Uses and dangers of peer-to-peer and instant messaging in a business environment

T.Quaden[1], S.M.Furnell[1], M.Papadaki[2] and G.Pinkney[2]

[1] Network Research Group, University of Plymouth, Plymouth, United Kingdom
[2] Symantec, Hines Meadow, St Cloud Way, Maidenhead, Berkshire, United Kingdom
e-mail: info@network-research-group.org

Abstract

Peer-to-peer (P2P) and instant messaging (IM) applications have become very popular ways of downloading the newest media files and to chat with friends. When introduced to a business environment and not properly managed these applications present the business with new risks that might not be accounted for. This research paper focuses on the dangers of P2P and IM applications from the perspective of an organisation and discusses some measurements that can be taken to minimise these. It was found that both IM and P2P applications open up holes for all kinds of malware to enter the corporate network. Furthermore due to the nature of the majority of content downloaded from P2P networks (copyrighted files and inappropriate material) a business might be held liable for illegal or inappropriate material downloaded by its employees. Even though, when properly managed, IM software can greatly increase business performance, if unmanaged can lead to incidents such as data or even identity theft/spoofing. There are several ways to minimise or prevent the risks of using such applications. Well-defined security policies can help educate users of the risks; management software helps detect, block or manage IM & P2P applications; and some companies even offer Enterprise IM solutions.

Keywords

Insider threats, Peer-to-peer (P2P), Instant Messaging (IM)

1. Introduction

In today's world with broadband Internet access widely available, peer-to-peer (P2P) and instant messaging (IM) applications have become more popular than ever. As Figure 1 shows, by mid 2004, 90% of commercial and non-commercial enterprises in North America were using IM software (Ostermann Research, 2004) and market research firm IDC estimated that more that 506 million people world wide would be using IM products by 2008 (Leavitt, 2005).

P2P applications share a similar popularity. A study in 2004 found that about 40% of business Internet users have used P2P applications to download and share files online using their business network (Ostermann Research, 2004). One of the most popular P2P applications, Kazaa which uses the FastTrack filesharing network, usually has in excess of 2 million users online at any time (see Figure 2).

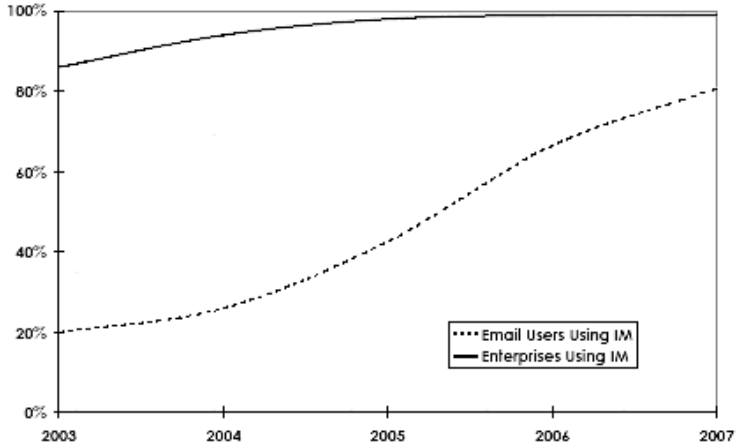

Figure 1: predicted increase in IM use (Ostermann Research, 2004)

Some of these applications also have legitimate uses in a business environment but they can also introduce new problems to the business networks they are used on, especially if not properly managed. This paper starts by identifying some legitimate uses of such applications in a business environment, discusses some of the problems associated with them and follows up with suggestions on how to avoid these problems.

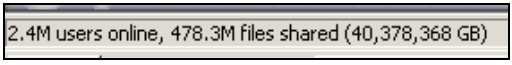

Figure 2: Number of users on Kazaa network and amount of files shared

2. Business uses of IM & P2P

If used properly, IM can help increase business performance. IM offers faster response times than e-mail, and is cheaper and less intrusive than using a telephone. The study "Measuring IM Productivity in the Enterprise" conducted in 2004 by the Radicati Group, found that the use of IM can save a company an average of 40 minutes per user every day, resulting in about $37.5 million per year in productivity savings when applied to a 5.000 employee company (Instant Messaging Planet, 2004).

