



Greenhouse: Single-Service Rehosting of Linux-Based Firmware Binaries in User-Space Emulation

Hui Jun Tay, Kyle Zeng, Jayakrishna Menon Vadayath,
Arvind S Raj, Audrey Dutcher, Tejesh Reddy, Wil Gibbs,
Zion Basque, Fangzhou Dong, Zack Smith, Adam Doupé,
Tiffany Bao, Yan Shoshitaishvili, Ruoyu Wang

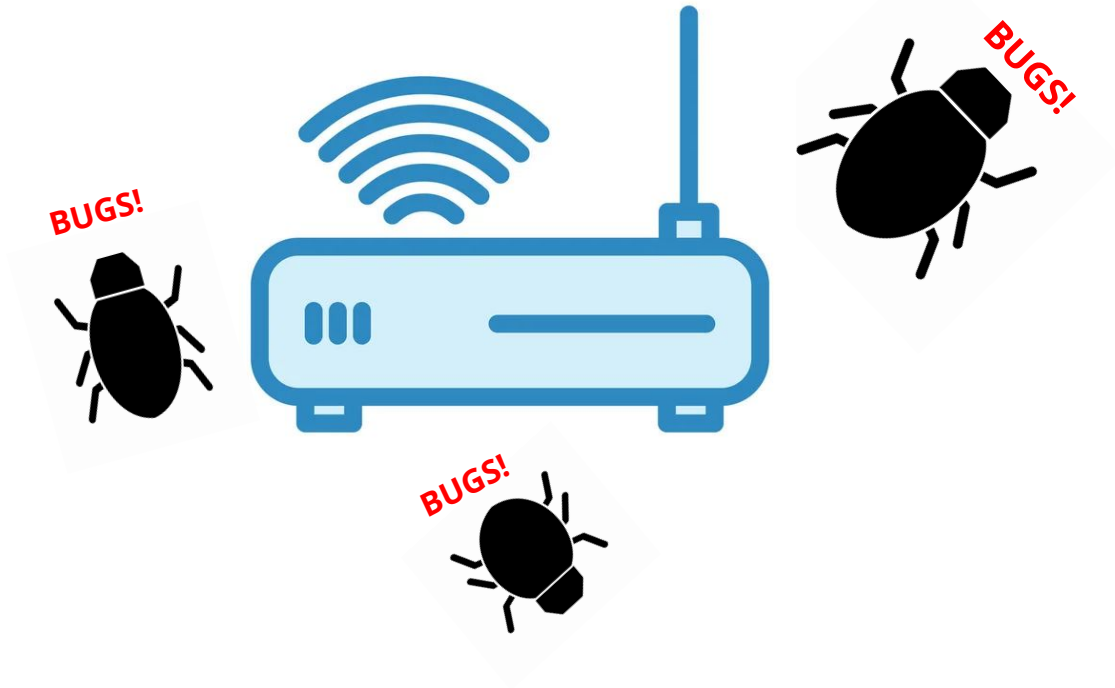




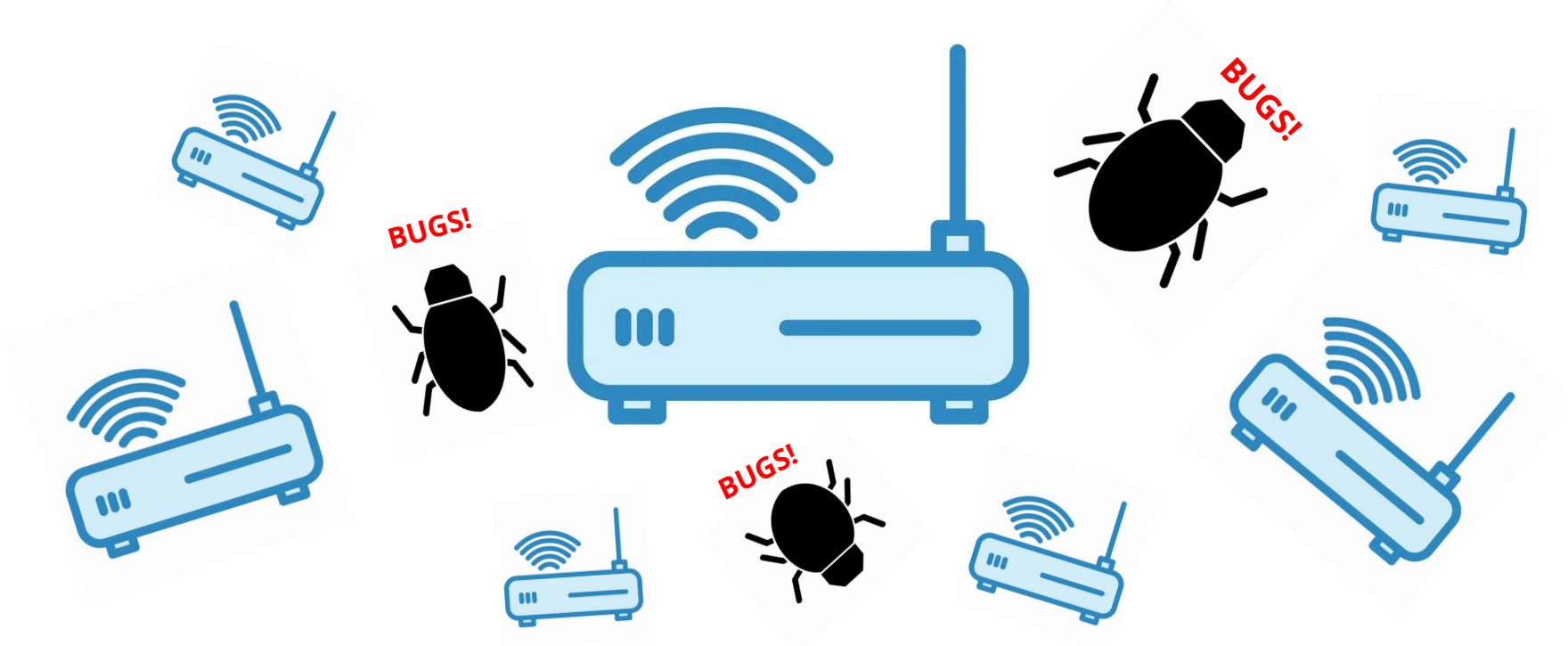
Problem



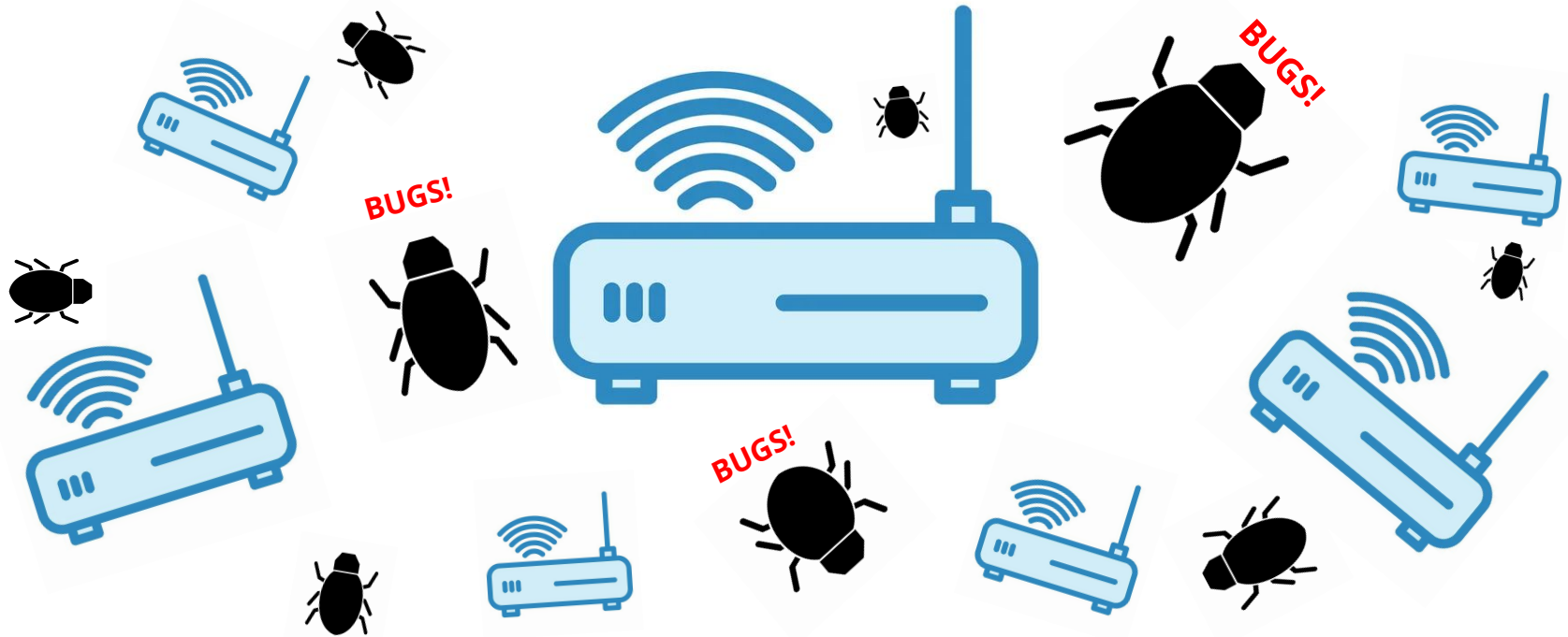
Problem



> Problem



> Problem



> Problem



Problem



Problem



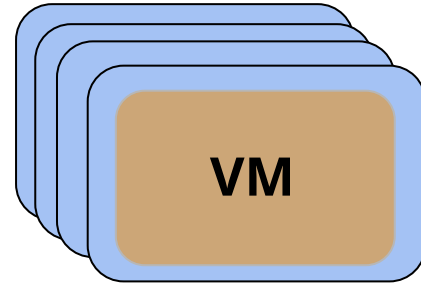
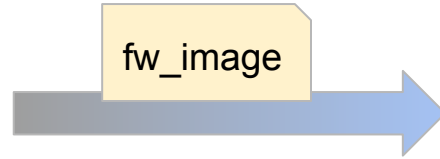
IDA



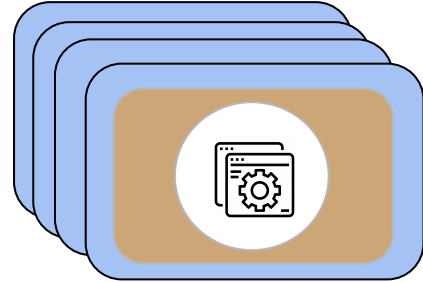
GDB
The GNU Project
Debugger



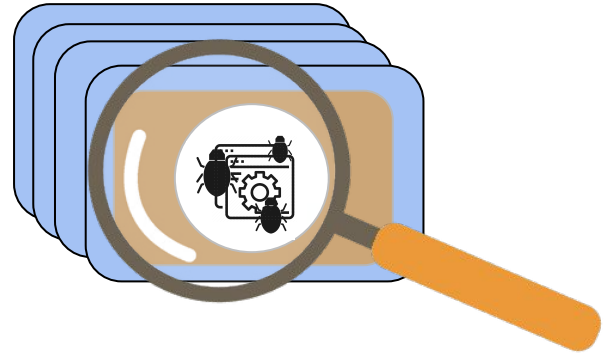
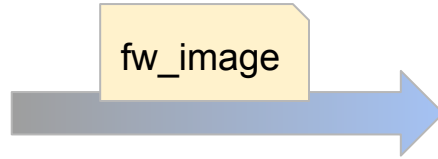
Rehosting



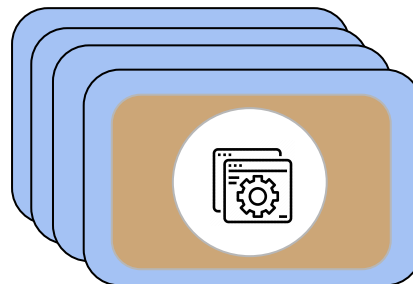
Rehosting



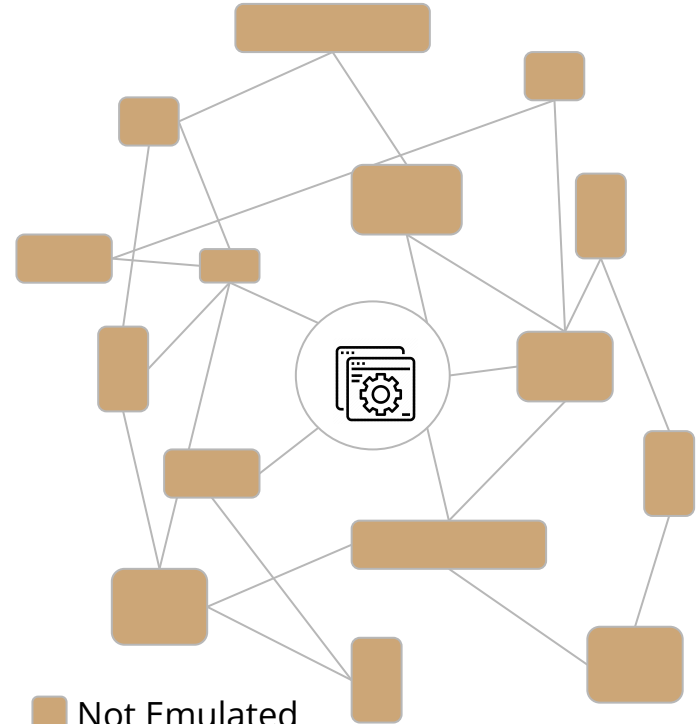
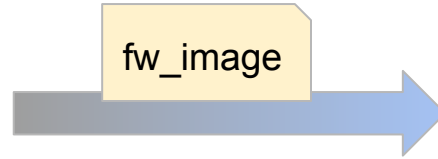
Rehosting






Rehosting

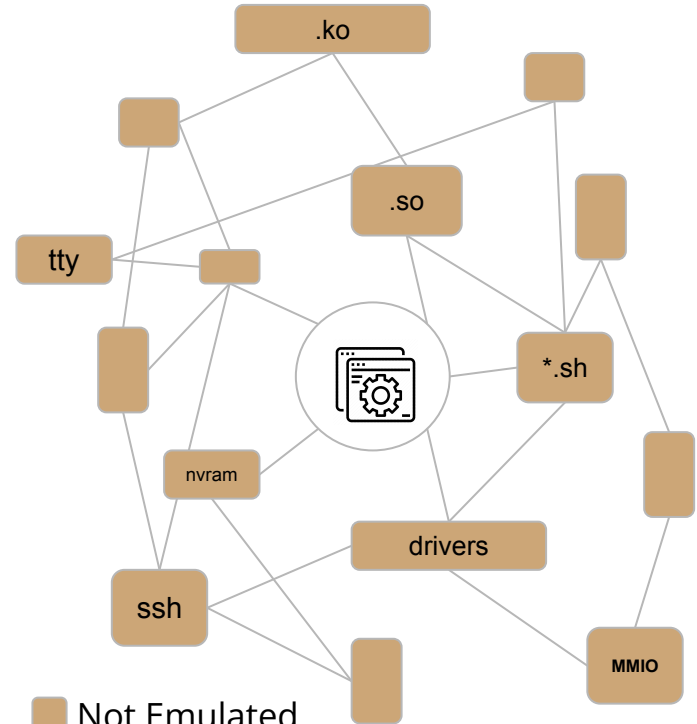
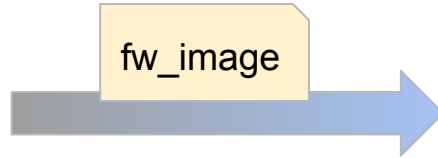


