SP2023 Week 11 • 2023-04-09

UEFI and EC Firmware Reverse Engineering

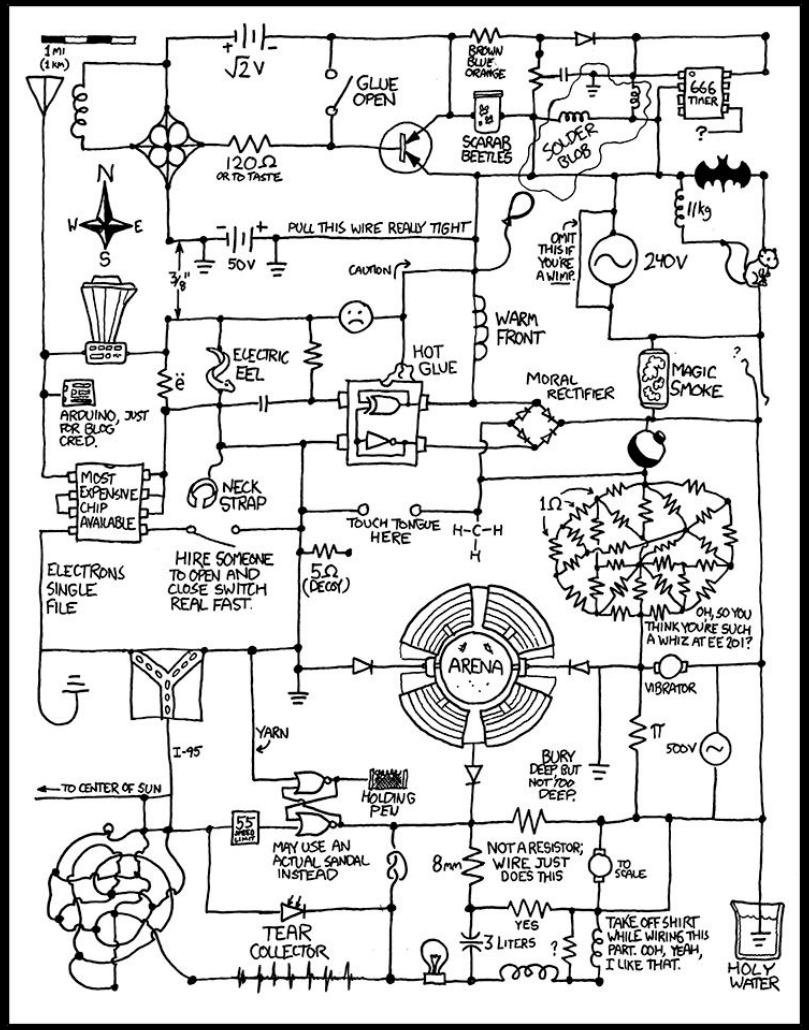
@crowfish

Announcements

- PlaidCTF 2023
  - April 14-16, we will be working together IRL! (room TBD in Siebel CS)

ctf.sigpwny.com

sigpwny{security_by_obscurity}



motivation

- PC firmware documentation is sparse at best
  - few partially open source firmwares
  - chromeos, system76, framework, etc
- improperly decommissioned surplus device
  - setup pw not removed
  - MDM, proprietary anti theft blob(Absolute CompuTrace, Intel AMT, etc) still configured
- Remove OEM restrictions in firmware
  - wireless card whitelist
  - locked down features
  - can even support future chipset and CPU with firmware modification!

where are setup PW stored?

- used to be stored in volatile memory
  - RTC module
  - remove clock battery to reset
- generally either NVRAM or EC in modern machines
  - more difficult to reset
- all of it is security by obscurity
  - you don't see setup pw option in open source firmware

