車載エレクトロニクスへのサイバー攻撃を解析するためのログ機能の提案

Proposal of Log Functions for Analyzing Cyber-Attacks on In-Vehicle Electronics

五十嵐貴久・マネジメント分科会・情報セキュリティ大学院大学

Abstract - As modern cars are all controlled by ECUs, they also attract Cyber-Attacks. Cyber-Attacks are also expected to diversify. When a car accident occurs, it is necessary to distinguish whether the cause is Cyber-Attacks, human error, or system error. If it was due to Cyber-Attacks, the need for in-vehicle logging function will increase more and more.
In this paper, we propose Multi-Layered Log Integrity Technology(MLLIT for short) in order to protect in-vehicle data from attackers. In the threat analysis, the integrity was higher when the data was stored hierarchically.

研究の背景

DEFCONにて自動車へのサイバー攻撃手法を発表され、その脅威は現実味を帯びてきた。攻撃への対策として、車載ログ機能は不可欠な機能である。

現状の車載ログの問題点

- サイバー攻撃を対象とした統合的なログ取得機能について、標準化した技術はないこと。
- 車載機器が生成したデータは、保全していない若しくは、個々に保全しており、統合管理する仕組みがないこと。
- ログを改ざん・消失から保護する仕組みが不十分であること。

本研究の目的は、攻撃の流れを裏付け、サイバー攻撃を判別し、解析するために記録するべきデータ・記録場所の条件を明らかにし、プライバシー保護も合わせて検討した多層型ログ保全技術を提案すること。

多層型ログ保全技術

（Multi-Layered Log Integrity Technology 、 MLLIT）

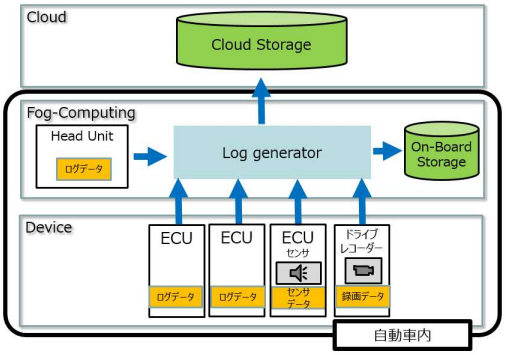
車載ログ・データを車載機器それぞれに、残しておくと攻撃者による改ざんや交通事故・盗難による滅失の脅威がある。車載ログ・データをセキュアに保全するためエンドポイントのログ・データを自動車内でリアルタイムに収集し、ダイナミックにOn-board storageとCloudに分けて保全する構成を考え三層構造とする。

(1)データ量・保全場所の特性・プライバシーを考慮し、ログ・データの保全場所を分類する。

(2)「信頼の基点」を設定

改ざんされている疑念を排除するため、ログ・データのHash値を別に保管する。

	On-board	Cloud
保存リアルタイム性	あり	劣る
捜査機関のデータ回収容易性	インターフェース次第 令状の必要可能性もあり	サーバが国内でも令状可能性大 海外サーバは、ICPO経由
通信料	なし	あり
外部ネットワーク転送容量制限	–	あり
データ欠落（外部ネットワーク通信時）	–	回線不備により大幅に欠落する可能性がある
データ欠落（転送時の仕様依存）	生成元に近いほど、RAWデータ	転送項目の仕様依存
情報漏洩（Privacy保護）	物理的な侵入や盗難の虞	可能性あり



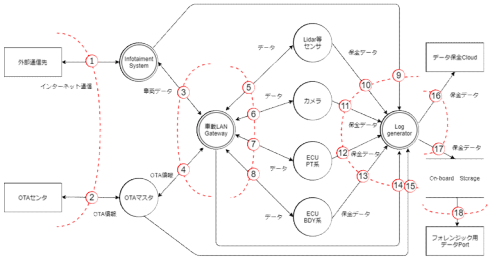
(3)ログ・データ取得の優先度レベル分け

	取得ログ・データ項目	事業用自動車（バス、トラック等）	自家用自動車	
			ハイエンドモデル	ローエンドモデル
発生原因切り分けレベル	攻撃の入口(外部との接続口) 攻撃の出口(直接的な指令データ)	○	○	○
攻撃経路・攻撃手法解析レベル	攻撃の入口と攻撃の出口を結ぶ経路において生成されるログ・データ	○	○	△
先進機能実データ保全レベル	実データ（カメラ・センサー）	○	△	△

高

評価

MLLITをモデル化したDFDから得たエントリーポイントに対してSTRIDEによる脅威分析を実施し、多層構造は、完全性を高める結果を得た。



まとめ

(1)サイバー攻撃を検出するため、必要である。
(2)攻撃経路・攻撃手法を明らかにする
(3)多層構造は完全性を高める
(4)「信頼の基点」の設定
(5)プライバシーに関する情報の保存場所はユーザーに選択権を持たせる。