Real-Time Communications (UC-IOT) Security for the Financial Sector

2016

The number of data protection and compliance regulations facing banks and other financial sector businesses is growing, but many organisations do not realise that the scope of these regulations extends beyond data orientated applications and services. Changes in business communication have brought phone services and related applications within the scope of these regulations.

Introduction

Both business and personal communications technology has changed radically over the past few years, this is particularly true in the financial services(FS) sector. Activities which once relied on the standard phone system are now more likely to take place over an IP based network and routed over the Internet. In many cases users are not even aware of the change as new phone systems are likely to connect to service provider via an IP connection. In other cases, the change is obvious. Users are adopting *Unified Communications* (UC) applications such as Instant Messaging (IM) and video calls in preference to the standard fixed line or mobile phone.

A PWC FS survey shows that cybercrime is still the second most common type of economic crime reported by FS respondents (after asset misappropriation), 38% in 2011 vs 39% in 2015 (this compares to only 16% in 2011 vs 17% in 2015 in other industries). However, PWC views this percentage of respondents as alarmingly low, in their experience it has shown that a clear majority of FS organisations (especially retail banks) suffered cybercrime during the survey period. These changes have implications for both security and compliance, particularly in the financial sector.

Cyber Security

On the other hand, cybercrime is growing and the methods are constantly evolving, it has been reported that there is no abatement in attacks on banks' infrastructure. Some recent attacks have installed hardware in bank branch systems to enable transactions to be manipulated via mobile networks. The market in FS has seen dramatic increases in FS economic crime, from outages created by Distributed Denial of Service (DDOS) attacks to massive ATM withdrawals effected by organised criminal groups gaining meaningful access to data, once the data has been hacked following the DDOS attacks.

It is widely understood that data applications on IP networks are at risk of cyber-attack all of the time. This is why web sites provide encryption and authentication and why firewalls are used on virtually all Internet connections.

What is less well understood is that moving phone services to an IP network exposes those services to attack. Potential attacks include denial of service attacks that leave a phone system inoperable as well as unauthorised monitoring of calls and leakage of confidential information. Unified Communication applications and calls made over mobile networks are also vulnerable to these attacks. Many of these attacks are specific to the communications applications in use and need specific security controls. These attacks are not blocked by the security measures designed for data applications.

Compliance

> ***"Today's incidents, yesterday's strategies –As the digital channel in financial services continues to evolve, cybersecurity has become a business risk, rather than simply a technical risk"-*** *The Global State of Information Security® Survey (an annual, worldwide study by PwC, CIO magazine, and CSO magazine)*

In the UK, the Bank of England has declared cybercrime a major risk to the FS sector and, along with other FS regulators in the UK, co-ordinated a major cyber-attack in November 2013 to 'stress test' UK banks in an exercise known as 'Waking Shark II'. The Bank's report on this exercise cited a need both for greater co-ordination within the sector and for educating firms about the need to report major incidents to regulators. In the same month, the New York State Department announced that it would require the banks under its regulation to answer questions in a real-time online test in order to assess their cybersecurity policies and processes.

Additionally, in the U.S., regulators have increased the visibility of cybercrime by requiring cyber incidents which have had material impact to be disclosed in registered public company filings.

Several large FS organisations have thus been prompted to disclose within their 10K filings with the SEC that they have been targeted by cyber-attacks.

Even in Lebanon, where online banking activities are less developed and banks therefore do not perceive the cybercrime risk as material, significant losses from cybercrime in the FS sector have emerged. The Banking Control Commission of Lebanon has initiated reviews of IT security in banks with a view to strengthening cyber defences.

Knowledge is power, FS organisations have been co-ordinating to share threat intelligence for years. Collaborating to share cyber threat data helps organisations deal quickly and proactively with cybercrime. In Luxembourg, where the FS sector is dominant, such collaboration is of strategic importance to the economy at large.

The largest FS organisations are also catching on to the need to deter (rather than just detect) cybercrime.

In Europe, the financial services sector operates within its own set of both national and European regulations and is subject to a broader set of compliance controls. Specific regulations for the financial services sector include MIFID II which is expected to come into force in January 2018. While this is still some time in the future, preparing for MIFID II requires significant advance planning as the regulations include a requirement for indentified areas in the financial services sector to record all communications. This requirement applies to all forms of communication including calls made in fixed line phones, mobile devices or UC applications.

