

Evolución de la seguridad en aplicaciones de comercio electrónico

Dr. Gonzalo Álvarez Marañón

Quién

- o Investigador en criptografía y criptoanálisis en el CSIC
- o Creador del **Criptonomicón**
- o Auditor de seguridad de aplicaciones web
- o Autor de los libros **Los mejores trucos para Internet** y **Seguridad informática para empresas y particulares**
- o gonzaloalvarez.com



Qué

- I. Un poco de historia
- II. Bienvenido al mundo real, Neo
- III. Pero, ¿qué son los ataques web?
- IV. ¿Medidas de protección?
- V. Conclusiones

Cuándo



o Definición

- Distribución, compra, venta, marketing de servicios y productos a través de sistemas electrónicos: Internet
- o Años **70**: Electronic Data Interchange (EDI)
- o Años **90**: servidores web seguros con carritos de la compra y pagos con tarjeta de crédito
- o **1998-2000**: El boom de las punto com
- o **2000-2001**: El crack de las punto com
- o **2004+**: Reaparecen las viejas formas de delito: picaresca, extorsión, fraude, crimen organizado

Cree lo increíble

- Comercio electrónico = Aplicación web
- El mundo real **no** es lo que nos han enseñado a creer
 - Cortafuegos
 - SSL
 - Bastionado/Parches
 - Arquitectura segura de red
 - Auditorías de seguridad



Cortafuegos

- Aísla la red privada de Internet
- Sólo se permite acceso a unos servicios y el resto se prohíbe



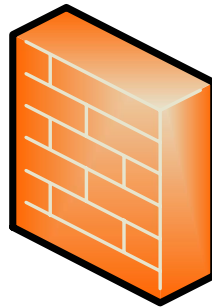
Cortafuegos

o Ventajas

- ▣ **Sólo** deja abiertos puerto 80 y 443
- ▣ Detiene algunos ataques **DoS**

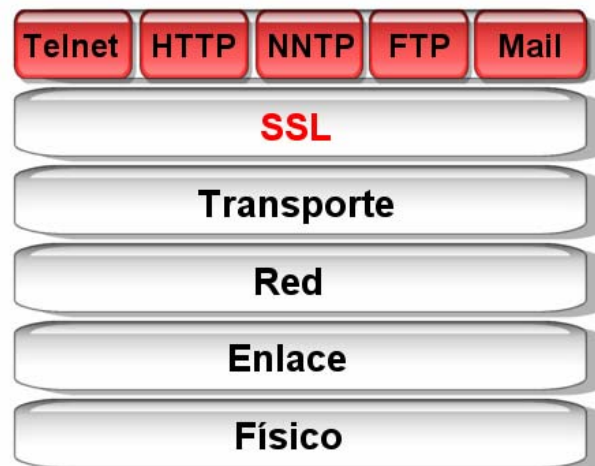
o Limitaciones

- ▣ No entienden el significado de **HTTP**
- ▣ Dejan pasar el **100%** de los ataques web



SSL

- Confidencialidad: cifrado de datos
- Integridad de mensajes
- Autenticación de servidores mediante certificados
- Autenticación de cliente con certificados (opcional)



SSL

o Ventajas

- ❑ **Cifra** el contenido de las comunicaciones: **canal** seguro
- ❑ Permite **autenticar** servidores (y clientes)

o Limitaciones

- ❑ Sólo protege los datos en **tránsito**, no en origen ni destino
- ❑ Los ataques web **pasan** cifrados, pero pasan
- ❑ No proporciona un **mecanismo de pago** seguro
- ❑ Dificulta la labor del **IDS**



Bastionado/Parches

- o **Bastionado** de la plataforma
 - **SO** Eliminación de servicios innecesarios, configuración de permisos, eliminación de archivos, etc.
 - **Web** Eliminación de extras, borrado de aplicaciones de ejemplo, configuración segura, etc.
- o Aplicación de **parches**
 - Solucionan vulnerabilidades descubiertas en los productos
 - Actualización religiosa de parches



