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するという考え方である。マルウェアはコンピュータの普及に伴い盛んに研究されてきた分野であるが、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 2018 年頃のことである。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、命令セットが異なる 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。昨今、IoT 機器の実行環境としてコンテナやユニカーネルなどの環境が提案されており、実行環境は多様化してきている。

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。アプリケーション実行環境として、ラズビアン環境、コンテナ環境、ユニカーネル環境を対象に、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。いずれの環境も、IoT 機器の機能としてウェブサーバを想定し、ウェブサーバアプリケーションをインストールする。評価指標として、マルウェアの実行可否および脅威スコアを用い、マルウェアの影響を定量的に推定する。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。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。ラズビアン環境の評価環境として、エミュレータ型仮想化ソフトウェアである QEMU を用いて Raspberry Pi OS を動作させ、マルウェアの実行、実行結果の取得、脅威スコア算出を自動化する環境を構築した。

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。自動化を行うことで、一つのマルウェアごとに 180 秒程度掛かっていた評価を 100 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うことでその有効性を示した。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。