April 2015

自動車の情報をセキュリティー脅威から守る

TPM(Trusted Platform Module)を使い自動車 ECU の セキュアなファームウェアのリモート更新をデモンストレーション

TPM (Trusted Platform Module)をハードウェア信頼基点として使い、自動車の中の ECU で用いられているファームウェアのセキュアなリモート更新のデモンストレーションをします。当デモは、最近公開された TCG TPM 2.0 Automotive Thin Profile(以下 URL)の重要なコンセプトを紹介します。
http://www.trustedcomputinggroup.org/resources/tcg_tpm_20_library_profile_for_automotivethin

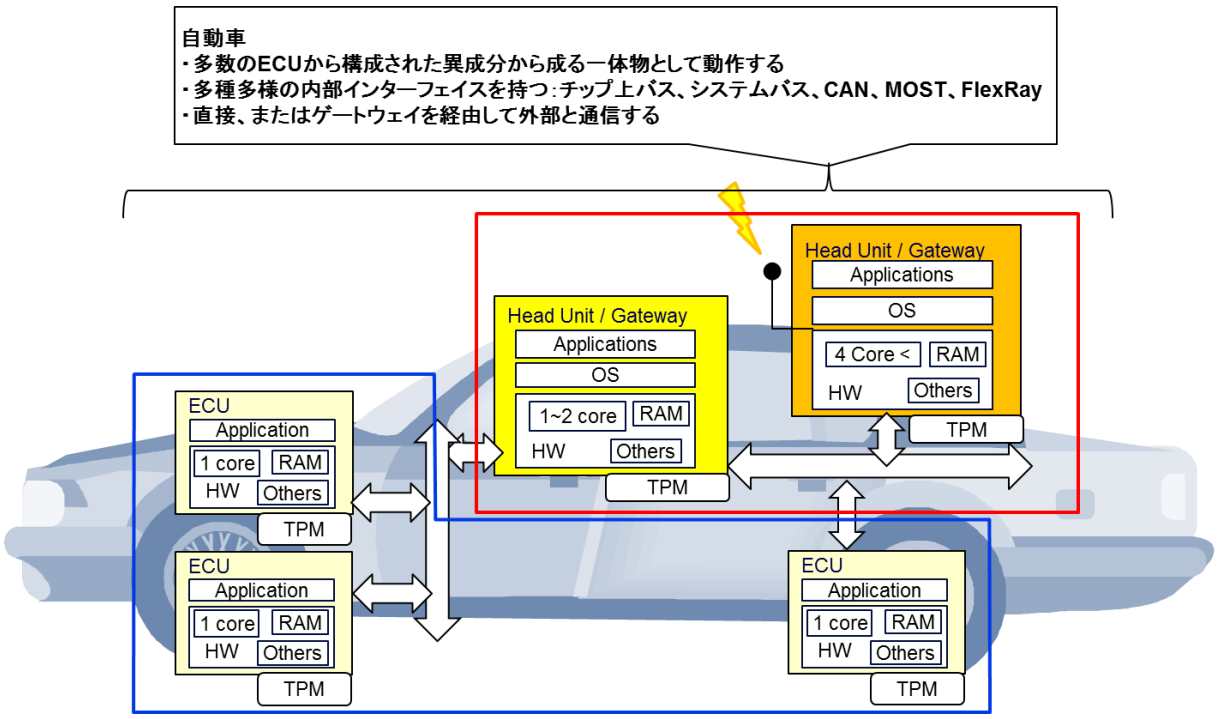
セキュアなリモート更新は、次の 3 つのステップを使って実施されます。

1. その時点での自動車ソフトウェアとハードウェア内の構成、状態を遠隔で正確に把握する。（TPM に基づく測定、測定値の TPM 自身、および第三者による検証可能性保証、TNC プロトコルを用いての通信）

2. 意図されたソフトウェア更新が完了したことを検証し、証拠保存する。（TPM に基づく測定、測定値の TPM 自身、および第三者による検証可能性保証、TNC プロトコルを用いての通信）

