

¿La banca online es vulnerable? (1ª Parte)

Después de ver el informe realizado [por Hugo Vázquez \(Director Técnico de PENTEST, Consultores de Seguridad Telemática\)](#) podemos pensar que aun queda mucho trabajo en la banca online. Pero tampoco podemos olvidar los nuevos métodos empleados por las entidades bancarias, en este informe se aportan también ideas para un futuro mas seguro.



El informe sobre la banca online fue certificado por el esCERT y es el resultado de varios meses de investigación. Recomendamos su lectura completa y ver los ejemplos de ataques reales.

Informe:

Banca Electrónica Nuevos Vectores de Ataque. 1º Parte.

RESUMEN EJECUTIVO

RESUMEN TÉCNICO

1. OBJETIVO DEL DOCUMENTO

2. ESCENARIO COMÚN. PRECEDENTES

- Primer nivel de validación
- Segundo nivel de validación (firma)

3. VECTOR DE ATAQUE PRINCIPAL

- Lógica del mecanismo de protección (2ª validación o firma)
- El talón de Aquiles de los sistemas de firma
- Inyecciones de Código Internas

4. NUEVO VECTOR DE ATAQUE

5. DESCRIPCIÓN DE UN ATAQUE EN UN CASO REAL

6. VARIACIONES

- Captura de coordenadas del teclado virtual
- Decodificación directa de las coordenadas del teclado
- Troyanización del teclado virtual

7. RECOMENDACIONES FINALES

8. CONCLUSIONES

RESUMEN EJECUTIVO

El acceso en Internet a las aplicaciones web de uso restringido, se protege normalmente mediante una combinación de usuario y contraseña que se debe facilitar antes de entrar en la zona privada .

La banca on-line emplea además como sistema de seguridad adicional, y para las operaciones de riesgo, un mecanismo de protección conocido habitualmente como firma . Cuando un usuario desea realizar una transferencia entre cuentas por ejemplo, se le solicita que se identifique (que firme). Esta identificación se lleva a cabo de distintas maneras en función del banco: unas entidades utilizan teclados virtuales, otras una tarjeta de coordenadas, otros dispositivos físicos que generan claves de un solo uso, etc...

Lo que tienen en común todos estos sistemas de firma, es que están destinados a identificar al usuario que realiza la operación, para esa operación en particular. Dicha identificación se realiza gracias a una información que el usuario envía al servidor. La confianza de este mecanismo de seguridad, radica principalmente en que la información que el usuario envía solo autoriza dicha operación, de manera que para cada gestión bancaria hay que volver a introducir la firma correspondiente. Este mecanismo es muy propio del sector de la banca y se viene utilizando para evitar cierto tipo de ataque muy conocido en el mundo de la seguridad informática.

El informe que a continuación se expone presenta un perfil de los resultados obtenidos en el estudio de los mecanismos de seguridad utilizados habitualmente por el sector de la banca electrónica, en concreto el sistema de firma para operaciones de riesgo. Dicho perfil demuestra que independientemente de la solución empleada (teclados virtuales, tarjetas de coordenadas, etc) existen distintas posibilidades de afectar la seguridad de dichos sistemas.

Las metodologías que se describen en el siguiente informe no son nuevas ni presentan ninguna técnica desconocida o novedosa en cuanto a la base técnica en la que se sustentan. El presente informe sin embargo, sí que muestra un nuevo enfoque en el uso de las técnicas tradicionales de intrusión para conseguir romper la seguridad de los sistemas de firma que utiliza la banca electrónica.

Las conclusiones que se desprenden del estudio es que actualmente, la gran mayoría de métodos de firma que utiliza la banca electrónica son susceptibles de verse comprometidos por toda una serie de vectores de ataque.

RESUMEN TÉCNICO

La protección de las aplicaciones web viene siendo desde hace varios años uno de los mayores retos de los programadores. La dificultad de la protección de dichas aplicaciones radica en gran parte en que el protocolo de base que se utiliza para las comunicaciones entre el cliente y el servidor (http/https) no es seguro.

Uno de los mayores problemas del protocolo http, es la inexistencia de un mecanismo de seguimiento de sesión que sea formalmente seguro. Desde hace muchos años vienen realizándose distintas propuestas relativas a dichos mecanismos, por ejemplo la RFC 2109 de Febrero de 1997, la RFC 2964 y 2965 de Octubre de 2000, etc, o las posteriores propuestas de algunos fabricantes en

concreto.

La problemática de la inseguridad del seguimiento de sesión en comunicaciones http ha intentado solventarse en el entorno bancario mediante el uso de un mecanismo de validación (la firma) que adolece de un contexto de sesión, y que por lo tanto en principio no es vulnerable a ataques de secuestro de sesión.

La firma en el sector de la banca electrónica, es aquella identificación que se le solicita al usuario cada vez que este quiere realizar una operación delicada. Esta identificación, independientemente del método empleado (teclados virtuales, tarjetas de coordenadas, "tokens", claves de un solo uso, o combinaciones de varios de los anteriores) tiene por objeto validar al usuario solo para esa operación en concreto.

