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

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

ASU Arizona State University

sefcom security engineering for future computing
Problem
Problem
Problem
Problem

BUGS!

BUGS!

BUGS!
Problem
Problem
Rehosting
Rehosting

fw_image
Rehosting
Rehosting

fw_image
Rehosting

fw_image

Not Emulated
Emulated
Dependent
Rehosting

fw_image

Not Emulated
Emulated
Dependent
Rehosting

fw_image

Not Emulated
Emulated
Dependent
Rehosting

Full-system emulation
Rehosting

Full-system emulation

fw_image

Not Emulated
Emulated (built-in QEMU)
Rehosting

Full-system emulation
- Jetset (USENIX 2021)
- FirmAE (ACSAC 2020)
- Pretender (USENIX 2019)
- ...etc

Not Emulated
- Emulated (built-in QEMU)
- Emulated (extended)
Rehosting

**Full-system emulation**
- High overhead
- Rigid environment

fw_image

Not Emulated
Emulated (built-in QEMU)
Emulated (extended)
Rehosting
Rehosting

fw_image

>`_`

>`_`

>`_`
Rehosting
Rehosting
Rehosting
Rehosting
Rehosting

- Models
- Stubs
- Wrappers
Rehosting

- Models
- Stubs
- Wrappers
Rehosting

fw_image
Rehosting
Rehosting

fw_image
Rehosting
Rehosting
Rehosting

fw_image

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

fw_image

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

Full-system emulation

fw_image

EMU system
Rehosting

Full-system emulation
Rehosting

User-space emulation
Rehosting

User-space emulation
- Lightweight
- Flexible
Rehosting

User-space emulation

- Lightweight
- Flexible
Rehosting

User-space emulation
- Lightweight
- Flexible
Greenhouse

Rehosting Stages
- Unpack
- Execute
- Connect
- Interact

Diagram:
- Extractor
- Runner
- Checker
- Fixer
- Exporter

- fw_image
- rehosted service
- traces
- interventions
- roadblocks

Rehosting Stages:
1. Unpack
2. Execute
3. Connect
4. Interact
Roadblocks and Interventions

- Example: ASUS GPL_WL500W_1985

Diagram:
- Unpack
- Execute
- Connect
- Interact
- Runner
  - traces
  - interventions
- Checker
  - roadblocks
- Fixer
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

```
Unpack

Execute

Connect

Interact
```

**Network Device:**
192.168.1.1

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

```
Runner

traces

interventions

Fixer

roadblocks

Checker
```
Roadblocks and Interventions

- Example: ASUS GPL_WL500W_1985

Unpack → Execute → Connect → Interact

Runner

Fixer

Checker

Stdout:
.. Successful Bind 0 ..
curl:
.. <html><head></head><body></body></html>
Roadblocks and Interventions

- Example: ASUS GPL_WL500W_1985

Unpack

Execute

Connect

Interact

Runner

traces

Fixer

Checker

Missing targets:
{/var/run', 'index.asp', '/etc/TZ', ..}

NVRAM:
http_passwd= Unknown
http_username= Unknown

Roadblocks and Interventions

47
Roadblocks and Interventions

- Example: ASUS GPL_WL500W_1985

Unpack → Execute → Connect → Interact

Runner
- traces
- interventions

Fixer
- roadblocks

Checker

NVRAM:
- http_password=
- 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

Unpack ➔ Execute ➔ Connect ➔ Interact

Runner ➔ Checker ➔ Fixer

Stdout:
.. connect: No such file or directory
Connect to server failed.
connect cfm failed
..
<Binary Patching>

- Detect branch that leads to exit

Unpack → Execute → Connect → Interact

Runner

Fixer

Checker

Patcher

traces

interventions

roadblocks

Patch:

EXIT
Binary Patching

- Switch branch to jump to new code

Unpack -> Execute -> Connect -> Interact

Runner

Fixer

Checker

Patcher

traces

interventions

roadblocks

Patch:

EXIT
Binary Patching

- Example: Tenda US_AP5V1.0BR_V1.0.0.13_3920_TDE01

Unpack → Execute → Connect → Interact

Stdout:
.. connect: No such file or directory
..
webs: Listening for HTTP requests at address 120.10.128.64
..
• Repeat roadblocks and interventions again
Binaty Patching

- Example: Tenda US_AP5V1.0BR_V1.0.0.13_3920_TDE01

Unpack → Runner → Checker

Success!

Executor

Fixer

Interventions

Roadblocks

Traces
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 Rehosted Firmware

- **Greenhouse**: 2,841 (39.8%)
- **FirmAE**: 2,403 (33.7%)
Evaluation vs FirmAE

# of Rehosted Firmware

- **Greenhouse**: 1,578 (22.1%)
- **Greenhouse ∩ FirmAE**: 1,268 (17.8%)
- **FirmAE**: 1,140 (15.9%)
Evaluation vs FirmAE

# of Rehosted Firmware

- Greenhouse U FirmAE: 3,986 (55.8%)
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