静的解析技術を用いたIoTシステム検証の効率化

An Improvement of IoT Systems Verification using Static Code Analyzer

ものづくり支援センター　堀　　武司
産 業 シ ス テ ム 部　本間　稔規

■研究の背景

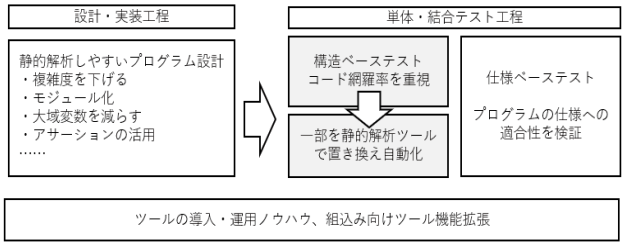
社会へのIoTシステムの普及に伴い、それらを支えるソフトウェアのセキュリティ品質確保が一層重要となっています。通信ソフトウェアにおけるセキュリティ脆弱性の多くは、不正なメモリ操作などの単純な欠陥が原因であり、これらの欠陥を効率的に除去しセキュリティ脆弱性を未然防止する技術が求められています。近年、ソースコードを自動解析し不正メモリ操作等の欠陥を検出する静的解析技術が注目されていますが、高価な商用製品が多く、中小企業での活用は困難です。そこで、無償利用可能なオープンソースの解析ツールの活用によって、IoTシステムのセキュリティ脆弱性の検証作業の効率化を実現するための取組みを行いました。

■研究の要点

１．オープンソースもしくは無償で利用可能な静的解析ツールの調査及び性能評価
２．IoTシステム向けの特殊なソフトウェア環境に対応するための、解析ツールの機能拡張
３．静的解析技術を活用した、IoT向けソフトウェアテスト作業の効率化手法の検討

モジュール	問題の種別						
	整数桁溢れ	バッファ溢れ	Null参照	事前条件	無効代入	その他	計
net	1	1	−	1	1	4	8
netdev	2	0	−	0	−	0	2
netinet	5	1	−	3	−	5	14
netinet6	9	1	−	9	−	19	38
tcp	14	−	1	3	4	6	28
計	31	3	1	16	5	34	90

infer ツールによるTINET解析結果



提案するテスト効率化手法の概要

■研究の成果

１．無償利用可能なオープンソース静的解析ツールの候補を調査し、infer、clangの２ツールを中心にセキュリティ脆弱性に対する解析能力の評価を行いました。
２．オープンソース組込みTCP/IPソフトウェアTINET（TOPPERSプロジェクト）のソースコードに対して両ツールを適用したところ、欠陥検出はそれぞれ90件（infer）、７件（clang）となり、inferがより多くの欠陥を検出することができました。一方、TINETの既知脆弱性27件のうちinferで直接検出できたのは４件（約15%）であり、inferツールによる解析のみでは検出できない脆弱性が多数存在することが明らかとなりました。
３．inferツールの解析能力を強化するため、組込み向けOSであるμITRONのサービスコールの不正呼び出し等の欠陥検出を可能とする機能を追加しました。
４．既存の欠陥検出テスト工程の一部をinterなどの静的解析ツールで置き換えることで工数削減を図る効率化手法を構築し、ガイド文書等を作成しました。これらの成果は、IoTシステム検証に関する企業支援で活用する予定です。