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, makes 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 adequate security practices (e.g., regular software patches). Vulnerable IoT devices make home networks prone 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 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.

The goal of this doctoral thesis is to develop algorithms, methods, and software systems to detect vulnerable devices and attacks in the context of home Internet of Things. This deployment is currently used for studying Internet of Things devices in home networks.

The student may visit our collaborators in Princeton. The candidate should be able to write (scientific writing) and communicate fluently in English.
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 Christophides from Inria and Nick Feamster from Princeton.

Principales activités

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

Avantages sociaux

- Subsidised catering service
- Partially-reimbursed public transport