

Fiedka the Firmware Editor

Advancing from CLIs to GUIs

Daniel Maslowski



Agenda

Introduction and Scope
 Current State
 Roadmap and Contributing





Introduction and Scope



Hello, I am Daniel :-)





Work and education O IT security and computer science O software engineer O infrastructure and web O applications and UI

Open Source contributions O hardware and firmware O operating systems O software distributions O reverse engineering







Graphical Firmware Editor O UEFI/PSP/ME Filesystem Exploration O Flash Usage Visualization O TPM Event Log O Platform State Investigation O Secure Boot Key Management





_

Firmware is software that is hard to get to. - Bryan Cantrill



~ ~



 UX/UI design and hardware design/manufacturing are both complex and still learning about agile and open processes.



~ ~



 UX/UI design and hardware design/manufacturing are both complex and still learning about agile and open processes.

We need more tools and feedback.





 UX/UI design and hardware design/manufacturing are both complex and still learning about agile and open processes.

We need more tools and feedback.

for education, to speed up understanding
 for research, to gain security through transparency
 for development, to support sustainability



Problem Statement

Full firmware images differ depending on vendor, platform, OEM, and other factors.



ୖୖ

Problem Statement

Full firmware images differ depending on vendor, platform, OEM, and other factors.

Building tools is a huge investment.



Problem Statement

Full firmware images differ depending on vendor, platform, OEM, and other factors.

Building tools is a huge investment.

Intel x86
IFD, ME, UEFI, ...
AMD x86
PSP, SMU, UEFI, ...
other platforms
ARM, RISC-V, Xtensa, DSPs, ...



Other Tools

/ / / / ~ / / / / ~ / / / / ~ • AMI's Module Management Tool (MMTool) RED BIOS EDITOR 🖸 Intel FMMT 🖸 ifdtool 🛈 uefi-firmware-parser • MFT (Mimoja's Firmware Toolkit) ① MEAnalyzer 🕑 mecleaner 🕑 Fiano 🕑 tpmtool Converged Security Suite • efiXplorer Õ



Trees and Tables

/// ~ / /// ~ / /// ~

Name	Action	Туре	Subtype	Text
✓ UEFI image		Image	UEFI	
Padding		Padding	Non-empty	
IFD0BACE-6F0A-4085-901E-F6210		Volume	FFSv2	
EfiSystemNvDataFvGuid		Volume	NVRAM	
Padding		Padding	Non-empty	
FTW store		FTW store		
Padding		Padding	Empty (0xFF)	
FDC store		FDC store		
FiSystenNvDataFvGuid		Volume	NVRAM	
- VSS store		VSS store		
EfiGlobalVariableGuid		VSS entry	Auth	PK
EfiGlobalVariableGuid		VSS entry	Auth	KEK
EfiImageSecurityDatabase		VSS entry	Auth	db
EfiImageSecurityDatabase		VSS entry	Auth	dbx
Free space		Free space		
Padding		Padding	Non-empty	
Intel microcode		Microcode	Intel	
Intel microcode		Microcode	Intel	
Padding		Padding	Non-empty	
CF1406C5-3FEC-47EB-A6C3-B71A3		Volume	FFSv2	
Padding		Padding	Non-empty	

Found volume magic at 0x6af000

Firmware Volume: 8c8ce578-8a3d-4f1c-9935-896185c32dd3 attr 0x0004fe Firmware Volume Blocks: (1617, 0x1000) Section 0: type 0x18, size 0x1014 (4116 bytes) (Free-form GUID File 2: 05ca020b-0fcl-11dc-9011-00173153eb8 type 0x01, attr 0x00 Firmware Volume: 8c8ce578-8a3d-4flc-9935-8961885c32dd3 attr 0x00 Firmware Volume Blocks: (32, 0x1000)

ME Analyzer v1.160.0 r212				
1.rom (1	1.rom (1/1)			
Family	ME			
Version	4.1.3.1038			
Release	Production			
Туре	Extracted			
SKU	AMT			
Date	2008-12-17			
Size	0×1FB000			
Chipset Support	ICH9M			
Latest	No			



General Concepts \sim / / / \sim / / / \sim / / / \sim /

The hard part phases/stages, payloads, chains (non-)volatility, static vs dynamic, persistency, reset...



General Concepts

The hard part O phases/stages, payloads, chains O (non-)volatility, static vs dynamic, persistency, reset...

The easy part Storage, files => file systems metadata, properties, inputs to boot flow (much volatility!)





