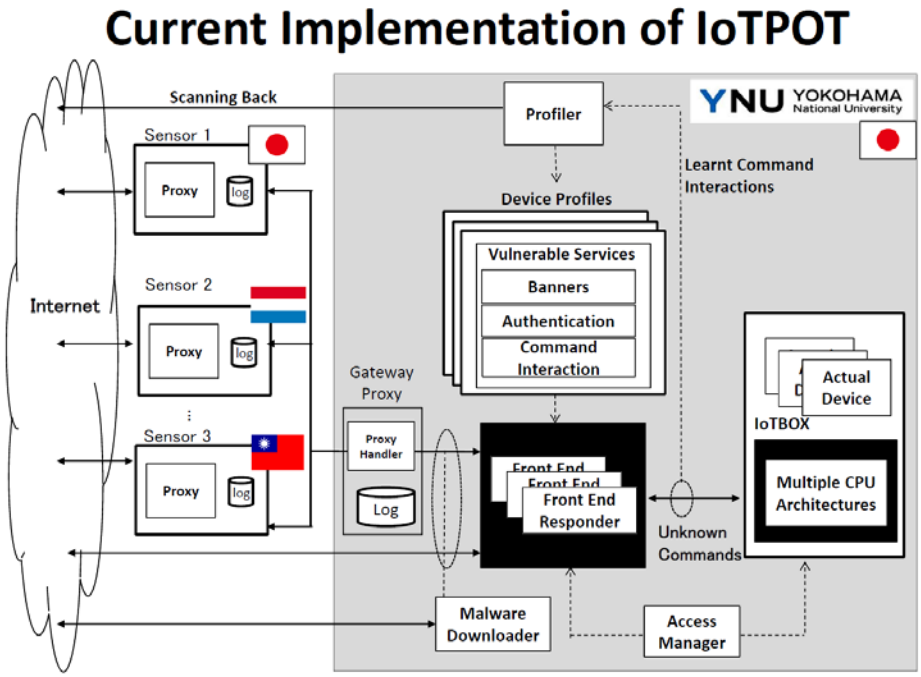
解説記事 No.1　吉岡克成准教授の研究グループ

身の回りに潜む知られざるサイバー攻撃を発見せよ！
サイバー攻撃を誘い込む新たな"おとり":「IoTPOT」の開発

吉岡克成准教授の研究グループは、インターネットに接続された家電製品、産業機器、医療機器、カメラ、センサなどの IoT 機器に対するサイバー攻撃の脅威を観測するために、脆弱な機器を模擬した新しいハニーポット[*1]「IoTPOT」を開発し、IoT におけるサイバー攻撃の実態状況の観測を行いました。



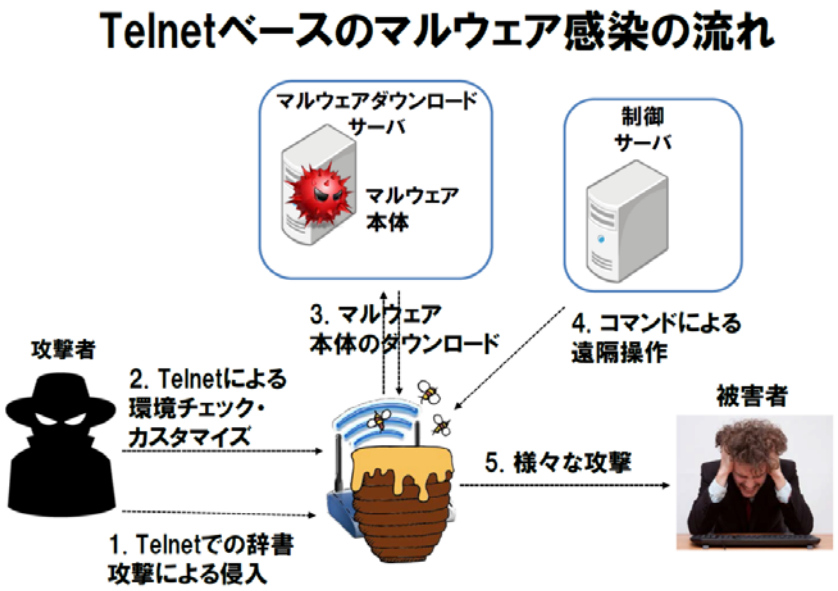
IoT 機器へのサイバー攻撃を観測する仕組みである IoTPOT は世界各国に分散配置されるセンサ群(本年度中に 10 か国に展開予定)と横浜国立大学内に構築されたバックエンドシステム(図の灰色部分)からなります。センサに届くサイバー攻撃は全てバックエンドシステムに転送されます。バックエンドシステムではセンサ群を通じて世界中から届くサイバー攻撃に対して、セキュリティレベルの低い機器を模擬した応答を行うことで、攻撃者を惹きつけ、攻撃の観測、分析やマルウェア(不正プログラム)の収集を行います。

