Hiding your data in plain sight

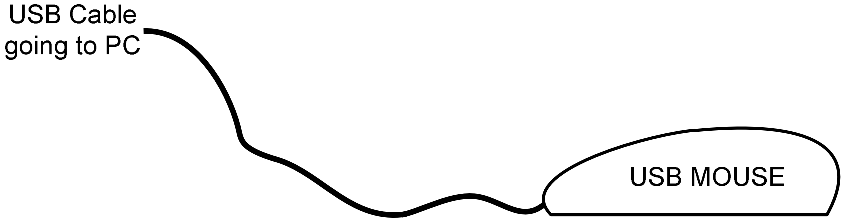
This article will describe the possibility of hiding data in any kind of USB hardware. Even though USB data carriers come in various sizes and forms, which already sometimes makes them hard to recognize, this approach could even make it worse. Any USB device could be a data carrier and thus from a forensics point of view, any USB device should be taken into account when investigating a computer. Or, for example, from a company protection point of view, any USB device could be used to transport data out of the company.

The reason for writing this article is that the approach described in it has already been developed by me around 2007, while I was still working for the company Fox-IT. I presented part of this paper during a presentation I gave on the ENFSC 2007 congress, but since then I never made the full research completely public. I recently decided to redo my research and to work the idea out further. Since the information in this article is still current, I decided to spread the knowledge on it by publishing this article.

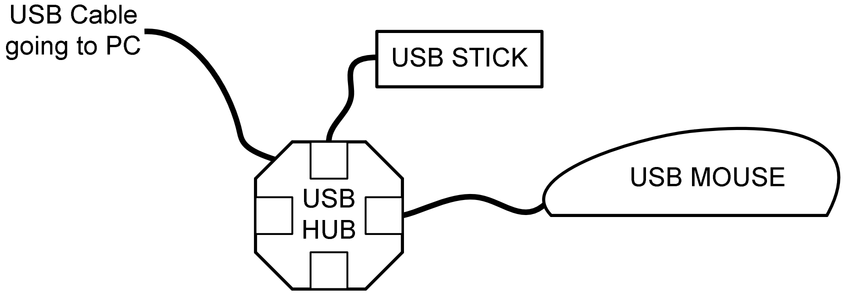
Any brands shown on the pictures in this paper are chosen because they were fairly cheap and available during the research. The approach described in this paper has nothing to do with the specific brands being used.

Theory

The theory behind the hiding of the data is pretty simple. A normal USB device will have a USB cable which can be connected to a USB port on the computer. This simple fact is shown in the schematic below using a USB mouse.



An alternative would be to connect the USB device to the computer through a USB hub. This USB hub can then also be used to connect other USB devices, for example a USB stick. This approach is shown in the schematic below.



The data hiding technique will take the second approach with the USB hub, but instead of connecting everything together like normal usage would be, the different devices will be combined together. The USB hub and the USB stick (which is a data carrier) will be combined with the USB mouse, resulting in one device. This way, only the USB mouse will be connected to the computer while its internals will contain the USB hub and the USB stick. So the USB stick will in fact be hidden inside the USB mouse. Anyone encountering the USB mouse will probably not suspect the USB hub and USB stick inside of it and thus the mouse can be used to secretly store data on it.

The described approach does not limit itself to hiding data, this approach can also be used to create a malware infected USB item. By combining the hiding of the hardware with an autorun kind of malware this combination could be used to spread malware and infect systems. Quite a lot of people nowadays are aware of the risks of inserting a USB stick in their system since that can lead to a malware infection. However probably no one will have that same idea about inserting a USB mouse into their system. Using the hardware hiding technique, any USB device can be a disguised malware infected data carrier.

Theory in action

The following part of this article will show the before mentioned theory in action. To show the possibilities of the approach the target will be to hide a USB data carrier inside a USB mouse. A mouse has a very limited space to add hardware inside of it, meaning that if hiding hardware is possible in this limited space it can also be done in much bigger USB devices like a USB keyboard or a USB printer.