P2P applications are mainly used to download and share all kinds of files, such as music, movies, and software applications. Most of these however are copyrighted and are therefore distributed illegally, which can lead to expensive law suits for which companies can be held liable. There are, however, some legitimate uses of P2P technology within a business. P2P can be used as a means to increase a business' storage capacity or to use previously unused processing power among their workstations and servers. University of Wisconsin researchers estimated that on

average most businesses only use about 25% of their available storage (Computerworld, 2001). Using P2P technologies, businesses would be able maximise the storage they use and therefore be able to save money that was previously spent on storage servers. These P2P applications, however, differ entirely from those like Kazaa, which generally have no legitimate use in a business environment and only use up valuable bandwidth.

3. Problems & Risks associated with IM & P2P

Most IM and P2P applications used in enterprises are consumer-grade clients that are not specifically made for use in business environments and in most cases have been brought into the business network by users installing their own clients without the IT department's permission or knowledge (see Figure 3). In March 2004 the mean number of different IM applications in use by employees throughout American businesses reached 2.9 (see Figure 4). The result of this is that in many businesses employees use a variety of different IM and P2P applications that are not managed in a proper way and therefore present the business network with new risks not accounted for.

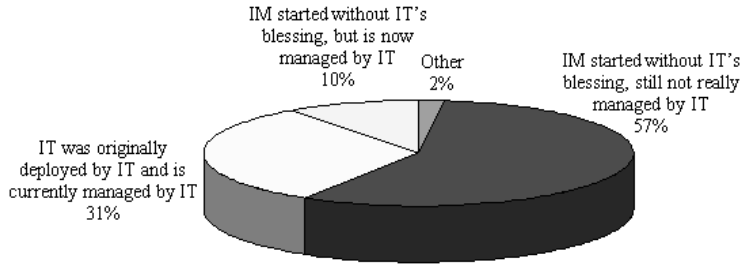

Figure 3: Methods by which IM entered the business (Ostermann Research, 2004)

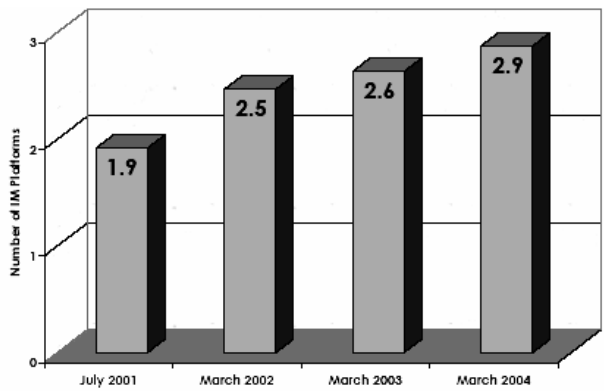

Figure 4: Mean Number of IM Platforms per Enterprise (Ostermann Research, 2004)

3.1 Copyright Violation

The most obvious danger to a business that comes to mind when users use P2P applications is copyright violations. This is due to the fact that most users use such applications to download media files (i.e. music or movies). Most of these are protected by copyrights which makes downloading such files without having purchased them illegal. If such copyrights violations are detected within a business it can lead to lawsuits that can cost the business considerable amounts in fines and in terms of reputation loss. In early 2005 the British Phonographic Industry (BPI) announced that in 23 cases illegal music uploaders had to pay up to £4500 as compensation (Leyden, 2005). More serious cases in the U.S. made illegal movie sharers pay up to $30,000 or even up to $150,000 if it was done 'wilfully' (Sherriff, 2004).