4 ヶ月で IoT 機器 15 万台から 90 万回もの攻撃が

IoT の発展とともに、IoT 機器を標的としたサイバー攻撃が急激に増加しています。約 100 個の IP アドレスを持つ「IoTPOT」を用いて、2015 年 4 月から 7 月の 4 か月間に行った観測では、約 15 万台の IoT 機器から 90 万回の攻撃を確認しました。これらは既存のハニーポットでは確認できなかったものです。攻撃を仕掛けてきた IoT 機器は、家庭用機器をはじめ、駐車場管理システム、ビル制御システムといったインフラ機器に至るまで、確認できただけで 361 種類に及びます。

Telnet[*2]を通じたウイルスの拡散が確認

捕えたコンピューター・ウイルス（マルウェア）の分析結果から、主に乗っ取られた IoT 機器はインターネット上の特定サイトやサーバーへ一斉にアクセスし、サービスを妨害する DDoS 攻撃を行うとともに、Telnet[*2]を通じた更なるコンピューター・ウイルスの拡散を行うことが確認できました。これらのコンピューター・ウイルスは 5 種類以上存在し、一部の種類は、頻繁に更新を行い、より多くの種類の機器に感染するよう急速に進化していることが分かりました。



社会インフラへ対するテロに利用される懸念も

現在の IoT 機器に対するサイバー攻撃の主流は DDoS 攻撃を目的としているため、感染した IoT 機器の保有者自身は被害を体感しにくいですが、大勢の人が集まる商業施設や空港などの管理システムを乗っ取り、テロに利用するなど重大な犯罪が発生するリスクがあります。吉岡克成准教授の研究グループでは、引き続き IoT におけるサイバー攻撃実態の観測、分析、対策に関する研究を行い、セキュリティ対策の確立を目指しています。

[*1] ネットワーク攻撃やコンピューター・ウイルスの振舞いなどを調査するために、わざと侵入しやすいよう脆弱な設定を施しネットワークに設置した「囮（おとり）」の観測用システムです。

[*2] インターネットやイントラネットなどのネットワークにおいて、ネットワークにつながれた他のコンピュータを遠隔操作するための仕組みのひとつで、30 年以上前に作られた通信プロトコルです。セキュリティ上の問題が指摘されており、インターネット上では使用が控えられるのが常識と考えられていましたが、多くの IoT 機器上で動作しており、コンピューター・ウイルス感染の原因となっています。

掲載論文・雑誌記事

1. "IoTPOT: A Novel Honeypot for Revealing Current IoT Threats", Y. M. Pa Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, C. Rossow, *Journal of Information Processing*, Vol.24 No.3, 522-533, (May 2016)
2. "マルウェアに感染する IoT デバイスが激増　ネットワーク攻撃に悪用",『PROVISION』88 号 特別インタビュー 2，2016 年 2 月
3. NHK くらし☆解説　「IoT ブームとセキュリティー」,2016 年 2 月

関連 URL

1. 先端科学高等研究院　情報・物理セキュリティ研究ユニット
2. 情報・物理セキュリティ研究拠点

文：荒井恒宣（YNU-IAS）、レイアウト：佐藤英梨（YNU―IAS）