Retos de la privacidad y la intimidad en el siglo XXI

Alfredo Chirino

Intimidad e Internet

- Problemas:
  - Proliferación de las redes de comunicaciones y su uso cotidiano:
    - Banca electrónica
- Comercio electrónico: B2B y B2C
  - Dos graves amenazas:
    - Intimidad
    - Confidencialidad

Anonimato e Internet

- Rastro del uso de Internet:
  - Dirección IP
  - Navegador
  - Sistema operativo
  - Dirección de correo electrónico
  - Páginas visitadas, fotos vistas, documentos leídos, formularios, entre otros.

Anonimato e Internet

- Cookies: hábitos de navegación, gustos, otros.

 Petits et Maman

Necesidad de una “falsa personalidad”

- Evitar dar datos auténticos, en la medida en que el servicio recibido a cambio lo permita:
  - Crear una identidad ficticia: nombre y apellidos
- Dirección, edad, sexo, otros.
- Almacenar esta información en una tarjeta vCard.

Navegación anónima

- Filtro de seguridad entre su navegador y el sitio web que desea visitar.
  - Se conecta al anonimizador.
  - Introduce el URL de la página que desea.
  - Éste se adentra en la Red en busca de la página.
- Se la presenta en su navegador
- El sitio web registra la dirección del anonimizador y no la suya.

Correo y anonimidad

- Cuenta de correo web con servicios como Yahoo, Hotmail, Terra, MixMail, otros.
- Datos de la cuenta falsos.
- Dar de alta una docena de cuentas de correo web.

Correo y anonimidad

- Utilizar esas direcciones de correo recién obtenidas para:
  - Rellenar formularios cuando sea absolutamente necesario dar una dirección que funcione.
  - Participar en listas.
  - Escribir anónimamente.

El rastro de la navegación

- Amenazas:
  - Todos los internautas poseen e intercambian información confidencial.
  - Redes de escucha mundiales: Echelon, Enfopol, Carnívoro.
  - Hackers, intrusos, competencia, otros.
  - Defensa: criptografía.

Rastros en la World Wide Web

- El historial de navegación.
- Contiene la dirección de todas las páginas que ha visitado en el pasado.
- Permite a cualquier persona con acceso a su ordenador, bien sea físicamente o a través de Internet, obtener información detallada de qué sitios visitó y a qué hora.

Rastros en la World Wide Web

- En el caso de formularios, aparecerá incluso el contenido que se escribió en ellos.
- Barra dirección.
- Ejemplo de configuración.

Más rastros

- Caché del navegador.
- Almacena en el disco del usuario las páginas ya vistas, imágenes cargadas, programas, documentos, otros.
- Información que revela mucho acerca de sus gustos y de lo que ha estado haciendo en Internet.
- Ejemplo de configuración.
- Cambio de sitio.

El correo y sus rastros

- Almacén de correos electrónicos.
- Contiene todos los mensajes que ha enviado y recibido.
- Blanco típico de un atacante.
- Cambiándolo de sitio se burla el ataque.
- Ejemplo de configuración.

Los SSL como un medio de seguridad

- Protocolo de propósito general para establecer comunicaciones seguras.
- Propuesto en 1994 por Netscape Communications Corporation junto con su primera versión del Navigator.

Los SSL como un medio de seguridad

- Crea un canal blindado para transmitir los datos confidenciales desde el ordenador del cliente hasta el servidor.
- Solución de seguridad implantada en servidores de comercio electrónico.

Limitaciones del SSL

- Sólo protege transacciones entre dos puntos: el servidor web y el navegador.
- SSL carece de capacidad para completar el proceso comercial.
- No protege al comprador del riesgo de un comerciante deshonesto utilizando su tarjeta.
- Los comerciantes se encuentran indefensos.

Limitaciones del SSL

- Sólo garantiza la confidencialidad e integridad de los datos privados en tránsito.

La criptografía como un medio de defensa

- Claves cortas significan tiempos cortos para probar todas las posibilidades.
- Los navegadores estándar utilizan criptografía de 40 ó 56 bits de longitud de clave: criptografía de juguete.
- Longitud de clave de 128 bits, como mínimo.
- Ejemplo: certificados digitales.

