

Project Number: HNH-HH08-45

INSTANT MESSAGING IN ENTERPRISES

An Interactive Qualifying Project Report

submitted to the Faculty

of the

WORCESTER POLYTECHNIC INSTITUTE

in partial fulfillment of the requirements for the

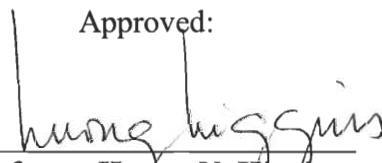
Degree of Bachelor of Science

by

  
\_\_\_\_\_  
**Nathan A. Makowski**

Date: July 14<sup>th</sup> 2003

Approved:

  
\_\_\_\_\_  
**Professor Huong N. Higgins**  
Advisor

## **Abstract**

This project aims at exploring the security issues of using instant messaging in enterprises, and measures for improving instant messaging security. Instant messaging can have significant social implications, and has potential to become the primary means of workplace communication. It was found that using instant messaging can result in serious security risks, including threats to network security and the loss of confidential information. However, these risks can be mitigated by user policies, educating users, and using secure instant messaging software.

# Table of Contents

Abstract .....	i
Table of Contents .....	ii
1 Introduction .....	1
2 Literature Review .....	4
2.1 Instant Messaging Background .....	4
2.2 Instant Messaging Industry .....	5
2.3 Enterprise Instant Messaging .....	5
2.4 Social Implications of Instant Messaging .....	7
3 Methodology .....	11
3.1 Planning and Research .....	11
3.2 Analysis .....	11
3.3 Project Plan .....	13
4 Findings .....	14
4.1 Security Issues .....	14
4.1.1 Control .....	16
4.1.2 Network Security .....	17
4.1.3 Social Engineering .....	18
4.1.4 Worms and Viruses .....	19
4.1.5 Encryption .....	21
4.1.6 Software Flaws .....	22
4.2 Security Measures .....	23
4.2.1 User Policies .....	24

4.2.2	User Awareness .....	25
4.2.3	Secure IM Software .....	27
4.2.4	Network Security .....	29
4.2.5	Standards.....	30
4.3	Products .....	32
4.3.1	AOL Instant Messenger Enterprise Gateway .....	33
4.3.2	Communicator Hub.....	33
4.3.3	Lotus Sametime .....	34
4.3.4	Microsoft Real Time Communications Server .....	35
4.3.5	Trillian Pro .....	36
4.4	Security Issues Summary.....	37
5	Conclusions .....	38
	References.....	40

# 1 Introduction

This project involved researching the current state of instant messaging (IM) technology, how it is evolving into a business worthy application, what security issues are associated with it, and what options a company has to protect itself from those security issues. Instant messaging is a private, text based communication tool that is not all that dissimilar from an Internet chat room. To this point it has been used primarily by consumers as a means for conducting personal conversations, however, the benefits of its use in business environments are quickly being realized.

There were three main goals associated with this research. First was to learn of the security risks involved in using instant messaging in enterprises. Unfortunately, the most common instant messaging clients, those intended for consumer use, were not designed with security in mind, and are often installed by employees without the knowledge or approval of their company. The second goal was to determine what measures can be taken to minimize those risks. One such example is the use of Enterprise Instant Messaging (EIM) packages, which are IM software packages designed specifically for businesses. These packages contain additional security and control features that are not present in consumer IM products. The third and final goal was to evaluate potential implications its use could have on the social environment of a business.

Research for this project was done primarily though the Internet, using various news articles, editorials, and white papers on the subject. The first step was to learn what functionality instant messaging offers that makes its use in a business environment desirable, as well as the social implications of that use both to the individual users and to a company's community as a whole. Upon understanding why a company should be

interested in instant messaging, the research then began to focus on the security issues associated with its use, as well as what options are available to minimize the threats posed by those issues.

The results of this research show that there are numerous security issues with consumer instant messaging clients. Issues include those of a technical nature, such as the lack of control features, threats posed to network security, vulnerability to viruses, lack of encryption, and software bugs, as well as non-technical issues such as social engineering and user awareness. While the issues are significant, the research has also shown that there are a number of measures a company may take to mitigate the risks caused by unsecured instant messaging. These measures include creating user policies to define how IM may be used, educating users of IM's risks and how to deal with them, using a secure EIM implementation, and keeping antivirus and network security software up to date. It was also found that there is currently a lack of IM standards for developers to use, which has caused some companies to hold back with any plans for IM implementations of their own. However, it is shown that for the companies that are ready to deploy IM on their networks, there are numerous software packages already available that range in both cost and scope, and should cover the needs of any business. It was discovered that many believe the use of instant messaging to have significant implications, including the ability greatly improve productivity; to bring together global communities, and ultimately having the potential to become the primary means communication in the workplace.

Instant messaging security is an important issue that should not be ignored. In order to prevent the loss of information or other damage to a company, it is vital that any company who has had consumer IM software installed on their network, willingly or not,

be aware of the risks associated with it, and what measures can be taken to address them. There are numerous options available to improve security; companies just need to take the time to determine what is the best course of action for them.

The report proceeds as follows. Section 2 is a literature review with general background information and a discussion of social implications. Section 3 is the methodology for how the research and analysis for this project was conducted. Section 4 contains the research findings about security issues, security measures, and a brief overview of some current instant messaging products. Finally, section 5 contains conclusions based on the research findings.

## **2 Literature Review**

### **2.1 *Instant Messaging Background***

Instant messaging (IM) is an Internet communication tool that creates a private chat room for two people to converse. Each user has a unique screen name, much like an E-Mail address. Typical IM software provides what is known as a buddy list. Buddy lists are along the same idea as an address book. Users add user names to their buddy list of the people they wish to keep track of. The buddy list in turn alerts the user whenever someone on his or her list is online and available to chat. Most IM software provides features that go above and beyond the basic messaging functionality. Some examples include file sharing, voice/video conferencing, remote access, and collaboration tools. (Dalton, 2003) IM is a great tool if you are sharing small amounts of information or need a quick reply to a question. It typically gets a response faster than email and costs less to operate than a telephone. (Langa, 2001)

Credit for the creation of instant messaging is given to an Israeli company, Mirabilis, who in November of 1996 released a product named ICQ. It was a standard instant messaging implementation based upon peer-to-peer communications. It allowed people on the Internet from all over the world to communicate in real time. Within six months of its release, the product had attracted nearly a million users, and went on to become the largest Internet communications network within a year. Due to its success, America Online purchased the company in 1998 for \$287 million. (Stewart, 2001)



## **2.2 Instant Messaging Industry**

Today the instant messaging industry is segmented among three main IM clients, which are AOL's AOL Instant Messenger, Microsoft's MSN Messenger, and Yahoo's Yahoo Messenger. The client software for each of these implementations is available free to download and use. Because each of these companies developed their IM technology independently, none of these clients are compatible with each other, resulting in people often having to install multiple clients in order to reach all of the people they wish to communicate with. It is estimated that over 500 million computers will have instant messaging software installed on them by the year 2005. (Symantec, 2003)

