SecHack365

# 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.

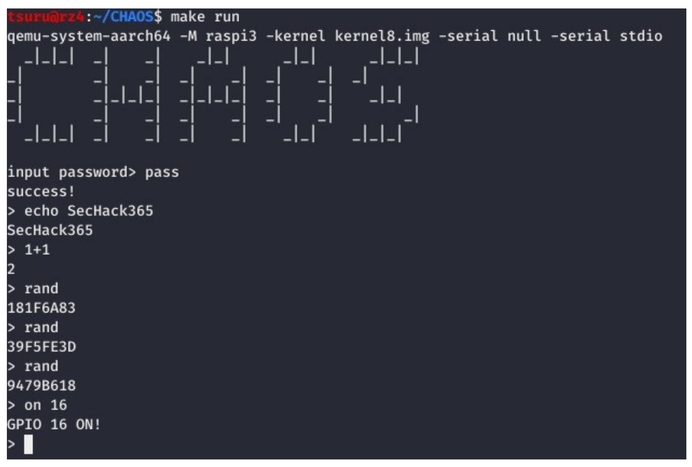
**特徴**

- **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**

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.

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

## CHAOS Shell



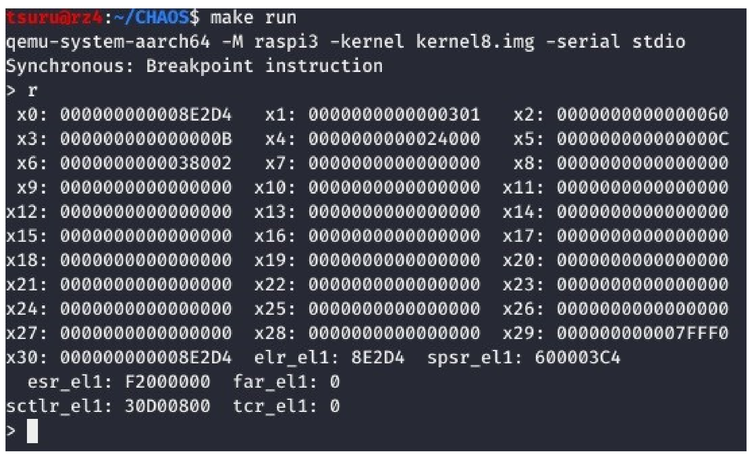

対応コマンド例

- 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




### 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'r'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ります．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

国立研究開発法人 情報通信研究機構