ISSN 2346-9307

SKOPEIN

La Justicia en manos de la Ciencia

Abuso Sexual Infantil

Daniela S. Raffaele

Revelado de Escritura Indentada de Carbón

Ana B. Glina

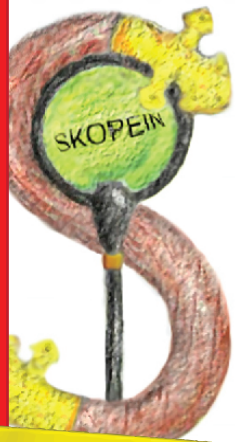
Prevención de Fraude Electrónico

Diego A. Alvarez

Entrevista Exclusiva a:

Maria Fernanda Ferreyro

Experta en balística y armas portátiles



Revista de Criminalística de publicación trimestral
Año I · Nº 1 · Sep - Nov 2013 *Reedición Mayo 2014*

Imagenes de la portada
Abuso Sexual Infantil:
http://autismodiario.org/wp-content/uploads/2012/01/abuso_sex.jpg
Prevención de Fraude:
http://borrowbits.com/wp-content/uploads/2013/06/http.jpeg

Propietarios

Alvarez, Diego Alejandro
Diribarne, Carlos María
Spano, Luciana Daniela

N° de Edición

Año 1, N° 1
Septiembre 2013
2° Edición, Mayo 2014

ISSN

2346-9307

AVISO LEGAL

Skopein es una revista online de difusión gratuita y sin fines de lucro destinada al público hispanoparlante de todas partes del mundo, ofreciéndoles a estudiantes, graduados y profesionales, un espacio para publicar sus artículos científicos y divulgativos, con su respectivo registro digital de propiedad intelectual, detallado en el siguiente apartado. Por lo tanto, la revista no se hace responsable de las opiniones y comentarios que los lectores expresen en nuestros distintos medios (como ser el foro o nuestras redes sociales), ni de las opiniones y comentarios de los colaboradores que publican dentro de la misma, y en ningún caso representando nuestra opinión, ya que la misma sólo se verá reflejada dentro de las notas de la Editorial.

El equipo revisa el contenido de los artículos publicados para minimizar el plagio. No obstante, los recursos que manejamos son limitados, por lo que pueden existir fallas en el proceso de búsqueda. Si reconoce citas no señaladas de la manera debida, comuníquese con nosotros desde la sección de contacto, o regístrese en nuestro foro para participar dentro del mismo.

Registro de propiedad Intelectual

Scopometría

Del griego "*Skopein*" que significa examen y "*metron*" medida

"Técnicas y procedimientos derivados de la física, basados en la observación y la medición aplicadas a comparaciones de cosas con fines de identificación".

Jorge O. Silveyra,
Peritajes Scopométricos
2005, Ed. La Rocca

AGRADECIMIENTOS

Muchas personas colaboraron con este proyecto, ya sea directamente, enviándonos sus trabajos de investigacion o en tareas organizativas; o de manera indirecta, siendo apoyados por nuestro entorno cercano, o con mensajes de aliento en las redes sociales, y no sería posible brindar el merecido agradecimiento nombrando a todos ellos.

Les damos un especial agradecimiento a nuestros profesores de IUPFA por darnos su apoyo incondicional en este proyecto, tecnólogos por naturaleza, siempre dispuestos a colaborar y brindar su vasta experiencia con el fin de mejorar las técnicas que permiten el esclarecimiento de los hechos.

También agradecemos el contacto y las palabras de aliento que nos dió Carol Henderson, profesora de leyes y fundadora del ***National Clearinghouse for Science, Technology and the Law*** (NCSTL), y por su difusión en su país, que nos motiva a eventualmente armar una versión de la revista en inglés.

Y por supuesto, no podemos dejar de lado a todos nuestros autores, que han apostado a publicar en nuestra revista, la cual no sería posible sin ellos, y a nuestros lectores, estudiantes, profesionales e interesados en la Criminalística, que, con firme rigor científico y técnico, practican estas ciencias para dar con la verdad objetiva.

A todos ellos, MUCHAS GRACIAS!

El Equipo SKOPEIN

Equipo Skopein

Dirección General

Alvarez, Diego
Diribarne, Carlos

Jefe de Redacción

Glina, Ana
Spano, Luciana

Autores en este número

Arce, Silvina M.
Alvarez, Diego A.
Diribarne, Carlos M.
Gamarra Viglione, Gabriel A.
Glina, Ana B.
Sanchez Espinoza, David R.
Raffaele, Daniela S.

