Applying GDPR to data-in-transit, the need for enhanced cybersecurity

UM Labs R&D

GDPR and the Security of Network & Information Systems Regulations (NIS) which are part of the UK government's National Cyber Security Strategy are highlighting the need to ensure that information processing assets are protected. However, most of the attention is on traditional data processing, information stored in databases and used by applications such as CRM and ERP, data at rest. Developments in communication technology have exposed information exchanged over real-time communication services to a higher level of security risk. Protecting these services should be high on the agenda. This white paper from UM Labs R&D highlights the risks and outlines a solution.

Regulatory Background

The growing incidence of security failures and the loss of personal data has generated a raft of more stringent and comprehensive compliance regulations. When compliance is discussed, most people think of protecting names, address and credit card details in static databases. This is important, but it is equally important to protect data-in-transit. Data-in-transit includes voice and video calls and Instant Messages. The European Union's General Data Protection Regulation (GDPR) places requirements on all data processors to protect personal data. The European Union Agency for Network and Information Security (ENISA) specifically include calls and IM within their definition of data processing.

Article 24 of Regulation 2016/679 (GDPR) establishes a requirement that service providers:

1. Take appropriate technical and organisational measures to protect the transmission networks and the services provided.

2. Take the appropriate steps to ensure the integrity of networks, and report to the authorities the security breaches with significant impact on the operation of networks.

These GDPR requirements were based on earlier directives issued by the EU, specifically directive 2001/21/EC, and reference article 13a of that directive.

ENISA has engaged national regulators from the different EU Member States in a number of meetings and workshops to develop a technical guideline concerning these security measures, called: Technical guidelines for Minimum Security Measures. These guidelines provides guidance to National Regulatory Authorities (NRA) on the technical details of implementing paragraphs 1 and 2 of Article 13a: how to ensure that providers assess risks and take appropriate security measures”

Paragraph SO11 (Security Objective 11) of the ENISA guidelines specifies requirements of access and control for a multi-level protection.

Communication Services

There is little point in investing in security technology to protect back-end databases if your business relies on poorly protected communications services. Most business are using IP based phone systems, now Unified Communications platforms either on premise or from a cloud service (UCC) these come from vendors such as Cisco, Microsoft, Avaya, Mitel, Unify and others. An increasing number of these

systems rely on IP networks for phone service delivery and connection to global phone network. The trend to extend these systems to provide services such as video and IM and to integrate them with back-office applications to provide an Enterprise set of applications as is TEA (Telephony Enterprise Application).

One of the benefits of IP based phone or UC system is its flexibility, for example enabling remote and roaming users from smartphones to connect into the corporate service. Many IP phone and UC systems are installed without adequate security controls, particularly where there are connections to external services and remote users. Securing the protocols and applications which drive these systems is a complex task which cannot be addressed by applying the same security controls used for an email system or website. Without adequate security, phones and UC systems are open to a range of attacks including unauthorised call monitoring, call hijacking, password recovery attacks and sophisticated denial or service attacks.

Deploying and IP based phone or UC system without adequate security fails to meet Data Protection (GDRP, NIS, California Consumer Act 2018) requirement of *taking appropriate technical and organisational measures* to protect data in transit.

Data in Transit

Data in transit, is data actively moving information from one location to another, such as across the internet or through a private network or VPN. Applying security measures to data in transit protects that data while it's traveling from network to network or being transferred from a local storage device to a cloud storage device – wherever data is moving its vulnerable, effective data protection measures for in transit data are critical as data is often considered less secure while in motion.

UM Labs R&D provides the essential security needed to protect data-in-transit and assist in ensuring that your data processing meets the growing number of data protection compliance regulations. One of the key technologies is the ability to encrypt (defence level-HSM, AES 128 or 256-Mikey Ticket frame) that data.

