G-15

IoT デバイス用ハニーポットの構築

Construction of Honeypots for IoT Devices

○小寺　建輝 [1]，泉　隆 [2]（日本大学）
*Tateki Kodera[1], Takashi Izumi[2] (Nihon University)

The IoT (Internet of Things) is a concept that all sorts of things connect to the Internet.　Small IoT device has less resources such as a CPU and a memory, and it is difficult to implement sufficient security features to the device.　Additionally, the attack techniques to IoT devices are considered unknown threats that is different from the attack techniques to PC etc.　This report describes the construction method of the IoT honey pot for analyzing attack techniques to the IoT devices.

1. はじめに

IoT(Internet of Things)とは、ありとあらゆるモノがインターネットに接続する概念である。IoT デバイスは車、POS 端末、家電、医療装置などデバイスの種類が様々であり、2020 年までに 250 億台まで増加すると見込まれている[1]。しかし、IoT デバイスの普及に伴い、そのセキュリティが問題視されている。特に、小型 IoT デバイスは CPU やメモリ等のリソースが少ないため、デバイス自体に十分なセキュリティ機能を実装することが難しいと考えられる。さらに、IoT デバイスに対する脅威は従来の攻撃手法とは異なった、未知なる脅威が多くなることも考えられる。

本報告では、IoT デバイスへの攻撃を分析するためのハニーポット(IoT ハニーポット)の構築手法について検討する。

2. IoT デバイスに対する脅威

IoT デバイスは従来、インターネットにつながっていなかったモノがインターネットに接続されることにより、インターネットを介して外部から攻撃を受ける可能性がある。IoT デバイスに対する具体的な脅威を以下に示す。

2.1 IoT デバイスとマルウェア

現在の組込み機器の CPU は x86、ARM、MIPS、PPC など多種多様な CPU アーキテクチャが採用され[2]、OS は Linux 系の組込み OS が多く採用されている[3]。現在では PC などに使用されている x86 や amd64 アーキテクチャで動作するマルウェアが主流であるが、組込み機器が IoT デバイスとしてインターネットに接続することで、ARM、MIPS、PPC などのアーキテクチャの Linux 上で動作する未知のマルウェアが増加することが考えられる。

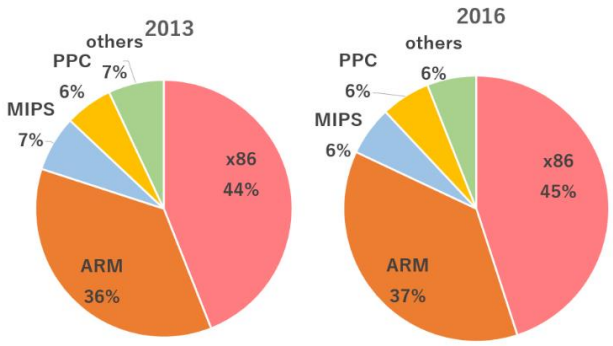

Figure1. Embedded CPU architecture market share

2.2 telnet ベースの攻撃[4]

近年、Linux 系組込み機器を発信元とした宛先ポート 23/TCP(telnet)に対するアクセスが増加しており、IoT デバイスでは、telnet ベースの攻撃が増加すると考えられる。IoT デバイスへの telnet ベースの攻撃は以下のステップで行われる。

1. Nmap[5]などのツールなどを用いたホストスキャン
2 .辞書攻撃や総当り攻撃による不正ログイン
3. IoT デバイスの詳細調査
4. CPU アーキテクチャに合わせたマルウェアのダウンロード
5. 不正プログラムの実行
6. ネットワーク内のデバイスの探索・感染

3. IoT ハニーポットの構築

ハニーポットとは、あえて脆弱性をもたせたマシンを外部ネットワークからアクセスできる状態にして、外部から意図的に攻撃を行わせることで、そのマシンの環境における攻撃を観測・研究するためのシステムである。

1:日大理工・学部・情報　2:日大理工・教員・情報

3.1 攻撃モデルと取得するデータ

本研究で構築するハニーポットでは、2 章で示したような多種多様な CPU アーキテクチャで動作する IoT デバイスへの telnet ベースの攻撃を観測する。また、これら一連の攻撃で記録されるログイン試行ログ・パケットキャプチャファイル・コマンド実行ログ・ダウンロードされたマルウェアなどのデータを取得する。

