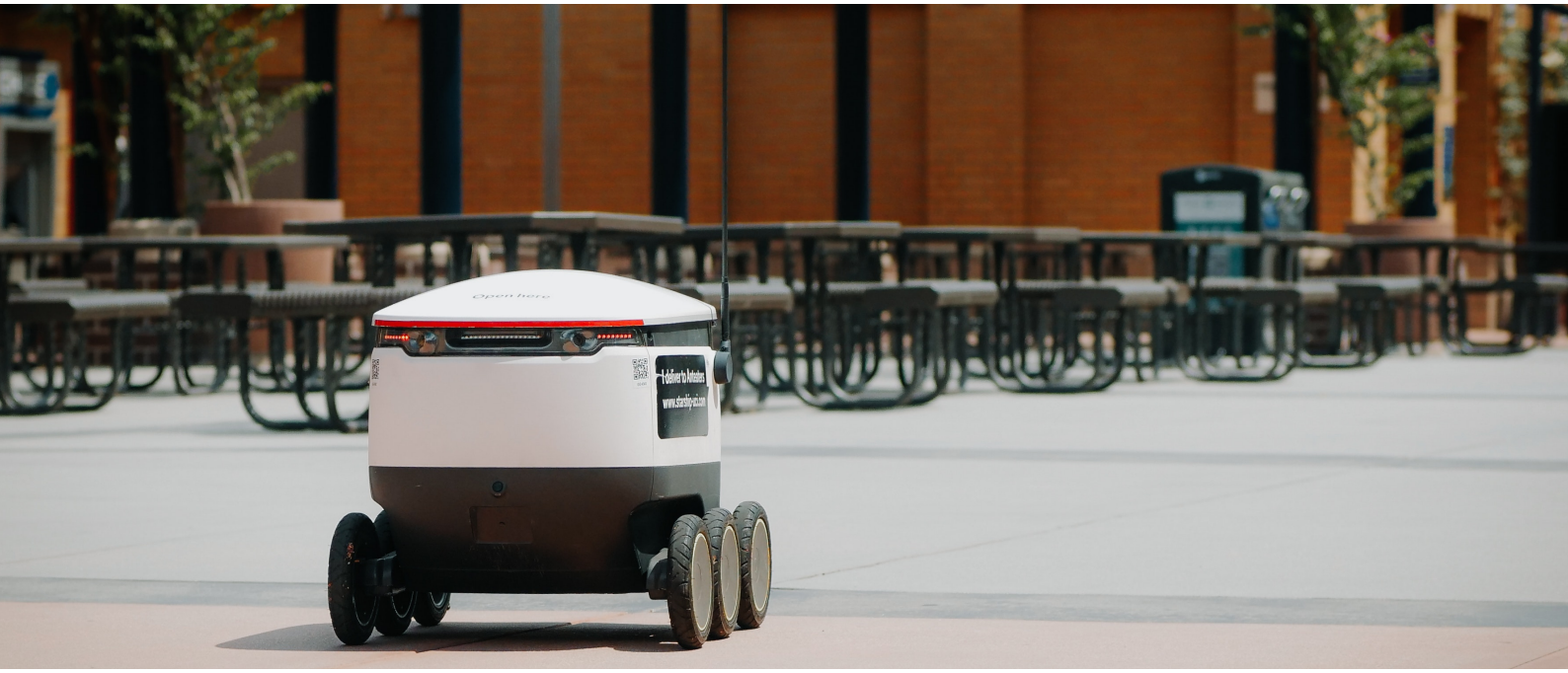
Case Study

SE*link*™

Making Robots Security Enabled to overcome the intrinsic resource limitations



Background

The increased digitalisation and mobility of services has led to a rapid increase in the sale and use of robots. The automative capabilities of the robotic system makes it a convenient tool to integrate across various domains of daily operation - from large industries to common households. According to the International federation of robotics, the market for professional service robots grew in 2020 by 12% to USD 6.7 billion, and service robots is only one branch of robotics! Just like any other fast-paced and innovative industry, security is often overlooked by manufacturers in the design and production phase. Despite the great advantages and promising future, robotics holds major concerns in terms of threats that can potentially affect both humans and machines. This includes maliciously hijacking and control of robots causing serious economic and financial losses.

Challenge

Robotic systems suffer from several security vulnerabilities that can be exploited to launch dangerous attacks. Such attacks are possible due to the lack of security by design of robotic systems and the reliance on open communication channels. As such, robots shall be protected from unauthorised access preventing attackers from breaching into these systems to inject malware and malicious data. Therefore, the authentication process should be designed to reach the highest possible security level to reduce the illegal access to robots and users. On the other hand, lightweight strong cryptographic algorithms and protocols at the network and/or at the physical layer are mandatory to ensure secure communication with minimal overhead in terms of delay and required resources.

