Hechos, mitos y realidades sobre criptografía: relación con soberanía tecnológica

Antonio Araujo Brett[1] Víctor Bravo[1]

[1]Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres
Nodo Mérida

CENDITEL, 2008

Licencia de Uso

Agenda

Fallas de Seguridad son ataques internos

Hecho o Mito: ¿Muchas fallas seguridad son producto de complejidad interna?

Fallas de Seguridad son ataques internos

Hecho: $\approx$ 75% de ataques tienen un componente interno

Fallas de Seguridad son ataques internos

Hecho: $\approx$ 75% de ataques tienen un componente interno

¿Porqué?

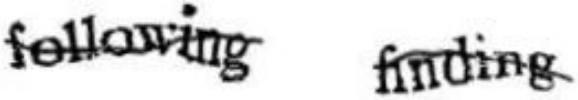
- Conocimiento del Entorno
- Intenciones (p.e. Empleado disgustado)
- Factor Humano (Acceso físico, olvidos, etc.)

Inicios de la Seguridad de la Información

- Aparición de la criptografía
- Lógica Computacional, Maquina de Turing
- Computador Enigma (Segunda Guerra Mundial)
- Principal objetivo: Sistemas Operativos, Acceso Físico
- CAPTCHA

Un poco de historia...

- Algoritmos de Cifrado Simétricos: DES, 3DES, AES
- Algoritmos de Cifrado asimétricos, DSA, RSA
- Aparición de criptosistemas: p.e. OpenSSL
- Applied Cryptography, Bruce Schneier (1996)
- CAPTCHA



La Seguridad de la Información hoy

- Énfasis en la gestión de Vulnerabilidades (Propietario vs. Libre)
- Uso masivo de autenticación basada en contraseñas
- Seguridad en la Web: Virus,Phising, SPAM, Scripting
- Utilización de Infraestructura de Clave Pública para la Web (viene del sector bancario)
- Técnicas Forenses (pruebas digitales)

Investigación en La Seguridad de la Información

- Formas de Autenticación: `Saber si soy el que digo ser`
- Eliminación de Carga para el usuario
- Amenaza para la Web
- Hacker ético
- Técnicas Forenses

Preguntas, Dudas y Comentarios

¿?