3.2 IoT ハニーポットの構成

本研究で構築する IoT ハニーポットの構成図を Figure2 に示す。

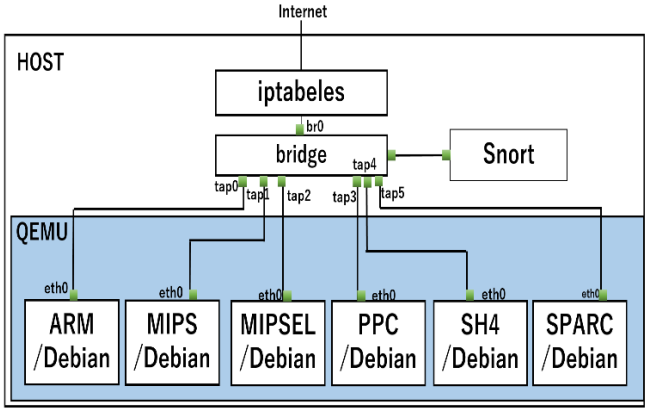

Figure2. Diagram of IoT honeypots

本ハニーポットでは、QEMU[6]を用いて ARM、MIPS、MIPSEL、SPARC、PPC、SH4 の 6 つ CPU アーキテクチャのデバイスをエミュレーションする。QEMU とは様々な CPU アーキクチャのデバイスをエミュレーションするオープンソースソフトウェアである。それぞれの IoT デバイスには Linux 系 OS の Debian をインストールする。それぞれのハニーポットでは、不正アクセスされた後の攻撃者の行動を記録する必要があるため、攻撃者にログインを成功させる必要がある。そのため、ログイン ID とパスワードをともに「user」、管理者権限（root ユーザ）のパスワードを「root」に設定し推測されやすいものにした。

また、TAP とブリッジによりネットワーク信号を分岐し、ゲストマシンとホストマシンで同じネットワーク体系を利用できるようにすることで外部との通信を可能し、ルータでは外部からの 23 番ポート(telnet)への接続を内部ネットワークのゲストマシンへ通すようにポートマッピングの設定を行うことで telnet 接続を可能にする。なお、ハニーポットでは侵入に成功した攻撃者が、侵入したデバイスを踏み台にして他のマシンに攻撃を試みる可能性がある。これを防ぐために、パケットフィルタリング機能を制御するためのツールである iptables を用いてハニーポットからインターネットへの接続回数を制限する。

ログイン試行ログ、コマンド実行ログ、ダウンロードされたマルウェアはデバイス自体に保存されるが、パケットキャプチャファイルは Snort[7]を用いて取得する。Snort とは、ネットワーク型 IDS(Intrusion Detection System:侵入検知システム)である。Snort によりネットワーク内に流れるすべてのパケットの監視や、パケットキャプチャファイルとしての取得ができる。また、ネットワーク型 IDS は NIC(Network Interface Card)に IP アドレスを振らないステルスモードで運用できるため、攻撃者に認識されることがないという利点がある。しかし、各デバイスで保存されるログは攻撃者に削除される可能性があり、またログを保存できるログサーバなどを用意し、デバイスで取得されるログを定期的にログサーバに転送するシステムを構築する必要がある。

5. まとめ・今後の方針

本報告では、Linux 系 OS で動作する、多種多様な CPU アーキテクチャのデバイスをエミュレーションした IoT ハニーポットの構築を行った。

今後は、継続的にハニーポットを観察し、IoT デバイスへの攻撃手法について分析を行う。また、分析結果に基づき IoT デバイスのセキュリティ対策についても検討していく。

参考文献

[1] Gartner「NewsRoom」,https://www.gartner.co.jp/press/html/pr201404,2016-9
[2]VDCReserch:「AMD reveals roadmap for ARM and x86 SoCs」,http://hackerboards.com/amd-reveals-arm-and-x86-soc-and-apu-plans/,2016-9
[3]VDCReserch:「The Global Market for IoT & EmbeddedOperatingSystem」,http://www.vdcresearch.com/_Documents/briefs/IoT/15-iot-embedded-op-systems.pdf,2016-9
[4]警察庁:「IoT 機器を標的とした攻撃の観測について」,https://www.npa.go.jp/cyberpolice/detect/pdf/20151215_1.pdf,2016-9
[5] Gordon Lyon,「Nmap リファレンスガイド(Man Page)」, https://nmap.org/,2016-9
[6] Fabrice Bellard,「QEMU CPU エミュレータユーザドキュメト」,http://www.h7.dion.ne.jp/~qemu-win/qemu-doc-ja.html,2016-9
[7] Sourcefire,「Snort - Network Intrusion Detection&PreventionSystem」,https://www.snort.org/,2016-9