PhD Student: Han Wang, RISE Cybersecurity Lab, Kista Stockholm <han.wang@ri.se>
Main Supervisor: Shahid Raza, RISE Cybersecurity

Title: Device Fingerprinting and Identification at IoT edge with Federated Learning

Abstract:
The impact of Internet of Things (IoT) will keep penetrating deeply in our daily life including homes, public buildings, industries and even cities. Due to the prompt release and widespread need of IoT devices, it is getting harder to trace the background information and history of the device. It risks the devices being vulnerable to various attacks. A well-designed authentication mechanism helps administrator monitoring the devices and recording their behaviors within the network. However, most of the approaches to device identification are device-type-based which are still deficient to trace the source of the vulnerabilities of the device. Moreover, General Data Protection Regulation (GDPR) encouraged and some cases mandated to share only the minimal amount of data, enforcing privacy-by-default and by-design. To comply with EU policy, Federated learning seems to be ideal solution to the privacy-persevering objective. In this paper, we aim to fingerprint the device not only the deice-type but also the manufactures, vendors and any actors behind the device. Furthermore, we examine the performance of different state-of-the-art machine learning methods and Federated Learning between centralized and decentralized manner.

The PhD student who works on this has started last February and currently writing a paper on IoT device fingerprinting and identification on IoT edge with Federated Learning.

This work is done in collaboration with Northeastern University and is partly funded by RISE internal funding and partly by the EU Horizon 2020 COCNCORDIA, a project that is building an EU cybersecurity center of excellence.