自動車 IT システムのセキュリティを総合的、体系的で経済効率性の高いものに

今日の自動車 IT システムは、かつてないほど緊密にネットワーク化されているため、これを不正操作から保護し、道路利用者すべての安全を確保する必要があります。このために、使用可能なリソースをできるだけ有効に利用する、総合的で体系的なアプローチが求められています。そのようなアプローチの 1 つである、総合的なセキュリティ概念には、セキュリティレベルおよびセキュリティプロファイルにより定義される安全区分が採用されています。

Looking at the Big Picture

大局を見据えて

執筆者

Martin Emele 博士：
ETAS
セキュリティ製品
事業部長

Benjamin Glas 博士：
ETAS
暗号学および
セキュア通信の専門家

Marko Wolf 氏：
ESCRYPT 社
エンジニアリング
事業部長

Thomas Wollinger 博士：
ESCRYPT 社
マネージング
ディレクター

自動車や家電製品、あるいは近年発展してきている IoT（モノのインターネット）など、どの分野の組込みセキュリティにもたくさんの難問が待ち受けています。かつては自己完結型だったモジュールがシステム全体に、さらにはシステム外のインターネットにまで開放されるようになり、攻撃ベクターやウィークポイント、および単純なエラー原因の数の急増を招いています。製品を信頼できる形で確実に機能させるということは、もはや単なる機能安全の問題というだけではなく IT セキュリティの問題の 1 つでもあります。製品を正しく機能させられるかどうかはすべて安全性次第ではありますが、セキュリティは完全性や知的所有権の保護に、さらにはユーザーの個人情報の保護にもますます深く関係するようになってきました。

一番弱い部分が最初に壊れます

セキュリティ違反が発生した場合、それが悪意のある攻撃者によるものであろうと技術上の不具合によるものであろうと、システム全体のセキュリティに関して責任を問われるのはシステム内の最も弱い部分になります。自動車分野では、広く分散している開発プロセスおよび価値創造チェーンについて考えるときにこのことを頭に入れておくことが特に重要です。安全区分の標準化により、セキュリティ用の開発リソースを早期に経済面を重視しながら実用的な形で確実に利用できるようにする、総合的体系的な枠組みができました。この安全区分は、「何を保護しなければならないのか？」、そして「どの程度の保護が必要なのか？」という 2 つの質問に対する答えを知るのに役立ちます。

セキュリティの目的は価値を守ることです。しかし、価値が異なれば、保護が必要になる側面も異なります。最も重要な側面は、可用性とともに機密性、完全性、および信憑性です。これらの各側面の保護に対する重み付けは、システムやサブシステムにより異なります。この重み付けの情報がセキュリティプロファイルに書き込まれます。多くの場合、セキュリティプロファイルはドメインレベルにおけるあるクラスのシステムの特徴を表すものであり、「何を保護しなければならないのか？」という質問に対する答えをセキュリティの側面別尺度によるベクターという形で示しています。

それぞれにどの程度の保護が必要でしょうか

必要な保護のレベルは、脅威の危険性を評価することにより決められます。セキュリティターゲットに反する事柄が原因で起こると予想される結果や出費について考慮する必要があります。たとえば、エンジンのセンサーが機能しなくなってしまうよりも、ブレーキが故障してしまう方が重大です。もう 1 つ考慮しなければならないのは、セキュリティ違反が発生する可能性です。

ここでは、能力、リソース、予備知識、攻撃の期限、および攻撃者の意欲などの要因を考慮する必要があります。つまり、「何を？」および「どの程度？」に対する答えによってセキュリティレベルが設定され、そのセキュリティレベルによって、必要な保護の強さの度合い（なし～非常に高い）が定量化されます。

一方、セキュリティプロファイルでは、絶えず更新し推奨される保護手段の中から、セキュリティ方策を意図的に選択することができます。ドメインごとに異なるプロファイル要件を反映して、セキュリティ概念の枠組みを構成する方策のパッケージを定義することが可能です。これにより、標準化されて実績もある手段を正しく採用し、適切に設定できるようになると同時に、継続的な改良プロセスを、システムや会社の境界を越えて確実に実施できるようになります。

他の領域からのアプローチ

他の領域ではすでに多くのアプローチが採用されて評価されているので、今後アクションを起こすための基礎としてそれらを役立てることができます。たとえば、評価および保証のサブエリアを、国際的に認識されているきめ細かい枠組みとして共通基準（CC）にすることができます。ドイツの連邦政府情報技術セキュリティ庁（BSI）が素案を作成した IT ベースラ

リスク分析により、製品およびシステムにセキュリティプロファイルおよびセキュリティレベルが割り当てられます。セキュリティ方策および開発プロセスはこの区分に基づいて導き出されます。

インプロテクションは、最新のテクノロジーを使用してセキュリティ方策の識別および IT システムへの実装を行うためのシンプルなルールで構成されています。一方、自動化技術の領域では、IEC 62443 規格が製品および IT システムのセキュリティレベルに関連しています。

最後に、自動車分野については、目的や必要性に応じた包括的な一連のルールが各種の安全性レベル（ASIL：Automotive Safety Integrity Level）およびプロセス仕様とともに ISO 26262 に規定されています。しかし、自動車セキュリティ分野に直接適合していて自動車のライフサイクル全体に適用可能な手順はまだ登場していません。

業界全体に導入してメリットを最大に

セキュリティの安全区分を社内で採用すると、開発コストを削減し、セキュリティレベルの定義を全製品にわたって統一させることができます。しかし、この考え方を最大限に生かすためには、業界全体で安全区分を採用し、標準規格に基づいて運用していく必要があります。ISO、AUTOSAR、または SAE などの組織は、体系化されたセキュリティ概念の実装を目的とする国際的に認められた機関です。ETAS および ESCRYPT は、開発段階だけでなく量産工程の段階についても、脅威やリスクの分析からセキュリティレベルの定義や適切なテスト・分析メソッドの選択に至るすべての領域でメーカーおよびベンダーの皆様のお役に立つことができます。これにより、経済効率性の高い方法でリソースを使用して、1 つ 1 つのセキュリティ目標をしっかりと達成できるようになります。

セキュリティレベル別の段階的方策の例