Diseño del sitio

Alvarez, Diego

Diseño de la revista

Pino, Fernando
Diribarne, Carlos

Diseño del logo

Diribarne, Braian

Posicionamiento y difusión

Alvarez, Diego
Glina, Ana

Administrador del Foro

Spano, Luciana

NOTA EDITORIAL: Nacimiento de SKOPEIN

Estamos complacidos de haber podido convertir una idea surgida entre estudiantes universitarios, en un proyecto que avanzó con mucho esfuerzo, cubriendo los espacios de ocio, e incluso dejando de lado nuestras tareas y obligaciones cotidianas, hasta materializarse en esta revista que hoy nos enorgullece: SKOPEIN

Profesores, maestros, instructores, colegas, padres, amigos y muchas otras personas, nos aportaron a lo largo de nuestra vida conocimientos que creemos necesarios retransmitir para continuar con la cadena de la información de la cual todos somos un simple eslabón.

Nos encontramos con muchas personas de nuestro entorno que poseían el mismo interés, pero que no tenían el incentivo ni las herramientas suficientes con el cual poder decantar sus conocimientos y experiencias, y compartirlos.

Perteneciendo a una generación en la que la tecnología reina en la mayoría de nuestros aspectos, tuvimos la posibilidad de utilizar para este provecho los medios informáticos, que nos permitieron alcanzar, algo que hubiera sido económicamente imposible en otros tiempos, a un público especifico, tanto comprometidos con nuestra materia como simples autodidactas interesados por la misma.

Gracias a estos medios podemos difundir ***Revista Skopein,*** un espacio que pretende no sólo alcanzar al público local, sino atravesar todos los limites que nos separan, tanto idiomáticos, como culturales y geográficos, ya que consideramos que la ciencia no tiene patria y su lenguaje es de interpretación universal.

Los Directores

La Justicia en manos de la Ciencia

SKOPEIN

Prevención de Fraude Electrónico:

El desafío que enfrentan las nuevas tecnologías para la identificación inteligente de usuarios fraudulentos

*Diego A. Alvarez**
dalvarez@skopein.org

Introducción

Desde los inicios de la WWW y de las transacciones y movimientos de dinero a través de este medio, los negocios online, bancos y otras instituciones financieras se han visto en la necesidad de crear un método eficaz para la detección y prevención de fraudes provocados por cibercriminales, a fin de protegerse ellos mismos, y lograr la confianza necesaria en los usuarios para que operen seguros en su plataforma.

Por desgracia, y debido al constante avance y evolución de las tecnologías digitales, los fraudulentos han evadido e incluso manipulado una y otra vez todo método de prevención propuesto por estos comercios electrónicos, obligándolos a investigar y crear nuevos atributos que permitan la correcta individualización de dispositivos, y así permitir una re-identificación de un usuario que ya ha cometido o ha intentado cometer fraude.

Contraseña y dirección IP

En un principio, y por mucho tiempo, se ha considerado a la contraseña que utilizan los usuarios para ingresar a un sitio web, como un atributo válido para re-identificar a un fraudulento y evitar que opere de manera ilícita nuevamente. En efecto, un usuario que no desea ser detectado, inventará u omitirá otros datos de registro como domicilio, titularidad, email, teléfono, etc., pero difícilmente la contraseña, ya que la misma deberá ser fácil de recordar, y su constante modificación no le permitirá eventualmente ingresar al sitio, manteniendo por lo menos su lógica.

El problema que presentaba identificar estafadores por medio de coincidencias o similitud de contraseñas radicaba en que muchos de éstos utilizaban una ***password*** común, que coincidía con un sinnúmero de otros usuarios que la compartían pero operaban normalmente en el sitio y no podrían vincularse de manera alguna. Se trataba de contraseñas construidas con sencillas combinaciones de teclas (como por ejemplo: 741852963, 123456, QWERTY, 1Q2W3E4R, ASDFGH, 789456123; entre otras variantes) o conformados por nombres propios o comunes (ALEJANDRO, SUSANA, CAMION, AMARILLO, etc.), e incluso el propio nombre de la plataforma sobre la que operan, resultando imposible una detección eficaz[1].

Otro atributo muy tenido en cuenta a comienzos del nuevo siglo, y utilizado muchas veces en combinación con la anterior para

(*) Estudiante de Criminalística (IUPFA). Rep. de Prevención de Fraude Electrónico. Webmaster de ***e-commerce***
(1) Además, y acorde al estándar internacional de seguridad, se ha dejado de utilizar este atributo para el análisis de fraude por el riesgo que supone su conocimiento, al ser un dato privado de acceso.

reforzar vinculación, fue la dirección IP. Se trata de un número que se le asigna a la interfaz (elemento de conexión) de un dispositivo dentro de una red que utilice el protocolo IP. Hace unos años, cada PC conectada a internet contaba con una IP única que la identificaba, pero esto ya no es así porque las direcciones IP comenzaron a escasear ante la expansión masiva de internet.