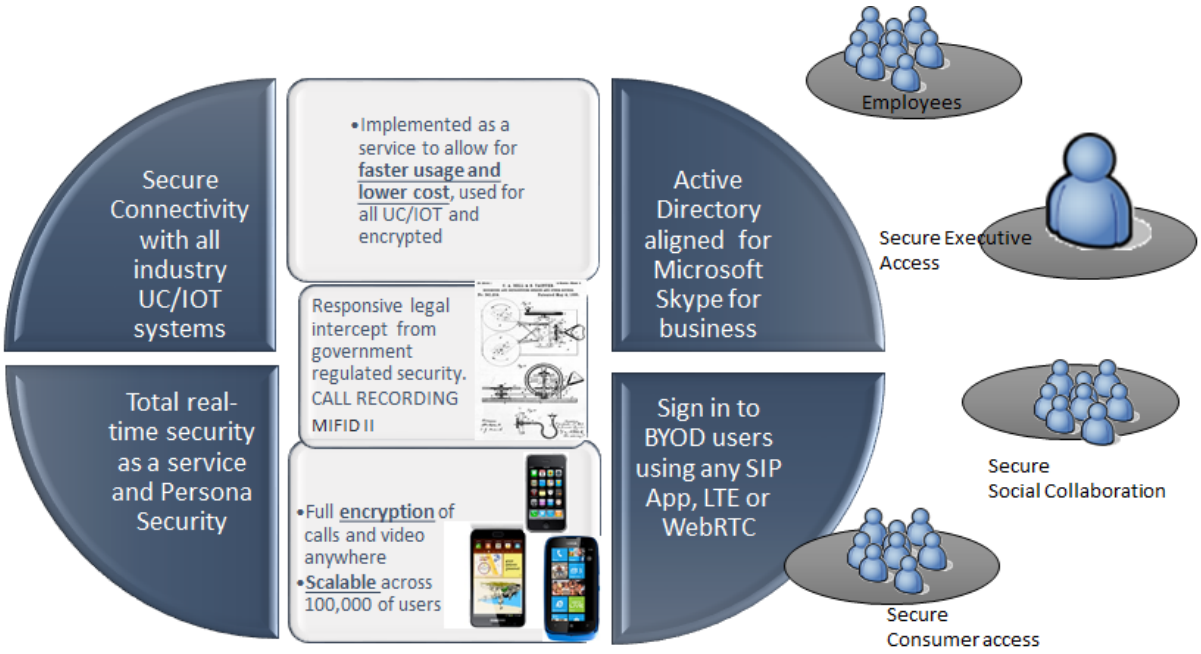
In common with all other industry sectors, the financial services sector is also bound by the European General Data Protection Regulation. This regulation, issued in January 2016, defines wide ranging measures to protect personal data. The fact that it is a *regulation* instead of a *directive* means it will be directly applicable to all EU member states without a need for national implementing legislation. The regulation requires all commercial organisations processing personal data to implement effective cyber security measures to protect data from misuse. The regulations also require organisations to demonstrate that these controls are in place. The penalties for failing to comply with the regulation are server, fines of up to €20 Million or 4% of total worldwide annual revenue, whichever is the greater.

To assist companies in their efforts to comply with the regulation, the European Union Agency for Network and Information Security (ENISA) have published a set of technical guidelines. These guidelines make it clear that the regulation applies to all forms of data transfer and communication including IP based phone services, mobile networks and UC services.

Technical Challenges

There are some technical challenges to addressing the security problems and meeting the compliance requirements. Firstly, as IP based voice and UC services face very specific security threats then targeted security controls are needed. Organisations running these services without effective security will not be able to meet the European General Data Protection Regulation (GDPR)

Secondly combing the security measures needed to meet the European GDPR with the need for MIFID II compliance can be a challenge. For example, the obvious way to meet the GDPR's requirement for data protection is to use encryption. This encryption service can make meeting the MIFID II requirement for call recording difficult. Fortunately, there are 21st century solutions.



UM Labs R & D

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; if not your business is at risk.

Tomorrow 60 billion end points for Internet of Everything (IOE/IOT) will be at risk to attack, so keeping ahead of the thinking and delivering safe IP connectivity over three layers, network, application and content is crucial and UM Labs is a UK based R&D company specialising in designing and developing security solution for Real-Time Communication applications.

As a creative 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.

The UM Labs products are widely deployed in all industry sectors. These products have been tested and evaluated by leading security consultancies and by national and regional telecommunications providers and have demonstrated to provide the security and compliance needed to meet the security and compliance needs of the financial sector.

Contact www.um-labs.com or marketing@um-labs.com