UEFI NVRAM

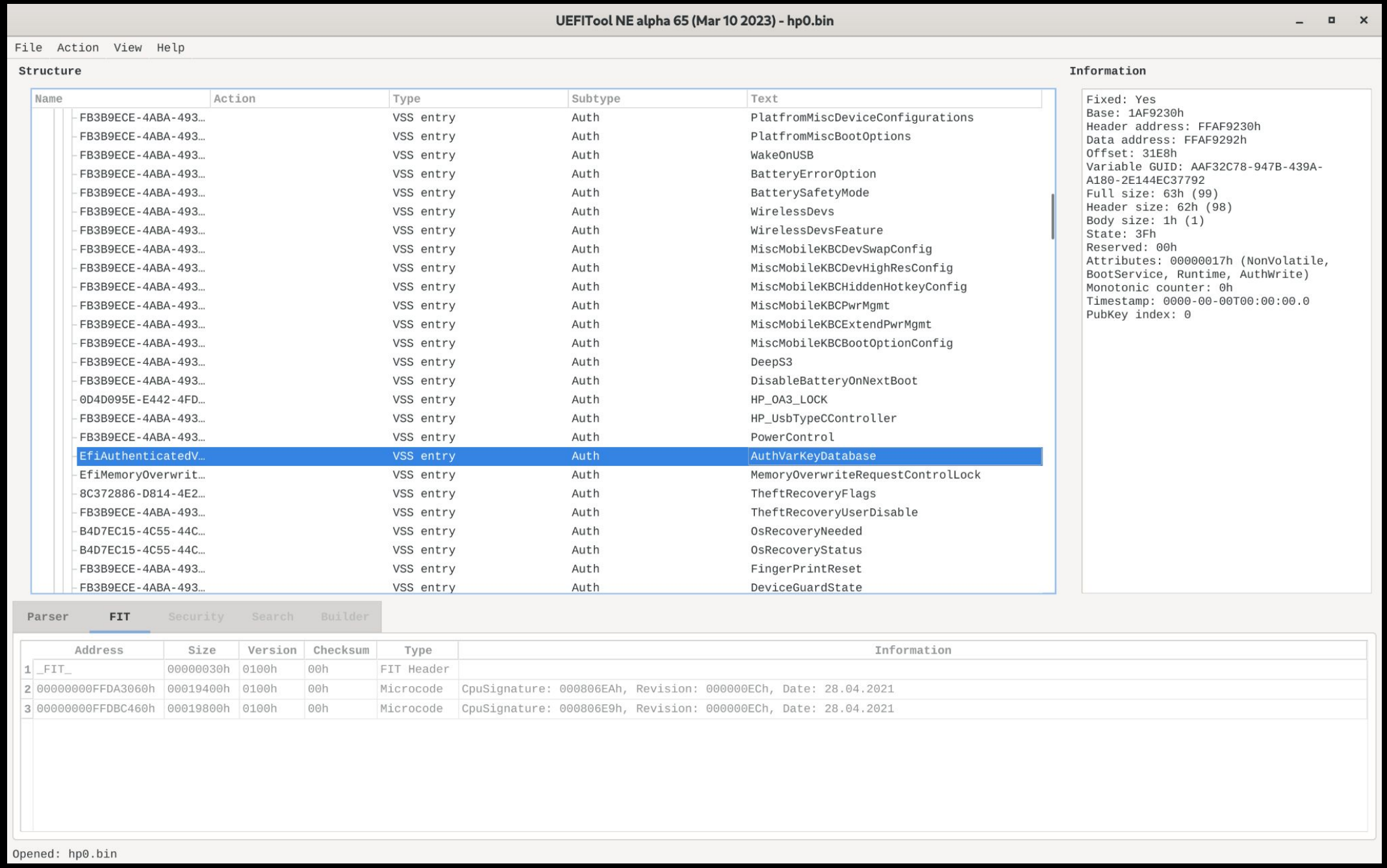
- non volatile random access memory
- access by `efivar` on linux or `nvram on macOS`
- stores system configuration variables
  - system speaker volume, brightness, etc
  - uefi settings, boot order, last known hardware config etc
  - imported secureboot certificates
  - TPM configuration
  - including MDM and anti theft configuration

UEFI NVRAM

- similar to env variables in your OS, but for FW
- some variables are hidden or not writable from userland
- modify hidden NVRAM var through external reprogramming
  - either ISP flash or physically remove EEPROM IC
  - many Intel PCH prevent successful ISP flash
- 25xx SPI NOR flash EEPROM: easy to read/write
  - hardware is pretty standard: the work is in firmware reverse engineering
  - generally can get away with clearing the entire NVRAM region

UEFI ROM Flashing

- read firmware: `minipro -p W25Q128JV -r filename.bin`
- open in UEFItool
  - find offsets for configuration options need to erase
- clear offsets by writing 0xff or 0x00
- generate updated checksum using uefitool and save(optional)
- write firmware: `minipro -p W25Q128JV -r modified.bin`
- first POST will take a few minutes
  - reset configuration and update firmware after successful POST