It is predicted that the number of people using IM at work worldwide will grow from around 65million today to 255million by the end of 2006, in which case it will have surpassed E-Mail to become the number one method of online communication. (Hallett, 2003) Software developers are beginning to realize that there is a ton of money ready to be made off of enterprise instant messaging systems and are now hurrying to get competitive products to market. It is expected that the total amount companies spend on instant messaging products shall increase from around \$133million in 2001 to \$1.1billion by 2005. (Chediak, 2001)

## **2.3 Enterprise Instant Messaging**

While IM was not developed with enterprise use in mind, it was only a matter of time before enterprises began to realize the benefits it could provide them. Instant messaging can allow employees to communicate instantly from anywhere, which is particularly appealing for traveling employees as it gives them the ability to communicate

as if they were in the office with everyone else. It can allow instant communications between clients and vendors, providing the ability to give real time customer support over the Internet. Instant messaging can also cut down on the amount of E-Mail a company sends and receives, which can be significant due to the amount of time people can spend sorting through junk E-Mail. The same can be said for the amount of phone calls employees make. IBM, for example, has measured a 5% drop in their phone usage since they have installed instant messaging in their offices. (Brockmeier, 2003) It is expected that as instant messaging becomes increasingly popular, it will in time be able to reduce a company's E-Mail volume by up to 40% and voice mail by up to 15%. (McDonald, 2002)

Many instant messaging products developed specifically for the enterprise have the ability to manage presence. Presence is the ability to see whether other people are online and available to be contacted. It creates a link between people and their communication devices. For example, imagine an employee working on a particular file and they reach a point where they need consultation before they can proceed. With their enterprise IM application, they would be able to see that their supervisor is online and available. The employee could then send the supervisor an instant message and through the software's collaboration tools, together they could go over the file and decide how to proceed. Neither would have had to leave their desks, they could communicate at their own pace, doing other things in between messages if need be. Decisions could have been made faster than what would have been possible if the question had been sent through E-Mail or had a face-to-face meeting been required. Presence along with the real-time communications capabilities of instant messaging can increase the flow of information

and decrease the time spent waiting for answers, giving it a very real and measurable ROI.

## ***2.4 Social Implications of Instant Messaging***

Perhaps the most interesting and significant aspect of instant messaging is its social implications. It is a technology that has the potential to fundamentally change the way in which people communicate. In fact the true value of instant messaging can only be appreciated when viewed in its social context. Possibly the largest asset any business has its social network, which is a community formed of its employees, business partners, and perhaps even competitors. It is from this network that thoughts and ideas are created, discovered, promoted, or destroyed. (Weinberger, 2002) Companies are able to function because of communication. Information gets passed from one person to another, groups work together on projects, problems and concerns get expressed, and these things are mission critical to the very operation of a business. Instant messaging can bring a community closer together than any other communication technology, perhaps even closer than what is possible in real life. IM provides its users with a digital presence, rather than a physical presence, meaning they are not held back by normal physical constraints. With instant messaging, a person could in theory have individual conversations with multiple people all at the same time. These people could be in another building, another state, or even in another country. People communicating through instant messaging do not even have to speak the same language, as the technology is capable of real time translation. This alone has the potential to bring together global communities where people from one branch of a company can communicate with those in another branch on the other side of the world, yet talk as if they were sitting in the same office.

The ability to change society is what makes instant messaging so unique, interesting and important, and is enough reason to make it hard to believe that IM will not succeed.

(Dyson, 2002)

Instant messaging on the surface may appear to be just like an instant E-Mail, but it is often not perceived that way. It is considered to be more along the lines of an actual face-to-face communication. What is unique about it though is that because the people communicating are not really “seeing” or “hearing” each other, people tend to be more open and honest in what they say, often saying things they never would have in a face-to-face conversation. This too is significant because it means more ideas will get out, more opinions will be expressed, and ultimately the overall value of the communications will increase. It gives people the ability to spend more time thinking about what exactly they want to say and how they want to say it. They have ample time to think about the implications of what they might say and as a result, may decide differently. Likewise, because instant messaging communications are not face-to-face, race, gender and age become unknown, thus freeing people from the perceptions and prejudices of every day life.

Because communities can form through instant messaging, social norms, and consequently, deviants from those norms, will develop that are unique to these online communities. This can already be seen on the consumer instant messaging networks, which have their own language, and ideas about acceptable practices. People using these networks over the years have found ways to express emotion through text, something that is usually not worried about with other types of text based communications, and is further proof of instant messaging being thought of more like a verbal communication. Much

like in real life, people will have reputations that are unique to their online presence. People need to worry about what they say, how they behave, because it has the potential to damage their reputation not only online but offline as well. (Enbysk, Undated)

Among all the societal benefits of instant messaging, there are also a few issues. Perhaps the most significant issue is privacy. There is some question about whether or not a company should have the right to monitor instant messaging conversations. (Hillson, 2002) Monitoring E-Mail is a fairly common practice, however because instant messaging networks are perceived as a community, monitoring what is said may give users the perception that they are being suppressed. At the same time it is important that a company protect itself from the loss of confidential information.

The presence management functions of instant messaging are also a privacy concern because it creates a situation where a person can be tracked wherever they are, at all times, anywhere in the world. Whether a person is in a taxi on a cell phone, in a conference with their PDA (Personal Digital Assistant), or sitting at the computer in their office, their presence is always reflected accordingly. The communication benefits of this are tremendous, but there is something to be said for being able to get away from it all, a luxury that presence management will make that much more difficult to achieve.

Another issue, and one that has even slowed the adoption of IM to an extent, has been that it is often viewed as a time wasting technology. There are some grounds for this belief as most people to this point have used instant messaging at work primarily for personal communications with friends or family. Approximately 88% of current users of IM in the workplace use it only for personal communications. It should be noted however that this same belief has been applied to E-Mail, web access, and even the telephone

throughout history (Hallett, 2003) Regardless, there is no doubt that if IM is misused, it can indeed have negative effects on productivity.

## **3 Methodology**

### **3.1 *Planning and Research***

Information for this project was gathered primarily via the Internet, specifically web news articles, editorials, white papers, and product pages. A preliminary research helped compile a general list of technical and non-technical security issues, as well as list of measures that can be taken to protect against IM related security risks. Each item on these lists was then further researched for additional detail. The survey of IM products was also conducted through Internet information research.

### **3.2 *Analysis***

After the information gathering was complete, the identified security issues were grouped into categories with other similar or related issues. The category titles that were chosen were based on the relation among the issues. For example, issues that involved threats to the security of a network were grouped into the network security section. The categories that were decided upon were: control, network security, social engineering, worms and viruses, encryption, and software flaws. Likewise, security measures that were of the same type were also grouped into categories, which were: standards, user policies, user awareness, secure IM software, and network security. In some instances, the analysis brought about additional issues or measures, in which case they would be further researched and worked into the existing categories.

