Una Introducción a la Seguridad en Sistemas Informáticos

J.A. Gutiérrez <jagutierrez@unizar.es>

¿Qué es "Problema de Seguridad"?

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

¿Los sistemas son seguros?

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

Razones para la inseguridad (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 sistemas.

Razones para la inseguridad (redes)

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

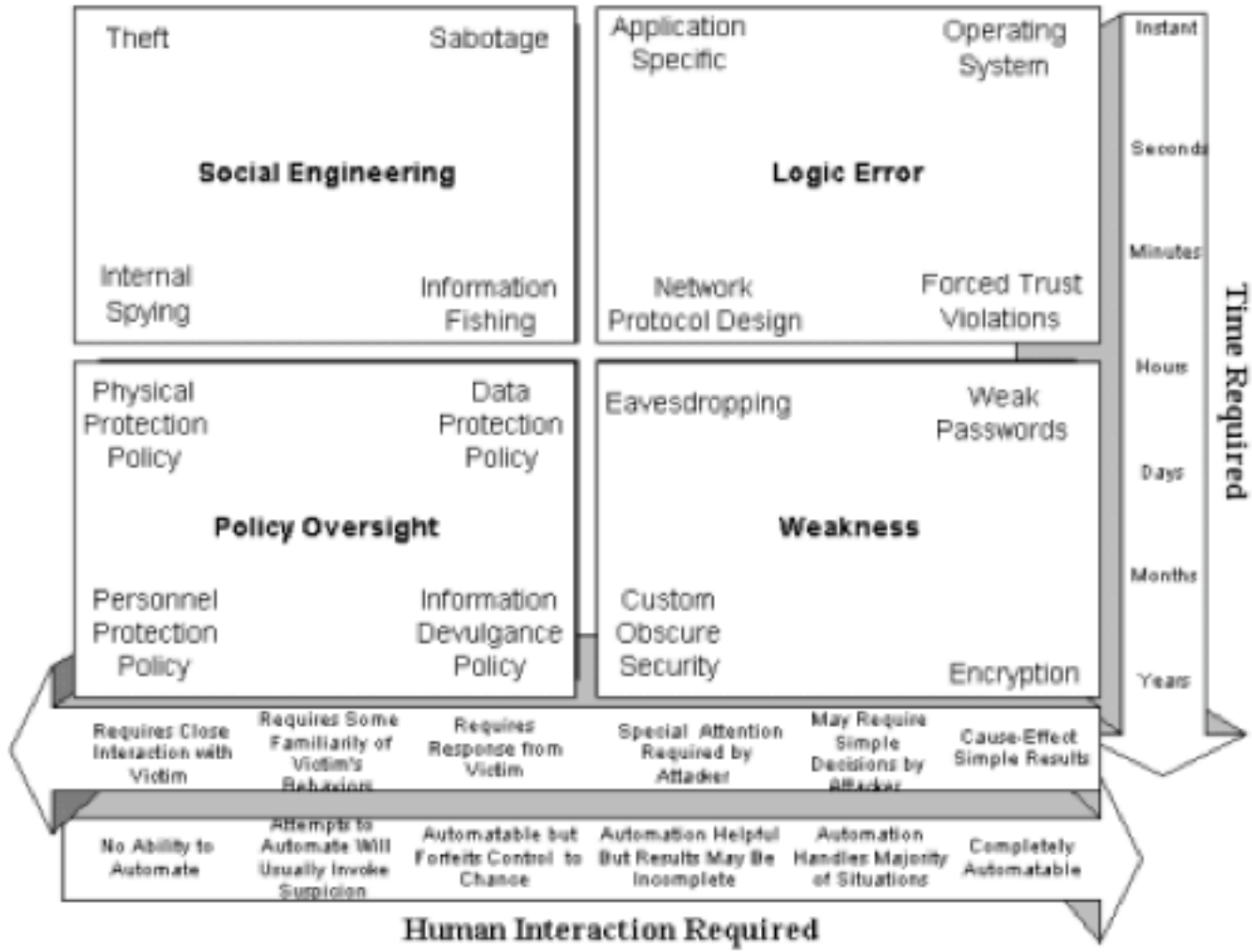
Razones para la inseguridad (sistemas)

- Instalaciones "por defecto" no pensadas para la seguridad.

Razones para la inseguridad (sistemas)

- Facilitar al máximo todo al usuario, automatización. Seguridad vs. Comodidad.
- Complejidad de los sistemas, interacciones no previstas.
- Sistemas "distribuidos"
- Históricamente, desconocimiento en temas de seguridad por parte de los programadores.

Tipos de problemas



- http://www.swordsoft.com/compvuln_draft.pdf

Problemas (por efecto)

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

Problemas (por acceso)

- Remoto anónimo.
- Remoto autentificado.
- Local autentificado.
- Local anónimo.

Problemas (Métodos)

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

Problemas (por atacante)

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

Fallos típicos

- 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.

Conceptos básicos

- Inglés.
- Programación. (teoría)
- Lenguajes de alto nivel. (S.O. - C)
- Ensamblador (varios).
- Manejo de sistemas operativos. (niveles usuario, programador y administrador)

Conceptos básicos

- Conocimiento de protocolos de comunicaciones.
- Conocimiento de aplicaciones típicas.
- Estudio de los fallos ya publicados.

Fallos típicos en Unix

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

Fallos 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

Evolución

- Ataques "personales" para controlar determinados recursos en concreto. Internos.
- Ataques aleatorios para usar recursos como puente.
- Ataques automáticos para realizar DoS distribuidos o bots de IRC.
- Ataques automáticos sin objetivo particular. Gusanos.

Seguridad a nivel de usuario.

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

Seguridad a nivel de usuario.

- Passwords seguros

Seguridad 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.

Seguridad a nivel de administración

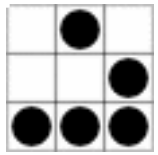
- Políticas de seguridad.
- Diseño estricto de la red y los servicios.
- Barreras de acceso.
- Copias de seguridad, recuperación ante desastres

Seguridad a nivel de administración

- Recuperación ante desastres.

Seguridad a nivel de administración

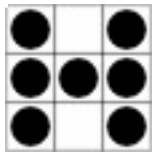
- Configuración correcta de la red.
- Cifrado de las comunicaciones.
- Protocolos seguros de autentificación.
- Medidas preventivas.
- Trampas (Honeypots)
- Departamento legal. Registros. LSSI.



Fauna. Hacker

- The world is full of fascinating problems waiting to be solved.
- No problem should ever have to be solved twice.
- Boredom and drudgery are evil.
- Freedom is good.
- Attitude is no substitute for competence.

http://www.catb.org/~esr/hacker-emblem/



Otros

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

http://www.jargon.org

Recursos

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

```
Memory fault
root@localhost# echo “cracker::0:0:I Own You:/:/bin/sh” >> /etc/passwd
root@localhost# id
uid=0(root) gid=0(root)
root@localhost# _
```