HRoTおよびTEEを用いた外部検証可能な組み込みシステム

An Embedded System Architecture Supporting Attestation Based on a Hardware Root of Trust and TEE

加藤寛章・マネジメント分科会・情報セキュリティ大学院大学

The rapid proliferation of IoT devices has introduced significant cybersecurity challenges, particularly due to the inherent constraints of embedded systems, such as limited computational resources, exposure to physical attacks, and deployment in remote environments. To mitigate these risks, we propose an attestation-capable embedded system leveraging Trusted Execution Environments (TEEs) and a hardware root of trust to verify the integrity of embedded devices. The system is designed to be implemented using Arm TrustZone for Cortex-M and the open-source secure element TROPIC01. This poster presents the system architecture and outlines the proposed implementation approach.

背景と目的

IoT機器の特徴

■性能に制約がある
　一般的なPCなどに用いられている機能が使えない
■管理が難しい
　一度配置されたら、アクセスしづらい場合もある
■コスト制約
　一部の製品を除き、安価で販売されるため開発コストをかけづらい

脅威

■物理的なアクセスが容易
　攻撃者の手にデバイスが渡りやすい
　内部を分解されてしまう可能性
■アップデートされない場合がある
　管理の難しさにより、適切なアップデートがされないまま運用されてしまう可能性がある。
■意図しない動作
　攻撃者によるソフトウェア改変により、意図しない動作が発生する可能性がある。

現状

■STマイクロエレクトロニクス社MCUのセキュリティ機能
　・STM32L5シリーズよりCortex-M33アーキテクチャの導入による組み込み機器向けTEE(TrustZone)への対応
　・STM32U5シリーズより、デバイス固有鍵の導入
　・STM32H5シリーズ一部製品では物理攻撃への耐性を持つソフトウェア(Secure Manager)の製造時の導入
■スマホ等には耐タンパーハードウェアとしてSecure Elementの活用
■ArmによるPSA CertifiedなどIoT機器向けセキュリティ認証

研究内容

現状の課題

■Cortex-Mベースの機器においてセキュリティを意識した実装は限定的(Tan et al., 2024)
　・例）TrustZoneによる隔離をしていない
　・例）特権モードを利用していない
　・例）Memory Protection Unitを活用していない
■耐タンパーハードウェアとしてのSecure Elementの利用しづらさ
　・ベンダーとNDA契約を結ばないとハードウェア詳細情報が入手できない
　・SDKを利用するための情報が限定的
■組み込み機器を外部から検証する仕組み(Remote Attestation)が普及していない
　・TrustZoneを利用したRemote Attestationの実装やAttestationの枠組み自体は存在しているがあまり普及していない
　・Remote Attestationに用いられる鍵管理をハードウェアレベルで実装かつTEEを活用した公開実装はない

実装

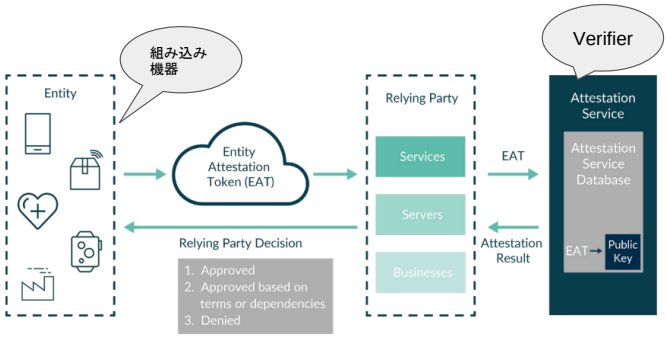
■組み込み機器向けTEE
　・評価ボードNUCLEO-L552ZEQ(Cortex-M33)を用いたTrustZoneを利用したソフトウェア実装を確認
　・Secure WorldとNon-secure Worldの使い分け
　　○分岐命令によるNon-secure WorldからSecure Worldへの遷移
　　○Non-secure Worldに対するSecure Worldからの割り込み
■SecureElement：TROPIC01
　・TROPIC SQUARE社によるオープンソースSecure Element
　　○ハードウェア詳細についてHDLレベルで公開
　　○書込み済みファームウェアも公開
　　○SDKおよびAPI仕様書についても公開
　・評価ボードNUCLEO-F439ZIを用いて動作を確認
　　○乱数生成
　　○ECC鍵生成

今後の計画

■組み込み機器側でAttestationに用の署名済みEntity Attestation Token
　・IETFによるAttestationの規格
　・Secure Elementを用いた署名
　・ハードウェアに信頼の起点
■Attestation関連処理をTEE内部での実装
　・Entity Attestation TokenをTrustZoneにおけるSecure Worldで生成
■VERAISONを用いたAttestation検証サービスの実装
　・Attestation検証サービスの実装であるVERAISONをサーバーに実装
　・Cortex-Mベース組込み機器のみならず、Cortex-Aベースの機器を含む幅広い機器のAttestationを目指す
　・IoTシステム全体としてのセキュリティ

VERAISON

上記画像引用：https://github.com/veraison/.github/blob/main/veraison-logo.png



上記画像引用：https://www.psacertified.org/app/uploads/2020/02/PSA-Certified-Entity-Attestation-Overview-Whitepaper.pdf