2009 International Conference on Computer Engineering and Applications
IPCSIT vol.2 (2011) © (2011) IACSIT Press, Singapore

Mitigating the Security Risks of Unified Communications

Fernando Almeida [1 +], Jose Cruz [2] and Jose Oliveira [3]

[1 +] Faculty of Engineering of University of Porto, DEEC, +351 22 508 1440, almd@fe.up.pt

[2] Faculty of Engineering of University of Porto, DEI, +351 22 557 4103, jmcruz@fe.up.pt

[3] Faculty of Economics of University of Porto, INESC Porto, +351 22 209 4050, jmo@inescporto.pt

Abstract. Unified Communications (UC) have the potential to dramatically simplify and improve enterprise communications, reducing costs and improving revenue opportunities. However, these benefits do not come without risks. The introduction of an IP-based UC solution brings an array of new vulnerabilities into the enterprise, exploited by a growing number of malicious programs. This paper presents the most common of risks faced by the major dominant technologies used in unified communications solutions and an approach to mitigate them.

Keywords: Unified Communications, security, VoIP, instant messaging.

1. Introduction

The concept of Unified Communications (UC) appeared in the Information Technology (IT) world in the past few years. By integrating real-time and non-real time communications with business processes, while presenting a consistent unified user interface and experience across multiple devices and media types, UC provides productivity improvements to individuals, workgroups, and companies. It's important to recognize that UC is not a single product, but it is a composite of various components, including messaging (email, Instant Messaging, voice, video), calling (audio, video), conferencing (audio, Web, video), presence, and mobility [1]. These elements are all tied in together with the user's desktop and/or device of choice, providing a consistent user experience.

UC solutions can lead to significant cost savings, adding value to a range of business processes and facilitating more effective collaborative work. By providing an integrated portfolio of capabilities and services, UC enable organizations to increase business agility and leverage increasingly dynamic and flexible working practices [2]. Companies of all sizes are adopting unified communications and the collaboration capabilities it fosters to boost productivity and innovation, increase mobility and enhance flexibility. Upon interviewing 315 network and telecommunications decision-makers at European enterprises, Forrester finds that enterprise implementation of Voice over IP (VoIP) in Europe is strongly entering the mass adoption phase. UC is firmly on the agenda considering that 35% of firms say UC is a priority, and 18% have implemented some element of UC [3].

Clearly, within the context of UC-driven communications enabled business processes, converged voice and data IP networks are being entrusted to carry the essential functions of conducting business to and from the remote worker, the supply chain and the partner ecosystem. It is crucial for an organization to keep these networks secure in a manner that prevents leaks of customer records and protects intellectual property and proprietary information.

2. Security of Unified Communications

2.1. Concerns around security

On the end of 2007, Dimension Data, a world leader in the provision and management of specialist IT infrastructure solutions, conducted a research survey around unified communications. In that survey, 390 IT managers/decision makers and 524 IT users from 13 countries in Europe, North America, Asia Pacific, Middle East and Africa were targeted. The respondents were asked about their perceptions of the inherent levels of security and potential risks associated with unified communications.

The survey concluded that the majority of IT users (52%) perceive unified communications to be as secure as most other Information and Communication Technologies (ICT). IT managers take a slightly more cautions view, with 31% believing that it is as secure as other ICT technologies [4]. These results indicate that IT managers are aware of the new risk types that are associated with unified communications, while IT users are probably reasonably unaware of the risks they might be exposed to and expose their organizations to when using communications technologies other than basic communications, such as email.

In that survey, IT manager were asked to indicate which unified communications technologies they believe posed the greatest risk to the organizations. The results are illustrated in Figure 1.

