Unicus™ A Cybersecurity Platform for Real-Time Applications on IP networks

UM Labs
2-6 Boundary Way
London
SE1 8HP

The Unicus™ Platform

The Unicus™ was designed by UM Labs as a basis for providing security for real-time communication services on IP networks. The platform was initially conceived as part of an R&D program to secure audio and video calls but has now been applied to addressing other security requirements including streaming audio and video from surveillance cameras, body-worn cameras and drones. The Unicus™ platform secures communication on any IP network including 5G and in future 6G networks. The flexibility in the Unicus™ architecture enables both *Core* and *Edge* deployments. This means that Unicus™ meets current and future needs in defence, government and commercial sectors. Unicus™ can secure static networks, such as an organisation's connection to the global fixed line and mobile phone network and enable the rapid deployment of dynamic networks using technologies including private 5G to respond to emergency situations.

This white paper shows why Unicus™ is needed, outlines the Unicus™ architecture and demonstrates how Unicus™ will meet future needs.

Background

The 21st century has seen significant advances in the network applications and services used by both businesses and consumers with a focus on the development and deployment of real-time communication (RTC) applications. There are now multiple providers offering on-line voice and video conferencing services; phone companies are migrating their networks to provide IP delivery and in doing so are offering a broader range of services. IP networks are now used for live streaming from both static and mobile surveillance cameras. Live streaming from body-worm cameras and from drones significantly improves the timeliness and increases the value of the feed. The trend is continuing, innovations such as Metaverse and IEEE's work on the Hyperspace Transaction Protocol (HSTP) which is intended to deliver connectivity to drones, robots and other smart devices are just two examples.

The successful deployment of real-time services and the security and integrity of the information transmitted is highly dependent on effective protection against cyber security threats. The complexity of the protocols driving the applications and the real-time requirements means that specialist controls are required to provide effective protection and to safeguard the information assets. The Unicus™ platform from UM Labs implements a unique layered architecture to secure the applications in current use and is extendable to incorporate future applications.

Protocol Development

The protocols used to drive the newer generation of network applications and services are more flexible and more complex than those used in the early years of the Internet. Back then popular applications included web and email. While these applications are still widely used, newer services have required the development of other protocols.

Web and email follow a simple client/server model, a client (web browser or email application) connects to a server and requests information from or sends information to the server. The interaction is initiated by the client. With applications such as IP telephony, this client/server model breaks down. A phone, whether it is a hardware device on a desk, a smartphone or a software application is both a client and a server. A client when you make an audio or video call, a server when someone calls you.

At the network level, the operation of the early protocols was relatively straightforward. Servers listened for incoming connections on a *well-known port*. A port is simply an identifier so that the underlying operating system can route an incoming connection request to the appropriate application service. Email uses the SMTP protocol which has been assigned port 25. Web services use port 80 for HTTP or 443 for encrypted HTTPS connections. By adopting a standard set of ports, multiple application services can run at a single network address and an application client can request a connection to any appropriate application server.

Newer protocols, particularly those delivering audio/video media streams do not adhere to this model. While protocols such as the Session Initiation Protocol (SIP) use a well-known port (5060 for clear-text or 5061 for encrypted connections), this port is used only for call set-up, call termination and other control functions (signalling). Media streams, audio and video, use dynamic ports set up via SIP using an intermediate protocol, the Session Description Protocol (SDP). Each active call requires at least two media ports while video calls will use more. Other protocols such as RTSP and RTMP for streaming video use a similar approach.

Legacy Security Technology

When the Internet became widely available and attacks on Internet connected systems meant that security controls were needed, the answer was to deploy a firewall. Firewalls are still in widespread use today and play an essential role in securing Internet connected systems, but their architecture was designed to work with *firewall friendly* client/server applications running on fixed ports.

At a fundamental level, firewalls work by limiting access to the well-known ports used by applications, for example allowing access to a web server but blocking everything else. There are a number of methods to implement these security controls, port filtering, stateful packet inspection, proxies and others. Products described as next generation firewalls have additional functions but still rely on the same basic technology. While this approach can handle applications using a single fixed port, it does not provide the same security for applications using multiple ports. As an example, a firewall handling traffic for a SIP system built to support 1,000 active calls would require at least 2,000 open ports and possibly many more. A large number of open ports reduces the effectiveness of the firewall's security controls.

