STACK

Pushing back against IoT attacks

25 years | ITEA 4
1998–2023

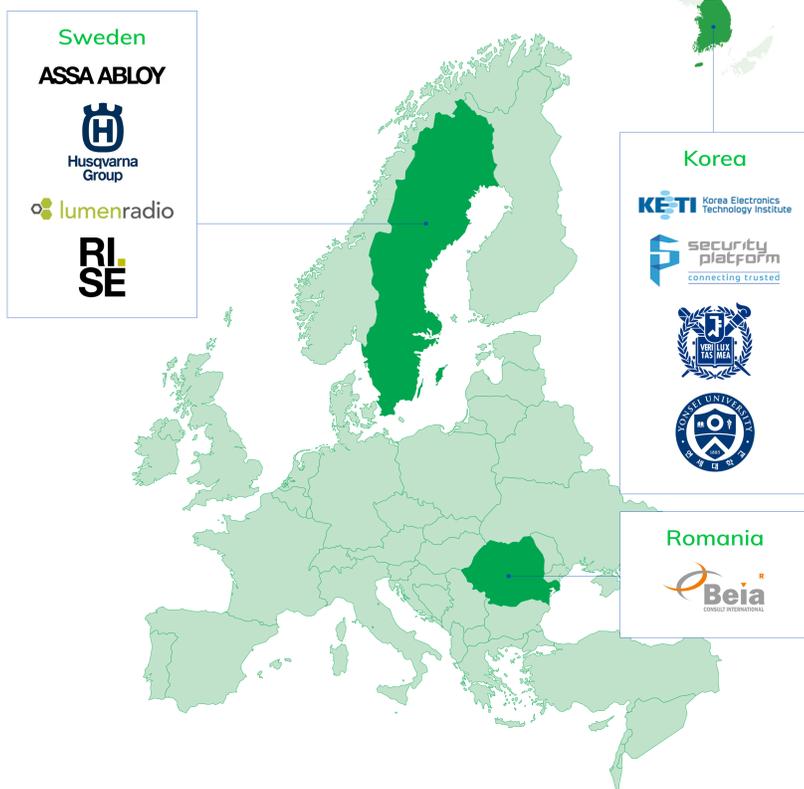## Project summary

The goal of STACK is to let IoT networks maintain their functionality in both benign environments and more challenging situations, such as when IoT networks are under attack or exposed to harsh radio environments and cross-technology interference. Solving these challenges will enable a new class of IoT applications that provide a certain Quality of Service (QoS), even when under attack.

Consortium

Sweden
ASSA ABLOY
Husqvarna Group
lumenradio
RISE

Korea
KETI — Korea Electronics Technology Institute
security platform — connecting trusted

Romania
Beia

Project duration

December 2020 - December 2023

Key results

> Mechanisms and algorithms to detect attacks in IoT mesh networks

> Support for collecting large-scale data for training ML algorithms for attack detection in IoT mesh networks

> On-board ML training for embedded/mobile platforms

AI-based
Attack Detection & Mitigation

More Robust IoT
Smart meters   Smart doors

STACK project website

SCAN ME

https://agile.ro/stack/

STACK YouTube channel

SCAN ME

https://bit.ly/3Ee8VHK

Contact

Thiemo Voigt
RISE - Sweden
E: thiemo.voigt@ri.se T: +46 10 228 43 48