USB Storage

Overview

There are a few reasons why many USB Sticks have an upgradeable firmware:

- There is no additional cost for a rewriteable storage for the firmware, it can be placed on the big NAND flash chip with a small bootloader in ROM
- The flash chip market is evolving quickly and not all chips are fully compatible. Many compatibility issues can be fixed in firmware.
- Some vendors want to implement special features such as CD Emulation or a Write-Protect Switch
- There are many leaked tools

The Russian sites below are best viewed with Chrome due to the built-in translation feature.

Overview of USB Sticks with information about contained chip and matching tool:
http://flashboot.ru/iflash/

Overview of available leaked tools:
http://flashboot.ru/files/

Unfortunately the existence of a leaked tool for a given chip does not necessarily mean that the firmware can be upgraded. Some tools only provide other features such as the following:

- Change configuration data (Product Name, VID, PID) so that it matches for the OEM Vendor
- Enable CD Emulation
- Change capacity of stick (Sticks are typically sold with 4/8/16/32/64 GB capacity and a stick with enough good blocks for 25 GB is often software-limited to 16 GB.
- Do a low-level format

Some leaked firmware images appear to be partial and do not contain USB descriptors and no 8051 interrupt table.
Partial firmware images probably are nothing more than a fancy way to abstract differences in
flash geometry, where a simple static table would not be expressive enough.
It is conceivable that they also implement block management functions as this is an area where
new features might be developed to improve the product while access to a given hardware
can be expected to be reasonably efficient and generic enough so as to not require firmware
update. High level features such as volume management and USB vendor/product/serial IDs
should be found in the updated part too.
With a little bit of dedication one can probably figure out how to get information in and out and thus dump the whole of the firmware (for example 4 bytes of firmware per USB descriptor read in the VID/PID

Popular chips

Phison USB2 / USB3 controllers

All vulnerable -- see BlackHat talk and Psychson

ALCOR AU698X

- Leaked tool: ALCOR MP_v14.01.24.00.zip
  Contains many .bin files, which actually contain hex data
- Unpacking hex data results in raw 8051 code with interrupt table, code mapped at 0xC000
- No USB Descriptors found, it is possible that the upgradeable code is only used for interfacing the NAND Flash
- => Probably vulnerable

SMI SM325X/SM326X

- Many variants of recovery tool available, downland
  RecoverTool_V2.00.33_L1224.exe
  http://www.usbdev.ru/files/smi/
- Exe file contains rar with 500 .BIN files

- Examined two example files, found 8051 code starting at 0x800 in file, mapped at 0x8000 in address space
- USB Descriptors found
- => Most likely vulnerable

Skymedi SK62XX SK66XX

- Available tool: http://flashboot.ru/files/file/4/ SK6211_PDT_20090828.rar
- Contains ihex files with valid 8051 code, but no USB Descriptors found
- => Probably vulnerable

Solid State System SSS6677, SSS6690 and SSS6691

- Tool available: http://flashboot.ru/files/file/270/ SSS_MP_Utility_v2162.rar
- Contains valid 8051 code, but no USB Descriptors found
- => Probably vulnerable

Innostor IS903-A2, IS903-A3

- Tool available: http://flashboot.ru/files/file/379/ Innostor_IS903_MP_Package_V105_04_1303281.7z
- Found valid 8051 code, but no USB descriptors
- => Probably vulnerable

Updated by Karsten over 9 years ago · 1 revisions