

Redshift: Manipulating Signal Propagation Delay via Continuous-Wave Lasers +MTG

立命館大学
森 悠仁

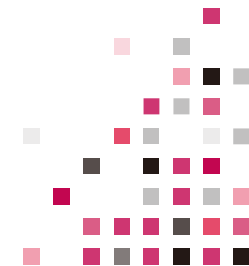
Futurize.

きみの意志が、未来。



前回までの内容

- GPUによるメモリ書き換え監視を用いた高信頼アンチチートシステムの速度改善
- 速度改善を行うためにはボトルネックの計測が必要
- ホスト側からデバイスのボトルネックを計測するにはいくつか障害がある
- 数値の信頼性の検証を行っていた





今回やったこと

- Redshift: Manipulating Signal Propagation Delay via Continuous-Wave Lasers という論文(の2.1まで)を読んだ
- 菅原研の方々とMTGした
- MTG中に出てきた議論の内容を確認した





背景: チップへの物理攻撃


• サイドチャネル攻撃

- コンピュータのシステムの外から物理的な特性を用いて情報窃取する

• フォールトインジェクション攻撃

- コンピュータのシステムの外から物理的な特性を用いてフォールトを仕込む
- フォールト: 何らかの計算時のエラー; メモリ破壊や計算遅延を含む

• レーザフォールトインジェクション攻撃

- 標的チップにレーザ刺激を与えることでフォールトを仕込む攻撃
 - 半導体回路は、光電効果により光エネルギーに対して脆弱(未調査)
 - エネルギーによってチップの一部が励起して確率的にビットが反転する
 - レーザを当てる座標を制御することで、攻撃箇所を絞れる
- 




課題：LFI攻撃の難しさ

● LFIには特殊なレーザを使う

- チップの電位情報はクロックがはねたタイミングのみに更新が行われる
- 1クロックの範囲内でビットフリップに十分なエネルギーを注入する必要
- 十分に短い時間で過不足ないエネルギーを与える必要がある
 - 与えすぎると燃える
 - LFI実行時には冷却装置を外す必要もある

● 課題： 短パルス高エネルギーのレーザは高い

- ある研究では€ 15万 (30M円ぐらい)
 - 後の試算では\$ 5万～15万(7.5M～22M) ぐらい
 - いずれにせよ一般的な攻撃者には用意できない
- 

問題：フォールトの観測の難しさ

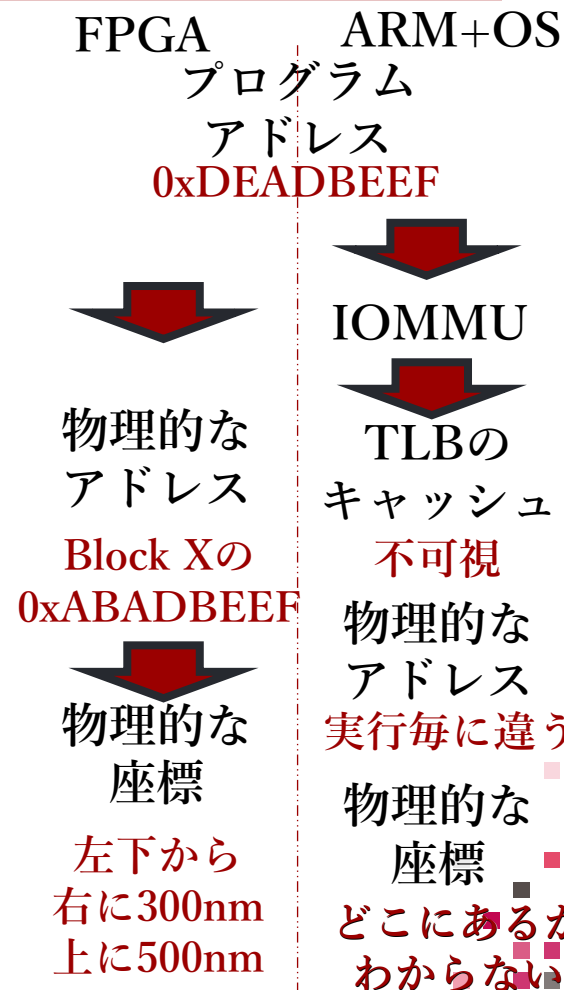
• 市販ボードでのLFI実証

- ソフトウェアが使うアドレスは物理アドレスに対応
- BRAMでは物理アドレスは座標に対応する
- レーザを狙ったアドレスの座標に当てれば特定のアドレス範囲でビットフリップ可能

• ARMでのLFI実証

• Rock5 Model Aというシングルボードコンピュータ

- 同じ場所にレーザを照射してもフリップするアドレスが違う
- 何ビットフリップするかもわからない
- 何がフリップしているか確定していない





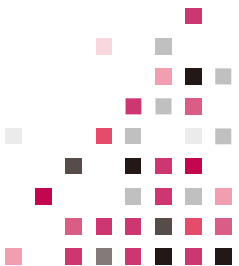
ARMでのLFI実証

- DC CIVAC命令

- Clean and Invalidate data cache by address to Point of Coherency
- キャッシュラインに対してフラッシュを行う
 - CPUのキャッシュ上のデータはライン単位で管理される
- TLB更新後にキャッシュラインを書き戻し、無効化する目的の命令

- Rock5 Model A

- Cortex A76(高性能)なチップとA55(省電力)なチップが積まれている
- それぞれクアッドコアで4つずつ持っている
- 内部では1コアずつ命令キャッシュとデータキャッシュを持つ
- A76とA55は3MBのL3キャッシュを共有している
- 他にもNPU, FPUが積まれているがキャッシュはCPUと共有





ARMでのLFI実証

- レーザ注入後にDC CIVAC命令を実行した
 1. メモリ領域を大きく確保し、全部”a”で埋めた
 2. チップにレーザーを注入した
 3. チップ上の領域にエラーが見られたらDC CIVAC命令を発行した
 - DC CIVAC命令実行後にはフォルトは改めて検出されなかった
 - 使用コアを制限した後にレーザー注入した
 - Tasksetコマンドで使用するコアを制限した
 - 先の実験を再度行った
 - A76にはコアの単独利用をしたときフォルトが検出された
- 