Industry

Smart Cities
Social and Industrial Robots

Challenge

- ROS - Robot Operative Systems development frameworks are not designed to manage secure data and fail in guarding against unauthorised access
- Most Robots features are programmable and easily accessible

Goals

- Overcoming the intrinsic robots limitation with the focus on ensuring how to secure robotic system's software, hardware and communication while reducing cost of operations

Solution

SE*link*™ provides a zero trust security model combined with software-defined network segmentation and whitelisting practices. Delivering Data, Device, Network Security and Control in one single solution

Solution

Robots are programmable machines that rely on widely accessible robots specific operating systems like open source Robotic Operating System (ROS). These systems are equally vulnerable to the same type of attacks the computer systems are. Besides, the presence of some unique advanced capabilities like freedom of movement, physical actuators, multiple sensors, cameras and microphones, the different modes of operation (autonomous, tele-operated) and the presence of different communication channels makes robot security a much more complicated topic than the regular IT security. As with all cyber-physical systems, the attack surface is huge.

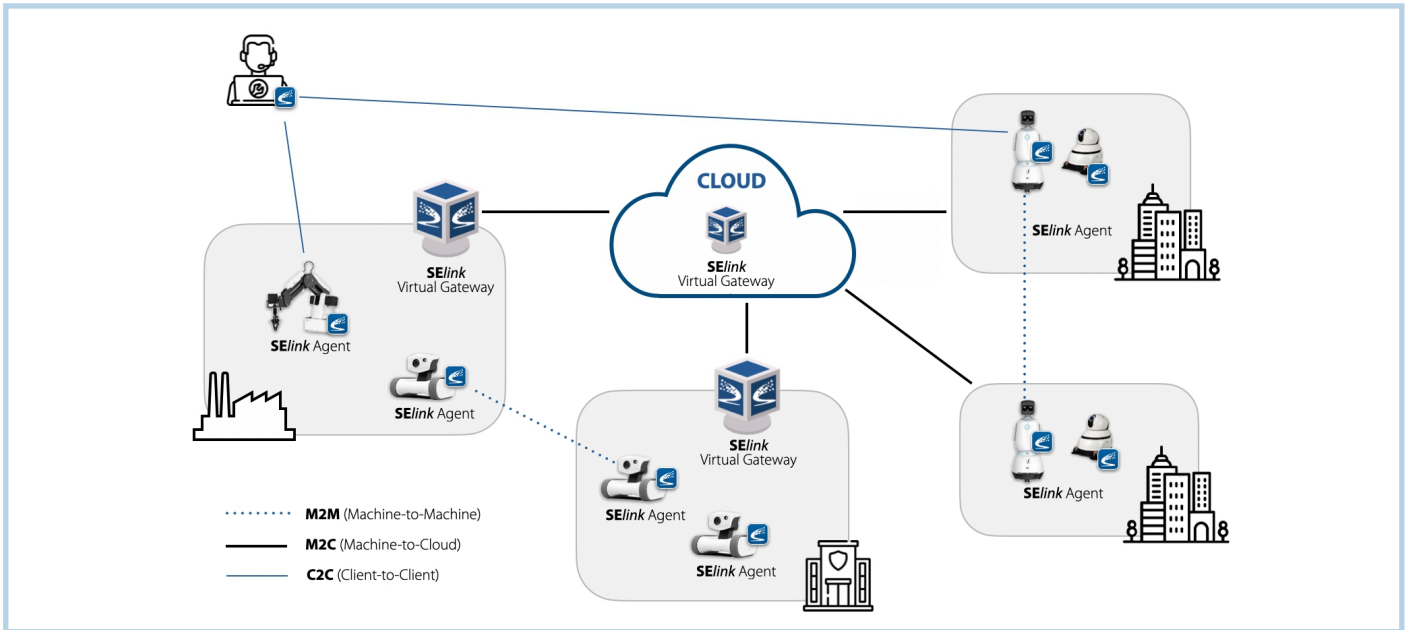
SE*link*™ is a service-oriented, secure, virtual networking solution to protect end-point and network alike. It is able to replicate heterogenous clients and server behaviours in a seamless way, as in a private LAN; when a field Robot is connected to Command Operation Center (COC) server through SE*link*™, it is virtually relocated in the same COC server LAN.

The SElink™ Gateway performs Robots "virtualisation", showing to the server the original MAC address and a unique, registered, identifier for each Robot.

The advantages are overwhelming. SElink™ protects both the data channel and the access to the communication channel, which can only be used by authorised processes. This ensures that the Command Center server is protected even in the event that the Robot is compromised, for example, in the event of a supply chain attack. Devices affected by vulnerabilities, even without vendor knowledge, are at risk of infecting the network provider with major infrastructural risks and significant potential damage. Robots would no longer need public static IP addresses to the benefit of a reduction of the attack surface. Lightweight protocols and zero encryption overhead are featured benefits of SE*link*™ as band availability and integration of security is no longer a limit. Easy to be integrated in any environment, over any protocol, portable, multi-device with the benefit of crypto-agility. Furthermore, SE*link*™ security techniques are resilient and resistant to quantum computing attacks.

Benefits

1. **Zero Trust Network Access and Assumed Breach model** strategies
2. **Lightweight protocols** for bandwidth sensitive and resource-constrained devices
3. **Zero Encryption Overhead** compared to TLS/SSL
4. **Free from third-party vendor dependancies** for the integration of security into heterogeneous devices
5. **Enhanced system longevity and resilience** to quantum attacks
6. **Seamless encryption updates, redesign-free** through Crypto agility
7. **Rationalisation of operational costs:** NO VPN, NO PKI infrastructures, NO static IP addresses
8. **Efficiency and ease of management**



Blu5 Group
info@blu5group.com
www.blu5group.com