自動車技術会　サイバーセキュリティ講座　企画提案書

1. 講座名	Practical ECU hacking (UDS Security Access)
2. 講座概要	本オンライン講座は、ハンズオン形式で「UDS Security Access暗号アルゴリズム解析」を行う。 具体的には「暗号処理の実行時間測定とソースコード解析、Keyを推測、Security Access成功まで」を体験する。 これにより、攻撃者の視点、思考や攻撃の仕組みを理解し、ECUのセキュリティ確保に役立てて頂くことを目的とする。
3. 想定する受講者	自動車業界のエンジニアで実践的なセキュリティ技術を学びたいと考えている方
4. 習得する技術	暗号アルゴリズム解析手法
5. 受講の前提条件	・簡単な英会話スキル （本講座は弊社講師が英語で行います/日本人スタッフもサポートします） ・情報セキュリティ及びUDS Security Accessの基礎的な用語を理解している ・講師の指示に従ってPythonでコードを書ける ・C++のコードを読める（ソースコードを解析して頂くため）
6. 日数（時間数）	半日（3時間）
7. 最大受講人数	5人
8. セミナー講師	Tien Phan (WHITE MOTION)
9. 受講者の制限	無し
10. 実習機材	Zoomを使用できるPC（Zoom経由で演習用PCにリモートアクセスして頂きます）
11. 到達目標	演習で行う一連の攻撃プロセスを理解する
12. 講座計画	UDS Security Accessの暗号アルゴリズム解析 ①Side channel（1時間） - Pythonでエクスプロイトコードを作成し、PC内に仮想的に構築したECUに対して、Security Accessコマンドを送信 - 暗号処理の実行時間からKeyを推測し、Security Access成功までを体験する ②Weak algorism（1時間） ③Strong algorism（1時間） - 講座用に準備したソースコードより、暗号アルゴリズムを解析 - Pythonでエクスプロイトコードを作成し、Security Access成功までを体験する
13. 開催時期	2023年1月13日（金）