Full Stack IoT Security from Core to Edge

One of the more difficult cybersecurity challenges is protecting the Internet of Things (IoT). IoT covers everything from environmental controls to managing drones and other complex autonomous vehicles. Unsurprisingly the reliance on IoT is increasing in both defence and civilian sectors. So, why is effective IoT security a challenge and how can that challenge be met?

IoT, as its name suggests, connects a wide range of *things* or devices using IP networks. Connected IoT devices range from simple sensors or actuators, for example a temperature sensor and heating system to more complex devices such as an unmanned aerial vehicle (UAVs). In all cases the device needs to connect back to a central control point. Both the device and control point need to be protected against attack and the data transmission between the two must be protected. In this context protection means:

- Protecting the device from attack and unauthorised access
- Protecting the control point from attack and unauthorised access
- Ensuring that the control point can reliably identify and authenticate the devices it is managing
- Ensuring that the devices allow only an identified and authorised control point to connect
- Ensuring the privacy and integrity of the data exchanged between the control point and the device

The level of security required depends on the application; a UAV used in defence will have a higher-level requirement than an environmental sensor in a house, but all IoT applications need these basic security controls. Effectively implementing the controls is more complex than applying security to other network applications. This is because the security measures must apply to a range of different device types and work with variety of different application protocols.

Many IoT devices are very simple with limited processing power; even the more complex devices have constraints that restrict the ability to add security functions. In addition, a device must be managed and secured through its lifetime, from initial deployment through successive upgrades and reconfigurations to end of life.

Providing effective security for the IoT devices, the central control point and the data exchanged between them requires that security controls are implemented at multiple levels. Network level controls are needed to protect against penetration attacks and Denial of Service (DoS) attacks. Application-level controls protect against threats that misuse application protocols or exploit vulnerabilities within those protocols. Content level controls protect information flows between the device and control point. There are at least 12 different standardised IoT specific protocols and many more *ad-hoc* solutions that build on generic network protocols. An effective security technology must be able to validate any deployed protocol.

The Unicus® platform from UM Labs is designed to protect all real-time communication applications on IP networks. It has the ability to secure across all of the OSI Model Layers, set against all of the standards from network, IP application and IP content/media, with a CORE native cloud deployment and an EDGE system on a chip implementation with it is uniquely positioned deployments to de-risk from cyber-attacks over the huge attack surfaces. The Unicus Core runs in any public, private or hybrid cloud. Variants of Unicus protect RTC IOT, sensors, robotics, Drones, CCTV, Bodycam, Metaverse and ESN voice and video, which is used in surveillance, and this includes all streaming video extended reality applications.

Unicus® IoT from UM Labs secures any EDGE application that runs over an IP network with the Unicus® platform providing full-stack security for real-time communications applications. The platform's layered architecture secures at the network, application, and content levels. Feedback between the layers ensures security controls are co-ordinated across the full network stack and optimises the response to any attack. For example, if an attack is detected at the application level, countermeasures are more effective if they are pushed down the stack to the network level or even pushed out to the network infrastructure by instructing a perimeter router to block the attack at the network boundary. The application layer also controls the content layer by ensuring that data transferred between an IoT device and it's control point is validated and where appropriate encrypted. The encryption services provided by Unicus include modern Post Quantum Cryptography (PQC) algorithms to guard against a future attack by a quantum computer. See our previous article on PQC.

The Unicus application layer implements each of the protected protocols. This ensures that all operations are validated and correctly authorised. To support multiple IoT protocols, Unicus ® provides a framework to accept plugin protocol modules. Unicus ® IoT includes support for a number of popular protocols; additional protocols many be quickly added.

To meet the specific challenges of IoT, UM Labs built an implementation of the Unicus ® architecture suitable for running on low-powered systems to protect IoT devices. This implementation, Unicus ® Edge, includes the same layered architecture as the Unicus ® Core including a full implementation of the appropriate IoT protocol. Working together, Unicus ® Core and Edge ensure that all communication between the IoT device and the control point is fully authenticated and protected. The Unicus ® Core includes a provisioning service for deployed Edge Devices to manage the device's configuration. This provisioning process is fully authenticated and encrypted to ensuring that the Edge Devices are protected through their lifetime. The Unicus ® Edge Device is available as a library for integration with an IoT devices or running on a small-scale Arm or other processor protecting one or more IoT devices with limited capability.

UM Labs is at DPRTE in Farnborough on the 26th and 27th March, come and see us on stand 136, visit our website at www.um-labs.com or contact us at info@um-labs.com.