Georeferenciación a nuestras espaldas

¿INVASIÓN O VENTAJA?

La idea para la columna de este número surgió de una plática con mi padre, comentando acerca de un texto que él presentó como parte del espacio de la Academia de Ciencias de Morelos en el periódico La Unión de Morelos el pasado 18 de abril [1]. En éste, habla sobre la disparidad de las cifras reportadas ante la manifestación dirigida por Javier Sicilia en Cuernavaca el pasado 6 de abril, y acerca de métodos que podrían utilizarse para tener una estimación más precisa. Yo, como buen consultor, le sugerí algo bonito y preciso en teoría, pero impracticable para todos los que no contamos con el poder coercitivo gubernamental: acceder a los registros de las compañías de telefonía celular, para averiguar cuántas personas entraron durante el periodo de nuestro interés a la región por donde cruzó la marcha. A fin de cuentas, una muy alta proporcionón de la población hoy en día cuenta con teléfono celular, y podría ser una buena manera no sólo de estimar la magnitud de la marcha, sino de hacerlo a lo largo del tiempo que duró.

Ahora, dado que la información que poseen las telefónicas no es pública, dejamos la conversación a un nivel puramente especulativo —seguros de que las autoridades de Seguridad Pública tienen acceso a estos datos, pero que a la mayor parte de nosotros nos resultan inalcanzables, como no sea a través de una órden judicial.

En los días siguientes a esta conversación, sin embargo, se presentaron varias noticias que se me hicieron interesantes, y que vinculan a esta discusión relativa a la participación ciudadana en la política nacional con temáticas más cercanas a las que toca esta revista: el cómputo ubicuo, la rastreabilidad de un dispositivo móvil, la seguridad de la información de geolocalización, y nuestro derecho a controlar quién tiene acceso a ella.

Gunnar Wolf es administrador de sistemas para el Instituto de Investigaciones Económicas de la UNAM y desarrollador del proyecto Debian GNU/Linux.
www.gwolf.org

Compañías telefónicas

En el diario alemán «Zeit Online» encontré un artículo publicado el 26 de marzo [2] que ilustra precisamente la profundidad de esta información: Malte Spitz, del Partido Verde alemán, presentó una demanda judicial para obligar a Deutsche Telekom a entregarle todos los datos suyos que tuvieran registrados en los últimos seis meses. Los datos están disponibles en crudo y adicionalmente se realizó una simple aplicación [3] para presentar esta información de una manera fácil de comprender. La aplicación nos permite apreciar la profundidad de los patrones de comportamiento que puede construirse de cada uno de nosotros: ubicación geográfica, llamadas y mensajes recibidos/enviados, conexión de datos, etcétera.

Si bien la geolocalización es mucho menos precisa que la que arrojaría un GPS (es obtenida por triangulación entre las torres de telefonía celular, resultando en una precisión de unos cien metros), el punto más importante es que esta información se genera y almacena centralmente, en las instalaciones del proveedor de telecomunicaciones, e independientemente de las capacidades tecnológicas de nuestro teléfono.

Y si bien Malte Spitz tuvo acceso a sus datos a través de los canales legales, ¿qué tanto podemos confiar en que dichos datos estén adecuadamente protegidos de los ojos de atacantes capaces de vulnerar servidores conectados a Internet? Precisamente, el experimento de Spitz fue llevado a cabo para sustentar el peligro de la ordenanza de 2008 que obliga (y por tanto permite) a las compañías de telecomunicaciones a guardar esta información por medio año —ordenanza que en marzo de 2010 fue declarada inconstitucional. En México nos hemos topado una y otra vez con casos en que datos confidenciales han sido encontrados en el mercado negro. ¿Qué nos garantiza que esta información, escalofriantemente precisa acerca de nuestros hábitos, no está disponible al mejor postor?

