Alta seguridad

Caducidad

- ¿Cada cuanto las cambiamos?

¿Cada cuánto reiniciamos?

Robustez

- ¿Aleatorias?

¿Baja seguridad con números 0-9?

Número de contraseñas

- ¿En cuantos servicios estamos dados de alta?
 - ordenador personal, empresa, gmail, hotmail, uc3m, foros, etc.
- ¿Cuántas contraseñas diferentes utilizamos?
 - Baja seguridad
 - Alta seguridad

Caducidad

- ¿Cada cuanto las cambiamos?
 - Cuando reinstalamos
 - Cada mes :-P

Robustez

- ¿Aleatorias?

Número de contraseñas

- ¿En cuantos servicios estamos dados de alta?
 - ordenador personal, empresa, gmail, hotmail, uc3m, foros, etc.
- ¿Cuántas contraseñas diferentes utilizamos?
 - Baja seguridad
 - Alta seguridad

Caducidad

- ¿Cada cuanto las cambiamos?
 - Cuando reinstalamos
 - Cada mes :-P

Robustez

- ¿Aleatorias?

Número de contraseñas

- ¿En cuantos servicios estamos dados de alta?
 - ordenador personal, empresa, gmail, hotmail, uc3m, foros, etc.
- ¿Cuántas contraseñas diferentes utilizamos?
 - Baja seguridad
 - Alta seguridad

Caducidad

- ¿Cada cuanto las cambiamos?
 - Cuando reinstalamos
 - Cada mes :-P

Robustez

- ¿Aleatorias?

Número de contraseñas

- ¿En cuantos servicios estamos dados de alta?
 - ordenador personal, empresa, gmail, hotmail, uc3m, foros, etc.
- ¿Cuántas contraseñas diferentes utilizamos?
 - Baja seguridad
 - Alta seguridad

Caducidad

- ¿Cada cuanto las cambiamos?
 - Cuando reinstalamos
 - Cada mes :-P

Robustez

- ¿Aleatorias?

Número de contraseñas

- ¿En cuantos servicios estamos dados de alta?
 - ordenador personal, empresa, gmail, hotmail, uc3m, foros, etc.
- ¿Cuántas contraseñas diferentes utilizamos?
 - Baja seguridad
 - Alta seguridad

Caducidad

- ¿Cada cuanto las cambiamos?
 - Cuando reinstalamos
 - Cada mes :-P

Robustez

- ¿Aleatorias?
 - Terminaciones por meses (01-12)
 - Palabras diccionario

Número de contraseñas

- ¿En cuantos servicios estamos dados de alta?
 - ordenador personal, empresa, gmail, hotmail, uc3m, foros, etc.
- ¿Cuántas contraseñas diferentes utilizamos?
 - Baja seguridad
 - Alta seguridad

Caducidad

- ¿Cada cuanto las cambiamos?
 - Cuando reinstalamos
 - Cada mes :-P

Robustez

- ¿Aleatorias?
 - Terminaciones por meses (01-12)
 - Palabras diccionario

Número de contraseñas

- ¿En cuantos servicios estamos dados de alta?
 - ordenador personal, empresa, gmail, hotmail, uc3m, foros, etc.
- ¿Cuántas contraseñas diferentes utilizamos?
 - Baja seguridad
 - Alta seguridad

Caducidad

- ¿Cada cuanto las cambiamos?
 - Cuando reinstalamos
 - Cada mes :-P

Robustez

- ¿Aleatorias?
 - Terminaciones por meses (01-12)
 - Palabras diccionario

Número de contraseñas

- ¿En cuantos servicios estamos dados de alta?
 - ordenador personal, empresa, gmail, hotmail, uc3m, foros, etc.
- ¿Cuántas contraseñas diferentes utilizamos?
 - Baja seguridad
 - Alta seguridad

Caducidad

- ¿Cada cuanto las cambiamos?
 - Cuando reinstalamos
 - Cada mes :-P

Robustez

- ¿Aleatorias?
 - Terminaciones por meses (01-12)
 - Palabras diccionario

pwman

- Línea de comandos
- Linux

pwsafe

- Parecida al pwman

Password-Gorilla

- Multiplataforma
- Interfaz gráfica

Parte III

Cifrado de ficheros

Mcrypt

- Disponible en todas las distribuciones linux
- Funcionamiento
 - `mcrypt [-a algoritmo] archivo`
 - Introducir contraseña
 - `mdecrypt archivo.nc`
 - `mcrypt -list`

Shred

- Borrado seguro
 - `shred -n 10 -u -z -v fichero`
 - Shredder Service Menu en KDE

Parte IV

Cifrado de sistema de ficheros

Tipos

- Partición
- Caja fuerte

Herramientas

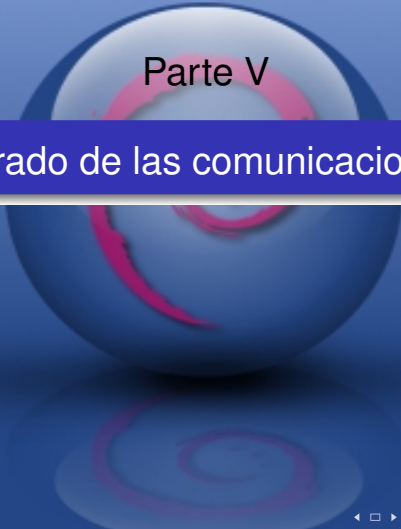
- Cryptoloop
- Loop-AES
- Dmccrypt
- Truecrypt

Dmccrypt

- Soporte en el kernel
 - Device Mapper Support + Crypt target support
 - AES cipher algorithms
- Crear el volumen (si no es una partición)
 - `dd if=/dev/urandom of=cajafuerte bs= 1k count=100000`
- Utilizar el volumen
 - `losetup /dev/loop/0 cajafuerte`
 - `cryptsetup -y create mycrypt /dev/loop/0`
 - `dmsetup ls`
 - `mkfs.ext2 /dev/mapper/mycrypt` (elegir sistema de ficheros)
 - `mount /dev/mapper/mycrypt /mnt`
 - Se lee/escribe
 - `umount /mnt`
 - `cryptsetup remove mycrypt`

Truecrypt

- Herramienta gráfica
- Multiplataforma
- Volumen oculto



Parte V

Cifrado de las comunicaciones

SSL

- Módulo Apache
- openssl
- Autoridad de certificación
 - CA.pl / openssl
- Aumento tráfico en la red

GNUPG

- Crear par de claves
- Exportar clave
 - `export GPGKEY=<Key-Id>`
 - Opcional
- Formato ASCII
 - `gpg --export -a <Key-ID> > mykey.asc`
- Hacer copia de seguridad de las claves
 - Pendrive + contenedor cifrado

GPA

- Interfaz gráfica para GPG

FireGPG

- Módulo Firefox
- Soporte GPG para gmail

Parte VI

Referencias

Referencias

- Criptografía y Seguridad en Computadores (Manuel J.Lucena)
- <http://www.openssl.org/>
- <http://getfiregpg.org/>
- <https://help.ubuntu.com/community/FolderEncryption>
- <https://help.ubuntu.com/community/EncryptedFilesystems>
- <https://help.ubuntu.com/community/GnuPrivacyGuardHowto>
- <https://help.ubuntu.com/community/GPGKeyOnUSBDrive>