2018-00448 - [Campagne CORDI-S-CRI Paris] Securing Internet of Things devices in home networks

Level of qualifications required: Graduate degree or equivalent
Function: PhD Position

Context

Within the framework of a partnership

- Collaboration between Inria MiMove and Princeton University within the Associate team HOMENET: https://team.inria.fr/homenet/

Objective

The goal of this Doctoral thesis is to develop algorithms, methods, and software systems to detect vulnerable devices, intrusion, and attacks in the context of home Internet of Things.

Is regular travel foreseen for this post? The student may visit our collaborators in Princeton.

Assignment

Research context:

Modern households are deploying Internet of Things (IoT) devices at a fast pace. The heterogeneity of these devices, which range from low-end sensors to smart TVs, make securing home IoT particularly challenging. To make matters worse, many consumer-IoT devices are hard or impossible to secure because device manufacturers fail to adopt security best practices (e.g., regular software patches). Vulnerable IoT devices make home networks open to attacks or privacy leaks and make the Internet subject to large-scale Distributed Denial of Service (DDoS) attacks such as the Dyn Attack by the Mirai botnet. Securing home networks is particularly challenging. IoT devices are more diverse than those in a managed, conventional network, in terms of both the devices themselves, their introduction to the home network, and the software they run. In an enterprise network, for instance, network administrators often enforce device and software homogeneity to ease management and maintenance. Home users may connect a broad array of devices, applications, and services. In conventional networks, expert administrators are responsible for managing the network. For example, they take steps to secure end hosts such as applying security patches. In contrast, most home networks do not have a technically skilled network administrator.

The MiMove team at Inria is working in collaboration with Nick Feamster's group at Princeton University on a project that proposes a novel network-based approach to secure home IoT devices: instead of trying to secure an increasing number of heterogeneous devices, focus on securing the network connecting them. With no communication, malicious devices cannot compromise other devices or launch attacks. We propose to develop a system that relies on defense mechanisms deployed directly at the user's home.

Assignments:

The goal of this doctoral thesis is to develop algorithms, methods, and software systems to detect vulnerable devices, intrusion, and attacks. To achieve this goal, we will take a data-driven approach. Inria together with Princeton University runs a small deployment of boxes (Raspberry Pi's and Odroid boxes) in homes in France and the USA. This deployment is currently used for studying Internet quality of experience. We plan to extend it to study IoT security issues. The student will also have access to a testbed of IoT devices, which can be used for running controlled experiments. The plan is for the student to use these datasets to develop methods to identify the types of connected IoT devices and associate them with known IoT vulnerabilities from public databases (e.g., SHODAN, OWASP or other). For identifying devices, we are interested in analyzing network traffic generated by IP-enabled devices (e.g., IP packet headers, TCP packet headers, ...
send/receive rates, DNS requests). Our analysis aims to extract device profiles in terms of distinct activity patterns (traffic rate, busyness, idle periods) [1] and sequences of DNS lookups to service IPs specific to a device or its manufacturer [2]. The research will involve both (1) identifying the trade-offs between the cost of different feature extraction methods (traffic metadata vs. DNS-based signatures) and the precision of the device type classification techniques and (2) exploiting state-of-the-art classification techniques that can accurately identify the unique software and hardware characteristics of devices.

The student will also develop methods to detect attacks. In particular, we aim at detecting anomalous behavior that derives from normal activity. IoT devices have mostly a single purpose functionality compared to general-purpose computers (e.g., mobile phones, desktops, and servers), which result in simpler network dynamics. Unfortunately, the sparsity of the traffic/probing data points per IoT device collected from a particular network brings new challenges to typical anomaly detection methods. IoT devices usually spend long periods of silence and may generate bursts of downlink traffic depending on the user activity [3]. To address this issue, we plan to profile the normal behavior of IoT devices as it is manifested by historical data collected within or across home networks. Furthermore, to improve IoT situational awareness we are interested in correlating security events or alert data from heterogeneous information sources [4] e.g., combining anomalies in traffic/probing data of IoT devices with system runtime data of smart home apps or apps. In essence, the methods must analyze different features of device behavior and thus we plan to study multidimensional anomaly/outlier detection techniques.

**References:**


**Collaboration:**

The student will be co-advised by Renata Teixeira and Vassilis Chirstophides from Inria and Nick Feamster from Princeton.

**Main activities**

**Main activities:**
- Analysis of network traffic from IoT devices
- Development of methods to identify IoT devices
- Development of anomaly detection methods to detect threats from IoT devices
- Development of a system that integrates device identification and anomaly detection methods
- Evaluation of the developed system in home networks

**Additional activities:**

- Writing of research papers
- Presentation of research work in conferences, seminars

**Benefits package**

- Subsidised catering service
- Partially-reimbursed public transport

**General Information**

- **Theme/Domain**: Distributed Systems and middleware
- **System & Networks (BAP E)**
**The keys to success**

The candidate should have a strong background in computer networks (TCP/IP and application layer protocols, HTTP(S), in particular) and computer systems performance measurement. The candidate should have knowledge of data analysis techniques (statistics, data mining, machine learning) and some related tools such as Matlab or gnu R.

The candidate should be able to write (scientific writing) and communicate fluently in English.

**Conditions for application**

**Defence Security**:  
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST). Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

**Recruitment Policy**:  
As part of its diversity policy, all Inria positions are accessible to people with disabilities.

**Warning**: you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.