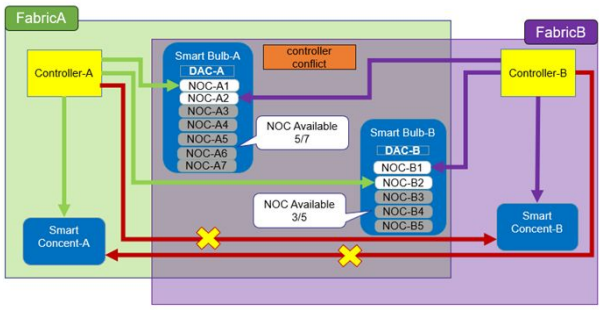
スマートホーム向け規格Matterの競合についてのセキュリティ問題

Security Issues Arising from Controller Conflicts in the Matter Smart Home Standard

須田光・ネットワーク分科会・情報セキュリティ大学院大学

The smart home standard Matter is a communication standard designed to enable devices from different manufacturers to be connected through a common specification. While Matter allows multiple users and services to control the same device, it may also introduce potential risks related to permission separation and state consistency. This study aims to clarify how conflicts among multiple Controllers acting as control entities in Matter affect access control and the identification of management entities, and conducts experimental verification to this end. The results show that, although the specification requires explicit user consent when removing pairing information, this consent process is omitted in actual implementations, allowing a third-party Controller to revoke the control privileges of another Controller. In addition, the accumulation, sharing, and unintended persistence of pairing information between devices and Controllers make it difficult for users to accurately understand management entities and the scope of impact. Furthermore, in environments where Matter coexists with legacy smart home protocols, state inconsistencies were also observed. Based on these findings, this study demonstrates through empirical observations on real devices that, in multi-Admin environments, the interaction of specifications, implementations, and operational practices can lead to unintended privilege revocation and state inconsistencies.

背景



スマートホーム向け規格Matterは、デバイスやベンダー間の相互運用性を特徴としており、一つのデバイスを複数のControllerで競合して操作させることができるMulti-Admin環境に対応している。

研究目的

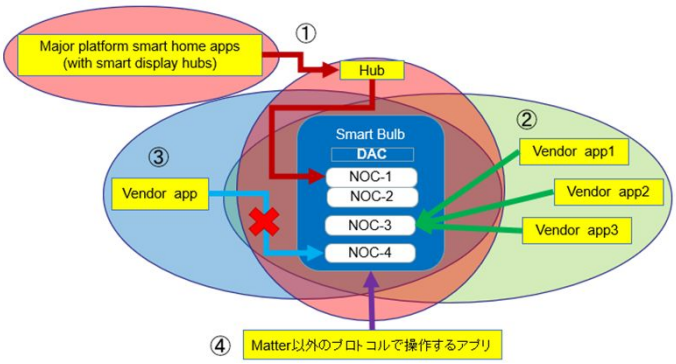
「Matter」におけるMulti-Admin環境での競合が起こすセキュリティおよび運用の整合性に与える影響を実機で検証し、その要因と課題を整理すること。
①Matterにおけるアクセス制御は、複数のControllerが同一デバイスを操作する場合にも適切に機能しているか？
②Matterにおいて、デバイスの証明書管理や上限管理などの挙動は、ユーザーに正しく可視化・理解可能な形で提供されているか？

検証結果

①CommissioningしたControllerはFabric情報を取得でき、明示的なユーザ同意があれば削除（RemoveFabric）できると仕様書で定義されている。
→実環境では明示的同意なく第三者が登録したFabric情報を削除できることを実機で確認
→仮想デバイスによる検証で、削除時の詳細ログを取得することで、実際にRemoveFabricが行われていることを確認

②複数Controllerによる競合操作時、Controllerの操作とデバイス内部の NOC（Node Operational Certificate）管理状態が一致しない挙動を複数確認。

- 利用者の認識以上にNOCが消費・保存される挙動
- NOCの共有により、デバイスを操作できるControllerの把握が困難になる挙動
- コミッショニング失敗時における意図していないNOCの保存
- Matter/非Matter操作併存時に状態が不整合となる挙動



今後の展望

- 本研究で明らかになった問題の内部実装要因の切り分け
- 検証対象とするデバイスカテゴリの拡張（ロック/センサー等、影響が重大な機器）
- Matter／非Matter混在環境における制御方式の整理