UEFITool NE alpha 65 (Mar 10 2023) - hp0.bin
File Action View Help
Structure
Information
Name Action Type Subtype Text
FB3B9ECE-4ABA-493… VSS entry Auth PlatfromMiscDeviceConfigurations
FB3B9ECE-4ABA-493… VSS entry Auth PlatfromMiscBootOptions
FB3B9ECE-4ABA-493… VSS entry Auth WakeOnUSB
FB3B9ECE-4ABA-493… VSS entry Auth BatteryErrorOption
FB3B9ECE-4ABA-493… VSS entry Auth BatterySafetyMode
FB3B9ECE-4ABA-493… VSS entry Auth WirelessDevs
FB3B9ECE-4ABA-493… VSS entry Auth WirelessDevsFeature
FB3B9ECE-4ABA-493… VSS entry Auth MiscMobileKBCDevSwapConfig
FB3B9ECE-4ABA-493… VSS entry Auth MiscMobileKBCDevHighResConfig
FB3B9ECE-4ABA-493… VSS entry Auth MiscMobileKBCHiddenHotkeyConfig
FB3B9ECE-4ABA-493… VSS entry Auth MiscMobileKBCPwrMgmt
FB3B9ECE-4ABA-493… VSS entry Auth MiscMobileKBCExtendPwrMgmt
FB3B9ECE-4ABA-493… VSS entry Auth MiscMobileKBCBootOptionConfig
FB3B9ECE-4ABA-493… VSS entry Auth DeepS3
FB3B9ECE-4ABA-493… VSS entry Auth DisableBatteryOnNextBoot
0D4D095E-E442-4FD… VSS entry Auth HP_OA3_LOCK
FB3B9ECE-4ABA-493… VSS entry Auth HP_UsbTypeCController
FB3B9ECE-4ABA-493… VSS entry Auth PowerControl
EfiAuthenticatedV… VSS entry Auth AuthVarKeyDatabase
EfiMemoryOverwrit… VSS entry Auth MemoryOverwriteRequestControlLock
8C372886-D814-4E2… VSS entry Auth TheftRecoveryFlags
FB3B9ECE-4ABA-493… VSS entry Auth TheftRecoveryUserDisable
B4D7EC15-4C55-44C… VSS entry Auth OsRecoveryNeeded
B4D7EC15-4C55-44C… VSS entry Auth OsRecoveryStatus
FB3B9ECE-4ABA-493… VSS entry Auth FingerPrintReset
FB3B9ECE-4ABA-493… VSS entry Auth DeviceGuardState
Fixed: Yes
Base: 1AF9230h
Header address: FFAF9230h
Data address: FFAF9292h
Offset: 31E8h
Variable GUID: AAF32C78-947B-439A-A180-2E144EC37792
Full size: 63h (99)
Header size: 62h (98)
Body size: 1h (1)
State: 3Fh
Reserved: 00h
Attributes: 00000017h (NonVolatile, BootService, Runtime, AuthWrite)
Monotonic counter: 0h
Timestamp: 0000-00-00T00:00:00.0
PubKey index: 0
Parser FIT Security Search Builder
Address Size Version Checksum Type Information
1 _FIT_ 00000030h 0100h 00h FIT Header
2 00000000FFDA3060h 00019400h 0100h 00h Microcode CpuSignature: 000806EAh, Revision: 000000ECh, Date: 28.04.2021
3 00000000FFDBC460h 00019800h 0100h 00h Microcode CpuSignature: 000806E9h, Revision: 000000ECh, Date: 28.04.2021
Opened: hp0.bin

manufacturer specific

- Apple: look for "svs store" section within NVRAM
- HP: look for variable containing "User00" or "User01"
- Dell: clear the both NVRAM regions including checksums
  - make note of service tag before
- Lenovo
  - clear protected region in EC microcontroller
  - older models have vulnerable system fw allowing you to do without disassembling device
- chrome OS(any manufacturer)
  - nonstandard uefi layout not supported by uefitool
  - look for string 'gbb' in hexdump

