Autenticación & Encripción más allá de los passwords

Cómo conservar información sensitiva lejos del alcance de los enemigos

Presentado por:
Armando Carvajal

Contenido de la charla

- Conceptos básicos
- Problemática
- Impacto Financiero
- Impacto en el modelo de seguridad
- Tecnologías en desarrollo
- Propuesta de solución
- Conclusiones, Bibliografía

Conceptos Básicos

Encripción

- Criptografía: Del griego krypto (esconder) y grapho (escribir)
- Criptosistema: Método secreto de escritura
- Las disciplinas Criptografía y Criptoanálisis forman una nueva disciplina llamada Criptología
- Criptografía: Es el diseño de cifras
- Criptoanálisis: Se encarga de romper las cifras

Algoritmos de flujo simétricos

- DES: Cifra bloques de 64 bits (8 carácteres) y utiliza claves de 56 bits
- AES de 56 bits: Estándar de encriptación avanzado que reemplazó al algoritmo DES

Autenticación

- Autenticación es sinónimo de confidencialidad
- La autenticación fuerte incluye tokens o USB con claves de 64 caracteres
- Lo ideal al autenticarse: Algo que el usuario posee (la usb, el token), algo que el usuario conoce la clave y el usuario.

Problemática

Vulnerabilidades de Windows

- Vulnerabilidad de XP: Arranque con disco NTFS, DOS y Knoppix tiene acceso al disco completo NTFS
- Vulnerabilidad de acceso a disco XP: Al Iniciar con disco de W2000 y entrar a la consola de recuperación. Se tiene acceso total al disco
- Sacar un disco duro y colocarlo como esclavo en un segundo equipo: Nuevamente se tiene acceso completo
- Múltiples Puertas traseras

Vulnerabilidades internas

- Empleado que lleva el computador a su casa y se lo roban
- El administrador de la red que entra a cada equipo sin dejar rastro
- Usuarios curiosos que conocen alguna debilidad del sistema operativo
- Empleados que conocen los procesos internos de la organización

Los sistemas operativos de hoy

- No hacen encriptación de los contenidos
- No hacen encriptación de los archivos adjuntos de los correos electrónicos
- No encriptan archivos, carpetas o el disco duro
- No hay políticas de encriptación por extensión de archivo
- No hay políticas de encriptación por empresa o por grupos de empleados de la organización

Impacto Financiero

Impacto Financiero

- Una empresa que su fuerza de ventas usa portátiles o PDA
- Cuánto le cuesta a la organización el robo de la información de un portátil que moviliza el empleado?

Ej: Equipos robados en España para el período 2004

Impacto en el Sistema de Seguridad

Recordemos: Propiedades de un sistema de información

- **Confidencialidad:** Los recursos del sistema sólo pueden ser accedidos por los elementos autorizados
- **Integridad:** Los recursos del sistema sólo pueden ser modificados o alterados por los elementos autorizados
- **Disponibilidad:** Los recursos del sistema deben permanecer accesibles a los elementos autorizados

Qué variables afecta

- Confidencialidad: Una entrada no autorizada al portátil robado pone en riesgo información privada
- Integridad: la información es modificada o alterada por un usuario no autorizado. Fórmulas de nuestro negocio en la competencia
- Disponibilidad: El usuario Móvil generalmente no hace backups, los datos del portátil no son accesibles por los usuarios

Tecnologías en desarrollo

Tecnologías

- AES: Estándar Avanzado de encripción que reemplaza a DES
- IDEA: Algoritmo de encripción de datos internacional
- OpenSSL: Laves públicas o asimétricas
- Open PGP: Llaves públicas a nivel de aplicaciones en el modelo OSI

