Case Study

SElink™

Improving security and quality of real-time video transmissions in mission critical operations

Background

With the convergence of Internet technologies and broadband wireless communications, mission-critical services for emergency communications are undergoing tremendous change and growth. To be effective, public safety and emergency response organisations need strategies and capabilities to communicate, collaborate, and operate efficiently and effectively. As video becomes pervasive in many industries, mission critical activities have incorporated video as a tool to remote monitoring and control operations as well as increase efficiency. Video can be streamed from a robot, a drone, body or security camera and the timely delivery of critical imagery can be the difference between success or failure of a mission. Video systems therefore need to work in all conditions, including harsh environments. Despite mission critical ops rely on advanced sensor technology, limitations do exist in regard to available bandwidth, platform scalability, system latency and security of the entire data flow.

Challenge

Efficient and effective communications of high quality visual content with low bandwidth is a fundamental challenge. Many mission-critical communication networks cannot provide sufficient bandwidth to carry the precision of these camera sensors in real-time live operations. Video needs to be able to stream consistently and reliably to and from a host of different devices, platforms, browsers and mediums, on-premises servers or the cloud. Video footage needs to be obtained quickly and deliver critical metadata, with built-in cyber safeguards and hardening such as automatic encryption and authentication.

Industry

Law enforcement
Mission Critical Operations

Challenge

- Implement a solution offering reduced bandwidth requirements, high scalability, and a lower total cost of ownership while maintaining the integrity of mission-critical video and data

Goals

- Reduce the surface of attack across field devices, link and SOC
- Improve QoS and bandwidth consumption
- Seamless security integration and management spanning multiple platforms and devices
- Strengthen access control mechanisms for increased isolation and protection against supply chain attacks
- Keep the hardware requirements at the minimum level at the SOC and field devices alike

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

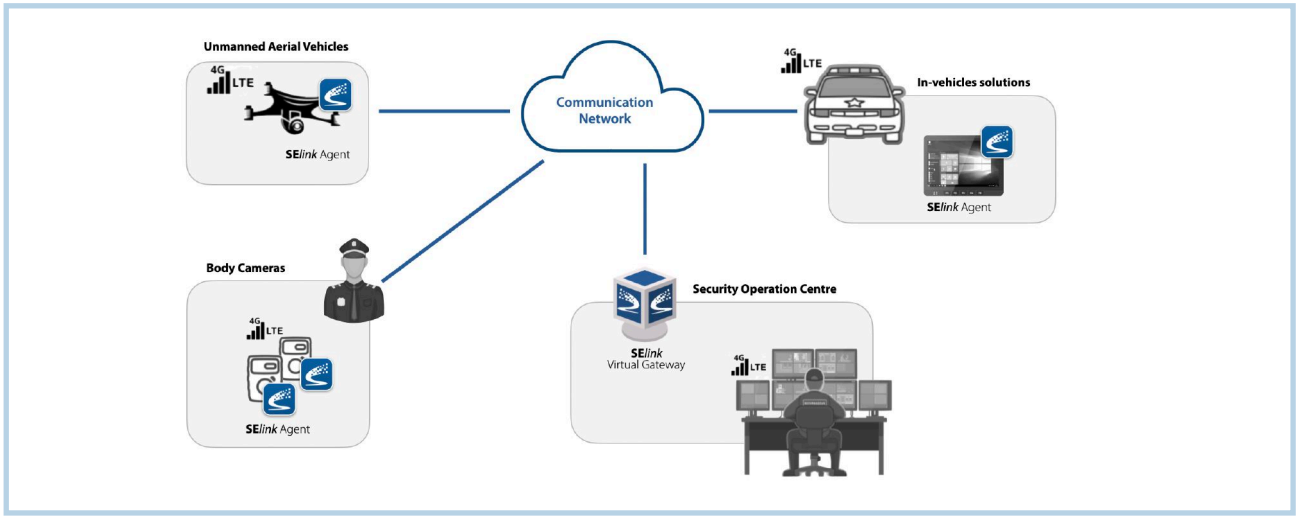
Mission critical users require enhancements on availability, reliability, security. Critical missions require remote and immediate access to data and the ability to stream securely and in real time, from cameras and devices at multiple locations to the Security Operation Center (SOC), even over a challenging connectivity environment.

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 a situation awareness device is connected to the SOC server through SE*link*™, it is virtually relocated in the same SOC server LAN.

The SElink™ Gateway performs device "virtualisation" showing to the server the original MAC address and a unique, registered, identifier for each Satellite device in the network. 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 controlled by Zero Trust Access mechanisms confining malware to its origin. This ensures that the Security Operation Center server is protected even in the event that a situation awareness field device is compromised, for example in the event of a supply chain attack. Field devices no longer need public static IP addresses to the benefit of a reduction of the attack surface as well as operational costs. SElink is suitable for use in broadcasting and multicasting, does not require special stages for network session establishment between the client and server, and is resilient to data packet losses in the network infrastructure. SElink lightweight protocols are optimised for video streaming constrained devices, where a certain degree of packet loss is possible, providing increased data transfer reliability and enhanced security properties, resilient to quantum attacks, compared to the DTLS protocol. SElink encryption techniques are fast and introduce ZERO overhead making security integration into bandwidth sensitive devices no longer an issue and resource utilisation efficient. Smart mechanisms such as automatic session recovery and packets aggregation over the same packet header prevent packet filtering from providers and improve service availability. Easy to integrate 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. **Low-bandwidth strategies coupled with smart mechanisms** to improve QoS and availability of service
4. **Zero Encryption Overhead** compared to DTLS/SSL
5. **Seamless and rapid encryption updates, redesign-free** supported by crypto agility features
6. **Rationalisation of operational costs:** NO VPN, NO static IP addresses, required
7. **Efficiency and ease of management** through network virtualisation



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