

CHAOS

Common Hackable Adaptable Operating System

拡張性に優れて自由に改造できる組込みOS

学習駆動コース / 坂井ゼミ / 都留 悠哉

Abstract

CHAOS は "拡張性に優れて自由に改造できる" をコンセプトに開発した組込みOSです。

特徴

- フルスクラッチ開発 (独自カーネル)
- Raspberry Pi で動作可能 (aarch64)
- 開発にはGNUツールチェーンだけを使用



<https://github.com/75u2u/CHAOS>

セキュリティ機能として、通常の組込み機器ではバッファオーバーフロー脆弱性の対策するためにICEやJTAGを使うところ、それらを使うことなくOS内に**デバッガ(Kernel Debugger)**を実装することで不正メモリアクセスの迅速な対策と解析ができます。

CHAOS Shell

```

root@chaos:~/CHAOS$ make run
qemu-system-aarch64 -M raspi3 -kernel kernel8.img -serial null -serial stdio
[Kernel Boot Log]
input password> pass
success!
> echo SecHack365
SecHack365
> 1+1
2
> rand
181F6A83
> rand
39F5FE3D
> rand
9479B618
> on 16
GPIO 16 ON!
    
```

対応コマンド例

- echo
- rand
- on
- off
- help
- reboot
- shutdown

CHAOSと対話するための基本となるプログラム

入力したコマンドは、char型のbuf配列に格納されてstrcmpで対応する文字列を比較して処理を決めています。コマンドは増やしたり減らしたり、処理内容を自由に改造できます。

Kernel Debugger

```

root@chaos:~/CHAOS$ make run
qemu-system-aarch64 -M raspi3 -kernel kernel8.img -serial stdio
Synchronous: Breakpoint instruction
> r
x0: 0000000000008E2D4 x1: 000000000000301 x2: 000000000000006
x3: 000000000000000B x4: 000000000002400 x5: 00000000000000C
x6: 00000000000038002 x7: 000000000000000 x8: 000000000000000
x9: 000000000000000 x10: 000000000000000 x11: 000000000000000
x12: 000000000000000 x13: 000000000000000 x14: 000000000000000
x15: 000000000000000 x16: 000000000000000 x17: 000000000000000
x18: 000000000000000 x19: 000000000000000 x20: 000000000000000
x21: 000000000000000 x22: 000000000000000 x23: 000000000000000
x24: 000000000000000 x25: 000000000000000 x26: 000000000000000
x27: 000000000000000 x28: 000000000000000 x29: 000000000007FFF0
x30: 0000000000008E2D4 elr_el1: 8E2D4 spsr_el1: 600003C4
esr_el1: F2000000 far_el1: 0
sctlr_el1: 30D00800 tcr_el1: 0
    
```

CHAOS用に独自開発したデバッガ

トラップ例外の例外ハンドラを設定しておき、ブレークポイントでブレークしたらトラップ例外が発生し、例外ハンドラでレジスタの退避をした後に'g'コマンドを受け取ると退避していたレジスタの値をダンプさせることで実現。

Summary

CHAOSはOSSとして公開中なので自由に改造してほしいです。こんな機能追加したよ！バグ見つけたよ！というのがあればバンバンissueやPull Requestを投げてください！開発者は大変うれしがるので、CHAOSをhackして自分だけのオリジナル組込みOSを作りましょう！

How to hack

1. CHAOSをclone
2. READMEを読んで環境構築
3. QEMUで動作確認
4. Raspberry Piで動作確認
5. Enjoy Hacking !!

CHAOSの最新情報は開発者のTwitterやブログでチェック！



<https://twitter.com/75u2u>



<https://75u2u.github.io>