Seguridad en Servicios Web

Eduardo Vela - sirdarckcat@google.com

Quien soy yo?

- Estudie (sin terminar) la carrera de Ingeniería en Sistemas en el Tec de Monterrey (Edo de México).

  •He trabajado en hi5.com en México, alibaba.com en China y (ahora) en google.com en Estados Unidos

- Me gusta viajar, he presentado investigaciones en diversas conferencias alrededor del mundo..

- Publique un libro a finales del año pasado, estoy trabajando en otro.

Aviso

No vengo a hablar en representacion de Google, lo que diga es mi opinion personal.

De que voy a hablar en 20 minutos?

De servicios web (aplicaciones que viven en la nube) y navegadores.

- **The good**
  - Las ventajas que tienen los servicios web.
- **The bad**
  - Los problemas que hoy en dia ponen tus datos en peligro.
- **The ugly**
  - La forma en la que se estan abusando los problemas.

The good

- **Servicios Web**
- Correo
- Calendario
- IM
- Video Conferencia
- Ofimática
- Sitios web
- Blogs
- Compras
- Mapas
- Juegos
- Videos
- Música
- etc..

Servicios Web

- Usan HTML/CSS/JS y otras tecnologías para presentarte la interfaz a la aplicación.
- Todo se almacena en la nube.
- Puedes acceder a los servicios desde cualquier computadora, desde cualquier lugar del mundo.
- Requieren conexión a internet para trabajar correctamente (aunque hay excepciones).

Seguridad en la tierra

- **Cuando instalas un programa en tu computadora, este tiene acceso a todos tus archivos, y programas ☹.**

- **Las vulnerabilidades que afectan estas aplicaciones involucran que alguien puede ejecutar un programa en tu computadora sin tu permiso.**

- **Incluso hoy en día, los virus y troyanos hacen esto mas que nada, para robar tu información y usar tu computadora para atacar otras computadoras.**

Seguridad en la nube

- **Cada sitio web es como una aplicación. Y cada aplicación solo tiene acceso a sus propios datos (www.juegos.com no puede leer la información de www.banco.com).**

- **Las vulnerabilidades que afectan aplicaciones web, son las que permiten a un sitio web maligno:**

•Leer información de otros sitios.
•Modificar información de otros sitios.
•Acceder a información no autorizada.

- **Los sitios web usan *passwords*, *OTPs*, certificados, y *cookies* para validar la identidad de los usuarios.**

The bad

- **Cualquier problema de seguridad puede poner tus datos en riesgo, ya sea:**
  - El servidor.
  - La aplicación web.
  - La red.
  - Tu navegador.
  - Tu sistema operativo.
- **Proteger tu información significa proteger todas las capas donde puede haber problemas.**

Seguridad en el servidor

- La mayoría de las veces, en aplicaciones web, son cientos o miles de servidores trabajando simultáneamente.
- La seguridad de los servidores depende de los administradores de sistemas.
- Se deben aplicar políticas de seguridad que protegen los servidores de amenazas externas (solo exponer los servicios deseados).

Seguridad en la aplicación web

- Las aplicaciones web son programas que se comunican con tu navegador usando HTTP.

- La seguridad de la aplicación web depende de los programadores, y las librerías usadas para desarrollar el programa.

- El diseño y código deben ser auditados por problemas de seguridad para minimizar el riesgo de que tengan problemas.

Seguridad en tu navegador

•La seguridad en tu navegador protege varias cosas:

•El cifrado (en su caso) entre navegador y servidor.
•Que el código corriendo en un sitio, no pueda acceder a otro.
•Que el código que una web ejecuta, no pueda comprometer la seguridad del sistema operativo.

•La seguridad de tu navegador depende de que tan a menudo se actualice, del diseño y calidad del código del mismo.

The ugly

En las Noticias

- **Vulnerabilidad en Facebook permite revelar contenido privado de otros usuarios.**
- **Vulnerabilidad en IE 6/7/8 (MHTML) usada para acceder a cuentas de activistas políticos.**
- **Vulnerabilidad en Live Mail permite cambiar *password* de otros usuarios.**
- **Se detectan ataques de *phishing* contra empleados del gobierno koreano y norteamericano.**
- **Usuarios de Iran encuentran certificados falsos SSL al usar Google.**

Problemas

- **Principales problemas de seguridad que afectan servicios web.**
  - Cross Site Scripting
  - Cross Site Request Forgery
  - Logic Flaw
  - Problemas de seguridad en navegadores / plugins
  - Personas
- **No son específicos de ningún proveedor, la mayoría tiene problemas en la misma medida.**

Problemas

Cross Site Scripting

•Si en un sitio web, un servicio tiene una vulnerabilidad de XSS, todos los servicios hospedados en ese sitio son afectados.

•Una vulnerabilidad de XSS le permite a un atacante tomar control de todos los servicios en un sitio web.

•La mejor manera de proteger un servicio contra XSS es aislándolo de otros servicios lo mas posible (mail.proveedor.com vs. www.proveedor.com/mail).

Problemas

Logic Flaw

•Una aplicación le permite a un usuario acceder a la información de otro usuario.

•La mejor manera de proteger contra problemas de este tipo es el uso consistente de librerías que se encargan de controles de acceso.

•Similar a este, CSRF es un ataque que le permite a un sitio web iniciar acciones a otro sitio web sin la autorización del usuario.

Problemas

Navegadores

•Una vulnerabilidad en un navegador o *plugin* hace posible a un atacante robar información de cualquier sitio, o ejecutar código en la computadora del usuario.

•Mantener navegadores actualizados permite a usuarios permanecer seguros, pero existen vulnerabilidades que son explotadas cuando aun no existe un parche.

•El diseño del navegador puede hacer estos problemas mas difíciles de explotar.

Problemas

Personas

•Los seres humanos aun son la principal vulnerabilidad en los servicios.
•Phishing
•Ingenieria Social
•Malware
•Falta de actualizaciones

•Mas empresas y usuarios son comprometidos diariamente por phishing que por explotar todas las vulnerabilidades antes mencionadas juntas.

Y ahora que?

En los proveedores de servicios de cloud computing mayores (Microsoft, Amazon, Google):

- **Las servicios web viven en servidores que son monitoreados 24/7 por cientos de ingenieros.**

- **Las aplicaciones web son desarrolladas por desarrolladores y auditadas por ingenieros de seguridad.**

- **Los datos son cifrados usando algoritmos que protegen la confidencialidad de los datos.**

El Fin!