corna / me_cleaner

Watch 56 Star 745 Fork 34

Code Issues 7 Pull requests 0 Projects 0 Wiki Pulse Graphs

Tool for partial deblobbing of Intel ME/TXE firmware images

43 commits 1 branch 1 release 3 contributors GPL-3.0

Branch: master New pull request Find file Clone or download

corna Add --truncate Latest commit 0ac4b4b 12 days ago

COPYING	Initial commit	5 months ago
README.md	Relocate FTPR to the top of the ME region	2 months ago
me_cleaner.py	Add --truncate	12 days ago

README.md

ME cleaner

A cleaner for Intel ME/TXE images.

This tools removes any unnecessary partition from an Intel ME/TXE firmware, reducing its size and its ability to interact with the system. It should work both with coreboot and with the factory firmware.

Currently this tool:

- Scans the FPT (partition table) and checks that everything is correct
- Removes any partition entry (except for FTPR) from FPT
- Removes any partition except for the fundamental one (FTPR)
- Removes the EFFS presence flag
- Corrects the FPT checksum
- Removes any non-essential LZMA or Huffman compressed module from the FTPR partition (pre-Skylake only)
- Relocates the remaining parts of the FTPR partition to the top of the ME region (pre-Skylake only)
- Checks the validity of the RSA signature of the FTPR partition

Don't forget to power cycle your PC after flashing the modified ME/TXE image (power off and power on, not just reboot).

See the current status or a more detailed description of me_cleaner.

Special thanks to Federico Amedeo Izzo for his help during the study of Intel ME.