Generalmente esta validación se pide en el último paso de confirmación de una operación de riesgo (por ejemplo una transferencia económica), y únicamente valida los datos enviados en el paso del formulario antes mencionado.

El siguiente informe pretende mostrar como este esquema de validación, que se emplea para evitar la suplantación de identidad es vulnerable a los mismos ataques que se vienen empleando para secuestrar sesiones http, utilizando las mismas técnicas, únicamente en un contexto y unas circunstancias distintas a las habituales.

Siendo estrictos, este informe no presenta ninguna técnica nueva ni innovadora, sin embargo, sí demuestra que la aplicación de las técnicas de ataque clásicas, en ciertos escenarios, y haciendo uso de un poco de imaginación pueden poner en riesgo gran parte de los sistemas de firma actualmente en uso por el sector de la banca electrónica.

En el siguiente texto se hace referencia a conceptos como Inyección de Código, Cross Site Scripting, Envenenamiento de Caché, Sesión http, Identificador de Sesión, Cookie, Secuencia o Estado de una sesión, etc.

La explicación detallada de cada una de estos conceptos particulares no es el objetivo de este documento, por lo que se recomienda estar familiarizado con dicha terminología.

OBJETO DEL DOCUMENTO

El presente documento tiene por objeto mostrar nuevas estrategias o vectores de ataque a los sistemas de autenticación de banca electrónica. Este documento está basado en la investigación concreta de una entidad bancaria, y sus conclusiones afectan a un ámbito lo suficientemente amplio como para poder aplicarse a cualquier entorno web, aunque son de especial interés sus repercusiones en el entorno de la banca.

Este documento NO tiene por objeto convertirse en una guía de explotación práctica, ni ser una referencia para llevar a cabo acciones ilegales sobre sistemas telemáticos.

Toda la información que se muestra a continuación, se ha obtenido lícitamente mediante la observación del comportamiento lógico de una aplicación.

Sus conclusiones son el fruto de un minucioso estudio sobre un sistema de banca online. Las técnicas que se explican pueden no ser aplicables directamente en muchos casos.

ESCENARIO COMÚN. PRECEDENTES

Primer nivel de validación

Los sistemas de banca on-line, habitualmente utilizan dos niveles de autenticación. El primer nivel es el que se emplea para dar acceso al usuario a su entorno de banca electrónica, es decir, es el primer usuario y contraseña que pide el aplicativo. Con esta validación, el usuario puede realizar tareas de supervisión , puede ver datos, pero no modificarlos (generalmente). Esto supone, poder comprobar el estado de las cuentas, su saldo, etc. Este primer nivel, puede usar distintos tipos de autenticación: usuario y contraseña estáticos, tarjeta de coordenadas, "token" físico, etc. Sea cual sea el método de validación, una vez autenticado, el usuario (su navegador) obtiene una serie de identificadores de sesión y/u otros parámetros que le sirven al servidor para llevar a cabo el seguimiento del cliente. Es decir, que el servidor, mantiene el estado de la sesión y puede diferenciar a varios clientes gracias a esta información que ambos extremos de la comunicación intercambian entre si en la capa de aplicación (http/https).

Esta mecánica no tiene nada de novedoso, y es con sus pequeñas variaciones e implementaciones, el esquema comúnmente empleado para llevar a cabo el seguimiento de sesión en aplicaciones que usan el protocolo http. Por otra parte como es de dominio público, este mecanismo no es completamente seguro... En una comunicación TCP/IP que utiliza un solo "socket", el estado de la sesión se implementa en el nivel 4 de la capa OSI (TCP), mediante el uso de números de secuencia. En una comunicación http, se utilizan varios "sockets", de manera que no es factible, utilizar el esquema clásico de TCP. Para solucionar este problema, el seguimiento de sesión se realiza a nivel de aplicación, mediante el uso de cierta información (identificadores de sesión, cookies, etc) que le permite al servidor, diferenciar a los clientes entre si. Aunque existen métodos de seguimiento de sesión más seguros, cómo por ejemplo a través del propio protocolo SSL, solo algunos fabricantes lo implementan, y no es común verlo en producción por motivos cuya explicación no es el objetivo de este documento.

¿Por qué no son seguros los sistemas de seguimiento de sesión http comúnmente utilizados?

Tal y como se ha comentado, el seguimiento de las sesiones http se lleva a cabo mediante un cierta información , que se transmite a través del propio protocolo http, ya sea en la URL, en las cabeceras, etc. Dicha información es accesible a través de client side scripting , es decir, lenguajes de programación cuya finalidad principal es ejecutarse en el lado del cliente de la comunicación http. Dichos lenguajes (javascript, HTML, DHTML, etc), han ido evolucionando con el objetivo de añadir funcionalidad a la navegación web, y es este aumento en la funcionalidad lo que también ha incrementado la inseguridad de este tipo de comunicaciones. Muchas veces dichos lenguajes han intentado eliminar parte de la carga de trabajo del servidor, a costa de mayor poder de ejecución en el lado del cliente. En la actualidad, todos los datos que se puedan utilizar para llevar a cabo un seguimiento de sesión http, se envíen como se envíen, son susceptibles de ser capturados de manera directa o indirecta mediante client side scripting . Y esto es un problema.