Rehosting



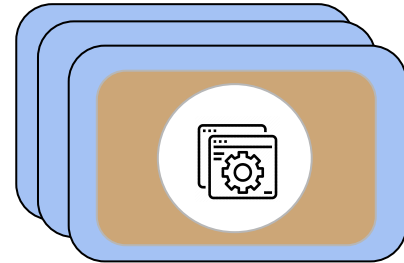
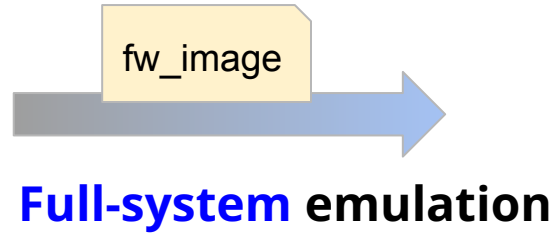
-  Not Emulated
-  Emulated
-  Dependent

> Rehosting

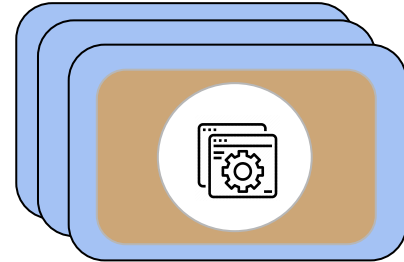
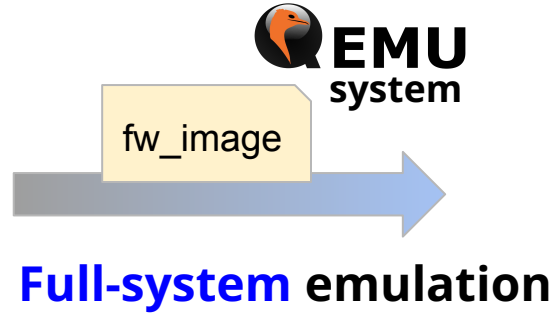