3.2 Inappropriate material

One popular use for P2P application is the downloading of inappropriate material such as pornography. Viewing of inappropriate accounted for 47% of computer abuses in the UK in 2004 (Audit Commission, 2005). Viewing of inappropriate material creates can create a hostile work environment and result in damaging the reputation of a business quite considerably. To demonstrate how inappropriate material can damage a business' reputation just consider this simple example: an employee finds an image or video clip of some inappropriate nature (e.g. pornography or some racist/sexist joke) and decides to use the company email to send it on to a bunch of friends. These (possibly working at different businesses) then send it on to others. Eventually this email could somehow end up in someone's email that might be offended by it and because the original source is still in the email header they can recognise the person and most likely also the business it originated from. This could give the entire business a bad reputation and might even result in loss of business with companies that feel offended by it.

In the case of employees viewing illegal material (e.g. child pornography) the business can possibly be held liable for it which can result in high fines and in confiscation of network hardware for investigation resulting in business disruption and bad publicity.

Additionally the downloading of inappropriate material wastes network bandwidth that could otherwise be used for legitimate business operations.

3.3 Malware

Another serious risk when using P2P and IM software is malware. There have been hundreds of viruses, Trojans and other malicious pieces of software circulating the various P2P and IM networks. The Symantec search web site (Symantec, 2005) comes up with 441 results for Kazaa, 605 results for MSN, 418 results for ICQ, 100 results for AIM and 936 results for IRC when searching for malware and vulnerabilities. IMLogic has set up a threat center to monitor IM and P2P threats worldwide. During the first week of September 2005 alone it reports 43 different malicious pieces of software that circulated P2P and IM networks, most of them

circulating the IRC network (IMLogic, 2005a). This shows the vast amount of vulnerabilities and risks of malware infection when using such applications.

Bruce Hughes, director of malicious-code research at security firm TruSecure, found that about 45% out of 4,778 files he downloaded with Kazaa contained malicious code such as viruses or Trojans (Wired News, 2004). Hughes also considered that about 85% of the malicious files can easily be detected by up-to-date anti virus software. To confirm these statistics, 30 executable files (.exe) were downloaded during this research using Kazaa while running Mc Affee VirusScan Enterprise 7.0.0. Out of the 30 files downloaded 14 were found to be infected by the Trojan 'Downloader-TS' and one file by the virus 'W32/HLLP.Hantaner.dam' (see Figure 5). Considering that 50% of the files downloaded were infected by malware, the results are similar to Hughes' research, demonstrating the high risk of malware infection when using P2P applications such as Kazaa.

