What’s the diff?

Diffing firmware images

Daniel Maslowski

Agenda

- AMD PSP Platforms
- Diffing Flash Images

How it started

How it started

pietrushnic (11 Sep 2024):

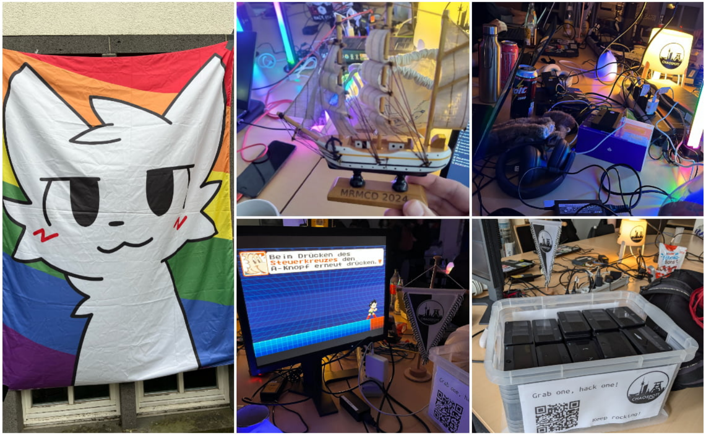
> *[…] find certain services working between given versions of PSP.*

How it started

pietrushnic (11 Sep 2024):

[…] find certain services working between given versions of PSP.

MRMCD 2024 (6-10 Oct):



AMD PSP Platforms

Documentation

Not much public official documentation on low-level details exists[1].

[1] https://www.amd.com/en/search/documentation/hub.html
[2] https://doc.coreboot.org/soc/amd/psp_integration.html
[3] https://github.com/system76/romulan/

Documentation

Not much public official documentation on low-level details exists[1].

3rd Party

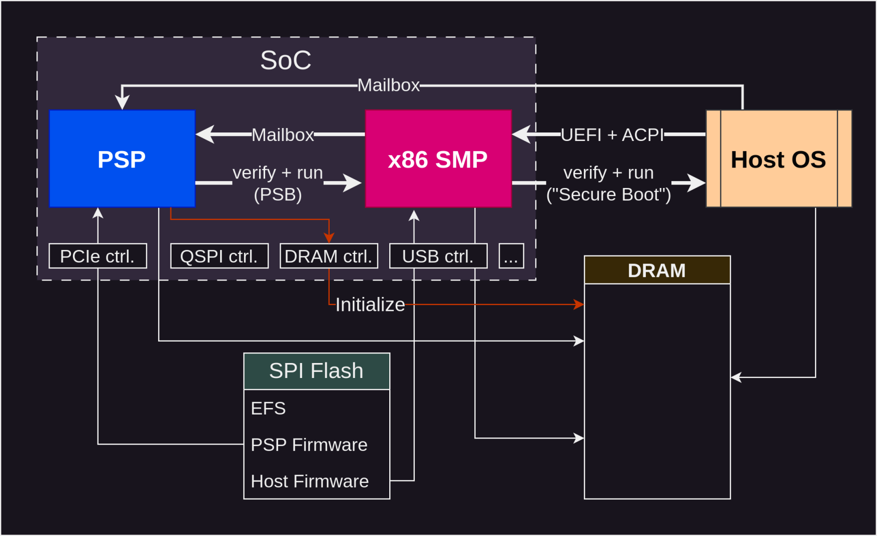
- parts in coreboot docs and code[2]
- parts in Fiano, Immune and Converged Security Suite
- forums, e.g., Win-Raid
- Dasharo community :)
- reverse engineering, e.g., MFT, PSPReverse, Platbox
- System 76 / Jeremy Soller's Romulan[3]
- my own efforts