- Not Emulated
- Emulated
- Dependent

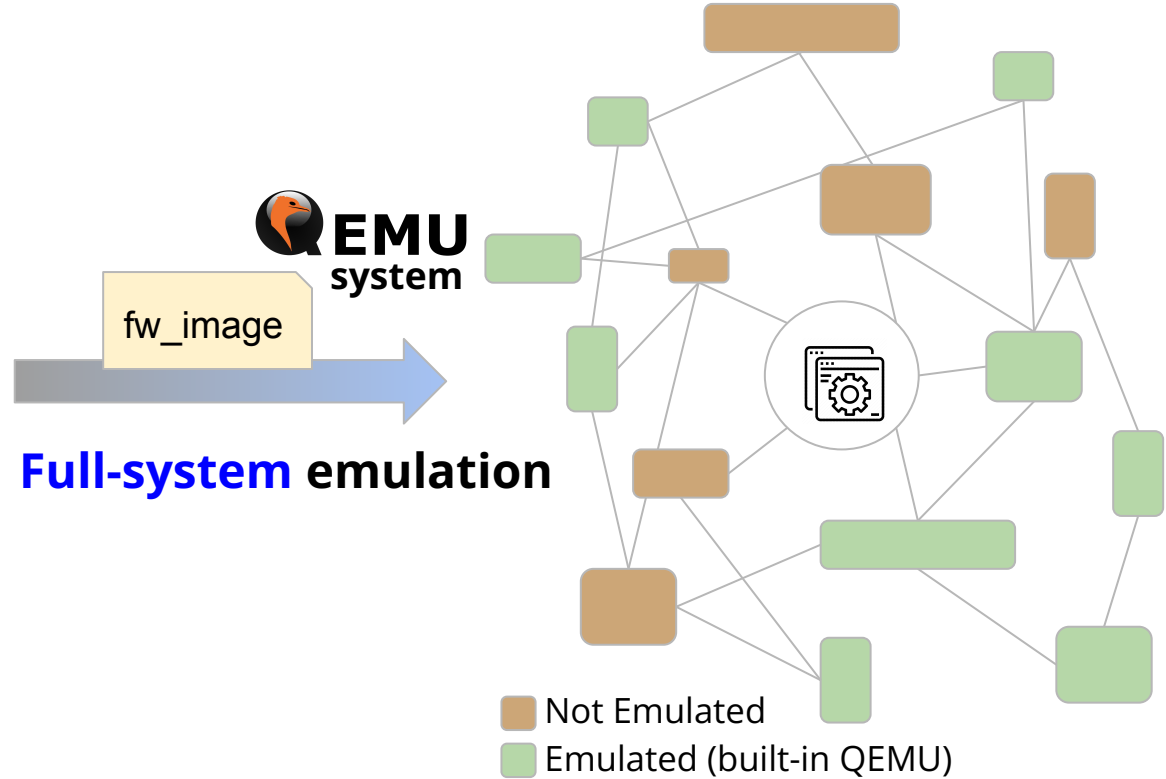
Rehosting



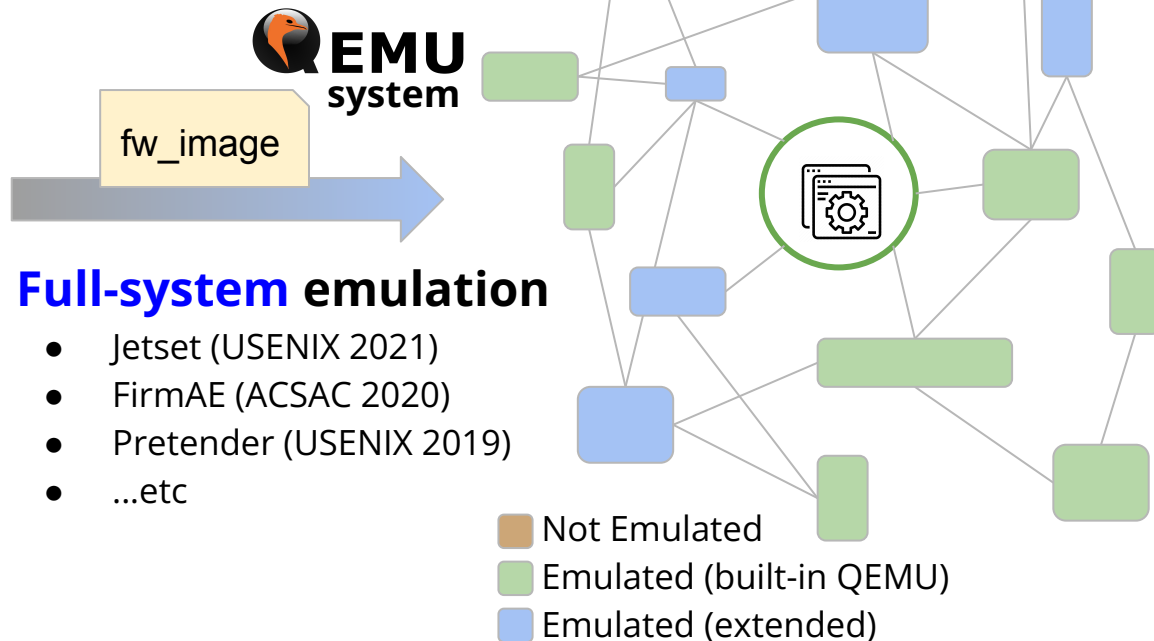
Rehosting



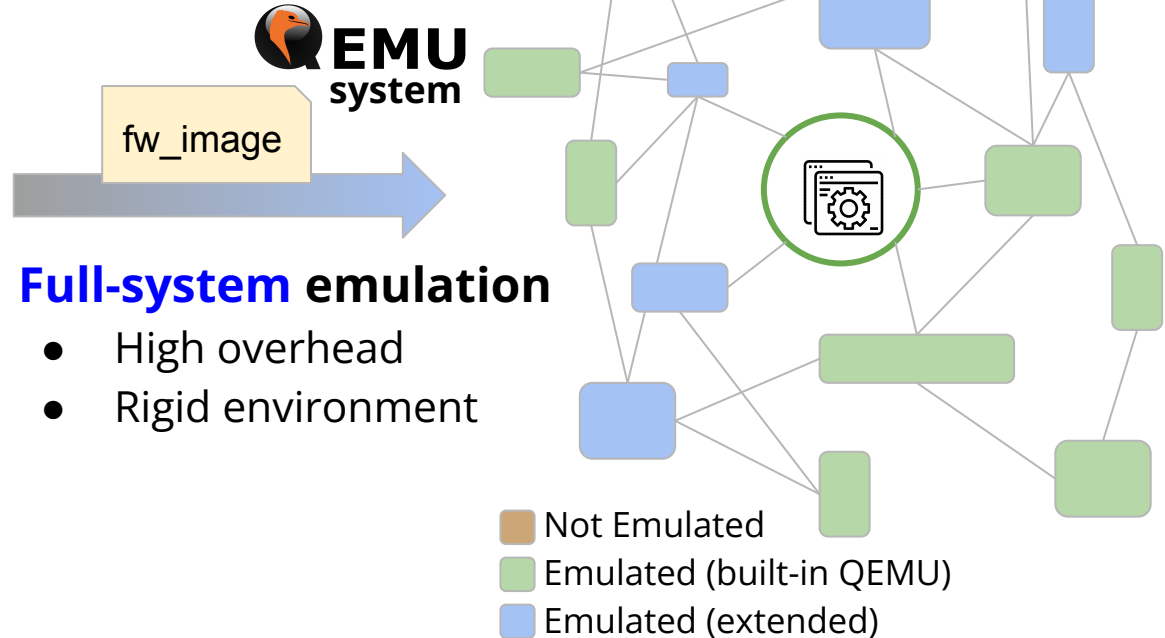
Rehosting



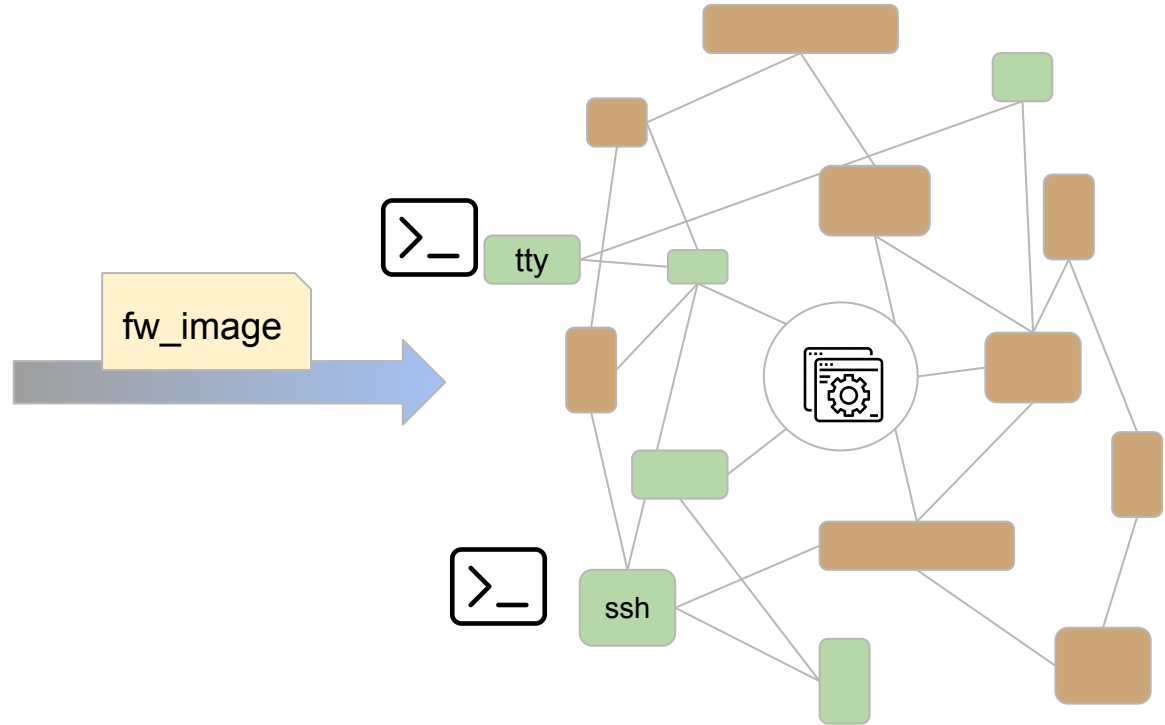
Rehosting



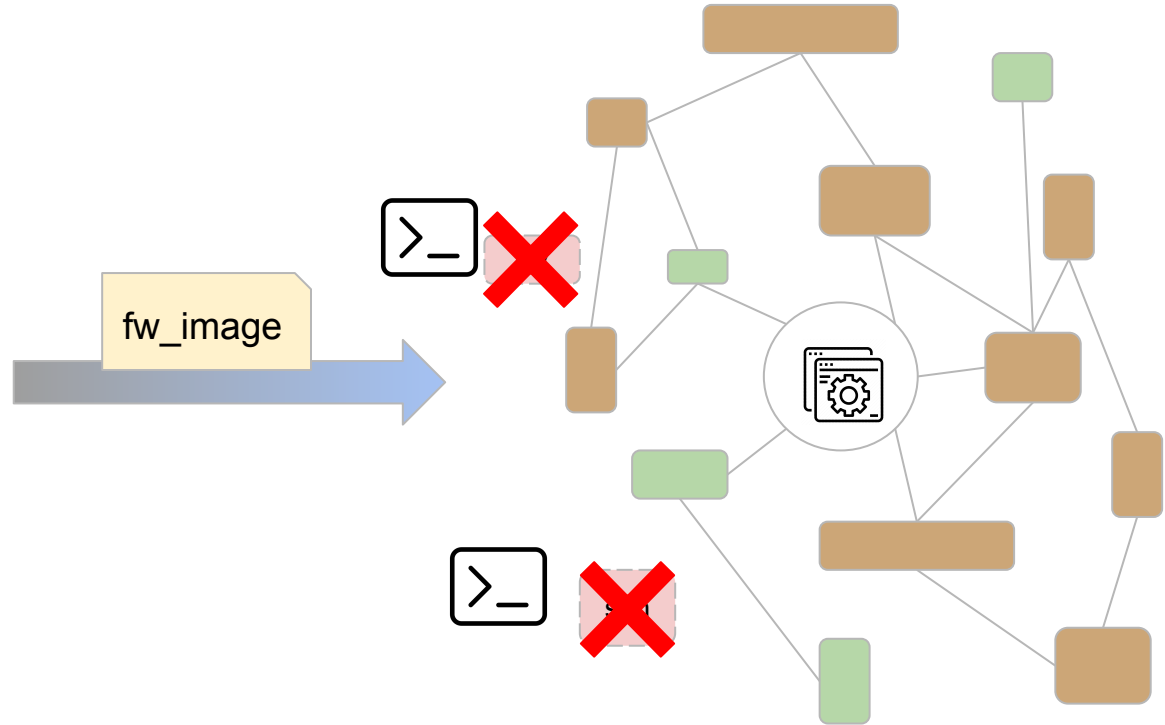
Rehosting



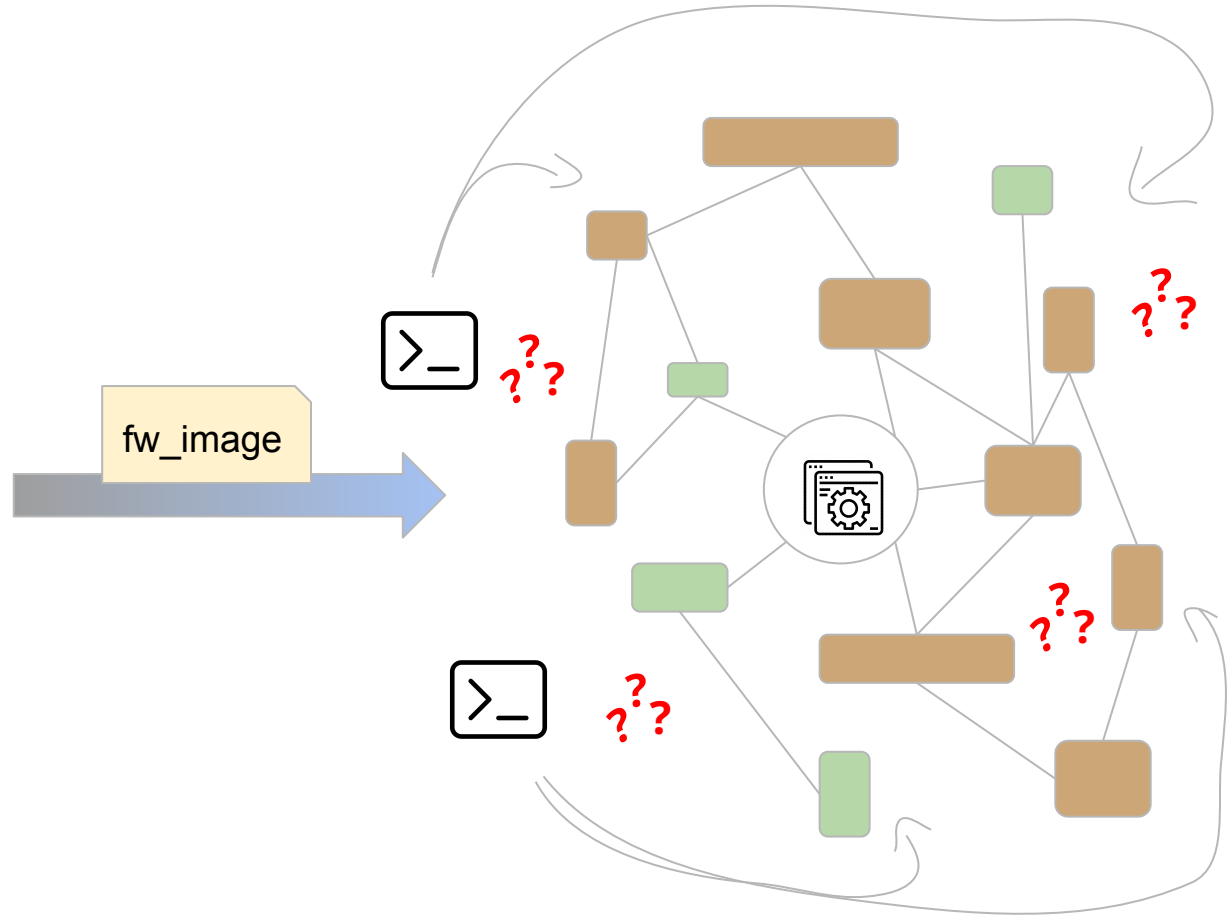
Rehosting



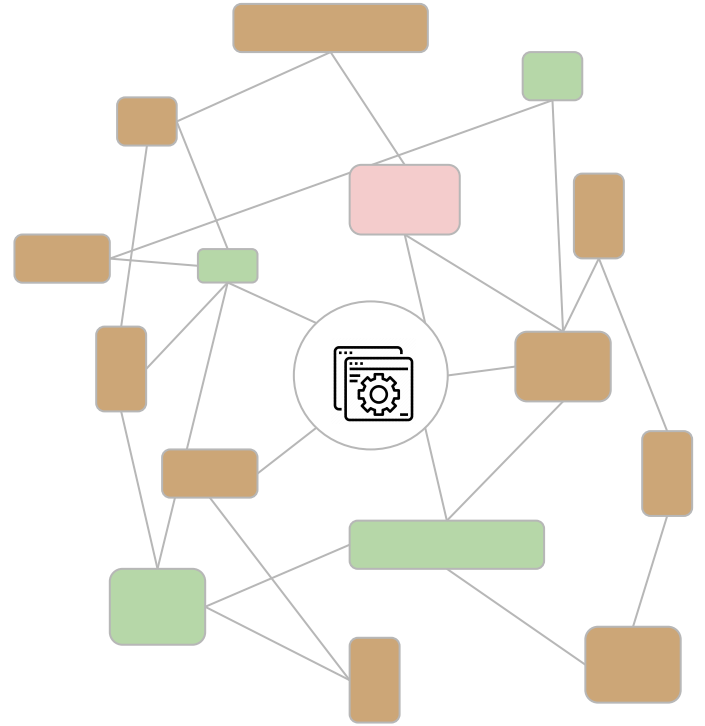
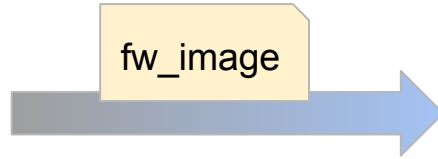
Rehosting



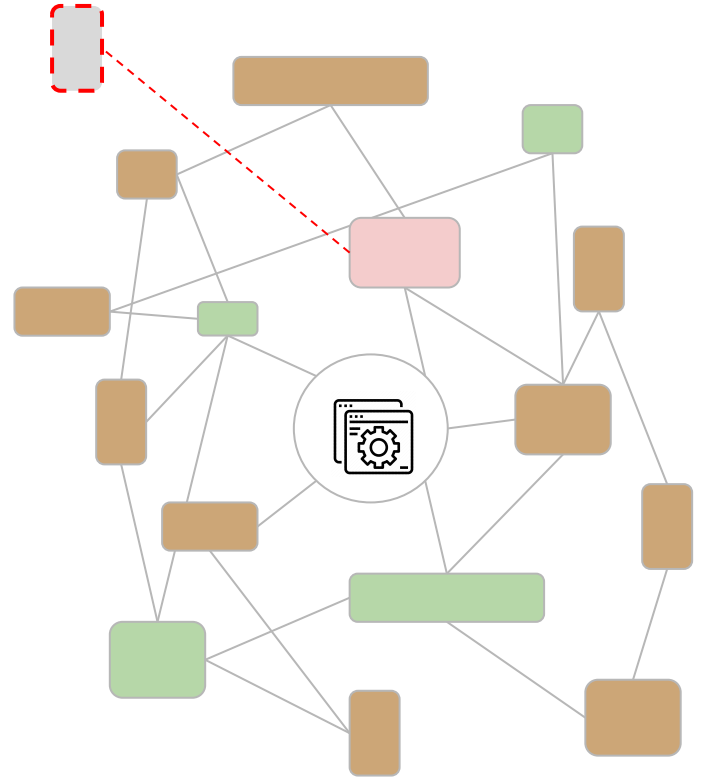
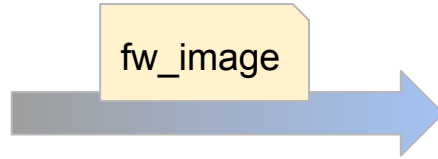
> Rehosting



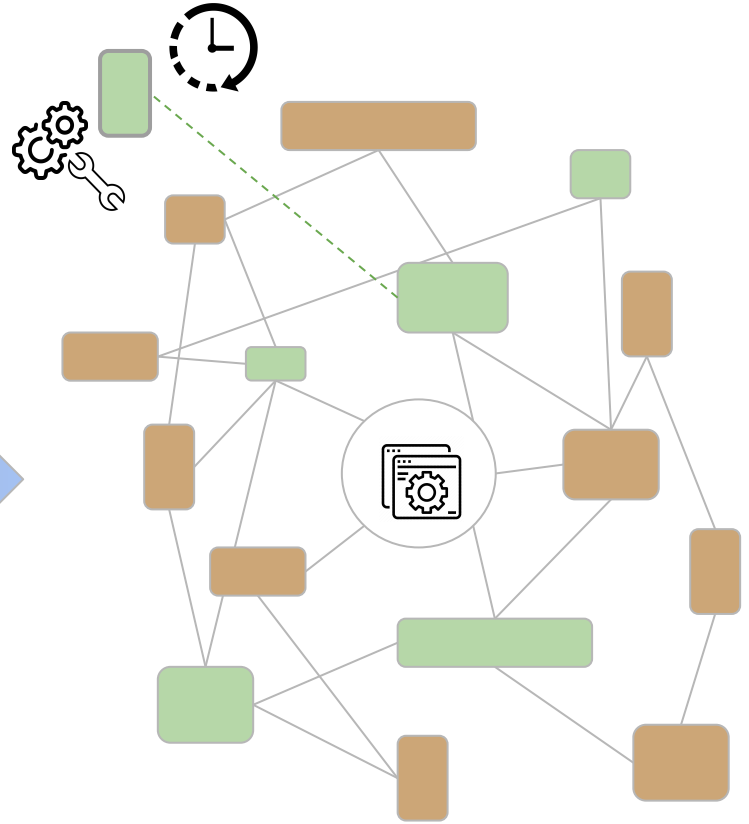
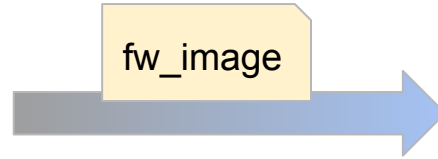
Rehosting



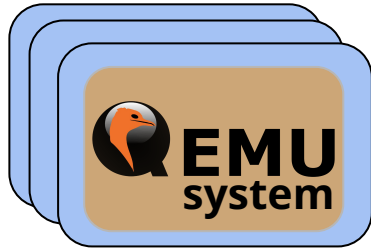
Rehosting



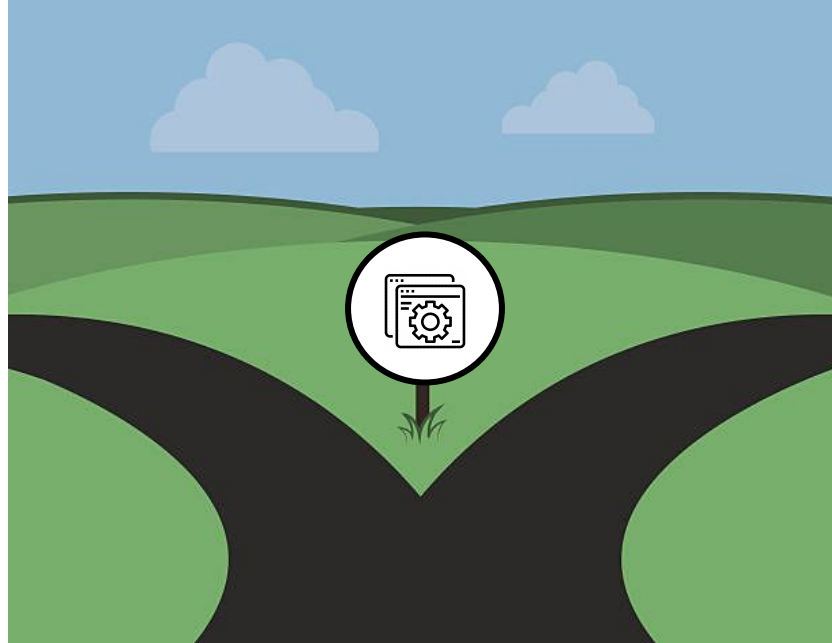
Rehosting



Rehosting



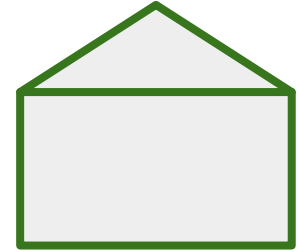
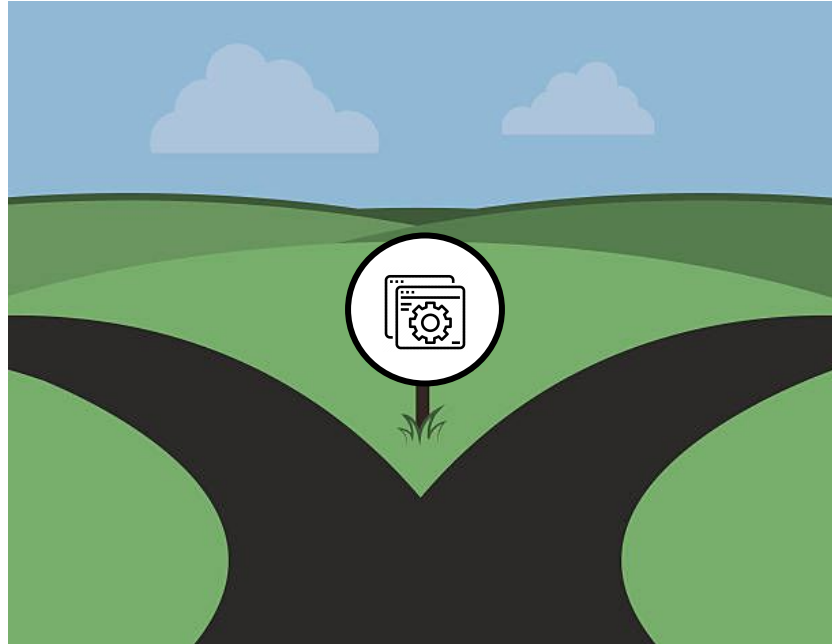
- Models
- Stubs
- Wrappers



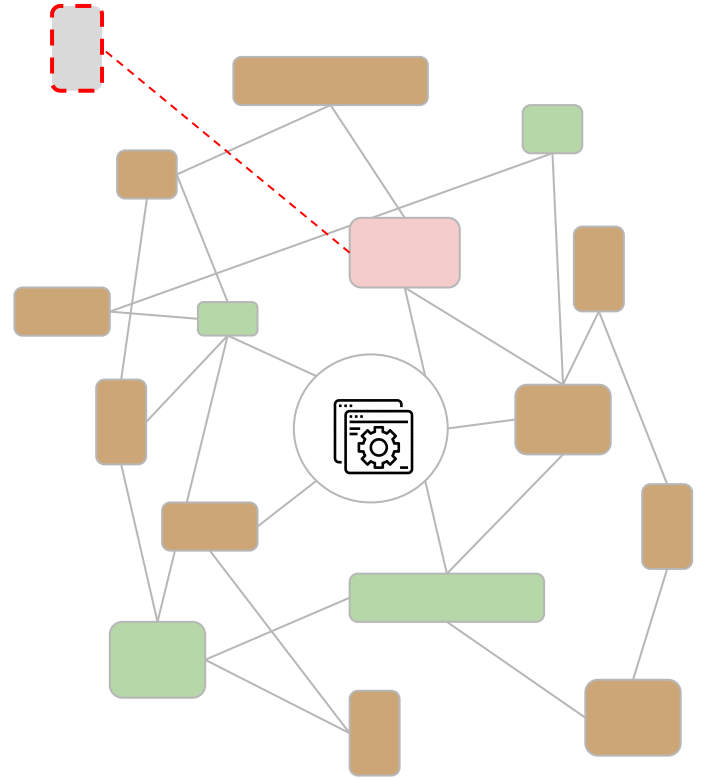
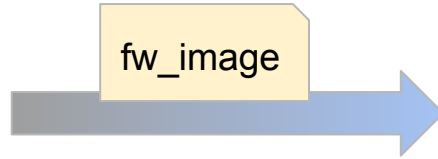
Rehosting