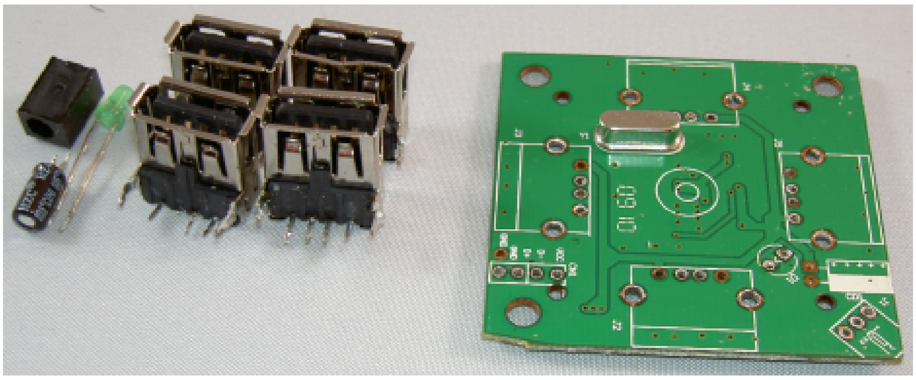
The hardware that will be put together can be seen on the picture on the right. A USB hub, a USB mouse and a USB stick will be combined and only the USB mouse will be left in the end.

The specific USB mouse used in this example contains an internal color changing LED which besides giving the mouse a nice glow also makes the hiding a bit harder. When the LED is blocked by the added hardware it might give an indication that something is wrong with the mouse. This makes it more challenging to perform the trick with this mouse, the trick would be much easier with a more plain mouse.

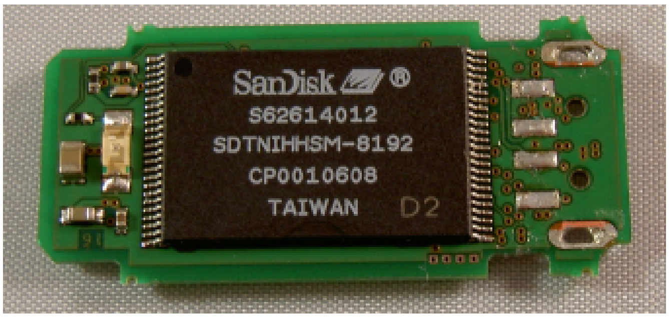
Stripping the components

Since the space inside the mouse is very limited it will not be possible to just fit a USB hub and USB stick inside it. It will be needed to lose as many unnecessary parts as possible. The outer shell of the USB hub can be removed which leaves the cable and the PCB[1] with several components. Any component on the PCB that is not needed will be stripped by desoldering, including the cable, different connectors and the signal LED. The result will be a PCB mainly containing the USB hub chip and some small components that are necessary for the chip to work. The result of the stripping of the USB hub can be seen below.

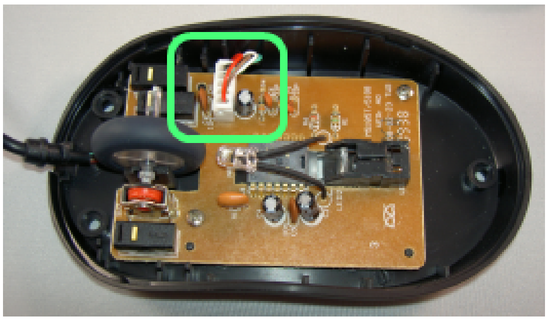
[1] Printed Circuit Board, the (usually green) board on which most of the electronic components are located.



Stripping the USB stick is much easier than stripping the USB hub. USB sticks usually only contain a plastic encasing and a USB connector besides their main PCB, an exception to this being the reinforced and special protected USB sticks, which are therefore less suitable to use for this kind of projects. After removing the outer casing of the USB stick the USB connector can be desoldered, resulting in a small PCB containing the memory chip and some other small components. The result can be seen in the following image.



