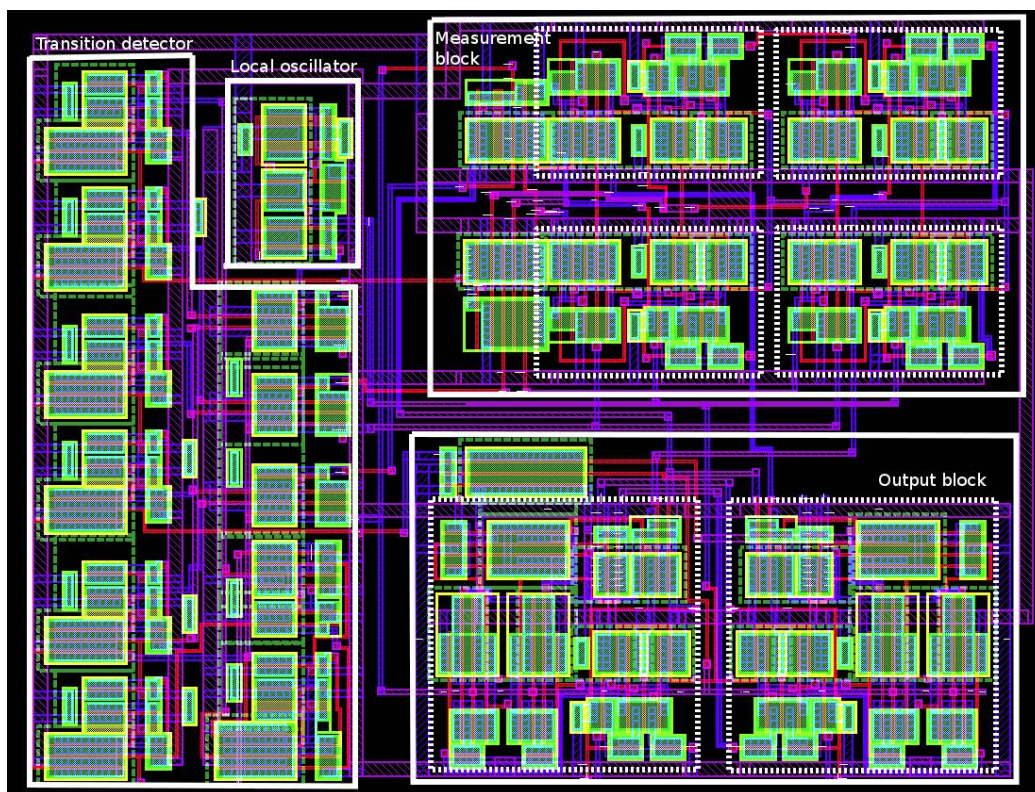


Sensores para proteger de 'ataques' a los dispositivos electrónicos

Investigadores de la Universidad de Huelva (UHU) han desarrollado un nuevo mecanismo que garantiza la seguridad de los sistemas electrónicos frente a los intentos de acceso a información particular restringida. El programa permite, por ejemplo, proteger al usuario del intento de acceso cibernético a las claves personales de su ordenador, tarjeta de crédito o cuenta corriente.

Fundación Descubre

14/1/2014 10:32 CEST



Esquema de uno de los sensores. / UHU-Fundación Descubre

Un equipo del departamento de Ingeniería Electrónica de Sistemas Informáticos y Automática de la Escuela Politécnica Superior La Rábida de la Universidad de Huelva (UHU) ha creado un nuevo mecanismo que garantiza la seguridad de los sistemas electrónicos frente a aquellos ataques utilizados para obtener información de carácter restringido de un determinado usuario.

En concreto, los expertos se han basado en la modificación puntual de la frecuencia de la señal de reloj (encargada de coordinar las rutinas internas) de cada dispositivo. Es decir, esta alteración no permite al sistema disponer del tiempo suficiente para realizar una acción determinada y de esta forma, este es 'engañado' al considerar que la operación ya ha sido efectuada correctamente.

El equipo se ha basado en la modificación puntual de la frecuencia de la señal de reloj

En el trabajo, publicado en la revista [Sensors](#), los investigadores han desarrollado e implementado un sensor configurable que permite proteger a los dispositivos electrónicos sin necesidad de modificar el diseño del sensor.

“Este componente mejora el comportamiento de parámetros como el consumo de potencia, la resolución o la adaptación a diferentes tecnologías. Además, permite la incorporación de nuevos mecanismos como las alarmas, capaces de alertar al sistema de un ataque para que éste pueda alterar o eliminar la información confidencial gracias a este aviso previo”, explica uno de los investigadores, Raúl Jiménez-Naharro.

El mecanismo consiste en la creación de un nuevo sensor capaz de determinar si la frecuencia de la señal de reloj se encuentra dentro o fuera de un rango adecuado, el cual permite identificar cuándo se está produciendo un ataque en un dispositivo determinado.

“En el caso de que la señal se encuentre dentro del rango apropiado, el sistema no ‘ve’ al sensor, es decir, éste no tiene influencia ninguna sobre él y no se produce ninguna modificación”, sostiene Jiménez-Naharro. “Sin embargo, en el caso de estar fuera del rango, el sensor no permite el paso de dicha señal y paraliza la operación hasta que dicha frecuencia vuelve a estar en el nivel correcto, es decir, cuando la amenaza ha desaparecido”.

Un mecanismo aplicable

La aplicabilidad de este nuevo mecanismo de seguridad está relacionada

con cualquier sistema que sea susceptible de ser atacado con el fin de extraer información confidencial o alterar el comportamiento para el que fue diseñado.

“Además del ámbito económico a la hora de proteger el acceso a las tarjetas de crédito o cuentas corrientes, su utilidad se extiende a la esfera doméstica donde un usuario puede acceder a servicios como canales de pago sin abonar la cuota correspondiente o también en el sector aeronáutico, ya que ciertos ataques en el piloto automático de un avión pueden alterar su rumbo sin que éste sea detectado”, apunta el investigador.

Asimismo, el trabajo ha permitido abrir nuevas líneas de investigación con el objetivo de desarrollar diferentes estrategias de acción ante otros tipos de ataques que pueden recibir los dispositivos. “Por otro lado, si nos centramos en la parte de diseño, pretendemos mejorar aún más las características y el comportamiento (en el sentido de incluir nuevas funcionalidades) del sensor”, apostilla.

Estos resultados son fruto del proyecto de excelencia *CRIPTO-BIO: Diseño Microelectrónico para autenticación cripto-biométrica*, financiado por la Consejería de Economía, Innovación, Ciencia y Empleo de la Junta de Andalucía y que incluyó la colaboración entre investigadores de las Universidades de Sevilla, Huelva y Politécnica de Madrid y del Instituto de Microelectrónica de Sevilla (CSIC).

Copyright: **Creative Commons**

TAGS

DISPOSITIVOS ELECTRÓNICOS | SENSORES | SEGURIDAD |

Creative Commons 4.0

You can copy, distribute and transform the contents of SINC. [Read the conditions of our license](#)