[1] https://www.amd.com/en/search/documentation/hub.html

[2] https://doc.coreboot.org/soc/amd/psp_integration.html

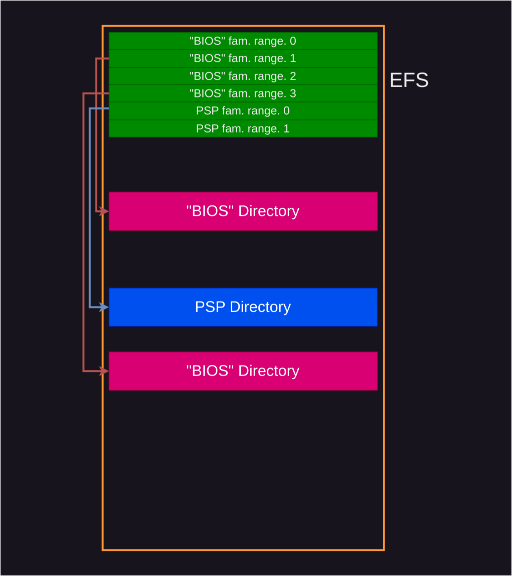
[3] https://github.com/system76/romulan/

Hardware Platform and Flow[4]

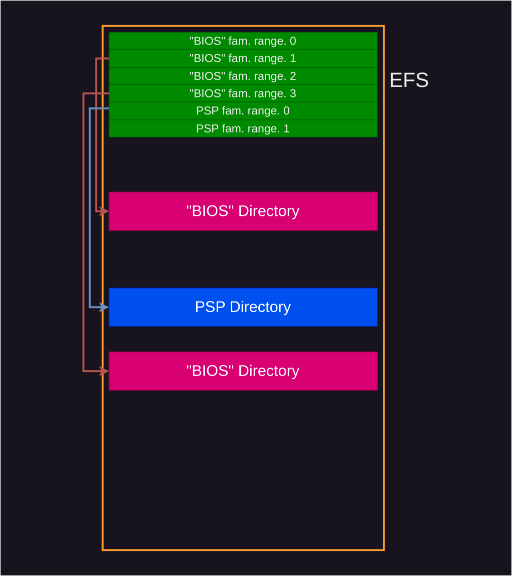


[4] https://labs.ioactive.com/2024/02/exploring-amd-platform-secure-boot.html

Data in Flash



Data in Flash



Embedded Firmware Structure

- pointers to different *kinds* of directories
  - immediate
  - combo
- multiple refs to same dir
  - deduplicate
- multiple refs to same file
  - can be ignored
- variants of nesting
- PSP directory may contain BIOS directory
- level 2 directories

Diffing Flash Images

Challenges

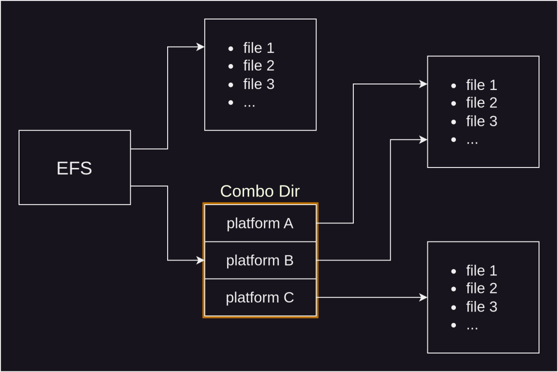
different

- sizes
- slots in EFS used
- platforms targeted
- components
- metadata (or none)
- signatures
- OEM customizations
- ways to build directories

Challenges

different

- sizes
- slots in EFS used
- platforms targeted
- components
- metadata (or none)
- signatures
- OEM customizations
- ways to build directories



Strategy

What *can* be compared?

Strategy

What *can* be compared?

Two Lists

```
a          b'
b          c
d    vs    d
e          e
           f
```

Strategy

What *can* be compared?

Two Lists

a		b'
b		c
d	vs	d
e		e
		f

Only in 1

a

Strategy

What *can* be compared?

Two Lists

```
a         b'
b         c
d    vs   d
e         e
          f
```

Only in 1

```
a
```

Common

```
b != b'
d == d
e == e
```

Strategy

What *can* be compared?

Two Lists			Only in 1	Common	Only in 2
a		b'	a	b != b'	c
b		c		d == d	f
d	vs	d		e == e	
e		e			
		f			

DEMO

Thanks! :)

Follow Me

Daniel Maslowski

https://github.com/orangecms
https://twitter.com/orangecms
https://mastodon.social/@cyrevolt
https://twitch.tv/cyrevolt
https://youtube.com/@cyrevolt

https://fiedka.app

https://github.com/fiedka/romulan

https://metaspora.org/big-diff.pdf