令和4年度 コンピュータ科学科卒業論文要旨

高田・松原 研究室	氏　　名	大 羽　俊 輔
卒業論文題目	IoT機器を想定した実行環境におけるマルウェアの影響評価	

IoT 機器の増加に伴い、マルウェアによる IoT 機器への攻撃リスクが高まっている。IoT とは、実世界のモノをインターネットに接続し、インターネットを介して情報を相互にやり取りできるようにするという考え方である。マルウェアの分野はコンピュータの普及に伴い盛んに研究が行われてきた領域ではあるが、IoT 機器を攻撃対象としたマルウェアが盛んに研究されるようになったのは IoT 機器が普及してきたここ数年のことである。パーソナルコンピュータの多くが x86_64 プロセッサで動作している一方で、IoT 機器の多くは ARM プロセッサで動作している。従来のマルウェアの解析・検出手法の多くは x86_64 アーキテクチャに特化しており、ARM アーキテクチャに対して容易に転用することができない。そのため、ARM アーキテクチャを攻撃対象としたマルウェアの更なる研究が求められている。

本研究では、IoT 機器の実環境を想定した環境においてマルウェアがどのような影響を与えるのかを定量的に示すことを目的として、評価手法の提案とその手法を用いた評価実験を行う。評価対象となる環境として、ウェブサーバを想定したラズビアン環境、コンテナ環境、ユニカーネル環境を提案し、それぞれの環境においてマルウェアを実行した際に実行環境やサービスにどのような影響を与えるのかを評価する。コンテナ環境およびユニカーネル環境は IoT 機器の実行環境として近年注目されている環境である。評価を行う上で、評価指標として実行の可否および脅威スコアを用い、マルウェアの影響の程度を定量的に計測する。これらの指標を用いて各環境におけるマルウェアの影響を比較することで、3 つの環境の特性を示すことができる。実行の可否は、マルウェアが実行可能かどうかを示す指標であり、マルウェアを実行した結果が正常終了または一定時間実行状態であったものを実行可能、異常終了したものを実行不可と判定する。脅威スコアは、実行したマルウェアがどの程度脅威となるかを示す値であり、マルウェアの実行の可否とそのマルウェアの分類に応じて算出される。評価実験は、ラズビアン環境のみを対象に行った。環境構築として、まずエミュレータ型仮想化ソフトウェアである QEMU を用いて RaspberryPiOS を動作させ、さらに、評価時間を短縮するために評価の自動化を行った。

評価実験の結果、実行の可否および脅威スコアを求めることに成功し、提案手法を用いることでマルウェアの影響を定量的に示すことが出来ることが分かった。加えて、実行に失敗したマルウェアの終了ステータスを分析することで、実行に失敗するマルウェアの多くが不正なメモリ参照または存在しないコマンドの参照により実行に失敗していることが明らかになり、使用可能なコマンドを制限することでマルウェアの影響を抑制できること示唆する結果となった。また、自動化を行うことで、一つのサンプルごとに 200 秒程度掛かっていた評価を 90 秒程度で行えることが示され提案手法の有用性が示された。

本研究では、IoT 機器の実環境を想定した 3 つの実行環境においてマルウェアがどのような影響を与えるのかを定量的に示す手法を提案し、ラズビアン環境において実際に評価実験を行った。今後の課題として、残る 2 つの環境でも評価実験を行うことや、脅威スコアを厳密に算出するために実際のマルウェアの振る舞いから脅威の程度を評価すること、評価にかかる時間をさらに短縮することなどが挙げられる。