

Actualizarse o sufrir, esa es la cuestión

Gestión de la seguridad en un entorno cambiante

Autor: Sebastián Bortnik

Licencia

El presente trabajo es publicado bajo una licencia de Creative Commons, Atribución-No Comercial-Compartir Obras Derivadas Igual 2.5 Argentina

Usted es libre de:

- copiar, distribuir, exhibir, y ejecutar la obra.
- hacer obras derivadas de ella.

Bajo las siguientes condiciones:

- Usted debe atribuir la obra en la forma especificada por el autor o el licenciante.
- Usted no puede usar esta obra con fines comerciales.
- Si usted altera, transforma, o crea sobre esta obra, sólo podrá distribuir la obra derivada resultante bajo una licencia idéntica a ésta.

<http://creativecommons.org/licenses/by-nc-sa/2.5/ar/>

Introducción

Sabido es que la tecnología evoluciona a pasos agigantados y que los tiempos de aparición de nuevas tecnologías son cada vez más cortos.

Sin embargo, particularmente en Seguridad, y al tratarse de riesgos, ya no es importante, sino más bien imprescindible mantenerse actualizado de los nuevos ataques. Puedo no conocer una nueva tecnología, puedo tomarme mi tiempo (prudencial) para aprender un nuevo protocolo o un nuevo sistema operativo; pero si me dedico a seguridad no puedo tomarme un tiempo para conocer un nuevo vector de ataque y la evolución de los mismos. La seguridad se gestiona en un entorno donde lo único constante es el cambio.

Las amenazas evolucionan permanentemente de forma tal que no es posible garantizar la efectividad de una contramedida a lo largo del tiempo. Para graficar esto, se presenta la evolución de dos ataques y sus respectivas contramedidas de forma simple y gráfica.

Keyloggers y teclados virtuales

(a) Algunas definiciones

Uno de los métodos más utilizados, por los ladrones y estafadores actuales para obtener información sensible, cuando se utiliza un sistema informático, son los **Keyloggers (del inglés Key = Tecla y Log = Registro)**.

Un keylogger es una herramienta para detectar y registrar las pulsaciones del teclado en un sistema. Pueden ser tanto por Hardware como por software, aunque los primeros no son tan conocidos. A pesar de que los keylogger son utilizados con fines malignos, también pueden ser utilizados con otros fines sin la intención de generar un daño. No son una amenaza para el sistema sino para el usuario y su privacidad [1]; pueden capturar información como contraseñas de correos o cuentas bancarias [2], entre otras, y por lo tanto atentar contra información sensible del usuario que pueden consumarse con otros tipos de ataques como extracción de dinero de una cuenta bancaria u otros ataques sin ánimos de lucro [3].

En el caso particular de los ataques informáticos, los keyloggers por hardware no tienen mucho sentido ya que en su mayoría son visibles. Los ataques por keylogger por lo general están incluidos en algún troyano o gusano que se instala en la Pc y envía la información capturada al atacante. [4]

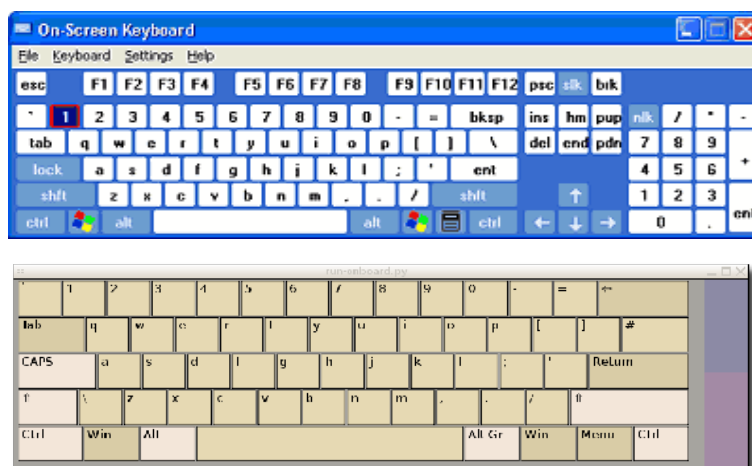
(b) Contramedidas

La contramedida más utilizada para prevenirse de los keyloggers son los teclados virtuales. Estos consisten en mostrar en pantalla la imagen de un teclado y dar al usuario la posibilidad de ingresar información haciendo clic con el mouse sobre el teclado en pantalla. De esta forma, las herramientas que captan las teclas que se pulsan no registrarán la información ingresada.