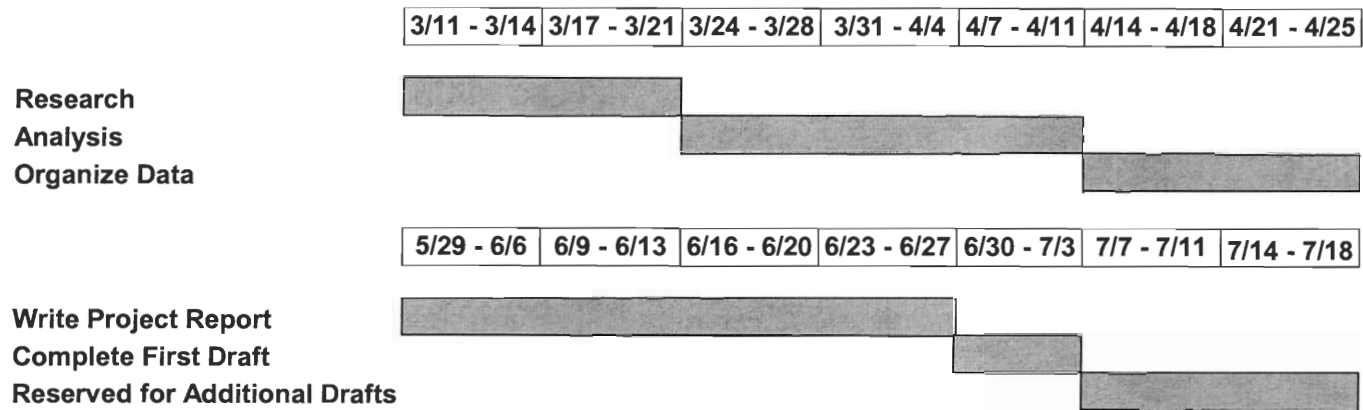
For the product overview section, it would not have been possible to provide information on every instant messaging product encountered during the research phase,

therefore only a select few products were chosen. They were selected primarily based on their unique approaches to secure instant messaging, in order to show the various types of options that are available. The products that were selected are: AOL's Instant Messenger Enterprise Gateway, Communicator Inc.'s Communicator Hub, Microsoft's Real Time Communication Server, IBM's Lotus Sametime, and Cerulean Studios' Trillian Pro.



### 3.3 Project Plan

This project attempted to follow the schedule shown below as closely as possible.



## **4 Findings**

The research resulted in a list of security issues, as well as a list of measures that may help improve security. Instant messaging security issues consist of inadequate control features, threats to network security, the potential for loss of confidential information by means of social engineering or information theft, vulnerability to worms and viruses, the lack of encryption for messages and transferred files, and flaws in the software's design. Measures that may be taken to mitigate the effects of these security issues include developing user policies to define how IM may be used, educating users on the risks of instant messaging and how they may avoid them, implementing secure EIM software packages, and keeping network security features up to date. It was also found that there is currently a lack of instant messaging standards, which has to some extent slowed the progress of IM from a security standpoint. This lack of standards has made many companies decide to wait before buying into IM, but for those that are ready, there are a number of instant messaging products currently available that should be able to meet the needs of businesses of all types and sizes.

### **4.1 Security Issues**

Instant messaging was not really designed with security in mind; it was designed to be an entertaining communication tool. (Langa, 2001) Only recently has its use as a business application been considered. Unfortunately, the consumer IM clients have significant security issues that must be addressed if IM is to reach its full potential in the workplace. Issues discussed in this section include: control, network security, social engineering, worms and viruses, encryption, and software flaws.

Consumer IM clients often lack important control features. Most do not offer any means to manage accounts from a centralized location; meaning it is the users, not the company, who is in control of the software. This can be a real problem because of the network security risks associated with IM use. IM software opens up ports on a company's firewall, which may allow a hacker easy access to the network. It is very difficult to block IM software at the firewall, because it has been designed to use any means necessary to find a way through. Only with proper control features could its use be prevented.

Instant messaging today is possibly even less secure than E-Mail, especially in regard to worms and viruses. For example, most viruses sent through email need to be downloaded and executed by the user, where as with instant messaging a hacker in theory only needs a persons screen name to be able to send the virus, hack into that persons computer, and execute the virus their own. (Frase, 2002) There are many ways a hacker may gain entry to a system, but one particular method is through exploiting flaws in IM software. Companies have put so much effort into securing things such as E-Mail and web access, that it is forcing hackers to look for other ways to attack systems. IM, because of its relative youth and its known flaws, is likely to be a prime target for hackers in the immediate future. (Vamosi, 2002)

Perhaps the most serious issue a company must be concerned with in regard to instant messaging is the loss of confidential information. (Frase, 2002) This could occur many different ways. One possibility is for a hacker to use social engineering tactics, such as impersonating someone familiar, to dupe a user into giving out company information. Another possibility would be for a hacker to eavesdrop on a conversation, or

intercept files being sent between clients. This would not be entirely difficult, as many IM clients do not encrypt the messages or files sent through their networks.

Despite all of these issues, it is expected that the free IM clients will have found their way into 70% of businesses by the end of 2003. (Frase, 2002)

#### **4.1.1 Control**

Most IM software today lacks significant control features. For a matter of fact, some of the IM clients don't even allow users to specify that only the people they know may initiate a conversation with them and/or add them to their buddy list. This can be a problem because there is IM targeting worms in existence that use the buddy lists to spread to other users. (Frase, 2002) This means that users can be put at risk just by having someone add them to their list. Without the ability to control this, there is little that can be done to protect oneself from such viruses.

The lack of control is also apparent by the fact that in many cases, IM software is downloaded and installed by the user, without the permission or even knowledge of the company. (Barlas, 2002) If a company does not regulate the use of IM on their networks, they leave themselves open to many serious security threats, such as IP address exposure, eavesdropping, and viruses obtained through file transfers. (Frase, 2002) Companies need to be in control of the software on their networks if they wish to ensure its security.

The password systems of the consumer IM clients are under control of the users rather than the company, as they are usually personal accounts. These password systems also have very limited protection. If a user has their password stolen, they may not know how to deal with such a situation, and may to decide to ignore it entirely. This is a problem because then you have someone out there who is able to use this account,

impersonate the original user, and potentially cause problems for anyone on that person's buddy list. On the other hand, if a company's IT department had been in control over the password, the user would have been able to report the problem and had it dealt with appropriately. It is the users who are the biggest security threat with instant messaging, or any kind of network software for that matter. Without adequate control, companies will have a much more difficult time preventing and dealing with issues as they arise.

#### **4.1.2 Network Security**

Many companies attempt to block IM software by blocking the ports it uses to connect to the Internet. This is a very ineffective technique, however, as most IM clients were built to find any way possible to get through to the Internet. (Dalton, 2003) If the software finds that its normal port has been blocked, it can search for an open port and auto configure itself to use that port. Often the software is designed to first try ports that the developers know companies are not likely to block (such as those used for FTP, HTTP, or Telnet access). (Vamosi, 2002) Once the IM client has found a port to use, those ports remain open throughout the entire time that the user is signed in. It would not be difficult for a hacker to gain entry to the system through those open ports. In the case that the software is unable to find a port it may use, it can then attempt to use a proxy. The proxy has the ability to disguise the packets sent by the IM software so that to a firewall, they appear to be HTTP packets and thus are allowed to pass through. (Hindocha, 2003) There are a large number of proxy servers available that may be used for this purpose, so many that it would be nearly impossible to block them all. Most people don't realize that even if they are having an IM conversation with the person in the cubicle next to them, the messages still have to travel out of the company's network,

over the Internet, to the IM server, and back again. There are ample opportunities for hackers to hijack that message along the way.