Current State



How it started

inspired by Ryan's *iutk2*render flash usage from fmap fixtures
utk-web, rendering fixtures

Flash Usage			
blocks	512	100%	2M
zero (0x00)	0	0%	OM
free (0xff)	259	50.59%	1.01M
used	253	49.41%	0.99M
0x00000000 			
0x00020000			
0x00040000			
0x00060000			
0x00080000			
0x000a0000			
0x000c0000			
0x000e0000			
0x00100000			
0x00120000			
0x00140000			
0x00160000			
0x00180000			
0x001a0000			
0x001c0000			
0x001e0000			

 Color palette suitable for color-blind people
 blocks display usage: free, used, all-zero



Demo

A3MSTX 3.60 PSPTool 0xx8000 0x188000 0x40000 0x58000 0x3x0000 0x168000 0x440000 0x268000 Flash Usage 0x630000 enter substring blocks 4096 100% 16M 30 0.7396 destination destination zero (0x00) 0.12M . tree (0xff) 1695 41.38% 6.62M hash E284 hash 6AE5 size 16 size 4096 used 2371 57.89% 9.26M 8x082+8008 0x002c0000 SEC GASKET-0x24 0x124 8x882e8888 0100301000 address 0x546000 address 0x547900 version A.2.3.27 A.2.4.25 version 0x00320000 destination destination magic \$PS1 magic \$PS1 8x08348008 hash EA50 hash E895 0x00360000 60BB 60BB signing key signing key 0x00350000 size 6240 size 6208 blocks used: 2 blocks used: 2 0x00320000 5728 5696 signed signed 0x003/0000 0x00320000 uncompressed 0 uncompressed 0 0x00400000 packed 6240 packed 6208 0x00420000 0x00440000 0x00460000 0102450000 0x224 MP2_FW~0x25 0x024w2000 address 0x549200 address 0x54ab00 0x094c0000 A 2 3 27 31801 version version 0x004c0000 destination destination magic \$PS1 signing key 76E9 0x00500000 hash EA50 0x00520000 signing key 60BB hash 1E3D blocks used: 3 0x00540000 size 6240 size 8945 blocks used: 2 0x00560000 signed 5728 signed 7601 0x00580000 uncompressed 0 uncompressed 0 0100501000 nacked 6240 nacked 8945 0x005c0000 010050000 0x00600000 9x99629999 0x125 0v225 0x54ce00 0v550900 address version 5221 address version 4211 destination signing key 76E9 destination signing key 76E9 0x016c0000 hash D802 hash 9906 0x0060000 0x00700000 0x00700000 blocks used: 4 blocks used: 3 size 15012 size 9188 7844 signed 12669 signed 0x00740000 0x00762000 uncompressed 0 uncompressed 0 0x00760000 packed 15012 packed 9188

	DRIVER	R_ENTRIES~0x28	✓			ABL0~0x30	
address	0x552d00	version	0.8.0.60	address	0x56b500	version	19.4.3.0



How it's going

Electron app with Go-based WASM back-end and file picker
 UI components: Directory, Entry, Fmap, navigation, search
 Storybook UI development environment

Fiedka - analyze a firmware image			Í
A52MIX_1.31 FA49 51C8 E527 0	3FE 5C60 4F1C 61C0 FUID or name substring	Flash Usage	-
FA4974FC-AF1D-4E5D-BDC5-DACD6D27BAEC		blocks	4095 20016 2641
		free (8xff)	1755 43.6% 6.96M
cus	833-4510-4817-9EDC-1391-010422C	used	2289 55.88% 8.94M
undefined bytes, 6 lites 51C81E99-DF1A-4DC5-9966-0B8D9AA09CAD (843	66C9E-CD61-4B6E-8BC7-384541382842)	0x60503000	
Anit.specyborerspi	LegacyBegion	0xt01010101	
Cualtur	Caultinkis		
ConVideo	A86278EC-A892-4696-8876-383396CT0993	0x80140000	
E5274881-D739-4209-9882-7C564B19E263 (C0492	C7F-75E2-487C-B2DD-000E6CF7B905)	0xt01x9000 0xt01c0000 0xt01e0000	
Sapther	DjcDar	0x60220000	
by the cost data of the cost of the second rest of	BOPEX SPEI_PCD_PROTOCOL_GUID pair Answersester CRAAA type FULLY_ALEVER type FULLY_ALEVER type type	0.1102.01000 0.1102.01000 0.1102.01000 0.1102.01000 0.1102.01000 0.1102.01000 0.1102.01000	
		0x80320000	
Magfine gade 02000FC7-014-4-0008-03/04 605543464-F64 type: 0515-V_ELETYDE_DRYVER live: Mocks used: NaN	Anphu godt 1200000-EXEC-4273-0121-40264-000013 New DRI_DV_FLICTVPE_DRIVER New Biocks unset: NaN	0xt0360000 0xt0350000 0xt0350000 0xt03c0000 0xt03c0000 0xt03c0000	
		0x00400000	
India Juni 1972-4465 5255-4455 505C-020525578228 Spec et al. (%) FARTYPE_DEVICES Sec. Mickis used: NAN	gui pozetich-zoz-woz-koz-organizaczen gui pozetich-zoz-woz-koz-organizaczen goz bit-y-y-tertrine, zonose libre biocis used, hun	0xt0449099 0xt0469090 0xt0469090 0xt0449099 0xt0449099 0xt0449099	
		0x0050000	