Los teclados virtuales se deben utilizar solo para ingresar la información sensible (contraseñas, números de cuenta) ya que, obviamente, son más incómodos que utilizar el teclado tradicional.

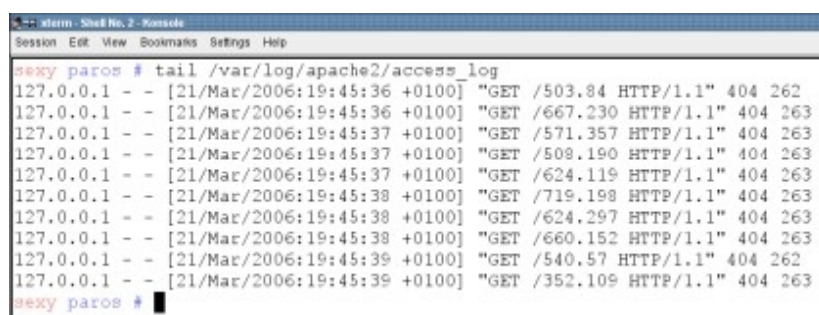
(c) Evolución

En función de los conceptos antes explicados se crearon los teclados vituales como los que se presentan a continuación; incluidos por defecto en Windows y Linux respectivamente.



Pero la evolución de las técnicas utilizadas por los atacantes hicieron que estas contramedidas, **antes efectivas**, ahora se volvieran vulnerables a nuevos tipos de ataques.

Con la creación de los teclados virtuales comenzaron a aparecer nuevas técnicas en los “keyloggers”, dicho entre comillas ya que ahora algunos de ellos podían capturar, además de la información del teclado, las coordenadas donde se hacía clic con el mouse. De esta forma, conociendo la web que el usuario ingresó (por el teclado) y las coordenadas del teclado virtual se podían deducir los datos que se ingresaron.



```
sexy paros # tail /var/log/apache2/access_log
127.0.0.1 - - [21/Mar/2006:19:45:36 +0100] "GET /503.84 HTTP/1.1" 404 262
127.0.0.1 - - [21/Mar/2006:19:45:36 +0100] "GET /667.230 HTTP/1.1" 404 263
127.0.0.1 - - [21/Mar/2006:19:45:37 +0100] "GET /571.357 HTTP/1.1" 404 263
127.0.0.1 - - [21/Mar/2006:19:45:37 +0100] "GET /508.190 HTTP/1.1" 404 263
127.0.0.1 - - [21/Mar/2006:19:45:37 +0100] "GET /624.119 HTTP/1.1" 404 263
127.0.0.1 - - [21/Mar/2006:19:45:38 +0100] "GET /719.198 HTTP/1.1" 404 263
127.0.0.1 - - [21/Mar/2006:19:45:38 +0100] "GET /624.297 HTTP/1.1" 404 263
127.0.0.1 - - [21/Mar/2006:19:45:38 +0100] "GET /660.152 HTTP/1.1" 404 263
127.0.0.1 - - [21/Mar/2006:19:45:39 +0100] "GET /540.57 HTTP/1.1" 404 262
127.0.0.1 - - [21/Mar/2006:19:45:39 +0100] "GET /352.109 HTTP/1.1" 404 263
sexy paros #
```

Ejemplo de captura de coordenadas por un troyano [5]

Como se puede observar, **la creación de la nueva contramedida dispara la posterior creación de un nuevo ataque**, incluso aprovechando la contramedida.

Para este ataque, los teclados virtuales tuvieron que evolucionar y lo hicieron modificando el orden de las letras de forma tal que este apareciera modificado respecto a la ubicación de las teclas en el dispositivo físico. De esta forma, se prevenía que se tomen las coordenadas y se comparen con un teclado normal.



Ejemplo de teclado virtual alfabético



Ejemplo de teclado virtual numérico de un reconocido banco

Este método de todas formas fue vulnerado de forma muy simple: conociendo las coordenadas, la página web y cómo distribuía el teclado virtual dicha página web se podían obtener los datos de todas formas por lo que muchos usuarios seguían siendo atacados en determinados sitios más populares.

La solución a este nuevo ataque consistió en **alterar el orden de las teclas cada vez que se cargaba un teclado virtual de forma aleatoria**. Es decir, si yo ingresaba a la página web de mi banco tres veces seguidas, en cada una tendría una distribución del teclado virtual diferente. De esta forma, se solucionaban los ataques a través de obtención de coordenadas en combinación con keyloggers tradicionales.