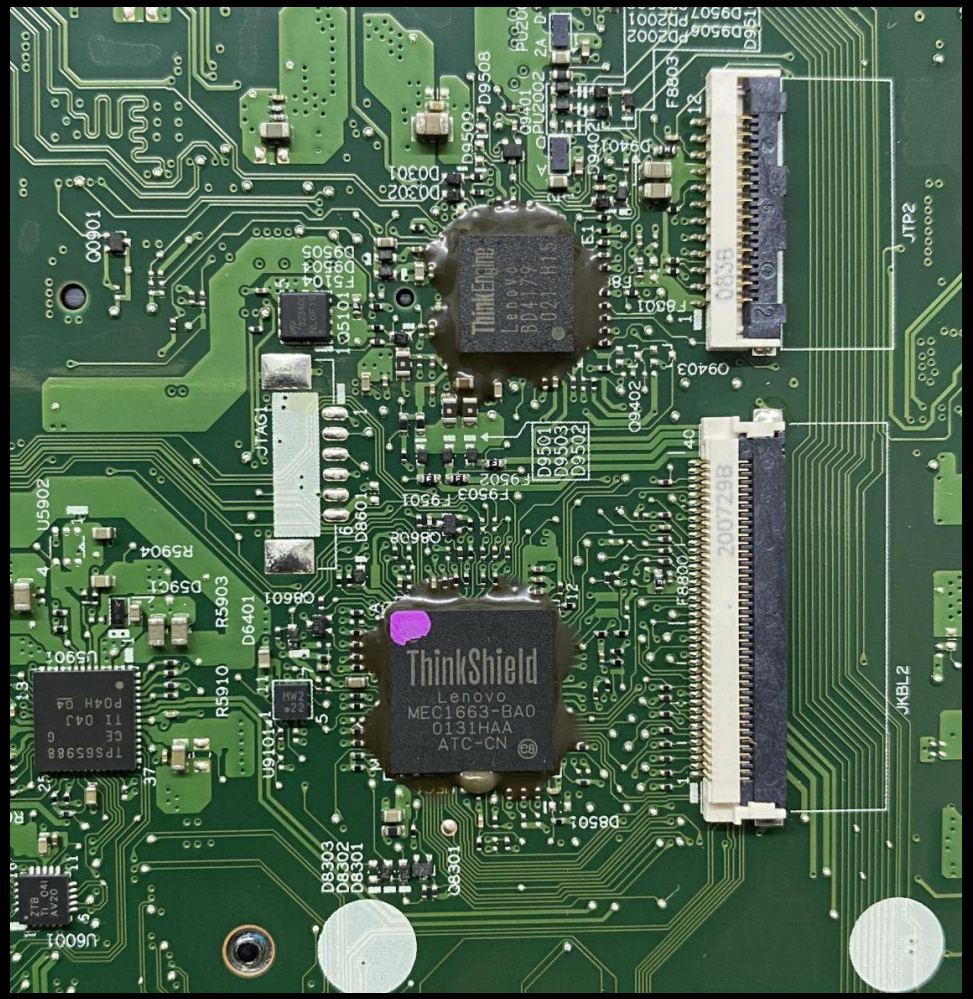
Embedded Controller(EC)

- microcontroller ASIC responsible for low level functions
  - thermal management/fan control
  - internal keyboard mouse I/O
  - assists in boot process
  - communicates with CPU over LPC bus
- found on all laptops, most desktop motherboards
- contains user writable flash: not accessible in userland at all

Embedded Controller(EC)

- more difficult to flash than UEFI ROM
- password stored in “Direct JTAG and Direct LPC-protected memory”
  - may be called other brand names in different manufacturers
  - usually the first few blocks of flash memory: see datasheet
- each manufacturer has different pinout/functions
  - Nuvoton
  - ITE
  - Microchip/MEC
  - others
- requires significantly more hardware reverse engineering

EC Flashing



- look for JTAG/ISP connector onboard
- parallel programming interface through keyboard connector
  - more signals to break out
- external flash last resort: difficult to remove and replace chip

flashing hardware

- RT809H
  - proprietary hardware and software
  - most support for EC microcontroller onboard flash devices
  - expensive: FPGA based
- TL866II
  - proprietary hardware, open source software
- raspberry pi + flashrom
  - open source hardware and software
- flashrom internal flash
  - for mac + chrome devices

credits/tools

- **uefitool:** github.com/LongSoft/UEFITool
- **minipro**: gitlab.com/DavidGriffith/minipro
- **badcaps forum:** badcaps.net
- **chromium EC docs:** chromium.googlesource.com/chromiumos/platform/ec/
- **ghostlyhaks forum:** ghostlyhaks.com

Next Meetings

2023-04-13 - This Thursday

- Esoteric Programming Languages with Pete and Richard
- Learn about unusual programming languages for CTF

2023-04-14 - This Friday

- PlaidCTF 2023
- Our next big in-person CTF as a team!

2023-04-20 - Next Thursday

- Block Ciphers with Sagnik and Anakin
- Learn about block ciphers and become an AES god!

sigpwny{security_by_obscurity}

SIGPwny