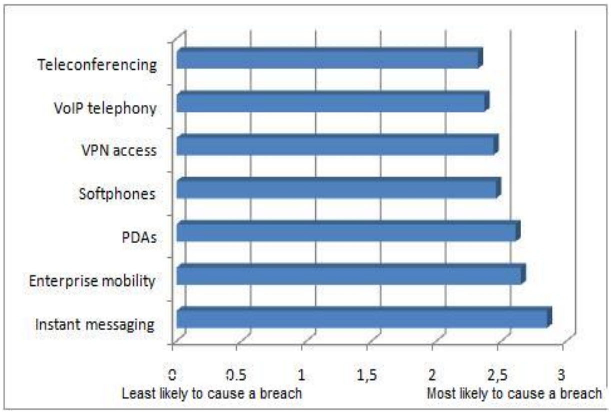

Fig. 1: IT opinion about risks of UC technologies [4]

Instant Messaging (IM) received the highest risk rating. This could be attributed to the high levels of public IM penetration into corporate environments. On the same way, enterprise mobility and PDAs also received high risk ratings. This indicates that IT managers are concerned with technologies that are harder to control, given the high level of end user penetration and limited organizational policies or procedures around these technologies in the corporate environment [4].

2.2. Type of risks

We can broadly identify three categories of threat in relation to unified communications:

- Theft of service – such as toll fraud through the unauthorized use of UC resources;
- Denial of service – implies a deliberate or accidental attack against services and applications that render them unusable for IT user;
- Privacy and compliance – focuses on interception of communications and confidentiality challenges associated with the conformance of corporate compliance policies and legislation.

Theft of service is as much a policy definition and enforcement issue as it is a technology risk. The mitigation of threats to theft of service in enterprise UC deployments centres around the application of best practices and the enforcement of good policies covering topics such as strong passwords, authentication of end-points and users to the system, and tools to monitor call patterns and events.

The underlying architecture of IP networks make them vulnerable to DoS attacks unless specifically configured to identify and limit their effects. DoS attacks can be managed at two key levels: the network and the application/operating system level [5]. At the network level, IT managers can limit traffic to strategic service to the IP ports necessary to function and block all other traffic to these devices. They can also enable network-centric security configurations to ensure the correct operation of Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS) and other network services. At the operational level, they can ensure that applications are patched to the latest security levels and protect servers through deployment of anti-virus software.

Finally, the third threat refers to the violation of personal privacy. This can take many forms but the most common are: compromising voice mail or unified messaging servers, intercepting voice packets on the network and gain physical access to analogue devices or voice gateways.

On the following sections, we will look to the potential risks and corresponding mitigation options associated with the top three dominant technologies used in unified communications, which are: Instant Messaging (IM), Private Branch Exchange (PBX) and Conferencing.

3. Risks of Instant Messaging

Instant Messaging applications allow employees to easily communicate and share files with other IM users in a real-time session similar to a private chat room. IM solutions are also used in organizations where IM communication is part of the corporate culture and presents significant business advantages. However, without proper control, IM poses a significant security threat on many fronts, mainly in terms of theft of service and privacy. Apparently, attending to the fact that most IM services are already free, there is little threat of theft of services [6]. However, it is common to see attacks in terms of identity theft and identity ambiguity. The most frequent used attack is stealing the account information of an unsuspecting user [7].

To get the account information of a user, the hacker can use a password-stealing trojan horse. If the password for the instant messaging client is saved on the computer, the attacker could send a trojan to an unsuspecting user. When executed, the trojan would find the password for the instant messaging account used by the victim and send it back to the hacker. Another potential attack is related with unauthorized disclosure of information. Information disclosure could occur without the use of a trojan horse. Since the data that is being transmitted over the instant messaging network is not encrypted, a network sniffer, which can sniff data on most types of networks, can be used to capture the instant messaging traffic. By using sniffer, a hacker could inspect the packets from an entire instant messaging session. This can be very dangerous, as he may gain access to privileged information. This is particularly dangerous in the corporate environment, in which proprietary or other confidential information may be transmitted along the instant messaging network.

The safest way to ensure organizational control over identity and credentials is to implement a corporate IM system. By implementing it, the organization obtains control over functionality of the system, resulting in better levels of compliance with corporate policy. This will provide corporate control over user credentials and published names as well as password and usage policies. In addition, file transfer can be disabled if necessary and messages can be logged and archived for future analysis. Whether using a corporate IM system or a public IM service, content filtering applications should be implemented to ensure that these communication channels are not being used to transmit files containing viruses and other malicious software.