Firewalls operate at the network level examining the source and destination of each packet in a data stream. This limits their ability to detect attacks operating at higher levels targeting the application protocol or data content. For most firewalls, attacks at these higher levels are indistinguishable from a valid request. For example, a request to stop a streaming video session, which would be a very effective attack against a static or mobile surveillance camera, will pass through a firewall as the bogus request uses a valid protocol request over the same channel as the request to start the stream.

The firewall security model makes allow or block decisions for each packet in a data stream, this does not provide protection for data relayed by the firewall. To overcome this limitation, VPN technology with integrated encryption is implemented either as an option on the firewall or as a standalone service. VPN technologies that provide encryption include IPSec and SSL VPN. Other VPNs such as MPLS do not offer encryption as part of the core protocol. While VPNs protect a data stream, there are very blunt tools to use with real-time applications. On a connection carrying multiple audio/video calls or multiple surveillance feeds, all sessions will be encrypted with the same key (keys may be refreshed at intervals). A compromised key will leave all sessions exposed.

A better solution for protecting real-time data-in-transit is the Secure Real-time Transport Protocol (SRTP). With SRTP new keys are negotiated for each media steam. An audio-video call will have at least 4 keys, one for each transmitted and received audio stream and one for each video stream. In the unlikely event of a key compromise, the exposure is limited. SRTP also authenticates every audio or video packet transmitted to protect against media injection attacks. Finally, SRTP is optimised for real-time operation, it will tolerate a low level of packet loss which does not affect the audio or video quality rather than requesting a re-transmission which will introduce latency.

Network Address Translation

Network address translation (NAT) is used on virtually all networks. It separates the address space on public and private networks and operates by translating the network addresses used on data steams as they pass between public and private networks. NAT is a standard feature of firewalls. Unfortunately, NAT complicates the deployment of real-time applications. Some firewalls attempt to address this problem by adding *SIP Aware* features for IP telephony and similar features for other protocols. These features, collectively known as Application Level Gateways (ALG) are often unreliable and create more problems than they solve. This has become such an issue that the UK's NICC recommend against the use of SIP ALGs (NICC, 2017).

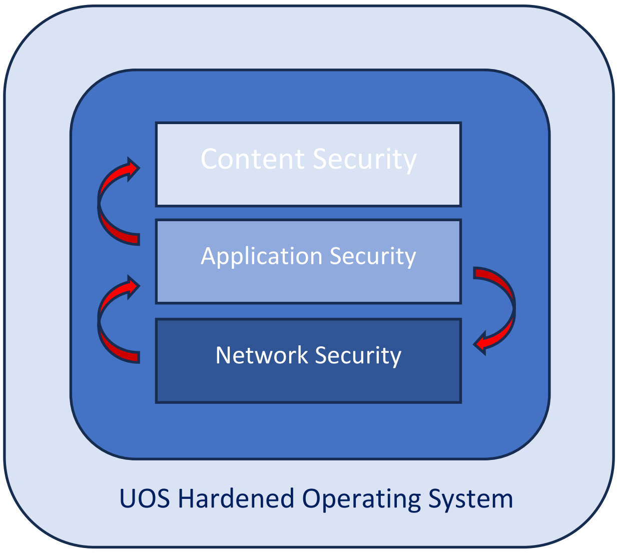
The Unicus Platform

The complexity of the newer application protocols and the limitations of legacy security technology leaves the services provided by those protocols at risk of attack unless specialist security controls are implemented. There are many examples of the consequences of a successful attack including Distributed Denial of Service (DDoS) attacks on multiple UK IP telephony service providers (Wright, 2021), and multiple fraud attacks leaving providers with significant costs. The Communications Fraud Control Association estimated that global losses resulting from fraud were almost $40 Billion (CFCA, 2021),

To combat this threat, UM Labs developed the Unicus™ platform. Unicus™ is designed to provide security at multiple levels (network, application and content) and to combine the security controls at those levels into a single policy management system. This ensures that the security modules at each level are co-ordinated, and avoids the challenges of attempting to set up separate firewalls and higher-level security controls while providing elevated security.

Unicus™ implements feed-back between the security layers. This feedback is bi-directional, with lower layers providing configuration information to higher layers and higher layers pushing static and dynamic security controls down to lower layers.

The network security layer is responsible for controlling connections to and from the system. This layer operates as an IP firewall but differs from standalone firewalls in that its configuration is derived from the security policy; there is no requirement for manual configuration. The network security layer also collects information about the system's network connections and feeds that information up to the application security layer where it is used to ensure correct operation of the supported applications and their underlying protocols.