Nuevamente los ataques evolucionaron y apareció nuevo código malicioso que incluía, además de capturas del teclado, las capturas de pantalla cada vez que se realizaba un clic del mouse. De esta forma, se podía obtener la clave o número de cuenta del usuario con un conjunto muy pequeño de imágenes enviadas al atacante en conjunto con el registro del teclado [6].

Como último paso de evolución conocida de estas técnicas, se han registrado troyanos que pueden grabar en formato de video la navegación de un usuario por una página web [7].

Como se puede observar, la evolución de las técnicas de ataque han hecho que los teclados virtuales no sean una protección suficiente y efectiva para la protección del usuario hoy en día, muy a pesar de haber sido una contramedida contundente en otros tiempos.

Ataques automáticos (password cracking, spambots) y CAPTCHA

(a) Algunas definiciones

Los ataques automáticos (o automatizados), como su nombre lo indica, son aquellos que pueden ejecutar gran cantidad de instrucciones a gran cantidad de víctimas sin la necesidad de intervención humana.

Un tipo de estos ataques, denominado Password cracking, se basa en realizar un ataque de fuerza bruta para descubrir una contraseña. Esto quiere decir, probar todas las contraseñas posibles de forma automatizada (con un ordenador) hasta encontrar la clave de acceso correcta. Es decir, si se supone una contraseña numérica, de un dígito, un programa podría probar los dígitos del 0 al 9 hasta encontrar el correcto. Los ordenadores pueden desarrollar este método con claves más complejas y más extensas, un humano no.

Otro ejemplo de un ataque automatizado es el spam. Una persona podría enviar manualmente una cantidad importante de correos electrónicos, pero un programa supera las capacidades humanas. Adicionalmente, se utilizan herramientas automáticas para generar spam, por ejemplo, como comentarios en blogs o sitios webs.

También se utilizan herramientas automatizadas para generar cuentas de correo en Internet, o rellenar formularios web en diferentes sitios, en cantidad.

(b) Contramedidas

Para mitigar un ataque automatizado, es necesaria una herramienta que permita distinguir si la acción está siendo ejecutada por un humano, o por una herramienta automatizada. Para ello, existe una herramienta denominada CAPTCHA (acrónimo de **C**ompletely **A**utomated **P**ublic Turing test to tell **C**omputers and **H**umans **A**part – en español: Prueba de Turing pública y automática para diferenciar a máquinas y humanos [8]).

Un CAPTCHA es una prueba utilizada para identificar si el usuario es o no humano.

Por lo general, la herramienta consiste en solicitar al usuario la realización de una tarea que únicamente debería poder ser realizada, de forma satisfactoria, por un humano, y no por una herramienta automatizada.

(c) Evolución

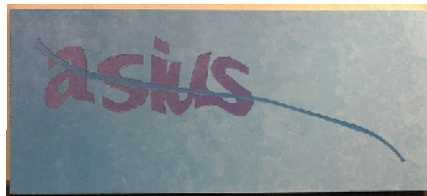
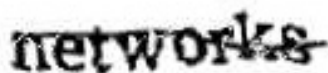
Los CAPTCHAS tradicionales constan de una serie de letras incrustadas en formato de imagen y solicitan al usuario ingresar los caracteres que aparecen en la imagen. Algunos ejemplos pueden verse a continuación:



Al igual que con los keyloggers, las primeras contramedidas fueron efectivas solo al principio. La evolución de técnicas de reconocimiento de texto en imágenes [9] hicieron muy simple desarrollar herramientas que puedan completar el CAPTCHA sin ningún inconveniente.

Posteriormente, la primer evolución de los CAPTCHAS consistió en la deformación más acentuada de los caracteres, como en los ejemplos que se ven

a continuación:



Sin embargo, es posible encontrar variedad de noticias sobre herramientas que han logrado descifrar también CAPTCHAS más complejos de este tipo. Es el caso, por ejemplo, de los ataques que han logrado vulnerar los CAPTCHAS de Yahoo [10], Windows Live, Google o Gmail [11].

Adicionalmente, muchos CAPTCHAs se volvieron indescifrables incluso para humanos [12]. De esta forma, el objetivo de la contramedida de seguridad tampoco se encuentra cumplido, al restar usabilidad a los servicios.