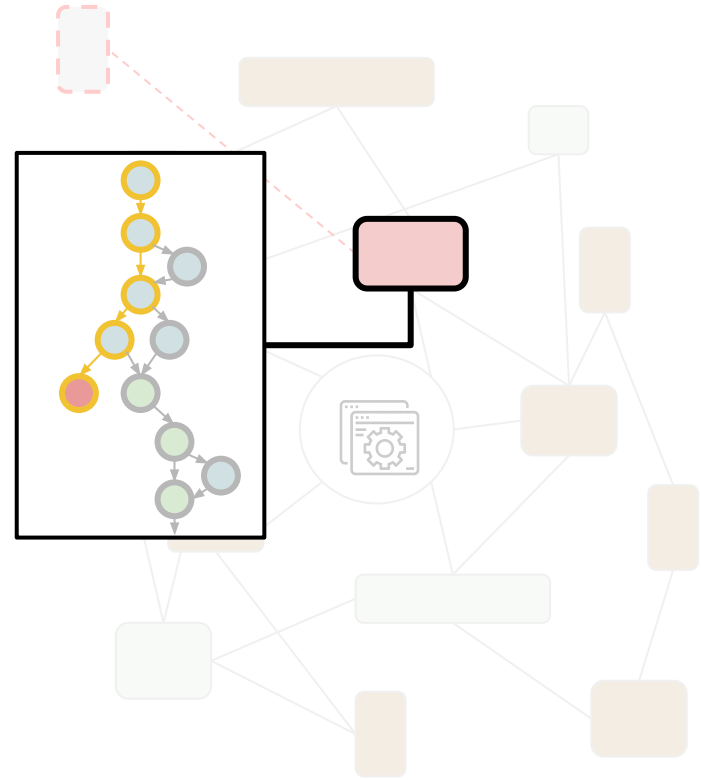
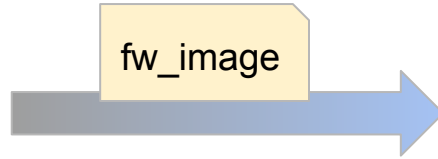
- Models
- Stubs
- Wrappers



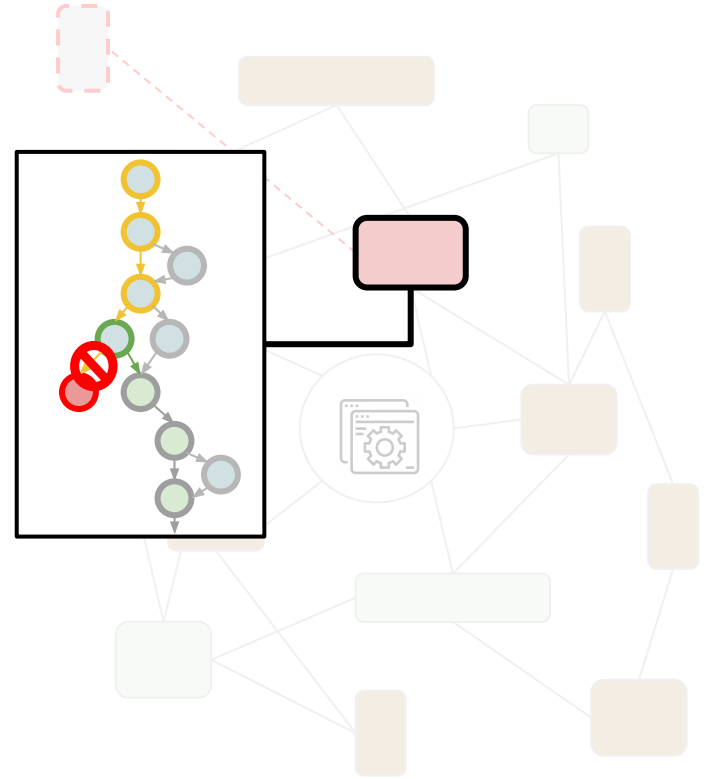
Rehosting



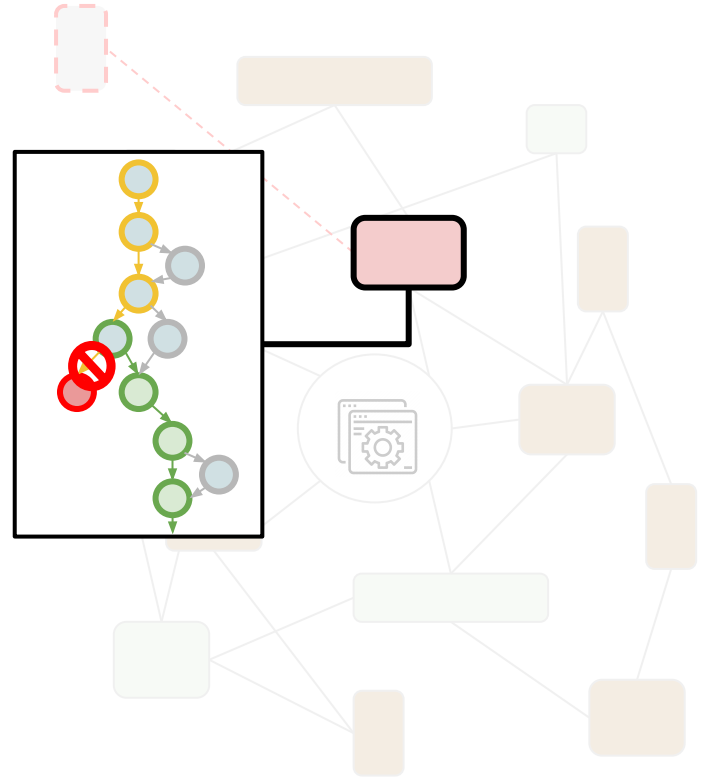
Rehosting



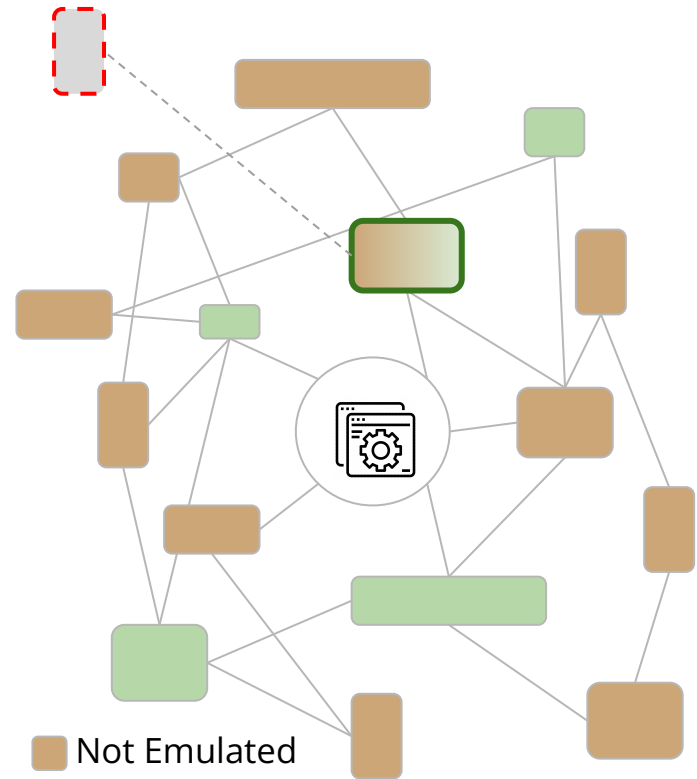
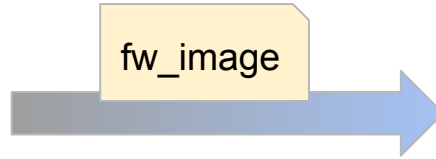
Rehosting






Rehosting

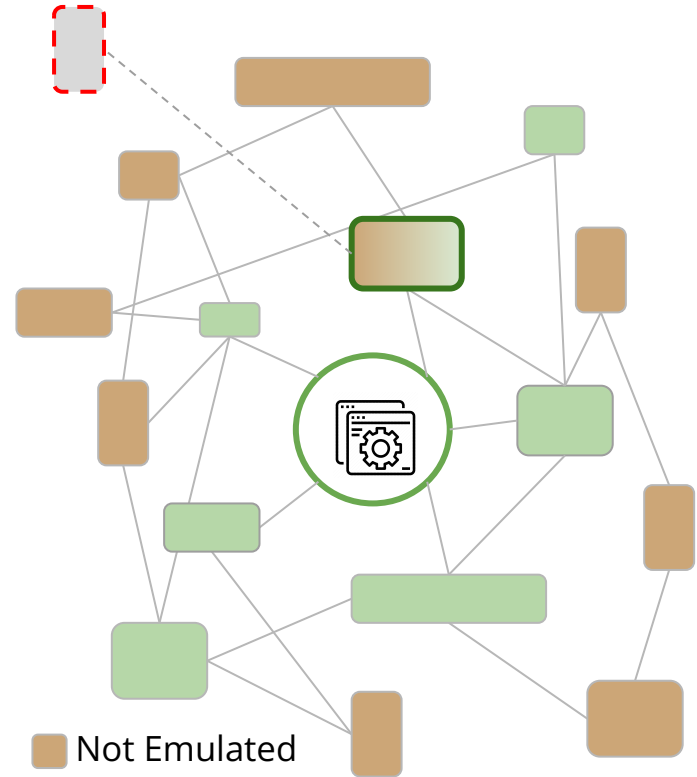
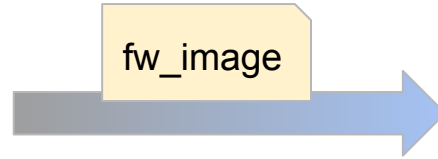





Rehosting



-  Not Emulated
-  Emulated
-  Emulated (Limited/Incomplete)

Rehosting



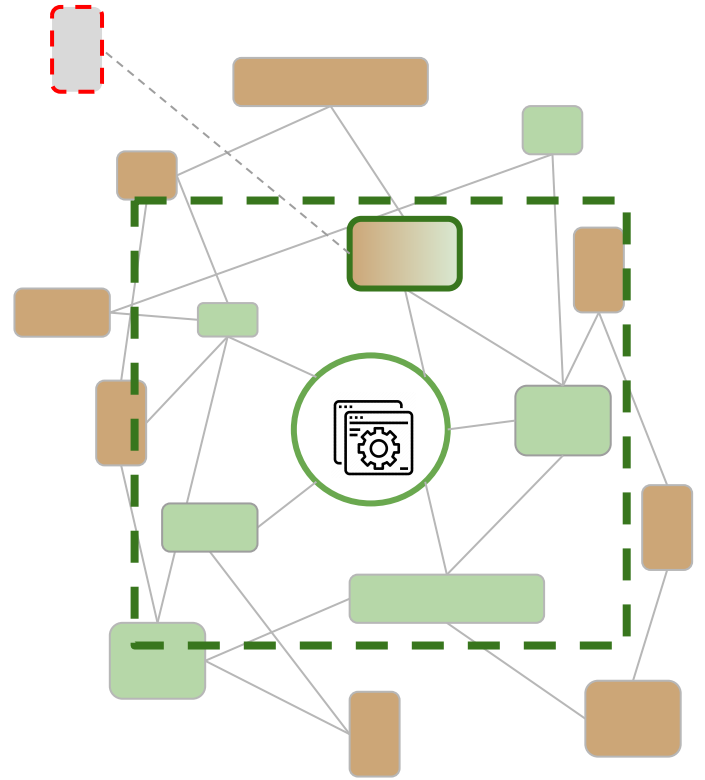
-  Not Emulated
-  Emulated
-  Emulated (Limited/Incomplete)

Rehosting

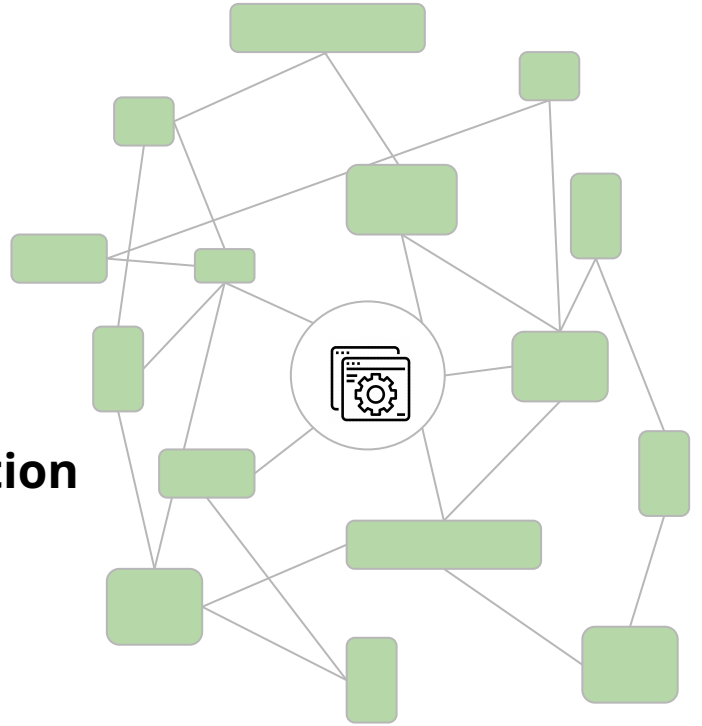
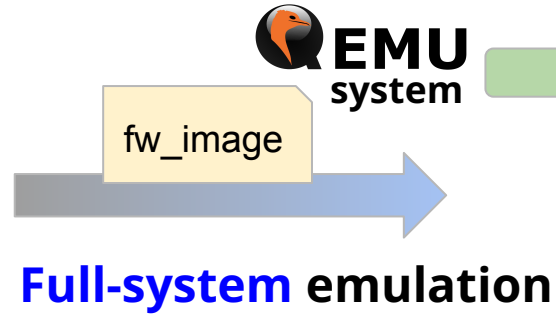


fw_image

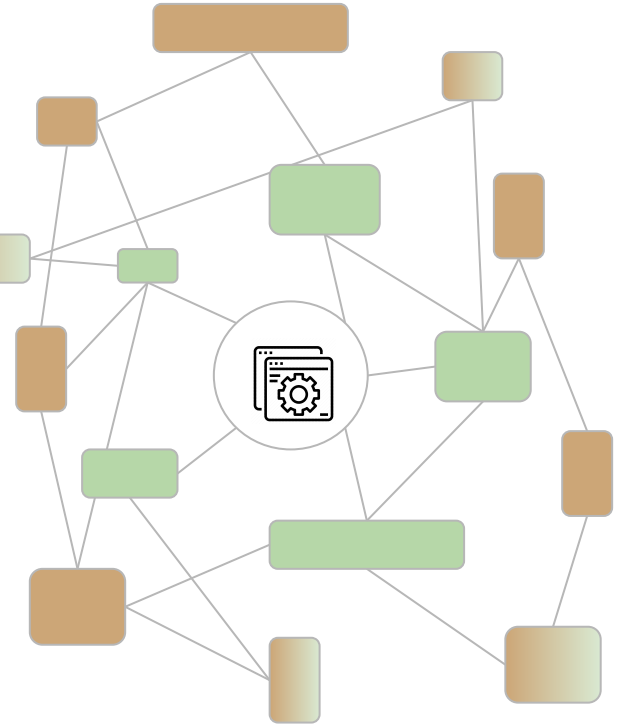
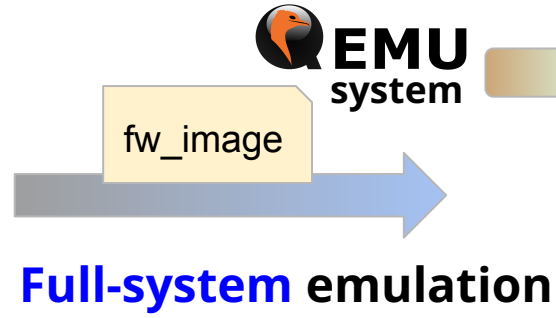
CVE-2022-40067 ...
CVE-2022-40076
(Tenda AC21, *httpd*)



