HyprProbe

ソフトウェアのみで実機デバッグを可能にするための
ハイパーバイザ型OSデバッガ

SecHack365
学習駆動コース 坂井ゼミ
番匠 夏希
プロフィール

HyprProbeはデバッグにハイパーバイザを利用することで、
ソフトウェアのみで**より高度**なデバッグを可能にします

バグで変な挙動をしたときにすぐに検知して停止するための機構を複数搭載

ここで止めてデバッグ開始できるように

正常に動作している状態 ➡ バグが発生した状態 ➡ 通常デバッガで見れる いろいろ壊して止まった状態

どこがバグ発生元かの特定が難しい

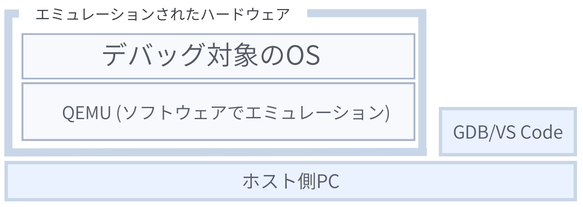
デバッグ対象のRaspberry Pi 4

GDBでのデバッグの様子

HyprProbeと既存手法の比較

ソフトウェア ⟵ ハードウェア

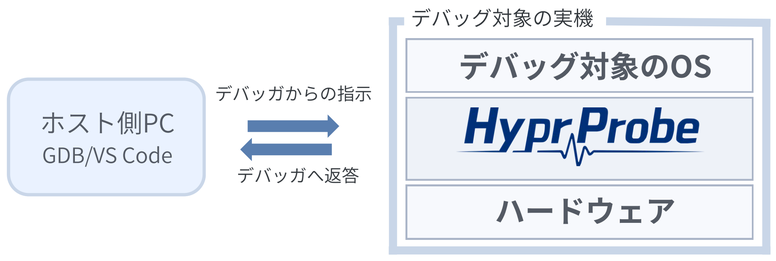
QEMU
ソフトウェアのみで動作



ソフトウェアでのエミュレーションにより、
デバッグ対象のプログラムを実行

実機固有のバグ: **再現不可能**
追加機材: **不必要**
デバッグに掛かるコスト: **低**
壊れる前/瞬間の検知: **手動**

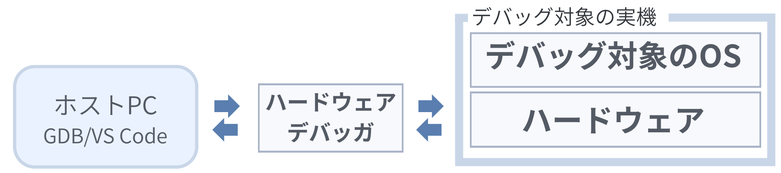
HyprProbe
実機上でソフトウェアで動作



実機内でプログラムを実行して、HyprProbeで監視

実機固有のバグ: **再現可能**
追加機材: **不必要**
デバッグに掛かるコスト: **低**
壊れる前/瞬間の検知: **自動**

JTAG/SWD
ハードウェアデバッガ
実機上で動作



実機で実行して、
その実機に対応するハードウェアデバッガを接続

実機固有のバグ: **再現可能**
追加機材: **必要**
デバッグに掛かるコスト: **高**
壊れる前/瞬間の検知: **手動**

HyprProbeの3つの特徴

1.実機でデバッグが可能

- GDB / VS Codeといった**デバッガに接続**してOSなどのベアメタルプログラムを実行中に止めたり、変数やレジスタの中身を見ることができる
- GDBで利用できる機能の**殆どをサポート**
  - breakpoint/watchpoint/レジスタ、メモリの値の参照
- HyprProbe**専用**のコマンドも複数サポート
  - 例外ハンドラ内では例外元のbacktraceも表示可能
  - 簡単に再起動をかけられる など

2. デバッグを簡単に開始できる

- 導入が**世界一簡単**
  - GitHubからダウンロードして、いつものプログラムの代わりに起動するだけ
  - DTBを解析して**自動でセットアップ**を行ってくれる
  - **ソフトウェアのみ**、追加のハードウェアいらずでデバッグ可能
- デバッグ出力も簡単に
  - semihostingへの対応により、デバッグ出力が簡単

もともとUARTで**67行**必要だったHelloWorldのコードが、**11行**で書けるように!

3.プログラムがバグで壊れる前/瞬間に検知できる

壊れる前

- **スタックオーバーフロー検知**
- **メモリ領域へのアクセスを監視**
  - メモリアクセスが適切かを検証して適切でなければ停止して通知
  - 通常のメモリ領域とUART0のMMIO領域へのアクセス以外はブロックするといったデバイスごとの設定も可能

**バグにより壊れる前に検知して
問題が発生したプログラム部分を表示**

壊れる瞬間

- **例外処理失敗検知**
  - 再帰的に例外が発生した時に停止して表示できる
  - 例外のネストにより壊れたときの情報が取れなくなるのを防げる
- **異常IRQ検知**
  - 割込みの設定ミス(デバイス側未処理のままEOIする)などで割込み頻度が多すぎるときに警告を表示
  - 一定時間割込みが処理されなかった場合、通知する
- **例外理由の可視化**
  - デバッグ対象のプログラムで例外がハンドルされなかった場合に表示する

**バグにより壊れる瞬間に検知して
プログラムが壊れたときの情報を保持して表示**

HyprProbeの現状

現在、QEMU上と**Raspberry Pi 4**上での動作を確認しています。
今後はRaspberry Pi 5やその他AArch64ボードでの動作を確認していきます。

Raspberry Pi 4での動作デモ動画

HyprProbeのデモ

デモではHyprProbeがGDB / VS Code上で動作して、
実際に再帰例外、不正MMIOが発生の検知を行っています。

また、コード、ドキュメントについても
MITライセンスでGitHubに公開しています。

動作デモ動画

Natsu-B/
aarch64_type1_hypervisor

謝辞: この場をお借りして、一年間大変お世話になりましたトレーナー、アシスタント、トレーニーをはじめとしたSecHack365関係者の皆様に心より感謝申し上げます。
ありがとうございました!!!