Real-Time Communications Security is now the bedrock of Cloud Services, story behind the innovation.

2017

Real-Time Communications (RTC) is the most important paradigm shift on the use of personal and business data, since the telephone was invented. All internet communications are being conducted at real-life speed, integrated methods of RTC are being embedded in business applications, personal use crosses business use, therefore all Data that is consumed, stored can be used in these communications from anywhere, anytime, which makes for a large cyber-attack surface with expose personal data content being the target.

Introduction

Since the telephone was invented the world has become a smaller place, actual telephone numbers (not counting extensions) having each a three-digit area code may contain up to 7,919,900 unique phone numbers. Taken a modern look at what has happened since the introduction, the Mobile phone shows no other technology has impacted us in the same way. It's the fastest growing manmade phenomenon ever, from zero to 7.2 billion devices in three decades.

So much so, a study recently released by Deloitte found that Americans collectively check their smartphones upwards of 8 billion times per day. That's an aggregate number that refers to the number of times all Americans throughout the country look at their mobile devices on a daily basis, by the fact that the USA does this, the chances are these numbers are well into a trillion globally.

Gadgets like tablets, smartphones and not-so-smart phones are multiplying five times faster than we are, with our population growing at a rate of about two people per second, or 1.2% annually.

Why does this matter, well this revolution has made it here because of the internet and how the internet technology such as IP provides a way to connect that can grow and be managed.

In fact, the IP addressing mechanism can be seen as the new telephone number, according to Reserved IP addresses there are 588,514,304 reserved addresses and since there are 4,294,967,296 (2^32) IPv4 addresses in total, there are 3,706,452,992 public addresses out there today, with the latest introduction of IPV6, this means a potential IP address for every person and beyond.

How we use these new devices is also crucial, social media and social messaging such as WhatsApp (Facebook) with a 1 billion users per month, shows we have adapted the plain old telephone from voice too real-time Instant messaging, plus voice and are about to embark on the evolution bringing video into the picture, all based on the Internet technology.

This is the foundation of how we are today, all communication is this, so what does this mean for our everyday lives, it means clearly that if we are discussing, informing, transacting, selling, buying, supporting, educating in a real-time session we will be using this technology from now on.

All communications are being conducted at real-life speed, therefore all Data that is used in these communications, either via a link or live are exposed to potential Cyber-attacks.

Business communication technology and traditional methods of everyday business communications will find a major step forward in productivity and further ahead in their business development as there will be a greater focus on developing on the go aspects in the face of impersonal forms of communication that are merely transactional. The soft skills that characterize this will become even more vital in bridging the gap between technology and face-to-face communication.

For businesses, it is no longer a question of if, but when, a hacker is going to breach their perimeter security. With 2016 having the most data breaches recorded in a single year, businesses must take serious measures to protect their assets. And yet, despite a strong focus on perimeter security, most organisations are missing one important and easily protected layer: the document level, the real-time communications that surround this and how we engage.

However, intervention by the regulating authorities of Europe, USA and Asia have played their trump card, data protection is now the biggest new business risk to a company who hold any type of personal data on their customers, partners, employees and with the advent of the General Data Protection Regulation (GDPR) and similar in the other territories, means significant fines for not protecting this data. (See Cyber Security policy, Technical White papers www.um-labs.com)

Cyber Criminals can access all internet traffic via multi-levels, the attacks are designed to disrupt, open and copy, this happens at the network level, application level and the content levels within the technology infrastructure.

Still Cyber Security has to be compliant and assured in today's world of strict regulations, it must also be delivered fast and implemented across technology platforms, and in this it must deliver both mobile and desktop securely from attack.

Network level security addresses the IP level threats faced buy all IP connected applications and systems. The need for IP Network security for data application is well established. There is a whole industry devoted to developing data firewalls to protect against threats at this level. RTC applications run on the same IP networks as data applications and therefore need the same protection.

The security threats at the IP Network level include:

1.Denial of Service attacks (Dos) and distributed DoS attacks.

2. Flooding attacks

3. Malformed packet attacks

4. Port scanning and service enumeration attacks

DoS attacks, attacks designed to disrupt a network service, are a growing problem. Businesses with an Internet presence are a common target where the attack can be motivated by a political protest or for financial gain.

The obvious question is: if firewalls are designed to protect data applications from DoS attacks, can they do the same for real-time communication applications? The answer is no, because the protocols used for RTC are not *firewall friendly.* Configuring a firewall to handle SIP and the related protocol used to handle audio and video streams in calls, the Real-time Transport Protocol (RTP), means opening up a large port range. This reduces the firewall's security to a level where a competent firewall administrator would not want to apply the necessary configuration.

The only effective way to implement the necessary IP security controls is as part of a comprehensive real-time communication security product.