Propuesta de solución

Safeboot

- Control de Acceso a computadores: Autentificación del usuario en "preboot", es decir, antes del acceso al área de trabajo del disco y antes de la carga del sistema operativo
- Encriptación de Disco Duro: Encriptación, ultrarápido en tiempo real, de los medios magnéticos disponibles (disco duro, disquetes, cintas, zip...)
- Encriptación de Archivos y carpetas: Transparente, persistente y obligatoria de Archivos y Carpetas en su dispositivo o fuera del dispositivo como las Unidades Removibles USB, Servidores de Archivos centrales

Safeboot

- Administración Centralizada: La administración centralizada permite un fácil sistema de configuración y puesta en marcha
- La instalación de clientes de una forma segura y centralizada
- Permite manejar consolas de administración distribuidas, sub-administradores del sistema son capaces de administrar en forma restringida

Safeboot

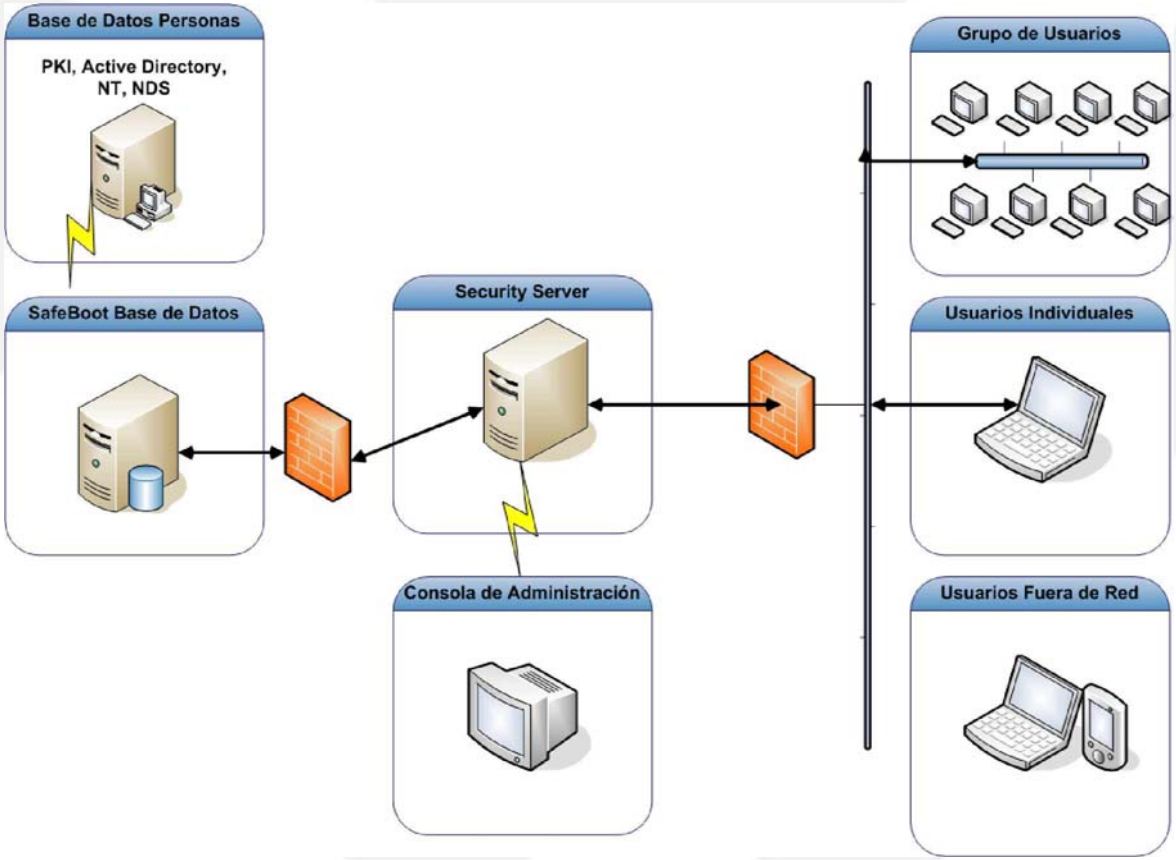
- En caso de olvido de password SafeBoot cuenta con un procedimiento rígido que permite reiniciar el password de una forma 100% segura a través de la misma consola o por medio de una página web que trae incorporada