The application security layer is responsible for controlling the operation of the protocols driving the secured applications. Details will depend on the applications supported. For Internet telephony the protocols are SIP and a number of related protocols, for streaming video they and RTSP and a set of related protocols, some of which are shared with Internet telephony. In all cases the application security layer is a full implementation of the protocol which enables complex application-level attacks to be detected and blocked.

When the application layer detects a threat, it can block the threat at that level or push the blocking action down to the network level. If Unicus™ is running in the cloud, the blocking action may be pushed to the network perimeter using APIs provided by the cloud service. Blocking a threat as early as possible limits the impact of that attack.

As the application security layer understands the application protocol it is able to validate every request. This check operates by maintaining state information on every active session (e.g. phone call, streaming video session). With this information, an attempt to disrupt a session is immediately detected and can be blocked. When a new session is permitted, the application security layer pushes session details up to the content security layer so that the session data can be relayed. The state information maintained by Unicus™ is not related to the state maintained by *stateful packet inspection* which is implemented by many firewalls. Stateful packet inspection attempts to correlate between individual network packets and operates over a period time measured in seconds. The state maintained by Unicus™ relates to an entire session, for example a phone call or video stream. A session could last many hours.

The application security layer and the content security layer cooperate to provide data-in-transit protection. The exact mechanism depends on the protocols and application in use, but typically means providing encryption on a session-by-session basis and ensuring that every network packet accepted or forwarded is checked and is part of a previously authorised session.

The encryption service provided by Unicus™ applies to both session set-up (signalling) and the transmitted data (media). The terms signalling and media originate from the telco world but are equally applicable to all real-time communications protocols. The method used to protect signalling and media depends on the protocols in use, but typically signalling is protected with Transport Level Security (TLS) and media is protected with Secure Real-Time Transport Protocol (SRTP). TLS is widely used including protecting access to web sites such as on-line banking and other financial services. TLS supports a wide range of encryption algorithms, the most commonly deployed for RTC services is the Advanced Encryption Standard (AES). TLS includes mechanisms to securely establish and exchange session encryption keys used to protect transmitted data. Unicus™ can optionally add additional security to this process through the use of an external Hardware Security Module (HSM) where master keys are stored, and elements of the processing needed to establish a TLS session are completed.

SRTP is designed specifically for protecting real-time media flows. It too uses AES for data encryption but relies on an external key exchange mechanism to set up session keys. Unicus supports all commonly used key exchange protocols plus some less frequently used options providing a higher level of security.

Unicus always generates new session keys for each new connection and each new media stream (video session or a call). Session keys are never retained ensuring perfect forward secrecy.

The media encryption services on Unicus™ are implemented as multi-threaded module taking full advantage of modern multi-core hardware. This implementation ensures that on a correctly configured virtual machine or hardware platform, the latency introduced by the encryption services is maintained below 20 µ seconds (approx. 1000th of the normal acceptable latency budget).

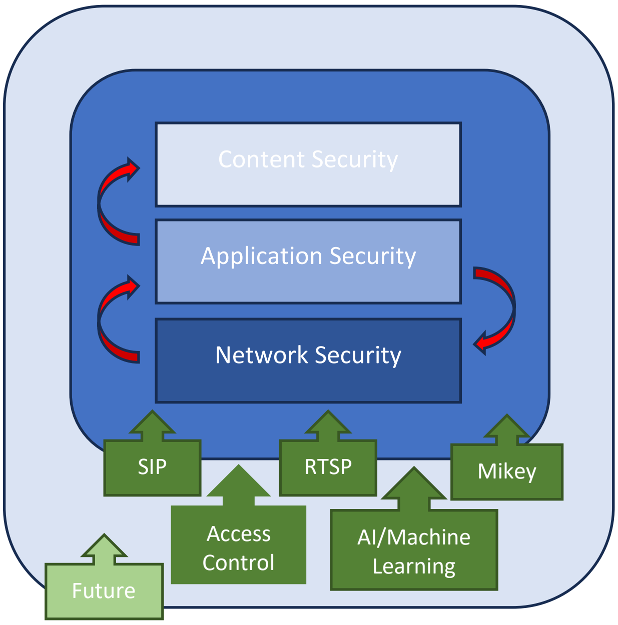
Firewalls and NAT

The network security layer in the Unicus™ platform provides the functions normally implemented by a firewall. This includes both NAT traversal (managing information flow through a local NAT gateway) and Far-end NAT traversal (managing information flow through remote NAT gateways, for example connecting to devices on 4G/5G networks). The network security layer protects both the applications in use and Unicus™ itself. This means that there is no requirement to install a separate firewall. However, recognising that most organisations have a strict policy on using firewalls on all network interconnections, Unicus includes features which enable it to coexist with a firewall while avoiding the complexity of managing two separate systems.