Proveedores de hardware

También en días recientes se publicaron noticias acerca de la información de ubicación que guardan los teléfo-

"LA TECNOLOGÍA VA CAMBIANDO NUESTRA VIDA, Y LO QUE PARA MUCHOS PUEDE SER VISTO COMO UNA INVASIÓN A LA PRIVACIDAD, PARA MUCHOS OTROS REPRESENTA LA GRAN CONVENIENCIA DE CONTAR CON UNA UBICACIÓN RAZONABLEMENTE PRECISA EN UN TIEMPO ACEPTABLE Y PODER COMPARTIRLA CON NUESTROS CONTACTOS FACILMENTE."

nos inteligentes. Los equipos iPhone e iPad de Apple que corren el iOS versión 4 o superior guardan un registro histórico de los puntos por los que ha pasado el usuario [4]. Y si bien esto no debería sorprendernos, hay tres puntos clave en lo revelado:

- Los datos son guardados sin cifrado, y son incluídos en todo respaldo hecho al dispositivo.
- La licencia de uso del software permite expresamente a Apple recolectar, usar y compartir información precisa respecto a la ubicación, incluyendo la ubicación geográfica en tiempo real de tu dispositivo.
- La información recopilada no se limita a una ventana de tiempo preestablecida, sino que durará la vida entera del equipo.

Para verificar (y/o jugar con) esta funcionalidad, pueden instalar en cualquier computadora con la que hayan sincronizado un iPhone o iPad el iPhoneTracker (MacOS) [5] o iPhoneTrackerWin (Windows) [6]. En el sitio del iPhoneTracker hay una interesante lista de cuestionamientos.

Claro, pero el que Apple controle los dispositivos que los usuarios han comprado no es novedad. Quienes me conozcan, probablemente esperan que haga a continuación una apología de por qué el software libre es más seguro, y por qué deberían todos cambiar a un teléfono basado en el sistema Android. Sin embargo, la situación no es tan distinta ahí.

Con la salvedad de que para que éste archivo exista el usuario tiene que haber aceptado previamente que el teléfono provea servicios relacionados con los datos de geolocalización (sin duda una muy importante característica de los equipos, y que poca gente dejará desactivada), los teléfonos Android guardan también información con nivel de detalle muy similar [7]. Al menos, la información no se mantiene a largo plazo: los dispositivos Android guardan solamente las últimas 50 ubicaciones derivadas de torres celulares, y hasta 200 derivadas de redes WiFi. Ahora, de este último punto podemos aún jalar más hilo: Si bien el contrato de licencia del software de Apple permite que reciban todos los datos de ubicación, hasta el momento han negado estar utilizándolos. Sin embargo, al autorizar a Android, explícitamente estamos autorizando que esta información sea reportada a Google. Adicionalmente, los dispositivos con Android notifican a Google la ubicación de cada red inalámbrica que encuentran, como lo demuestra el sitio Web desarrollado por Samy Kamkar [8].

Conclusión

Sé que este texto puede ser leído como una carta escrita por un paranóico de las teorías de la conspiración. No es así, estoy consciente de que la tecnología va cambiando nuestra vida, y lo que para muchos puede ser visto como una invasión a la privacidad, para muchos otros representa la gran conveniencia de contar con una ubicación razonablemente precisa en un tiempo aceptable y poder compartirla con nuestros contactos facilmente.

Mi convocatoria, claro, al tiempo que lleva a que tengamos conciencia de los insospechados ojos que pueden estar aprendiendo de nuestras vidas con cualquier tipo de fines, también lleva a que, como desarrolladores de aplicaciones, sepamos ser creativos y aprovechar la información que tenemos a nuestro alcance — ¡Porque sin duda podrán encontrar también maneras lícitas y atractivas de emplear estas fuentes de información! SG

››Por Gunnar Wolf

Referencias

[1] Kurt B. Wolf. *"¿Cuántos miles marchamos?"*, La Unión de Morelos, 18 de abril 2011, pag. 34. http://bit.ly/sg32r5

[2] Kai Biermann. *"Betrayed by our own data"*, Zeit Online. http://bit.ly/sg32r6

[3] "Tell-all telephone", Zeit Online. http://bit.ly/sg32r7

[4] Dan Goodin. *"iPhones secretly track scary amount of your movements"*. The Register. http://bit.ly/sg32r8

[5] Alasdair Allan, Pete Warden. *"iPhoneTracker"*. http://bit.ly/sg32r9

[6] Huseyin T. "iPhoneTrackerWin". http://bit.ly/sg32r10

[7] Matthen Panzarino. *"It's not just the iPhone, Android stores your location data too"*. The Next Web. http://tnw.co/sg32r11

[8] Samy Kamkar. *"Android Map"*. http://bit.ly/sg32r12