

## How to Protect Your USB Ports

Written by Marco Attard  
10 March 2017

---

Customers worried about BadUSB, the malware able to maliciously reprogram USB chips? Developer Robert Fisk has a hardware solution with the USG, a "firewall for your USB ports."



BadUSB is a sinister piece of malware able to bypass the OS, antivirus software and other security measures. It can attack by hopping into PCs through the USB port, for example via USB sticks supplied by customers or colleagues. This led to Fisk working on a hardware solution for access to untrusted USB devices, without need for a USB condom or disabling USB ports.

The USG is plug and play, and is compatible with many devices with a USB port, be it modern Windows, Mac OS and Linux machines or legacy and embedded systems. It supports mass storage (flash drives), keyboards and mice, but cannot handle hubs and only uses 12Mbps USB hardware.

It has 2 USB connectors, each tied to an own ARM controller. The controllers communicate with each other using a limited set of instructions in order to stop attacks such as BadUSB, isolating such malware while passing the required data. The device is fully open source down to the firmware, and "the truly paranoid" can build their own firmware.

Currently Fisk sells USB v1.0 drives directly, and does not want to outsource production over fears the design might be compromised. The willing can also order the hardware and build their own v0.9 device by following the instructions.

Go [USG](#)