Application level security controls threats aimed directly at the RTC protocols and applications. The complexity of these protocols means that there is a long list of potential threats. These threats can be combated only by implementing a range of security controls directed at the application level. In RTC terms this means targeting security controls at the protocol messages responsible for functions such as tracking the status of connecting devices and managing calls.

The security threats at the application level include:

1. Denial of Service attacks (Dos) and distributed DoS attacks.
2. Flooding attacks
3. Malformed message attacks
4. Directory harvesting attacks
5. Authentication attacks
6. Call fraud attacks
7. Protocol violation attacks

DoS attacks at the application level include flooding attacks, where the targeted system is flooded with requests, and also more subtle attacks where smaller numbers of invalid messages are sent with the aim of disrupting a service.

Content level security protects the content delivered by RTC applications. This includes voice and video calls, text and other content delivered via Instant Messaging applications and *meta content* such as presence information indicating the availability status of colleagues. All of these content types are potential attack targets.

The most obvious attack is eavesdropping, listening in on voice and video calls or monitoring presence data to gather information on the identity of users. There are also a number of more subtle attacks including:

1. Media injection (replacing or disrupting voice or video streams)
2. Media level denial of service attacks
3. Call Hijacking attacks (taking over one leg of an established call)

European Privacy Regulation (GDPR) pushes for the implementation of multi-layer privacy information notices in order to ease their understanding by the public. This would be essential given the very large amount of information to be included in the notice under the GDPR.

Multi-Layer can be extended in all aspects of how data is stored and accessed, framed and made available, in a risk assessment the security official must take note that Cyber Criminals can access all internet traffic via multi-level attacks, access to the network is usually the starting point followed by application level and then to the content where the data resides.

Cloud is the most compelling technology shift in the last twenty years and being able to operate across all public, private and Hybrid helps keep compliance manageable, helps security protection of users and maintains lower business risk.

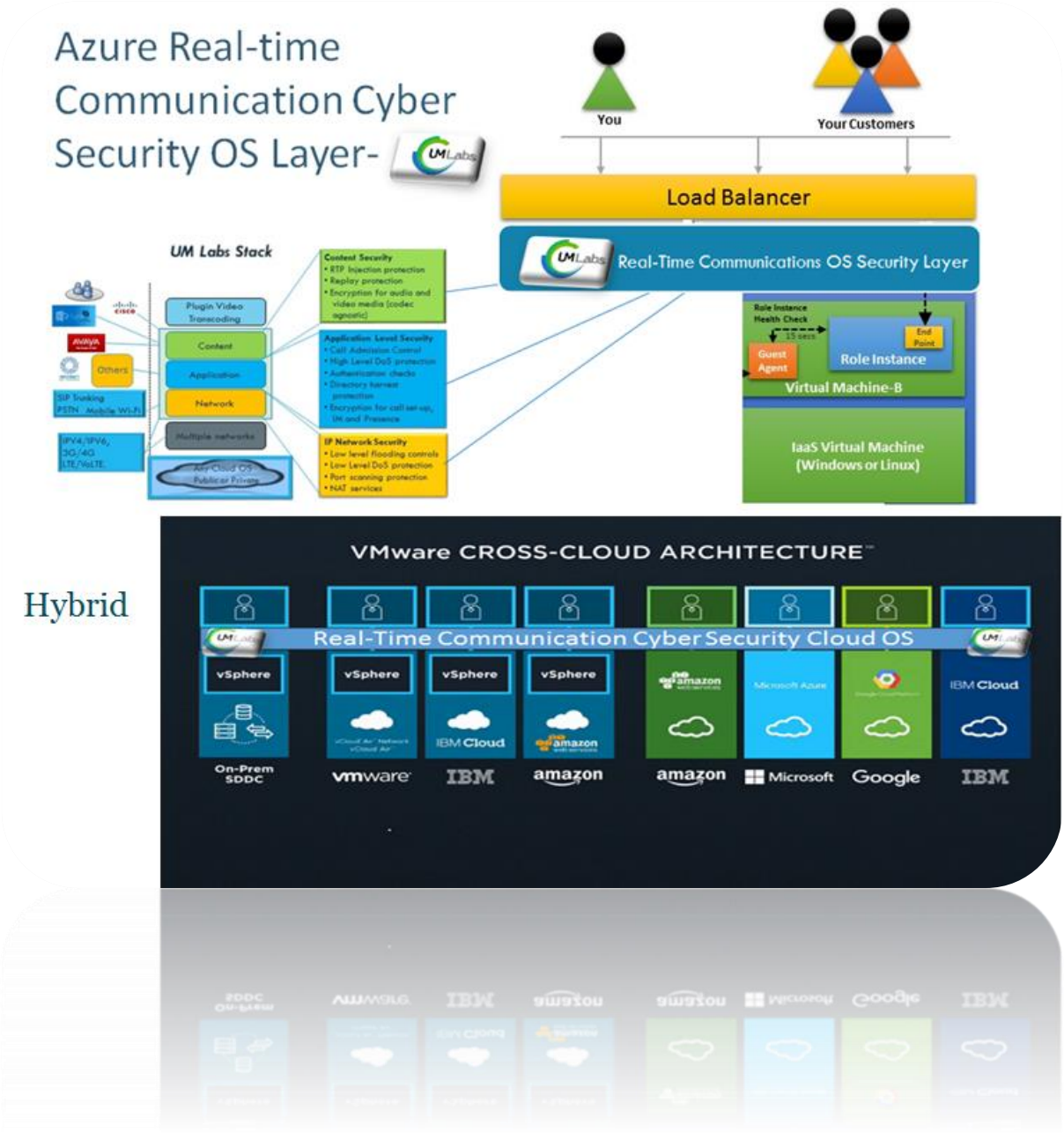
Once an organisation has implemented reasonable integrated multi-layered technologies to mitigate the IT security risk of traditional network infrastructures.