Quantum Safe Cryptography

Unicus™ employs both symmetric key cryptography where the same key is used to encrypt and decrypt data (for example AES) and asymmetric key cryptography which requires a public key and private key (for example RSA and elliptic curve). Asymmetric key cryptography is used by TLS to set up new connections and to establish a symmetric key for encrypting bulk data. The asymmetric algorithms in use today are vulnerable to attack using Shor's algorithm (Shor, 1994). Shor's algorithm requires a quantum computer. Suitable devices do not yet exist, but there is a risk that encrypted communication sessions recorded today could be decrypted in the future when quantum computers capable of running Shor's algorithm are developed. Information which needs safeguarding for an extended period is at risk.

To combat this risk, Unicus™ includes a number of quantum safe asymmetric encryption algorithms. These are the result of extensive analysis by NIST (NIST, 2022). These algorithms are available as a zero-cost option for Unicus and protects all cryptographic functions from future attacks.



Protocol Standards

Unicus secures applications running protocols defined by recognised standards bodies such as IETF, ITU and IEEE. The use of standards ensures that Unicus can protect application service from any standards compliant vendor.

Application Modules

Unicus is designed to be extendable to provide security for new applications and protocols as they are developed and deployed. The layered security architecture provides a framework where new modules may be added to the system to provide support for a new protocol. The protocols needed to secure IP telephony and streaming video (SIP, RTSP and others) are implemented as modules, modules are also used to provide supporting services, for example Access Control, Machine Learning and key exchange protocols.

Edge/Core Architecture

The Unicus™ platform offers both core and edge deployments. Unicus™ core systems may be deployed in any public or private cloud, while edge devices are deployed at the network edge protecting devices capturing real-time data. Some applications, such as audio/video calls using SIP require only a core system as the end-user devices (phones) have enough local security controls to enable a secure connection to the core. Other applications such as streaming video use much simpler devices which lack local security functions. IoT devices have a similar limitation. An edge device provides the missing security functions enabling a secure connection to the Unicus core. Edge devices are configured and managed by the Unicus™ core. Together the edge and core ensure a secure communication channel for data-in-transit and provide security for the data collection devices. Both core and edge devices use the same layered architecture and incorporate the same level of security including support for quantum-safe encryption. Edge devices may be deployed on small scale Intel or Arm hardware, as software modules on a smartphone or may be delivered as a tool kit for integration into an existing device, for example a camera or drone. When the edge operates on a hardware device it will communicate with data collection devices on a personal area network. For static cameras this could be a wired connection, for mobile devices wireless is more likely. The ability to deploy on a low-cost standard hardware device means that the edge device can be combined with other functions including setting up private 5G network to provide secure communication between devices and a link back to a central location.

Recording and Archiving

The ability to record and archive communications is, for many, an essential component of a secure communications network. In many sectors there are regulatory requirements for recording communications and for archiving those recording for several years. Unicus™ provides policy-driven recording. Selected sessions may be tagged for recording depending on the source and destination of the session. Unicus™ does not provide archiving but can upload completed recordings to a selected 3rd party product or service.

Unicus Today

Unicus™ is currently available in two versions, Unicus™ RTC which secures IP telephony services using SIP and replated protocols and Unicus™ SVSS which secures streaming video services using RTSP, RTMP, ONVIF and related protocols.

Unicus Benefits

Unicus™ offers a unique solution to the challenge of implementing and securing network applications. Unicus is the only available solution which provides integrated full-stack security for a growing range of real-time communication applications. Alternative approaches, building a similar set of capabilities with a set of separate component products cannot match the Unicus™ architecture because they will lack the close integration of the security controls and will be unable to benefit the feed-back between the security layers that which is at the core of the Unicus™ design.

