30-05-2012

Un investigador de Cambridge descubre la puerta trasera en circuitos integrados de uso militar

JJ Velasco
alt1040

Hoy en día es complicado encontrar un sistema electrónico que se haya construido mediante lógica discreta, es decir con circuitos integrados que contienen puertas lógicas o biestables, sino que por regla general se suelen abordar los diseños utilizando una buena parte de dispositivos electrónicos programables, ya sean microcontroladores o dispositivos lógicos programables, como las FPGAs. Una de las ventajas de utilizar este tipo de dispositivos es es mucho más complicado realizar ingeniería inversa puesto que hay que averiguar la programación del dispositivo y si, además, pasamos al ámbito de los circuitos electrónicos de ámbito militar, la protección del hardware contra este tipo de prácticas es mucho mejor. Hasta ahora, ésta siempre ha sido la tesis que se había manejado para los chips para aplicaciones militares, sin embargo, un investigador de la Universidad de Cambridge ha publicado unas notas relativas a sus investigaciones en el ámbito de la seguridad del hardware que vienen a tambalear estos cimientos puesto que, según indica, ha descubierto puertas traseras en algunos circuitos integrados que son utilizados en aplicaciones militares de Estados Unidos.

¿Y qué es una puerta trasera en un circuito integrado? Básicamente es un concepto similar al de las puertas traseras del mundo del software, es decir, un mecanismo que permite que el fabricante o un tercero pueda acceder al código con el que se ha programado el circuito integrado sin demasiado esfuerzo y, por tanto, poder obtener un diseño completo del sistema, alterar la programación del dispositivo o borrarla.

Según comenta el Doctor Sergei P. Skorobogatov del Laboratorio de Computación de la Universidad de Cambridge, este hallazgo era algo esperado y que ya había sido advertido por algunas agencias de inteligencia como el MI5 del Reino Unido o la NSA de Estados Unidos y, con la idea de comprobarlo, ha desarrollado un sistema de detección que permita verificar la existencia de puertas traseras en dispositivos electrónicos programables.

La sorpresa se la han encontrado al analizar un circuito integrado muy utilizado dentro de la industria del militar de Estados Unidos y que se presuponía muy seguro puesto que se había hecho un gran énfasis, durante su diseño, en el cifrado del código almacenado en éste. Sin embargo, por muy seguro que era este chip y su grado de utilización en aplicaciones militares, el circuito integrado era fabricado en China y, por lo que ha podido comprobar el Doctor Skorobogatov, el fabricante había insertado una puerta trasera (modificando el *layout* del circuito integrado) que podía ser activada con "una clave" que permitía extraer el software grabado en él, alterarlo o, directamente, borrarlo independientemente de las medidas de seguridad que hubiese insertado el integrador del circuito.

Si tenemos en cuenta que, según Skorobogatov, este chip se utiliza en sistemas de armas, plantas de energía nuclear o incluso medios de transporte, la existencia de esta puerta trasera es toda una amenaza. De todas formas, para que no cunda el pánico, este investigador no ha dado pista alguna sobre el circuito integrado en cuestión pero, la verdad, da mucho que pensar que un dispositivo para aplicaciones críticas se envíe a fabricar, precisamente, a China.

Más del 90% de los circuitos integrados que se fabrican en el mundo tienen su origen en China y parece claro que, tras leer las conclusiones de Skorobogatov, no estaría de más realizar ciertas comprobaciones y verificaciones para certificar que un circuito integrado es seguro y no presenta ningún tipo de alteración; precisamente ahí es donde entra el sistema de validación que ha realizado y con el que pretende evitar este tipo de vulnerabilidades.

¿Amenaza real o auto-promoción? La verdad es que las conclusiones publicadas por Skorobogatov dan mucho que pensar y, desde luego, no sería muy descabellado que este tipo de cosas pudiesen ocurrir. Sin embargo, bajo mi punto de vista, nadie en su sano juicio fabricaría componentes para aplicaciones muy críticas en terceros países sin el adecuado control de calidad y supervisión, ¿verdad? Vale la pena echarle un vistazo a un informe publicado la semana pasada por el Comité de Servicios Armados del Senado de Estados Unidos y los 1.800 casos de circuitos electrónicos vulnerables no solamente por "mala fe" sino también por intentos de ahorrar en su fabricación.

Fuente:
http://alt1040.com/2012/05/puerta-trasera-circuitos-integrados-uso-militar?utm_source=self&utm_medium=banner&utm_campaign=Destacados%2BHome