Posteriormente aparecieron nuevas técnicas, entre ellas, los CAPTCHAs matemáticos [13], que consistían en ingresar, no el texto que aparecía en la imagen, sino el resultado de una cuenta matemática. En un principio, esta cuenta aparecía en formato de texto. Por ejemplo, se ingresaba en formato texto “2 + 3” y el usuario debía ingresar el resultado (5). La técnica fue rápidamente vulnerada al permitir al atacante extraer muy fácilmente la cuenta en formato de texto plano. Se realizaron otras pruebas, como ingresar en formato de texto las operaciones (“2 más 3”) o operaciones matemáticas en formato de imagen, como se muestra en la siguiente imagen:

Qualifying question

Just to prove you are a human, please answer the following math challenge.

Q: $1 + 3 - 0 + 3 + 3 * 3 * 0 = ?$

A:

mandatory

Note: If you do not know the answer to this question, reload the page and you'll get another question.

Los CAPTCHAs matemáticos, además, traen mayores problemas a los usuarios legítimos, para identificarse como humanos, teniendo en cuenta que ciertas personas no pueden resolver algunas cuentas, por diferentes motivos.

☐ Всен
☐ Только зарегистрированным пользователям
☐ Никому

Показывать информацию обо мне

Защита от автоматической регистрации

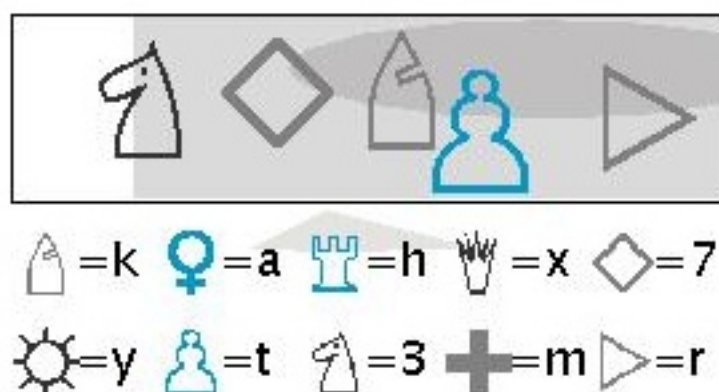
$$\lim_{x \rightarrow 0} \ln \left(2 + \sqrt{\arctg x \cdot \sin \frac{1}{x}} \right)$$

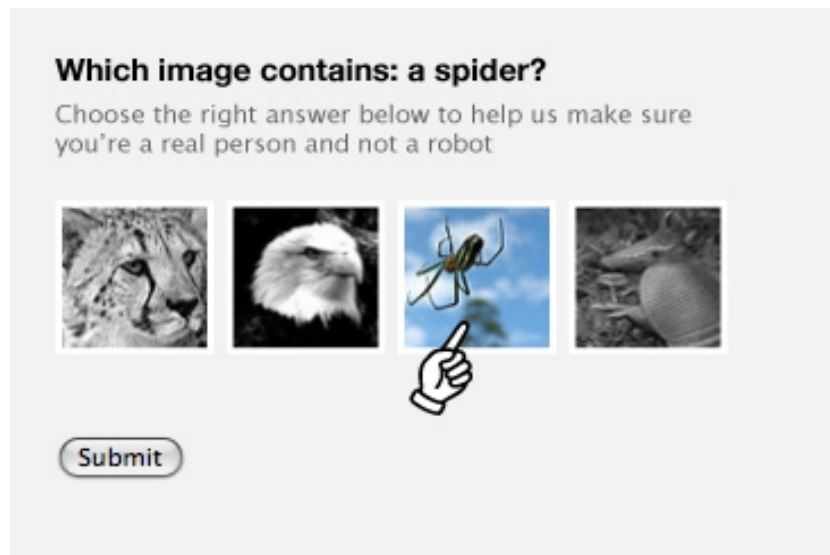
Введите ответ

<http://forum.academ.org/>

Posteriormente, aparecieron nuevos tipos de CAPTCHAS, como por ejemplo, los CAPTCHAS de audio. Estos fueron creados también, con el fin de permitir a los usuarios no videntes, el acceso a ciertos servicios protegidos por este método. Los CAPTCHAS de audio también fueron vulnerados por los atacantes [14], descifrando las ondas de sonido emitidas.

Existen nuevos casos de CAPTCHAS que, en un principio, aparentan ser más seguros que los métodos tradicionales, como los que se muestran a continuación:





En este último caso, el CAPTCHA consiste en “seleccionar todas las imágenes de gatos”[15].

En estos casos, actualmente los niveles de seguridad son mayores, debido a que las herramientas automatizadas están preparadas para vulnerar los CAPTCHAS de caracteres o matemáticos. Pero... ¿por cuánto tiempo?