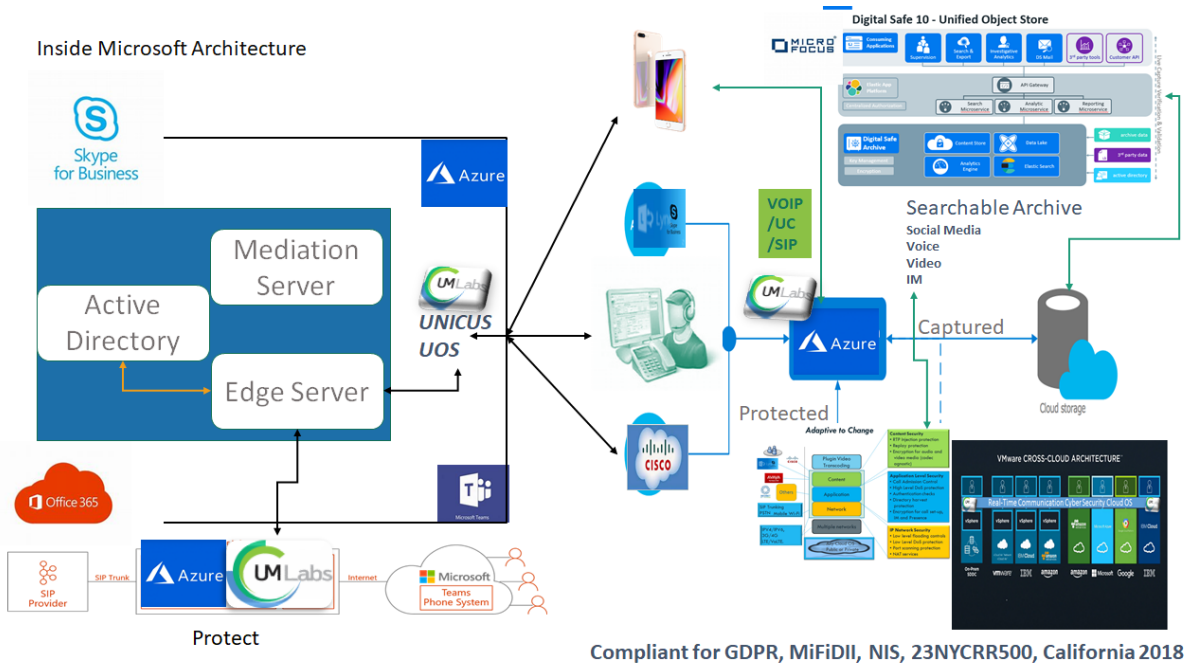
Meeting the complete set of compliance requirements is not straight forward. Some regulations such as Europe's GDPR and The California Consumer Privacy Act of 2018 from the USA call for encryption, while others such a MIFID II, 23NYCRR 500 require the recording of communications. Organizations may also need to implement call/video/IM recording to meet internal audit requirements. Data in Transit recording, and encryption cannot be combined without adding additional layers of complexity. Complexity is always the enemy of good security.

Encryption

The obvious technology to protect data in transit is encryption; GDPR recommends its use. Encryption is a fundamental component that helps ensure confidentiality of workloads and in the cloud, this becomes crucial to help with protection. As an example, Microsoft Azure provides customers with several offerings to manage and control the security of customer data, including the means to encrypt all of the following:

- Data at rest
- Data in transit
- Data during processing

Services such as Azure provide a range of encryption technologies for data protection, including the use of VPN technologies for data in transit. While VPNs are widely used, they offer a generic capability and were designed for non-real-time applications such as database updates and web services.



While many may view web services as a real-time application, the reality is that an acceptable response to a request is measured in seconds, while a real-time communications service must deliver data with a latency measured in milliseconds. As an example, a simple audio call transmits 50 packets per second in each direction. Applying encryption to protect the data transmitted by RTC services requires a custom designed approach rather than relying on a generic approach. Many RTC deployments have not implemented encryption making them an attractive target for an attacker.

The risk profile for data in transit or data at rest depends on the security measures that are in place to secure data in either state. Protecting sensitive data both in transit and at rest is imperative for modern enterprises as attackers find increasingly innovative ways to compromise systems and steal data.

RTC Services

The migration of Real Time Communication (RTC) services to IP networks brings those services within the data processing realm and makes them subject to the same data in transit and data at rest compliance regulations. In Europe, the General Data Protection Regulation (GDPR) and in the USA, California Consumer Act 2018, specifically applies to voice, video and Instant Messaging use. GDPR requires that all personal information is protected and strongly recommends the use of encryption to protect both data in transit and data at rest. Other compliance regulations, for example the European MIFID-II regulation, the New York 23NYCRR500, California Consumer Act 2018 and NIS Directive require that all communications within selected segments of the financial service industry are legally recorded. Combining this requirement with GDPR's recommendation for encryption is a challenge but can be delivered through an end to end service. Meeting the challenge requires a new approach; one which is able to protect against the threats facing phone and UC services, which provides the

technology needed to meet current regulatory requirements and which can support the trend towards cloud computing.