IM software is designed to always be running in the background. In many cases if the user attempts to close their buddy list, it simply disappears from the screen and continues to run in the background, constantly letting others know of the users presence (which is what allows other users to see that they are online). (Langa, 2001) This is significant because it essentially turns the software into an “always on” security threat. So long as a user is online, hackers can see that they are there, which only makes it easier for them to attempt an attack.

It is also important to remember that its not just the company’s own network that one needs be concerned with. Because many IM clients connect to an external server, there is also the possibility that the IM server itself could come under attack. If a hacker were to gain access to one of these servers, they could monitor all conversations as they take place or even launch denial of service attacks, which bombard a network with useless traffic in order to essentially slow its operation to a halt. (Symantec, 2003)

### **4.1.3 Social Engineering**

Social Engineering is a technique used by hackers to attempt to trick IM users into giving out information about a company’s security system or to convince a user to download a virus (usually disguised as some other file type that the user would expect to be receiving). (Gaudin, 2002) The concept of social engineering works because people are generally too trusting, they don’t think that IM can be used against them, and are overall just ignorant of the security risks associated with it. The problem is augmented by the common practice of using the software for personal communications (with friends,

family, etc.) rather than business purposes. If people are using the software mostly for entertainment and not as a business tool, they will likely be less cautious when receiving a message from people they do not know. (Lyman, 2002) What makes social engineering so dangerous is that it does not make any difference how many security measures a company places on their network, as no firewall will stop it. If a user is tricked into downloading a trojan horse virus or giving out security information, attackers may gain nearly unlimited access to the company's network (Hindocha, 2003)

Social engineering can be accomplished a number of different ways. A common technique is to send an instant message to a user offering some interesting opportunity, such as entering a contest. The user is prompted to click a link to reach the contest page, when in actuality clicking the link results in a virus being placed on the users computer. (Gaudin, 2002) Another technique is to try to befriend the user, carry on a casual conversation until they trust the hacker, at which time the hacker attempts to send them a virus disguised as a normal file. People need to remember that there is no way to be sure that who you think you are talking to is who is really on the other end of the conversation. Just because it's a familiar screen name, it doesn't mean that that's actually the person sitting at the other computer. This is especially true in an enterprise where it wouldn't be entirely uncommon to receive instant messages from unfamiliar people. (Frase, 2002) At the moment there is no sure solution to this problem. Educating users can go a long way towards minimizing it, but it is by no means a foolproof answer.

#### **4.1.4 Worms and Viruses**

There are many worms and viruses that are designed specifically to spread through IM networks. Unfortunately, antivirus software is nowhere near as good at

dealing with IM viruses as they are with viruses spread through E-Mail. There is currently no antivirus software that can specifically seek out incoming instant messages, because the messages are often so well disguised. It is possible to install gateway antivirus software on proxy servers or firewall servers, but these options can cause significant performance degradation across the entire network, and are likely to be too overwhelmed to prevent a virus infection through IM anyway. (Frase, 2002) Some standard antivirus software can scan the files downloaded through the file sharing features, but this usually doesn't happen until after the file has been downloaded. The lack of standards in the IM industry has been a big factor in holding back anti virus software developers because as it is now, the software is constantly changing, there are no set rules, thus software designed to work with the clients available now may not function correctly with future versions. (Hindocha, 2003) It is likely that as antivirus software gets better and better at catching viruses sent through E-Mail, more viruses will be developed to spread through IM instead, so the threat is only going to increase.

Trojan horse viruses that spread through IM can allow hackers full access to not only the infected computer, but also the entire network it is on. Even if the infected computer has a dynamic IP address (a different IP address each time the computer connects to the network), the virus is capable of sending that address back to the hacker each time the infected computer logs on. A hacker can then use that address to gain access to the network using the ports being opened by the IM software. This is significant because if the hacker does not need to attempt to open up additional ports then there is less of a chance they will be discovered. These same trojan viruses can be designed to also send the users password back to the hacker. (Hindocha, 2003) With these trojan



viruses in place, a hacker has the ability to use the infected computer and potentially all of the computers on that network to conduct large scale denial of service attacks.

#### **4.1.5 Encryption**

Many IM clients do not encrypt the messages sent by users, but instead send the messages in plaintext format. (Hindocha, 2003) This is a considerable design flaw, especially considering there are hacker “tools” which have been made to enable spying on unencrypted instant messages. The lack of encryption only makes it easier for hackers to break into conversations. (Dalton, 2003) This is yet another example of a problem that really isn’t difficult to solve, as there are numerous encryption algorithms available, but just hasn’t been dealt with yet because of the lack of standards. If various IM products are going to be able to communicate with each other, then their encryption techniques need to be compatible as well.

People often get a false sense of security using IM because of its speed. Because it is an instant communication, it is easy to equate it with a face-to-face conversation, in the sense that as soon as something is said, it is gone and not accessible by outsiders. This however couldn’t be further from the truth. Some IM software keeps a log of all communications. For a matter of fact, some companies, such as those in the financial industry, are required by law to keep such logs. It is vital that these logs also be secured and encrypted or those who weren’t meant to see them may access them, long after the conversations had taken place. (Hindocha, 2003) It is not a good idea to talk about sensitive information over an IM conversation because these logs are kept. No IM conversation should be considered confidential. In many cases, the user agreements of IM software specifically warn of talking about confidential, or mission critical information

over IM. (Langa, 2001) The developers realize that there is just not enough protection in place to make such conversations safe, and these user agreements are just their way of covering themselves.

Not only are the conversations not encrypted, but also neither is the files sent through the file sharing functions. (Symantec, 2003) This is particularly troublesome if IM is to be used in a business because the ability to send important documents quickly among employees would be one of the main uses of the technology. If those files are not encrypted then anyone could intercept them and read them with little difficulty.

#### **4.1.6 Software Flaws**

All software has bugs and IM clients are no exception. Most IM clients have bugs or design flaws that make a hackers job even easier. Security was certainly not a focus during the development of the current generation of consumer IM clients. Things like scalability, user friendliness, and useful features were given much more thought. In all likelihood though, even as future generations of instant messaging software are designed with more security, their added complexity will probably result in more bugs and thus more leverage for hackers. (Lymen, 2002) With additional security features in place however, the main way hackers are likely to attack IM is through exploits in the actual software. As a result of this, as standards are developed which make the various clients compatible with each other, IM developers will need to focus more on secure design in order to differentiate there products from those of their competitors. (Hindocha, 2003)

The address book features found in many E-Mail programs have been a favorite target of viruses for some time now, as they provide the viruses with more locations to spread to. The buddy lists used by IM clients are likely to be the equivalent point of focus

for viruses that spread through IM networks. If a virus were designed to spread in such a fashion, it could potentially spread to tens of millions of users within a few hours.