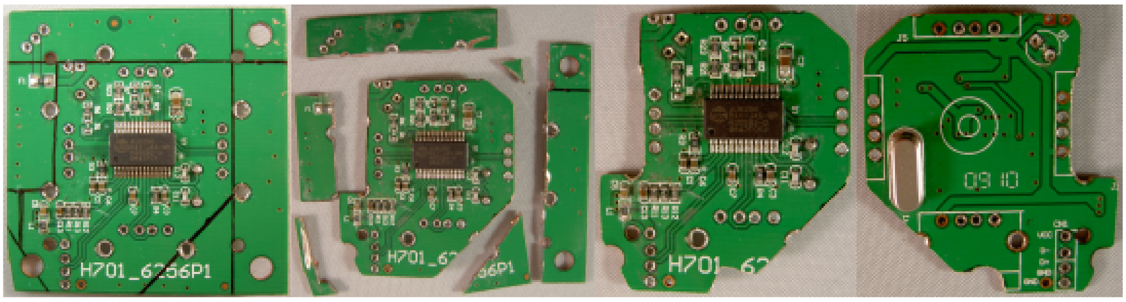
The USB mouse will not be stripped down further, however, to make more room it would be possible to cut away some of the plastic inside it, or even to reduce the size of the PCB. Inside the USB mouse the USB cable will be connected to the PCB, this can be done by soldering or by a connector. The image below shows the connector inside the mouse used in the example, in this case the cable is connected by a connector.



This connector inside the mouse will be disconnected as this cable will be connected to the USB hub. To connect the cable to the USB hub the wires will be cut and then soldered to the PCB of the USB hub.

Modification of the USB hub

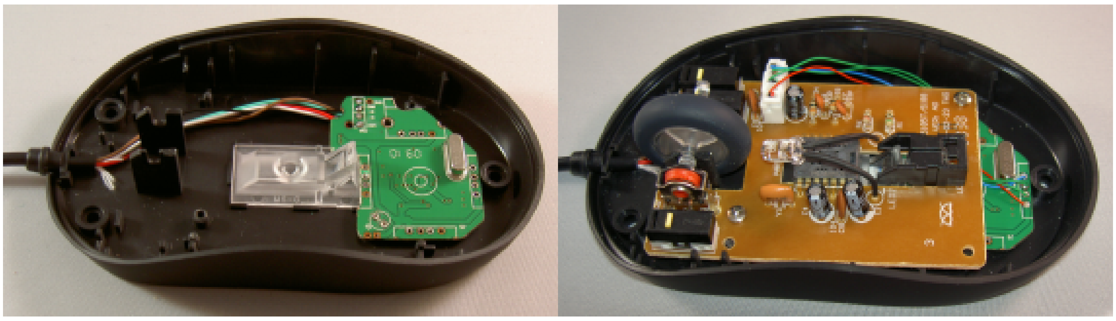
It would be possible to put the USB hub PCB on top of the mouse PCB, however, this would block the before mentioned internal color changing LED of the mouse. To avoid this, the PCB of the USB hub will be placed underneath the mouse PCB in a pretty narrow location.
To be able to fit the USB hub underneath the mouse PCB it has to be adjusted to make it smaller. The PCB of the USB hub contains quite some space where the USB connectors were located, since the USB connectors got removed this space is no longer needed. A large part of this unneeded space can be removed from the PCB and will thus result in a quite a bit smaller PCB.
The four pictures below show the modification of the USB hub PCB. The first two pictures show the parts of the PCB that got cut off to make it smaller. The last two pictures show the resulting PCB from two sides.



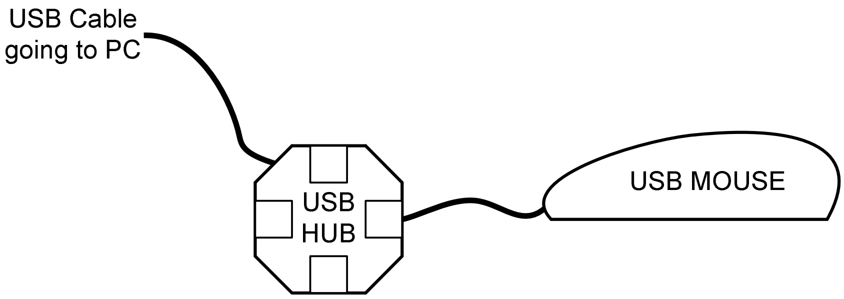
The PCB is now small enough to fit perfectly inside the mouse underneath the PCB of the mouse and will thus not block the internal color changing LED.