Tradicionalmente, los intrusos han venido utilizando técnicas como Cross Site Scripting o

Inyección de Código , para capturar las credenciales de una sesión válida y así poder suplantar la identidad del usuario.

Actualmente, no existe, al menos formalmente demostrado, ninguna aplicación web, invulnerable a un secuestro de sesión o suplantación de identidad.

Contrariamente a la creencia popular, ni tan siquiera la comprobación de la IP de origen de conexión es suficiente como para impedir ataques de secuestro de sesión. Librerías como XMLhttp, permiten construir peticiones http a bajo nivel, y hacer que la propia víctima sea quien realice dichas peticiones en lugar del atacante, es decir, a modo de proxy , invalidando así la protección por IP

de la aplicación web del servidor.

Segundo nivel de validación (firma)

El sector de la banca, consciente de la existencia del problema de secuestro de sesiones, ha venido utilizando un segundo nivel de autenticación, dentro de la propia sesión.

Esta segunda autenticación se pide en todas aquellas operaciones de riesgo, como por ejemplo, una transacción económica, una orden de compra/venta de acciones, un cambio de contraseña, etc. Es decir, todas aquellas operaciones que puedan suponer pérdidas económicas o daños inmediatos a la entidad, en caso de fallo. Esta segunda contraseña, se suele pedir en el último paso del formulario de la operación crítica, pongamos por ejemplo, una transferencia bancaria a una cuenta externa. Es en este último paso (la confirmación final de los datos), cuando se realiza esta segunda autenticación (firma), y que a diferencia de la primera no sirve para generar ninguna sesión sino que únicamente es un mecanismo para confirmar la identidad del usuario que realiza esa operación en concreto dentro de la sesión válida. La finalidad de este mecanismo es evitar que un atacante pueda hacer uso de una sesión válida en la aplicación bancaria (por ejemplo, si alguien olvida cerrar la sesión con su banco en un ordenador de acceso público). La autenticación en este segundo nivel, puede ser, al igual que en el primer nivel, mediante contraseña estática, mediante teclado virtual, tarjeta de coordenadas, "token" físico, o una combinación de varios de los anteriores métodos. En cualquier caso, la segunda autenticación (firma) no sirve para obtener una sesión, y por lo tanto, en principio, no parece ser susceptible de un ataque de secuestro de sesión, en cuanto no existe un nuevo contexto de sesión.

Este sistema de protección de las sesiones de banca electrónica, se ha considerado desde siempre seguro, al menos conceptualmente. Si analizamos la lógica de este esquema de protección, vemos que al parecer, en el peor de los casos, un intruso, podría secuestrar una sesión de un usuario de banca (mediante obtención del estado de la sesión), pero nunca podría realizar una operación de riesgo. Es decir, que el intruso podría visualizar los datos de las cuentas de la víctima, pero nunca podría realizar un movimiento económico, pues como se ha descrito, la segunda autenticación no es susceptible a secuestros de sesión.

Teniendo en cuenta que además, las comunicaciones de banca on-line van cifradas mediante "Secure Socket" Layer", no parece viable poder acceder a los datos de validación del segundo nivel, al menos, sin estar en el mismo segmento físico que la víctima (mediante un clásico ataque tipo SSL man-in-the-middle). No hablaremos de este caso concreto, ya extensamente documentado y conocido.

En definitiva, el punto fuerte de los sistemas de banca on-line, ha sido desde siempre, este segundo nivel de autenticación también conocido como firma.

Continúa:

[Informe 1ª parte del informe](#)

[Informe 2ª parte del informe](#)

[Informe 3ª parte del informe](#)

[Informe 4ª parte del informe](#)

[Informe 5ª parte del informe](#)

Hugo Vázquez Caramés
(Director Técnico de PENTEST, Consultores de Seguridad Telemática)
<http://www.pentest.es>

Nota: La empresa española [PENTEST](#) tal vez sea una de las mejores del entorno europeo en la realización de Tests de Intrusión. Empresa que basa su éxito en la recluta para cada tipo de proyecto de los mejores "Pen-Testers" existentes en la problemática a auditar. Una vez seleccionados, forma un equipo de auditores o "Tiger Team" que pone al servicio del cliente. Normalmente los "Tiger Team" de [PENTEST](#) no solo son los mejores, sino también los más motivados pues trabajan a partir de la propia libertad de sus conocimientos y experiencia y de la que concede Pentest para el desarrollo de su función profesional.

[Artículo completo](#)

Fecha artículo: 2006-06-20 20:00:05 - url artículo: <http://www.internautas.org/html/800.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org