Security of IoT: Intrusion Detection and Prevention

Mots clés :

- Directeur de thèse : osman SALEM
- Co-encadrant(s) :
- Unité de recherche : Laboratoire d'Informatique PARis ENscartes
- Ecole doctorale : École Doctorale Informatique, Télécommunications, Électronique de Paris
- Domaine scientifique principal: Sciences et technologies de l'information et de la communication

Résumé du projet de recherche (Langue 1)

With the proliferation of IoT devices in our daily life, and the myriad of exiting vulnerabilities (and misconfigured devices) conduct to the rise of weaponized [1] IoT and Thingbot, which are participating in several attacks [2] (such DDoS, reflection, amplification, etc.). Furthermore, the ability to insert instructions or change the running behavior of such devices leave the door open for other malicious software, such as ransomwares that target devices used to control human environment. Recently, industry and providers start developing a security framework, and considering some security mechanisms in the IoT. However, they still far from providing secure devices. The BASHILTE malware compromised more than million IoT, and a lot of other malware used to compromise IoT are reported in the web. Like existing servers and OS, IoT devices requires hardening and other security mechanisms (intrusion detection/prevention, anomaly detection, etc.) as a second line of defense. Therefore, the main objective of this research project is to propose security mechanisms compatible with the restrained resources (processing, memory, energy, etc.) of IoT devices. We want to search, propose, implement security framework in IoT, which aims to detect and prevent malicious activities from compromising the Thing and transforming it into zombie.

The research work aims to achieve the following tasks:
- State of art of existing solutions and security framework for IoT
- Proposing a new security framework (IDS/IPS, NAC, etc.) adequate with resources of IoT
- Implementation of proposed framework to conduct experimentations
- Performance analysis and comparison with existing solutions

Informations complémentaires (Langue 1)

References: