June 25, 2019

AN ANTI-TAMPET METHOD TO PROTECT TPM BE HACKING

HP INC

An Anti-tamper method to Protect TPM be Hacking

Abstraction

For high security laptop or PC, TPM is the security kernel of modern computer which includes important data, for example, key or pins. However, there are many reports show it can be hacked by software or physical attacking. Current TPM are slightly harder to attack, but not very much harder. Infineon, TPM IC provider, commented that they knew this was possible due to the high skill level necessary for success. Here we introduce a method to protect it by a micro switch sensor with a firmware in EC.

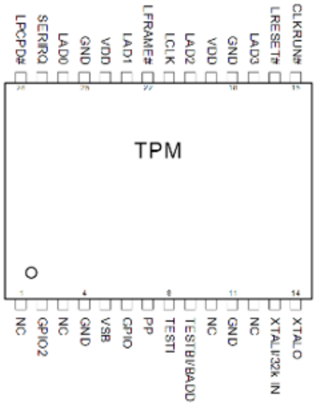
Method

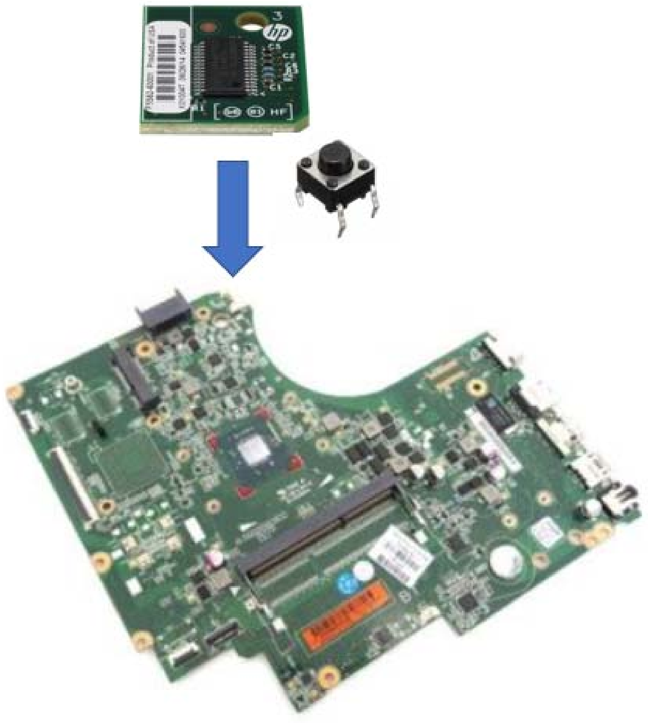
Physical attacking on TPM are always interesting topic for hacker. For example, the lock bit of several devices with on-chip EPROM can be erased by focusing UV light on the security lock cell, which is located sufficiently far from the rest of memory. The following is a simple way to unmount the TPM module and reverse by utility.

One method revealed a hack way at Black Hat event. The method is wicked-hard, involving removal of the chip's case and top layer, then tapping into a data bus to get at unencrypted data. The core die inside TPM is a smart card controller, the silicon die is glued to the other side, and connected using thin gold or aluminum bonding wires. The chip side of the plastic plate is then covered with epoxy resin. Removing the chip is easy. First, we use a sharp knife or hand lathe to cut away the plastic behind the chip module until the epoxy resin becomes visible. Then settling a few drops of fuming nitric acid on the resin and wait until some of it has dissolved. The other way appearing to be done is a capacitive sensor to detect the continued presence of the passivation layer, or an optical sensor under an opaque coating.

The following is the bottom view of the TPM module, we can see there is a connector between motherboard and it.

The following is the pin assignment of TPM, it uses LPC to communication with external micro controller.





We put a micro switch sensor between the TPM and motherboard, and the output pin is connecting to on GPIO of EC controller. The VCC of TPM are provided by battery of mother board so the power is keeping even the computer is turned off. When there is someone that wants to hack it, it will trigger the micro switch sensor and interrupt the ISR of EC, then EC will send wrong key 3 times to block it on purpose to physically lock TPM. And then all the security data inside TPM will be destroyed.

Algorithm

```
EC_ISR which is trigger by micro switch()
{
   Block TPM ()


}
```

```
Block TPM ()
{
  Send wrong key 3 times to block it on purpose.
 }
```

Disclosed by David Ke, HP Inc.