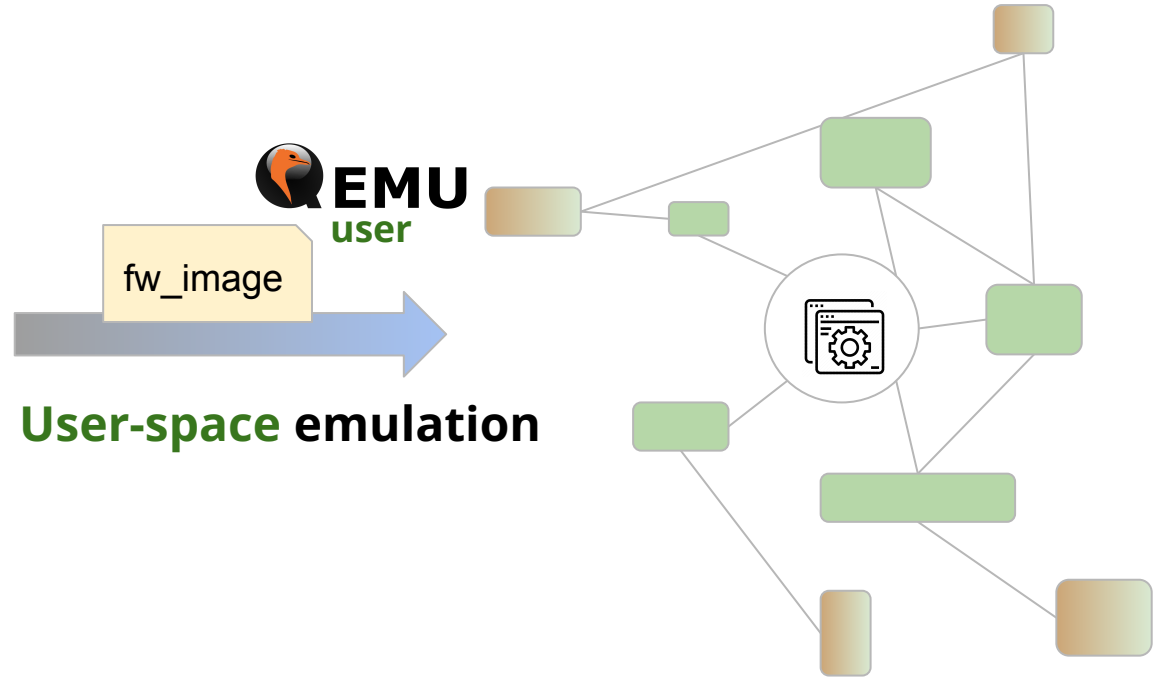
Rehosting



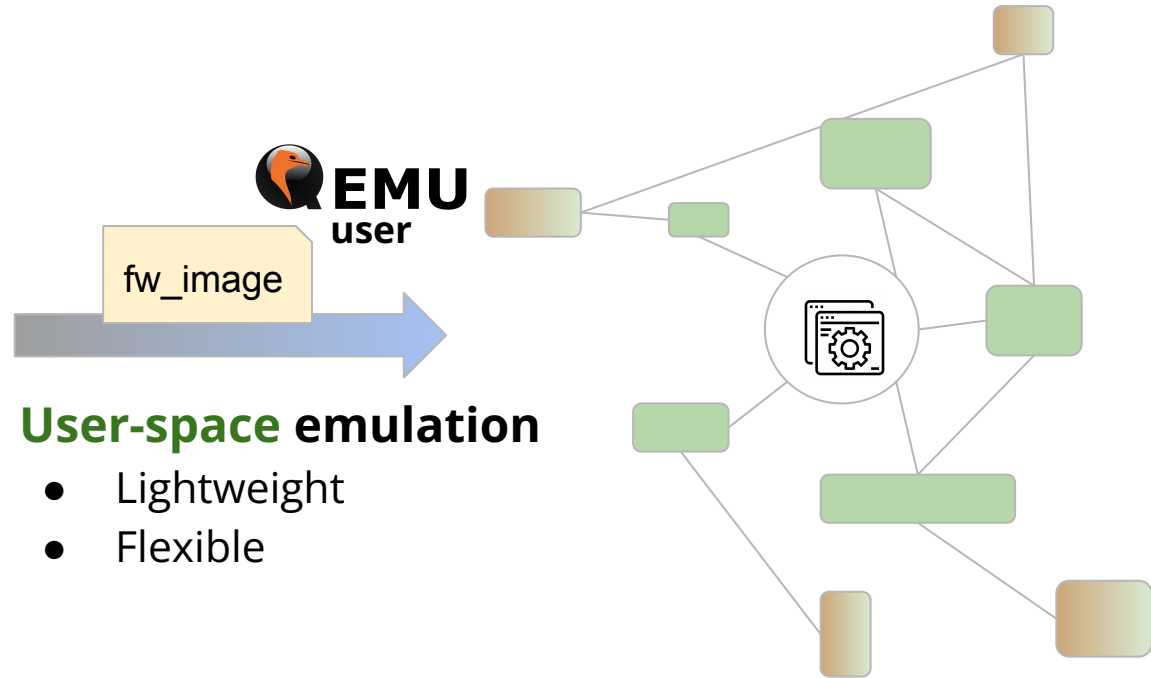
Rehosting



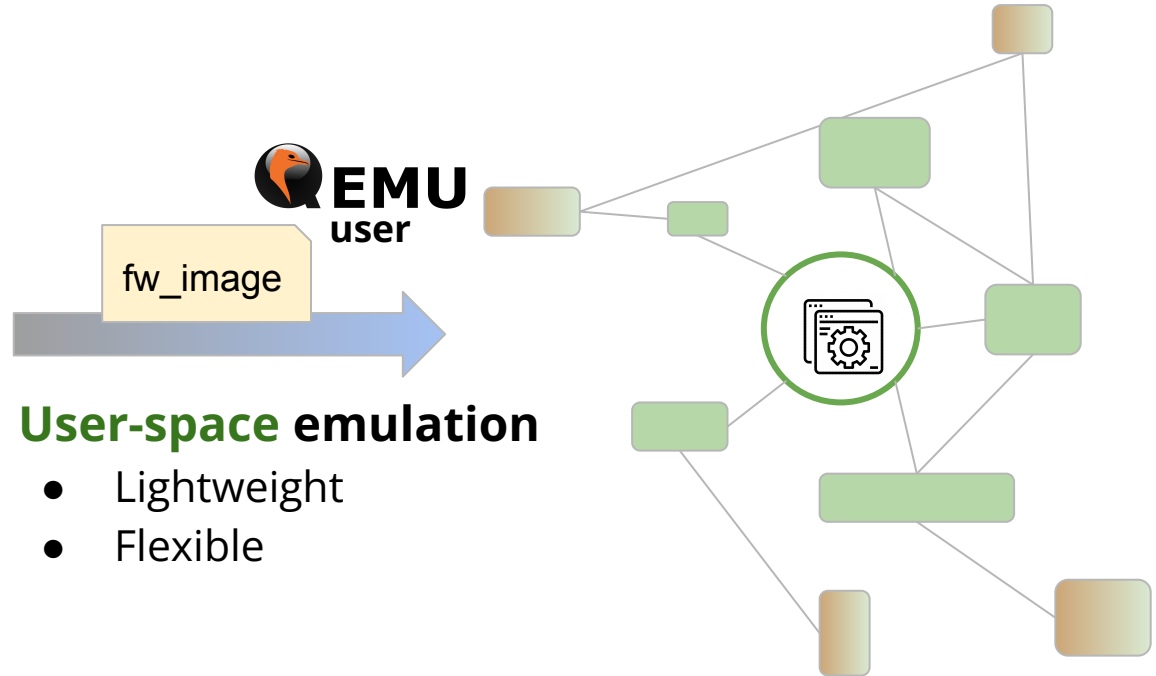
Rehosting



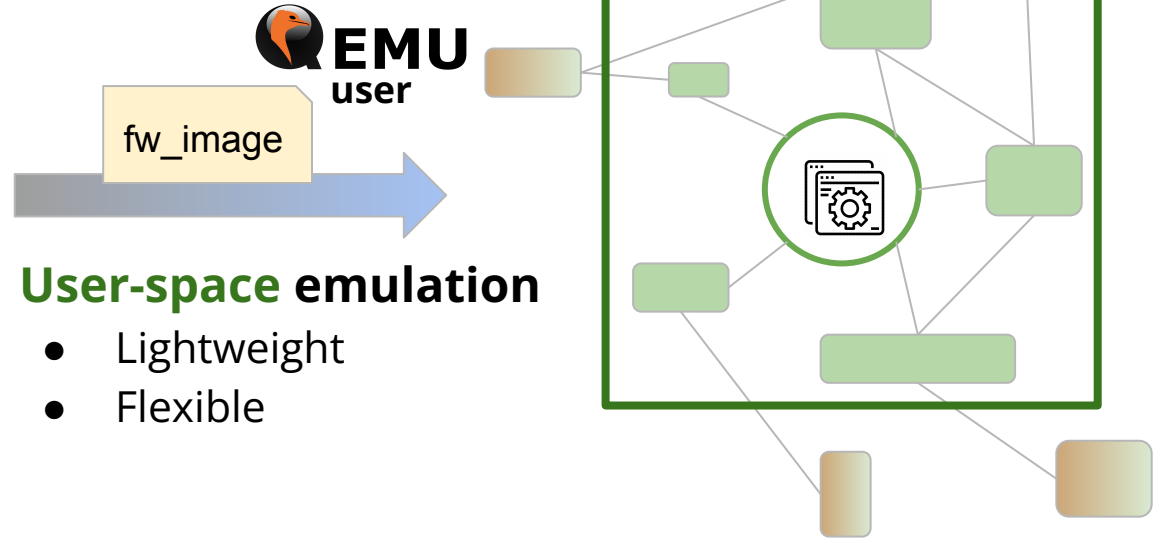
Rehosting



Rehosting



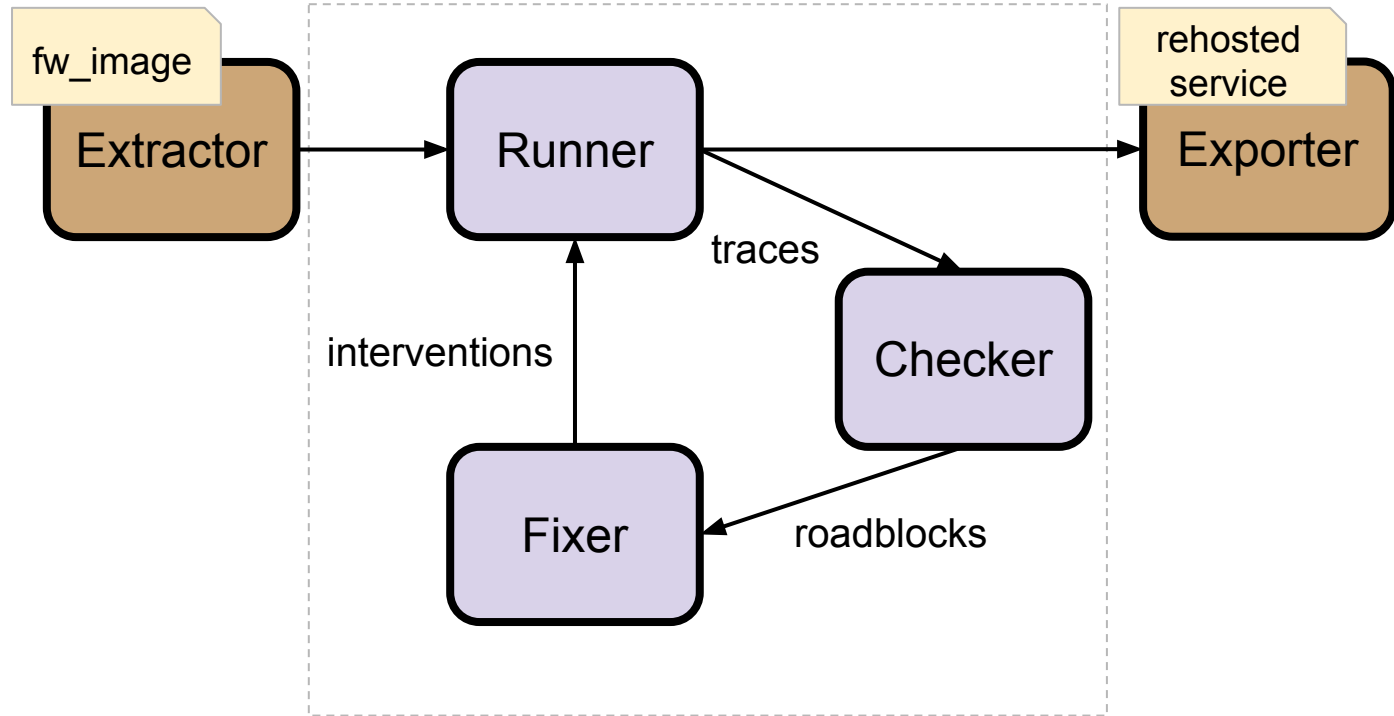
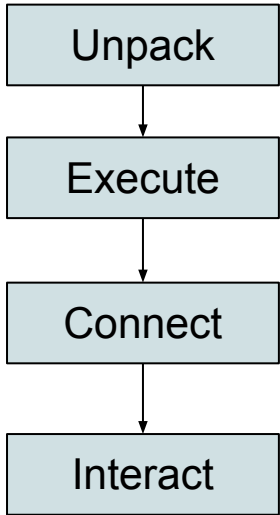
Rehosting





