「デジタル回路設計における耐ハードウェアトロイ設計仕様の研究開発」

早稲田大学 理工学術院総合研究所 次席研究員　大屋 優

半導体が脅かされるシナリオ
- soc設計の変化に伴う部品のブラックボックス化 -

悪意のある動作をする機器の作成
- ハードウェアトロイを挿入することで実現 -

半導体の設計段階における重要性
- ハードウェアトロイの設計・挿入が容易 -

設計段階

- デジタル回路やハードウェアの知識があれば設計できる
- ソフトウェアで記述できるため、プログラム上でハードウェアトロイとモジュールやゲートを接続すれば挿入ができてしまう

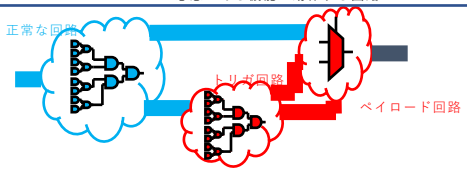
製造段階

- 実チップに対して後付け的に、ハードウェアトロイを接続しなければならず、技術・コストの両面において障壁が高い

ハードウェアトロイの構成
- トリガ回路とペイロード回路 -

トリガ回路：悪意のある機能を動作させる条件を設定する回路

ペイロード回路：不正な値でデータを上書きしたり等、悪意のある機能が動作する回路



ハードウェアトロイの悪影響
- 立場によって求められることが異なる -

今後は悪性・悪用がキーワードとなってくる

IPベンダ：自分の設計にセキュリティホールが存在しないかチェックして、悪用されない様にしたい

SoCベンダ：サードパーティIPに悪性の機能もしくは悪用される機能が存在しないかをチェックしたい

悪性・悪用される機能は分かるのか
- 答えは簡単、現状ではなす術がなくわからない -

直面している問題を真面目に解決するためには、人間の意図を反映させたシステムを作る必要がある

誰かにとっての仕様は誰かにとっての悪性になる

- コードはただのコード、コード自体に悪性も何もない
- 悪性とは、人間が判断（定義）しなければならない問題

DfT(テスト容易化)技術は制御・観測性が共に高い

- 攻撃者から見て極めて悪用し易い回路部分である
- BIST回路等に対して特別な処理をする必要が出てくる可能性

既存技術（Taint Propagation）の検証
- ハードウェアトロイ検出には向いていない -

プロパティ検証ベースのセキュリティ検証技術

ベンチマーク	機能	検出
AES-T800	電力サイドチャネルによる秘密鍵の漏洩	
BasicRSA-T100	秘密鍵の漏洩	✓
BasicRSA-T300	秘密鍵の漏洩	✓
b19-T300	80386プロセッサのアドレス参照を意図しない値にする	
PIC16F84-T300	任意の値(ここでは定数)を Primary Output にする	
wb conmax-T200	レジスタのアドレスを変更する	

本研究で対象とする領域
- 既存技術でカバーできない領域に挑戦する -

3つの検証手法の研究開発に繋がる
1. Port Identification
2. Address Identification
3. Data Identification

ベンチマーク	機能	検出	検証技術
AES-T800	電力サイドチャネルによる秘密鍵の漏洩		Port
BasicRSA-T100	秘密鍵の漏洩	✓	
BasicRSA-T300	秘密鍵の漏洩	✓	
b19-T300	80386プロセッサのアドレス参照を意図しない値にする		Address
PIC16F84-T300	任意の値(ここでは定数)を Primary Output にする		Data
wb conmax-T200	レジスタのアドレスを変更する		Address

Port identification
- 不正な入出力ポートやゲート接続の有無の検証 -

ポートを検証するだけの機能でも、検出できるハードウェアトロイが存在する

想定する設計者の入力する情報：
1. 検証したいモジュールの名前 ポートの名前
2. モジュールレベルでの接続
3. ポートレベルでの接続

Address identification
- 不正なアドレスの参照の有無を検証する -

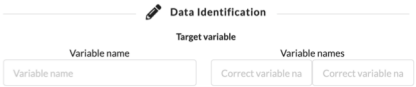
想定する機能の概要
・指定されたレジスタの値の参照や代入に関するコードを全てリストアップする
・その中で参照がズレているコードをwarningとして伝える

想定する設計者の入力する情報：
1. 検証したいレジスタ/メモリの名前
2. MSB
3. LSB
4. データ幅
5. アドレス幅
6. ワード数

Data identification
- 不正な値の書き換えや漏洩の有無を検証する -

想定する機能の概要
・低い確率の状態遷移（閾値はユーザが検出段階のステップで入力）に関するコードをリストアップする
・ユーザが入力した検証したい変数の正しい代入関係が一致しない場合にwarningとして伝える

想定する設計者の入力する情報：
1. 変数名
2. 期待する変数や代入される値



Advanced Information and Communication Technology for Innovation
ACT-i