'Crackean' el sistema de algunos mandos de apertura de coches y edificios

Los mandos de apertura que utilizan el sistema de encriptación *RFID KeeLoq* -muy utilizado en Europa y EEUU para poder acceder a coches, garajes y edificios sin necesidad de abrir con las llaves-, tienen una vulnerabilidad que permite 'crackearlos' desde una distancia de 100 metros sin dejar rastro, según informan expertos en seguridad de la universidad alemana del Ruhr-Bochum (RUB).

SINC 10/4/2008 15:38 CEST

Foto: SINC.

El descubrimiento forma parte de la actividad investigadora que realiza el equipo del profesor Christof Paar, del Grupo de Seguridad en las Comunicaciones del departamento de Informática e Ingeniería Eléctrica de la RUB. Paar explica que el fallo detectado "permite a personas no autorizadas acceder a edificios y automóviles después de realizar una escucha remota desde distancias de hasta 100 metros".

La vulnerabilidad afecta a todos los sistemas de control de acceso para edificios y automóviles que utilizan el cifrado *KeeLoq*. Para demostrarlo, los investigadores aplicaron las últimas tecnologías en descifrado de código, y

elaboraron varios tipos de ataques. El más “devastador” es la clonación de las llaves que incorporan esa tecnología en automóviles y edificios desde distancias de hasta 100 metros. “Mediante la intercepción de sólo dos mensajes, personas no autorizadas pueden duplicar su llave y abrir su garaje o desbloquear su automóvil”, afirma el profesor Paar. Mediante otro ataque malintencionado, es posible manipular remotamente la puerta de un garaje o de un coche, de modo que las llaves legítimas dejen de funcionar.

El sistema *KeeLoq* consiste en un transpondedor de identificación por radiofrecuencia (RFID) -incluido, por ejemplo, en la llave de un coche-, y un receptor -por ejemplo incluido en la puerta del automóvil-. Tanto el receptor como el transpondedor utilizan *KeeLoq* como método de encriptado para proteger la transmisión que se realiza a distancia. El ataque realizado por el equipo de Bochum permite recuperar las claves criptográficas secretas incluidas tanto en el receptor como en el transpondedor. El ataque se basa en la medida del consumo eléctrico del receptor. Aplicando los denominados métodos de “análisis de canales laterales a las trazas de potencia”, los investigadores pudieron extraer la clave del fabricante de los receptores.

La eficacia del ataque se ha confirmado realizándolo en sistemas reales que utilizan *KeeLoq*. Este sistema se utiliza para el control de acceso desde mediados de la década de 1990, y según algunas estimaciones es el más utilizado en Europa y EE UU. Además de su uso frecuente en mandos de apertura de puertas de garaje y otras aplicaciones de acceso a edificios, varios fabricantes de automóviles, como Toyota/Lexus, basan su protección antirrobo en sistemas que se suponen seguros y que utilizan *KeeLoq*.