GRUPO DE INVESTIGACIÓN BISITE .usal.es

VNiVERSiDAD D SALAMANCA
CAMPUS DE EXCELENCIA INTERNACIONAL

MEJORANDO LA SEGURIDAD DE LAS PCB FRENTE A HACKEOS

Autor: Jorge Herrera Santos
Revisado:

Fecha: 12/04/2019 **Versión:** 1.0

CONTENIDO

1. OBJETIVOS

La seguridad en aspectos como el IoT es uno de los aspectos que está centrando la atención en el mundo del diseño y la fabricación de dispositivos electrónicos debido al aumento significativo en el uso de este tipo de dispositivos. Aplicando las estrategias descritas a continuación, se disminuirá mucho el posible riesgo de intrusión, aunque no garantiza que el dispositivo sea totalmente seguro.

2. PROTECCIÓN CONTRA INTERFERENCIAS ELECTROMAGNÉTICAS (EMI)

EMIs producidas por el circuito pueden dar al atacante información de que está pasando en el circuito usando “sniffers” baratos. EMIs producidas por los hackers pueden manipular o confundir nuestro circuito. La solución sería proteger el circuito mediante “shields” mecánicos hechos de materiales que protejan la electrónica de interferencias electromagnéticas.

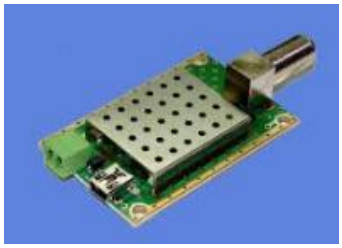

Figura 1. Shield metálico protegiendo frente a EMI

3. CIRCUITOS A PRUEBA DE MANIPULACIONES

La mejor manera de mitigar el riesgo es diseñar el dispositivo a prueba de manipulaciones con el objetivo de detectar si alguien ha tenido acceso a la PCB. La idea es adoptar medidas como incluir interruptores físicos que sean activados cuando el dispositivo es abierto. Una vez se detecte esa brecha de seguridad, se pondrán en marcha una serie de contramedidas:

- Mandar una señal de alerta. Esto es posible si el circuito incluye comunicaciones inalámbricas o físicas con otro dispositivo.
- Borrar memorias que tenga el dispositivo.
- Cortar la alimentación del dispositivo.

- En casos de dispositivos que necesiten una seguridad extrema, se puede destruir el dispositivo con un pequeño explosivo.
- Incorporando sensores inductivos al diseño de la PCB que, mediante una placa metálica colocada en la carcasa mecánica, detecten la manipulación cuando la carcasa es abierta.

Figura 2. PCB con sensores inductivos incorporados

4. ESCONDIENDO COMPONENTES

La idea es dificultar la obtención de datos del circuito mediante el diseño de este mismo. Para esto se puede recurrir a las siguientes estrategias:

- **Cubrir los chips en epoxy:** si pines y componentes son cubiertos con epoxy será más difícil para los hackers tener acceso a ellos.

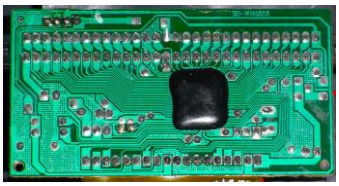

Figura 3. Chip cubierto con epoxy

- **Usar componentes de difícil acceso:** algunos componentes son difíciles de aprovechar por su naturaleza. Matrices de rejillas de bolas (BGA en sus siglas en inglés), por ejemplo, tienen los contactos por debajo del paquete. Esto hace casi imposible acceder a los pines.

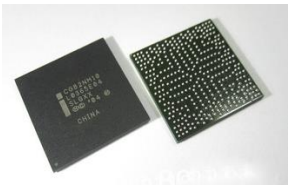

Figura 4. Chip BGA

- **Usar vías ciegas y vías enterradas:** mediante el uso de vías no solo se ahorra espacio, sino que además de protege la información. Es casi imposible acceder a ellas, por lo que lo que sea que se esté transmitiendo por ellas.

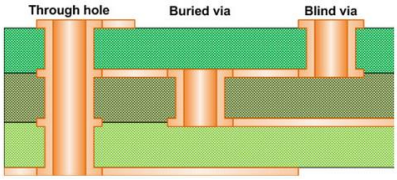

Figura 5. Tipos de vías

- **Relleno de la vía no conductivo:** rellenando, colocando o tapando las vías con un material no conductor a la hora de fabricar la PCB ayudará a garantizar que estas vías no sean fácilmente localizables.
- **Borrando el nombre de los chips:** los chips están sellados son su nombre. Si un atacante conoce a que chips que enfrenta, puede conocer sus vulnerabilidades. Borrar el nombre de los chips lijándolos de tal forma que su identidad sea desconocida hará más difícil el trabajo de los hackers.

Encriptando la información mediante hardware

Encriptando la información desde la capa física mediante el uso de chips criptográficos añade una capa más de protección en el envío y tratamiento de los datos.

5. REFERENCIAS

[1] *Altium Blog.* *IoT Security: Physical Layer Security for IoT PCBs.* *10 mayo 2017*

[2] *Steve Melito.* *What is EMI Shielding and Why is it Important for Your Design?* *7 marzo 2017*

[3] *Jorge Rivera.* *Seguridad criptográfica en IoT.* *18 abril 2016*

[4] *Texas Instruments. Case Tamper Detection Reference Design Using Inductive Sensing. Junio 2017*