Putting the parts together

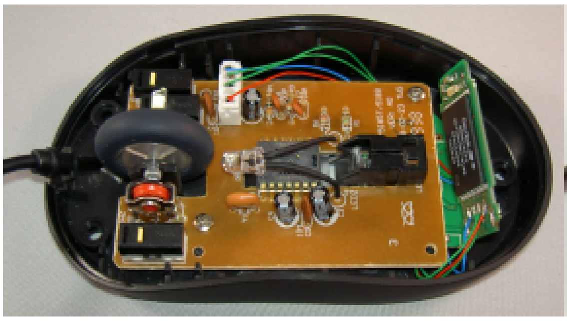
The following two pictures show the adjusted USB hub PCB soldered to the original USB connector of the mouse, beneath the PCB of the mouse itself. The hardware of the mouse is then wired to one of the USB ports of the USB hub.



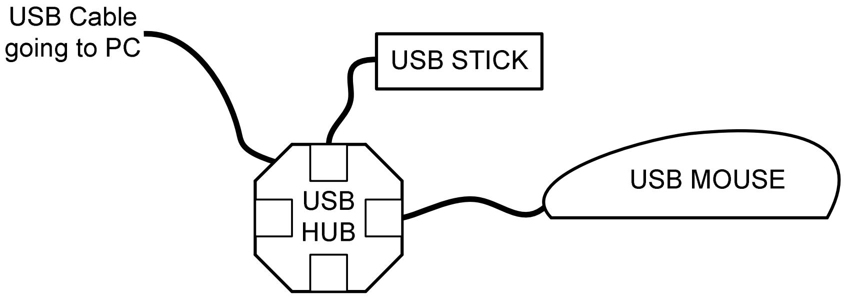
Instead of using connectors, the USB hub and mouse are connected by soldering the wires directly to the USB hub PCB. The schematic below shows the connections from the images above, the mouse will be connected through the USB hub and can thus be used again like normal when connected to a computer.



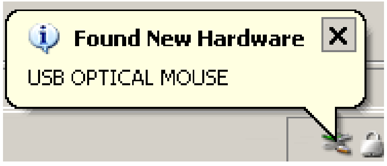
The next step will be to connect the USB stick to one of the other available ports of the USB hub. This also will be done by soldering wires directly between the components. After this step the mouse is ready and can be put together. The two steps are shown below, with the right picture showing the mouse connected, including the color changing LED still working.



The USB stick is connected like shown in the schematic below. There are still two USB ports left on the USB hub that was used. These ports could be used to connect two more USB devices, for example to be able to store more data inside the mouse.

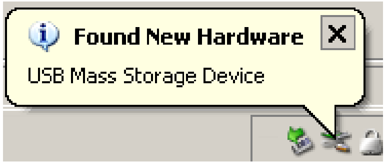


After everything is done correctly and the mouse has been put together the mouse can be connected to a computer again. When connected the computer will find both the hardware devices, like shown in the images below.



Found New Hardware ☒

USB OPTICAL MOUSE



Found New Hardware ☒

USB Mass Storage Device

The mouse as well as the USB stick can now be used on the computer. Any data stored on the USB stick will now be hidden inside the mouse

Project variations

This project used a USB mouse as the device to hide data inside, variations to this approach are possible. A USB keyboard for example already has quite some more space to perform this project. Even bigger devices like printers might enable this project without having to strip the items from their components to make them smaller. Some devices sporting a USB connection are equipped with an internal USB hub, for example monitors or USB keyboards, in those cases it is not even needed to use an extra USB hub. Or it could even be possible to only use a USB hub, if the USB hub is big enough it would be possible to fit a data carrier inside it.

The example was using premade USB devices to show how easy it is to get these parts and to get a clearer image on how the approach works. However if an attacker really would want to make something small enough to fit inside anything, he could just create a small PCB only containing a USB hub chip together with a data storage chip and some soldering pads.

Conclusion

While this research does not in any means break the USB protocol, it does extend what is possible with USB and for what purposes it can be used. Since any USB device can contain data, it is not enough to just focus on the obvious USB data carriers like USB hard drives or USB sticks. This is especially important for IT based forensic investigations. Any forensic IT investigator should keep in mind that when performing a forensic investigation, any USB device could be a data carrier and thus should be taking into account when acquiring evidence. Indicators that a device has been tampered with could for example be broken seals or markings on the screws. Data stored on a hidden data carrier could be anything like sensitive information, illegal things or cryptographic keys.

Also, besides hiding data any attacker could also try to infect another system by creating a malware infected USB device, people should take this into account when plugging any USB device into their systems.

Thijs (Thice) Bosschert
http://www.thice.nl