NGI EXPLORERS

CHALLENGE #33
SCU-IOT-03

Securing and Protecting Resource-Contained IoT Devices

Meet the expectations of this US Node through the technology challenge described below

GOALS

Monitoring and securing IoT devices in a real-time and scalable manner is challenging. Since IoT devices are resource constrained, they are more vulnerable against DoS and DDoS attacks. Existing research shows that even a low-rate SYN attack can increase the energy consumption of these devices and could also result in disconnection and device failure. Understanding the impact of various attacks on different hardware architectures, operating system types, and networking protocols stacks is necessary to design defense mechanisms. Designing fast, low-overhead techniques is necessary to first classify device type and then identify the various types of attacks and their severity for each device.

DETAILS

(1) profiling and modeling the effect of attacks on the operation and energy consumption of IoT devices, (2) novel algorithms for fast, low-overhead classification of IoT devices and attacks.

SKILLS REQUIRED

Wireless communication, operating system, machine learning, security algorithms

FUNDED BY NGI

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825183