

IoT における TPM の処理のスケジューリング

本澤 翔矢[†] 吉浦 紀晃[†]埼玉大学理工学研究科[†]

1. はじめに

IoT(Internet of Things) は、相互に接続されたモノのネットワークである。ネットワークに接続する以上、セキュリティは重要であり、攻撃者が IoT デバイスに侵入してデータを改ざんしたり、デバイスのシステム構成を変更したりする危険性が常にある。この問題に対処するため、TPM(Trusted Platform Module) はサーバやパーソナルコンピュータなどの汎用コンピュータで広く使用されており、コンピュータシステムの改ざんを防止するハードウェアベースのセキュリティとして機能し、上位アプリケーションには暗号サービスを提供している。

TPM は、専用のトラステッドコンピューティング技術とは異なり、TPM とコンピュータシステムとの結合度が低いため、汎用コンピュータだけでなく、組み込みシステムなど、様々なコンピューティングシステムに広く利用できる。Di Lu ら[1]が提案した TPM 拡張スキーム(xTSeH)により、TPM 搭載機器から未搭載機器へ TPM 機能が拡張され、機器間の認証における時間的な評価がされた。しかし、TPM へのリクエストが大量に送られた際、通常より実行時間が掛かり、IoT 機器のリアルタイム性が損なわれる可能性がある指摘されている。本研究では、IoT 機器のリアルタイム性を損なわないために、TPM へのリクエストに優先順位を付け、本方法をシミュレーションし、評価をする。

2. TPM(Trusted Platform Module)

TPM は、TCG(Trusted Computing Group)[2]によって提唱されたマイクロチップであり、コンピュータプラットフォームの整合性を検証するために使用される。主な機能として、非対称鍵の生成、データの暗号化/復号化、署名、TPM 間での鍵の移行などの暗号処理に加え、乱数生成やハッシュ処理などがあり、暗号鍵のような少量のデータを安全に保管する機能も備えている。TPM の目的は、ハードウェアベースのセキュリティをプラットフォームに提供することであり、

これはソフトウェアベースのものと比較して、改ざんされにくいと考えられている。

3. 関連研究

Di Lu ら[1]は TPM 拡張スキームである xTSeH(図 1)を提案している。IoT を活用した eHealth システムにおいて、スマートセンサーである SED(Smart Embedded Devices)のデータ改ざんを防ぐために TPM が採用されている。しかし、各 SED に TPM を搭載するにはシステムリソースが限られているため、ネットワークを介して、TPM の機能を搭載した SED から未搭載のものに拡張する TPM 拡張スキームである xTSeH を提案している。xTSeH は図 1 において、TPM のある SED (TSED) から TPM のない SED (N-TSED) に TPM を拡張している。TSED と N-TSED の間の通信は Proxy-V と Proxy-P と名付けられたプロキシがネットワークを介して行う。SdwTPM は N-TSED のシステム構成情報(OS のバージョンなど)を収集するもので、整合性検証を行う際はシステム構成情報を Proxy-P を介して TSED に送信する。TPM は TPM 内のデータと SdwTPM 内のデータとの間の整合性検証を行い、N-TSED が改ざんされていないかどうかを確認している。そして、これらの手法の時間的な評価を行っている。

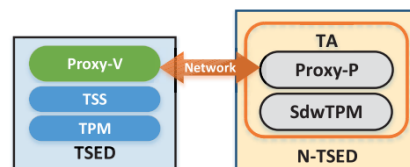


図 1: xTSeH の概要[1]

本研究では[1]で定義された以下の 3 つのプロトコルに対して優先度を付ける。

- TBP(Trusted Booting Protocol)
N-TSED 起動時に実行され、SdwTPM からシステム構成情報を TSED に送信し、TPM で整合性検証を行う。
- NAP(Node Authentication Protocol)
2 つの N-TSED の通信時に実行され、通信開始前に 2 つの N-TSED の整合性検証を行い、通信するための共有鍵・秘密鍵を作成する。
- RVP(Remote Verification Protocol)
N-TSED が一定時間通信を行わない時に実行され、N-TSED の整合性検証を行う。また、

Scheduling of TPM processes in IoT
Shoya Honzawa[†], Noriaki Yoshiura[†]
Graduate School of Science and Engineering, Saitama University[†]

NAP で N-TSED それぞれに対して整合性検証を行う時にも利用される。

4. 実験内容

本研究では 3 つのプロトコルと IoT 機器に優先度を付け、シミュレーションを行う。プロトコルの優先度は次のように定める。起動時に実行する TBP は高く NAP を実行すると RVP を実行する必要がないことから、 $TBP > NAP > RVP$ とする。IoT 機器は利用者が任意に定められるものとし、利用者が決定するものとする。TPM での処理（以下では TPM タスク）に対する優先度の付与方法として以下の 3 つを考えた。IoT 機器の数は 2 個以上として①～③をプリエンプティブなしとありでそれぞれシミュレーションを行う。