Al igual que en el caso de los teclados virtuales, los CAPTCHAS han evolucionado a la par de los ataques y herramientas para descifrarlos y seguirán variando, acorde los cambios en las herramientas de ataques automatizados evolucionen. Nuevamente, los primeros CAPTCHAS, entonces efectivos (y seguros), hoy no representan una capa de seguridad avanzada contra los ataques automatizados explicados en esta sección.

Conclusiones

En seguridad, para protegernos de cualquier tipo de ataque, debemos crear o implementar alguna contramedida para eliminar o disminuir el riesgo de que dicho ataque se efectivice. Una vez implementada una contramedida uno generalmente se pregunta: **¿es efectiva esta contramedida?** Seguramente la respuesta en muchos casos será afirmativa y la solución implementada satisficará nuestros requerimientos de seguridad.

En los ejemplos desarrollados en el presente, es posible observar que ciertas contramedidas son efectivas, solo durante un tiempo determinado. El desarrollo y evolución de los ataques, hacen que una contramedida, hoy efectiva (y segura), mañana ya no lo sea.

Entonces, cabe hacerse una pregunta más: **¿por cuánto tiempo será efectiva mi contramedida?** Pensado en terminos de gestión, debo establecer un procedimiento que defina un periodo en el cuál debo analizar cada una de las contramedidas implementadas en mi Plan de Seguridad y preguntarme: **¿Sigue siendo efectiva la contramedida?**

Muchas veces, nuevas contramedidas tienen un tiempo de vida muy corto en el cual podemos asegurar su efectividad e ignorar esto puede ser crucial para quienes trabajan en seguridad.

Quienes invierten en seguridad, deben saber que son inversiones que posiblemente sean a corto plazo si no se establecen procedimientos para el seguimiento y control del plan de seguridad. Como ya se ha dicho tantas veces, **la seguridad no es un producto, es un proceso**. Es decir, no es un objetivo que queremos alcanzar, sino un principio que debemos gestionar.

Y este proceso está cada vez más definido por un entorno extremadamente cambiante que no puede ser desconocido por ningún eslabón de la cadena de protección de un sistema.

Referencias

[1]Keyloggers: Qué son y cómo detectarlos

<http://www.viruslist.com/sp/analysis?pubid=207270912#prot>

[2]Video ejemplo keylogger tradicional

http://www.hispasec.com/laboratorio/troyano_captura_banesto.htm

[3]Secuestro de cuentas Hotmail

<http://seguinfo.blogspot.com/2006/12/secuestro-de-cuentas-hotmail.html>

[4]Más información sobre Keyloggers

<http://es.wikipedia.org/wiki/Keylogger>

<http://www.segu-info.com.ar/malware/keylogger.htm>

<http://www.segu-info.com.ar/articulos/46-keylogger.htm>

[5]Banca Electrónica - Nuevos Vectores de Ataque

http://seguridad.internautas.org/archivos/banca_electronica.pdf

[6]Vídeo ejemplo keylogger con captura de pantalla

http://www.hispasec.com/laboratorio/troyano_captura_cajamurcia.htm

[7]Troyano bancario captura en vídeo la pantalla del usuario

<http://seguinfo.blogspot.com/2006/09/troyano-bancario-captura-en-vdeo-la.html>

[8]Prueba de Turing

http://es.wikipedia.org/wiki/Prueba_de_Turing

[9]OCR - Optical character recognition

http://en.wikipedia.org/wiki/Optical_character_recognition

[10]Hacking al CAPTCHA de Yahoo!

<http://seguinfo.blogspot.com/2008/01/saltan-el-captcha-de-yahoo.html>

<http://seguinfo.blogspot.com/2008/01/captcha-de-yahoo-hackeado.html>

[11]Cayeron los CAPTCHAS de Windows Live y Google

<http://seguinfo.blogspot.com/2008/02/cayeron-los-captchas-de-windows-live-y.html>

[12]CAPTCHAs: Cada día más difícil demostrar que eres humano.

http://www.ingleslaboral.com/index.php?option=com_content&task=view&id=33&Itemid=1

[13]CAPTCHAS matemáticos

<http://seguinfo.blogspot.com/2008/02/cayeron-los-captchas-de-windows-live-y.html>

[14]Los CAPTCHAS de audio ya no son un obstáculo

<http://seguinfo.blogspot.com/2008/05/los-captchas-de-audio-ya-no-son-un.html>

[15]Excelente método de CAPTCHA

<http://seguinfo.blogspot.com/2007/12/excelente-mtodo-captcha.html>

El presente artículo puede ser descargado desde el blog personal del autor, en:

<http://unmundobinario.wordpress.com/articulos/>