Greenhouse

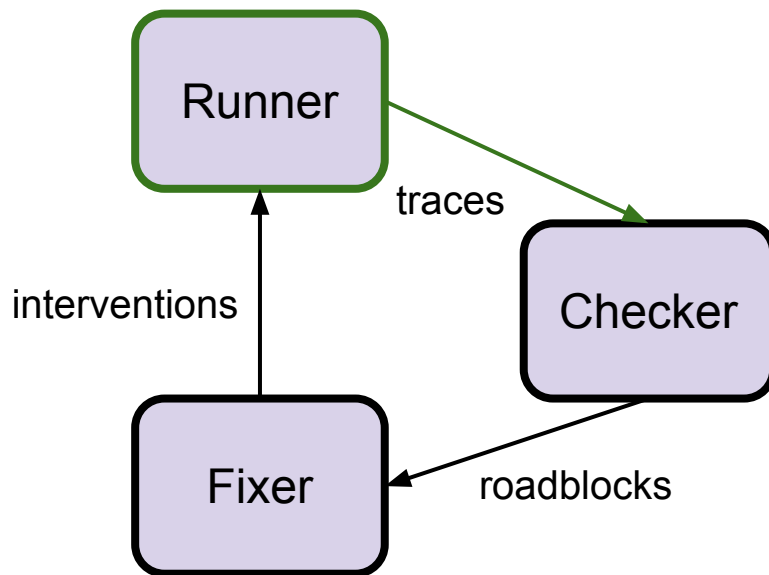
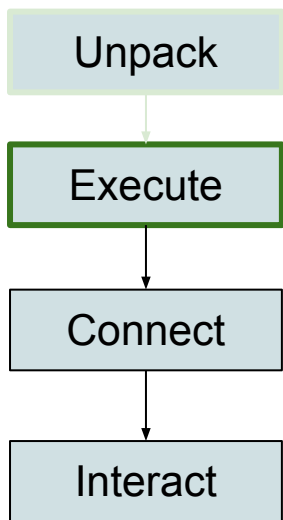
Rehosting Stages





Roadblocks and Interventions

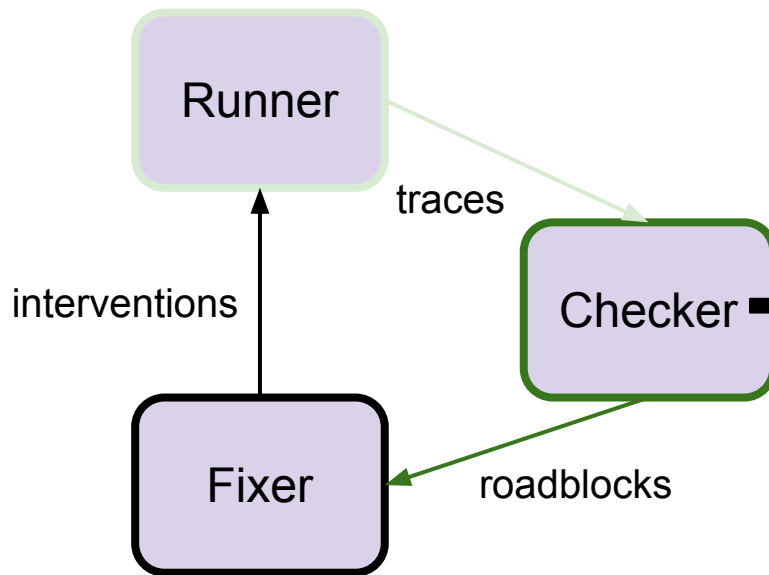
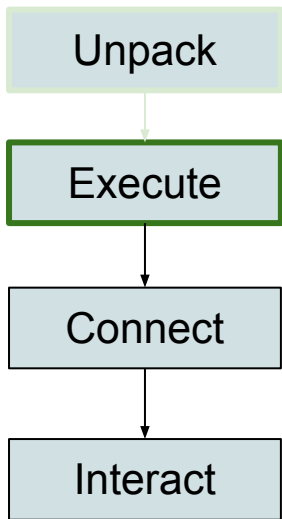
- Example: ASUS GPL_WL500W_1985





Roadblocks and Interventions

- Example: ASUS GPL_WL500W_1985



Stdout:

```
..  
"can't bind to any  
address"  
Exit 2
```

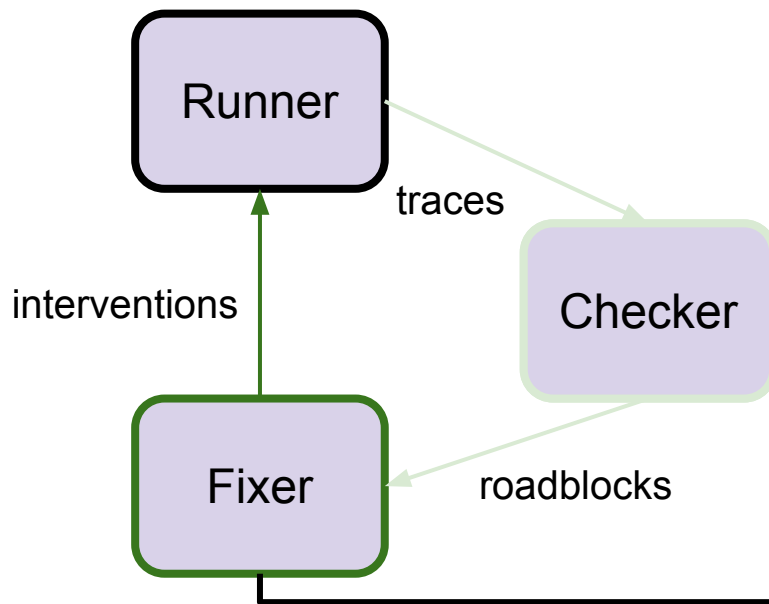
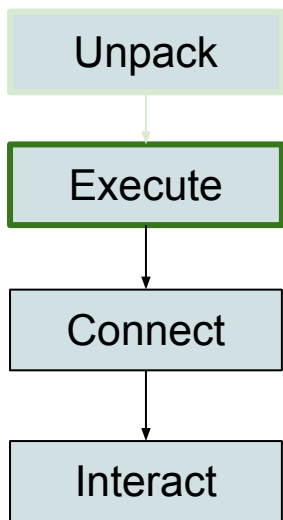
Stderr:

```
..  
[GreenHouseQEM  
U] IP: 192.168.1.1  
..
```



Roadblocks and Interventions

- Example: ASUS GPL_WL500W_1985



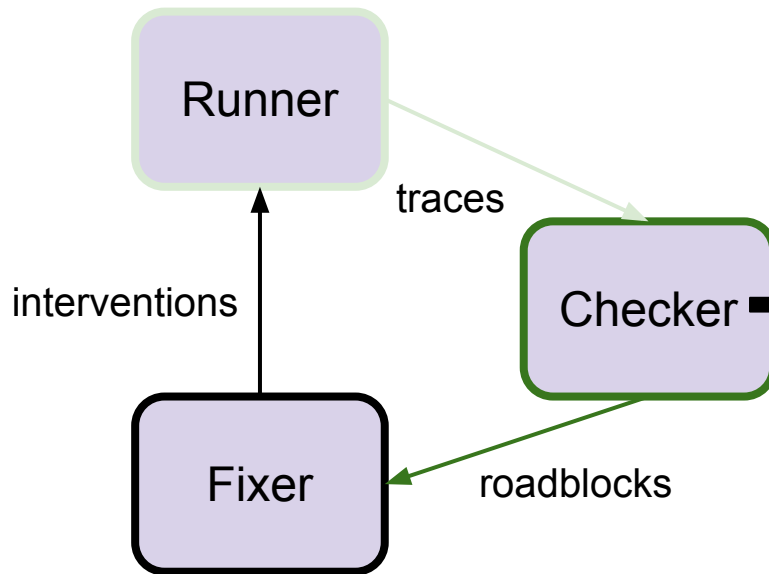
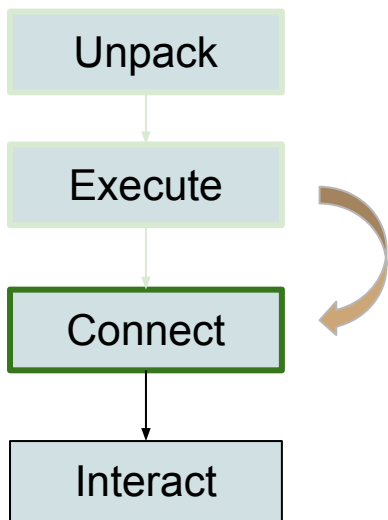
Network Device:
192.168.1.1

Update *run.sh*:
+ create dummy tap device



Roadblocks and Interventions

- Example: ASUS GPL_WL500W_1985

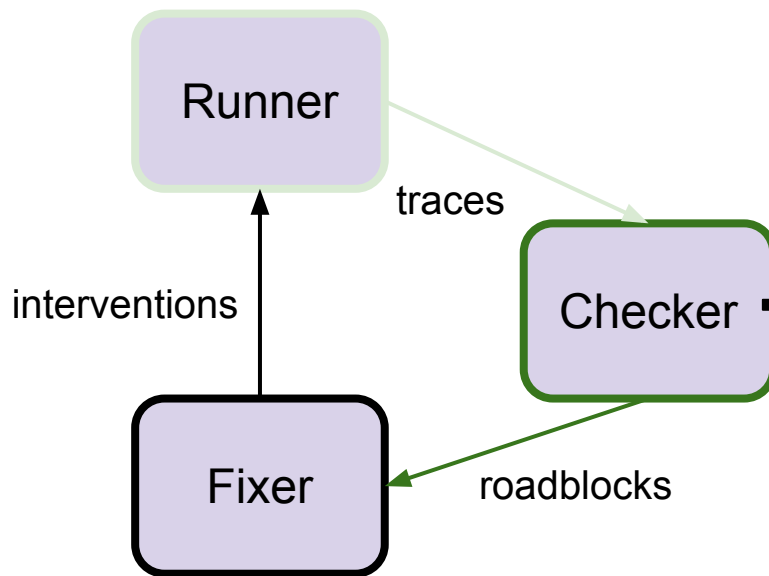
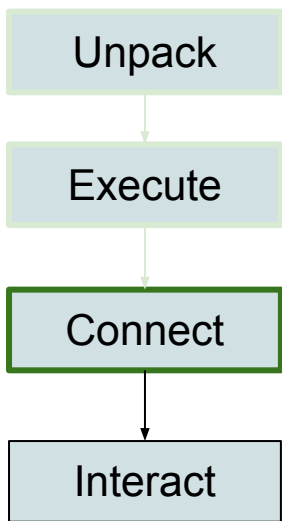


```
Stdout:  
..  
Successful Bind 0  
..  
curl:  
..  
<html><head>  
</head><body>  
</body></html>
```



Roadblocks and Interventions

- Example: ASUS GPL_WL500W_1985



NVRAM:

http_passwd=
Unknown
http_username=
Unknown

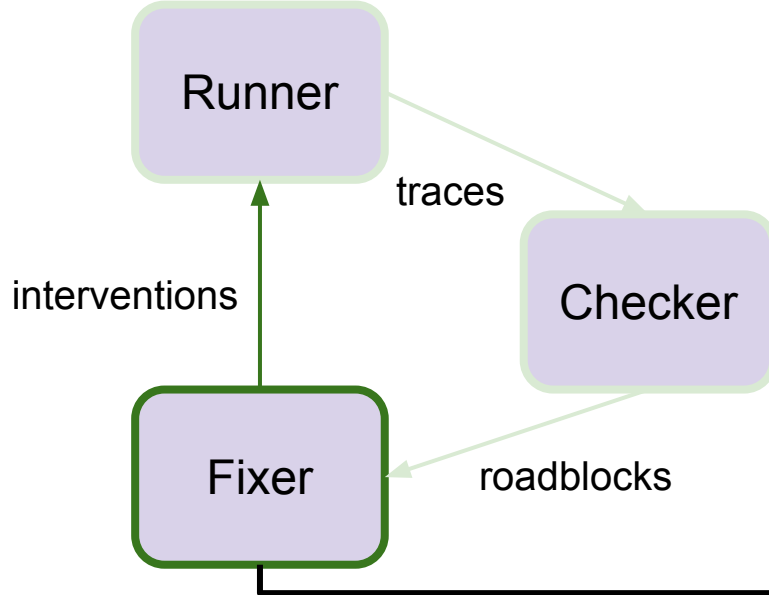
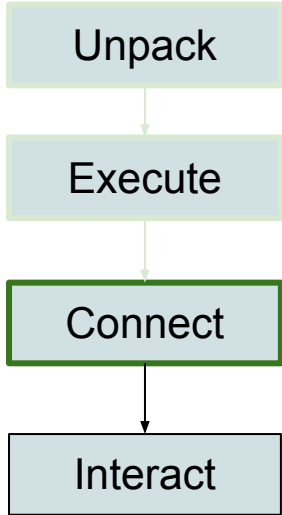
Missing targets:

```
{'/var/run',  
'index.asp',  
'/etc/TZ', ..}
```



Roadblocks and Interventions

- Example: ASUS GPL_WL500W_1985

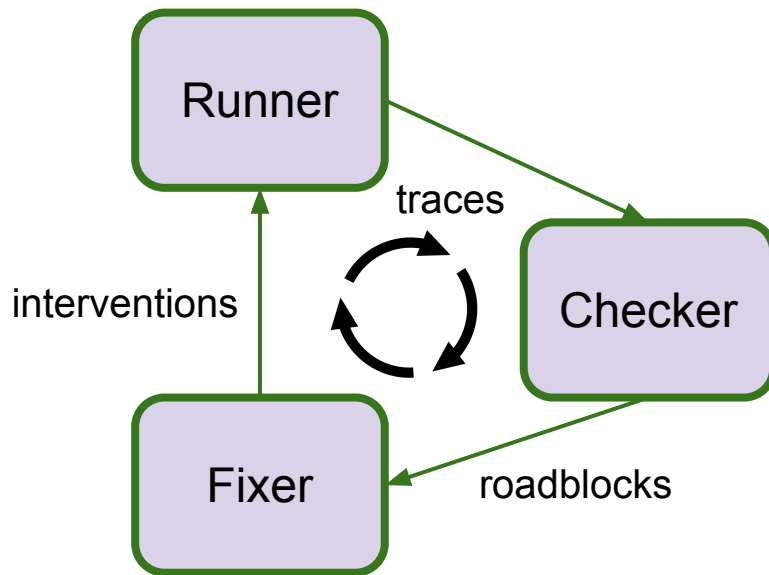
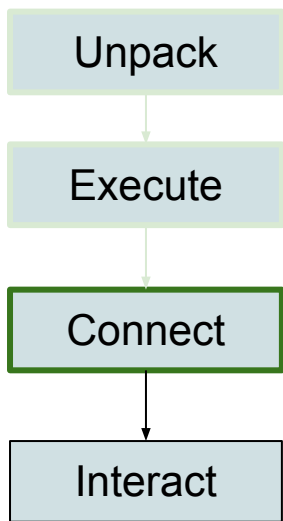


```
NVRAM:  
http_passwd=  
http_username=  
admin  
  
Create:  
/etc/TZ  
/var/run/  
  
Copy:  
/www/*.asp  
/www/*.html
```