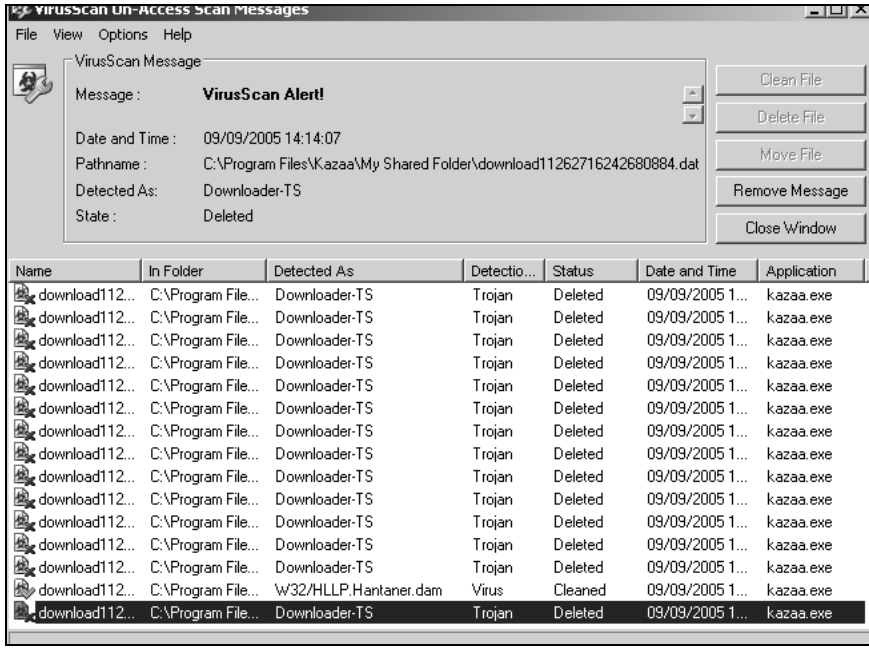

Figure 5: Trojans and viruses found downloading software from Kazaa

Many of these worms or Trojans can compromise system security by creating backdoors or lowering system security leaving systems vulnerable against more active attacks such as system intrusions. An example of this is 'Gabby.a', a worm that targets AOL's AIM and ICQ networks tries to trick users into clicking a hyperlink that leads to a webpage which then infects the user's computer with a worm that opens a backdoor into the system and stops windows services such as firewalls and antivirus software (Leavitt, 2005).

The main problem is that most IM and P2P applications are very adept at circumventing network firewalls and intrusion detection systems (IDSs) by finding

open ports to use and therefore opening up security holes in otherwise fairly secure networks. This makes it very hard if not impossible to block all P2P and IM traffic from passing through the firewall. Additionally most IM applications use different ports and protocols to communicate with their servers making it even harder for administrators to block all of them.

Even when blocked some employees will still have the desire to use them and may find ways around the block by changing the ports the applications use in the configurations or by using applications such as Hopster. Hopster acts as an anonymous proxy between the user's computer and other computer on the Internet and enables users of popular P2P and IM application to bypass censoring firewalls and proxies by making traffic look like 'innocent' HTTP requests (Hopster, 2005).

3.4 Data theft

The risk of data theft applies to both P2P and IM software. Due to the nature of P2P applications where users share files on their computer with the rest of the P2P network users it can happen, especially when used by unknowing users, that folders with private/confidential data are accidentally shared. This can obviously damage a business quite considerably. A very good example of such an incident happened start of 2005 when highly confidential documents about human traffickers belonging to the Dutch armed forces were found online. They contained at least 75 pages of phone numbers and tapped conversations, and (according to Dutch newspapers) they were first found on a P2P network in unencrypted form (Libbenga, 2005). It is assumed that an employee of the Dutch armed forces took the documents home to work on and accidentally shared his entire hard drive when using a P2P application.

Since most IM applications also allow file transfers between users this risk also exists, but in most cases the user would deliberately have to send the files to someone else. This however, is not the only way in which data can be stolen. Most consumer-grade IM clients (e.g. MSN Messenger, AIM) do not support internal network routing. This means that even if the recipient of a message is within the same internal network, the message is first sent to an external server and then back into the network. This fact combined with the fact that most clients also do not support any form of encryption means that intercepted messages can easily be read with the use of any standard packer sniffer, further increasing the risk of confidential data being stolen.

3.5 Identity theft and spoofing

Another concern with the use of consumer-grade IM applications is that users choose their own names which are not controlled by any company policies. This can lead to an outsider pretending to be a co-worker and using social engineering attacks to gain confidential data or valuable information to use in an attack against the business network. IM Authentication mechanisms also often lack sufficient encryption, which can result in account hijacking and further social engineering attacks by outsiders and competitors.

4. Recommendations

Since it is very difficult, if not impossible, to block all P2P and IM traffic, it becomes very important to have defined security policies regarding the use of such applications. SurfControl, a corporate Internet security vendor, conducted a survey of U.S. businesses that identified that even though 90% of respondents had a policy regarding Internet use but only 51% had a policy regarding the use of IM software (Leavitt, 2005). This shows that many businesses either do not seem to be fully aware of the security risks involved or do not realise how many of their employees actually use IM.

Especially in small to medium sized enterprises, where policies are easier to enforce, a well- designed policy that educates the users on the dangers of IM and P2P might help reduce the use of such applications considerably. Policies could either completely forbid the use of such applications or in cases where employees use consumer-grade IM applications for their work they could specify a specific client that all users may use in order to provide more control. If the business knows what applications are used and knows about the protocol used by these, it becomes much easier to monitor the network traffic and discover any unusual behaviour such as the propagation of malware or inappropriate material.

