L-006

Media IoT 向け軽量セキュリティフレームワーク
Light weight security framework for Media Internet of Things

金子 格[1]
Itaru Kaneko

1. はじめに

インターネット上に接続される通信機能を持ったセンサーなどの機器はしだいに数を増やしている．今後，そのサイズが減少するとともに，爆発的に数を増すと予想されている．これまでよりも格段に多くの「物」にセンサーとインターネット接続機能が登載された状態は，物のインターネット，Internet of Things とも呼ばれている．

ここで最も多くのトラフィックを占めると考えられるのが映像情報である．そして映像の多くは，そのままあらゆる場所に伝送されるのではなく，特定の方法で処理をされた上で送信されると考えられる．なぜならば，人間社会においてあらゆる空間や物の映像を送信することはプライバシーに対する大きな脅威となるからである．

映像とその処理装置，処理結果の送信装置などは，人間が固定的に接続するのではなく，用途に応じて動的に構築されるようになる，と予想される．

このようにアドホックな接続が，センサー，処理装置，送信器，その先の受信装置にたいし接続された場合に，はたしてそのようなネットワークに適したセキュリティフレームワークがあるだろうか．本報告では，どのような機能をそのようなネットワークが持つべきであるかを考察する．また新しいフレームワークであるため，今後どのようにその有効性を検討するか，についても考察する．

2. 想定される Media IoT のフレームワーク

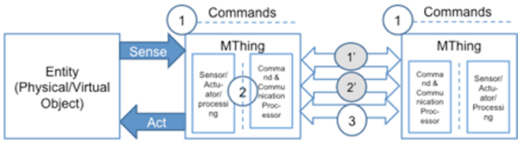

図 1 MPEG IoMTW のオブジェクト, MThing

図 1 に ISO/IEC JTC 1/SC 29/WG 11 で標準化を進めようとしている IoMTW のオブジェクトである MThing を示す．MThing はネットワーク上のオブジェクトであり分散メディア環境の構成要素として検討されている．ネットワーク上のこうした MThing が多数連携して IoMTW が構築される．

本稿では多数の MThing からなるネットワーク構造の相互認証についての要求条件について検討する．

3. MThing の用途

MThing は現状人間が装着する，いわゆるウエアラブルデバイスを想定している．そのようなデバイスは衣服や様々な携帯品に付属する．現在でも様々な携帯品電子機器がワイヤレスネットワークで連携している．たとえば bluetooth 機器は一旦ペアリングすれば，あとは装着するだけでネットワーク接続が行われる．筆者は将来このような携帯ではネットワーク機器がさらに多数利用され，自由に着脱でき，それが MThing で想定すべき利用状況であると考える．

4. MThing の要求条件

MThing のセキュリティに関する要求条件について検討する．

4.1 多数の MThing の認証

まず多数の MThing の認証フレームワークが必要ではないかと考えられる．MThing は衣料，装飾品，携帯品に組み込まれ，それらと同時に日常的に頻繁に着脱が行われると想定される．現在でも Brue Tooth 機器はそうした着脱に応じたネットワークの認証と接続の機構がある．BrueTooth 機器ではまずペアリングを行う必要がある．一旦ペアリング済の機器は装着しただけで認証とネットワークの接続が行われ音声映像などが伝送可能となる．

しかし MThing がさらに広く装着可能な無数の映像機器を接続するために利用するとすると，これでは不十分である．たとえば帽子，靴，時計などは BrueTooth 機器よりもはるかに多くを毎日交換して利用する．このような機器をすべてペアリングするのは現実的ではない．ある程度機器を信用して，自動的に接続を可能とする方法が提供されるべきである．

4.2 セキュリティの強化

一方多数の MThing を機能させるから，これらのセキュリティはこれまで以上に厳重に守られる必要がある．特に中継を行う MThing からの情報漏洩はぜったいに不可能であるような機構が必要である．

その場合，ペアリングはあまり有用なメカニズムではない．仮に信頼のおける中継機器のみをペアリングし，信頼できない機器はペアリングしなければペアリングをセキュリティの強化に利用することになる．しかし，仮にそのようなメカニズムがありペアリングの可否を機器に確認されても，通常の利用者にとってペアリングが安全かどうか判断する能力がないことがほとんである．したがって，利用者がペアリングの可不可を選択できることは，あまりセキュリティ上は役立たない．それに代わる安全性を確保するセキュリティ機構が必要であると考える．

