UM Labs R&D secures Nvidia's Omniverse Developments-SDK

The Omniverse SDK provides the perfect platform for developing and running applications for Cloud eXtended Reality (CXR), Virtual Reality and building digital twins, with one notable limitation; data transferred between the cloud rendering platform and the display device is not fully protected. For many applications this may be an inconvenience but for those where compliance is a critical factor this represents a real showstopper. Creating solutions for finance, defence, healthcare, critical communications or other industrial applications means these challenges need to be appropriately addressed.

UM Labs, a UK R&D group with experts in defence (war tested) and many years of technology in cyber PIA (protect, intercept, archive) policy by design, has created the UNICUS® innovative platform specialising in protecting real time communication on IP networks, addressed all layers of IP and the proactive problems solving that protects data in transit with strong encryption up to Post Quantum Cryptography (PQC) level and provides full-stack security for both display devices and CXR servers, whether hosted on any cloud platform, private data centre servers or on-premises local server.

The solution, *Unicus® CXR,* provides a high performance, low latency, security capability provided as two components: Unicus Core and Unicus Edge. Unicus Core runs as a virtual machine instance in the same cloud as the Nvidia cloud rendering servers running CXR SDK. Unicus Edge can run on a suitable client device or a system on the same local network as the client device. Together, Edge and Core ensure signalling traffic, responsible for session setup and management, and the media streams carrying audio and video traffic are fully encrypted. This includes protecting the key exchange process for setting up media encryption keys. Unicus Edge and Core also ensure that CXR clients and servers are fully protected from attack. A single Unicus Core can be scaled to manage multiple connecting clients and to protect multiple back-end servers, all while achieving low latency and high performance. A flexible deployment model allows each client to have its own embedded Edge functions, or a single standalone Edge device may protect multiple CXR clients on the same local network.

While developing a 5G Network Showcase for Belfast City Council, BT identified the need to address problems with its CloudXR application. Specifically, the challenges of how to protect the media and signalling flows associated with the application and how to overcome the Network Address Translation (NAT) used in the 5G network path. Rejecting conventional VPN solutions, BT selected the UM Labs *Unicus® CXR* technology to provide the high performance, low latency, security solution necessary for the application. In the deployment, BT developed a CXR application using Nvidia's Cloud XR SDK to show past present and future views of Belfast City. The application running on iPads, overlays extended reality views in the *City Speech* and *City Streets* section of City Hall's visitor exhibition. Connecting over BT's 5G network to an AWS wavelength zone to provide low latency connections, cloud rendering is processed in AWS running on Windows servers equipped with Nvidia A10G Tensor Core GPUs.

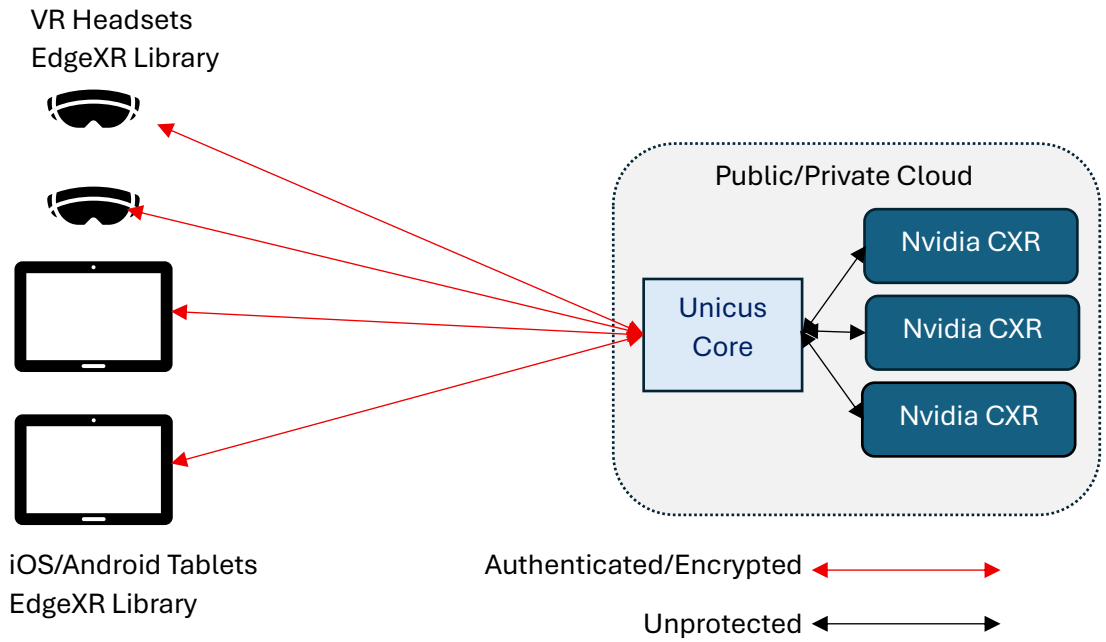
Tests by BT confirmed that the UM Labs technology provided the level of security needed for deployment of their CXR application in locations with elevated security requirements, solved

the problem of NAT and far-end NAT traversal and did so without adding latency to the video streams.

Janet Burns, BT's Business Development Director, commented: *The trial of this immersive experience is a fantastic example of how to use wireless connectivity so that people can see it, touch it, feel it and understand it. UM-Labs an Innovation Martlesham partner has provided the unique Unicus Core and Unicus Edge data in transit cyber security that secures all of the IP network, applications and content/media across the 5G network and using the NVIDIA/AWS in cloud deployments.*

Implementation was straightforward. Unicus SVSS core was installed in BT's AWS wavelength zone and configured to manage connections from multiple iPad clients and relay those connections to multiple Windows servers running the CXR service. A single instance of Unicus SVSS is able to support multiple servers and relay client connections to those servers. Each connecting client required a dedicated server. A simple broker service managed the client/server mapping. Adding the Unicus SVSS core required no changes to the CXR server application.

BT chose iPad client devices for the Belfast project, UM Labs provided the Unicus EdgeXR library to link with BT's application on iOS, but similar libraries are available for Android and other operating systems to enable the use of a range of tablets and headsets.




```
import ARKit
import EdgeXR
:
:
edgexr_init()
```

Unicus Edge was provided as a library linked to BT's iOS application. This required only a 2-line change to the client application; to import the library definition and to initialise the library. The Edge library manged all connections to the CXR servers in the AWS cloud. Each connection request was authenticated using mutual certificate checks and the RTSP signalling encrypted using TLS ensuring that the key exchange for media encryption was fully protected. The BT project used traditional algorithms (RSA, Elliptic Curve), but PQC algorithms meeting FIPS 203 and 204 standards may be used.

Unicus SVSS core provides a management interface to monitor and configure the iOS clients, to provide provisioning and to provide certificate management using an integrated Certificate Authority backed by any suitable root CA.