(Symantec, 2003)

Many clients even have fairly simplistic password systems, which leave them vulnerable to having their accounts stolen, which in turn can result in those accounts being used to spread viruses or being used in denial of service attacks. If a hacker is able to steal another users account, the hacker may be able to impersonate that individual. He could contact all of the people on that persons buddy list and try to get information from them or send them viruses. Those people would likely be trusting, as they wouldn't realize that the person they were talking to wasn't who they believed it to be. (Symantec, 2003) Passwords are a very basic form of security, but that doesn't mean they should be implemented in a non-chalant fashion.

## **4.2 Security Measures**

Instant messaging today is going through the same growing pains that E-Mail went through some time ago. Actually, in time it is likely that IM security will be handled very much the same way that E-Mail security is done now, meaning people will be basically free to use it, but there will be measures in place to make it as secure as possible. (Barlas, 2002) Measures discussed in this section include: user policies, user awareness, secure IM software, network security, and standards.

Right now, IM is often installed without the permission of the company. This practice really needs to stop, or IT departments may find themselves overwhelmed with the number of threats they need to deal with. Unfortunately IM is very difficult to block outright, thus they must rely on sound user policies, and the compliance of the users with

those policies, if they are going to beat this problem. Likewise, anti virus was and in many ways remains ill equipped to deal with the new IM threats it is facing. It is therefore important that employees be educated on the threats of IM and how to deal with and avoid them.

Many of these problems are avoidable by selecting an enterprise IM solution, which generally provides better overall security and functionality. But this too has its drawbacks, such as cost and lack of interoperability with the popular IM networks. (Frase, 2002) If IM is going to become a serious communication tool in the workplace, companies are going to have to be sure it is handled correctly.

Standards are one critical area where IM is currently lacking. Standards result in better security by allowing the developers to spend less time deciding how their software will work, and more time ensuring that it is as secure as possible. Much effort has been put into developing an IM standard, now it is only a matter of time until we will begin to see if developers will embrace the standard. (Lowe, 2002)

#### **4.2.1 User Policies**

Companies should create user policies to address the IM issue (or include it in their existing policies). They need to specify how, if at all, it can be used, and who can use it. These are very situational decisions; some companies may opt to allow everyone to have IM, while others may provide it to only those who “need” it. What is most important about a user policy is making sure the users are aware of its existence and what exactly it states. They also need to know the consequences of ignoring the policy, both to the company and to themselves. It is important to remember that a policy has no value if it is not enforced. It may be a good idea to forbid giving out any company related

information, any logon info, the clicking of links sent over IM, or sending instant messages to people outside of the company. (Gaudin, 2002) Users policies are not there to hassle the users, they are there to protect the interests of the company. Even if the users end up ignoring them, at least the policies existence will have the company covered legally if such a situation came about. Unfortunately, a recent survey suggests as much as 70% of businesses don't include guidelines on the acceptable use of instant messaging in their user policies. (Woods, 2002)

Usually employees have to make due with the software that is provided to them. IM seems to be one of the exceptions to this rule. More often than not IM clients are installed without the approval of the company. While it may not be easy (or worthwhile considering the required effort) for companies to stop this practice outright, it is a double standard that may be best dealt with in the user policy. (Lowe, 2002) Employees could be told that they are not allowed to download software without approval, and they are responsible for any problems that arise if they choose to ignore this rule.

#### **4.2.2 User Awareness**

A survey of network security managers found that 58% of them say that the improper use of communications software, such as E-Mail and IM, is the biggest threat to their company's network. (Woods, 2002) Educating users is an effective way to minimize the IM security risk. If the users are aware of the risks then they will have much better situational awareness. They will know what to look out for, and how to prevent and deal with situations as they come about. Plain and simple, education improves a company's ability to respond to security threats. Employees need to know about the ease of getting a virus through IM, and the various tactics a hacker may use to try to transfer a virus. The

better educated the users are, the less success hackers will have with attacking through IM. If hackers don't have success with IM, they'll eventually just look elsewhere instead. (Hindocho, 2003)

Users need to be taught that they shouldn't use unsecured IM for conversations that may involve sensitive information. Financial info, medical info, confidential company info, mission critical info, these are things that probably should be kept to other forms of communication. (Enbysk, Undated) Again it is important to remember that IM is a situational tool. It is most effective when used in the proper circumstances. If you need to ask someone a question that does not need an immediate answer, but you would like a faster than E-Mail response, then is a good time to use IM. If you are traveling and need to send or receive a status update to/from the main office, then is a good time to use IM. If you want to set up a meeting, be it a conference or just lunch, then is also a good time to use IM.

Inform users that what they can say over IM should not be considered private and can be seen by others. Some systems will log all IM conversations, but even if the company does not specifically log the conversation, it is possible for either individual taking part in the conversation to save a copy of it. They may also copy and paste the text into a text file or in another IM conversation. Saying the wrong thing in an unsecured conversation, especially when you can't be 100% sure of who is on the other end, could lead to some embarrassing situations, and potentially even damage a person's reputation. It would be wise to suggest to employees that they be as careful with what they say over IM as they are with E-Mail, if not more so. (Enbysk, Undated) There are companies working on the development of digital certificate technology to be used for instant

messaging (much the same way that similar technology has been under development for E-Mail for some time now). In time this could add an additional level of security and an assurance that people really are who the application says they are. (Clancy, 2002)

### **4.2.3 Secure IM Software**

Companies likely don't want to block IM entirely because after all, its use does have numerous and significant benefits. However, without sufficient security features, it's just not worth the risk. The up and coming answer to IM's security issues are enterprise class instant messaging software packages. Right now there are over 25 million users of instant messaging at work in the U.S., but only 6 million of those are using enterprise class systems. (Brockmeier, 2003) These are IM implementations that have been designed from the ground up with enterprise use in mind. They generally are more secure and offer additional control features to make them more acceptable to companies who are concerned with the security of their network. With the standard IM clients, it can be difficult if not impossible to disable specific features (such as file transfer), but enterprise solutions should allow each company to decide exactly which features they do and do not wish to offer to their employees. (Lowe, 2002) Enterprise class IM solutions are probably the future of the industry, but their progress has been held back by the lack of an IM standard. (Lyman, 2002) It may seem strange to have to pay for something that traditionally has been available free for download, but the additional security and control features are well worth the price.

Instant messaging is going to have to include encryption before it is going to be seriously considered by enterprises to be a worthwhile investment. Today we are beginning to see many enterprise IM packages add encryption to the messages they send.

However if a company is not yet ready to put down the money for a full enterprise IM solution, there are other options. There are programs available, such as Cerulean Studios' Trillian Pro, which can encrypt the messages sent by the standard popular IM clients. (Hindocha, 2003) It is also important to remember that encryption is only a partial solution. No available option solves the problem of firewall ports being opened up by the IM software. (Woods, 2002)

Another option would be for a company to develop a propriety IM solution on their own. The problem with this option is that it would likely have less functionality than the packages they could purchase, and after all, why reinvent the wheel. A propriety solution would not be able to communicate with other IM networks, meaning it would likely be limited to use only within the company. This will be less true as a standard becomes more widely available, but in the mean time it may be difficult to future proof the software with the intention of having it connect to other networks sometime in the future. (Dalton, 2003)

Whether a company is using an enterprise class IM package or sticking with the standard IM clients, they need to be sure to keep their software up to date. Download all of the patches and updates that become available for the software, ASAP. These updates often fix security flaws that have been discovered since the last release. But also be cautious, as these updates may also introduce new security flaws for hackers to exploit. In any case it would likely take hackers some time before they could discover these new flaws, so it is still important to keep software updated. Some IM software has the ability to auto update itself as the patches become available. This is a good option to have



because it takes the responsibility away from the users, who often don't remember to download updates, or don't consider it to be important.

