Monthly Research 2017.3

TrustZone のユースケースと動向

F F R I , Inc.
http://www.ffri.jp

E-Mail: research-feedback[at]ffri.jp
Twitter: @FFRI_Research

目次

- TrustZone 概要
  - TrustZone のユースケース
  - Cortex-A の TrustZone
  - Cortex-M の TrustZone
  - よく知られている TEE 実装
- TEE 実装の脆弱性
  - 詳しい説明
- まとめ
- 参考情報

TrustZone 概要

- ARM TrustZone とは
  - ARM プロセッサが提供するセキュリティ機構
  - メモリを Secure な領域と非 Secure な領域に分割し、
    重要なコード、データを隔離することで機密性、完全性を高める
    - NFC や認証処理などへの適用が想定されている
  - Cortex-A 系と Cortex-M 系で TrustZone の仕組みが異なる

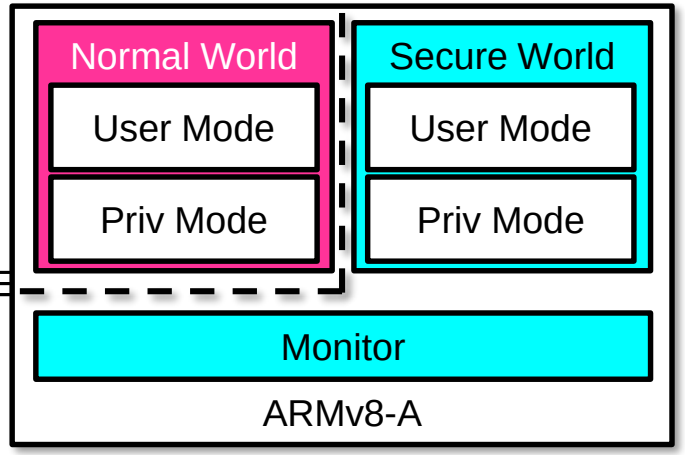
- TEE (Trusted Execution Environment)
  - TrustZone などで実現される Secure な実行環境のこと
  - Trusted Application や Trusted OSなどの設計は標準化されている
  - GlobalPlatform と Trusted Computing Group が標準化
    - GlobalPlatform は Visa などの IC カードの標準化組織

TrustZoneのユースケース

- Android 7.0 では TrustZone 等を使ったキーストアの実装が必須になっている
- ARM はスマートデバイスで TrustZone を活用し資産を保護する例を紹介している
- モバイルペイメント
  - カード情報や取引情報などを Secure な領域に保存
    - デバイス使用者やカード会社は意図しない決済の発生を防ぐ
- コンテンツマネジメント
  - コンテンツに対するユーザーの再生限度やそれをチェックするコード、コンテンツ管理データ等を Secure な領域に保存
    - コンテンツの提供者がコンテンツやサービスをデバイスユーザーによって不正利用されることから保護
- 認証情報の保持
  - 指紋情報など認証に利用する情報を Secure な領域に保存
    - ユーザーは不正なモバイルへのアクセスや認証を阻止できる

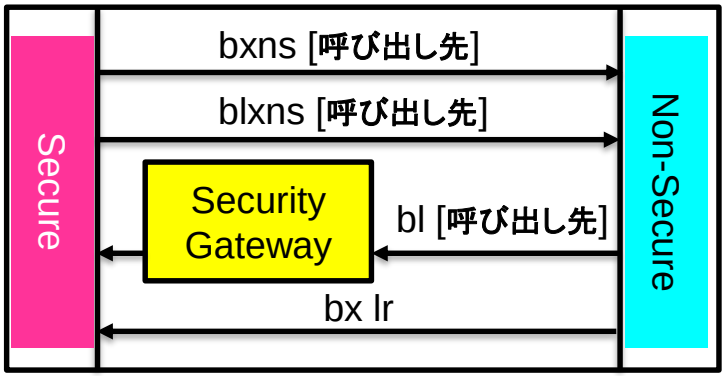
Cortex-A の TrustZone

- Cortex-A
  - モバイルデバイスやネットワーク機器などに利用される
  - アーキテクチャは ARMv7-A 及び ARMv8-A
- TrustZone
  - Secure WorldとNormal World
    - Secure World では Trusted OSが動作
    - モニターモード によって各領域の分離を行う
      - モニターモードに対するエントリは SMC 命令などを利用する
- 詳細は FFRI Monthly Research 2013年3月号に掲載



Cortex-M の TrustZone

- State を使った実装
  - TrustZone の概念はそのままに低電力チップ向けに最適化した方法
  - メモリごとに State が設定され、メモリ空間が分離されている
    - Secure State, Non-Secure State、, Non-Secure Callable Stateの3種
  - IDAU か SAU によってメモリ空間を管理する
- 下記の方法で各Stateを遷移する
- Non-Secure から Secure への遷移
  - BL 命令でセキュリティゲートウェイを経由する
  - BX 命令で Secure の関数へ戻る
- Secure から Non-Secure への遷移
  - BXNS や BLXNS 命令で Non-Secure の関数を呼び出す
- ARMv8-M アーキテクチャから採用
  - 対応しているプロセッサは Cortex-M23/M33
- 詳細は FFRI Monthly Research 2016年2月号で掲載