IT security becomes the process of applying security measures to ensure confidentiality, integrity, and availability of data. IT security attempts to assure the protection of assets, which includes data, desktops, servers, buildings, and most importantly, humans. The goal of IT security is to protect data both in transit and at rest. Countermeasures can be put in place in order to increase the security of data. Some of these measures include, but are not limited to, access control, awareness training, audit and accountability, risk assessment, penetration testing, vulnerability management, and security assessment and authorization.

The world is now both Cloud and Real-Time Communications, MarketsandMarkets estimates that the enterprise collaboration market will rise at a CAGR (compound annual growth rate) from $26.7 billion in 2016 to $49.5 billion in 2021. The research firm also expects the cloud collaboration market to rise at a CAGR of 12.7% from $23.4 billion in 2016 to $42.6 billion in calendar 2021.

Cloud shifts business models from Cap-Ex to Op-Ex, value is now set on the user activity and aligns to costs set for the applications that drive the communications (VOIP, Video, IM, Presence), so now there is pay for usage model for security and operation.

There is a point, particularly for businesses, about understanding how technology works. As we migrate towards the Internet of Things, there's a potential opportunity where you move from a model where the price of a service is the provision of data – personal data, or corporate data. It should be a differentiator, which people can use when selecting that service, including how secure they think it is and what reputation it has for security.



Therefore, RTC Cyber Security OS is about providing protection to users, be these VOIP, Video, IM or presence users, or IOT sensor on an IPV4 or IPV6 access end point. This approach will allow for wide distribution and fast implementation together with overall management coming as an overlay umbrella that is compliant and assured.

RTC Cyber Security for all UC, IOT activity becomes the new infrastructure, it is represented as the new Telephone Network in a way that reflects todays internet development, it is the new Security Infrastructure as a service (IaaS) with keys too open and close in a fully protective world.

Technology enabled applications (TEA) are communication solutions that go beyond traditional unified communications solutions (VOIP, Video, IM, Presence) and many companies are finding improved employee production and customer satisfaction by embedding RTC into their application infrastructure. From ERP, CRM, and out to mobile devices, TEA makes it easier to connect. Today, one of the challenges for TEA, for that matter, are a lack of solutions to ensure quality of service (QoS), compliant Cyber Security or service level agreement (SLA) adherence.

UM-Labs R&D-"We work to protect your business from criminal Interference" Cyber Security is the fastest growing challenge in today's world of the Internet, everyday 24 hours a day there is a breach, a theft of data, listening on phone calls/video calls, messaging (IM) and even your location.

Businesses have in the past tried to control attacks with outdated computing technics and this legacy is set against a back drop of keeping in with the status quo. The thirst for internet content and the fast growing use of Cloud technology increases the volume of criminal cyber-attacks on Video chat, Internet phone calls, IM and location.

Over 234 million people use these communication services in business every day, a 21st century solution is required to protect and manage your business. UM-Labs are a creative and advanced R&D company with experts in compute security software design, smart mobile technology and cloud computing. The cloud solution is a unique layer of real time security software.

This protects and encrypts Internet communications across all of the cloud variants, it is easy to install and scales to thousands of users from one virtual server, compliant tested and certified customer reference sites in Europe and the US.

Adopting UM-Labs 21st Century Innovation in Cyber Security will allow for true encrypted security on all Unified Communications and provide integration across the entire business, with no added capital cost. Cyber Security OS layer in any cloud is fully compliant and tested against new regulation GDPR, NIS and ENISA guidelines in the EU/UK and HR1770 in the USA.

Unified Communication applications such as Microsoft S4B or Cisco Spark or Avaya IPPBX and 500 others are protected from a layer in either a Public, Private Cloud and Hybrid Cloud. Fraud, DDOS attacks and hacking are rendered solved through the cloud layer of all UC applications.

This reduces all risk while enhancing the ROI for the business and being compliance tested and approved means assured.

Contact UM-Labs R&D today. **Info@um-labs.com**


UMLabs