

Zero-configuration Security for the Internet of Things

Open Postdoc position

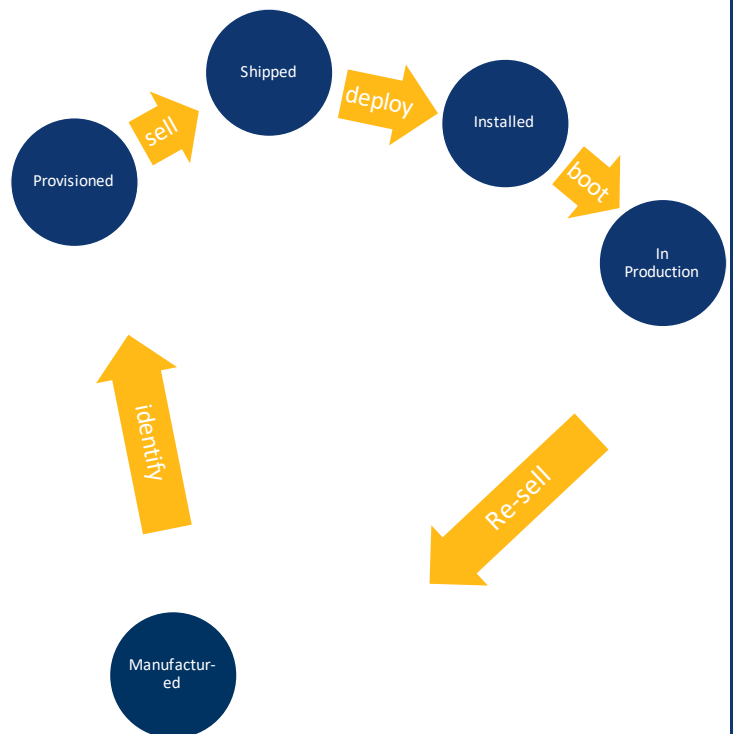
Description of Work

The journey of an Internet of Things (IoT) device, *the mote*, begins on the manufacturer's bed of nails. Constrained in terms of memory, processing and energy, the mote typically lacks a user-friendly interface. The manufacturer gives the mote its identity, including a serial number and possibly a set of cryptographic keys. Once sold, the mote leaves the manufacturer's premises and is shipped to a remote site where it can be stored for years before getting deployed.

Human actions are slow and error-prone. Deploying thousands of motes from different origins that require manual human input during deployment is time consuming. It is paramount to automate the process such that the only required action in a remote site before the mote starts operating is the push of a button.

For this to happen, once the mote boots it needs to go through the *enrollment* process. This entails mutual authentication, authorization and domain-specific parameter distribution. Most likely, only the manufacturer is in possession of the cryptographic keys that were initially provisioned to the mote. The challenge is that the manufacturer may be offline at the time when the mote boots. Existing solutions assume that the manufacturer is online at all times, which does not hold for IoT use cases.

You will design, implement and validate a networking protocol that allows the mote to enroll at a new



administrative domain with zero configuration required by the human. We will use the existing Internet Engineering Task Force (IETF) work as our starting point and define the missing pieces when these protocols are applied in the IoT use cases. If you are so inclined, you will contribute to the IETF standardization.

Key Facts

- Type of position: Postdoc
 - Location: Inria-Paris, France
 - Supervisor: Mališa Vučinić, PhD
malisa.vucinic@inria.fr
 - Keywords: Network Security, Internet of Things, Wireless Sensor Networks
 - Inria Team: EVA
<https://team.inria.fr/eva>
 - Application deadline: June 15th, 2019.
- Candidates are encouraged to apply now.**
- Expected start date: September 1st, 2019
 - Duration: 16 months
 - Skills desired: Programming C/Python, Computer Security
 - Monthly salary: 2 653 €
 - Vacation: approx. 45 days per year