- ① 各プロトコルの優先度だけを付ける。
- ② TBP と RVP は（プロトコルの優先度） + （IoT 機器の優先度）を付ける。NAP は（プロトコルの優先度） + （通信する 2 つの IoT 機器の内の高い方の優先度）を付ける。ただし、TBP の TPM タスクが NAP と RVP よりも優先度が高くなるようにする。
- ③ TBP と RVP は②と同じ付与方法である。NAP は（プロトコルの優先度） + （通信する 2 つの IoT 機器の優先度の合計）を付ける。ただし、TBP の TPM タスクが NAP と RVP よりも優先度が高くなるようにする。

シミュレーションでは、1ms ごとに複数の IoT 機器と 1 つの TPM の状態を変化させていく。このとき、TPM タスクは TPM を占有し、実行時間は [1] の実験結果より 596ms とする。処理待ちの TPM タスクはキューに保存する。時間的な評価は TPM タスクの待ち時間とし図 2、3 のように計測する。TBP と RVP は TPM タスクが enqueue() されてから実行完了するまでの時間を計測する。NAP は通信する 2 つの IoT 機器の TPM タスクが enqueue() されてから 2 つとも実行完了するまでの時間を計測する。

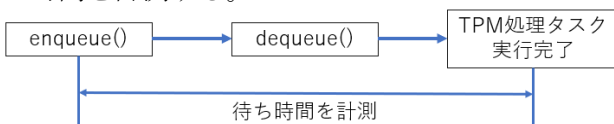


図 2: TBP と RVP の時間計測

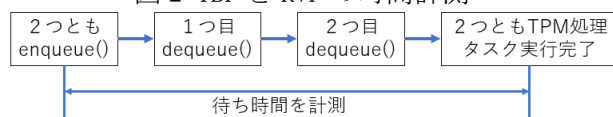


図 3: NAP の時間計測

5. 実験結果

プリエンプティブなしの結果を説明する。①～③の場合も同じ結果であり、TBP は処理される

順番に約 600ms、約 1200ms と約 600ms ずつ増加する。NAP は約 1200ms 掛かり、IoT 機器が増加すると最初の NAP は IoT 機器が 3 個以上で 1800ms、2400ms と増加していく。RVP は IoT 機器が 1 分以上通信を行わなければ実行されないため、計測できなかった。プリエンプティブなしは IoT 機器の増加で待ち時間が増加する。

プリエンプティブありは、TBP と RVP はプリエンプティブなしと待ち時間は変わらなかったが、プリエンプティブありのため、TBP は優先度の高い IoT 機器から順に処理された。NAP も約 1200ms 掛かるのは同じであったが、③の場合、高い優先度と低い優先度のペアと、その間の優先度のペアにおいて、TPM タスクの優先度が中間の優先度 2 つのペアの方が高くなることもある。このとき高い優先度の TPM 処理が割り込みされ後回しになるため約 2400ms の待ち時間となる。

6. 考察

本研究では優先度の付け方をシミュレーションし評価しているが、ほとんどの場合 TPM タスク実行完了までの待ち時間に差はない。しかし、③の場合において、高優先度の IoT 機器が低優先度の IoT 機器と通信している際に中間の優先度の 2 つの IoT 機器に割り込みされるとリアルタイム性に影響が出てしまう可能性がある。そのため、高優先度の IoT 機器を最優先に処理する必要がある場合は②の優先度の付け方が妥当であると考えられる。

7. おわりに

本研究では、IoT 機器のセキュリティをハードウェアベースで行う TPM のタスクに優先度を付けシミュレーションを行った。1 つの TPM が対応できる IoT 機器の数や優先度の付け方が妥当かを評価している。しかし、1 つの TPM しか考慮しておらず、複数個の TPM があつた場合には TPM 処理タスクの待ち時間は減少するであろう。また、実際の IoT 機器に当てはめた場合の検証は今後の課題となる。

参考文献

- [1] D. Lu et al., xTSeH: A Trusted Platform Module Sharing Scheme Towards Smart IoT-eHealth Devices, IEEE Journal on Selected Areas in Communications, vol. 39, no. 2, pp. 370-383, Feb. 2021.
- [2] TCG Specification Architecture Overview, T.C.Group, TCG Specification Revision 1, 2007, pp. 1-24.