ISS-A-026

Broker における盗聴を防ぐ MQTT エッジプロキシの機能拡張

遊亀　嘉生†　　藤野　貴之††
† 近畿大学大学院　システム工学研究科　　†† 近畿大学　工学部

1. はじめに

IoT(Internet of Things)とはデバイスがインターネット上での通信を可能とする概念である. IoT 環境の通信方式としては MQTT が広く使用されている. MQTT では, TLS によって通信路を保護しても, 中間者である Broker からは情報が読めてしまう問題がある. 本稿はこの問題に対処することを目標とする.

2. MQTT 及び MQTT エッジプロキシ

2.1 MQTT とセキュリティの問題

MQTT（MQ Telemetry Transport）とはパブリッシュ/サブスクライブ型の仕組みを使用する軽量なメッセージングプロトコルである. MQTT では, Broker は Publisher から発行されたメッセージのトピックとペイロードを読むことができるため, Broker がセキュリティ侵害されることによってメッセージの改ざんや, 情報の盗聴, 漏洩が起こる可能性がある.

2.2 MQTT エッジプロキシ

MQTT エッジプロキシは, Publisher には手を加えず, Publisher から発行されたメッセージに透過的に TLS を付加するものである[1]. MQTT エッジプロキシを用いることで, クライアント, サーバ間の盗聴を防ぐことができる. しかし, 依然として Broker は情報を読むことができる.

3. MQTLS

Broker のセキュリティ問題を扱った先行研究として, MQTLS がある[2]. MQTLS はクライアント, サーバの間で使用される MQTT 対応プロトコルである. MQTLS プロトコルは client-to-Broker-to-client（CBC）セキュリティセマンティクスに基づいている. MQTLS プロトコルでは, CBC セキュリティセマンティクスを実装するため, ペイロード暗号鍵, ペイロードシーケンス番号, トピック暗号鍵, ワンタイム配送鍵を規定, 使用する.

MQTLS の問題点は以下のとおりである.

①Publisher, Broker, Subscriber 全てを MQTLS プロトコルに対応させなければならないため, 既に Publisher が展開されてしまった後に導入することは困難である.

②リソースの制約がある Publisher に多数の暗号処理を要求する. 具体的に, Publisher は従来の TLS 通信路確立（トピック暗号鍵確立）の処理に加えて, 証明書を使用した Subscriber の認証をしたり, Subscriber の数だけワンタイム配送鍵を生成したりしなければならない.

③Publisher は一般に複数存在するため, 一旦確立したペイロード暗号鍵を更新するためには, 全 Publisher 間で新しいペイロード暗号鍵を共有する仕組みが必要である. MQTLS にその機能はないため, ペイロード暗号鍵が仮に漏洩したとしても更新することはできない.

4. 提案手法

CBC セキュリティセマンティクスの要件は, Publisher と Subscriber の間でペイロード暗号鍵を安全に共有すること, ペイロードシーケンス番号を付与することで悪意あるメッセージ挿入やメッセージ削除を検知することである. MQTLS は, 2 つの要件を TLS のメッセージを拡張することで実現している. これに対し本研究では, MQTT エッジプロキシが存在することを前提に, MQTT のアプリケーションとしてこの 2 つの要件を実現することを提案する. これは MQTLS の問題点①②を解決するものである. Publisher を除く MQTT エッジプロキシ, 全 Subscriber が参加する専用のトピックチャネルを用意する（本稿では"control"とする）. 使用する Broker は MQTT データを配送する Broker と同じでも異なってもよい. ペイロード暗号鍵の情報漏洩のリスクを低減するため, Subscriber はペイロード暗号鍵を送信してほしい専用のトピック（本稿では"abc123"とする）を Publisher にトピック"control"で通知する. トピック"abc123"でやりとりされるメッセージは, 全て通信相手の公開鍵で暗号化されるものとする. エッジプロキシ, Broker, Subscriber は一般に十分なリソースを保持するため, 暗号処理は負担にならない. ペイロードシーケンス番号は, メッセージフォーマットの一部として提供することを提案する.

5. まとめ

本研究では, Broker による盗聴を防ぐために, MQTLS が提案した CBC セキュリティセマンティクスを MQTT エッジプロキシの機能を拡張して実現することを提案した. 現時点では, 通信相手の公開鍵による暗号化及び, クライアント間において, 共通鍵によるメッセージの暗号化と復号化が可能であることを確認している. 今後の課題として, まず提案手法を完全に実装し, 動作を検証する必要がある.

参考文献

[1] 遊亀嘉生, 藤野貴之, “IoT メッセージングの通信路保全を可能とする MQTT エッジプロキシの実装と評価” 2020 年度(第 71 回)電気・情報関連学会中国支部連合大会, rentai200173 2020 年 10 月 24 日

[2] Hyunwoo Lee, Junghwan Lim, Ted “Taekyoung” Kwon, “MQTLS: Toward Secure MQTT Communication with an Untrusted Broker,” International Conference on Information and Communication Technology Convergence (ICTC), 2019.