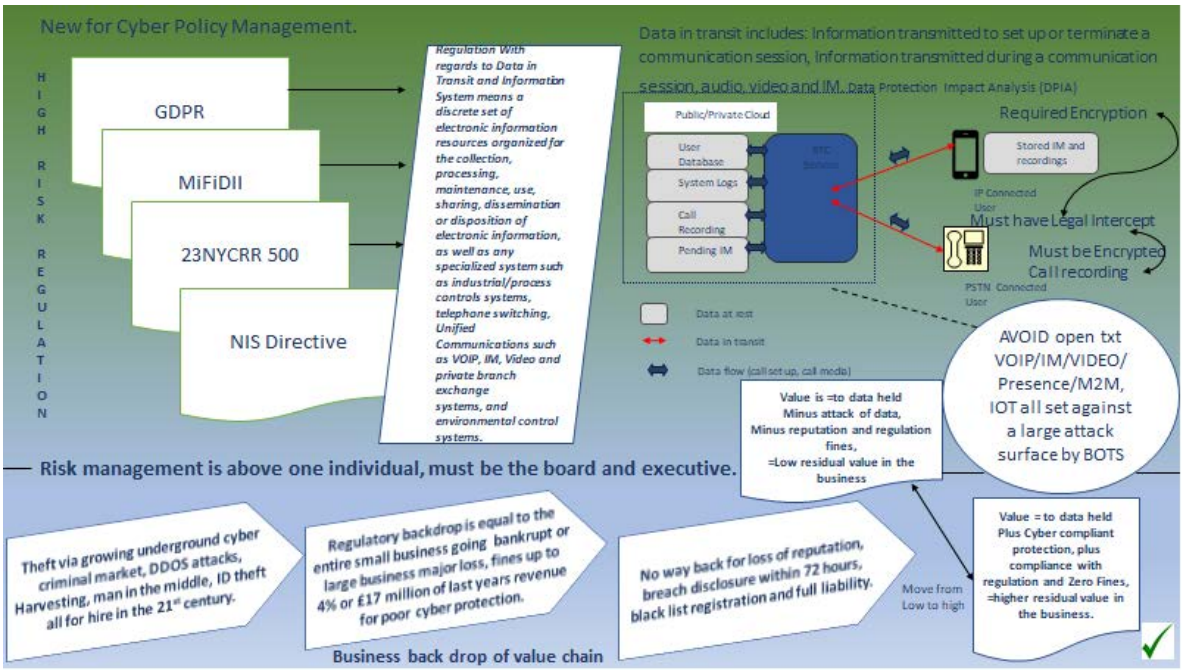
Unicus from UM Labs R&D

Unicus™ is the UM Labs R&D solution for securing RTC services and protecting data in transit. Unicus is centred on UOS, a hardened operating system serving as a platform for the cyber security controls needed to secure RTC services and meet new and existing regulatory requirements. The system runs in any public or private cloud providing a security protecting any standards based RTC service including voice, video and Instant Messaging.

UM Labs R&D addresses both data protection requirements which promote the use of encryption, and regulatory requirements which specify call recording by implementing industry standard encryption protocols designed specifically for RTC and combining those protocols with proven encryption algorithms such as AES. The protocols and algorithms are widely implemented in smart-phones, tablets, laptops and in many IP phone handsets. The encryption protocols work by generating a new set of encryption keys for each call. The keys are discarded at the end of the call. A number of key exchange protocols to securely generate and set up these keys are supported. This includes the use of specialist Hardware Security Modules (HSM) for use where a higher level of crypto security is needed. For all the supported protocols, the UM Labs system participates in the key exchange and is therefore able to record the resulting call where needed.

Selective Archiving for Legal intercept and compliance

Unicus uses a policy engine to select the data in transit (voice/video/ IM) sessions for archiving. All calls including encrypted calls are selected for archiving. RTC Cyber Security UOS is able to process encrypted calls because it controls the call setup and participates in the protocol used to exchange the encryption keys for the call. Archived calls are processed to produce a playable recording; this recording is then uploaded, as an example to Micro Focus Digital Safe or Retain Unified Archiving over an encrypted connection.



Data in Transit Retrieval

The archived voice, video, and IM data is accessible by end users and administrators directly through the Digital Safe or Retain user interface, an email plugin, or the Digital Safe/Retain mobile archive app. End users can access and search their personal archive, administrators, or other named users can access, search and perform eDiscovery on the entire Retain archive. This enables your organization to quickly access, search, and audit the encrypted archived data.

Digital Safe/Retain includes built-in eDiscovery tools that allow you to easily search all data stored in the archive, place litigation holds, print, forward, save, redact, and export archived data. Digital Safe/Retain enables regulatory compliance with MiFID-II, GDPR and other regulations through secure encrypted archiving, data access control, the audit trail (enabling you to have record of all activity), WORM storage, quick and easy access and search of the archive, and mailbox and messages deletion (fulfilling the “right to be forgotten”)

Overall, today’s legacy point solutions cannot mitigate attacks on multi-levels, encrypt to different levels and as Data in Transit attack surface is large enough to have many holes in defences, it is clear a new approach is required and fast as the risk to the organisation’s residual value becomes a major problem for all CISO’s. The R&D done and actioned by UM-Labs R&D and partners, brings a service offering which can be implemented and delivered quickly at a ROI level which reduces the risk profile.

Contact -Marketing@um-labs.com

Implementing ENISA Technical Guidelines on Security Measures for Unified Communication Systems and Networks

See www.um-labs.com

UM Labs
2-6 Boundary Row
London SE1 8HP, United Kingdom