Integrations

💽 UEFI: parsing via Fiano's utk pkg

OPSP: experimental branch using Converged Security Suite

TPM: components to render a log (basics)

fixtures from tpmtool, PRs open

EV_EFI_GP	T_EVENT		
Event	"Disk Guid - 00000000-C5D3-98AD-A5D0-0844A28DF096"		
	SHA1: fdf06fbb281efabfe317ec56061b24798cda4c9d		
Digests	SHA256: 8d38c857cff8ff0b5e94abe94366f84dcdcd7e9cbbd0c6d67e26e69fd4b4dfdd		
EFI boot se	rvices app		
Event	"Image loaded at address 0x3123249176 with 93054b"		
	SHA1: f19f8e338af1998bf933b5fbe28a80c1dc0c34fd		
Digests	SHA256: 7c1a8614c3e3d6a5b6c2897ea4e94c8092c658b6d16a7459fa038526f25f4cc3		
EFI boot se	rvices app		
Event	"Image loaded at address 0x3093762072 with 9605120b"		
	SHA1: 2eb9a7daab81bbd9bfe258662e2b18b790714b6d		
Digests	SHA256: 7ae77c55430d6140e976a244de37241bbdbe46b67605f620df2b0683ee3b9ef9		



, Demo / / / / ~ / / / ~ / / / ~ / /

File	e Edit	View	Window	Help	
Fi	iedka	- an	alyze a	firmware	imag
s	elect file				





Roadmap and Contributing





integrate PSP, IFD/ME, CBFS parsing - back-end work required edit/save; MVP: delete DXE in OVMF - utk already has that :)



~ ~

Ideas

Emulation O dxelate, peimulate: wrap a DXE/PEIM in a monitored OVMF O on click of a DXE/PEIM, create OVMF image and run QEMU O likewise, leverage PSPEmu O UEFI runtime service analysis (SMM?)



Emulation

O dxelate, peimulate: wrap a DXE/PEIM in a monitored OVMF
 O on click of a DXE/PEIM, create OVMF image and run QEMU
 O likewise, leverage PSPEmu
 O UEFI runtime service analysis (SMM?)

Bootable ISO O create an image with Linux, Fiedka, u-root, CLI tools etc O the firmware development counterpart to Kali O possibly extend SystemRescueCD





EFI variables and Secure Boot O look into rhboot/efivar and canonical/go-efilib O integrate with go-uefi





EFI variables and Secure Boot O look into rhboot/efivar and canonical/go-efilib O integrate with go-uefi

TPM / Integrity

log display; tpmtool, go-attestation
 immune Guard agent health report
 tpm-js for simulation and debugging



UI / Web

Visualizations O DMI, SMBIOS, etc O ACPI tables, Device Tree O IFR (Intermediate Forms Representation) - firmware menu O platform and memory setup (page tables, interrupts, MSRs) O integrate CPUID visualiser



Visualization API

```
Transforms
export const flattenVolumes = (volumes) =>
 volumes.reduce((acc, curr) => {
   if (curr.Value.Files) {
     curr.Value.Files.forEach((f) => {
       if (f.Type === FILE_TYPE_FV_IMAGE) {
        getFvsFromFile(f).forEach((fv) => {
          acc.push({ parent: f, ...fv });
        });
       }
     });
   acc.push(curr);
   return acc;
 }, []):
```



Do you have any ideas? Please submit! :-)

https://github.com/fiedka/fiedka/issues





Thanks!



Links

Project Website https://fiedka.app/

Slides https://metaspora.org/fiedka-osfc2021.pdf

Previous Talk Introducing utk-web - a web developer's view on firmware https://metaspora.org/introducing-utk-web-rc3.pdf