Los certificados digitales

- En el mundo físico la identificación se realiza mediante la presentación de documentos acreditativos como el DNI.
- Contienen una serie de datos significativos vinculados al individuo.
- Verificación de la identidad de la persona por evaluación visual.
- En casos especiales, comparando su firma manuscrita.

Los certificados digitales

- Documento electrónico acreditativo.
- Firma electrónica: permite atestiguar la identidad del portador de este certificado y comprobar la validez de documentos.

Información incluida en los certificados

- El código identificativo único del certificado.
- La identificación del prestador de servicios de certificación que expide el certificado.
- La firma electrónica avanzada del prestador de servicios de certificación.

Información incluida en los certificados

- La identificación del signatario, por su nombre y apellidos o a través de un seudónimo que conste como tal de manera inequívoca.

Otras informaciones del certificado

- Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del signatario.
- El comienzo y el fin del período de validez del certificado, fuera de los cuales no podrá utilizarse.

Otras informaciones del certificado

- Los límites de uso del certificado.
- Los límites del valor de las transacciones para las que puede utilizarse el certificado.

Usos del certificado

- Acceso por medio del navegador a sitios web restringidos.
- Entrada en intranets corporativas y edificios.
- Firmar software para Internet: applets, ActiveX, otros.
- Confidencialidad en procesos con la administración.
- Transacciones comerciales seguras.

Correos y certificados

- Muy sencillo falsificar correos y manipular su contenido.
- Con los correos queda constancia de la dirección IP de la máquina que envió el correo.
- La firma digital previene ataques de suplantación y contra la integridad.

¿Cómo es posible proteger los secretos?

- Contraseñas.
- Ingeniería social.
- Cifrado de información confidencial.
- Cómo borrar a fondo.
- Mensajes de correo más seguros.
- Esteganografía.
- Cortafuegos.

Contraseñas

- Necesidad de docenas de contraseñas.
- Costumbre: contraseña única para todo.
- Si se compromete por ataque hacker, acceso a todos los servicios. Utilizar contraseña distinta para cada servicio: almacenarlas de forma segura.

La ingeniería social

- Técnicas de cracking destinadas a entrar en redes u obtener secretos, basadas en engañar a la gente para que revelen contraseñas y otra información confidencial. Apelan a las inclinaciones más profundas de la persona: el miedo, el deseo, la codicia o incluso la bondad. Hacerse pasar por administrador de un sistema o técnico de un proveedor de servicios de Internet.

El cifrado de archivos

- Cualquier persona con acceso físico a su PC podrá leer su contenido.
- Hackers podrían acceder a su disco duro a través de Internet.
- La mejor defensa: el cifrado.
- PGP.

El borrado seguro

- Cuando borra un fichero, éste no desaparece físicamente.
- El puntero es liberado, mientras que la información a que apuntaba permanece hasta ser sobrescrita por otro fichero.
- Rastro de información en el disco duro.
- Utilidades de borrado seguro.

Correspondencia segura

- Correo web también cifrado.
  - HushMail.
- Mensajes que se autodestruyen al ser leídos.
  - 1on1mail: destruye los mensajes inmediatamente después de que el lector los lea.

Correspondencia segura

- Mensajes de correo disimulados dentro del spam.
- Spam Mimic.

Esteganografía

- Transmisión de información de forma inadvertida u oculta.
- Ocultar mensajes en recipientes u otros mensajes aparentemente inofensivos, de los que nadie sospecharía como portadores de información secreta.

Esteganografía

- Dentro de música, texto, vídeo, imágenes...
- Aplicaciones en marcas de agua y copyright.

Conclusiones

- Internet abre a las puertas al flujo bidireccional de información.
- Las nuevas tecnologías pueden transformar el mundo en una gran cámara de vigilancia electrónica.
- Numerosos productos y técnicas que nos ayudan a protegernos.

Referencias

- Álvarez, G. (s.f.). Internet segura para todos los usuarios.
- Base de datos de legislación.
- Conocimientos del autor.
- Protocolos de Internet.