4.3 鍵配布，SPIM 配布

動的，継続的なセキュリティ水準の維持のためには，セキュリティ鍵とセキュリティ処理実装するモジュール(SPIM)は配布更新が可能であるべきだろう．

[1] 東京工芸大学 工学部コンピュータ応用学科

一方で鍵配布においては，鍵配布，SPIM 配布経路におけるセキュリティが問題になる．鍵インフラにおいて暗号化復号化の実装と鍵配布経路におけるセキュリティ不良によるセキュリティ侵害は防げない(暗号化，復号モジュール自体のセキュリティに問題があれば情報は漏洩する)から，これらのセキュリティをどう認証するか，という問題が生じる．

そこで，鍵配布，SPIM 配布において配布された鍵や SPIM が信頼できることを確認可能とするような，何等かの軽量な仕組みが必要になるものと考えられる．

この仕組みは，柔軟性がない MThings の自由な接続を制約するものであってはいけないし，一方で悪意ある実装者が攻撃用の鍵や SPIM を，正規のものと偽装して配布することは完全に防げなければならない．

4.4 オフライン動作

鍵および SPIM の認証についての一つのアイデアはオンラインで鍵や SPIM の信頼性を検証することである．MThings の利用形態を見ると常にオンライン状態を仮定することは望ましくない．海中深く，あるいは地球をはるか遠く離れていても，鍵や SPIM の信頼性の認証が可能でなければならないと考える．

一方で，そのように無認証で接続を行うことは，プライバシーの保護においてリスクとなりえる．したがって接続する機器が，一定の規範をまもった信頼できるものであることを，簡単に確認できることが望ましい．

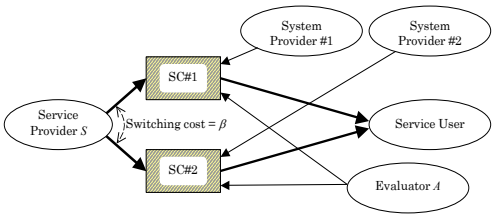

図 2 MLSM

5. Blockchain と MLSM

このような柔軟，軽量，かつ強固なセキュリティを実現する一つの可能性として，Blockchain と MLSM の利用が考えられる．MLSM は筆者がフレキシブル，軽量かつ，安全性の高いセキュリティフレームワークとして提唱しているモデルである．MLSM の構造を図 2 に示す．MLSM は SPIM(図では SC)の交換が可能であり，かつ自動的は Evaluater が組み込まれていることが特徴である．Evaluator とは SC を評価するが問題があればすぐに新しい SC と交換する．この時，SC の交換コストをゼロと設定しておけば，Evaluater は交換費用の悪影響なく SC の問題を評価可能になるという点が MLSM の特徴である．

しかし実際には SC の交換コストはゼロであっても開発コストはゼロではない．そこで不良 SC が eject された後，追加の SC をどう補給するか．そのコストはだれがどうやって負担すべきか．という課題があった．

ここに Blockchain を利用することが考えられる．Blockchain 方式により Evaluatgor，SC の提供者の相互の匿名性を保ちつつ，特定の SC のセキュリティが失われた場合にそのコストが Evaluatoer に決してかからないよう，相互に決裁を可能とすれば，MLSM の安全性を維持しながら，複数の SC を提供し続けなければならないという問題点を解消できると考える．

6. 評価手法

最後に，このようなセキュリティフレームワークの評価方法について，何をどのように評価すべきかを考えてみたい．この機構は個々の SPIM には内部攻撃の可能性もあり，セキュリティに問題がある場合がありえるという前程に立って運用される．したがって，セキュリティ上評価すべきなのは，そのような事象がどの程度の確率で発見されるか．また，問題のある SPIM がどの程度拡散することができるか(拡散できない方がよい)という点を評価すべきだろうと考える．

その他にも，シミュレーションによって評価すべき数値があると思われる．今後シミュレーションを実施する際の課題であると考える．

7. まとめ

MPEG で議論が進んでいる MIoThings への要求条件について考察した．またそれらの要求条件を満たす手法の一つとして，Blockchain と MLSM からなるセキュリティフレームワークを提唱した．セキュリティの頑健さと SC の交換がうまく機能するかの確認は今後シミュレーションなどで確認していきたい．

参考文献

[1] Kaneko ITARU, “Probabilistic multilateral security model for ubiquitous multimedia services”, Proceedings. 24th International Conference on Distributed Computing Systems Workshops (2004).
[2] MPEG, “Use cases for Internet of Media-Things and Wearables”, http://mpeg.chiariglione.org/standards/exploration/internet-media-things-and-wearables (2016).