平成29年度 情報工学コース卒業研究報告要旨

高田・本田 研究室	氏　　名	伊 藤　弘 将
卒業研究題目	汎用ファジングツールを活用した 組込みTCP/IPスタックの脆弱性検出	

近年，IoT機器の数が爆発的に増加しており，身の回りのあらゆるものがインターネットに繋がる時代が到来しつつある．これに伴い，従来はインターネットに接続された汎用システムをターゲットとしてきた攻撃者が，組込みシステムを新たな攻撃対象とする危険性も高まっている．組込みシステムは，その性質・用途から，汎用システム以上に高い安全性が求められる．そのため，今後は組込みシステムにおいてもセキュリティ対策を行うことが重要である．

高いソフトウェアセキュリティを実現するためには，十分なソフトウェアの解析･テストが不可欠である．しかし，今後ますます複雑化する組込みソフトウェアに対し，人手のみで十分な解析･テストを行うことは困難になると予想されるため，自動化の需要が高まっている．自動化が可能なテストの1つとして，ファジングがある．ファジングは，ソフトウェアの不具合を発見するためのテスト手法の1つである．対象のソフトウェアに大量のデータを入力し，それに対する応答や挙動を監視することで不具合を検出する．また，ファジングを自動で行うツールをファジングツールと呼ぶ．ファジングに関する研究は，主に汎用システムの分野で，海外を中心として盛んに行われており，現在ではその有効性が認められ，組込みシステムの分野においても注目されている．

汎用システムにおいて最も洗練されたファジングツールの1つに，American Fuzzy Lop（以下，AFL）がある．AFLは，バイナリ実行時に得られる実行パスの情報を利用するファジングツールの一種であり，実際に様々なソフトウェアの脆弱性を発見した実績がある．しかし，そのほとんどは汎用システム上のソフトウェアを対象としており，AFLが組込みシステムのファジングに適用された前例は非常に少ない．

本研究では，AFLの動作原理とその特性について調査・評価し，組込みシステムのファジングに利用することを目的とする．はじめに，AFLのドキュメント・ソースコードをもとに，AFLによるファジングの仕組みを調査した．続いて，組込みシステム向けTCP/IPスタックlwIPを，汎用システム上でユーザプロセスとして動作させ，AFLを用いて実際にファジングを行った．さらに，与えるテストケースや，チェックサム検査の有無を変化させた際に，ファジングの経過を観察することで，AFLの特性を評価した．

様々なバージョンのlwIPに対してAFLでファジングを行った結果，1〜3時間程度の短時間なファジングで，ver1系・ver2系においてそれぞれ再現可能な脆弱性を発見することができた．異なるテストケースを与える実験では，TCPv4パケットをデータにもつEthernetフレームと，単純なテキストデータを，テストケースとしてそれぞれ与えた．結果として，検出されたパス数ではあまり差が見られなかったものの，一部のコードおいて，前者のほうがカバレッジが向上していることが確認された．また，チェックサム検査に関する実験では，検査を有効化した場合は，無効化した場合と比べて約6割程度のパスしか検出できないという結果となった．これらの実験により，AFLによるファジングの効果とその特性が確認された．また，AFLを組込みシステムのファジングに適用する際の困難点が明らかになった．今後の課題としては，困難点の解決方法を検討し，汎用システム上ではなく，組込みシステムの実機上で動作するプログラムをAFLでファジング可能にすることが挙げられる．