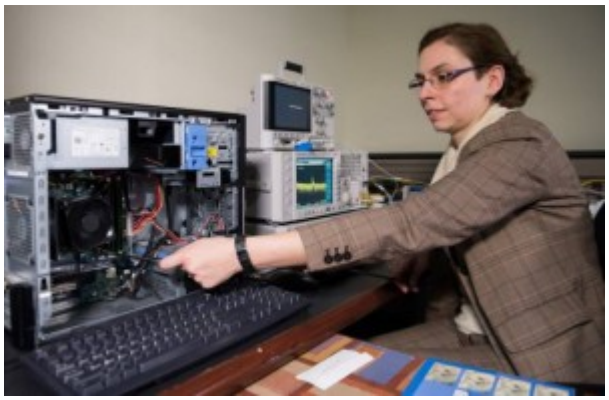
Hackear ordenadores inalámbricamente aunque no estén nunca conectados a internet ni a redes de telefonía celular



Incluso sin estar conectado a internet ni a una red de telefonía celular, un ordenador puede ser rastreado desde cierta distancia física por las débiles señales eléctricas que emiten sus componentes al funcionar, así como por otras señales sutiles. Un espacio público compartido con un hacker, o la actividad de este lo bastante cerca físicamente (por ejemplo en la vivienda de al lado), pueden dar pie a una operación de espionaje más eficaz de lo que podríamos imaginar. Este riesgo de seguridad, hasta donde se sabe, aún no está siendo explotado a fondo, pero es cuestión de tiempo que pase de ser empleado solo en eventuales operaciones de los servicios secretos a ser utilizado por ciberdelincuentes.

Las señales de canal lateral (señales provenientes de fuentes indirectas de información) emitidas por los ordenadores y los teléfonos móviles podrían proporcionar a los hackers una forma alternativa de ver qué están haciendo dichos dispositivos. Analizando las señales electrónicas de baja potencia emitidas por estos aparatos, incluso cuando no están transmitiendo en internet o en las redes celulares, los hackers pueden obtener información sobre operaciones informáticas e incluso hacer un seguimiento que les lleve a averiguar contraseñas.

Y los teléfonos inteligentes podrían incluso ser más vulnerables ante este tipo de espionaje.

El equipo de la profesora Alenka Zajic, del Instituto Tecnológico de Georgia (Georgia Tech), ubicado en la ciudad estadounidense de Atlanta, está investigando en qué puntos se originan esas "fugas" de información a fin de poder ayudar a los diseñadores de hardware y software a desarrollar estrategias para evitarlo. Estudiando emisiones de varios ordenadores, los investigadores han desarrollado una serie de baremos para medir la intensidad de las fugas, conocidas técnicamente como "señales de canal lateral", para ayudar a priorizar los esfuerzos de seguridad.

Dichas emisiones pueden ser medidas desde varios metros de distancia de un ordenador en funcionamiento, utilizando varios métodos de espionaje. Las emisiones electromagnéticas pueden ser recibidas usando antenas ocultas en un maletín, por ejemplo. Las emisiones acústicas, sonidos producidos por los componentes electrónicos, como los condensadores, pueden ser captadas por micrófonos especiales escondidos bajo las mesas. La información sobre las fluctuaciones energéticas, que puede ayudar a los hackers a determinar qué está haciendo el ordenador, puede ser medida a través de cargadores de batería falsos, enchufados cerca del transformador de corriente de un portátil.

Algunas señales pueden ser captadas con una simple radio AM/FM, mientras que otras requieren analizadores de espectro más sofisticados. Y los componentes de los ordenadores, como reguladores de voltaje, producen emisiones que pueden transportar señales producidas en otras partes de un ordenador portátil.

Como demostración, Zajic tecleó una contraseña simulada en un portátil que no estaba conectado a internet. Al otro lado de la pared, un colega utilizando otro portátil desconectado leyó la contraseña a medida que era tecleada al interceptar las

señales de canal lateral producidas por el software del teclado del primero, bajo condiciones propicias.

fuente:noticiasdelaciencia