応用研究

W03 無線・通信

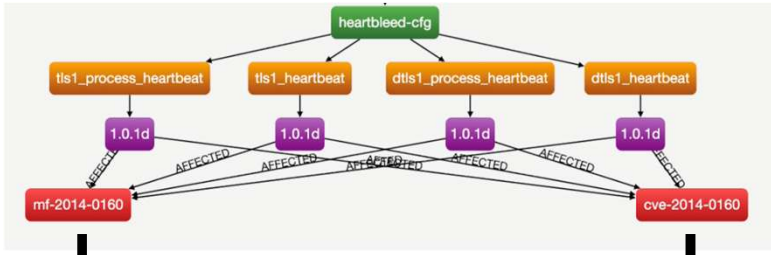
ファームウェア・ソフトウェアの機能検証によるセキュリティ向上技術

概要

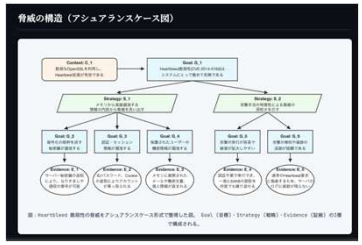
社会インフラの高機能化に伴い、ファームウェアやソフトウェアの脆弱性を狙うサイバー攻撃が深刻化しています。従来の対策では使われていない機能まで要対処と報告され、対応コストの増大やアラート疲労を招く課題がありました。本研究開発では機能レベルで構成情報を自動解析し、セキュリティ対策が必要な箇所を特定できるようにします。

特徴

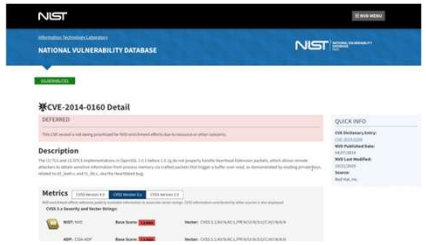
- サイバー攻撃に対しソフトウェアの脆弱性を正確に把握することが重要です。従来手法ではライブラリ単位でしか構成を把握できず、起動しないソフトウェアも検査対象に含まれるため、大量の警告が発生していました。
- ライブラリ単位より細かい機能レベルの構成情報の作成や、起動時に実際に動くプログラムの追跡などにより、優先的にセキュリティ対策を行うべき脆弱性を絞り込む取り組みを進めています。
- 解析結果と脆弱性の関係をグラフとして可視化し、外部の脆弱性情報や要対処の根拠をつけた検証レポートと連携させることで、効率的な検証・管理を実現しました。



機能レベルの依存関係



検証レポート



外部情報

今後の展開

- 解析の自動化をさらに発展させることで、継続的なセキュリティ検証の実現を目指します。また、より多くの種類のソフトウェアやファームウェアへの適用を進め、汎用性を高めていきます。

テーマ「京都府と共に創るいのちの未来」との関連

- 安心・安全を支えるサイバーフィジカルシステムにセキュリティ確保は不可欠です。本技術は、ファームウェア・ソフトウェアのセキュリティ向上をさせ、誰もが安全に暮らせる信頼性の高い持続可能な社会の実現に貢献します。

連絡先：波動ネットワーク研究所 担当 小津 喬 Email:wnl-contact@atr.jp

本研究は、JST経済安全保障重要技術育成プログラムJPMJKP24K1の支援により実施したものです。