Huellas Digitales, El Futuro De La Seguridad Web

Tomar Huellas Digitales Desde HTML5, El Futuro De La Seguridad Web

Tomar las huellas digitales desde HTML5 no es una locura total. La tendencia de la seguridad web es usar uno de los elementos mas seguros de la naturaleza: Las huellas digitales, y Canvas podría ser el medio para obtenerlas. Uno de los sistemas que han estado utilizando es la duradera Evercookie, un método de seguimiento que no se borra, la cual explota la funcionalidad en HTML5. ¿Como termina una Cookie que no se elimina en su navegador? Se prevee que al final del 2014, podría ser usada para tomar las Huellas Dactilares desde el elemento Canvas de HTML5.

Las **huellas digitales en Canvas** está causando un gran revuelo en estos momentos, gracias a un trabajo de investigación publicado por tres investigadores de Princeton que trabajan en conjunto con un equipo de compañeros belgas. En realidad ha estado en uso en la red durante los dos últimos años. La técnica se desarrolló a partir del código original de Evercookie, que era de código abierto, el cual se publicó en la Web en 2010.

Parece que la mayor parte de la toma de huellas dactilares desde Canvas se está **desarrollando por AddThis**. La compañía admite plenamente que han estado jugando con evercookies, y señaló que esto es «perfectamente legal dentro de las normas y los reglamentos, leyes y las políticas.»

El director general de AddThis dice que están buscando algo

mejor que una Cookie tradicional. Las huellas digitales desde Canvas es sin duda, la mejor opción. No hay archivos que se escriben en la computadora del usuario que se pueda eliminar o bloquear con facilidad, y las huellas digitales mas exactas e irrepetibles.

¿Cómo Funciona?

Una página web que desee tomar las huellas dactilares, escribirá de manera invisible un poco de texto a la ventana del navegador. AddThis escogió «**cwm fjordbank glyphs vext quiz**» utiliza cada letra del alfabeto. Algunos otros proveedores decidieron que simplemente escribiendo el alfabeto en orden funciona muy bien, también. El texto se representa con variaciones sutiles en cada equipo (debido a cosas como las fuentes que ha instalado, el reloj del sistema, etc), y en ese sentido, es muy similar a las huellas digitales reales. El rastreador analiza la salida para identificar al usuario y también funciona para mostrar anuncios orientados.

El inconveniente de esto, es que los anunciantes sacarán mayor provecho (como si ya no lo hicieran), en otras palabras, siendo la huella digital un elemento único del usuario, ellos seguirán mostrando anuncios específicos para cada individuo. ¡Genial! Pensarán algunas personas, pero, recordemos que esta utilidad usa el rastreo de datos en los sitios web que visitemos, lo que denota una clara invasión a la seguridad del usuario.