

Taller de Criptografía Aplicada

# Sistemas de Ficheros Cifrados

Andrés J. Díaz <[ajdiaz@gpul.org](mailto:ajdiaz@gpul.org)>

# ¿Por qué cifrar un FS?

---

- Los permisos del FS no son suficientes
  - Peligro: Modo single
  - Peligro: Comprometida clave root
  
- Los ficheros cifrados tienen limitaciones
  - Peligro: ¿dónde se almacena la clave privada?
  - Peligro: ¿dónde se encuentra el programa cifrador?
  - Peligro: ¿está cifrada la estructura de directorios?
  
- Los dispositivos móviles tienen peligros:
  - Peligro: Hurto del dispositivo
  - Peligro: Extravío del dispositivo
  
- Es más fácil que cifrar fichero a fichero

# ¿Qué necesitamos?

---

- Kernel 2.4 + cryptloop-patch
- Kernel 2.6
- losetup modificado (loop-aes-utils)
- mount :-)

# Configuración del kernel (I)

---

Device Drivers

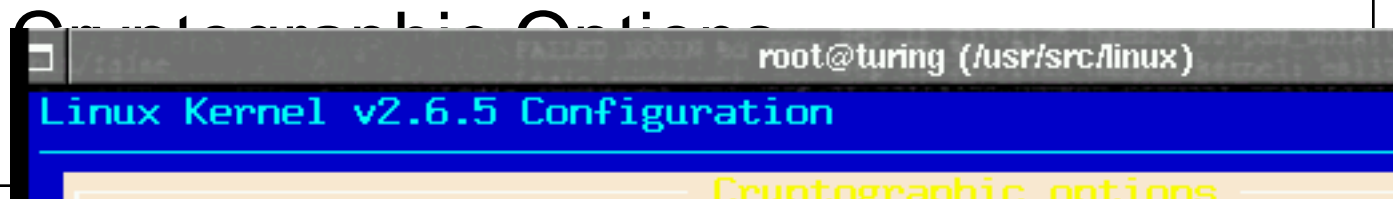
root@turing (/usr/src/linux)

Linux Kernel v2.6.5 Configuration

Block devices

# Configuración del kernel (y II)

---



A terminal window titled "root@turing (/usr/src/linux)" showing the "Linux Kernel v2.6.5 Configuration" menu. The current selection is "Cryptographic options".

```
root@turing (/usr/src/linux)
Linux Kernel v2.6.5 Configuration
Cryptographic options
```

# Creando el sistema de ficheros

---

## Pasos

- Rellenar el dispositivo con bytes aleatorios
- Enlazarlo a una interfaz de loopback
  - Ciframos la interfaz en el proceso
- Creamos el FS (mkfs.ext2, por ejemplo)
- Desenlazamos la interfaz

## ¿Qué utilizaremos?

- dd: Para rellenar el dispositivo
- losetup: Para gestionar la interfaz

[DEMO]

## Montando el FS

---

A "pelo":

```
mount -t ext2 -oencrypted=aes-256 device mntpt
```

Transparente:

- Editamos el fstab, añadiendo la opción encrypted

**[DEMO]**

# Comparativa

---

## Problemas de un CryptoFS:

- Más lento
- Incómodo (necesitamos proporcionar contraseña)

## Ventajas:

- Seguro
- Muy seguro



# URLs

---

## Cryptoloop HOWTO

□ <http://www.tldp.org/HOWTO/Cryptoloop-HOWTO/>

## Linux Kernel

□ <http://www.kernel.org>

## Rijndael

□ <http://www.esat.kuleuven.ac.be/~rijmen/rijndael/>

**¡GRACIAS!**  
(aplausos y preguntas)