4. Risks of Private Branch Exchange

IP PBX forms the core of real-time communications within the organizations. In most unified communications projects the PBX is an IP-based platform that provides integration to desktop applications for remote call control and presence. The IP PBX can be divided into two functions: one to process the signals and one to set up calls [8]. However, the IP PBX is treated as a single entity, since almost all IP PBXs are implemented on a single device.

The most typical security risks in a PBX system are related with denied of service and exposure of information.

A distributed denial of service (DoS) attack is the most serious threat that a VoIP system can face. It can affect any Internet-connected device and works by flooding networks with spurious traffic or server requests. The attack is generated by machines that have been compromised by a virus or other malware. The massive increase in traffic means the affected servers are unable to process any valid requests and the whole system grinds to a halt. Another vulnerability of VoIP is the ability of an outsider to eavesdrop on a private conversation. This concept is not new to IP data networks, and generally requires a packet analyzer to intercept IP packets, and in the case of VoIP, saving the data as an audio file. Hackers then have the ability to learn user ids and passwords, or worse, to gain knowledge of confidential business information. Another hack that is well known in data networks is spoofing, also known as a man in the middle attack. Spoofing requires hacking into a network and intercepting packets being sent between two parties. Once the IP address or phone number of the trusted host is discovered, hackers can use this attack to misdirect communications, modify data, or in the case of Caller ID Spoofing, transfer cash from a stolen credit number [9].

A way to mitigate these threats is to control the traffic across subsystems by access control functions within a firewall to protect from network resource consumption and attacks from malicious users. In order to maintain the confidentiality of all traffic, both signal and media streams should be encrypted. Each VoIP infrastructure entity should also be physically protected, preventing attackers to steal users' confidential information. Furthermore, since VoIP gateways are typically exposed to the DoS attack threats by the nature of having a connection to external public networks, a firewall device should be considered to mitigate the possibility of such DoS attacks. A firewall can not only be used to mitigate such attacks, but also prevent the other attacks by enabling additional features, like traffic shaping and protocol anomaly detection functions.

The mitigation of the possibilities of call interception and unveiling of confidential information can be done encrypting signaling and media protocol communication. In Figure 2, we present a possible implementation approach.

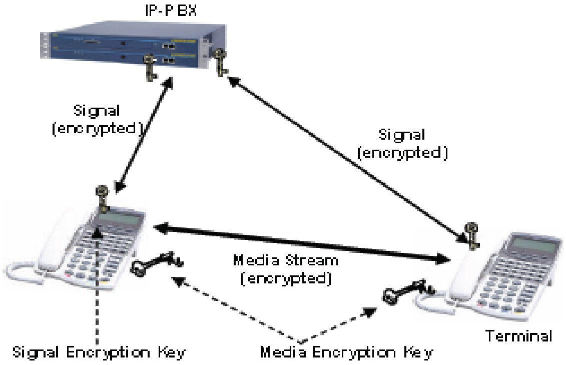

Fig. 2: Two types of encryption keys [8]

A key agreement is needed when VoIP communication is encrypted. As shown in figure 2, two encryption keys must be agreed upon. One key is for call signalling encryption, shared by both IP PBX and each terminal, and the other key is for a media stream encryption, shared by the two communicating terminals. In order to maintain the availability of the IP PBX during any failures, fault tolerance should also be considered. The IP PBX and application servers should have redundancy, allowing for provisioning when an accident, breakdown and/or the maintenance of equipment take place. In addition, the adoption of Uninterruptible Power Supplies (UPS) enables power failover redundancy to the VoIP system.

5. Risks of Conferencing

Conferencing applications or services offer the ability to blend audio and video conferencing and application sharing across multiple networks and endpoints. Using a conferencing application, groups can see, hear, text chat, present and share information in a collaborative manner. However, conferencing applications pose security threats as they involve and interact with many technologies within the enterprise. This risk is relevant, irrespective of whether the application is hosted externally or internally.