#### **4.2.4 Network Security**

The more instant messaging is used, the more appealing it will become to hackers as a way to break into systems. This is just a natural progression of the technology and is to be expected. The CERT Coordination Center, the "first computer security incident response team", already has reports of over ten thousand systems being compromised via IM. (Gaudin, 2002) An ideal way to secure IM would be to prevent its use, or at least the use of the unsecured consumer IM clients, would be to block it completely. Unfortunately it is very difficult to do so, both on the desktop and at the firewall. (Hindocha, 2003) To combat this, some suggest using a network logging system to monitor network traffic for suspected IM use. Let the users know that they are being watched and that unapproved IM is not allowed, and they will probably think twice about downloading it. (Dalton, 2003)

Trying to secure IM at the firewall level is not very effective, for reasons discussed earlier, but that does not mean you shouldn't still tighten it up as much as possible. It may not stop the best of hackers, but it may stop some, and either way, there is no reason to make their ability to launch an attack any easier than it already is.

Even though most anti virus software cannot directly filter incoming instant messages for viruses, it is still a very good idea to keep your virus software up to date. Make sure you download the latest virus definitions as soon as they become available. It may not stop viruses from entering the system, but at least it can catch viruses when they do reach the desktop level. Good anti virus software on all desktops can be considered the

last line of defense in keeping threats away. (Frase, 2002) Symantec's anti virus 2003 product is able to scan the files transferred over IM for various types of viruses, though not the messages themselves. Part of its functionality is to detect a virus, delete it, and then inform the user of the actions it has taken. In past versions, the user would have been presented with options about whether to delete the virus, quarantine it, or do nothing. This new way, the user has less involvement and thus is less likely to cause a problem by taking inappropriate action. (Gaudin, 2002)

Whenever possible, companies should try to handle any software updates at the server, be it downloading the latest virus definitions or installing the newest patch for the IM software. By doing updates remotely from the server, the company can be sure they are done properly and on a timely basis. Most importantly, by doing the updates from a central server, they take the responsibility away from the users. The less a company relies on its own employees to be smart about security, the better their security will actually be.

#### **4.2.5 Standards**

Standards are important to security because they create guidelines that a product must adhere to. As of today, there is no one dominant instant messaging standard. The consumer IM networks all have their own propriety protocols, which prevents the users of one service from communicating with those on another service. The companies behind these products have thus far been unwilling to open up their networks, mostly because each has their own community of users, which is how these products generate revenue. Each company includes advertisements to their IM client software, and they are able to charge for those ads based on the size of their community. Opening up their networks to competitors would essentially destroy their business model. (Brockmeier, 2003)

There are two frontrunners in the race to create a standard for enterprise instant messaging. These are SIMPLE (Session initiation protocol for Instant Messaging and Presence Leveraging Extensions), and XMPP (eXtensible Messaging and Presence Protocol). The body working on these standards is the Internet Engineering Task Force (IETF). So far, both protocols have the backing from major industry players. Microsoft, IBM, and Sun Microsystems have put their faith in SIMPLE, stating that they feel it is a better protocol for doing more things than just standard instant messaging (such as voice/video and presence through multiple devices). On the other hand, HP, Intel, Hitachi, and Sony have chosen XMPP for their upcoming products. The advantage of XMPP is that it was built specifically for instant messaging and presence, and it is also much further along in development than SIMPLE. It is expected that the IETF will complete the XMPP standard within a few months, where as there is much work yet to be done on SIMPLE. Despite the SIMPLE standard being incomplete, both IBM and Microsoft are releasing SIMPLE based products this year, but because they have had to fill in the incomplete parts of the protocol on their own, their products will not initially be compatible. The fact that IBM and Microsoft have both settled on a single standard has led some to believe that SIMPLE will ultimately become the dominant standard. On the other hand, given the relative advantages of both protocols, it seems more likely that it will take a hybrid standard to truly become accepted industry wide. (Moore, 2003)

Some companies have expressed the desire to wait for the consumer IM networks and EIM packages to be interoperable, through standards, before committing to a solution. They cite the vast community of users found on the consumer networks as a reason for waiting. On the other hand, some companies hope that such interoperability

never comes to be. The reasoning is that having EIM solutions based on a specific standard would create a community much like those found on the consumer products, except they would exist entirely in businesses and organizations, making for a more professional and controlled environment. (Saunders, 2003) Instant messaging has become as popular as it is today in no small part because of its uncontrolled nature. However what enterprises need is as much control over their instant messaging solutions as possible. Interoperability would only decrease their control, and thus it may not be as desirable or necessary as some have made it out to be. Regardless of how ~~of how~~ interoperability and the standards race turns out, it would be good advice for any company to make sure that the vendor they select for their instant messaging solution be able to provide a thorough plan on how they intend to handle the migration to these functions as they become available. (Weinberger, 2002)

### **4.3 Products**

This section contains a brief overview of a handful of current enterprise class IM products. Products covered include: AOL's AOL Instant Messenger Enterprise Gateway, Communicator Inc.'s Communicator Hub, IBM's Lotus Sametime, Microsoft's Real Time Communication Server, and Cerulean Studios' Trillian Pro. Every business has different needs and each will have to decide what is the best method for using instant messaging in their particular company. These products were selected because each represents a different approach to making instant messaging an enterprise worthy application. These products are from major players in the industry, and provide good examples of the different types of products available and what standard features and functionality to expect from EIM packages.

### **4.3.1 AOL Instant Messenger Enterprise Gateway**

AOL's Instant Messenger Enterprise Gateway was chosen because AOL's consumer IM network is the largest of the major vendors, so it is interesting to see how they have decided to handle an enterprise class product. The AIM Enterprise Gateway actually builds upon the consumer client, adding the features that are vital for enterprise use. New features include encryption of instant messages, routing of internal messages through the company's network so that they never cross the corporate firewall, creation and management of screen names directly from the corporate directory, permissions restrictions for software features at a group level, and message monitoring and logging. (AOL, 2003) What AOL has done with this product is taken its consumer client and added additional security and a means for a company to control its use. By doing so, they have kept the product very similar to the consumer client, thereby making it easy to use and being able to leverage its already vast user base as a major benefit. The down side of this approach seems to be that at least so far, some of the standard features found in the consumer client have not received a major upgrade. For example, the presence features of the enterprise product are not that much more advanced than what is available in the consumer client. This is disappointing as AOL's consumer client arguably has the least advanced presence and privacy features of all the consumer clients.