Roadblocks and Interventions

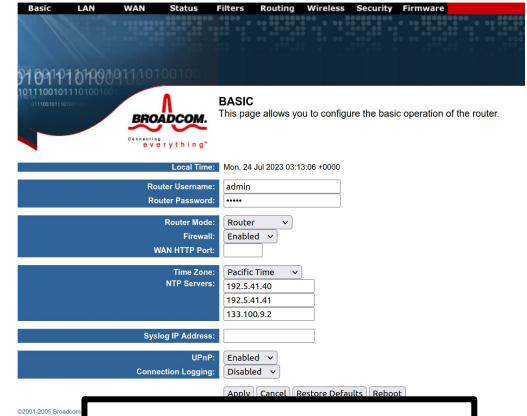
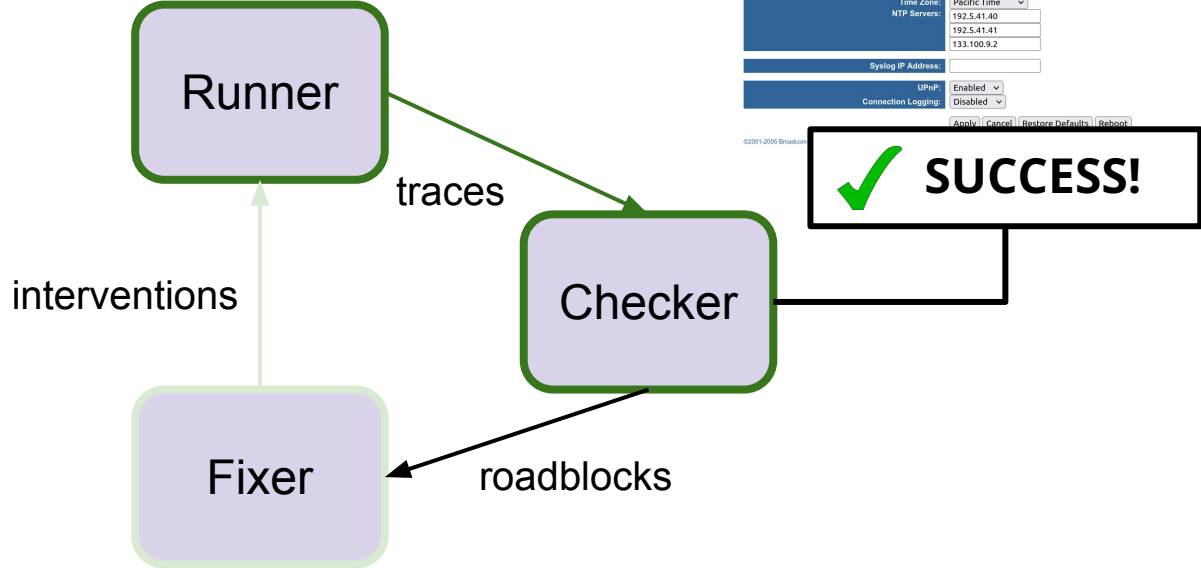
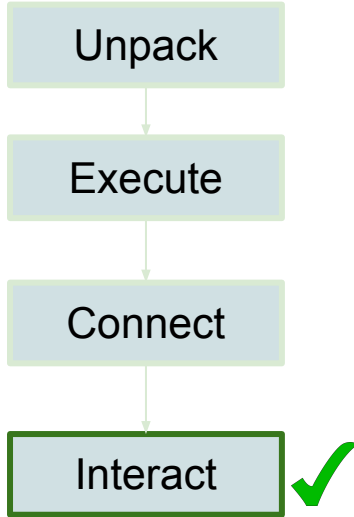
- Repeat and iteratively apply interventions until success





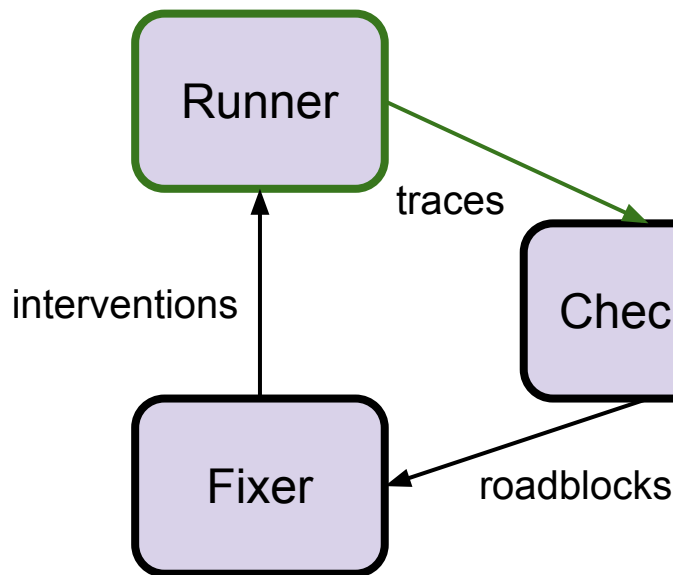
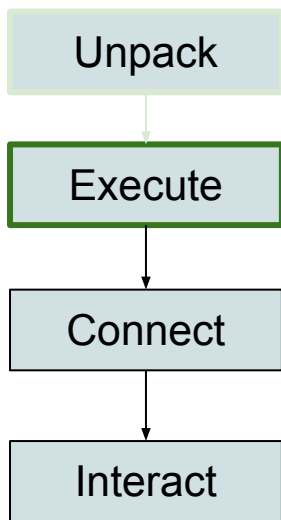
Roadblocks and Interventions

- Example: ASUS GPL_WL500W_1985



> Binary Patching

- Example: Tenda US_AP5V1.0BR_V1.0.0.13_3920_TDE01

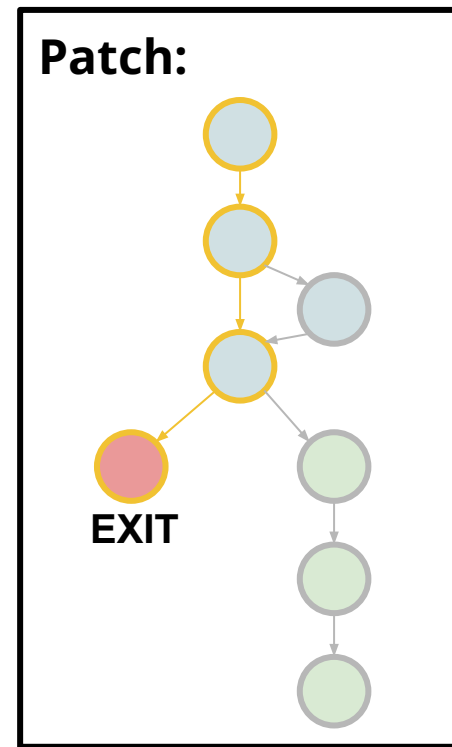
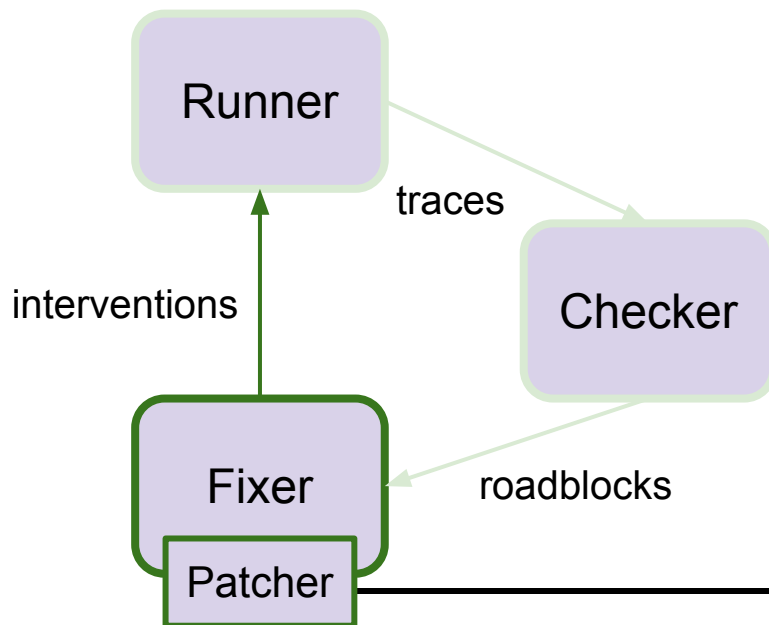
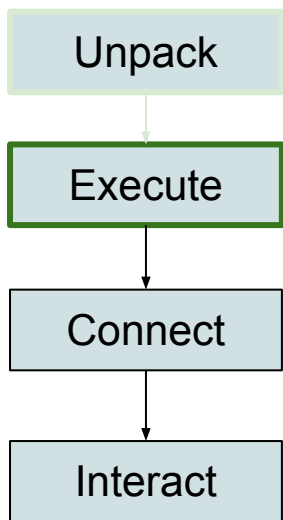


Stdout:

```
..  
connect: No such  
file or directory  
Connect to server  
failed.  
connect cfm  
failed  
..
```

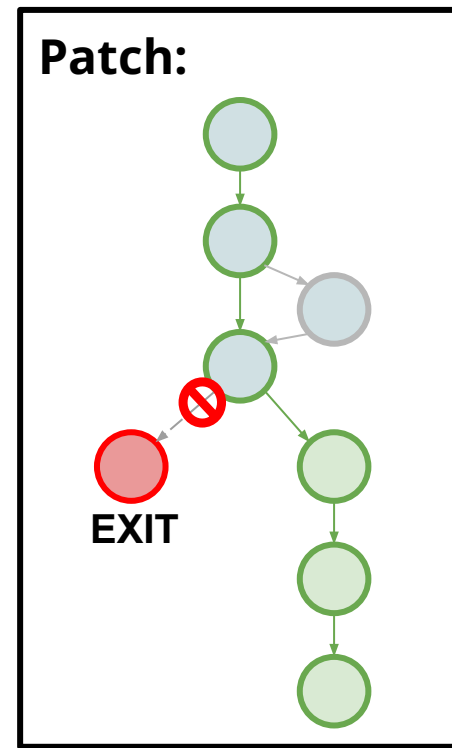
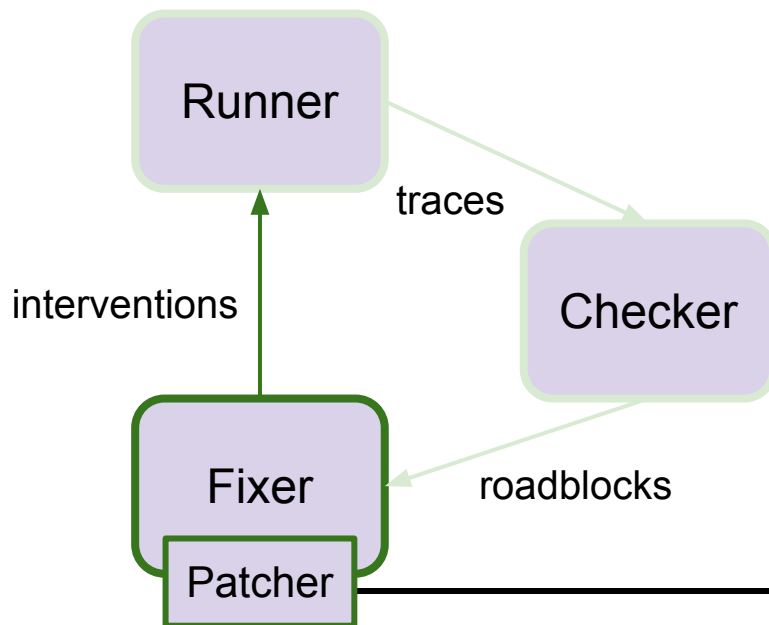
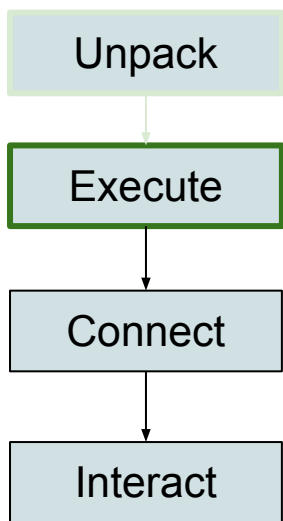
> Binary Patching

- Detect branch that leads to exit



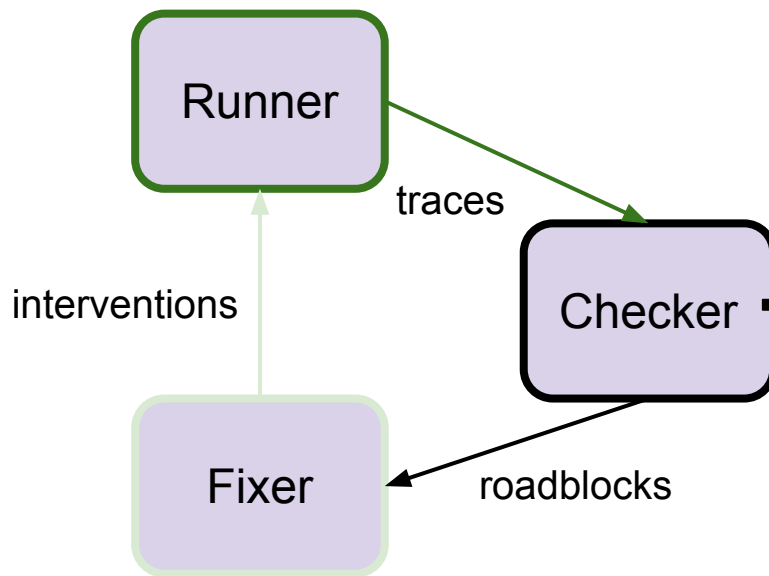
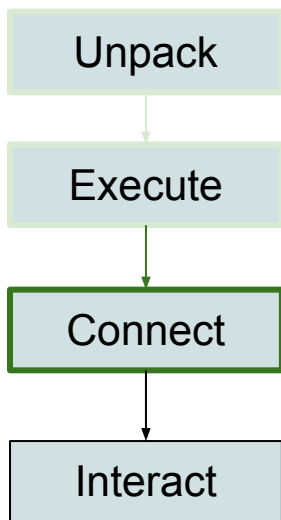
Binary Patching

- Switch branch to jump to new code



Binary Patching

- Example: Tenda US_AP5V1.0BR_V1.0.0.13_3920_TDE01

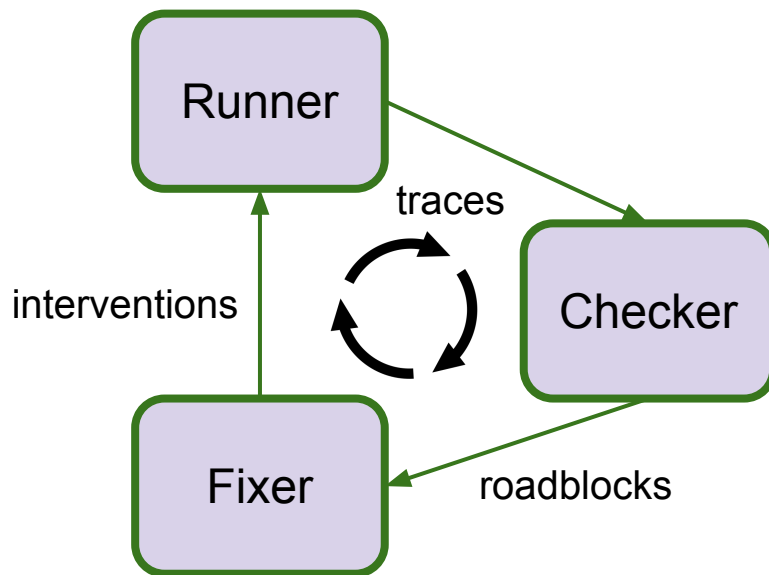
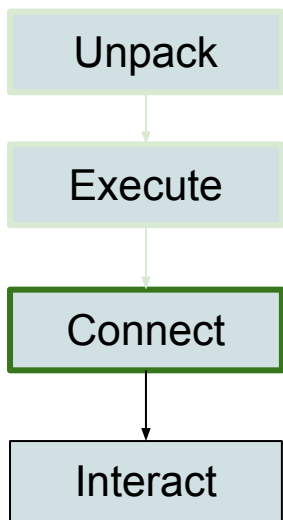