Audio and video do not communicate in the same manner as data information. They prefer a continuous stream of information to be transmitted and does not need confirmation as in the sending and receiving of a data packets. Displaying all of the body movements of the conference participants is not necessary. If some of the data transmission during a web conference is lost during the video transmission, then the only negative effect is unnatural movements such as a jerkin head. This latency is acceptable to most users of the video, but less so for the audio part of a conference. For this reason the User Datagram Protocol (UDP) is used.

The UDP is a transport service tuned more for audio and video transmission that prefers non-guaranteed datagram delivery and allows more direct access to the lower levels of the IP layer [10]. Therefore, conferencing applications that rely on UDP must deal directly with end-to-end communication problems that a TCP connection would have handled such as retransmission for failed delivery, and congestion avoidance. UDP can be considered a good protocol for streaming audio and video data, but also increases the security exposure because data packets can be less controlled and more open ports in the firewall are required [10].

An alternative approach to UDP was created to reduce the number of access points into the network. In this new approach, the web conference is tunneled through the normal TCP connection. The audio and video data is encapsulated as normal HTTP commands and transmitted over the TCP connection in the same way as web pages are displayed.

Another good practice is to choose a conferencing system that allocates random access codes for each conference ID rather than static attendance codes. Also, the conferencing services should allow the host review of the number of participants in a conference to determine if an additional party is present.

6. Conclusions

The drive for business agility is stimulating companies of all sizes to adopt unified communications as a primary vector for enhanced communication and collaboration capabilities between remotely located and mobile employees, its supply chain and partner ecosystem, and with customers. Organizations recognize the value of UC technologies for improving end user productivity, increasing customer satisfaction and reducing communications costs. These benefits, however, do not come without risks.

IT companies are dealing with three categories of threat when they adopt an unified communications solution: theft of service, denial of service, and privacy and compliance. Typical threats in these domains of risks for the five dominant technologies used in unified communications were identified and mitigated.

Concisely, the most important best practices that a company should follow are related with VPN technologies, firewall mechanisms and admission control security endpoints. The company should use VPNs to provide a secure pathway for communication with remote workers. A VPN’s built-in encryption feature enables secure connectivity with branch offices and business partners that are unreachable by private networks. At the firewall policy, IT manager should implement VoIP-ready firewalls that are capable of handling the latency-sensitive needs of voice traffic. Finally, IT manager should implement Network Access (or Admission) Control in order to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement so that network access is contingent on compliance with established security policies.

7. References

[1] R. Ascierto. The business case for unified communications. 2007, a*vailable on http://www.echocomms.co.uk*.

[2] Forrester. Unified communications transforms business communication. *Forrester Research Studies*. 2008, p. 3-8.

[3] G. Hill. Secure unified communications: managing risk to guarantee the benefits. *Dimension Data white papers*. 2008, p. 3-9.

[4] G. Hill. Securing IP telephony – Can you hear me now?, *Dimension Data white papers*. 2007, p. 2-4.

[5] S. Niccolini, K. Hertzler and T. Ewald. VoIP security best practice. *NEC white papers*. 2006, p. 9-19.

[6] L. Cox, A. Dalton, V. Marupadi. SmokeScreen: flexible privacy controls for presence-sharing. *Proc. of the 5th international conference on mobile systems, applications and services.* ACM Press, June 2007, pp. 233-245.

[7] R. Hulme. One for all: unified messaging comes of age. *Work Study.* 2003, **52** (3), pp. 141-144.

[8] S. Kim and Leem, C. Security of the internet-based instant messenger: risks and safeguards. *Internet Research.* 2005, **15** (1), pp. 88-98.

[9] K. McCurley. Information security and the economics of crime. 2007, *available on http://ic.epfl.ch/researchday*.

[10] J. Shore. IP Telephony Security: An overview. *Network World Special Reports Edition*. 2004, p. 5-8.