### **4.3.2 Communicator Hub**

Communicator Inc.'s Communicator Hub service is noteworthy because it aims to create large communities by connecting multiple companies from a single industry. Its intent is to promote communication among colleagues, suppliers and customers, to the benefit of all those involved. The financial industry in particular has been very successful

in its deployment of Communicator Hub. Currently there are over 30,000 users in eight of the world's largest financial institutions using the service, including J.P. Morgan, Merrill Lynch, Morgan Stanley, among others. Similar setups are being implemented for the government, and the insurance and healthcare industries. The communicator application can be accessed either from a web browser or a client application. It has the expected assortment of features, including secure messaging, collaboration tools, message logging, in addition to features such as application management (controlling application access through identity management) and specialized content management tools to allow companies to keep their own information private from other companies in the community. Because it is intended as an industry wide solution, the product is able to meet industry requirements where necessary, such as Patriot Act and HIPAA (Health Insurance Portability and Accountability Act) compliance. (Communicator Inc., 2003)

### **4.3.3 Lotus Sametime**

IBM's SIMPLE based "Lotus Sametime" (Soon to be renamed Lotus Web Conferencing and Lotus Instant messaging) is the current enterprise instant messaging leader with over 8 million users, including over 60% of the Global Fortune 100 companies and some of the worlds top commercial banks, automobile manufacturers, financial institutions, and pharmaceutical companies. Sametime offers standard enterprise IM features such as presence awareness, authentication and access controls, secure messaging, and directory support. It is comprised of three main components: The Sametime Server, which is used to manage the flow of communications through the network, be it audio/video, instant messages, or shared applications. Second is the Sametime Connect Client, which is the end user software that is used to communicate

with other users. Finally there is a developer toolkit, which allows a company to expand the software's capabilities to be able to interface with their own applications. Additional components are available that offer features such as allowing users to communicate with people outside the company's network, the ability to setup large scale web conferences, and to extend presence awareness to a users mobile phone or wireless PDA. (IBM, 2003)

#### **4.3.4 Microsoft Real Time Communications Server**

Microsoft's take on EIM has been somewhat different than that of others. Rather than creating a standalone instant messaging product, they have opted to develop a foundation for others to build upon. Their Real Time Communications Server does offer secure instant messaging, logging, and presence capabilities, but its goals go far beyond these features. Microsoft hopes to revolutionize the way people collaborate in the workplace by providing a single platform to manage and integrate video conferencing, telephony, application sharing, and other collaborative technologies. The product is built upon the Session Initiation Protocol (SIP) standard, and therefore can handle multiple types of communications and presence awareness across a number of different devices. It is available as a standalone product or as an add-on to Windows Server 2003. Parts of it will eventually be embedded into Microsoft Office, to allow for real time document sharing while communicating. (Microsoft, 2003) Developers and companies themselves will be able to use the platform to integrate with their own applications, so that it can meet their own specific needs. An example of this can be seen in the Reuters Group, a news and financial intelligence company, who has created its own messaging service based on the technology, for use by its employees. (Saunders, 2003)

### **4.3.5 Trillian Pro**

Cerulean Studios' Trillian Pro is a very unique product. It allows a person to communicate with all of the consumer IM networks using just a single program, essentially forcing interoperability. In addition to this, it adds some security features not found in the client software, such as message encryption and logging. Unfortunately, because the product is somewhat limited to what the actual client software is capable of, not all of its features work when communicating with any one particular network. For example, the encryption features are only available when communicating with someone using the AOL instant messenger or ICQ, while certain presence features will only work for people who are not using AOL or ICQ. (Cerulean Studios, 2003) The product was not actually designed as an enterprise solution, but it does provide some nice features that can improve IM security to an extent. It is a middle of the road option with fewer features than an enterprise class product but costs less, and has more security than the standard client software.



## 4.4 Security Issues Summary

Security Issue	Sources of Security Risks	Possible Measures	Recommendation
Lack of Control	Consumer IM software often installed without company's permission. Users rather than the company control accounts for consumer IM networks. Company cannot monitor or log conversations.	EIM Implementation, User Policies	EIM software implementations can be used to gain more control over users and logging. The user policy should disallow the downloading of consumer IM clients without company permission.
Network Security	Consumer IM designed to breach network from within, can switch ports as necessary and disguise traffic as HTTP or other types of packets. Opens firewall ports when software is running, may allow hacker access to entire network.	EIM Implementation, Tighten Firewall Settings	EIM software can have additional security measures to prevent the unnecessary opening of firewall ports. The firewall can be tuned to make it more difficult for users to connect using consumer clients, but nearly impossible to eliminate.
Social Engineering	Hackers may employ clever tactics to trick users into downloading viruses and other malicious software, or giving away company secrets.	Educate Users, User Policies	Users should be educated to know what to be on the lookout for and how to handle situations. User policy should warn against downloading files through IM.
Viruses	Viruses can be spread through buddy lists. Hacker needs only a users screen name to send a virus. Trojan horse viruses may facilitate a hackers attempt to break into a system.	Install Antivirus Software	Antivirus software cannot scan the actual messages for viruses, but they can catch them when they reach the desktop. Gateway anti virus software is an option but may be too overwhelmed to be effective.
Lack of Encryption	Consumer IM clients send messages in plaintext and do not encrypt files sent using file transfer features. Intercepted messages would be easy to decipher.	EIM Implementation	Most enterprise IM packages encrypt their messages, transferred files, and logs. Standards may result in encryption being added to consumer clients.
Software Flaws	Bugs in the software can provide ways for intruders to break into a network. As software updates become available, old bugs may be fixed but new ones may be introduced.	Keep Software Updated	Install updates as soon as they become available. May take hackers some time to discover new bugs. Handle updates automatically to take responsibility away from users.

## 5 Conclusions

This project involved researching the current state of instant messaging technology, the security risks posed by its use, and the measures that can be taken to mitigate these risks. The intent was to understand the security issues of using instant messaging in enterprises, to determine preventative measures to counter these issues, and to explore the social implications of instant messaging use. The research was done primarily through the Internet, using various web news articles, editorials, white pages, and product pages.

It was found that there are numerous security issues with consumer instant messaging clients that make their use in enterprises a significant risk. Issues include a lack of control features, threats to network security, social engineering performed on users, vulnerability to viruses, lack of encryption for messages and transferred files, and software flaws that hackers may exploit to gain entry to a system. The biggest threat to come from these issues is likely the loss of confidential information.

The research also found that while there is no sure solution for the threats caused by unsecured instant messaging, there are a number of measures that can be taken to help lessen their effects. Measures include developing user policies, educating users on the threats of IM and how to deal with and avoid them, implementing secure EIM software packages, and proper maintenance of network security software such as antivirus and firewall programs.

It was discovered that there is currently a lack of instant messaging standards. This results in an incompatibility between the various instant messaging products that are available, and has caused some companies to decide to wait for standards to be developed

before implementing instant messaging. For the companies who are ready for instant messaging, there are many products available, each with their own unique approach to secure instant messaging, which should suit the needs of businesses of all types and sizes.

Instant messaging has tremendous potential. It is a technology that in the short term can improve productivity simply through facilitating communication and collaboration. In the long term it has the potential to become the primary means of communication in a business. This is in no small part due to its ability to bring communities together on a global scale, by breaking language, ethnic, gender, and even sociological barriers.

