Empowering Tomorrow's Automotive Software
www.etas.com

組み込みシステムの脆弱性を識別 ESCRYPT セキュリティテストサービス

ハッカーの動向を理解

データのセキュリティを保つことは、今日の企業における最優先事項の 1 つです。しかし、残念ながら新しい脆弱性が日々発見され、そのすべてを常に把握することはほぼ不可能です。このため、経験豊富なセキュリティの専門家による組み込みシステムのテストが不可欠になります。ESCRYPT のプロフェッショナルたちが、時間面、コスト面、評価面に被害を与えうるセキュリティ上の弱点を詳しく調べて発見します。このプロ集団の目標は、セキュリティ上の脆弱性の発見と、その修正の包括的なサポートであり、いくつかのテスト方法を用いて、現実世界の攻撃者の戦略的、専門的な行為をシミュレートします。

有効なテスト方法

コードレビュー

状況によっては、コードレビューが、主なセキュリティコントロールを検証できる唯一の効率的な手段となる場合があります。たとえばアクセス制御、暗号化、データ保護、ログ記録、バックエンドシステムの通信や使用などです。

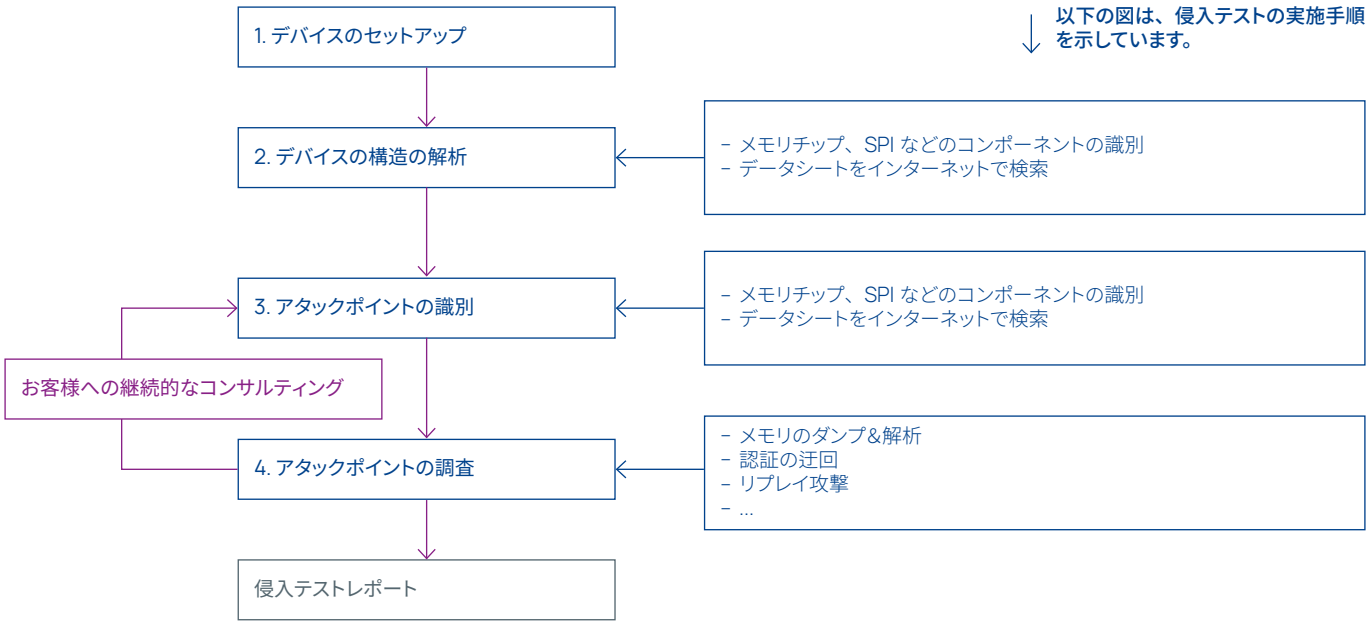
侵入テスト

侵入テストは、既知の攻撃理論や新たに識別された脆弱性を実際の攻撃に当てはめて、現実的な攻撃目標の実現や、他のセキュリティテストでは通常発見されない物理的な弱点の識別を行います。侵入テストには次のモジュールを含めることができます。

- 脆弱性スキャン
- 体系的なファジング
- エクスプロイトテスト
- リバースエンジニアリング
- 実装攻撃

機能テスト

セキュリティ機能テストでは、実装済みのセキュリティ機能の性能、正確さ、堅牢さを検証できます（暗号化アルゴリズム、セキュリティプロトコルなど）。



ETAS の主なサービス

- 組み込みシステムの重大なセキュリティ上の脅威が安全面、金銭面、または広報面の実際の損害へとつながる前に脅威を識別
- 組み込みシステムへの侵入がいかに困難または簡単かを現実的なコンセプトの証明に対する攻撃を用いてのデモンストレーション
- 組み込みシステムに含まれている保護を確認し、システムが（今も）セキュリティ攻撃を防御できるかをチェック
- 各攻撃の結果を詳細に示すドキュメント作成
- 経験豊富なテストチームが発見した各結果の正確な判断とリスク評価
- CVSS に基づくリスク評価
- 合理的なセキュリティを実現するために、識別されたセキュリティリスクを許容レベルに抑えた保護メカニズムの詳細提案

テストパッケージ

ETAS は、組み込みシステムの特別な要件に応じた個々のテストパッケージを提供しています。そのすべてのテスト方法とテストモジュールを組み合わせることが可能で、テスト範囲も適切に調整できます。組み込みデバイス用の標準的な侵入テストパッケージは、脆弱性スキャン、ファジング、エクスプロイトで構成されています。必要に応じてリバースエンジニアリングなどへ拡張することも可能です。あるいは、侵入テストを、重要なコード部分のコードレビューや機能テストと一緒に行うこともできます。

また、製品に関して潜在的なセキュリティリスクや起こりうる攻撃がある場合にその概要を迅速に示し、コスト効率のよい、結果志向のテスト手法を実現するために必要となる追加調査をご提案します。

ESCRYPT セキュリティテストサービスのアドバンテージ

- 組織の評判や信頼を危険にさらすハッカーからの攻撃を防止
- コスト効率のよいリスク管理の実現
- システムのダウンタイムによるコストの回避
- 規制要件の遵守と罰金の回避
- 企業イメージの向上と顧客ロイヤルティの維持

ETAS の製品とソリューションに関するお問い合わせ：
info@etas.com

製品の詳細情報：
www.etas.com/security-testing

ETAS/COM-JP/03-2023