Stdout:

```
..  
connect: No such  
file or directory  
..  
webs: Listening  
for HTTP requests  
at address  
120.10.128.64  
..
```

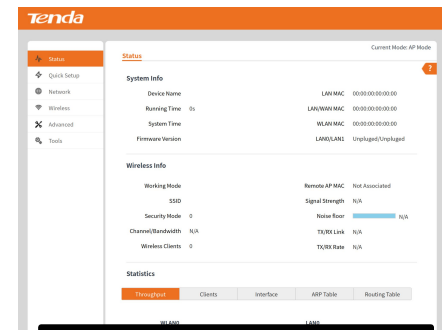
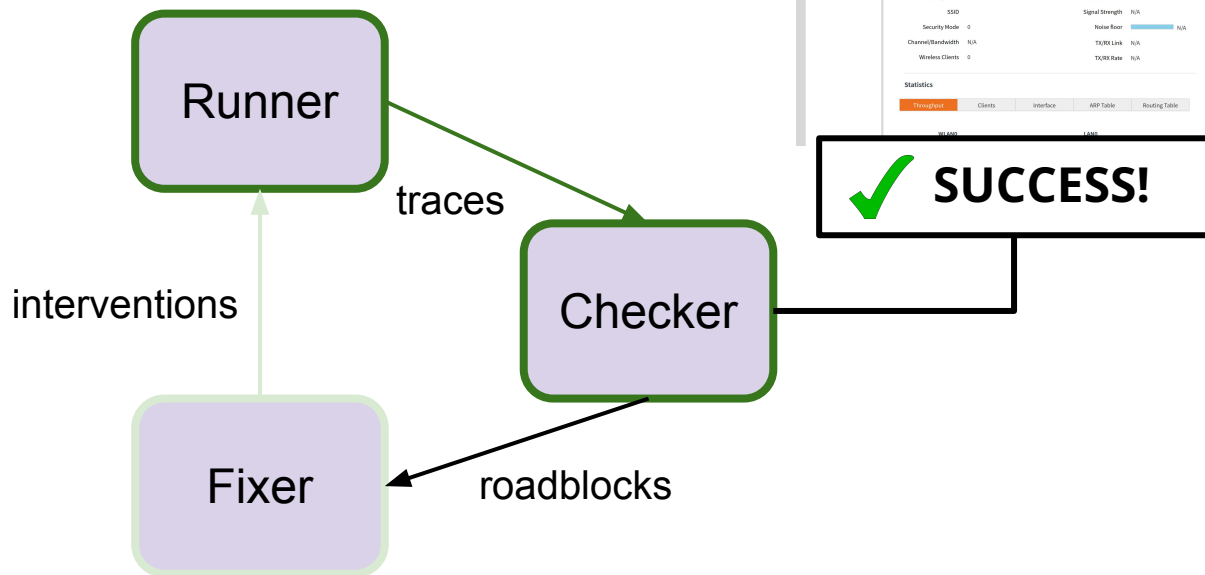
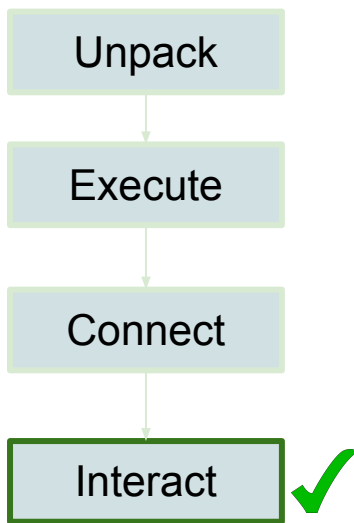
Binary Patching

- Repeat roadblocks and interventions again



Binary Patching

- Example: Tenda US_AP5V1.0BR_V1.0.0.13_3920_TDE01



Evaluation

- Dataset: **7,140** firmware images from 9 well-known manufacturers



Evaluation

- Dataset: **7,140** firmware images from 9 well-known manufacturers
- Automatically rehosted **2,841** HTTP firmware services
- Rehosted firmware is of sufficient fidelity for dynamic analysis
 - Routersploit replayed **717** web-based N-day attacks
 - Found **18,599** crashes across 733 binaries with AFL++
 - 358 crashes -> **26** zero-day vulnerabilities



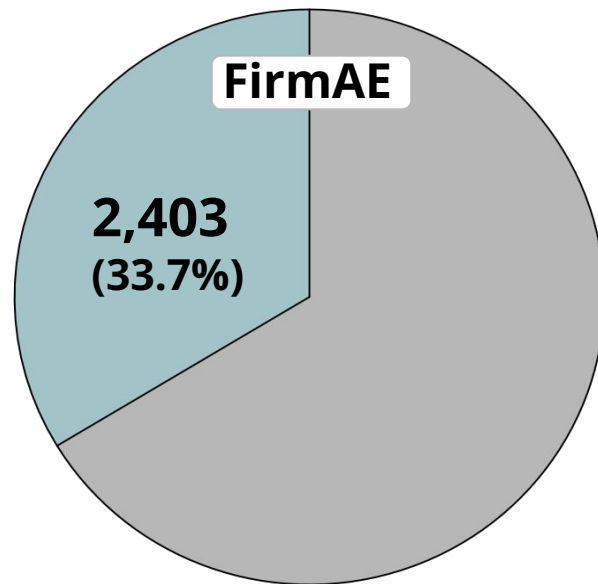
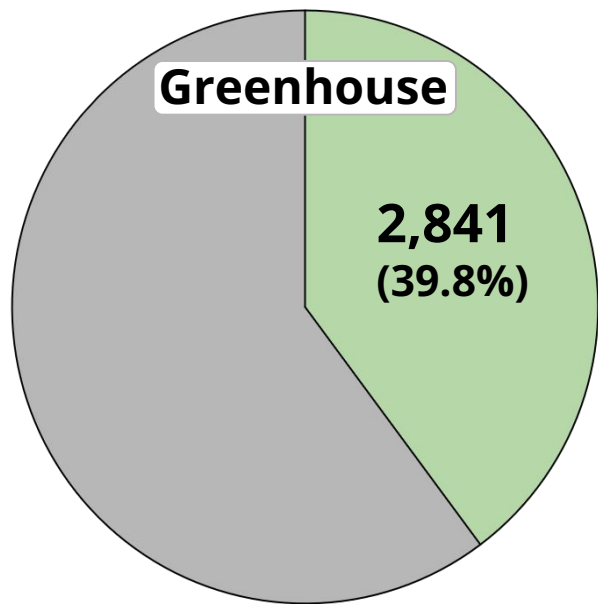
Evaluation

- Dataset: **7,140** firmware images from 9 well-known manufacturers
- Rehosted Services:
 - HTTP: **2,841**
 - UPnP: **1,822**
 - DNS: **1,650**



Evaluation vs FirmAE

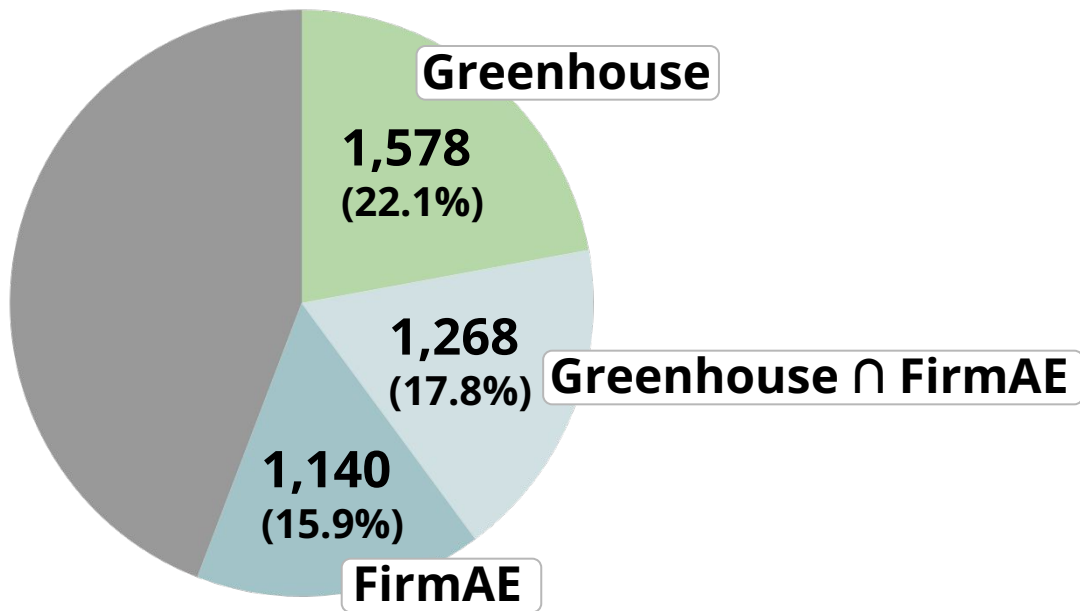
of Rehoused Firmware





Evaluation vs FirmAE

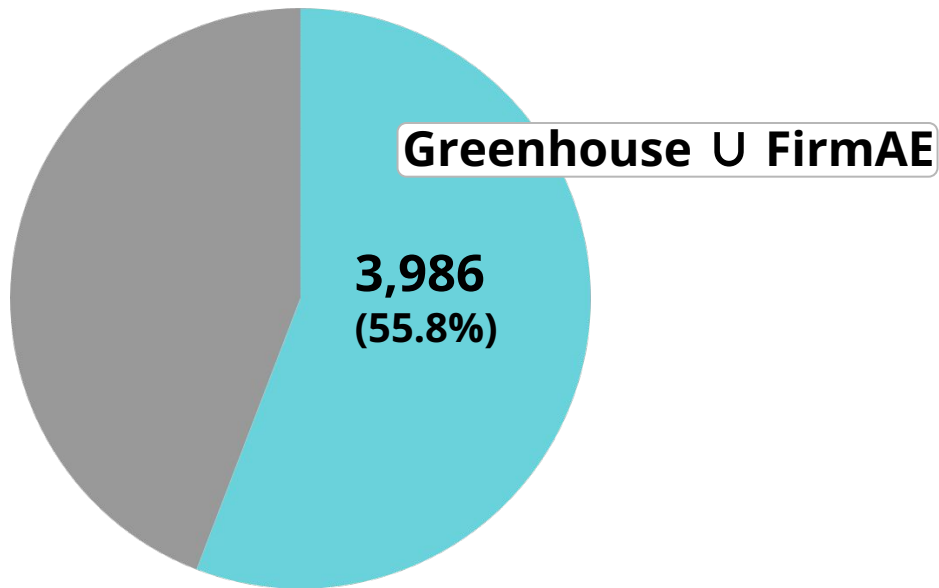
of Rehosted Firmware





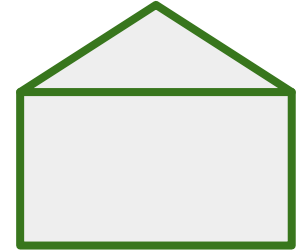
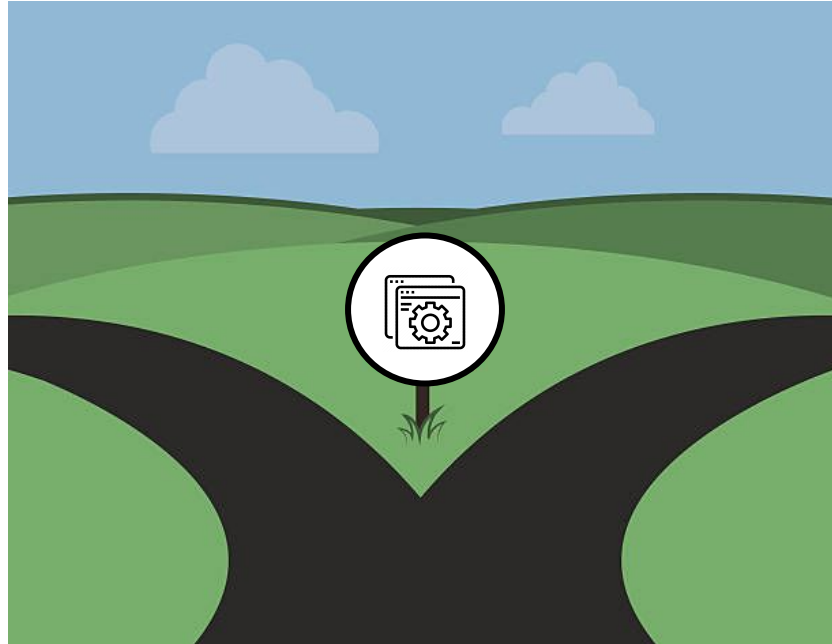
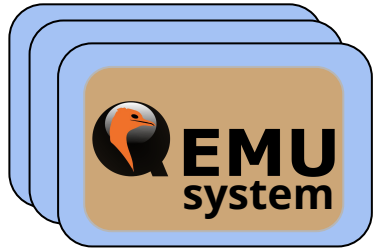
Evaluation vs FirmAE

of Rehosted Firmware

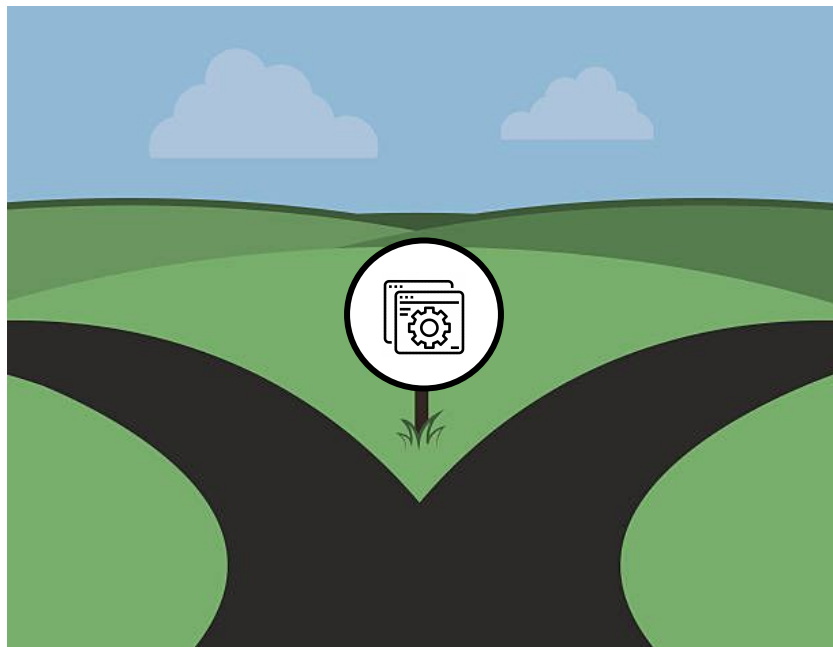




In Summary...



In Summary...



2,841
rehosted

3,981
combined

26
zero-days



Thank you!

Q & A



<https://github.com/sefcom/Greenhouse>

Hui Jun Tay (capysix)

htay2@asu.edu