Hoy en día, se trata de un elemento de identificación obsoleto, debido a que no siempre existe una sola IP por dispositivo que se conecta a la red, individualizando no un device, sino un conjunto que puede ser de unos pocos a cientos de computadoras compartiendo misma IP[2]. Asimismo, con el desarrollo de las laptops y tecnologías móviles (tablets, smartphones, etc.), su localización física y dirección IP cambian todo el tiempo, ya que ésta última no es estática, sino dinámica, por el uso de múltiples IPs. A esto se suma el hecho de que un cibernauta de medianos conocimientos sabe cómo ocultar su IP con el uso de servidores ***proxys***, manipulando también su localización.

Por todo esto, utilizar la dirección IP a fin de identificar un dispositivo ya no es un método que de certezas y seguridad, pero no deja de ser un dato válido e importante a tener en cuenta a la hora de reforzar cruces o vinculaciones con cuentas fraudulentas cuando exista controversia.

Cookie y Flash Cookie

La cookie es un archivo de texto que se graba en el ordenador del usuario, del cual se valen los servidores web para guardar y consultar información acerca de la actividad del cliente en un determinado sitio. Permite conocer los hábitos de navegación del usuario y sus preferencias por medio del servidor al que accede. De forma indirecta, este atributo permite identificar al dispositivo, ya que cada vez que el usuario se ***loguee*** en el sitio, le pedirá la cookie grabada en la computadora con anterioridad y así lo reconocerá.

Si bien es un medio para identificar positivamente un dispositivo[3], es fácil su manipulación con sólo cambiar el navegador, o simplemente eliminarlas con un programa de limpieza. De hecho, en 2010 se declaró oficialmente[4] a la cookie como una herramienta ya en desuso para la prevención[5]. Ante esto, hubo intentos de generar una mejor identificación creando cookies “invisibles” y de difícil eliminación, como la flash cookie, considerada la primera generación de prevención creada para tal fin, usado por Adobe Flash Player, y muy controvertido por las dudas que generaba en cuanto a la posible violación de la privacidad y seguridad del usuario. De todos modos, éstos seguían almacenándose en el dispositivo local, y podían ser eliminados por diferentes métodos, sin contar que hoy en día hay formas de navegación privada, permitiendo a los estafadores suprimir temporalmente las cookies y otros elementos flash a fin de evadir la identificación.

El avance tecnológico tanto en hardware como en software con infinidad de dispositivos móviles complicó aún más esta identificación en transacciones en línea, ya que algunos, como los productos que ofrece Apple, no son compatibles con flash y son capaces de bloquear las cookies del navegador, siendo ineficaz el reconocimiento mediante dicho elemento.

Nuevos atributos para Identificación

Dado todos los inconvenientes que representa identificar lo más categóricamente posible usuarios a fin de evitar la continuidad de fraudes, aparecieron plataformas online dedicadas a proveer servicios de forma tercerizada para combatir el cibercrimen. ThreatMetrix (THM) es un ejemplo de ellas, dirigida a bancos (por el

(2) Como aquellas que comparten mismo módem o servidor
(3) Si nos encontramos con dos cuentas que se loguean desde la misma cookie con poca diferencia de tiempo, es evidente que se trata del mismo dispositivo, y por lo tanto, muy probable que sea el mismo usuario
(4) Privacy Collides with Fraud Detection and Crumbles Flash Cookies, Gartner Research, 2010
(5) Lo primero que hace un fraudulento en su actividad delictiva para no ser identificado es bloquear o eliminar las cookies

homebanking), e-commerces y plataformas de pago, entre otros entes financieros y negocios online que involucren pagos y transacciones. Se trata de una plataforma de servicios "on-cloud"[6] que se encarga de detectar malware mediante herramientas y ***scores***[7] sofisticados, y utiliza tecnologías de identificación, a fin de evitar las estafas en transacciones online. Protege, además, las cuentas y las identidades de la misma, a través de defensa por niveles, denominados Device Id y Smart Id. Ambas aseguran el reconocimiento del dispositivo único, identificando con gran certeza las cuentas vinculadas a una sola persona, y así evitar el fraude con multicuentas o multiples usos de tarjetas de crédito robadas, sin necesidad de cookies ni archivos que se descarguen al disco local. De este modo, obteniendo una identidad individualizada del dispositivo utilizado, se los identificará a los usuarios cada vez que ingresen al sitio, aún si éstos eliminan cookies, utilizan proxys o navegación privada; además de generar una geolocalización real del origen del mismo, ya que recolecta una combinación de datos estáticos y dinámicos de los navegadores, sistemas operativos, posiblemente MAC Address[8], y paquetes de TCP/IP, para obtener un número único de identidad, supuestamente inalterable.