Bastionado/Parches

o Ventajas

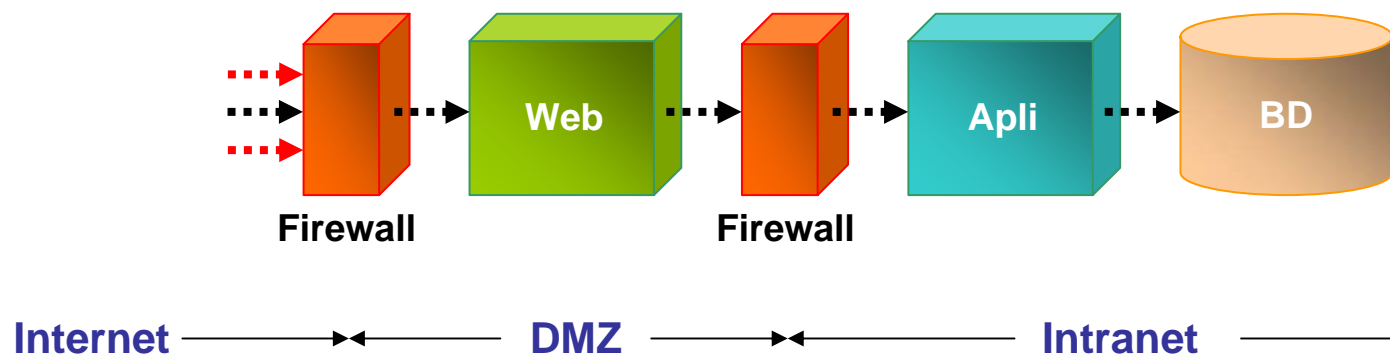
- ❑ **Fácil** bastionar: listas de comprobación, herramientas automatizadas, etc.
- ❑ **Fácil** actualizar: herramientas de gestión de actualizaciones
- ❑ Evitan ataques ya conocidos y solucionados

o Limitaciones

- ❑ Los parches llegan **tarde** y no solucionan el **mal** hecho
- ❑ Las aplicaciones web **no** se parchean
- ❑ La mayoría de ataques web no explotan agujeros de la plataforma, sino de la aplicación

Arquitectura segura de red

- o **Separación** por funcionalidad → separación de amenazas



Arquitectura segura de red

o Ventajas

- Será (casi) imposible acceder **directamente** a la BD

o Limitaciones

- Existen caminos **indirectos** para acceder a la BD a través de la aplicación
 - Inyección de **SQL**
 - Manipulación de **sesiones**
 - Acceso a los **logs**



Auditorías de seguridad

- Auditorías automatizadas **periódicas**
 - ❑ SO, Red, BD, Web
 - ❑ Con herramientas automatizadas: Nessus, WebInspect, AppScan
 - ❑ Solucionan la **mitad** del problema
- Auditorías manuales externas **puntuales**
 - ❑ Caja negra/gris/blanca
 - ❑ Completas
 - ❑ Solucionan el problema **una** vez



Auditorías automatizadas

- Las máquinas **no** son perfectas
 - Nunca encontrarán todos los agujeros (tampoco los humanos)
 - Algunos análisis no se pueden automatizar
 - Las aplicaciones se defienden contra las máquinas
 - Crean muchos falsos positivos



Auditorías de seguridad

o Ventajas

- Independencia
- Experiencia en seguridad

o Limitaciones

- Precio muy elevado
- Los sitios web cambian frecuentemente
- Sólo se realizan una vez

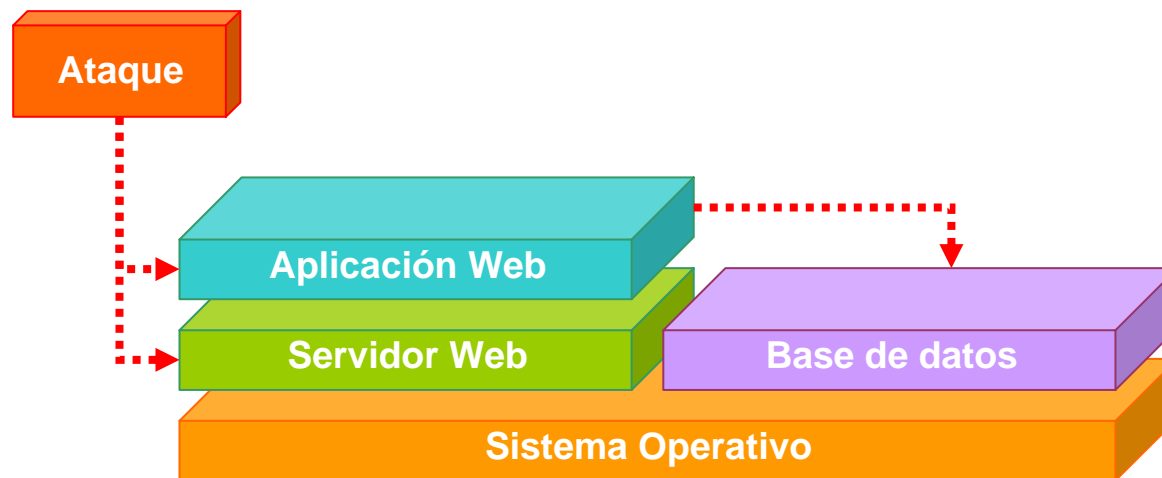


1 semana después

1 año después

¿Qué son los ataques web?

- Vulnerabilidades en la aplicación web: .NET, J2EE, PHP, etc.
- Vulnerabilidades en el servidor web: Apache, IIS, Tomcat, WebLogic, WebSphere, etc.



