Case Study

SElink™

Building a dynamic and scalable security posture for Smart Mobility

Background

Smart mobility has revolutionised the way we travel, integrating every mode of transportation through wireless communications and real time analytics to enhance traffic safety, comfort and efficiency. Contemporary vehicles are being modernised from an electro-mechanical motor to a complex cyber-physical system; however, this leaves them vulnerable to cyber attacks, since interdependencies can be maliciously exploited to damage each of the system components. As an expanding market valued at $34.04 billion in 2019, and is projected to reach $70.46 billion by 2027*, many companies and cities are interested in implementing intelligent networks; unfortunately, many policy makers, planners and industry leaders lack a comprehensive understanding of the cybersecurity practices and risks involved in regulating such complex technology.

Challenge

With the roll-out of electric vehicles (EVs), the EV charging demand is continuously growing and to meet this growing demand, electric vehicle charging stations (EVCSs) are being deployed for commercial and residential use. This nexus of EVs, EVCSs, and power grids creates complex cyber-physical systems. While security is front of mind when it comes to connected and autonomous vehicles, little consideration is given to the risks associated with electric vehicle (EV) charging stations. Research demonstrates that EV charging stations can be a conduit for DDoS attacks, ransomware, theft of ID, and could jeopardise the security of the power grid.

Industry

Smart Mobility
Electric Vehicle Charging Stations

Challenge

- Complex and long-lived systems of heterogeneous devices, applications, and technologies interconnected on public networks increasing the attack surface for threat actors

Goals

- Implement network virtualisation and segmentation for greater isolation and protection against supply chain attacks reaching the power grid
- Seamless security integration into multivendor devices
- Get rid of bulky and costly PKI infrastructures
- Reduce EVCS operational costs

Solution

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

Solution

EV chargers face numerous security threats that could have serious consequences. The most frequent scenario will be identity theft, data alteration, unauthorised access privileges, malware insertion, private & sensitive information theft, electricity flow manipulation and changes in operating parameters that may compromise charging stations' safety among many others. Furthermore, security lack or vulnerabilities in EVCS make it possible to launch large-scale cyber-attacks that also compromise security in the power grid.

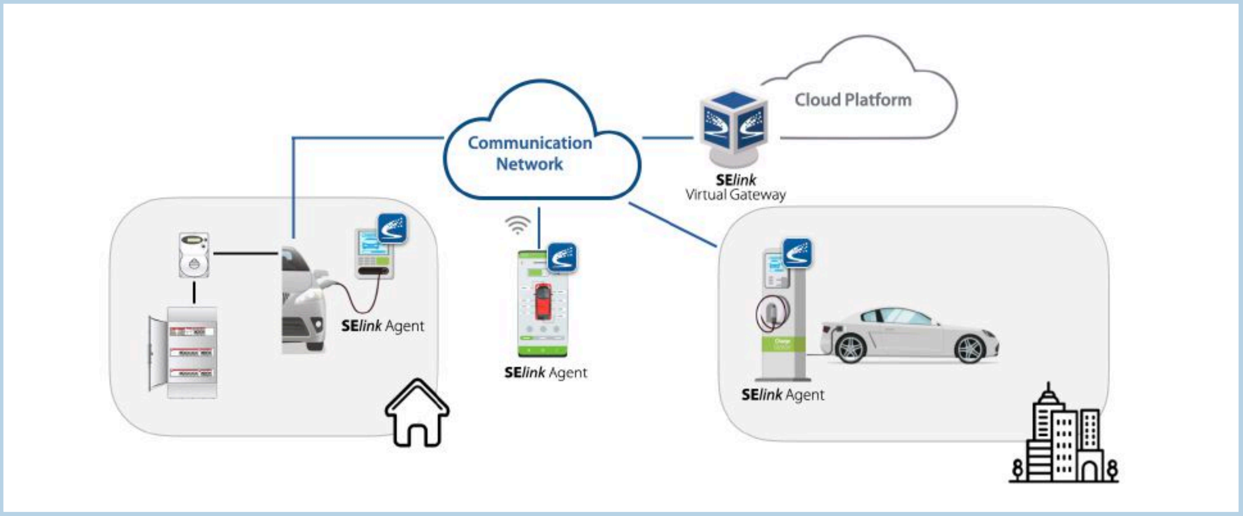
SE*link*™ is a service-oriented, secure, virtual networking solution to protect end-point and network alike. Able to replicate heterogenous clients and server behaviours in a seamless way, as in a private LAN; when an EVC Station is connected to the Charge Point Operators (CPO) server through SE*link*™, it is virtually relocated in the same CPO server LAN.

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

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 CPO server is protected even in the event that the EVC is compromised, for example in the event of a supply chain attack. Devices affected by vulnerabilities, even without vendor knowledge, may infect the network the provider with major infrastructural risks and significant potential damage. EVCs no longer need public static IP addresses to the benefit of a reduction of the attack surface as well as operational costs. Lightweight protocols and zero encryption overhead make band availability and the integration of security no longer a limit. Easy to be integrated in any environment, over any protocol, portable, multi-device with the benefit of crypto-agility, 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**


Communication Network
Cloud Platform
SElink Virtual Gateway
SElink Agent
SElink Agent
SElink Agent