Instant messaging security is important to businesses, as IM has numerous security issues that can result in serious threats to the security of a company's network. Failure to deal with the security threats of instant messaging can result in a loss of confidential information, damage to a company's or employees reputation, or compromised network security. Only with knowledge of the nature of IM's security issues and of the measures available to lessen their effects will a company be able to deal with the threats of instant messaging.

IM can have significant productivity and communication benefits, but if instant messaging security threats are not dealt with, IM's reputation may become damaged, potentially resulting in a lack of faith in IM technology. If people do not believe in instant messaging technology, IM will never get the opportunity to reach its full potential.

## References

- AOL. 2003. Product Page: AIM Enterprise Gateway. Retrieved May 10, 2003, from [http://enterprise.netscape.com/products/aimsvcs/aimgateway\\_ds.html](http://enterprise.netscape.com/products/aimsvcs/aimgateway_ds.html)
- Barlas, Demir., Nov. 1, 2002. Is Instant Messaging Enterprise Ready? Retrieved March 23, 2003, from <http://www.destinationKM.com/articles/default.asp?articleid=1008>
- Brockmeier, Joe., March 11, 2003. IM To Storm the Enterprise. Retrieved April 6, 2003, from <http://www.newsfactor.com/perl/story/20969.html>
- Chediak, Mark., Sept. 7, 2001. Instant Messaging Gets Serious. Retrieved March 30, 2003, from <http://www.redherring.com/mag/issue103/1300020130.html>
- Clancy, Heather., Oct. 11, 2002. Instant Messaging, Spam Issues Linger. Retrieved March 23, 2003, from <http://www.crn.com/Components/printArticle.asp?ArticleID=37956>
- Communicator Inc. 2003. Product Page: Communicator Hub Services. Retrieved May 10, 2003, from <http://www.communicatorinc.com/Products.html>
- Cerulean Studios. 2003. Product Page: Trillian Pro. Retrieved May 10, 2003, from <http://www.ceruleanstudios.com/trillianpro/index.html>
- Dalton, Curtis E. & Kannengeisser, William., Aug. 2002. Instant Headache Retrieved March 23, 2003, from <http://www.infosecuritymag.com/2002/aug/cover.shtml>
- Dyson, Esther., Oct. 1, 2002. Technology Needs to Change Us. Retrieved May 4, 2003, from <http://www.cio.com/archive/100102/dyson.html?printversion=yes>
- Enbysk, Monte., Undated. 10 tips for using instant messaging for business. Retrieved March 30, 2003, from <http://www.bcentral.com/articles/enbysk/135.asp?format-print>
- Frase, Dan., Jan. 1, 2002. The Instant Messaging Menace: Security Problems In The Enterprise and Some Solutions. Retrieved March 23, 2003, from [http://www.sans.org/rr/threats/IM\\_menace.php](http://www.sans.org/rr/threats/IM_menace.php)
- Gaudin, Sharon., Aug. 9, 2002. IM Users Being Duped into Security Laxes Retrieved March 23, 2003, from [http://www.instantmessagingplanet.com/security/print.php/10818\\_1444011](http://www.instantmessagingplanet.com/security/print.php/10818_1444011)
- Gaudin, Sharon., Aug. 14, 2002. Norton Antivirus Tackles Instant Messaging. Retrieved March 30, 2003, from <http://siliconvalley.internet.com/news/print.php/1446911>

Hallett, Tony., Feb. 2, 2003. IM a Rampant Security Risk. Retrieved March 23, 2003 from <http://www.silicon.com/news/500013/14/2752.html>

Hillson, Isaac., Dec. 2, 2002. Enterprise Messaging: Pop-Up Productivity. Retrieved March 30, 2003, from <Http://www.commweb.com/article/COM20021121S0003>

Hindocha, Neal., 2003. Threats to Instant Messaging, Symantec Security Response White Paper. Retrieved March 23, 2003, from <http://securityresponse.symantec.com/avcenter/reference/threats.to.instant.messaging.pdf>

Hindocha, Neal., Jan. 13, 2003. Instant Insecurity: Security Issues of Instant Messaging. Retrieved March 23, 2003, from <http://www.securityfocus.com/infocus/1657>

IBM. 2003. Product Page: Sametime. Retrieved May 10, 2003, from <http://www.lotus.com/products/lotussametime.nsf/wdocs/homepage>

Langa, Fred., Oct. 1, 2001. More Instant Messaging Security Holes. Retrieved March 23, 2003 from [http://www.informationweek.com/shared/printableArticle?doc\\_id=IWK20010927S0021](http://www.informationweek.com/shared/printableArticle?doc_id=IWK20010927S0021)

Lowe, Scott., Feb. 1, 2002. Admins: Take control of your organization's IM services. Retrieved March 30, 2003, from <http://www.techrepublic.com/article.jhtml?id=r00220020129low01.htm&src=search>

Lyman, Jay., Jun. 18, 2002. IM, Therefore I'm Hacked. Retrieved March 30, 2003, from <http://www.osopinion.com/perl/printer/18260/>

McDonald, Tim., May 31, 2002. Instant Messaging Enterprise Security Ramps Up. Retrieved March 30, 2003, from <http://newsfactor.com/perl/printer/18008/>

Microsoft. April 9, 2003. Press Release: Microsoft Real-Time Communications Server 2003 To Offer More Secure, Manageable Instant Messaging for Enterprise. Retrieved May 4, 2003, from <http://www.microsoft.com/presspass/press/2003/Apr03/04-09RealTimePR.asp>

Moore, Cathleen., April. 18, 2003. XMPP Rises to Face SIMPLE Standard. Retrieved May 4, 2003, from [http://www.infoworld.com/article/03/04/18/16imstandards\\_1.html](http://www.infoworld.com/article/03/04/18/16imstandards_1.html)

Richardson, Robert, Feb. 6, 2002. Instant Messaging Goes to Work. Retrieved March 30, 2003, from [http://www.convergence.com/article/printableArticle?doc\\_id=CMT20020205S0005](http://www.convergence.com/article/printableArticle?doc_id=CMT20020205S0005)

Saunders, Christopher., April 10, 2003. Microsoft: Greenwich On Schedule. Retrieved May 4, 2003, from <http://www.instantmessagingplanet.com/enterprise/print.php/2184241>

Stewart, Quinn., Jul. 9, 2001. History of Instant Messaging. Retrieved April 6, 2003, from <http://www.gslis.utexas.edu/~lis3121e/restrict/im/im1.html>

Symantec Enterprise Security. 2003. Securing Instant Messaging, White Paper. Retrieved March 23, 2003, from <http://securityresponse.symantec.com/avcenter/reference/secure.instant.messaging.pdf>

Vamosi, Robert., May 30, 2002. The next hacker target: Instant Messaging. Retrieved March 23, 2003, from <http://zdnet.com.com/2102-1107-928415.html>

Weinberger, David., March 28, 2002. Instant Business Managing. Retrieved March 30, 2003, from <http://www.darwinmag.com/read/swiftkick/column.html?ArticleID=293>

Woods, Bob., Jun. 24, 2002. Study: Instant Messaging Use Is A Big Security Threat. Retrieved March 23, 2003, from <http://www.smallbusinesscomputing.com/webmaster/print.php/1369981>