Pese a que pareciera haberse encontrado una solución definitiva para el reconocimiento eficaz de un dispositivo, estos nuevos atributos quedan en el plano teórico, ya que en la práctica se ha verificado que pocas veces han logrado individualizar a un fraudulento, e incluso muchas veces con menor rendimiento que el uso de la cookie común[9].

En la práctica forense, estos elementos pueden ser tenidos en cuenta como medios indirectos de carácter relativo en lo que respecta a identificación, pero nunca podrán ser considerados prueba, ya que sus resultados no indican certeza, sino sólo posibilidad [10].

Análisis de cruces en determinación de robo de cuenta

Existen múltiples formas de que un hacker pueda acceder a la información confidencial de acceso a la cuenta de un tercero, que van desde la adivinanza pura, probando combinaciones de contraseñas reiteradas veces, hasta el uso de ***keyloggers***, intercepción de datos por transferencia electrónica, y otras formas que requieren herramientas informáticas más sofisticadas. En todos los casos, será factor determinante el nivel de seguridad del sitio donde se encuentra la base de datos, y el conocimiento y experiencia que posee el usuario al tomar medidas preventivas que aseguren la protección de sus datos.

Muchas veces, los atributos antes mencionados tienen especial utilidad cuando se requiere saber si se ha robado una cuenta o se ha accedido a ella sin permiso. Basta con analizar los ***logueos*** de la cuenta que se sospecha fue ***hackeada***, observar primero sus comportamientos habituales (con cuántas cookies se ***loguea***, cuál IP utiliza más frecuentemente y de dónde proviene, navegadores y hábitos de navegación, etc.), y comparar con las últimas conductas, a fin de verificar que haya diferencias (nuevas cookies, IP distinta) y otros comportamientos sospechosos, como movimientos de dinero inusuales, o cambios de datos importantes (contraseña o dirección de envío, son los más comunes).

Asimismo, este análisis en mucho de los casos, no sólo permitirá determinar si se accedió de manera ilegítima a una cuenta, sino también especular sobre quién ha sido, mediante el análisis de cruces nuevos y extraños con otras cuentas por cookies y otros atributos que utiliza el usuario para ***loguearse*** con todas ellas, hasta dar con su cuenta personal, que delatará su información.

(6) "Sobre la nube", sin necesidad de instalar ningún hardware o software
(7) Puntajes de riesgo que se le asigna a determinada cuenta, por distintas variables preestablecidas, para darle mayor (o menor) relevancia a su análisis
(8)La dirección que corresponde a la tarjeta o dispositivo de red, teóricamente única y permanente
(9) En el caso del device, por ejemplo, expertos en desarrollo especularon recientemente que en realidad se trata de un archivo que se almacena en el disco local (como la cookie), pero de difícil eliminación; y que el smart está basado en la configuración del sistema, desacreditando su utilidad ya que, siendo así, computadoras compradas en misma casa de electrónica pueden coincidir en smart, incluso de forma masiva
(10) Cumple con sólo una de las dos condiciones del ***principio de mismidad:*** es igual a sí mismo, pero no es diferente al resto.

Conclusión

Si bien el cambio desde los inicios en los procesos de prevención es significativo, y hoy en día existen atributos complejos, secretos e invisibles que podrían individualizar un dispositivo casi con total seguridad (como, por ejemplo, una combinación de coincidencias en contraseña-cookie/device), el constante avance tecnológico tanto en hardware(por ej.: la incorporación al mercado de dispositivos de conexión móvil) como en software y utilización de servicios "oncloud", y el fácil acceso a la información en materia de prevención que poseen los cibercriminales, complica aún más la tarea de los analistas de riesgo de fraude, quienes pretenden desde el principio un método que capture globalmente a los usuarios fraudulentos, y que hoy por hoy sigue siendo una meta imposible de alcanzar.-

Bibliografía

- "Is your device ID ready for the FFIEC", ThreatMetrix WhitePaper, en http://www.idgconnect-direct.com/images/IDG/Smart-Device-ID-for%20Online-Banking.pdf

- "Privacy Collides with Fraud Detection and Crumbles Flash Cookies", Gartner Research, 2010

- "Identificar clientes por su IP: un mecanismo obsoleto", Ing. Eduardo González G., en http://www.webnova.com.ar/articulo.php?recurso=360

- Página oficial de THM: www.threatmetrix.com

- Propia experiencia del autor