Attack detection and mitigation for the Internet of Things

Keywords : Internet of Things; Network security; Intrusion Detection.

Lionel Metongnon, Ramin Sadre

Abstract – In the Internet of Things (IoT), it is envisioned that a huge amount of physical objects will become online. From a security perspective, the more devices are connected to communication networks, the more powerful cyber-attacks can become. The goal of this research project is to design, develop and evaluate new distributed attack detection and mitigation approaches for the IoT.

Introduction. The number of interconnected devices already surpasses the number of connected people. This difference will become even larger with the Internet of Things (IoT) [1]. In the IoT, it is envisioned that a huge amount of physical objects, somehow capable of interconnecting to each other and to the Internet, will become online. From a user experience perspective, IoT will make life more comfortable by creating an interconnected environment, supporting daily tasks and decisions. From a security perspective, however, the more devices are connected to the Internet, the more powerful cyber-attacks can become. IoT devices can be attacked to cause damage to the physical appliances connected to them. Furthermore, IoT devices can be infected and become part of a botnet or be misused to perform distributed attacks, such as powerful Distributed Reflection DoS attacks. A first botnet with provisions for infecting IoT devices has been already identified [2].

Distributed Monitoring System. One way to prevent the misuse of networked devices is by monitoring the network's incoming and outgoing traffic. A big challenge in securing the IoT in this way is its highly distributed character. As illustrated in Fig. 1, the IoT is not a monolithic structure but will soon consist of millions of local area and personal area networks (LANs and PANs) connected through border routers to the Internet infrastructure. Larger buildings will typically host several dozens of such LANs and PANs. Due to this distributed nature and the huge number of devices, we propose to monitor the networks' incoming and outgoing traffic at the border routers to detect and mitigate incoming and outgoing attacks.

Another challenge is the cost of a potential solution. IoT devices are not expensive (down to a few cents) and end-users will not be willing to spend several hundreds or thousands of Euros to protect them. We envisage an intrusion detection system (IDS) that can be implemented in the border routers. Typically, such routers for (non-commercial) end users are cheap embedded devices, though more powerful than IoT devices. Our solution should work on two levels: On a local network level, an IDS instance will perform a preliminary analysis of the traffic to detect malicious activities. To be scalable in the presence of a massive DoS attack, our solution will mainly operate on *flow level* and not rely on deep packet inspection.

The local network level will also provide input to a distributed collaborative level, which will be in charge of creating a consistent view on current threats. Such a collaborative approach will greatly increase the capability of the system to detect large-scale attacks and malfunctions, i.e., anomalous behavior that, although not suspicious and, hence, not detectable in an individual LAN or PAN, becomes visible when observed on a global scale.

Preliminary work. While network attacks against wired and WiFi networks have been extensively studied in the literature, there is, due to its young age, much less concrete information available on the characteristics of network attacks against the IoT. Furthermore, it is to a large extend unknown how complex IoT networks would behave in the presence of massive attacks.

Therefore, our first step has been to build *ns3* models [3] to simulate networks in which IoT devices using different types of communication technologies are attacked. An example model is shown in Fig. 2 where an attacker attempts to perform a network scan from the Internet against an IoT infrastructure mixing WiFi and 6LoWPAN networks. The insights that we have gained from our simulations allow us to better understand potential attack strategies and to parameterize our envisaged detection methods.

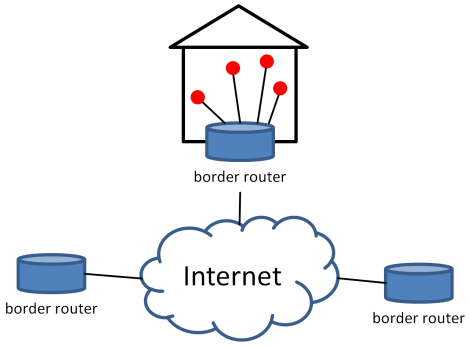

Figure 1: IoT network infrastructure.

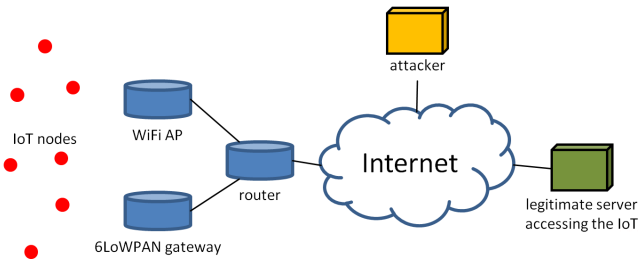

Figure 2: Model for network scan simulation.

References

[1] J. Frahim et al. Securing the Internet of Things: A Proposed Framework. http://www.cisco.com/web/about/security/intelligence/iot_framework.html

[2] Symantec. IoT Worm Used to Mine Cryptocurrency. http://www.symantec.com/connect/blogs/iot-worm-used-mine-cryptocurrency

[3] ns-3 simulator. https://www.nsnam.org/