Nuevas actuaciones

- Sistema de auditor'ias.
- Discusión en CERT-ES recomendaciones de seguridad.
- Colaboración en Proyectos fin de carrera.
- Proyecto CA-PGP.
- Encuesta de seguridad
- Validación de correos en listas
- ¿Mas ideas ?

Auditor'ias

- ubicado en las páginas WWW de RedIRIS, como piloto.
- Instituciones pequeñas (no clases B ;-)
- Análisis de Equipos conectados y vulnerabilidades evidentes.
- Superficial.
- Informe "privado" a la institución solicitante.

CERT-ES y recomendaciones de seguridad

CERT-ES: mas de 800 subscriptores.

Lista de seguridad alojada en RedIRIS.

Recomendaciones: Documento con información sobre configuración de seguridad.

Idea: Emplear lista CERT-ES para comentar y mejorar el documento.

1. Envio por parte de un "encargado" de una sección.

2. Discusión y comentarios en la lista

3. Elaboración de un documento definitivo.

Colaboración con centros en proyectos fin de carrera

Objetivos:

- Facilitar el desarrollo de proyectos a alumnos de enseñanzas técnicas (informática y telecomunicaciones).

- Poder reutilizar estos proyectos para mejorar los servicios de la Comunidad RedIRIs

Esta colaboración se realizará en principio a nivel personal entre los técnicos de RedIRIS y Centros interesados.

Proyectos de seguridad

- Sistema de Voto electrónico.
- Servidores de clave experimentales.
- Construcción de proxys para diversos protocolos (SMB, RPC,etc).
- Auditor'ias informáticas.
- Detecci'on de intrusión en Red (IDS)
- Drivers de dispositivos Hardware Criptogr'aficos.
- etc...

CA-PGP

Idea: Montar y experimentar con “redes de certificación” basadas en PGP.

No esta pensado como estructurar paralela al piloto de certificación de RedIRIS IRIS-PCA, ya que los requisitos para la participación van a ser mucho más “relajados” .

- En plan directamente experimental, sin responsabilidad directa.

- Empleo de PGP =¡5.0 o Gnupg (por revocaciónes de identidades)

- Servidor de claves “controlado” .

- Proporcionar mécanismos de validación al usuario final.

Estructura de certificación

Piramidal (como en X509)

Dos enfoques a escoger.

- Distribución de claves de CA a cualquier organismo (¿org==CIF?).

- Distribución geográfica

Los agentes de Registro son “ca”.

Las claves de CA son claves PGP con un identificador especial.

```
Type Bits KeyID      Created    Expires    Algorithm
sec  1024 0x69696969 2000-03-17 2001-01-12- RSA
uid  CA: Ca Raiz de la organización.
```

Servidor de claves “modificado”

Hace falta poder encontrar las claves de una forma “r’apida”: los servidores de claves son lo más apropiado.

Evitar que las claves “firmadas” salgan del servidor de claves (problemas con usuarios que pierden claves,etc) y que se puedan borrar sin problemas.

Servidor de claves modificado:

- Servidor HTTP modificado en vez de servidor de claves.

- Dos CGI.

    1. Actualización (POST): Deposita la clave en otro servidor oculto (redirección HTTP o reenv’io de datos).

2. Consulta: Consulta en el interior, si no hay nada se consulta al exterior.

3. Obtención de clave:

   (a) Se consulta en el exterior

   (b) se añada (actualización) al servidor de claves interno.

   (c) se consulta el servidor de claves interno y devuelve el resultado.

Con esto se consigue acceso a todas las claves, pero las modificaciones no se difunden al exterior.

Certificados de usuario

Certificado usuario == identificador de usuario firmado.

- Formato predefinido de certificado.
- Es posible "crear" una identidad PGP sobre una clave pública sin tener la clave privada.
- El usuario tiene después que firmar la identidad
- Inclusión de un hash con la información del DNI.

Comprobación de cadenas de certificación

Problema PGP

grafico:

Raiz

/ / CA CA / / CA Usuario1 — — Usuario2

Solución: Comprobación de CA': Script en servidor WWW.

Que falta por hacer

TODO y Poca cosa:

- Script de generación MD5 : 10-30 horas (varios sistemas).
- Script de validación de la raíz: 10-20 horas (CGI y Unix en principio).
- Keyserver modificado: 10 horas.
- Especifiación del sistema de CA: 20 horas.
- documentación usuario: 10 horas

Puesta en marcha en Septiembre (principios)

encuesta

Problema: falta de respuesta ante los grupos de IRIS-CERT, ¿Qué mas hace falta ?

Enviar una encuesta a los centros:

- Ver que medidas de seguridad se aplican.
- Ver que hace falta para mejorar el servicio.
- ¿Que se demanda por vuestra parte y por las organizaciones de IRIS-CERT

Envio de la encuesta a las listas de coordinación (IRIS-CERT) e instituciones

Validación automática de correos

Problema de envio automático de mensajes a listas de distribución.

- Aprobación sin intervención humana.
- Validación en función de criptografía de clave publica.
- Muy relacionado con la certificación ;-).

Otras muchas más

- Script de busquedas de contactos de seguridad.
- Script de gestión de claves X509v3.
- Prontuarios de seguridad.

Ruegos y preguntas