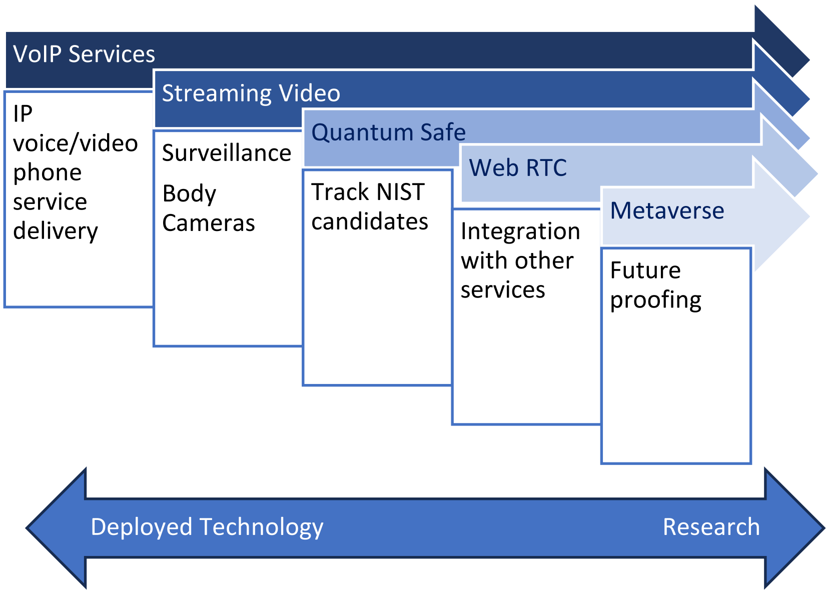
Feature	Benefit
Hardened Operating System	Complete system, easily installable in any public or private cloud
Layered Security Architecture	Co-ordinated security over the complete stack, avoiding the need to configure multiple products.
Zero-trust architecture	Validates *all* protocol requests, regardless of origin
Feedback between layers	Provides a level of security not possible when using multiple unrelated security point solutions; enhances efficiency of response to attack
Policy driven configuration	Lower-level security controls derived from defined policy, avoiding the complication of coordinating configuration across multiple systems
Service request authentication	Ability to authenticate *all* application requests using local or third-party database (Radius, LDAP, Active Directory).
Data-in-transit protection	Protects confidentiality and integrity of all session management and media data
Modular Architecture	Ability to adapt to new applications as they are developed.

Feature	Benefit
Public or private cloud deployment	Fast and flexible installation with ability to dynamically adapt to fluctuating loads

The Unicus™ architecture together with these operational benefits is the reason that Unicus™ was chosen to secure real-time services in carrier, government and defence deployments.

The Future

The Unicus™ road-map will see the continued development of additional protocol modules to support the next generation of real-time communication network applications. The ability to quickly add new protocol and application modules to the Unicus™ platform and have those new modules benefit from full-stack security makes Unicus™ the preferred choice for securing real-time applications in all government and business sectors. Our research program includes potential strategic technologies such as Metaverse and at a tactical level we are extending our quantum safe cryptography from VoIP services to streaming video and researching options for securing SMS services over IP networks.



The current and future capabilities of Unicus™ deliver an unrivalled security capability as no other single product is able to match the layered security architecture and to provide a migration path to offer the same level of security to new protocols and applications as they are developed. Unicus™ operates in a rapidly developing market. IP based telephony services (secured by Unicus™ RTC) are a relatively recent innovation in the delivery of communications services that have a history of over 100 years. This market is volatile, established services are challenged by new network applications that operate under a different paradigm. Zoom, Google Meet and others are dominating the conferencing market while Microsoft Teams is a significant threat to established telecommunications providers.

In a rapidly evolving ecosystem, any security investment must be able to address both current and future needs. UM Labs' committed research program ensures that Unicus™ can meet future needs protecting end-user investment and assisting service providers in the drive to establish new markets.

References

CFCA. (2021). *Communications Fraud Control Association – Fraud Loss Survey Report 2021*. Retrieved from https://cfca.org/wp-content/uploads/2021/12/CFCA-Fraud-Loss-Survey-2021-2.pdf

NICC. (2017). *Guidance for the use and secure implementation of*. Retrieved from https://niccstandards.org.uk/wp-content/uploads/2019/03/ND1440V1.1.1.pdf

NIST. (2022, July). *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*. Retrieved from https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Shor, P. (1994). *Algorithms for quantum computation: discrete logarithms and factoring*. Retrieved from IEEE Xplore: https://ieeexplore.ieee.org/document/365700

Wright, T. (2021, September 6). Retrieved from Unified Communications: https://www.uctoday.com/unified-communications/3-uk-voip-providers-hit-by-ddos-attacks/