Estudio de vulnerabilidades

○ Técnicas

- ❑ Gestión de errores
- ❑ Configuración servidor
- ❑ Validación de entrada
- ❑ Ideal para **herramientas automatizadas**

○ Lógicas o funcionales

- ❑ Errores permitidos por diseño, pero no previstos por el diseñador o no considerados un riesgo
- ❑ Errores que saltan a la vista, sólo identificados por **humanos**



Cómo protegerse

- o **Construir** de forma segura
 - Diseño/Codificación seguros
- o **Averiguar** si lo construido es seguro
 - Auditorías de seguridad
- o **Asegurar** lo que ya está construido
 - Cortafuegos de aplicación



Diseño/Codificación seguros

- Los programadores deberían conocer sus herramientas, lenguajes y plataformas
- La seguridad debería introducirse desde el diseño de la aplicación, no al final
- Los desarrolladores deberían estar concienciados en seguridad
 - El BO es el error más extendido y el más peligroso
 - El XSS es ubicuo y nada inofensivo
 - La inyección de SQL es muy frecuente y peligrosa

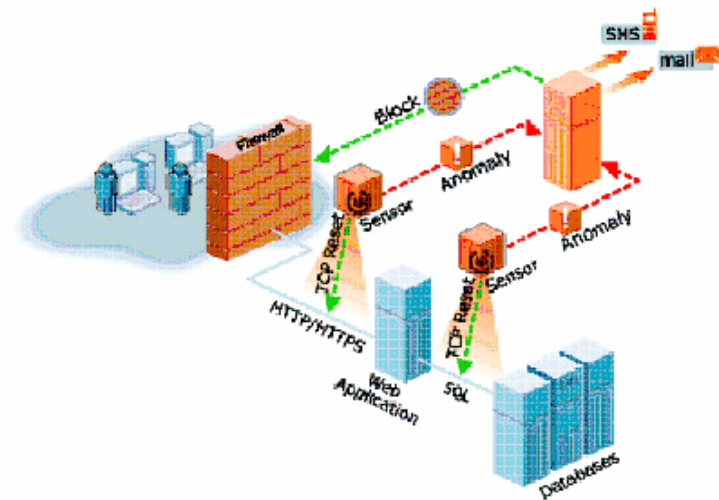
Cortafuegos de aplicación o IPS

o Ventajas

- ❑ Detecta los ataques **antes** de que lleguen al servidor en oposición a *análisis de logs*
- ❑ El CISO alcanza **paz** de espíritu

o Inconvenientes

- ❑ No detecta ataques **lógicos**
- ❑ Problemas de **escalamiento**
- ❑ Tan bueno como su **directiva**



Delitos informáticos

- Los bancos sólo se protegen a sí mismos:
 - **Phising** → La víctima paga
 - **Compras fraudulentas** → El comercio paga
- En la medida en que el banco no es responsable de las pérdidas ocasionadas, no hace nada por mejorar la seguridad



Delitos Informáticos: Adiós al comercio electrónico (17/2/2006)

- o **No cabe hablar de engaño bastante** por parte de los acusados por cuanto que nos encontramos ante una compra realizada no en un comercio abierto al público donde pueda existir una relación de confianza entre las partes compradora y vendedora que lleve a ésta a no comprobar si quien realiza la compra es realmente titular de la tarjeta usada como medio de pago, sino que se trata de una **compra-venta realizada a través de una página web** remitiendo la mercancía R.F.S.L. **sin realizar la más mínima comprobación** para cerciorarse de que quien realizaba el pedido era realmente el titular de la tarjeta a la que había que cargar el importe de la venta y no otra persona que usase ese número **FRAUDULENTAMENTE** como realmente sucedió, que **el perjuicio patrimonial no es consecuencia directa del ENGAÑO** empleado por los acusados sino de la **FALTA DE DILIGENCIA** por parte de la empresa vendedora. Por lo cual al ser inidóneo el engaño **no cabe hablar de delito de estafa**.

Problema de fondo de seguridad en el comercio electrónico

- Las nuevas tecnologías no son nuevas, de hecho son muy antiguas (años 60)
- Internet no está preparado para el comercio electrónico seguro: el **robo de identidad** es trivial
- Todo el peso de la culpa recae sobre la víctima
- Es necesaria una redistribución de la culpa



'En Internet nadie sabe que eres un perro'

Conclusiones

- Los controles de seguridad **tradicionales** (cortafuegos, SSL, bastionado, parches, escaneos rutinarios, arquitectura segura) **no** detienen ataques web
- Otras medidas de seguridad (codificación segura, cortafuegos de aplicación) protegen contra la mayoría de vulnerabilidades, aunque no todas
- No se ha avanzado (¿nada?) en seguridad
- No es posible estar 100% seguros, pero sí es posible **gestionar el riesgo**