Two-step process for secure registration of nodes in IoT systems

Milan Stojkov, University of Novi Sad, Faculty of Technical Sciences
Miloš Simić, University of Novi Sad, Faculty of Technical Sciences
Goran Sladić, University of Novi Sad, Faculty of Technical Sciences
Branko Milosavljević, University of Novi Sad, Faculty of Technical Sciences

Motivation

- Devices in IoT ecosystems are not secure by default
- IoT can be considered as multi-layered architecture
- The whole classes of security issues exist on each layer
- One of the first perception layer problem is registration of new nodes

Architectural assumptions

- IoT system consists of a lot of interconnected nodes scattered on some area
- These nodes are strategically grouped in a way that network segmentation can be made
- Every segment can have different types of nodes
- Every segment have one or more gateways
- Gateways communicate with services in cloud

Two-step process

- Communication takes place between three entities: a node, a gateway, and a cloud authentication service
- The process for the secure authentication of the new node in the subnetwork consists of two steps:
  1. the node, after key establishment, authenticates against a local gateway
  2. if the first step fails, the node authenticates with the authentication service in the cloud

Two-step process

- In the first step, the first substep is key establishment process based on ECCDH where one-way authentication of the node towards the gateway is performed in a secure manner
- After successful key establishment, the gateway selects a configured number of nodes which have to check if the registered node is available at specific intervals
- In the second step of this process, the node has to communicate directly with the authentication service which resides in the cloud
- The second step is performed only if the first step is finished unsuccessfully

Conclusion

- We addressed the problem of secure registration of the nodes
- The two-step process also proposes a solution for node capture attack
- The process is hardened with the second step that is only a backup step and does not burden the whole process by default
- The process has broad use such as in industrial IoT manufacturing processes, smart healthcare, smart grid, etc.

Thank you!