Safeboot

- Control de acceso a equipos por horario
- Control y bloqueo de programas
- Control de la calidad del password
- Auditoría centralizada de eventos de seguridad

Mayorista de Valor Agregado

Arquitectura



Conclusiones

- Robo o pérdida de Computador:

- Si alguien roba el computador de la empresa o se roban o pierden los discos duros SafeBoot mantendrá su información 100% protegida mediante la encriptación del sistema con el criptosistema AES

Conclusiones

Intento de Fuga de Información:

- Si alguien intenta sacar de la empresa documentos electrónicos, fotos, audio o videos protegidos por SafeBoot seguirán protegidos
- La tecnología llamada Encriptación Persistente mantiene los documentos encriptados incluso cuando salen del área de la empresa haciendo completamente ilegible la información

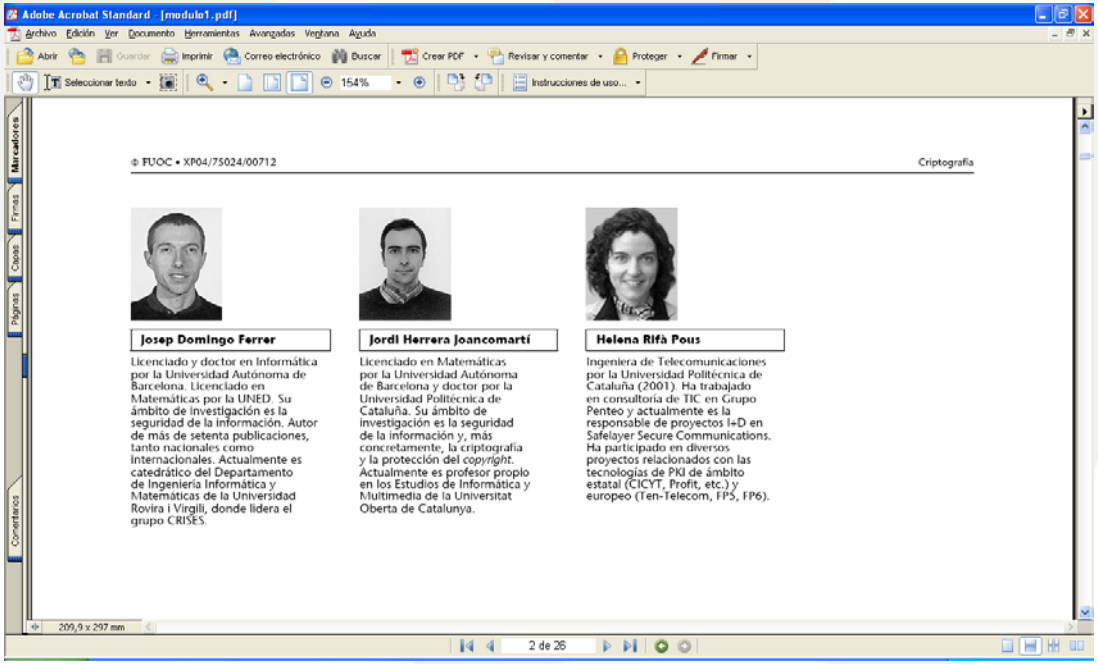
Conclusiones

- Compartir información importante:
- Compartir información ya no será un riesgo

  SafeBoot puede compartir información entre un grupo determinado al interior de su empresa evitando que alguien la lea por equivocación inclusive de los administradores de red de Microsoft

Bibliografía

- http://www.safeboot.com
- http://www.uoc.edu, Módulo de Criptografía en la maestría seguridad en redes de la Universidad Oberta de Cataluña



Gracias por su atención

Más información en www.mvaonline.com
Email: info@mvaonline.com

Lo esperamos en el área de Exhibición a las 6:00 PM