3. 更新動作と TPM 測定動作の(TPM によって生成された)監査ログを長期間セキュアに収納する。TNC プロトコルを用いた転送、ネットワークアクセスが可能な自己暗号化記憶装置や他の高信頼性の収納等を行う。

以下の図は、各部品（ヘッドユニット/ゲートウェイまたは ECU）のリモート更新における情報の流れの概念を示しています。

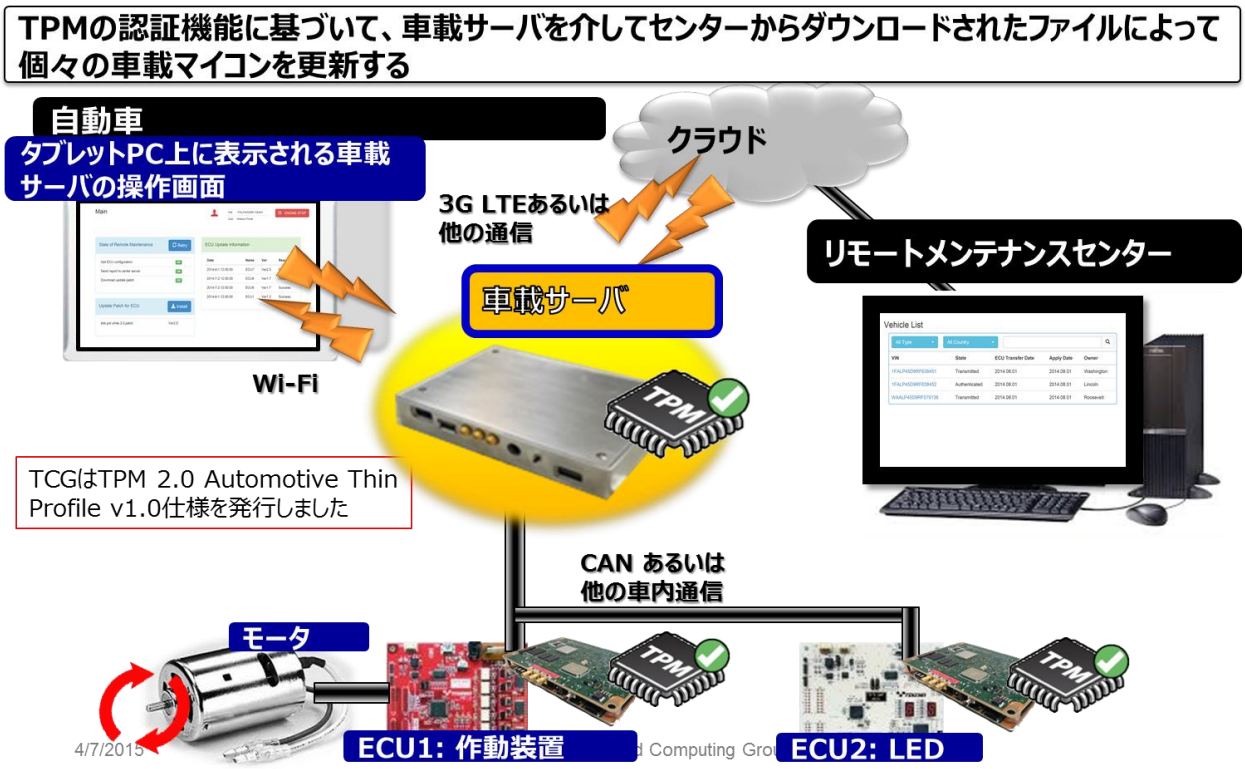


April 2015

デモシステムは以下 3 点を含み構成されています。

- リモートサービスセンターを模したノートパソコン
- ファームウェアのリモート更新が必要な自動車を模した自動車模型
- 接続用の各種通信モジュール

デモシステムの略図（以下）：デモの流れは、上記 3 つのステップから構成されます。



詳細については、以下 URL をご覧ください。

http://www.trustedcomputinggroup.org/resources/tcg_tpm_20_library_profile_for_automotivethin