

enISE



inteco



Instituto Nacional
de Tecnologías
de la Comunicación

Innovando en los sistemas de autenticación

ENISE - T23: Banca electrónica y pago seguro

Eulogio Naz Crespo

Socio fundador

DIVERSID



1. Introducción: ¿qué hacer con nuestros sistemas de control de acceso a la información?
2. Tabla comparativa de técnicas antifraude preventivas
3. Tabla comparativa de técnicas antifraude reactivas
4. Tabla comparativa de la efectividad de técnicas antifraude para la confirmación de operaciones sensibles
5. Comparativa de usabilidad: tarjeta coordenadas VS 3 claves OTP
6. Conclusiones: resultado de la comparativa de técnicas antifraude

¿Qué hacer con nuestros sistemas de control de acceso a la información?

1. Cifras sobre el fraude por deficientes controles de acceso y éxitos en la suplantación de personalidad:

- McAfee: Ciberespías y asociaciones criminales armadas con programas especiales, que roban información digital a empresas, generaron en 2008 pérdidas de mil millones de dólares.

- Gartner: Desde agosto de 2007 a septiembre de 2008, cinco millones de usuarios en EEUU han resultado estafados por medio del Phishing perdiendo una media de 351\$ cada uno (casi 1.800 millones de dólares). El número de víctimas se ha visto incrementado en un 39,8% respecto a la situación del año anterior.

- Los bancos de 22 países europeos perdieron 485 millones de euros por fraude en cajeros automáticos durante 2008 (European ATM Security Team)

2. La solución a éste problema pasa por renovar los sistemas aplicando técnicas antifraude innovadoras que superen las empleadas por los delincuentes.

3. Antes de decidir la técnica a emplear para renovar un sistema de control de acceso conviene conocer su eficacia, al día de hoy, frente a los fraudes más frecuentes.



Tabla comparativa de técnicas antifraude preventivas

Técnica antifraude VS Técnica de fraude	Phishing diferido	Phishing en tiempo real	Modificación on line de datos (Man in the Middle, Troyanos,...)
Certificado electrónico	Lo evita	Lo evita	No lo evita (1)
Autenticación con tarjeta de coordenadas	No lo evita (2)	Lo evita	No lo evita
Una clave OTP	Lo evita con condiciones	No lo evita	No lo evita
Dos claves OTP	Lo evita con condiciones	No lo evita	No lo evita
Una clave fija y dos OTP (3)	Lo evita	Lo evita	No lo evita
Tres claves OTP	Lo evita	Lo evita	No lo evita

- 1- En una máquina controlada por un troyano no se puede tener seguridad de qué se está firmando (ej.: Silentbanker); Security By Default: Fraude online con firma digital y SSL
- 2- Si en un proceso de phishing, o con un troyano, un defraudador se hace con una de nuestras claves de la tarjeta, ¿cómo podemos evitar que a base de reiterados intentos de operar llegue el caso en el que la clave solicitada por el banco coincida con la que tiene el defraudador?
- 3- Al utilizar una primera clave con valor fijo será fácil que un atacante pueda hacerse con ella y, enviándola de forma repetida y continuada, puede llegar a conseguir una denegación de servicio



Tabla comparativa de técnicas antifraude reactivas

Técnica antifraude VS Técnica de fraude	Phishing diferido	Phishing en tiempo real	Modificación on line de datos (Man in the Middle, Troyanos,...)
Servicios antiphishing	Lo evita después de ser detectado (4)	Lo evita después de ser detectado (4)	No lo evita
Antitroyanos	Lo evita después de ser detectado (5)	Lo evita después de ser detectado (5)	Lo evita después de ser detectado (5)

4- Estudios revelan que durante las 6 primeras horas de un ataque de Phishing se llegarían a concentrar el 51,6% de las visitas mientras que los servicios antiphishing reactivos mantienen medias superiores a las 6 horas de cierre

5- Pueden pasar días, o incluso semanas, hasta que un troyano llega por primera vez a un laboratorio antivirus



Tabla comparativa de la efectividad de técnicas antifraude para la confirmación de operaciones sensibles

Técnica antifraude VS Técnica de fraude	Phishing diferido	Phishing en tiempo real	Modificación on line de datos (Man in the Middle, Troyanos,...)
Acceso con clave fija y confirmación de operaciones con clave fija y SMS con clave OTP (6)	No evita la consulta	No evita la consulta	Lo evita (7)
Acceso con tres claves OTP y confirmación de operaciones con clave fija y SMS con clave OTP	Lo evita	Lo evita	Lo evita (7)
Acceso con tres claves OTP y confirmación de operaciones con tres claves OTP y dos canales de comunicación	Lo evita	Lo evita	Lo evita (8)

6- Al utilizar una clave con valor fijo será fácil que un atacante pueda hacerse con ella y, enviándola de forma repetida y continuada, puede llegar a conseguir una denegación de servicio además de una mala imagen de la entidad al llegarle al cliente los SMS de operaciones que él no ha solicitado.

7- No será cierto si existe la posibilidad de que un delincuente intercepte el SMS (ej.: cambiando el nº de móvil en la ficha del cliente).

8- Aunque como segundo canal se emplee un SMS que pudiera ser interceptado no afectaría a su seguridad ya que no es la clave que viaja en el SMS la que confirmará la operación.



Comparativa en usabilidad: tarjeta coordenadas VS 3 claves OTP

Pasos

0

Tener a mano ...

1

Introducir en la web usuario y...

2

Leer en la web...

3

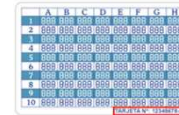
Obtener...

4

Introducir en la web...

Tarjeta de coordenadas

... cartera y tarjeta de coordenadas



... contraseña, generalmente estática y memorizada

... columna y fila

... la clave de la tarjeta correspondiente a la columna y fila

... la clave de la tarjeta de coordenadas

Tres claves OTP

... teléfono móvil y abrir aplicación



... clave 1 (leída en la aplicación)

... clave 2

... clave 3 tecleando la clave 2 en la aplicación del móvil

... la clave 3 (proporcionada por la aplicación)

DIVERSID
AUTENTICACIÓN



Resultado de la comparativa de técnicas antifraude

- Las técnicas de prevención del fraude parecen más eficaces que las reactivas que lo persiguen una vez realizado.
- Dentro de las técnicas preventivas destaca, por su sencillez y eficacia, el sistema de autenticación para el control de acceso basado en el Intercambio de tres claves OTP que consigue accesos sin posibilidad de fraudes de suplantación de personalidad, como el Phishing.
- Dentro de las técnicas para la confirmación de operaciones destaca, por su carencia actual de vulnerabilidades, la confirmación de operaciones con Intercambio de tres claves OTP, haciendo uso de dos canales de comunicación diferentes para dicho intercambio, que consigue eliminar la posibilidad de modificación fraudulenta de datos aplicando la técnica del Man In the Middle.



Muchas gracias



Instituto Nacional
de Tecnologías
de la Comunicación