自動車テクノロジーで使用される wolfSSL の製品

自動車メーカーが製品に搭載するカーエレクトロニクスは、年々パワーアップし多岐にわたっています。
コネクテッドカーがまだ成熟した技術、機能ではない現在、ハッキングや攻撃の可能性を常に考慮しておく必要があります。

コネクテッドデバイスがもたらすセキュリティリスクと中間者攻撃と戦うためには、フットプリントが小さく高品質でセキュリティ機能に妥協のないSSL/TLSと暗号ライブラリが必須コンポーネントといえるでしょう。

wolfSSL 組み込み SSL / TLS ライブラリ

- TLS 1.3とDTLS 1.2までをサポート
- ROMサイズ: **20-100kB**
- RAMサイズ: **1〜36kB /セッション**
- OpenSSLより最大で1/20まで小型化
- 多くのプラットフォームをサポート

wolfCrypt 暗号化ライブラリ

- wolfSSLに包含される暗号化エンジン
- 対象アルゴリズム:
  - Hash Functions
    - SHA-1, SHA-2(SHA-224/256/384/512), SHA-3, (MD2, MD4, MD5, RIPEMD, BLAKE2b)
  - Block Ciphers
    - AES, (DES, 3DES, Camellia, IDEA)
  - Stream Ciphers
    - ChaCha20, (ARC4, RABBIT, HC-128)
  - Authenticated Ciphers
    - AES-GCM, AES-CCM, Poly1305
  - Public Key Options
    - RSA, DH, EDH, ECC(NIST, Curve25519/448)
  - Public Key Signature
    - RSA, DSA, ECDSA, Ed25519/488
  - Password-based Key Derivation
    - HMAC, PBKDF, PBKDF2
- Hardware Crypto Support
  - PSA, CAAM, DSP Crypto, その他
- FIPS (Federal Information Processing Standards)
  -米国連邦システム内の機密または貴重なデータを保護するための必須基準
  - wolfCrypt v4 FIPS 140-2 Level 1 Certificate #3389
  - wolfCrypt FIPS 140-3 (検証中(2022年3月現在)

wolfSentry

製品組込み向けネットワーク侵入検知、防御

- Firewall：トラフィックのフィルタリング
- IDS：トラフィックを監視し、異常検知を通知
- IDPS：バススパムをブロックする動的対応
- コールバックによるドライバーやメーカーへのアラート通知

wolfMQTT

- **サイズ: 3.6kB**
- MQTT v5.0仕様に準拠
- TCP, TLS, MQTT-SNをサポート
- メッセージの整合性確保、暗号化が可能（wolfSSLライブラリ経由）

wolfSSH

- 安全なシェル、ファイル転送 (SSH, SFTP, SCP)
- SSH v2.0 サーバーに対応
- wolfCrypt暗号化ライブラリ(FIPS)を利用
- 商用有償サポート

wolfTPM

- 仕様に準拠したすべてのTPM 2.0 APIを提供
- SPI上の通信にTPM Interface Specification (TIS)を使用
- 鍵生成、RSA暗号化・復号化、ECC署名・検証、ECDHのラッパーを包含

wolfBoot

- **安全なファームウェア更新**
- **OS非依存、優れた移植性**
- フラッシュデバイスのマルチスロットパーティショニング
- ファームウェアイメージの整合性検証
- wolfCryptのデジタル署名アルゴリズム（DSA）を使用したファームウェアイメージの信頼性検証

cURL

安全なデータ転送

HIPAA、PCI DSS、EUのGDPRなどのデータセキュリティ規制に準拠し、ユーザー、拠点、パートナー間で重要なビジネス情報を安全に転送可能

- 商用サポートを提供
- 最適化およびコンサルティングを提供
- HTTPS用に100k以内 (32bit)のtinycurlライブラリ

自動車での wolfSSL 製品ユースケース

高い処理能力のV2Xデータ検証

- DSPでハードウェアの性能を最大限に引き出す
  - 暗号化アルゴリズムをDSPへオフロードする
- V2X環境における大容量データストリームの検証の難しさ
  - V2X環境での高いスループット-毎秒4,000件以上の検証

使用したwolfSSL製品:

- wolfCrypt、署名認証で使用
  - 検証を実行するコアを指定し、大量の検証要求を処理するためのDispatcher、カスタムビルドライブラリ
  - ARMコアに加えDSP上でも動作する暗号プリミティブ
  - 既存のBranpoolとNISTの実装に加え、中国市場向けにSM2公開鍵のサポートを実装

セキュアファームウェアアップデート

- 新しいファームウェアアップデートの取得および認証
- wolfSSL + cURLによるバックエンドサーバーへの電話接続
- i.MXデバイスのCAAMによるセキュリティ強化
- CAAMドライバがQNX上のハードウェア暗号化およびセキュア キー ストアの両方をサポート

使用したwolfSSL製品:

- cURL
- wolfSSL
  - キーストレージ検索のためCAAMドライバと統合
- wolfCrypt
  - CAAM

車とバックエンドの接続にTLS1.3

- MQTT、LibcURLを使用
  - HTTPプロキシにcURLを使用
- バックエンドと通信するための複雑なネットワークトポロジー - インフォテインメントとバックエンドの接続

使用したwolfSSL製品:

- wolfSSL
- wolfMQTT
- cURL

Autosar用NTP (Network Time Protocol)

- Ecosystem Time Sync
  - 例　ブレーキはマシンビジョンシステムと時間軸が同じ
  - 車内での定数時間の維持
  - Sub Millisec Time Sync
  - 暗号化されたセキュアリファレンスタイム
- 重要かつシンプルな機能
- なぜクルマにNTPが必要なのか？
  - スマートカーアプリにおけるサブシステムの同期

wolfSSLのテストおよびコードの品質

- 実機、マルチボードでのベンチマークテスト
  - コードサイズと起動時間の関係を常に注意
  - メモリリソースの測定
  - 定期的に手動で実行し、数値を更新
- アムステルダムで実際のSTM32F407をターゲットに機能テストを実施
  - フォワードアップデート、ロールバックをカバー
  - SPIフラッシュテスト
  - TPMテスト(InfineonのTPMモジュールを使用)
  - 組み合わせ可能なDSA+SHAアルゴリズムによるテスト