よく知られている TEE 実装

- それぞれのプロジェクトで Trusted OS やライブラリが提供されている
- Trusty TEE
  - Google が提供している Android 向けの TEE ソフトウェアコンポーネントセット
  - 現段階でサードパーティによる Trusted アプリの追加などは不可能
  - AOSP にソースコードが公開されている
- OP-TEE
  - STMicroelectronics と Linaro Security Working Group が提供している TEE ソリューション
  - GitHub にソースコードが公開されている
  - Cortex-A 系プロセッサを搭載する多数のボードをサポートしている
- ARM mbed
  - ARM が公開している IoT デバイス向けのプラットフォーム
  - ソースコードは mbed の公式サイトに公開されている
  - Cortex-M を搭載したボードで TEE を実現する

TEE 実装に対する脆弱性分析の研究発表

- スマホで利用されている TEE 実装に対する脆弱性分析
  - TrustZone TEEs An Attacker's Perspective (Gal Beniamini氏)
  - Microsoftが主催するセキュリティカンファレンス BlueHat ILでの発表
  - Qualcomm と Trustonic のコンポーネントが対象

- 両方共対策が不十分であり脆弱性があった
  - Secure なメモリを確保する際に ASLR が無効あるいはエントロピー不足
  - Stack cookie によるバッファオーバーフローの検知が無効あるいは実装不備

- 発表者はオープンソース化により多方面からレビューを受けることを提案

- TEE 実装のセキュリティメカニズムが不十分だと TA の脆弱性を攻撃された場合に信頼された実行環境が破綻するリスクがある

TEE 実装の脆弱性の詳細

- Qualcomm TEE 実装
  - ASLR 実装不足
    - 仕様として非 Secure 領域の OS は Secure 領域のユーザー空間(QSEE)に Trusted Application(Trustlet) をロードできる
    - QSEE へのロードは OS(QSEOS) が実施するが、メモリ変換テーブルの仮想メモリアドレスが限定的なので ASLR のエントロピーが弱くなっている
  - バッファオーバーフロー
    - Stack cookie などによりオーバーフローのチェックはしているが、Trustlet の殆どは BSS のバッファを使用し Stack cookie がランダムにならない
    - Trustlet のスタックは BSS の直後に確保されておりガードページがない
  - システムコール
    - QSEOS は QSEE からシステムコールでポインタを受け取るが、アドレスの領域を確認しないので QSEOS のカーネルメモリが破壊される恐れがある
- Trustonic
  - Trusted Application に対し ASLR や Stack cookie などのセキュリティ対策はない

まとめ

- TrustZone は Secure な領域と非 Secure な領域にメモリを分離する
  - Cortex-A 系と Cortex-M 系では実装に違いがある
- TrustZone の活用によって重要な資産を保護
  - ユーザーサイドの資産を保護するだけではなく、コンテンツ配信者がデバイス所有者からコンテンツを保護する用途でも有効
- TrustZone を利用するための TEE 実装は複数存在
  - 代表的なものとして OP-TEE や Trusty TEE など
- TEE 実装の脆弱性
  - ASLR や Stack cookie といったセキュリティ対策が実装不足であった
  - オープンソース化し多方面から実装に対するチェックを受けることが望ましい
  - ASLRやスタック保護が堅実なTEE実装を利用すべきである

参考情報

- ARM Security Technology
  - http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf
- セキュアハードウェアの登場とその分析
  - http://www.ffri.jp/assets/files/monthly_research/MR201303_TrustZone.pdf
- ARMv8-M TrustZone:組み込みデバイス向けアーキテクチャとセキュリティ機能
  - http://www.ffri.jp/assets/files/monthly_research/MR201602_ARMv8-M_TrustZone%EF%BC%9A_A_New_Security_Feature_for_Embedded_Systems_JPN.pdf
- ARMv8アーキテクチャ
  - https://www.arm.com/ja/products/processors/instruction-set-architectures/index.php
- 注目のセキュリティ技術「TrustZone」「TEE」についてARMが解説
  - http://news.mynavi.jp/articles/2013/12/09/arm_tee/
- TrustZone TEEs An Attacker's Perspective
  - https://microsoftrnd.co.il/Press%20Kit/BlueHat%20IL%20Decks/GalBeniamini.pdf
- Trusty TEE | Android Open Source Project
  - https://source.android.com/security/trusty/
- mbed OS | mbed
  - https://www.mbed.com/en/platform/mbed-os/
- OP-TEE
  - https://www.op-tee.org/
- ARM® コンパイラバージョン 6.3ソフトウェア開発ガイド
  - http://infocenter.arm.com/help/topic/com.arm.doc.dui0773dj/DUI0773DJ_software_development_guide.pdf