Case Study

SElink™

Cyber Security Defence Model for Public Transports based on Zero Trust

Background

With the rise in vehicle volume, the transportation infrastructure continues to expand from isolated nodes to large interconnected networks of devices comparable to IT systems, offering new traffic management strategies. The rapid adoption of smart technology along with information and communication technology to transportation and traffic management systems is needed to improve the safety, efficiency and sustainability of transportation networks. Public transportation vehicles are perhaps the most-exposed component of transit infrastructure. They carry a large number of individuals and contain a constantly increasing number of different technologies (including wirelessly connected systems). Transit agencies are also deploying an increasing number of technologies outside of the vehicle, including mobile apps for fare payment and real-time arrival information, automatic vehicle location, traffic signal priority, and onboard Wi-Fi.

Challenge

Transportation Systems, steadily transitioning from serial-based to IP, are establishing intricate networks of data sources, hardware units, sensors, infrastructure and communication technologies for wired and wireless communications. The maturity and adoption of the various emerging technologies vary greatly leading to complex interconnected ecosystems of smart and legacy technologies with high vulnerability and interoperability challenges. ITS are often deployed in unattended harsh environments thus requiring reliable, secure and scalable networks to link cameras, sensors, signage, signalling and vehicles to remote data and operations centres. Additionally, the power and memory constraints of sensor nodes make conventional security solutions impractical.

Industry

Public Transport Networks and Systems

Challenges

- Integration of OT and IT systems
- Legacy system interoperability
- Remote access to OT-IT systems and services
- Control over the Supply Chain Remote Access
- Continuous monitoring and remote maintenance
- Data Protection and Compliance

Goals

- Improving the reliability and efficiency of the service, reducing maintenance and repairing time, simplifying operations while enhancing cyber resilience against security threats.

Solution

SE*link*™ provides a zero trust security model combined with service-level virtual network segmentation, granular privileged access management. Delivering efficiency, security and control to Devices and Networks with a single integrated solution.

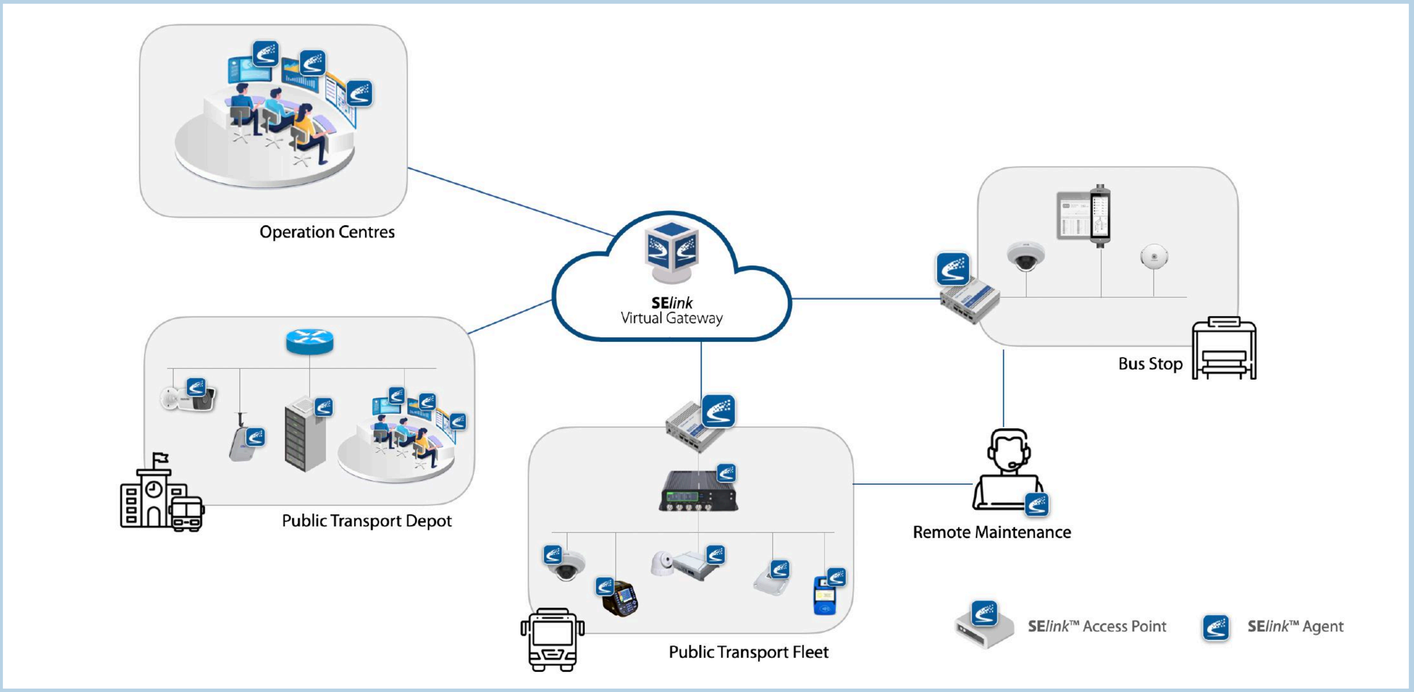
Solution

Building resilient and efficient Transportation Networks to support legacy and intelligent systems with a scalable and hybrid solution to accomodate evolving field technologies. Ensuring that the in-vehicle and infrastructure network is protected from attacks and yet efficient and fully functional. The combination of Virtual Networking and Zero trust Security strategies ensure protection from unauthorised device connections, from attacks via wireless and via compromised services.

Benefits for Resilience

1. **Zero Trust Network Access and Assumed Breach model** strategies for identity protection, authentication and access control
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 public/static IP addresses
8. **Efficiency and ease of management**

SE*link*™ is a **Zero trust virtual networking** solution for private networks, based on the **Assumed Breach model** for the **Resilience** and optimisation of distributed endpoints (vehicles, devices, sensors, users) and sites (Operations Control Centres, Suppliers). **SE*link*™** is able to replicate heterogenous clients and server behaviours in a seamless way, as in a private LAN; when field endpoints communicate with each other or send data to the Operations Control Center (OCC) server through SE*link*™, they are all virtually relocated in the same OCC server LAN. The **SElink™ Gateway performs Endpoint "virtualisation"**, showing to the server the original MAC address and a unique, registered, identifier for each endpoint. 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. **Access requests are continuously validated** for finely-tuned access to specific applications and services, compliant to endpoints' needs and privileges. **Zero Trust principles** minimise the need for traditional detection systems. **Network lockdown strategies closing all inbound ports** on each network node by default, make that **all packets** from **unauthorised client applications are dropped**. **Native anti-propagation mechanisms** prevent infection spreading in the event that devices are affected by vulnerabilities, even without vendor knowledge. This ensures that the Infrastructure servers are protected even in the event that the endpoint is compromised. Endpoints 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 for systems longevity. **Post Quantum Cryptography** ensures the highest level of security in authentication mechanisms.


Operation Centres
SElink
Virtual Gateway
Bus Stop
Public Transport Depot
Remote Maintenance
Public Transport Fleet
SElink™ Access Point
SElink™ Agent