Some companies specialise in developing IM management software which allows administrators to detect, block and manage IM and P2P traffic and authentication. An example of such software is IMLogic's IM detector pro (IMLogic, 2005b). Some of these management tools allow administrators to set up alerts that can be triggered by certain actions such as file transfers or keywords within IM conversations in order to reduce the risk of disgruntled employees handing out confidential data to competitors (Richeson, 2003).

The best option for businesses wanting to use IM is to purchase IM software specifically developed to be secure in business environments. There are companies that developed Enterprise IM (EIM) solutions, including AOL and IBM, that support features such as encryption, proper authentication against local directory service, internal network routing and many other features that otherwise require specialised IM management software. EIM also enables administrators to control client functionality allowing different users to use different features such as file transfers, voice and video chat depending on what they require to fulfil their job. Overall EIM solutions allow for much greater flexibility and customisation while providing a business with a secure IM solution that can greatly increase business performance and result in quicker responses and money savings.

5. Conclusions

This paper clearly identifies that P2P and IM applications can present a business with serious risks. It also identifies a lack of awareness of these risks on both user's and administrator's side. While some P2P applications were found to have little to no use within a business environment, IM applications, even though they present some

risks, can help greatly in improving business performance. There are many ways to manage the use of such applications but choosing the right policies and security measures depends entirely on each business' needs and budget. Businesses will have to assess the risks and compare them to the benefits that they can gain from IM technologies. Future research could investigate into ways of calculating return on investment of IM implementation and possible tools to aid with these calculations.

6. References

Audit Commission (2005), *ICT Fraud and Abuse 2004 - An update to yourbusiness@risk*. Audit Commission Publications, UK. June 2005

Computerworld (2001), "*Potential Uses Help Brighten Future of P2P*", http://www.computerworld.com/managementtopics/ebusiness/story/0,10801,58004,00.html, (Accessed 11.09.2005)

Hopster, (2005), www.hopster.com (accessed 11.09.2005)

IMLogic (2005a), *IMLogic threat center*, http://imlogic.com/im_threat_center/index_viewall.asp?mr=top3&hr=top3 (Accessed 11.09.2005)

IMLogic (2005b), *IM detector pro*, http://www.imlogic.com/products/im_detectorpro.asp (Accessed 11.09.2005)

Instant Messaging Planet (2004), "*Study: Enterprise IM Could Reap ROI in Days*", http://www.instantmessagingplanet.com/enterprise/article.php/3448631 (Accessed 11.09.2005)

Leavitt, N. (2005), "Instant Messaging: A New Target for Hackers", *IEEE Computer Society*, http://csdl2.computer.org/comp//mags/co/2005/07/r7020.pdf (Accessed 11.09.2005)

Leyden, J., (2005) "*BPI nails 'music pirates'*", published 04.03.2005, http://www.theregister.co.uk/ 2005/03/04/bpi_fileshare_settlements/ (Accessed 11.09.2005)

Libbenga, J., (2005), "Classified Dutch military documents found on P2P site", *The Register*, published 30.01.2005, http://www.theregister.co.uk/2005/01/30/dutch_classified_info_found_on_kazaa/ (Accessed 11.09.2005)

Ostermann Research (2004), "*Managing IM and P2P Threats in the Enterprise*", http://wp.bitpipe.com/resource/org_971197299_840/Osterman.pdf (Accessed 11.09.2005)

Richeson, J. (2003), "*Finding the Right Instant Messaging Solution for Your Company*", SANS Institute, http://www.tietronix.com/pressCenter/WhitePapers/Instant%20Messaging%20and%20Security.pdf (Accessed 11.09.2005)

Sherriff,L., (2004), "*MPAA takes filesharers to court*", published 17.11.2004, http://www.theregister.co.uk/ 2004/11/17/court_mpaa_suits/ (Accessed 11.09.2005)

Symantec (2005), Symantec search, http://www.symantec.com/search/ (Accessed 11.09.2005)

Wired News (2004), “Kazaa Delivers More Than Tunes”, http://www.wired.com/news/business/0,1367,61852,00.html (Accessed 11.09.2005)